NORME TEHNICE ŞI METODOLOGICE PENTRU APLICAREA LEGII PRIVIND SEMNĂTURA ELECTRONICĂ

CAPITOLUL I – Dispoziţii generale

Art.1 Orice persoană, fizică sau juridică, aflată pe teritoriul României poate beneficia de servicii de certificare în vederea utilizării semnăturii electronice în sensul definit de art. 4 din Legea nr. 455/2001 privind semnătura electronică, denumită în continuare *legea*.

Art. 2 (1) În înţelesul prezentelor norme, termenii utilizaţi au următoarele definiţii:

a) *Client* – beneficiarul serviciilor de certificare care, în baza unui contract încheiat cu un furnizor de servicii de certificare, denumit în continuare *furnizor*, deţine o pereche cheie publică – cheie privată şi are o identitate probată printr-un certificat digital emis de acel *furnizor*.

b) *Hash-code* – funcţie care returnează amprenta unui document electronic.

c) *Cheie privată* - un cod digital, cu caracter de unicitate, generat printr-un dispozitiv hardware şi / sau software specializat. În contextul semnăturii digitale, cheia privată reprezintă datele de creare a semnăturii electronice, aşa cum apar ele definite în *lege*.

d) *Cheia publică* - cod digital, perechea cheii private necesară verificării semnăturii electronice. În contextul semnăturii digitale, cheia publică reprezintă datele de verificare a semnăturii electronice, aşa cum apar ele definite în *lege*.

e) *Mecanismul de creare a semnăturii electronice:* Asupra documentului se aplică o funcţie hash-code, obţinându-se amprenta documentului. Printr-un algoritm, se aplică cheia privată peste amprenta documentului, rezultând semnătura electronică.

f) *Mecanismul de verificare a semnăturii electronice* se bazează pe utilizarea cheii publice, a funcţiei hash-code şi a semnăturii electronice primite. Verificarea semnăturii este o operaţie automată.

g) *Pagina web* – document electronic, disponibil prin Internet.

(2) În înţelesul prezentelor norme, abrevierile utilizate au următoarele semnificaţii:

a) *ETSI* – Institutul European de Standarde în Telecomunicaţii

b) *RFC* – desemnează documente care au fost supuse analizei publice în cadrul unui proces coordonat de Grupul de Lucru pentru Ingineria Internetului.

c) *FIPS* – desemnează standarde federale emise de Institutul Naţional de Standarde şi Tehnologie din Statele Unite ale Americii.

d) *IEEE* – Institutul de Inginerie Electrică şi Electronică.

e) *ITSEC* – desemnează standardele şi criteriile europene de evaluare a securităţii sistemelor informatice.

f) *RSA* – algoritmul de criptare cu cheie publică, dezvoltat de cercetătorii Rivest, Shamir şi Adleman.

g) *DSA* – Algoritmul de Semnătură Digitală.

h) *SHA* – Algoritm Securizat de Hash-code.

i) *PKI* – Infrastructură de chei publice.

j) *RTF* – format de document ce permite alinierea textului, introducerea unor caractere speciale, utilizarea culorilor şi a fonturilor de dimensiuni diferite, precum şi inserarea altor obiecte.

k) *PDF* – format ce permite transferarea documentelor electronice fără a afecta aranjarea în pagină; documentele pot conține text, imagini şi sunete.

l) *PostScript* – format de document utilizat în special pentru tipărire la imprimante PostScript.

m) *TXT* – format de document conținând exclusiv text.

CAPITOLUL II - Autoritatea de Reglementare şi Supraveghere

Art. 3 (1) Autoritatea de Reglementare şi Supraveghere, denumită în continuarea *autoritate* îşi generează sau achiziționează o pereche funcțională, cheie privată – cheie publică, şi trebuie să îşi protejeze cheia sa privată, utilizând un sistem fiabil şi luând precauțiile necesare pentru a preveni pierderea, dezvăluirea, modificarea sau utilizarea neautorizată a cheii sale private.

(2) Cheia privată nu poate fi dedusă în nici un fel din cheia sa publică pereche.

Art. 4 *Autoritatea* gestionează Registrul Furnizorilor de Servicii de Certificare, denumit în continuare *registrul*.

Art. 5 Conținutul informațional şi structura *registrului* sunt prezentate în anexa nr. 1.

Art. 6 (1) Actualizarea *registrului* se face exclusiv de către *autoritate* şi urmăreşte toate modificările survenite în statutul *furnizorului* - acreditare, terminarea perioadei de acreditare, suspendare, îmbogățirea tipurilor de certificate oferite.

(2) După fiecare actualizare, *autoritatea* transmite *furnizorului* o copie a documentului prevăzut la pct. 43 din anexa nr. 1.

Art. 7 *Autoritatea* gestionează datele utilizând un sistem informatic în măsură să asigure securitatea sistemelor, comunicațiilor, tranzacțiilor şi datelor conform standardelor recunoscute - ISO/IEC 15408-1,2,3 şi ISO 17799. În acest sens, se utilizează o soluție ce asigură managementul unei baze de date replicate, garantându-se accesul permanent, prin Internet.

Art. 8 *Autoritatea* face publice, spre consultare, următoarele date din *registru*:

a) Tip furnizor - persoană fizică sau juridică
b) Numele sau denumirea *furnizorului*
c) Data la care şi-a început activitatea
d) Cheia publică a furnizorului
e) Indicații privind acreditarea - acreditat sau neacreditat
f) Perioada de acreditare - început / sfârşit
g) Indicații privind dreptul de a emite certificate calificate
h) Descrierea politicii generale a *furnizorului*
i) Forma de organizare a *furnizorului* – societate comercială, regie autonomă, instituție publică,

organizație non-guvernamentală, alte tipuri

j) Adresa sau sediul - țară, oraş, județ / sector, stradă, număr, bloc, scară, etaj, apartament, cod poştal

k) Naționalitate, pentru persoană juridică

l) Cetățenie, pentru persoană fizică

m) Telefon, fax, email, adresă pagină web

n) Categoriile de servicii destinate publicului: tipul de certificate, mod de utilizare, pentru fiecare tip de certificate în parte

o) Tipurile de dispozitive de creare a semnăturii electronice utilizate

p) Situația dispozitivelor - dacă sunt sau nu omologate

q) Situația furnizorului: operațional, suspendat, activitatea încetată, în curs de transferare a activității, în curs de remediere a unor probleme identificate de *autoritate* - indicând termenul limită

r) Istoric al furnizorului: data de începere a activității, perioade de suspendare, perioade în care a avut dreptul de a emite certificate calificate, alte asemenea situații.

Art. 9 (1) Informațiile prevăzute în art. 8 din prezentele norme sunt disponibile public, prin Internet, în pagina web a *autorității*.

(2) Pagina web va mai conține informații cu privire la legea semnăturii electronice, normele tehnice şi metodologice privind aplicarea semnăturii electronice, informații generale cu privire la utilizarea semnăturii electronice, informații noi din domeniul semnăturii electronice, trimiteri către paginile web ale furnizorilor de servicii de certificare.

(3) *Autoritatea* va publica permanent tehnologiile Internet prin care se pot consulta informațiile prevăzute la alin. (1) şi (2).

CAPITOLUL III - Furnizorii de Servicii de Certificare

Secțiunea 1 – Dispoziții comune

Art. 10 (1) Un furnizor de servicii de certificare este obligat să genereze sau să achiziționeze o pereche funcțională cheie privată – cheie publică, şi să-şi protejeze cheia sa privată, utilizând un sistem fiabil şi luând precauțiile necesare pentru a preveni pierderea, dezvăluirea, modificarea sau utilizarea neautorizată a cheii sale private.

(2) Cheia privată nu poate fi dedusă în nici un fel din cheia sa publică pereche.

Art. 11 (1) Înainte de începerea activității, *furnizorul* va notifica *autoritatea*, conform formularului prevăzut în anexa nr. 2.

(2) Toate datele vor fi înaintate *autorității* pe suport de hârtie şi în format electronic, documentul electronic fiind semnat digital de către *furnizor* şi prezentat în unul din următoarele formate: RTF, PDF, TXT şi PostScript.

Art. 12 (1) Înregistrarea în *registru* se face pe baza unei cereri individuale.

(2) La primirea cererii, *autoritatea* include datele *furnizorului* în *registru* şi generează pentru acesta un cod de identificare format prin alipirea anului, lunii şi datei de începere a activității şi a numărului de ordine al *furnizorului*.

Secţiunea a 2-a – Furnizarea serviciilor de certificare calificată

Art. 13 (1) *Furnizorul* poate furniza servicii de certificare bazate pe certificate simple şi calificate.

