

HOTARARE nr. 1.259 din 13 decembrie 2001
privind aprobarea Normelor tehnice si metodologice pentru aplicarea Legii nr. 455/2001
privind semnatura electronica
Emitent : GVERNUL
Publicata in : MONITORUL OFICIAL nr. 847 din 28 decembrie 2001

In temeiul prevederilor art. 107 din Constitutia Romaniei si ale art. 52 din Legea nr.
455/2001 privind semnatura electronica

Guvernul Romaniei adopta prezenta hotarare.

ARTICOL UNIC

Se aproba Normele tehnice si metodologice pentru aplicarea Legii nr. 455/2001 privind
semnatura electronica, prevazute in anexa care face parte integranta din prezenta hotarare.

PRIM-MINISTRU
ADRIAN NASTASE

Contrasemneaza:
ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ
Ministrul comunicatiilor si
tehnologiei informatiei,
Dan Nica

Ministrul finantelor publice,
Mihai Nicolae Tanasescu

ANEXA 1

NORME TEHNICE SI METODOLOGICE
pentru aplicarea Legii nr. 455/2001 privind semnatura electronica

CAP. 1
Dispozitii generale

ART. 1

Orice persoana, fizica sau juridica, aflata pe teritoriul Romaniei poate beneficia de servicii
de certificare in vederea utilizarii semnaturii electronice in sensul definit a art. 4 din Legea nr.
455/2001 privind semnatura electronica, denumita in continuare lege.

ART. 2

(1) In intelesul prezentelor norme tehnice si metodologice, termenii utilizati au urmatoarele
definitii:

a) client - beneficiarul serviciilor de certificare, care, in baza unui contract incheiat cu un
furnizor de servicii de certificare, denumit in continuare furnizor, detine o pereche functionala
cheie publica-cheie privata si are o identitate probata printr-un certificat digital emis de acel
furnizor;

b) hash-code - functie care returneaza amprenta unui document electronic;

c) cheie privata - un cod digital cu caracter de unicitate, generat printr-un dispozitiv hardware si/sau software specializat. In contextul semnaturii digitale cheia privata reprezinta datele de creare a semnaturii electronice, asa cum apar ele definite in lege;

d) cheia publica - cod digital, perechea cheii private necesara verificarii semnaturii electronice. In contextul semnaturii digitale cheia publica reprezinta datele de verificare a semnaturii electronice, asa cum apar ele definite in lege;

e) mecanismul de creare a semnaturii electronice asupra documentului se aplica o functie hash-code, obtinandu-se amprenta documentului. Printr-un algoritm se aplica cheia privata peste amprenta documentului, rezultand semnatura electronica;

f) mecanismul de verificare a semnaturii electronice se bazeaza pe utilizarea cheii publice, a functiei hash-code si a semnaturii electronice primite. Verificarea semnaturii este o operatie automata;

g) pagina web - document electronic, disponibil prin internet.

(2) In intelesul prezentelor norme, abrevierile utilizate au urmatoarele semnificatii:

a) ETSI - Institutul European de Standarde in Telecomunicatii;

b) RFC - desemneaza documente care au fost supuse analizei publice in cadrul unui proces coordonat de Grupul de Lucru pentru Ingineria Internetului;

c) FIPS - desemneaza standarde federale emise de Institutul National de Standarde si Tehnologie din Statele Unite ale Americii;

d) IEEE - Institutul de Inginerie Electrica si Electronica;

e) ITSEC - desemneaza standardele si criteriile europene de evaluare a securitatii sistemelor informatice;

f) RSA - algoritmul de criptare cu cheie publica, dezvoltat de cercetatorii Rivest, Shamir si Adleman;

g) DSA - Algoritmul de Semnatura Digitala;

h) SHA - Algoritm Securizat de Hash-code;

i) PKI - Infrastructura de chei publice;

j) RTF - format de document ce permite alinierea textului, introducerea unor caractere speciale, utilizarea culorilor si a fonturilor de dimensiuni diferite, precum si inserarea altor obiecte;

k) PDF - format ce permite transferarea documentelor electronice fara a afecta aranjarea in pagina; documentele pot contine text, imagini si sunete;

l) Post-Script - format de document utilizat in special pentru tiparire la imprimante Post-Script.

m) TXT - format de document continand exclusiv text

CAP. 2

Autoritatea de reglementare si supraveghere

ART. 3

(1) Autoritatea de reglementare si supraveghere, denumita in continuare autoritate, genereaza sau achizitioneaza o pereche functionala cheie privata-cheie publica si trebuie sa isi protejeze cheia sa privata, utilizand un sistem fiabil si luand precautiile necesare pentru a preveni pierderea, dezvaluirea, modificarea sau utilizarea neautorizata a cheii sale private.

