

Norme tehnice și metodologice din 13 decembrie 2001 pentru aplicarea Legii nr. 455/2001 privind semnătura electronică

CAPITOLUL I: Dispoziții 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 a art. 4 din Legea nr. 455/2001 privind semnătura electronică, denumită în continuare lege.

Art. 2

(1) În înțelesul prezentelor norme tehnice și metodologice, termenii utilizați au următoarele definiții:

a) client – beneficiarul serviciilor de certificare, care, în baza unui contract încheiat cu un furnizor de servicii de certificare, denumit în continuare furnizor, deține o pereche funcțională cheie publică-cheie privată și are o identitate probată printr-un certificat digital emis de acel furnizor;

b) hash-code – funcție care returnează amprenta unui document electronic;

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

e) mecanismul de creare a semnăturii electronice – asupra documentului se aplică o funcție hash-code, obținându-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 funcției hash-code și semnăturii electronice primite. Verificarea semnăturii este operație automată;

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

(2) În înțelesul prezentelor norme, abrevierile utilizate au următoarele semnificații:

a) ETSI – Institutul European de Standarde în Telecomunicații;

- 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 Național de Standarde și Tehnologie din Statele Unite ale Americii;
- d)IEEE – Institutul de Inginerie Electrică și Electronică;
- e)ITSEC – desemnează standardele și criteriile europene de evaluare a securității sistemelor informatice;
- f)RSA – algoritmul de criptare cu cheie publică, dezvoltat de cercetătorii Rivest, Shamir și 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 și a fonturilor de dimensiuni diferite, precum și inserarea altor obiecte;
- k)PDF – format ce permite transferarea documentelor electronice fără a afecta aranjarea în pagină; documentele pot conține text, imagini și 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 și supraveghere

Art. 3

(1)Autoritatea de reglementare și supraveghere, denumită în continuare autoritate, generează sau achiziționează o pereche funcțională cheie privată-cheie publică și trebuie să își protejeze cheia sa privată, utilizând un sistem fiabil și 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 registru

Art. 5

Conținutul informațional și structura registrului sunt prezentate în anexa nr. 1.

Art. 6

(1) Actualizarea registrului se face exclusiv de către autoritate și urmărește toate modificările survenite statutul furnizorului – acreditare, terminarea perioadei de acreditare, suspendare, îmbogățirea tipurilor de certificate oferite.

(2) După fiecare actualizare autoritatea transmite furnizorului o copie de pe documentul 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 și datelor conform standardelor recunoscute – ISO/IEC 15408-1, 2, 3 și 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) tipul furnizorului – persoană fizică sau juridică;
- b) numele sau denumirea furnizorului;
- c) data la care și-a început activitatea;
- d) cheia publică a furnizorului;
- e) indicații privind acreditarea – acreditat sau neacreditat;
- f) perioada de acreditare – început/sfârșit;
- 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 neguvernamentală, alte tipuri;
- j) adresa sau sediul – țară, oraș, județ/sector, stradă număr, bloc, scară, etaj, apartament, cod poștal;
- k) naționalitatea, pentru persoană juridică;
- l) cetățenia, pentru persoană fizică;
- m) telefon, fax, e-mail, adresă în 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 semnăturii electronice utilizate;
- p) situația dispozitivelor – dacă sunt omologate sau nu;
- 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 la art. 8 din prezentele norme tehnice și metodologice 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 și metodologice privind aplicarea legii 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) și (2).

CAPITOLUL III: Furnizorii de servicii de certificare

SECȚIUNEA 1: Dispoziții comune

Art. 10

(1) Un furnizor este obligat să genereze sau să achiziționeze o pereche funcțională cheie privată-cheie publică și să își protejeze cheia sa privată, utilizând un sistem fiabil și 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 și în format electronic, documentul electronic fiind semnat digital de către furnizor și prezentat în unul dintre următoarele formate: RTF, PDF, TXT și PostScript.

Art. 12

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

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

SECȚIUNEA 2: Furnizarea serviciilor de certificare calificată

Art. 13

(1) Furnizorul poate furniza servicii de certificare bazate pe certificate simple și 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 și cu Recomandările ITU-T X. 509.