(2) Certificatul calificat va avea structura conformă cu anexa nr. 3, potrivit ETSI TS 101 862 v.1.2.1. (2001-06), RFC 2459, Recomandările ITU-T X.509.

(3) *Autoritatea* va publica eventualele modificări ale formatului descris, pe baza evoluţiei tehnologiilor sau a normele internaţionale recunoscute în domeniu.

(4) Certificatul are şi o rubrică de extensii. Lista celor mai uzuale extensii este dată în anexa nr. 4.

(5) Codul de identificare a certificatului calificat se formează prin alipirea codului de identificare al *furnizorului* şi a numărului de ordine al certificatului.

(6) Codul personal de identificare a semnatarului rezultă prin alipirea codului de identificare al *furnizorului*, iniţialele numelui sau pseudonimului semnatarului şi numărul de ordine al acestuia în lista clienţilor cu aceleaşi iniţiale.

Art. 14 (1) În vederea emiterii de certificate calificate, *furnizorul* trebuie să îndeplinească condiţiile enunţate în art.20-22 din *lege*.

(2) *Furnizorul* trebuie să dovedească *autorităţii* că dispune de resursele financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfăşurării activităţii de certificare şi trebuie să fie capabil să acopere pierderile suferite de către o persoană care îşi întemeiază conduita pe efectele juridice ale certificatelor calificate, până la concurenţa echivalentului în lei a sumei de 10.000 de Euro pentru fiecare risc asigurat. Riscul asigurat este fiecare prejudiciu produs, chiar dacă se produc mai multe asemenea prejudicii ca urmare a neîndeplinirii de către furnizor a unei obligaţii prevăzute de *lege*. *Furnizorul* va trebui să depună o scrisoare de garanţie din partea unei instituţii financiare de specialitate sau o poliţă de asigurare la o societate de asigurări, în favoarea *autorităţii*, în valoare cel puţin egală cu echivalentul în lei al sumei de 500.000 de Euro; scrisoarea de garanţie are forma din anexa nr. 5.

(3) *Furnizorul* trebuie să asigure un nivel de securitate a sistemelor, comunicaţiilor, tranzacţiilor şi datelor conform standardelor recunoscute - ISO/IEC 15408-1,2,3; ISO 17799; ETSI TS 101 456 v1.1.1 (2000-12); ITSEC-E3; FIPS 140-1.

(4) *Furnizorul* trebuie să asigure operarea rapidă a registrului de evidenţă a certificatelor, conform art. 20 lit. b) din lege; structura registrului este dată în anexa nr. 6.

(5) *Furnizorul* trebuie să folosească numai dispozitive securizate de creare a semnăturii electronice.

(6) *Autoritatea* verifică datele conţinute în documentaţia depusă, în termen de maximum 10 zile, în raport cu standardele recunoscute şi cu prezentele norme tehnice şi metodologice.

(7) *Autoritatea* trebuie să informeze *furnizorul*, în termen de maximum 10 zile, cu privire la îndeplinirea condiţiilor şi să solicite, dacă e cazul, completarea documentaţiei.

(8) În cazul în care toate criteriile sunt îndeplinite, *autoritatea* emite decizia prin care *furnizorul* dobândeşte dreptul de a furniza servicii de certificare calificată şi actualizează *registrul* înscriind noul statut al *furnizorului*. Decizia este comunicată *furnizorului* pe suport de hârtie şi în format electronic, semnat digital de *autoritate*.

(9) Dacă documentaţia nu a fost completată sau nu îndeplineşte condiţiile, *autoritatea* emite o decizie

motivată, prin care respinge solicitarea *furnizorului* de a i se acorda dreptul de furnizare de servicii de certificare calificată. Decizia este comunicată *furnizorului* pe suport de hârtie şi în format electronic, semnat digital de *autoritate*.

Art. 15 În cazul în care nu mai sunt îndeplinite condiţiile prevăzute în art.20-22 din *lege*, *autoritatea* va lua decizia de suspendare a dreptului *furnizorului* în cauză de a emite certificate calificate, până la remedierea neajunsurilor şi îndeplinirea tuturor condiţiilor legale. Decizia este comunicată *furnizorului* pe suport de hârtie şi în format electronic, semnat digital de *autoritate*.

Secţiunea a 3-a - Acreditarea voluntară

Art. 16 (1) *Furnizorul* care doreşte să-şi desfăşoare activitatea ca furnizor acreditat trebuie să solicite obţinerea acreditării din partea *autorităţii*.

(2) În acest sens, *furnizorul* trebuie să îndeplinească toate condiţiile necesare emiterii de certificate calificate şi să utilizeze dispozitive securizate de generare a semnăturii electronice omologate de o agenţie de omologare agreată de *autoritate*.

(3) Verificările se fac atât asupra declaraţiilor conţinute în documentaţia depusă la *autoritate* cât şi asupra concordanţei dintre sistemele, procedurile şi practicile afirmate şi cele existente în realitate.

(4) Auditul este realizat de *autoritate* sau de o terţă parte numită de aceasta, conform normelor europene pentru acest gen de activitate.

(5) *Autoritatea* trebuie să informeze *furnizorul*, în termen de maximum 30 de zile, cu privire la îndeplinirea condiţiilor şi să solicite, dacă e cazul, completarea documentaţiei.

Art. 17 (1) În cazul în care se constată că toate criteriile sunt îndeplinite, *autoritatea* decide acreditarea *furnizorului*.

(2) Decizia de acreditare, condiţiile şi efectele suspendării sau ale retragerii, sunt comunicate *furnizorului* pe suport de hârtie şi în format electronic, semnat digital de *autoritate*.

(3) La cererea *furnizorului*, *autoritatea* actualizează *registrul* prin înscrierea noul statut de furnizor acreditat. Se introduc informaţii despre garanţii, omologarea dispozitivelor, agenţia de omologare, perioada de acreditare.

Art. 18 (1) Durata acreditării este de 3 ani şi se poate reînnoi.

(2) Procedura de reînnoire este identică cu cea de obţinere a acreditării.

Art. 19 Suspendarea deciziei de acreditare se face în următoarele cazuri:

a) se constată că furnizorul nu mai îndeplineşte una sau mai multe din condiţiile prevăzute pentru acordarea deciziei de acreditare. În acest caz, *autoritatea* notifică *furnizorul* şi stabileşte un interval de timp de maximum 30 de zile în care *furnizorul* trebuie să remedieze deficienţele semnalate.

b) declanşarea procedurii falimentului furnizorului de servicii de certificare.

Art. 20 *Autoritatea* retrage decizia de acreditare în următoarele cazuri:

a) dacă *furnizorul* nu remediază deficienţele prevăzute la art. 19 lit. a din prezentele norme tehnice şi metodologice, în termenul acordat de către *autoritate*.

b) dacă intervine o hotărâre judecătorească definitivă şi irevocabilă prin care se declară falimentul *furnizorului.*

Secțiunea a 4-a – Agrearea agențiilor de omologare

Art. 21 (1) Decizia de agreare a agențiilor de omologare se face pe baza unei cereri a agenției către *autoritate* şi în urma verificării condițiilor menționate în normele europene pentru acest gen de activitate.

(2) Decizia de agreare este valabilă 1 an şi se poate reînnoi.

(3) Decizia se retrage în cazul în care se constată că agenția nu mai îndeplineşte condițiile prevăzute la alin. (1) şi (2). *Autoritatea* transmite agenției o notă explicativă în care descrie motivele retragerii deciziei de agreare.

CAPITOLUL IV – Proceduri de utilizare a semnăturii electronice

Art. 22 Principiul de funcționare şi procedurile de utilizare a semnăturii electronice sunt prevăzute în anexa nr. 7.

Art. 23 Orice persoană, fizică sau juridică, care doreşte ca un *furnizor* să-i elibereze un certificat trebuie:

a) să furnizeze informațiile cerute pentru tipul de certificat dorit, conform formularului prevăzut în anexa nr. 8.
b) să genereze sau să achiziționeze o pereche cheie privată - cheie publică; cheia privată nu poate fi dedusă în nici un fel din cheia sa publică pereche.
c) să probeze funcționalitatea perechii cheie privată – cheie publică;
d) să protejeze cheia privată de furturi, deteriorări, modificări ale conținutului sau alte compromiteri ale acesteia; este interzisă duplicarea cheii private;
e) să propună un nume sau un pseudonim distinct pentru identificare;
f) să supună examinării *furnizorului*: cererea de furnizare a unui certificat, acordul de a respecta obligațiile în calitate de client şi cheia sa publică.