(2) Cheia privata nu poate fi dedusa in nici un fel din cheia sa publica pereche.

ART. 4

Autoritatea gestioneaza Registrul furnizorilor de servicii de certificare, denumit in continuare registru

ART. 5

Continutul informational si structura registrului sunt prezentate in anexa nr. 1.

ART. 6

(1) Actualizarea registrului se face exclusiv de catre autoritate si urmareste toate modificarile survenite in statutul furnizorului - acreditare, terminarea perioadei de acreditare, suspendare, imbogatirea tipurilor de certificate oferite.

(2) Dupa fiecare actualizare autoritatea transmite furnizorului o copie de pe documentul prevazut la pct. 43 din anexa nr. 1.

ART. 7

Autoritatea gestioneaza datele utilizand un sistem informatic in masura sa asigure securitatea sistemelor comunicatiilor, tranzactiilor si datelor conform standardelor recunoscute - ISO/IEC 15408-1, 2, 3 si ISO 17799. In acest sens se utilizeaza o solutie ce asigura managementul unei baze de date replicate, garantandu-se accesul permanent prin Internet.

ART. 8

Autoritatea face publice, spre consultare urmatoarele date din registru:

- a) tipul furnizorului - persoana fizica sau juridica;
- b) numele sau denumirea furnizorului;
- c) data la care si-a inceput activitatea;
- d) cheia publica a furnizorului;
- e) indicatii privind acreditarea - acreditat sau neacreditat;
- f) perioada de acreditare - inceput/sfarsit;
- g) indicatii privind dreptul de a emite certificate calificate;
- h) descrierea politicii generale a furnizorului;
- i) forma de organizare a furnizorului - societate comerciala, regie autonoma, institutie publica, organizatie neguvernamentala, alte tipuri;
- j) adresa sau sediul - tara, oras, judet/sector, strada numar, bloc, scara, etaj, apartament, cod postal;
- k) nationalitatea, pentru persoana juridica;
- l) cetatenia, pentru persoana fizica;
- m) telefon, fax, e-mail, adresa in pagina web;
- n) categoriile de servicii destinate publicului: tipul de certificate, mod de utilizare, pentru fiecare tip de certificate
- o) tipurile de dispozitive de creare a semnaturii electronice utilizate;
- p) situatia dispozitivelor - daca sunt omologate sau nu;
- q) situatia furnizorului: operational, suspendat, activitatea incetata, in curs de transferare a activitatii, in curs de remediere a unor probleme identificate de autoritate indicand termenul limita;
- r) istoric al furnizorului: data de incepere a activitatii, perioade de suspendare, perioade in care a avut dreptul de a emite certificate calificate, alte asemenea situatii.

ART. 9

(1) Informatiile prevazute la art. 8 din prezentele norme tehnice si metodologice sunt disponibile public, prin Internet, in pagina web a autoritatii.

(2) Pagina web va mai contine informatii cu privire la legea semnaturii electronice, normele tehnice si metodologice privind aplicarea legii semnaturii electronice, informatii generale cu privire la utilizarea semnaturii electronice, informatii noi din domeniul semnaturii electronice, trimiteri catre paginile web ale furnizorilor de servicii de certificare.

(3) Autoritatea va publica permanent tehnologiile Internet prin care se pot consulta informatiile prevazute la alin. (1) si (2).

CAP. 3

Furnizorii de servicii de certificare

SECTIUNEA 1 Dispozitii comune

ART. 10

(1) Un furnizor este obligat sa genereze sau sa achizitioneze o pereche functionala cheie privata-cheie publica si sa isi protejeze cheia sa privata, utilizand un sistem fiabil si luand precautiile necesare pentru a preveni pierderea, dezvaluirea, modificarea sau utilizarea neautorizata a cheii sale private.

(2) Cheia privata nu poate fi dedusa in nici un fel din cheia sa publica pereche.

ART. 11

(1) Inainte de inceperea activitatii furnizorul va notifica autoritatea, conform formularului prevazut in anexa nr. 2.

(2) Toate datele vor fi inaintate autoritatii pe suport de hartie si in format electronic, documentul electronic fiind semnat digital de catre furnizor si prezentat in unul dintre urmatoarele formate: RTF, PDF, TXT si Post-Script.

ART. 12

(1) Inregistrarea in registru se face pe baza unei cereri individuale.

(2) La primirea cererii autoritatea include datele furnizorului in registru si genereaza pentru acesta un cod de identificare format prin alipirea anului, lunii si datei de incepere a activitatii si a numarului de ordine al furnizorului.

SECTIUNEA a 2-a Furnizarea serviciilor de certificare calificata

ART. 13

(1) Furnizorul poate furniza servicii de certificare bazate pe certificate simple si calificate.