(3) Autoritatea va publica eventualele modificări ale formatului descris, pe baza evoluției tehnologiilor sau a normelor internaționale recunoscute în domeniu.

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

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

(6) Codul personal de identificare a semnatarului rezultă prin alipirea codului de identificare a furnizorului, inițialele numelui sau pseudonimului semnatarului și numărul de ordine al acestuia în lista clienților cu aceleași inițiale.

Art. 14

(1)În vederea emiterii de certificate calificate furnizorul trebuie să îndeplinească condițiile enunțate la art. 20-22 din lege.

(2)Furnizorul trebuie să dovedească autorității că dispune de resursele financiare pentru acoperirea prejudiciilor pe care le-ar putea cauza cu prilejul desfășurării activității de certificare și trebuie să fie capabil să acopere pierderile suferite de către o persoană care își întemeiază conduita pe efectele juridice ale certificatelor calificate, până la concurența echivalentului în lei al sumei de 10.000 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 obligații prevăzute de lege. Furnizorul va trebui să depună o scrisoare de garanție din partea unei instituții financiare de specialitate sau o poliță de asigurare la o societate de asigurări, în favoarea autorității, în valoare ce puțin egală cu echivalentul în lei al sumei de 500.000 euro; scrisoarea de garanție are forma prevăzută în anexa nr. 5.

(3)Furnizorul trebuie să asigure un nivel de securitate a sistemelor, comunicațiilor, tranzacțiilor și 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 să asigure operarea rapidă a registrului de evidență a certificatelor, conform art. 20 lit. b) din lege; structura registrului este prezentată în anexa nr. 6.

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

(6)Autoritatea verifică datele conținute în documentația depusă, în termen de maximum 10 zile, în raport cu stan dardele recunoscute și cu prezentele norme tehnice ș metodologice.

(7)Autoritatea trebuie să informeze furnizorul, în termen de maximum 10 zile, cu privire la îndeplinirea condițiilor ș să solicite, dacă e cazul, completarea documentației.

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

(9)Dacă documentația nu a fost completată sau nu îndeplinește condițiile, 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 ș în format electronic, semnat digital de autoritate.

Art. 15

În cazul în care nu mai sunt îndeplinite condițiile prevăzute la 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 și îndeplinirea tuturor condițiilor legale. Decizia este comunicată furnizorului pe suport de hârtie și în format electronic, semnat digital de autoritate.

SECȚIUNEA 3: Acreditarea voluntară

Art. 16

(1)Furnizorul care dorește să își desfășoare activitatea ca furnizor acreditat trebuie să solicite obținerea acreditării din partea autorității.

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

(3)Verificările se fac atât asupra declarațiilor conținute în documentația depusă la autoritate, cât și asupra concordanței dintre sistemele, procedurile și practicile afirmate și cele existente în realitate.

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

(5)Autoritatea trebuie să informeze în termen de maximum 30 de zile furnizorul cu privire la îndeplinirea condițiilor și să solicite, dacă e cazul, completarea documentației.

Art. 17

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

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

(3)La cererea furnizorului autoritatea actualizează registrul prin înscrierea noului statut de furnizor acreditat. Se introduc informații despre garanții, omologarea dispozitivelor, agenția de omologare, perioada de acreditare.

Art. 18

(1)Durata acreditării este de 3 ani și se poate reînnoi.

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

Art. 19

Suspendarea deciziei de acreditare se face în următoarele cazuri:

a) se constată că furnizorul nu mai îndeplinește una sau mai multe dintre condițiile prevăzute pentru acordarea deciziei de acreditare. În acest caz autoritatea notifică furnizorului și stabilește un interval de timp de maximum 30 de zile în care furnizorul trebuie să remedieze deficiențele semnalate;

b) declanșarea procedurii falimentului furnizorului.

Art. 20

Autoritatea retrage decizia de acreditare în următoarele cazuri:

a) dacă furnizorul nu remediază deficiențele prevăzute a art. 19 lit. a), în termenul acordat de către autoritate;

b) dacă intervine o hotărâre judecătorească definitivă și revocabilă prin care se declară falimentul furnizorului.

