



CANCELARIA DE STAT A REPUBLICII MOLDOVA

Nr. 1453-1028

Chișinău

«23» 12 2013

Biroul Permanent
al Parlamentului
Republicii Moldova

Se prezintă spre examinare *proiectul de lege privind semnătura electronică și documentul electronic* (autor – Ministerul Tehnologiei Informației și Comunicațiilor), aprobat prin Hotărîrea Guvernului nr. 1042 din 23 decembrie 2013.

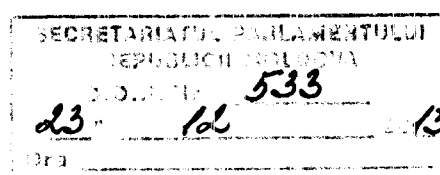
Anexă: Hotărîrea Guvernului nr. 1042 din 22 decembrie 2013 – 2 ex.

Proiectul de lege privind semnătura electronică
și documentul electronic
în ambele limbi – 1 ex.

Notă informativă – 1 ex.

Secretar general al Guvernului

Victor BODIU





GUVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr. 1042

din 23 decembrie 2013

Chișinău

**Pentru aprobarea proiectului de lege privind
semnătura electronică și documentul electronic**

Guvernul HOTĂRĂȘTE:

Se aprobă și se prezintă Parlamentului spre examinare proiectul de lege privind semnătura electronică și documentul electronic.

Prim-ministru

IURIE LEANCĂ

Contrasemnează:

Viceprim-ministru,
ministrul economiei

Valeriu LAZĂR

Ministrul tehnologiei
informației și comunicațiilor

Pavel Filip

Ministrul justiției

Oleg Efrim

PARLAMENTUL REPUBLICII MOLDOVA

LEGE

privind semnătura electronică și documentul electronic

Parlamentul adoptă prezenta lege organică.

Prezenta lege creează cadrul necesar aplicării Directivei nr. 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice, publicat în Jurnalul Oficial al Comunităților Europene nr. L 13 din 19 ianuarie 2000.

Capitolul I DISPOZIȚII GENERALE

Articolul 1. Scopul legii și domeniul de aplicare

(1) Prezenta lege stabilește regimul juridic al semnăturii electronice și al documentului electronic, inclusiv cerințele principale față de valabilitatea acestora și cerințele principale față de serviciile de certificare.

(2) Prezenta lege nu limitează modalitatea de utilizare a documentelor.

(3) Recunoașterea semnăturii electronice și a documentului electronic în afara Republicii Moldova se stabilește prin tratate internaționale la care Republica Moldova este parte. În cazul în care tratatele internaționale la care Republica Moldova este parte stabilesc alte norme decât cele stabilite de prezenta lege, se aplică normele tratatelor internaționale.

Articolul 2. Noțiuni principale

În sensul prezentei legi, se definesc următoarele noțiuni:

a) *acreditare voluntară* – autorizație care prevede drepturi și obligații specifice prestării de servicii de certificare, acordată, la cererea prestatorului de servicii de certificare în cauză, de către organul competent de stabilirea drepturilor și obligațiilor respective și de supravegherea respectării acestora, în cazul în care prestatorul de servicii de certificare nu are dreptul să exercite drepturile care decurg din autorizație pînă nu a primit decizia organului respectiv;

b) *autenticitate a documentului electronic* – calitate a documentului electronic care constă în faptul că acesta este semnat de persoana care deține o semnătură electronică autentică și este abilitată cu drept de semnătură;

c) *arhiva electronică securizată* – depozit structurat de documente electronice, care asigură confidențialitatea, nonrepudierea și integritatea acestora, și care garantează valoarea probantă a acestora în timp;

d) *certificat al cheii publice* – document electronic ce conține cheia publică, semnat cu semnătura electronică a prestatorului de servicii de certificare, ce atestă apartenența cheii respective titularului certificatului cheii publice, precum și permite identificarea acestui titular;

e) *certificat calificat al cheii publice* – certificat al cheii publice care întrunește cerințele prevăzute de articolul 31 din prezenta lege și este eliberat de un prestator de servicii de certificare, care întrunește cerințele prevăzute de articolul 26 din prezenta lege;

f) *cheie privată* – consecutivitate digitală unică, formată cu utilizarea dispozitivului de creare a semnăturii și destinate pentru crearea semnăturii respective;

g) *cheie publică* – consecutivitate digitală unică, formată cu utilizarea dispozitivului de creare a semnăturii, ce corespunde cheii private interdependente, destinată să verifice autenticitatea semnăturii electronice;

h) *circulație electronică a documentelor* – totalitatea proceselor de creare, prelucrare, expediere, recepționare, păstrare, modificare și/sau nimicire a documentelor electronice;

i) *date de creare a semnăturii electronice* – date unice, precum codurile sau cheile private, care sînt utilizate de semnatar pentru a crea o semnătură electronică;