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

(3) Autoritatea va publica eventualele modificari ale formatului descris, pe baza evolutiei tehnologiilor sau a normelor internationale recunoscute in domeniu.

(4) Certificatul are si o rubrica de extensii. Lista celor mai uzuale extensii este prevazuta in anexa nr. 4.

(5) Codul de identificare a certificatului calificat se formeaza prin alipirea codului de identificare a furnizorului si a numarului de ordine al certificatului.

(6) Codul personal de identificare a semnatarului rezulta prin alipirea codului de identificare a furnizorului, initialele numelui sau pseudonimului semnatarului si numarul de ordine al acestuia in lista clientilor cu aceleasi initiale.

ART. 14

(1) In vederea emiterii de certificate calificate furnizorul trebuie sa indeplineasca conditiile enuntate la art. 20-22 din lege.

(2) Furnizorul trebuie sa dovedeasca autoritatii ca dispune de resursele financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfasurarii activitati de certificare si trebuie sa fie capabil sa acopere pierderile suferite de catre o persoana care isi intemeiaza conduita pe efectele juridice ale certificatelor calificate, pana la concurenta echivalentului in lei al sumei de 10.000 euro pentru fiecare risc asigurat. Riscul asigurat este fiecare prejudiciu produs, chiar daca se produc mai multe asemenea prejudicii ca urmare a neindeplinirii de catre furnizor a unei obligatii prevazute de lege. Furnizorul va trebui sa depuna o scrisoare de garantie din partea unei instituti financiare de specialitate sau o polita de asigurare la o societate de asigurari, in favoarea autoritatii, in valoare cel putin egala cu

echivalentul in lei al sumei de 500.000 euro; scrisoarea de garantie are forma prevazuta in anexa nr. 5.

(3) Furnizorul trebuie sa asigure un nivel de securitate a sistemelor, comunicatiilor, tranzactiilor si datelor conform standardelor recunoscute - ISO/IEC 15408-1,2,3; ISO 17799; ETSI TS 101 456 v.1.1.1. (2000-12); ITSEC-E3 FIPS 140-1.

(4) Furnizorul trebuie sa asigure operarea rapida a registrului de evidenta a certificatelor, conform art. 20 lit. b) din lege; structura registrului este prezentata in anexa nr. 6.

(5) Furnizorul trebuie sa foloseasca numai dispozitive securizate de creare a semnaturii electronice.

(6) Autoritatea verifica datele continute in documentatia depusa, in termen de maximum 10 zile, in raport cu standardele recunoscute si cu prezentele norme tehnice si metodologice.

(7) Autoritatea trebuie sa informeze furnizorul, in termen de maximum 10 zile, cu privire la indeplinirea conditiilor si sa solicite, daca e cazul, completarea documentatiei.

(8) In cazul in care toate criteriile sunt indeplinite, autoritatea emite decizia prin care furnizorul dobandeste dreptul de a furniza servicii de certificare calificata si actualizeaza registrul inscriind noul statut al furnizorului. Decizia este comunicata furnizorului pe suport de hartie si in format electronic, semnat digital de autoritate.

(9) Daca documentatia nu a fost completata sau nu indeplineste conditiile, autoritatea emite o decizie motivata prin care respinge solicitarea furnizorului de a i se acorda dreptul de furnizare de servicii de certificare calificata. Decizia este comunicata furnizorului pe suport de hartie si in format electronic, semnat digital de autoritate.

ART. 15

In cazul in care nu mai sunt indeplinite conditiile prevazute la art. 20-22 din lege, autoritatea va lua decizia de suspendare a dreptului furnizorului in cauza de a emite certificate calificate, pana la remedierea neajunsurilor si indeplinirea tuturor conditiilor legale. Decizia este comunicata furnizorului pe suport de hartie si in format electronic, semnat digital de autoritate.

SECTIUNEA a 3-a

Acreditarea voluntara

ART. 16

(1) Furnizorul care doreste sa isi desfasoare activitatea ca furnizor acreditat trebuie sa solicite obtinerea acreditarii din partea autoritatii.

(2) In acest sens furnizorul trebuie sa indeplineasca toate conditiile necesare emiterii de certificate calificate si sa utilizeze dispozitive securizate de generare a semnaturii electronice, omologate de o agentie de omologare agreata de autoritate.

(3) Verificarile se fac atat asupra declaratiilor continute in documentatia depusa la autoritate, cat si asupra concordantei dintre sistemele, procedurile si practicile afirmate si cele existente in realitate.

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

(5) Autoritatea trebuie sa informeze in termen de maximum 30 de zile furnizorul cu privire la indeplinirea conditiilor si sa solicite, daca e cazul, completarea documentatiei.