Art. 24 La primirea cererii de eliberare a certificatului, *furnizorul* în cauză va verifica, înainte de eliberarea certificatului, următoarele aspecte:

a) dacă solicitantul certificatului este persoana identificată în cerere, prin procedura adecvată categoriei din care face parte certificatul;
b) dacă solicitantul certificatului deține cheia privată corespunzătoare cheii publice listată în certificat;
c) dacă informația listată în certificat este exactă;

Art. 25 (1) Durata verificării informațiilor din cerere şi a eliberării certificatului nu poate depăşi:

a) 1 zi lucrătoare, pentru certificatele simple;
b) 5 zile lucrătoare, pentru certificatele calificate.

(2) Termenele prevăzute la lit. a) şi b) se calculează din momentul primirii de către *furnizorul* în cauză a tuturor informațiilor cerute pentru acest scop.

Art. 26 *Furnizorul* de certificare nu poate emite un certificat fără consimțământul expres al celui pe numele căruia este emis.

Art. 27 Durata valabilității unui certificat, de la data comunicării către client, este de maximum 1 an.

Art. 28 Certificatul poate fi transmis solicitantului în următoarele modalități:

a) personal;
b) prin poştă, cu confirmare de primire;
c) prin poştă electronică - numai pentru certificate simple; observațiile, dacă există, se comunică pe aceeaşi cale *furnizorului*;

Art. 29 Prin acceptarea certificatului, clientul:

a) îşi asumă responsabilitatea controlului cheii sale private şi a luării unor măsuri pentru a preveni pierderea, dezvăluirea, modificarea sau utilizarea neautorizată a acesteia;
b) certifică veridicitatea informațiile conținute în certificat;
c) se angajează să folosească certificatul exclusiv în scopuri autorizate, conform *legii*;
d) nu are dreptul de a utiliza cheia sa privată corespunzătoare cheii publice listată în certificat pentru semnarea altor certificate, decât în cazurile în care acest lucru a fost prevăzut expres în contractul semnat cu furnizorul său de certificare.

Art. 30 (1) *Furnizorul* gestionează direct cheile publice ale clienților - persoane fizice şi persoane juridice. Gestionarea cheilor publice presupune, implicit, acordarea tuturor serviciilor de certificare prevăzute în contractul cu clienții.

(2) Serviciile de certificare se referă la emiterea, verificarea, suspendarea, reînnoirea, revocarea, şi furnizarea de informații cu privire la certificatele emise, precum şi depozitarea sigură a acestora pe durata valabilității lor, la care se adaugă o perioadă de minimum 10 ani de la data încetării valabilității certificatului, conform prevederilor art. 20 lit. h) din *lege*.

(3) Serviciile de verificare a semnăturilor electronice se asigură automat, prin Internet, asemenea servicii fiind menționate expres în contract.

Art. 31 (1) Arhivele unui *furnizor* aflat în cazul prevăzut la art. 24 alin. (4) din *lege* sunt preluate de *autoritate.*

(2) Formularul de informare cu privire la încetarea activității unui furnizor de servicii de certificare este prevăzut în anexa nr. 9.

(3) În cazul în care *autoritatea* dispune încetarea activității unui *furnizor* şi nu există un alt furnizor care să-i preia activitatea, aceasta va asigura revocarea certificatelor, dacă nu a fost deja realizată de către *furnizor*, pe cheltuiala *furnizorului*; va prelua şi va menține arhivele şi registrul electronic, fără conectare permanentă la Internet.

Art. 32 Un *furnizor* poate solicita unui alt *furnizor* eliberarea unui certificat, cel de-al doilea *furnizor* gestionând astfel cheia publică a primului. Această situație este prevăzută în anexa nr. 10.

CAPITOLUL V – Detalii tehnice

Secțiunea 1 - Datele de creare a semnăturii

Art. 33 Generarea datelor de creare a semnăturii electronice a *autorității* se face utilizând un sistem izolat, fiabil, proiectat special în acest scop, protejat împotriva utilizării neautorizate.

Art. 34 *Autoritatea* va folosi pentru semnătura electronică algoritmul RSA.

Art. 35 (1) Lungimea minimă a cheii private utilizate de un semnatar pentru crearea semnăturii electronice extinse trebuie să fie de minim:

a) 1024 de biți pentru algoritmul RSA;

b) 1024 de biți pentru algoritmul DSA;

c) 160 de biți pentru algoritmul DSA bazat pe curbe eliptice.

(2) Lungimea nu include secvența de biți 0 de pe cele mai semnificative poziții.

(3) Generarea repetată de date de creare a semnăturii electronice nu trebuie să coboare nivelul de siguranță a acesteia – fiind obligatorie condiția de unicitate. Se exclud procedeele de generare a datelor de creare a semnăturii electronice care, prin utilizare repetată, ar putea reduce calitatea cheii.

Art. 36 (1) Numărul minim de biți din datele de creare a semnăturii electronice determinați pe baza unor numere real aleatoare tehnice este de:

a) 1024 de biți pentru algoritmul RSA;

b) 1024 de biți pentru algoritmul DSA;

c) 160 de biți pentru algoritmul DSA bazat pe curbe eliptice.

(2) Este interzisă utilizarea numerelor pseudo-aleatoare ca punct de pornire în generarea datelor de creare a semnăturii.

(3) Dacă sistemul de generare este utilizat pentru obținerea cheilor mai multor semnatari, calitatea elementelor generate trebuie verificată statistic cel puțin o dată pe lună. Rezultatele testelor efectuate trebuie înregistrate. În cazul în care rezultatul testului este negativ, toate certificatele emise de la data ultimului test vor fi revocate.

Art. 37 (1) Dacă datele de creare a semnăturii sunt generate de furnizorul de servicii de certificare, acesta trebuie să asigure confidențialitatea acestora, precum şi a datelor pe baza cărora s-au generat cheile.

(2) Aceleaşi prevederi se aplică în cazul operațiunilor de transferare a datelor de creare a semnăturii în dispozitivele de creare a semnăturii, precum şi datelor de identificare a semnatarului necesare în cazul utilizării dispozitivului.

Art. 38 Dacă datele de creare a semnăturii sunt generate de un terț, acesta trebuie să utilizeze dispozitive de generare fiabile, protejate împotriva utilizării neautorizate. Fiecare acces la dispozitivul de generare a datelor de creare a semnăturii trebuie monitorizat.

Secţiunea a 2-a – Sisteme şi proceduri utilizate pentru crearea semnăturii electronice

Art. 39 *Autoritatea* foloseşte doar funcţia hash-code SHA-1 şi algoritmul de criptare RSA. Este interzisă utilizarea teoremei chinezeşti a resturilor.

Art. 40 (1) În vederea obţinerii unei semnături electronice extinse, se pot utiliza următoarele funcţii hash-code:

a) RIPEMD – 160

b) Funcţia SHA-I

(2) Pot fi folosite numere pseudo-aleatoare pentru a mări lungimea amprentei documentului. Algoritmii de criptare a amprentei, în cazul semnăturii electronice extinse, sunt:

a) RSA

b) DSA

c) DSA pe curbe eliptice potrivit ISO/IEC 14883-3, anexa A.2.2, IEEE standard P1363, secţiunile 5.3.3, 5.3.4

(3) În cazul algoritmilor ce implică numere aleatoare, se pot utiliza numere pseudo-aleatorii.

(4) Se consideră echivalente şi alte proceduri de creare a semnăturii, dacă oferă acelaşi nivel de securitate, certificat de un organism autorizat recunoscut.

Art. 41 Dacă pentru declanşarea procedurii de creare a semnăturii electronice se foloseşte o metodă de acces, anume proiectată pentru a preveni utilizarea neautorizată, codul respectiv nu mai trebuie folosit în alt scop.

Art. 42 Formatul semnăturii electronice trebuie să corespundă prevederilor legale în domeniu - PKCS#7 Standard de sintaxă al mesajelor criptate.

Art. 43 Rezultatul verificării unei semnături electronice extinse este sigur doar dacă se utilizează un dispozitiv de verificare a semnăturii electronice specificat de către furnizorul de servicii de certificare care a emis certificatul pe baza căruia se face validarea semnăturii.

Secţiunea a 3-a - Certificatele calificate

Art. 44 În cazul reînnoirii unui certificat calificat se emite un nou certificat, cu aceleaşi date de identificare şi de verificare a semnăturii electronice, dar cu alte date de valabilitate.

Art. 45 Formatul certificatului calificat, conform art. 13 din prezentele norme, trebuie să fie descris de către furnizor utilizând un limbaj formal standard - CCITT sau Recomandărilor ITU-T X.208 -, într-un document ataşat notificării către *autoritate*.