SECȚIUNEA 4: Agrearea agențiilor de omologare

Art. 21

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

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

(3) Decizia se retrage în cazul în care se constată că agenția nu mai îndeplinește condițiile prevăzute la alin. (1) și (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 și procedurile de utilizare a semnăturii electronice sunt prevăzute în anexa nr. 7.

Art. 23

Orice persoană, fizică sau juridică, care dorește ca un furnizor să îi 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 funcțională 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 și 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 listate în certificat;
- c) dacă informația listată în certificat este exactă.

Art. 25

(1) Durata verificării informațiilor din cerere și a eliberării certificatului nu poate depăși:

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

(2) Termenele prevăzute la alin. (1) se calculează din momentul primirii de către furnizorul în cauză a tuturor informațiilor cerute pentru acest scop.

Art. 26

Furnizorul nu poate emite un certificat fără consimțământul expres al celui pe numele căruia este emis.

Art. 27

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

Art. 28

Certificatul poate fi transmis solicitantului în următoarele modalități:

- a) personal;
- b) prin poștă, cu confirmare de primire;
- c) prin poștă electronică – numai pentru certificate simple; observațiile, dacă există, se comunică pe aceeași cale furnizorului.

Art. 29

Prin acceptarea certificatului clientul:

- a) își asumă responsabilitatea controlului cheii sale private și a luării unor măsuri pentru a preveni pierderea, dezvăluirea, modificarea sau utilizarea neautorizată a acesteia;
- b) certifică veridicitatea informațiilor conținute în certificate;
- 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 listate în certificat, pentru semnarea altor certificate, decât în cazurile în care acest lucru fost prevăzut expres în contractul semnat cu furnizorul său

Art. 30

(1)Furnizorul gestionează direct cheile publice ale clienților persoane fizice și 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 și furnizarea de informații cu privire la certificatele emise, precum și 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 și nu există un alt furnizor care să îi preia activitatea, aceasta va asigura revocarea certificatelor, dacă nu a fost deja realizată de către furnizor, pe cheltuiuala furnizorului; autoritatea va prelua și va menține arhivele și registrul electronic, fără conectare permanentă a 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)1.024 de biți pentru algoritmul RSA;

b)1.024 de biți pentru algoritmul DSA;

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

(2)Lungimea nu include secvența de 0 biți 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 reale aleatoare tehnice este de:

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

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

(3) Dacă sistemul de generare este utilizat pentru obținerea cheilor mai multor semnături, calitatea elementelor lor 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 și a datelor pe baza cărora s-au generat cheile.

(2) Aceleași prevederi se aplică în cazul operațiunilor de transferare a datelor de creare a semnăturii în dispozitivele de creare a semnăturii, precum și a 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.

SECȚIUNEA 2: Sisteme și proceduri utilizate pentru crearea semnăturii electronice

Art. 39

Autoritatea folosește doar funcția hash-code SHA-1 și algoritmul de criptare RSA. Este interzisă utilizarea teoremei chinezești a resturilor.

Art. 40

(1) În vederea obținerii unei semnături electronice extinse se pot utiliza următoarele funcții hash-code

- a) RIPEMD – 160;
- b) Funcția SHA-1.

(2) Pot fi folosite numere pseudoaleatorii pentru a măări 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, secțiunile 5.3.3, 5.3.4

(3) În cazul algoritmilor ce implică numere aleatorii se pot utiliza numere pseudoaleatorii.

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

Art. 41

Dacă pentru declanșarea procedurii de creare a semnăturii electronice se folosește 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.

SECȚIUNEA 3: Certificatele calificate

Art. 44

În cazul reînnoirii unui certificat calificat se emite un nou certificat cu aceleași date de identificare și de verificare a semnăturii electronice, dar cu alte date de valabilitate.

Art. 45

Formatul certificatului calificat, conform art. 13, trebuie să fie descris de către furnizor utilizând un limbaj formal standard – CCITT sau Recomandările ITU-T X.208 -, într-un document atașat notificării către autoritate.

Art. 46

Registrul electronic de evidență a certificatelor eliberate trebuie să corespundă unui format recunoscut internațional. 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 și profil CRL;
- d)RFC 2589 – LDAPv3 Extensii pentru servicii de director dinamic.