ART. 17

(1) In cazul in care se constata ca toate criteriile sunt indeplinite, autoritatea decide acreditarea furnizorului.

(2) Decizia de acreditare, conditiile si efectele suspendarii sau ale retragerii sunt comunicate furnizorului pe suport de hartie si in format electronic, semnat digital de autoritate.

(3) La cererea furnizorului autoritatea actualizeaza registrul prin inscrierea noului statut de furnizor acreditat. Se introduc informatii despre garantii, omologarea dispozitivelor, agentia de omologare, perioada de acreditare.

ART. 18

(1) Durata acreditarii este de 3 ani si se poate reinnoi.

(2) Procedura de reinnoire este identica cu cea de obtinere a acreditarii.

ART. 19

Suspendarea deciziei de acreditare se face in urmatoarele cazuri:

a) se constata ca furnizorul nu mai indeplineste una sau mai multe dintre conditiile prevazute pentru acordarea deciziei de acreditare. In acest caz autoritatea notifica furnizorului si stabileste un interval de timp de maximum 30 de zile in care furnizorul trebuie sa remedieze deficientele semnalate;

b) declansarea procedurii falimentului furnizorului.

ART. 20

Autoritatea retrage decizia de acreditare in urmatoarele cazuri:

a) daca furnizorul nu remediaza deficientele prevazute a art. 19 lit. a), in termenul acordat de catre autoritate;

b) daca intervine o hotarare judecatoreasca definitiva si revocabila prin care se declara falimentul furnizorului.

SECTIUNEA a 4-a

Agrearea agentilor de omologare

ART. 21

(1) Decizia de agreare a agentilor de omologare se face pe baza unei cereri a agentiei catre autoritate si in urma verificarii conditiilor mentionate in normele europene pentru acest gen de activitate.

(2) Decizia de agreare este valabila 1 an si se poate reinnoi.

(3) Decizia se retrage in cazul in care se constata ca agentia nu mai indeplineste conditiile prevazute la alin. (1) si (2). Autoritatea transmite agentiei o nota explicativa in care descrie motivele retragerii deciziei de agreare.

CAP. 4

Proceduri de utilizare a semnaturii electronice

ART. 22

Principiul de functionare si procedurile de utilizare a semnaturii electronice sunt prevazute in anexa nr. 7.

ART. 23

Orice persoana, fizica sau juridica, care doreste ca un furnizor sa ii elibereze un certificat trebuie:

a) sa furnizeze informatiile cerute pentru tipul de certificat dorit, conform formularului prevazut in anexa nr. 8;

b) sa genereze sau sa achizitioneze o pereche functionala cheia privata-cheie publica; cheia privata nu poate fi dedusa in nici un fel din cheia sa publica pereche;

c) sa probeze functionalitatea perechii cheia privata-cheie publica;

d) sa protejeze cheia privata de furturi, deteriorari, modificari ale continutului sau alte compromiteri ale acesteia este interzisa duplicarea cheii private;

e) sa propuna un nume sau un pseudonim distinct pentru identificare;

f) sa supuna examinarii furnizorului: cererea de furnizare a unui certificat, acordul de a respecta obligatiile in calitate de client si cheia sa publica.

ART. 24

La primirea cererii de eliberare a certificatului furnizorul in cauza va verifica, inainte de eliberarea certificatului, urmatoarele aspecte:

- a) daca solicitantul certificatului este persoana identificata in cerere, prin procedura adecvata categoriei din care face parte certificatul;
- b) daca solicitantul certificatului detine cheia privata corespunzatoare cheii publice listate in certificat;
- c) daca informatia listata in certificat este exacta.

ART. 25

(1) Durata verificarii informatiilor din cerere si a eliberarii certificatului nu poate depasi:

- a) o zi lucratoare, pentru certificatele simple;
- b) 5 zile lucratoare, pentru certificatele calificate.

(2) Termenele prevazute la alin. (1) se calculeaza din momentul primirii de catre furnizorul in cauza a tuturor informatiilor cerute pentru acest scop.

ART. 26

Furnizorul nu poate emite un certificat fara consimtamantul expres al celui pe numele caruia este emis.

ART. 27

Durata valabilitatii unui certificat este de maximum 1 an de la data comunicarii catre client.

ART. 28

Certificatul poate fi transmis solicitantului in urmatoarele modalitati:

- a) personal;
- b) prin posta, cu confirmare de primire;
- c) prin posta electronica - numai pentru certificate simple; observatiile, daca exista, se comunica pe aceeasi cale furnizorului.