Art. 46 Registrul electronic de evidenţă a certificatelor eliberate trebuie să corespundă unui format recunoscut internaţional. Următoarele standarde sunt recomandate:

a) 1988 CCITT (ITU-T) X.500 / ISO IS9594

b) RFC 2587 Internet X.509 Infrastructura de chei publice LDAPv2

c) RFC 2587 Internet X.509 Infrastructura de chei publice - certificate şi profil CRL

d) RFC 2589 - LDAPv3 Extensii pentru servicii de director dinamic

Secţiunea a 4-a - Revocarea certificatelor şi marcarea timpului

Art. 47 *Furnizorul* trebuie să informeze clienţii şi terţii care pot influenţa atributele clientului înscrise în certificatul calificat, cu privire la modul prin care pot solicita revocarea certificatului.

Art. 48 (1) Marca temporală dovedeşte existenţa unor date la un moment de timp precizat.
(2) Prin aplicarea unei astfel de mărci, numită time-stamp, se poate demonstra existenţa unor informaţii la momentul respectiv.
(3) Serviciile de marcare temporală pot fi furnizate de *furnizor* sau de terţi conform standardelor recunoscute - ETSI TS 101 861 Ştampilare temporală; ETSI TS 101 733 v1.2.2 (2000-12); RFC3161 Internet X.509 PKI Protocol de ştampilare temporală.
(4) În vederea menţionării datei şi a orei, se utilizează servicii bazate pe certificate calificate şi se foloseşte data şi ora Europei Centrale, ţinându-se seama de schimbarea orei - ora de vară / iarnă. Eroarea maximum admisă este de 1 minut.

CAPITOLUL VI - Alte prevederi

Art. 49 *Autoritatea* trebuie să verifice un *furnizor* cel puţin o dată la 2 ani sau când se modifică procedurile de lucru.

Art. 50 (1) *Autoritatea* dispune suspendarea activităţii *furnizorului,* până la încetarea cauzelor care au determinat luarea măsurii în următoarele situaţii:

a) *Furnizorul* a încălcat obligaţiile de confidenţialitate prevăzute la art. 15 alin. (1) din *lege*
b) Nu notifică *autoritatea* în condiţiile prevăzute la art. 13 alin. (1) şi (2) din *lege*
c) Complementar cu aplicarea sancţiunii contravenţionale prevăzute la art. 45 din *lege*
d) *Furnizorul* nu plăteşte în termenul stabilit despăgubirile la plata cărora a fost obligat printr-o decizie definitivă şi irevocabilă a unei instanţe judecătoreşti
e) *Furnizorul* nu achită, în cel mult 10 zile, costul operaţiunilor prevăzute la art. 31 alin (3) din prezentele norme tehnice şi metodologice.

(2) În această perioadă, *autoritatea* efectuează verificarea *furnizorului* şi comunică neajunsurile identificate. *Autoritatea* stabileşte un interval de timp de maxim 30 de zile în care *furnizorul* trebuie să rezolve problemele cu care se confruntă.
(3) Dacă *furnizorul* nu remediază deficienţele în termenul acordat, *autoritatea* dispune încetarea activităţii *furnizorului* şi / sau retragerea deciziei de acreditare şi / sau suspendarea dreptului de a emite certificate calificate, în funcţie de problemele identificate şi tipul de servicii oferite de *furnizor*.
(4) În perioada în care are activitatea suspendată, *furnizorul* are obligaţia să asigure serviciile de suspendare, revocare şi verificare a certificatelor, precum şi consultarea prin Internet a registrului electronic, cu excepţia cazului în care deficienţele se găsesc la nivelul acestor sisteme.

Art. 51 În cazurile prevăzute la art. 50, alin. (1), lit. d) şi e), din prezentele norme tehnice şi metodologice, *autoritatea* are dreptul de a emite pretenţii asupra scrisorii de garanţie sau a poliţei de asigurare, în limita prejudiciului creat.

Art. 52 (1) Dispozitivele de creare a semnăturii electronice constituie produse asociate semnăturii electronice, în sensul art. 4 pct. 15 din *lege*.

(2) Produsele asociate semnăturii electronice sunt prezumate a îndeplini condiţiile prevăzute la art. 4 pct. 8 şi art. 20 lit. f) din *lege* în cazul în care sunt conforme cu cel puţin unul dintre:

a) standardele române, sau părţile relevante ale acestora, care adoptă acele standarde europene armonizate ale căror numere de referinţă au fost publicate în Jurnalul Oficial al Comunităţilor Europene, în măsura în care condiţiile în cauză sunt acoperite de aceste standarde;
b) standardele europene armonizate ale căror numere de referinţă au fost publicate în Jurnalul Oficial al Comunităţilor Europene, în măsura în care condiţiile în cauză sunt acoperite de aceste standarde;
c) standardele române, sau părţile relevante ale acestora, adoptate potrivit dispoziţiilor legale în vigoare, în măsura în care condiţiile în cauză sunt acoperite de aceste standarde şi nu există standarde române din categoria celor prevăzute la lit. a) care să fie aplicabile.

(3) Lista standardelor prevăzute la alin. (2) se publică prin ordin al ministrului comunicaţiilor şi tehnologiei informaţiei.

Art.53 Dispozitivele securizate de creare a semnăturii electronice, recunoscute ca fiind conforme cu cerinţele anexei III a Directivei 1999/93/EC, de un organism desemnat de unul din statele membre ale Uniunii Europene să efectueze determinări ale conformităţii acestor dispozitive, sunt considerate omologate în sensul art. 11 alin. (2) din *lege*.

Art. 54 În conformitate cu art. 40 din *lege*, certificatul calificat eliberat de către un *furnizor* înregistrat într-unul din statele membre ale Uniunii Europene este recunoscut ca fiind echivalent din punct de vedere al efectelor juridice cu certificatul calificat eliberat de un furnizor de servicii de certificare cu domiciliul sau cu sediul în România în baza acordului european de asociere între România pe de o parte şi Comunitatea Europeană şi statele membre pe cealaltă parte.

Art. 55 Anexele nr. 1 – 10 fac parte integrantă din prezentele norme tehnice şi metodologice.

Anexa nr. 1

Domeniu	Semnătura electronică	*Cod domeniu*	SMEL
Titlu document	**CONȚINUTUL INFORMAȚIONAL ŞI STRUCTURA REGISTRULUI FURNIZORILOR DE SERVICII DE CERTIFICARE PENTRU SEMNĂTURA ELECTRONICĂ**	*Cod document*	01
		Pag	2

1.	Numărul de ordine al înregistrării, generat automat
2.	Cod de identificare furnizor (FSC)
3.	Tip furnizor (persoană fizică / juridică)
4.	Denumirea societății comerciale / Nume furnizor (pentru persoană fizică)
5.	Data la care a început activitatea
6.	Cheia publică a furnizorului
7.	Indicații privind acreditarea (acreditat / neacreditat)
8.	Perioada de acreditare (început / sfârşit)
9.	Indicații privind dreptul de a emite certificate calificate
10.	Descrierea politicii generale a FSC
11.	Descrierea sistemelor FSC
12.	Codul de proceduri şi practici al FSC
13.	Forma de organizare a societății (SA / SRL / Regie Autonomă / Instituție publică, organizație non-guvernamentală, alte tipuri)
14.	Adresa (țară, oraş, județ / sector, stradă, număr, bloc, scară, etaj, apartament, cod poştal);
15.	Naționalitate
16.	Cetățenie
17.	Telefon, fax, email, adresă pagină web
18.	Cod registrul comerțului / Cod fiscal (pentru persoană juridică)
19.	Banca furnizorului
20.	Numărul contului bancar al furnizorului
21.	Tipul garanției furnizorului
22.	Societatea de asigurări / Instituție financiară care garantează capacitatea financiară a furnizorului
23.	Suma asigurată / Suma acoperită prin scrisoarea de garanție
24.	Atribute certificat de bonitate: număr act, data, eliberat de…, verificat de…, data / ora verificării
25.	Atribute scrisoare de garanție: număr act, data, eliberat de…, verificat de…, data / ora verificării
26.	Atribute contract de asigurare: număr act, data, eliberat de…, verificat de…, data / ora verificării
27.	Atribute contract de închiriere sediu: număr act, data, eliberat de…, verificat de…, data / ora verificării
28.	Atribute act de proprietate sediu: număr act, data, eliberat de…, verificat de…, data / ora verificării
29.	Atribute adeverință privind datoriile către stat: număr act, data, eliberat de…, verificat de…, data / ora verificării, eliberată de banca prin care firma desfăşoară plăți şi încasări curente.
30.	Categoriile de servicii destinate publicului (tipul de certificate şi procedurile de securitate utilizate, structura certificatelor, mode de utilizare, pentru fiecare tip de certificate în parte)
31.	Tipurile de dispozitive de creare a semnăturii electronice utilizate
32.	Situația dispozitivelor (dacă sunt sau nu omologate)
33.	Agenția de omologare (dacă e cazul)
34.	Atribute atestare tehnică FSC: număr act, data, eliberat de…, verificat de…, data / ora verificării
35.	Situații critice: câmp ce poate conține referiri la ultima situație critică (de exemplu întreruperea temporară a activității FSC din cauza unor probleme tehnice, modificarea procedurilor FSC, sancțiuni etc)
36.	Data şi ora ultimei actualizări
37.	Data şi ora ultimei verificări
38.	Situația furnizorului (operațional, suspendat, activitatea încetată, în curs de transferare a activității, în curs de remediere a unor probleme identificate de ARS - indicând termenul limită)
39.	Motivul suspendării / reluării / încetării activității (dacă e cazul)
40.	FSC care preia gestiunea certificatelor (în cazul încetării activității furnizorului)
41.	Declarație ce confirmă exactitatea informațiilor de mai sus, semnat electronic de către FSC sau / şi ARS
42.	Identitatea operatorului din partea ARS care a introdus / modificat / şters înregistrare
43.	Un document, înglobând toate datele anterioare, semnat electronic de operatorul din partea MCTI care a introdus înregistrarea.

