

În temeiul prevederilor art. 25 din Legea nr. 455/2001 privind semnătura electronică, precum și ale art. 6 alin. (3) pct. 3 și ale art. 8 alin. (1), (3) și (5) din Ordonanța de urgență a Guvernului nr. 106/2008 privind înființarea Autorității Naționale pentru Comunicații,

PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU COMUNICAȚII

emite prezenta:

DECIZIE

privind mecanismul de verificare a semnăturilor electronice

Art. 1. – Prezenta decizie stabilește principiile generale referitoare la serviciile de verificare a semnăturilor electronice, pe care furnizorii de servicii de certificare trebuie să le pună la dispoziția utilizatorilor ca parte a serviciilor de certificare, în conformitate cu art. 30 din Normele tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică, aprobate prin Hotărârea Guvernului nr. 1259/2001, cu modificările și completările ulterioare.

Art. 2. – În înțelesul prezentei decizii, următorii termeni se definesc astfel:

a) *verificarea semnăturii electronice* – operațiunea tehnică ce are ca scop determinarea validității unei semnături electronice, realizată pe baza datelor de verificare a semnăturii electronice, cu ajutorul unui dispozitiv de verificare;

b) *verificator* – orice persoană care dorește verificarea unei semnături electronice și posedă datele de verificare a acesteia;

c) *mecanism de verificare a semnăturilor electronice (mecanism de verificare)* – serviciul de verificare a semnăturii electronice pe care furnizorul de servicii de

certificare îl pune la dispoziția utilizatorilor și terților la distanță, prin intermediul internetului.

Art. 3. – (1) Semnătura electronică aplicată unui document electronic este considerată validă dacă sunt îndeplinite următoarele condiții:

a) semnătura electronică a fost creată utilizându-se cheia privată aferentă certificatului digital folosit la semnare;

b) certificatul digital folosit la semnare era în perioada de valabilitate și nu era suspendat sau revocat la momentul creării semnăturii electronice;

c) documentul electronic nu a fost modificat ulterior aplicării semnăturii electronice.

Art. 4. – Mecanismul de verificare trebuie să garanteze că:

a) datele utilizate pentru verificarea semnăturii electronice corespund cu datele afișate verficatorului;

b) semnătura electronică este verificată cu certitudine, iar rezultatul verificării este corect afișat;

c) verficatorul poate să determine cu certitudine conținutul datelor semnate;

d) autenticitatea și valabilitatea certificatului solicitat în momentul verificării semnăturii electronice sunt verificate cu certitudine;

e) rezultatul verificării și identitatea semnatarului sunt corect afișate;

f) utilizarea unui pseudonim este clar indicată;

g) orice modificări care pot influența securitatea pot fi detectate.

Art. 5. – În vederea îndeplinirii condițiilor de la art. 4, furnizorul de servicii de certificare trebuie să implementeze următoarele măsuri tehnice:

a) operațiunea de verificare folosește următoarele date de intrare:

1. documentul inițial;

2. semnătura electronică aplicată documentului inițial;

3. certificatul pe baza căruia a fost creată semnătura electronică;

4. alte date de verificare a semnăturii electronice.

b) operațiunea de verificare poate avea următoarele rezultate:

1. verificare reușită – răspuns care indică că semnătura electronică este validă;
2. verificare eșuată – răspuns care indică că semnătura electronică nu este validă și precizează motivul care a determinat acest rezultat;
3. verificare incompletă – răspuns care indică că verificarea nu a eșuat, dar nu există suficiente informații pentru a se determina dacă semnătura electronică este sau nu este validă.

c) mecanismul de verificare conține măsuri de securitate împotriva atacurilor care ar avea ca scop alterarea procesului de verificare sau furnizarea către verificator a unor informații false cu privire la rezultatul procesului de verificare.

Art. 6. – Mecanismul de verificare trebuie să cuprindă cel puțin următoarele elemente:

- a) procesul de verificare a semnăturii electronice;
- b) interfața care permite introducerea documentului semnat care trebuie verificat și selectarea semnăturii care trebuie verificată (pentru documentele care au aplicate mai multe semnături);
- c) interfața de prezentare a documentului semnat, care să permită vizualizarea documentului în formatul în care a fost creat, oferind verficatorului posibilitatea de a identifica cu claritate conținutul documentului care a fost semnat;
- d) interfața de prezentare a informațiilor referitoare la identitatea semnatarului și a rezultatului verificării semnăturii electronice;
- e) comunicarea cu bazele de date ale furnizorului de servicii de certificare care conțin informațiile necesare verificării semnăturilor electronice.

Art. 7. – Mecanismul de verificare trebuie să permită verificarea documentelor care au aplicate mai multe semnături electronice, oferind utilizatorului posibilitatea de alegere a semnăturii electronice care trebuie verificată.

Art. 8. – Mecanismul de verificare trebuie să fie capabil să ofere verficatorului următoarele informații:

- a) numele sau pseudonimul persoanei asociate de către furnizorul de servicii de certificare cu certificatul folosit la semnare;
- b) momentul de timp la care semnătura a fost creată, atunci când această informație este disponibilă;
- c) informațiile conținute în certificatul semnatarului;
- d) lanțul de certificare.

Art. 9. – În vederea asigurării conformității cu cerințele prezentei decizii, se recomandă folosirea de dispozitive de verificare a semnăturii electronice și de proceduri conforme standardului SR CWA 14171:2003 (Proceduri pentru verificarea semnăturii electronice) și versiunile ulterioare ale acestuia.

**PREȘEDINTE,
Dorin Liviu NISTORAN**

București, 2008

Nr.