ART. 29

Prin acceptarea certificatului clientul:

- a) isi asuma responsabilitatea controlului cheii sale private si a luarii unor masuri pentru a preveni pierderea dezvaluirea, modificarea sau utilizarea neautorizata a acesteia;
- b) certifica veridicitatea informatiilor continute in certificat;
- c) se angajeaza sa foloseasca certificatul exclusiv in scopuri autorizate, conform legii;
- d) nu are dreptul de a utiliza cheia sa privata corespunzatoare cheii publice listate in certificat, pentru semnarea altor certificate, decat in cazurile in care acest lucru a fost prevazut expres in contractul semnat cu furnizorul sau.

ART. 30

(1) Furnizorul gestioneaza direct cheile publice ale clientilor persoane fizice si persoane juridice. Gestionarea cheilor publice presupune implicit acordarea tuturor serviciilor de certificare prevazute in contractul cu clientii.

(2) Serviciile de certificare se refera la emiterea, verificarea, suspendarea, reinnoirea, revocarea si furnizarea de informatii cu privire la certificatele emise, precum si depozitarea sigura a acestora pe durata valabilitatii lor, la care se adauga o perioada de minimum 10 ani de la data incetarii valabilitatii certificatului, conform prevederilor art. 20 lit. h) din lege.

(3) Serviciile de verificare a semnaturilor electronice se asigura automat, prin Internet, asemenea servicii fiind mentionate expres in contract.

ART. 31

(1) Arhivele unui furnizor aflat in cazul prevazut la art. 24 alin. (4) din lege sunt preluate de autoritate.

(2) Formularul de informare cu privire la incetarea activitatii unui furnizor de servicii de certificare este prevazut in anexa nr. 9.

(3) In cazul in care autoritatea dispune incetarea activitatii unui furnizor si nu exista un alt furnizor care sa ii preia activitatea, aceasta va asigura revocarea certificateor, daca nu a fost deja realizata de catre furnizor, pe cheltuiala furnizorului; autoritatea va prelua si va mentine arhivele si registrul electronic, fara conectare permanenta la Internet.

ART. 32

Un furnizor poate solicita unui alt furnizor eliberarea unui certificat, cel de-al doilea furnizor gestionand astfel cheia publica a primului. Aceasta situatie este prevazuta in anexa nr. 10.

CAP. 5

Detalii tehnice

SECTIUNEA 1

Datele de creare a semnaturii

ART. 33

Generarea datelor de creare a semnaturii electronice a autoritatii se face utilizand un sistem izolat, fiabil, proiectat special in acest scop, protejat impotriva utilizarii neautorizate.

ART. 34

Autoritatea va folosi pentru semnatura electronica algoritmul RSA.

ART. 35

(1) Lungimea minima a cheii private utilizate de un semnatar pentru crearea semnaturii electronice extinse trebuie sa fie de minim:

- a) 1.024 de biti pentru algoritmul RSA;
- b) 1.024 de biti pentru algoritmul DSA;
- c) 160 de biti pentru algoritmul DSA bazat pe curbe eliptice.

(2) Lungimea nu include secventa de 0 biti de pe cele mai semnificative pozitii.

(3) Generarea repetata de date de creare a semnaturii electronice nu trebuie sa coboare nivelul de siguranta a acesteia, fiind obligatorie conditia de unicitate. Se exclud procedeele de generare a datelor de creare a semnaturii electronice care, prin utilizare repetata, ar putea reduce calitatea cheii.

ART. 36

(1) Numarul minim de biti din datele de creare a semnaturii electronice determinati pe baza unor numere real aleatoare tehnice este de:

- a) 1.024 de biti pentru algoritmul RSA;
- b) 1.024 de biti pentru algoritmul DSA;
- c) 160 de biti pentru algoritmul DSA bazat pe curbe eliptice.

(2) Este interzisa utilizarea numerelor pseudoaleatorii ca punct de pornire in generarea datelor de creare a semnaturii.

(3) Daca sistemul de generare este utilizat pentru obtinerea cheilor mai multor semnatori, calitatea elementelor generate trebuie verificata statistic cel putin o data pe luna. Rezultatele testelor efectuate trebuie inregistrate. In cazul in care rezultatul testului este negativ, toate certificatele emise de la data ultimului test vor fi revocate.

ART. 37

(1) Daca datele de creare a semnaturii sunt generate de furnizorul de servicii de certificare, acesta trebuie sa asigure confidentialitatea acestora, precum si a datelor pe baza carora s-au generat cheile.

(2) Aceleasi prevederi se aplica in cazul operatiunilor de transferare a datelor de creare a semnaturii in dispozitivele de creare a semnaturii, precum si a datelor de identificare a semnatarului necesare in cazul utilizarii dispozitivului.