La punctele 10, 11 şi 12, *Furnizorul* trebuie să se refere la:

(a) procedura de solicitarea a certificatului

(b) tipuri de pseudonime admise - dacă e cazul

(c) metoda de includere în certificat a atributelor suplimentare

(d) orele de program

(e) modul de generare a datelor de creare a semnăturii furnizorului

(f) formatul datelor de creare a semnăturii furnizorului

(g) procedura de generare a datelor de creare a semnăturii clienţilor

(h) formatul datelor de creare a semnăturii clienţilor

(i) funcţiile hash şi procedurile de criptare folosite

(j) lista produselor asociate semnăturii electronice folosite şi recomandate

(k) formatul documentelor ce pot fi semnate electronic

(l) formatul şi perioada de valabilitate a certificatelor

(m) standarde tehnice şi metode de acces la registrul electronic de evidenţă a certificatelor eliberate

(n) intervalele de timp când se oferă servicii de ştampilare electronică a datei şi orei, dacă e cazul, conform art. 52 din prezentele norme

(o) metode detaliate de verificare a semnăturilor

(p) descrierea practicilor, procedurilor şi sistemelor care asigură securitatea şi integritatea datelor, accesul autorizat permanent la acestea şi previn orice acces neautorizat

(q) politicile de personal

(r) structura personalului

(s) parteneriate şi politica în domeniul

Domeniu	Semnătura electronică	*Cod domeniu*	SMEL
Titlu document	FORMULAR DE NOTIFICARE CĂTRE ARS PENTRU FURNIZORII DE SERVICII DE CERTIFICARE PENTRU SEMNĂTURA ELECTRONICĂ	*Cod document*	02
		Pag	2

FSC persoană fizică/juridică					
*Adresa**	*Ţara*	*Oraş*	*Sector*	*Strada*	*nr*
	bloc	*etaj*	*apt.*	*Cod poştal*	
	Tel	*Fax*		*E_mail*	*Web*
Cod înreg.Reg.Comerţului		*Cod fiscal*		*Tip societate***	
Banca	*Nr. cont bancar*	*Nr. act proprietate-contract închiriere pt. sediu*			
Naţionalitate		*Cetăţenie*			

*) Sediul Societății Comerciale/Adresa persoanei fizică
**) S.A., S.R.L., Regie Autonomă

Servicii de certifica-re oferite***	Emitere de certificate		
	Simple	Calificate, cu distribuire la client a DSCS****	Calificate, fără distribuire la client a DSCS
Data începerii activității			
Proceduri de secu-ritate utilizate (se vor detalia)			

Tipuri DSCS utilizate:	

***) Se va răspunde cu "Da" şi "Nu"
****) Dispozitiv Securizat de Creare a Semnăturii electronice

ÎNŞTIINŢARE - ANGAJAMENT

Subsemnatul înştiinţez Autoritatea de Reglementare şi Supraveghere pentru Semnătura Electronică (ARS)* referitor la desfăşurarea serviciilor de certificare menţionate în prezentul document, cu începere de la data de ……. (se va completa obligatoriu data).

Mă angajez să-mi desfăşor activitatea în conformitate cu prevederile Legii nr.455 din 18 iulie 2001 privind semnătura electronică pe care mă oblig să o respect întocmai, atât în litera cât şi în spiritul ei.

Mă oblig totodată să respect Normele metodologice româneşti privind aplicarea semnăturii electronice precum şi standardele europene şi internaţionale în domeniu şi să comunic clienţilor instrucţiunile practice de certificare, termenele şi condiţiile de utilizare a semnăturii electronice pusă la dispoziţie de firma mea.

Anexez la prezenta următoarea documentaţie:

1. Contractul de închiriere sau actul de proprietate pentru sediu.
2. Adeverinţa din partea Administraţiei Financiare de care aparţine firma, privind plata la zi a datoriilor către Stat.
3. Certificat de bonitate sau scrisoare de garanţie din partea băncii prin care firma desfăşoară plăţi şi încasări curente.
4. Copia contractului de asigurare pe numele firmei, la valoarea de 500.000 EURO (numai pentru Furnizorii de Servicii de Certificare acreditaţi, care eliberează certificate calificate).
5. Copia Certificatului de garanţie (numai pentru Furnizorii de Servicii de Certificare care emit certificate calificate):

   a. Pentru eliberarea certificatelor calificate depun

   o garanţie din partea unei instituţii financiare în favoarea ARS de cel puţin 500.000 EURO la banca … şi mă oblig să acopăr prejudiciile pe care le-aş putea cauza clientului, până la valoarea de 10.000 EURO/risc asigurat *sau*

   o poliţă de asigurare la o societate de asigurare în favoarea ARS de cel puţin 500.000 EURO şi mă oblig să acopăr prejudiciile pe care le-aş putea cauza clientului, până la valoarea de 10.000 EURO/risc asigurat
6. Cheia publică
7. Politica generală a FSC
8. Descrierea sistemelor FSC
9. Coduri de proceduri şi practici a FSC
10. Solicit / nu solicit acreditarea din partea ARS (se va tăia afirmaţia care nu rămâne valabilă).

REPREZENTANTUL FIRMEI Din partea ARS, primit documentaţia menţionată

Data şi ora

Anexa nr. 3

Domeniu	Semnătura electronică	*Cod domeniu*	SMEL
Titlu document	**CONȚINUTUL ŞI STRUCTURA CERTIFICATULUI CALIFICAT**	*Cod document*	03
		Pag.	2

Date despre FSC					
Numele Furnizorului de Servicii de Certificare					
*Adresa**	*Țara*	*Oraş*	*Sector*	*Strada*	*Nr.*
	bloc	*etaj*	*apt.*	*Cod poştal*	
	Tel	*Fax*	*Pagină Web*	*E_mail*	
Cetățenie / Naționalitate					

*) Dacă este persoană juridică, sediul acesteia

Date despre client							
Numele şi prenumele[1]							
Pseudonimul							
Adresa[2]	*Țara de rezidență*		*Județ/ Sector*				
	Oraş		*Strada*		*Nr.*		
	Bloc		*Scara*		*Apart.*		
	Cod poştal		*Telefon*		*Fax*		
	E-mail			*Pagină Web*			
Alte informații pe care clientul le dorește a fi cuprinse în certificat							

Tip certificat	***CERTIFICAT CALIFICAT***
Cheia publică	
Codul personal de identificare al semnatarului	
Cod de identificare al certificatului	
Extensiile semnăturii (vezi Anexa 9 din Normele metodologice privind aplicarea semnăturii electronice)	
Perioada de valabilitate a certificatului	
Informații privind limitele utilizării certificatului	

SEMNĂTURA ELECTRONICĂ EXTINSĂ A FSC EMITENT

[1] Pentru persoane juridice se va trece denumirea oficială a organizației
[2] Pentru persoane juridice se va trece adresa sediului organizației

Domeniu	Semnătura electronică	*Cod domeniu*	SMEL
Titlu document	**EXTENSIILE STANDARDIZATE ALE CERTIFICATELOR PENTRU SEMNĂTURA ELECTRONICĂ**	*Cod document*	04
		Pag.	2