SECȚIUNEA 4: Revocarea certificatelor și marcarea timpului

Art. 47

Furnizorul trebuie să informeze clienții și terții care pot influența atributele clientului, înscrise în certificatul calificat, cu privire la modul prin care pot solicita revocarea certificatului.

Art. 48

- (1)Marca temporală dovedește existența unor date la un moment de timp precizat.
- (2)Prin aplicarea unei astfel de mărci, numită time-stamp, se poate demonstra existența unor informații la momentul respectiv.
- (3)Serviciile de marcă temporală pot fi furnizate de furnizor sau de terți, conform standardelor recunoscute – ETSI TS 101 861 Ștampilare temporală; ETSI TS 101 733 v1. 2.2 (2000-12); RFC3161 Internet X.509 PKI Protocol de ștampilare temporală.
- (4)În vederea menționării datei și a orei se utilizează servicii bazate pe certificate calificate și se folosește data și ora Europei Centrale, ținându-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 puțin o dată la 2 ani sau când se modifică procedurile de lucru.

Art. 50

- (1)Autoritatea dispune suspendarea activității furnizorului până la încetarea cauzelor care au determinat luarea măsurii în următoarele situații:
 - a)furnizorul a încălcat obligațiile de confidențialitate prevăzute la art. 15 alin. (1) din lege;
 - b)furnizorul nu notifică autoritatea în condițiile prevăzute a art. 13 alin. (1) și (2) din lege;
 - c)complementar cu aplicarea sancțiunii contravenționale prevăzute la art. 45 din lege;

d) furnizorul nu plătește în termenul stabilit despăgubirile a plata cărora a fost obligat printr-o decizie definitivă și revocabilă a unei instanțe judecătorești;
e) furnizorul nu achită, în cel mult 10 zile, costul operațiunilor prevăzute la art. 31 alin. (3).

(2) În această perioadă autoritatea efectuează verifica rea furnizorului și comunică neajunsurile identificate. Autoritatea stabilește un interval de timp de maximum 30 de zile, în care furnizorul trebuie să rezolve problemele cu care se confruntă.

(3) Dacă furnizorul nu remediază deficiențele în termenul acordat, autoritatea dispune încetarea activității acestuia și/sau retragerea deciziei de acreditare și/sau suspendarea dreptului de a emite certificate calificate, în funcție de problemele identificate și de tipul de servicii oferite de furnizor.

(4) În perioada în care are activitatea suspendată, furnizorul are obligația să asigure serviciile de suspendare, revocare și verificare a certificatelor, precum și consultarea prin Internet a registrului electronic, cu excepția cazului în care deficiențele se găsesc la nivelul acestor sisteme.

Art. 51

În cazurile prevăzute la art. 50 alin. (1) lit. d) și e) autoritatea are dreptul de a emite pretenții asupra scrisorii de garanție sau a poliței 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 să îndeplinească condițiile prevăzute la art. pct. 8 și la art. 20 lit. f) din lege, în cazul în care sunt conforme cu cel puțin unul dintre:

a) standardele române sau părțile relevante ale acestora, care adoptă acele standarde europene armonizate ale căror numere de referință au fost publicate în Jurnalul Oficial al Comunităților Europene, în măsura în care condițiile în cauză sunt acoperite de aceste standarde;

b) standardele europene armonizate ale căror numere de referință au fost publicate în Jurnalul Oficial al Comunităților Europene, în măsura în care condițiile în cauză sunt acoperite de aceste standarde;

c) standardele române sau părțile relevante ale acestora, adoptate potrivit dispozițiilor legale în vigoare, în măsura în care condițiile în cauză sunt acoperite de aceste standarde și 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 comunicațiilor și tehnologie informației.

Art. 53

Dispozitivele securizate de creare semnăturii electronice, recunoscute ca fiind conforme cu cerințele anexei III a Directivei 1999/93/EC de un organism desemnat de unul dintre statele membre ale Uniunii Europene să efectueze determinări ale conformității 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 dintre 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 dintre România, pe de o parte, și Comunitatea Europeană și statele membre, pe de altă parte.

Art. 55

Anexele nr. 1-10 fac parte integrantă din prezentele norme tehnice și metodologice.