ART. 38

Daca datele de creare a semnaturii sunt generate de un tert, acesta trebuie sa utilizeze dispozitive de generare fiabile, protejate impotriva utilizarii neautorizate. Fiecare acces la dispozitivul de generare a datelor de creare a semnaturii trebuie monitorizat.

SECTIUNEA a 2-a

Sisteme si proceduri utilizate pentru crearea semnaturii electronice

ART. 39

Autoritatea foloseste doar functia hash-code SHA-1 si algoritmul de criptare RSA. Este interzisa utilizarea teoremei chinezeesti a resturilor.

ART. 40

(1) In vederea obtinerii unei semnaturi electronice extinse se pot utiliza urmatoarele functii hash-code;

- a) RIPEMD - 160;
- b) Functia SHA-1.

(2) Pot fi folosite numere pseudoaleatorii pentru a mari lungimea amprenteii documentului. Algoritmii de criptare a amprenteii, in cazul semnaturii electronice extinse, sunt

- a) RSA;
- b) DSA;
- c) DSA pe curbe eliptice potrivit ISO/IEC 14883-3 anexa A.2.2, IEEE standard P1363, sectiunile 5.3.3, 5.3.4

(3) In cazul algoritmilor ce implica numere aleatorii se pot utiliza numere pseudoaleatorii.

(4) Se considera echivalente si alte proceduri de creare a semnaturii, daca ofera acelasi nivel de securitate certificat de un organism autorizat recunoscut.

ART. 41

Daca pentru declansarea procedurii de creare a semnaturii electronice se foloseste o metoda de acces anume proiectata pentru a preveni utilizarea neautorizata, codul respectiv nu mai trebuie folosit in alt scop.

ART. 42

Formatul semnaturii electronice trebuie sa corespunda prevederilor legale in domeniu - PKCS#7 Standard de sintaxa al mesajelor criptate.

ART. 43

Rezultatul verificarii unei semnaturi electronice extinse este sigur doar daca se utilizeaza un dispozitiv de verificare a semnaturii electronice specificat de catre furnizorul de servicii de certificare care a emis certificatul pe baza caruia se face validarea semnaturii.

SECTIUNEA a 3-a

CertIFICATELE calificcate

ART. 44

In cazul renoirii unui certificat calificat se emite un nou certificat cu aceleasi date de identificare si de verificare a semnaturii electronice, dar cu alte date de valabilitate.

ART. 45

Formatul certificatului calificat, conform art. 13, trebuie sa fie descris de catre furnizor utilizand un limbaj formal standard - CCITT sau Recomandarile ITU-T X.208 -, intr-un document atasat notificarii catre autoritate.

ART. 46

Registrul electronic de evidenta a certificatelor eliberate trebuie sa corespunda unui format recunoscut international. Urmatoarele 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 si profil CRL;
- d) RFC 2589 - LDAPv3 Extensii pentru servicii de director dinamic.

SECTIUNEA a 4-a

Revocarea certificatelor si marcarea timpului

ART. 47

Furnizorul trebuie sa informeze clientii si tertii care pot influenta atributele clientului, inscise in certificatul calificat, cu privire la modul prin care pot solicita revocarea certificatului.

ART. 48

- (1) Marca temporala dovedeste existenta unor date la un moment de timp precizat.
- (2) Prin aplicarea unei astfel de marci, numita time-stamp, se poate demonstra existenta unor informatii la momentul respectiv.
- (3) Serviciile de marcare temporala pot fi furnizate de furnizor sau de tertii, conform standardelor recunoscute ETSI TS 101 861 Stampilare temporala; ETSI TS 101 733 v1. 2.2 (2000-12); RFC3161 Internet X.509 PKI Protocol de stampilare temporala.
- (4) In vederea mentionarii datei si a orei se utilizeaza servicii bazate pe certificate calificate si se foloseste data si ora Europei Centrale, tinandu-se seama de schimbarea orei - ora de vara/iarna. Eroarea maximum admisa este de 1 minut.

CAP. 6

Alte prevederi

ART. 49

Autoritatea trebuie sa verifice un furnizor cel putin o data la 2 ani sau cand se modifica procedurile de lucru.