Extensia	**Utilizat de**	**Utilizare**	**Critic***
A. Informaţii cu privire la chei şi politica de certificare			
AuthorityKeyIdentifier *Identificator pentru cheia publică a autorităţii*	*Toate*	*Identifică cheia publică corespunzătoare cheii private utilizată de Furnizorul de Certificare pentru a semna acest certificat*	*Nu*
KeyIdentifier *Identificator al cheii publice*	*Toate*	*Identificator unic, în funcţie de algoritmul utilizat*	*Nu*
AuthorityCertIssuer *Numele emitentului certificatului*	*Toate*	*Identifică autoritatea de emitere a certificatului; împreună cu numărul seriei, alternativă la identificatorul cheii*	*Nu*
AuthorityCertSerialNumber *Nr. seriei certificatului*	*Toate*	*Utilizat cu* Numele emitentului certificatului	*Nu*
SubjectKeyIdentifier *Identificatoru cheii subiectului*	*Toate*	*Identifică chei diferite pentru acelaşi subiect*	*Nu*
KeyUsage *Folosirea cheii*	*Toate*	*Defineşte scopuri specifice pentru utilizarea cheii (de exemplu, semnătura digitală, key agreement…)*	*Opţională*
PrivateKeyUsagePeriod *Perioada de utilizare a cheii private*	*Toate*	*Numai pentru cheile de semnătură digitală. Semnăturile pe documente datate în afara perioadei sunt invalide*	*Opţională*
CertificatePolicies *Politici de certificare*	*Toate*	*Identificatori şi calificatori ce identifică şi califică politicile de certificare ce se aplică unui certificat*	*Opţională*
PolicyIdentifiers *Identificatori de politici de certificare*	*Toate*	*OID = obiectul de identificare a unei politici*	*Opţională*
PolicyQualifiers *Atributele politicii de certificare*	*Toate*	*Mai multe informaţii privind politicile de certificare*	*Opţională*
PolicyMappings *Suprapunerea de politici*	*AC*	*Indică politici echivalente*	*Opţională*
B. Atribute certificat şi FSC			
SubjectAltName *Numele alternativ al subiectului*	*Toate*	*Utilizată pentru a lista numele alternative (de exemplu numele RFC822, adresa X400, adresa IP…)*	*Opţională*
IssuerAltName *Numele alternativ al emitentului*	*Toate*	*Listează numele alternative*	*Opţională*

SubjectDirectoryAttributes	*Toate*	*Listează orice atribut dorit (de exemplu supported algorithms)*	*Opțională*
C. Constrângeri ale căii de certificare			
BasicConstraints *Constrângeri de bază*	*Toate*	*Constrângeri privind rolul subiectului şi lungimea căii*	*DA*[*]
CA *Autoritatea de Certificare*	*Toate*	*Lungimea căii este semnificativă numai dacă valoarea lui cA =Adevărat*	*DA*[*]
PathLenConstraint *Constrângeri privind lungimea căii de certificare*	*AC*	*Numărul AC care sunt permise în calea de certificare; 0 indică faptul că AC poate să emită cerificate numai către entitatea finală*	*DA*[*]
NameConstraints *Constrângeri privind numele*	*AC*	*Limitează certificarea AC consecutive referitor la următorii doi parametri:* PermittedSubtrees şi ExcludedSubtrees	*Opțională*
PermittedSubtrees *Subarbori permişi*		*Numele din afara subarborilor indicați nu sunt permise*	*Opțională*
ExcludedSubtrees *Subarbori excluşi*		*Indică arborii excluşi*	
PolicyConstraints *Constrângeri ale politicii de certificare*	*Toate*	*Constrânge certificate emise de AC la politicile menționate în parametrul următor; Acestea se utilizează în conjuncție cu al doilea sau al treilea parametru*	*Opțională*
PolicySet *Set de politici de certificare*	*Toate*	*Acele politici de certificare la care se aplică constrângerile*	*Opțională*
RequireExplicitPolicy *Politici cerute explicit*	*Toate*	*Arată numărul de certificate care pot apare în calea indicată, înainte ca o politică explicită să fie cerută*	*Opțională*
InhibitPolicyMapping *Suprapunerea politicilor de inhibare*	*Toate*	*Arată numărul de certificate care pot apare în calea indicată, înainte ca suprapunerea politicilor să mai fie permisă*	*Opțională*
D. Identificarea listei de certificate revocate			
CrlDistributionPoints *Punctele de distribuire a LCR*	*Toate*	*Mecanism de divizare a LCR lungi în liste scurte*	
DistributionPoint *Punct de distribuire*	*Toate*	*Locație de la care se poate obține LCR*	*Opțională*
Reasons *Motive*	*Toate*	*Motive pentru care certificatele sunt incluse în LCR*	*Opțională*
CRLIssuer *Emitentul LCR*	*Toate*	*Numele componentei care emite LCR*	*Opțională*

"NU" - înseamnă că standardul cere ca extensia sa fie necritică

"OPȚIONALĂ" înseamnă că FSC care emite poate să aleagă dacă extensia este critică sau necritică.

"DA" înseamnă că standardul "Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocated List Profile"- standard recomandat de ETSI- permite câmpului respectiv să fie critic sau necritic, dar este recomandabil ca acesta să fie considerat critic.

Anexa nr. 5

ANTETUL INSTITUȚIEI FINANCIARE

Data: _____

Subiect :_____

Aceasta scrisoare confirmă că _____ (instituția financiară) garantează irevocabil efectuarea plății / plaților ordonate de _____ (FSC) până la limita de _____ (minim 500.000 Euro) din contul _____ (contul FSC).

Această garanție se referă la condițiile prevăzute în Legea şi Normele Metodologice privind aplicarea semnăturii electronice. Această scrisoare de garanție este validă până la data de _____ (data limită de valabilitate a scrisorii de garanție). Pentru verificări, contactați _____ (contact instituție financiară).

_____ (semnătură împuternicit al instituției financiare)

_____ (semnătură împuternicit FSC)

Domeniu	*Semnătura electronică*	*Cod domeniu*	SMEL
Titlu document	**CONȚINUTUL INFORMAȚIONAL MINIMAL AL REGISTRULUI DE EVIDENȚĂ A CERTIFICATELOR**	*Cod document*	06
		Pag	2