ART. 50

- (1) Autoritatea dispune suspendarea activitatii furnizorului pana la incetarea cauzelor care au determinat luarea masurii in urmatoarele situatii:
 - a) furnizorul a incalcat obligatiile de confidentialitate prevazute la art. 15 alin. (1) din lege;
 - b) furnizorul nu notifica autoritatea in conditiile prevazute la art. 13 alin. (1) si (2) din lege;
 - c) complementar cu aplicarea sanctiunii contraventionale prevazute la art. 45 din lege;
 - d) furnizorul nu plateste in termenul stabilit despagubirile la plata carora a fost obligat printr-o decizie definitiva si revocabila a unei instante judecatoresti;
 - e) furnizorul nu achita, in cel mult 10 zile, costul operatiunilor prevazute la art. 31 alin. (3).
- (2) In aceasta perioada autoritatea efectueaza verificarea furnizorului si comunica neajunsurile identificate. Autoritatea stabileste un interval de timp de maximum 30 de zile, in care furnizorul trebuie sa rezolve problemele cu care se confrunta.
- (3) Daca furnizorul nu remedieaza deficientele in termenul acordat, autoritatea dispune incetarea activitatii acestuia si/sau retragerea deciziei de acreditare si/sau suspendarea dreptului de a emite certificate calificate, in functie de problemele identificate si de tipul de servicii oferite de furnizor.
- (4) In perioada in care are activitatea suspendata, furnizorul are obligatia sa asigure serviciile de suspendare revocare si verificare a certificatelor, precum si consultarea prin

³identificatorul cheii ³ ³
 ~~~~~  
<sup>3</sup>AuthorityCertSerialNumber <sup>3</sup>Toate<sup>3</sup>Utilizat cu Numele emitentului <sup>3</sup>Nu <sup>3</sup>  
<sup>3</sup>Nr. seriei certificatului <sup>3</sup> <sup>3</sup>certificatului <sup>3</sup> <sup>3</sup>  
 ~~~~~  
³SubjectKeyIdentifier ³Toate³Identifica chei diferite pentru ³Nu ³
³Identificatoru cheii ³ ³acelasi subiect ³ ³
³subiectului ³ ³ ³ ³
 ~~~~~  
<sup>3</sup>KeyUsage <sup>3</sup>Toate<sup>3</sup>Defineste scopuri specifice <sup>3</sup>Optio- <sup>3</sup>  
<sup>3</sup>Folosirea cheii <sup>3</sup> <sup>3</sup>pentru utilizarea cheii (de <sup>3</sup>nala <sup>3</sup>  
<sup>3</sup> <sup>3</sup> <sup>3</sup>exemplu, semnatura digitala, <sup>3</sup> <sup>3</sup>  
<sup>3</sup> <sup>3</sup> <sup>3</sup>key agreement....) <sup>3</sup> <sup>3</sup>  
 ~~~~~  
³PrivateKeyUsagePeriod ³Toate³Numai pentru cheile de semnatura³Optio- ³
³Perioada de utilizare a cheii ³ ³digitala. Semnaturile pe docu- ³nala ³
³private ³ ³mente datate in afara perioadei ³ ³
³ ³ ³sunt invalide ³ ³
 ~~~~~  
<sup>3</sup>CertificatePolicies <sup>3</sup>Toate<sup>3</sup>Identificatori si calificatori <sup>3</sup>Optio- <sup>3</sup>  
<sup>3</sup>Politice de certificare <sup>3</sup> <sup>3</sup>ce identifica si califica poli- <sup>3</sup>nala <sup>3</sup>  
<sup>3</sup> <sup>3</sup> <sup>3</sup>ticile de certificare ce se <sup>3</sup> <sup>3</sup>  
<sup>3</sup> <sup>3</sup> <sup>3</sup>aplica unui certificat <sup>3</sup> <sup>3</sup>  
 ~~~~~  
³PolicyIdentifiers ³Toate³OID = obiectul de identificare ³Optio- ³
³Identificatori de politici de ³ ³a unei politici ³nala ³
³certificare ³ ³ ³ ³
 ~~~~~  
<sup>3</sup>PolicyQualifiers <sup>3</sup>Toate<sup>3</sup>Mai multe informatii privind <sup>3</sup>Optio- <sup>3</sup>  
<sup>3</sup>Atributele politicii de <sup>3</sup> <sup>3</sup>politicile de certificare <sup>3</sup>nala <sup>3</sup>  
<sup>3</sup>certificare <sup>3</sup> <sup>3</sup> <sup>3</sup> <sup>3</sup>  
 ~~~~~  
³Policy Mappings ³AC ³Indica politici echivalente ³Optio- ³
³Suprapunerea de politici ³ ³ ³nala ³
 ~~~~~  
<sup>3</sup> B. Atribute certificat si FSC <sup>3</sup>  
 ~~~~~  
³SubjectAltName ³Toate³Utilizata pentru a lista numele ³Optio- ³
³Numele alternativ al ³ ³alternative (de exemplu numele ³nala ³
³subiectului ³ ³RFC822, adresa X400, adresa ³ ³

³Nr. crt. ³Categorie de date 3 3
~
~

³ 1 ³Persoana (fizica/juridica) 3 3
~
~

³ 2 ³Denumirea persoanei juridice 3 3
~
~

³a. Date despre persoana fizica sau reprezentantul legal al persoanei juridice ³
~
~