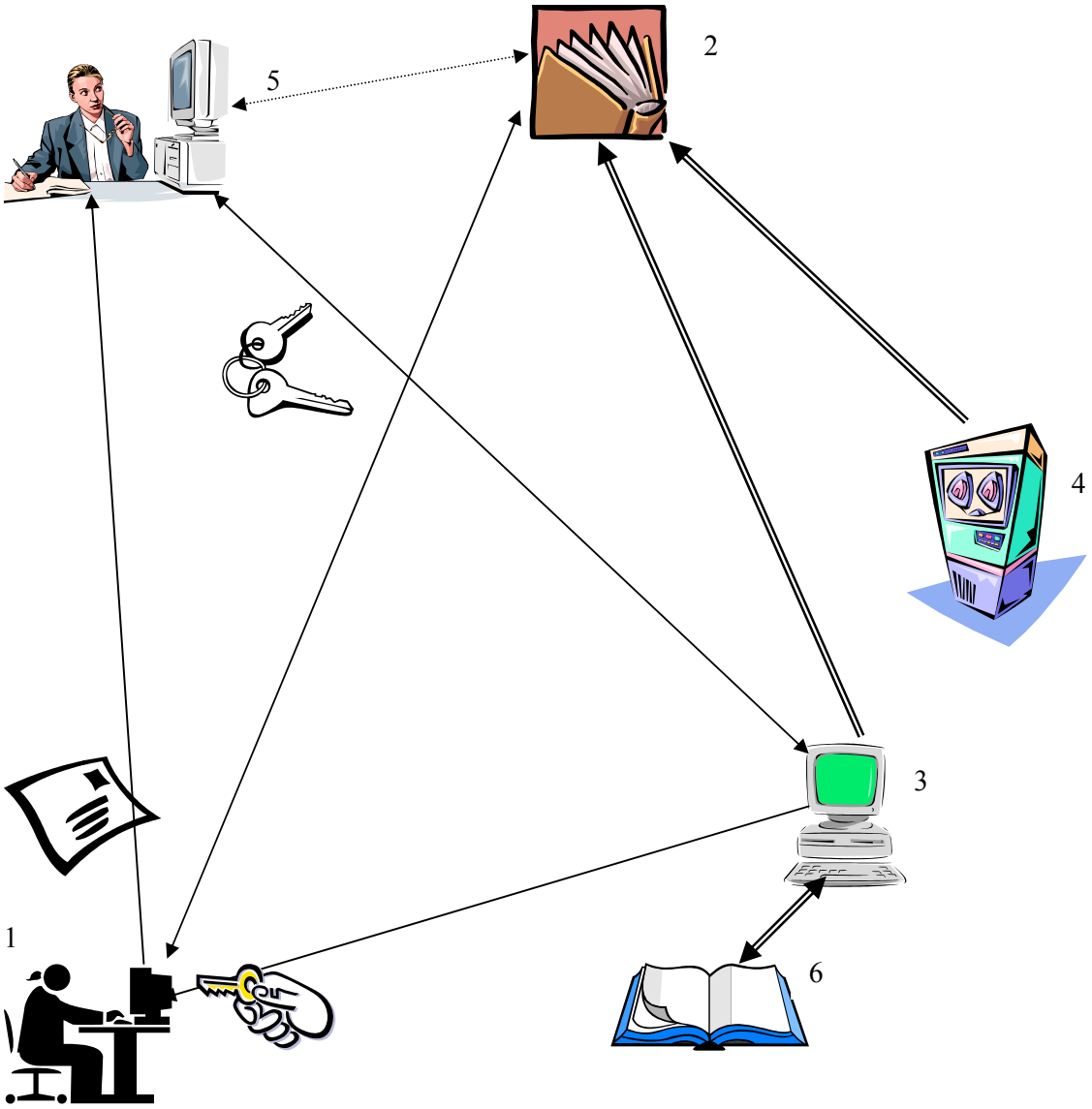
A. Date de identificare a clientului

Nr.crt	Categorie de date	
1	Persoană (fizică / juridică)	
2	Denumirea persoanei juridice	
a. Date despre persoana fizică sau reprezentantul legal al persoanei juridice		
3	Numele şi prenumele	
4	Pseudonimul	
5	Cod identificare client	
6	Data naşterii (ZZ/LL/AAAA)	
7	Locul naşterii	
b. Adresa persoanei fizice sau a reprezentantului legal al persoanei juridice		
8	Ţara	
9	Oraşul	
10	Sectorul	
11	Strada	
12	Nr.	
13	Bloc	
14	Apt.	
15	Cod poştal	
16	Tel.	
17	Fax	
18	E_mail	
c. Adresa sediului persoanei juridice		
19	Ţara	
20	Oraşul	
21	Sectorul	
22	Strada	
23	Nr.	
24	Bloc	
25	Apt.	
26	Cod poştal	
27	Tel.	
28	Fax	
29	E_mail	

B. Date despre certificat

30	Cod certificat	
31	Categorie certificat (simplu / calificat)	
32	Data emiterii certificatului	
33	Data încetării valabilității certificatului	
34	Data înştiinţării expirării valabilității certificatului	
35	Data expirării certificatului	
36	FSC care preia gestiunea certificatului	
37	Dacă există acordul clientului (DA /NU)	
38	Data revocării certificatului	

C. Certificatul propriu-zis (conform anexei 3)



Gestionarea şi utilizarea cheilor publice şi private pentru servicii de certificare

1 – Client, deținător al unui Certificat; 2 – Registrul Furnizorilor de Servicii de Certificare (RFSC) tinut de ARS; 3, 4 – Furnizori de Servicii de Certificare (pot exista mai mulți, în exemplu sunt doar doi furnizori: FSC1 şi FSC2); 5 –Destinatarul unui document semnat electronic; 6 – RC1-Registrul electronic de evidență a certificatelor eliberate de către FSC1.

Faza I: Înființarea ARS şi a RFSC

Faza II: Clientul consultă RFSC, îşi alege (în urma analizei informațiilor puse la dispoziție de furnizori conform Art. 14 din Lege) FSC din cele existente (în cazul nostru alege FSC1) şi semnează contractul cu acesta. Clientului i se eliberează certificatul (creat pe baza datelor din formularul de solicitare a certificatului) şi dispozitivul de creare a semnăturii electronice; Certificatul este inclus în RC1.

Faza III: Clientul expediază documentul ce poartă semnătura sa electronică. Cel ce îl recepționează verifică semnătura folosind cheia publică a clientului (din certificatul acestuia) Suplimentar, pentru o mai mare siguranță, el poate consultă RFSC pentru a obține cheia publică a FSC1 (necesară verificării semnăturii FSC1 de pe certificatul clientului).

Anexa nr. 8

Domeniu	Semnătura electronică	*Cod domeniu*	SMEL
Titlu document	**INFORMAȚII PUSE LA DISPOZIȚIE DE CLIENȚI ÎN VEDEREA CERTIFICĂRII APLICAȚIILOR – CERTIFICAT SIMPLU**	*Cod document*	08
		Pag.	3

Date obligatorii despre solicitant					
Numele şi prenumele		*Pseudonimul*		*E-mail*	

Date opționale despre solicitant							
Adresa	*Țara de rezidență*		*Oraş*		*Județ/Sector*		
	Strada		*Nr.*		*Bloc*	*Scara*	
	Etaj		*Apart.*		*Cod poştal*		
	Telefon		*Fax*				

Data naşterii (zz/ll/aaaa)		*B.I. /C.I. seria*		*Nr. B.I. / C.I.*	
Emis de		*Valabil până la data (zz/ll/aaaa)*		*Data emiterii (zz/ll/aaaa)*	
Paşaport nr.		*Emis de*		*Valabil până la (zz/ll/aaaa)*	
Permis auto nr.		*Emis de*		*Valabil până la*	
Tip card		*Banca emitentă*		*Nr. card*	*Data la care expiră cardul (zz/ll/aaaa)*

Date opționale despre soț/soție			
Numele şi prenumele		*Data naşterii (zz/ll/aaaa)*	

Date despre aplicații	
Tip aplicații (poştă electronică, navigare pe web, tranzacții mici şi de risc scăzut, subscrierea pe web la anumite servicii oferite de terți, etc.)	
Alte informații cerute de aplicațiile menționate mai sus	

Date obligatorii despre solicitant							
Numele şi prenumele		*Pseudonimul*		*Data naşterii (zz/ll/aaaa)*			
Adresa	*Țara de rezidență*		*Județ/Sector*		*Oraş*		
	Strada		*Nr.*		*Bloc*		
	Scara	*Apart.*		*Cod poştal*			
	Telefon		*Fax*		*E-mail*		
Seria B.I. /C.I.		*Nr. B.I. / C.I.*		*Data emiterii (zz/ll/aaaa)*			
Emis de		*Valabil până la data de (zz/ll/aaaa)*					
Paşaport nr.		*Emis de*		*Valabil până la data*		*ZZ / LL / AAAA*	
Permis auto nr.		*Emis de*		*Valabil până la data*		*ZZ / LL / AAAA*	
Tip card		*Banca emitentă*					
Nr. card		*Data la care expiră cardul*		*ZZ / LL / AAAA*			

Date opționale depre soț/soție			
Numele şi prenumele		*Data naşterii*	*ZZ / LL / AAAA*

Date despre aplicații	
Tip aplicație:poştă electronică, navigare pe web, tranzacții de orice tip, transfer de fişiere, validare de software, subscriere pe web la anumite servicii oferite de terți, etc.	
Alte informații cerute de aplicațiile menționate mai sus	

Date obligatorii despre persoana juridică (completate în prezența reprezentantului legal)*							
Numele domeniului		*Denumirea persoanei juridice*					
Adresa persoanei juridice	*Țara*		*Oraş*				
	Strada		*Nr.*		*Bloc*		
	Scara		*Apart.*		*Cod poştal*		
	Telefon		*Fax*		*E-mail*		
Nr. H.J. şi data de înființare a persoanei juridice			*Nr. de înregistrare la Registrul Comerțului*				
Nr. cod fiscal		*Banca la care îşi desfăşoară operațiunile curente*		*Nr. cont bancar*			

Date obligatorii despre persoana de contact desemnată de persoana juridică (completate în prezența persoanei de contact)*							
Numele şi prenumele		*Funcția în cadrul firmei*		*Data naşterii*	*ZZ / LL / AAAA*		
B.I. /C.I. seria		*Nr. B.I. / C.I.*		*Data emiterii*	*ZZ / LL / AAAA*		
Emis de		*Valabil până la data*	*ZZ / LL / AAAA*				
Paşaport nr.		*Emis de*		*Valabil până la data*	*ZZ / LL / AAAA*		
Permis auto nr.		*Emis de*		*Valabil până la data*	*ZZ / LL / AAAA*		
Tip card		*Banca emitentă*		*Nr. card*			
Data la care expiră cardul	*ZZ / LL / AAAA*						
Adresa	*Țara*		*Oraş*				
	Sector/Județ		*Strada*		*Nr.*		
	Bloc		*Scara*		*Apart.*		
Telefon		*Fax*		*E-mail*			

Date opționale despre soț/soție			
Numele şi prenumele		*Data naşterii*	*ZZ / LL / AAAA*

Date despre aplicații	
Tip aplicație: poştă electronică, navigare pe web, tranzacții de orice tip, transfer de fişiere, validare de software, subscriere pe web la anumite servicii oferite de terți, etc.	
Alte informații cerute de aplicațiile menționate mai sus	

*În cazul modificării formei sau statutului persoanei juridice, persoana juridică este obligată să reînnoiască contractul cu FSC.