³ 3 ³Numele si prenumele 3 3
~
~

³ 4 ³Pseudonimul 3 3
~
~

³ 5 ³Cod identificare client 3 3
~
~

³ 6 ³Data nasterii (ZZ/LL/AAAA) 3 3
~
~

³ 7 ³Locul nasterii 3 3
~
~

³b. Adresa persoanei fizice sau a reprezentantului legal al persoanei juridice ³
3 3
~
~

³ 8 ³Tara 3 3
~
~

³ 9 ³Orasul 3 3
~
~

³ 10 ³Sectorul 3 3
~
~

³ 11 ³Strada 3 3
~
~

³ 12 ³Nr. 3 3
~
~

³ 13 ³Bloc 3 3
~
~

³ 14 ³Apt. 3 3

~AAAAA
AAAAA

Titlu INFORMATII PUSE LA DISPOZITIE DE Cod 08
document CLIENTI IN VEDEREA CERTIFICARII document 33

APLICATIILOR - CERTIFICAT SIMPLU

AAAAA

Pag 2

AAAAA
AAAAA

AAAAA
AAAAA

AAAAA
AAAAA

Date obligatorii despre solicitant

AAAAA
AAAAA

Numele si Pseudonimul E-mail

prenumele

AAAAA
AAAAA

Date optionale despre solicitant

AAAAA
AAAAA

Tara de Oras Judet/Sector

rezidenta

Adresa

AAAAA
AAAAA

Strada Nr. Bloc Scara

AAAAA
AAAAA

Etaj Ap. Cod postal

AAAAA
AAAAA

Telefon Fax

AAAAA
AAAAA

Data B.I./C.I. seria Nr. B.I./

nasterii C.I.

(zz/ll/aaa)

a)

AAAAA
AAAAA

Emis de Valabil pana la Data

data (zz/ll/aaaa) emiterii

(zz/ll/aaaa)

AAAAA
AAAAA

³ ³ ³ ³ ³ data ³ ³
 ~~~~~  
<sup>3</sup>Permis auto nr. <sup>3</sup> <sup>3</sup>Emis de <sup>3</sup> <sup>3</sup>Valabil <sup>3</sup>ZZ/LL/AAAA <sup>3</sup>  
<sup>3</sup> <sup>3</sup> <sup>3</sup> <sup>3</sup>pana la <sup>3</sup> <sup>3</sup>  
<sup>3</sup> <sup>3</sup> <sup>3</sup> <sup>3</sup> data <sup>3</sup> <sup>3</sup>  
 ~~~~~  
³Tip card ³ ³Banca emitenta ³ ³Nr. card³ ³
 ~~~~~  
<sup>3</sup>Data la care <sup>3</sup> ZZ/LL/AAAA <sup>3</sup>  
<sup>3</sup>expira cardul <sup>3</sup> <sup>3</sup>  
 ~~~~~  
³ ³Tara ³ ³Oras ³ ³ ³
 ~~~~~  
<sup>3</sup> Adresa <sup>3</sup>Sector/Judet <sup>3</sup> <sup>3</sup>Strad <sup>3</sup> <sup>3</sup>Nr. <sup>3</sup> <sup>3</sup>  
 ~~~~~  
³ ³Bloc ³ ³Scara ³ ³Ap. ³ ³
 ~~~~~  
<sup>3</sup>Telefon <sup>3</sup> <sup>3</sup>Fax <sup>3</sup> <sup>3</sup>E-mail <sup>3</sup> <sup>3</sup>  
 ~~~~~  
³ Date optionale despre sot/sotie ³
 ~~~~~  
<sup>3</sup>Numele si prenumele <sup>3</sup> <sup>3</sup>Data nasterii <sup>3</sup>ZZ/LL/AAAA <sup>3</sup>  
 ~~~~~  
³ Data despre aplicatii ³
 ~~~~~  
<sup>3</sup>Tip aplicatie; posta electronica, navigare pe web, tranzactii de orice tip,<sup>3 3</sup>  
<sup>3</sup>transfer de fisiere, validare de software, subscribe pe web la anumite <sup>3 3</sup>  
<sup>3</sup>servicii oferite de terti, etc. <sup>3 3</sup>  
 ~~~~~  
³Alte informatii cerute de aplicatiile mentionate mai sus ^{3 3}
 ~~~~~

\*) In cazul modificarii formei sau statutului persoanei juridice, persoana juridica este obligata sa reinnoiasca contractul cu FSC  
 \*\*) In cazul in care se schimba reprezentantul legal sau persoana de contact, persoanele noi desemnate in aceste functii sunt obligate sa se prezinte