**În cazul în care se schimbă reprezentantul legal sau persoana de contact, persoanele noi desemnate în aceste funcții sunt obligate să se prezinte la FSC pentru a-şi completa datele cerute de FSC.

Domeniu	Semnătura electronică	*Cod domeniu*	SMEL
Titlu document	**MACHETA FORMULARULUI DE INFORMARE CU PRIVIRE LA ÎNCETAREA ACTIVITĂȚII UNUI FURNIZOR DE SERVICII DE CERTIFICARE**	*Cod document*	09
		Pag	2

Numele FSC				*Codul din Registrul FSC*				
Adresa	*Țara*			*Sector/Județ*		*Oraş*		
	Strada			*Nr.*		*Bloc*		
	Scara			*Apart.*		*Telefon*		
	Fax			*E-mail*		*Cod poştal*		
Codul din Registrul Comerțului		*Cod fiscal*			*Data începând cu care îşi încetează activitatea*		*ZZ/LL/AAAA*	
Data la care a înştiințat ARS	*ZZ/LL/ AAAA*	*Motivele încetării activității (existența şi natura împrejurării care justifică încetarea activită-ții, conf. art. 24, alin.1 din Lege)*						
Numele FSC care va prelua activitatea		*Codul din Registrul Furnizorilor de Servicii*						
Nr. de înreg. în Registrul Comerțului		*Codul fiscal*						
Adresa FSC care va prelua activitatea	*Strada*		*Nr.*		*Scara*			
	Etaj		*Apart.*					
	Oraş		*Sector/ Județ*		*Țara*			
	Tel.		*Fax*		*E-mail*			
Măsuri luate referitoare la clienți	*Revocarea certificatelor eliberate clienților (Lista certificatelor revocate) – se vor completa datele din Tabelul 1* *Preluarea certificatelor eliberate clienților (Lista certificatelor preluate) - se vor completa datele din Tabelul 2* *Măsurile luate pentru asigurarea arhivelor referitoare la clienți şi la certificatele emis, precum şi pentru asigurarea prelucrării datelor personale în condițiile Legii (conform art. 24 aliniatul 4 din Lege)*							

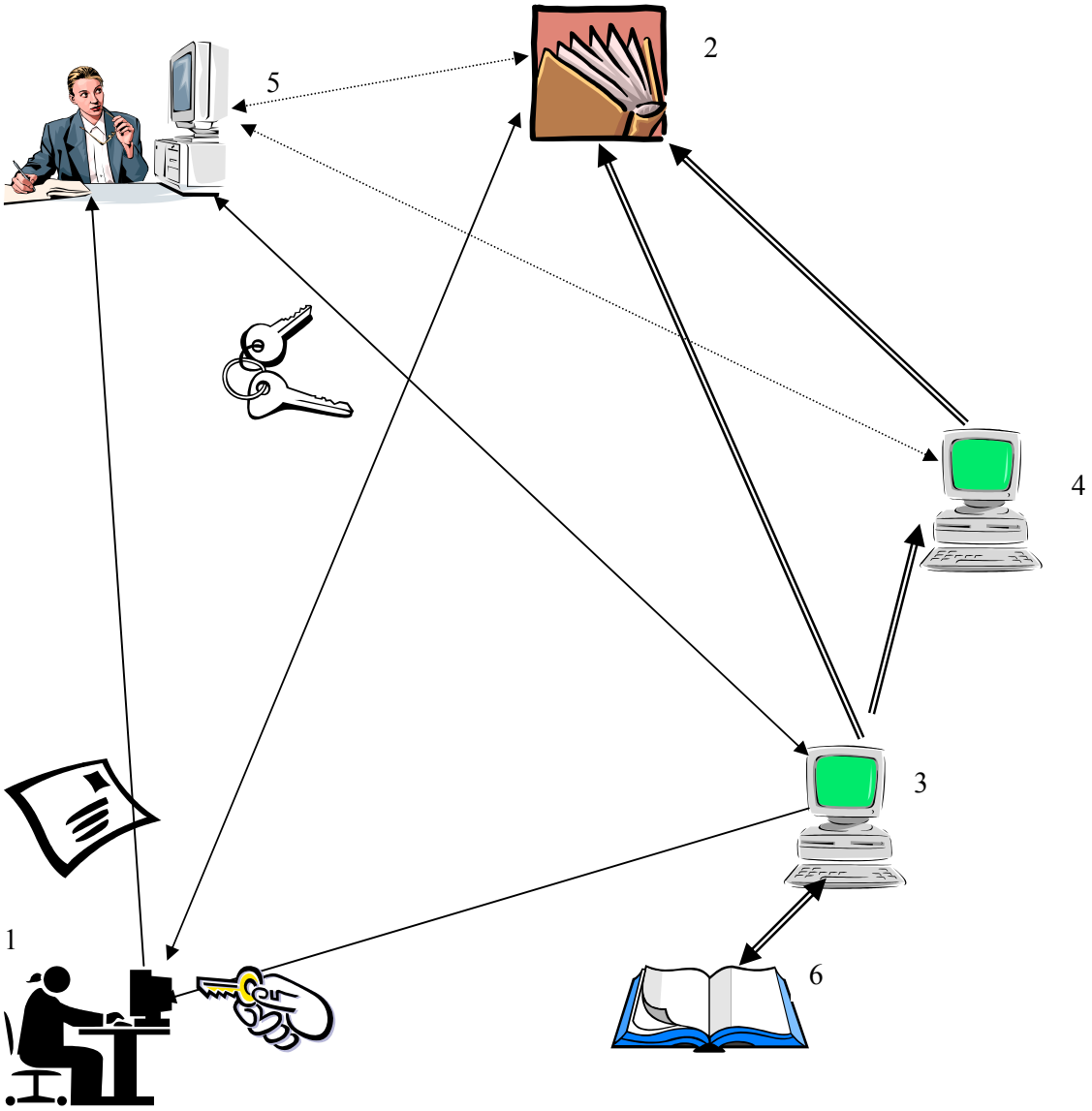
TABELUL 1 - Lista certificatelor revocate

Seria certificatului	*Data şi ora emiterii*	*Algoritmul semnăturii*	*Versiunea*
	ZZ/LL/AAAA hh/mm		

TABELUL 2 - Lista certificatelor valide preluate

Seria certificatului	*Data şi ora emiterii*	*Algoritmul semnăturii*	*Versiunea*	*Data la care expiră valabilitatea certificatului*
	ZZ/LL/AAAA hh/mm			

Anexa nr. 10



Structura ierarhică a FSC

1 – Client, deținător al unui Certificat; 2 – Registrul Furnizorilor de Servicii de Certificare (RFSC) tinut de ARS; 3, 4 – Furnizori de Servicii de Certificare (FSC2 gestionează cheia publică a FSC1); 5 –Destinatarul unui document semnat electronic; 6 – RC1- Registrul electronic de evidență a certificatelor eliberate de către FSC1.

Faza I: FSC1 solicită FSC2 eliberarea unui certificat. FSC2 gestionează cheia publică a FSC1.

Faza II: Clientul expediază documentul ce poartă semnătura sa electronică. Cel ce îl recepționează verifică semnătura folosind cheia publică a clientului (din certificatul acestuia) Suplimentar, pentru o mai mare siguranță, el poate consultă RFSC pentru a obține cheia publică a FSC1 (necesară verificării semnăturii FSC1 de pe certificatul clientului). Alternativ, clientul poate verifica semnătura FSC1 de pe certificatul clientului accesând certificatul FSC1 emis de FSC2 (aflat pe nivelul ierarhic superior). La rândul ei, semnătura FSC2 de pe certificatul FSC1 poate fi verificată apelând la RFSC sau la un FSC care gestionează cheia FSC2 şamd.