j) *date de verificare a semnăturii electronice* – date, precum codurile sau cheile publice, care sînt utilizate în scopul verificării unei semnături electronice;

k) *dispozitiv de creare a semnăturii electronice* – unitate de software și (sau) hardware configurată, utilizată pentru punerea în aplicare a datelor de creare a semnăturii;

l) *dispozitiv securizat de creare a semnăturii electronice* – dispozitiv de creare a semnăturii electronice care întrunește cerințele prevăzute de aliniatele (3) și (4) articolul 8 al prezentei legi;

m) *dispozitiv de verificare a semnăturii electronice* – unități de software și (sau) hardware configurate, utilizate la aplicarea datelor de verificare a semnăturilor;

n) *document electronic* – informația în formă electronică, creată, structurată, prelucrată, păstrată și/sau transmisă cu ajutorul computerului sau al altor dispozitive electronice, semnată cu semnătură electronică, în conformitate cu prezenta lege;

o) *destinatar al documentului electronic* – persoana fizică sau juridică, căreia îi este adresat documentul electronic sau altă persoană care, în condițiile legii sau ale contractului, recepționează documentul electronic;

p) *intermediar în circulația electronică a documentelor* – întreprinzător individual sau persoana juridică care, din însărcinarea alcătuitorului și/sau al

destinatarului documentului electronic, organizează și administrează sistemul de circulație electronică a documentelor și/sau prestează servicii legate de circulația electronică a documentelor;

q) *marca temporală* – atribut al documentului electronic, care, prin intermediul semnăturii electronice, certifică faptul că informația a existat la un moment de timp determinat, cu păstrarea autenticității și integrității documentului electronic;

r) *prestator de servicii de certificare* – întreprinzător individual sau persoana juridică care prestează servicii de certificare;

s) *produs asociat semnăturii electronice* – unități de hardware sau software sau componente specifice ale acestora, destinate pentru utilizare de un prestator de servicii de certificare la prestarea serviciilor de certificare sau pentru crearea sau verificarea semnăturilor electronice;

t) *registru împuternicirilor de reprezentare în baza semnăturii electronice* – registrul ținut în format electronic în care sînt consemnate împuternicirile de reprezentare în baza semnăturii electronice acordate de către persoane fizice sau juridice unei alte persoane;

u) *semnatar* – persoană care deține un dispozitiv de creare a semnăturii electronice și care acționează fie în nume propriu, fie în numele persoanei fizice, al persoanei juridice sau al entității pe care o reprezintă;

v) *semnătura electronică* – date în formă electronică, atașate la sau logic asociate cu alte date în formă electronică, și care sînt utilizate ca metodă de autentificare;

w) *servicii de certificare* – servicii de certificare a cheilor publice, de aplicare a mărcii temporale, precum și alte servicii conexe în domeniul semnăturii electronice;

x) *sistemul de circulație electronică a documentelor* – sistem tehnico-organizatoric ce asigură circulația documentelor electronice.

Capitolul II

REGIMUL JURIDIC AL SEMNĂTURII ELECTRONICE

Articolul 3. Principiile de utilizare a semnăturii electronice

Principiile de utilizare a semnăturii electronice sînt următoarele:

a) libertatea alegerii și utilizării oricărui tip de semnătură electronică, dacă cerința de utilizare a tipului concret de semnătură electronică, în corespundere cu obiectivele de utilizare a acesteia, nu este prevăzută în actele normative sau în acordul părților;

b) posibilitatea utilizării oricărei tehnologii și/sau a mijloacelor tehnice care permit utilizarea tipurilor concrete de semnătură electronică, în conformitate cu cerințele prezentei legi;

c) neadmiterea invocării lipsei de putere juridică a semnăturii electronice și/sau a documentului electronic semnat prin intermediul acesteia, doar în baza faptului că semnătura electronică nu a fost creată cu mîna proprie, dar cu utilizarea dispozitivului de creare a semnăturii și/sau a produsului asociat semnăturii electronice.

Articolul 4. Tipuri de semnături electronice

(1) Tipurile de semnături electronice, ale căror principii și mecanisme de utilizare sînt reglementate de prezenta lege, sînt următoarele:

- a) semnătura electronică simplă;
- b) semnătura electronică avansată necalificată;
- c) semnătura electronică avansată calificată.

(2) Semnătura electronică simplă este semnătura electronică utilizată ca metodă de autentificare, fără trimitere exclusiv la semnatar.

(3) Semnătura electronică avansată necalificată este o semnătură electronică ce îndeplinește următoarele cerințe:

- a) face trimitere exclusiv la semnatar;
- b) permite identificarea semnatarului;
- c) a fost creată prin mijloace pe care semnatarul le poate păstra exclusiv sub controlul său; și
- d) este legată de datele la care se raportează astfel încît orice modificare ulterioară a datelor poate fi detectată.

(4) Semnătura electronică avansată calificată este o semnătură electronică care îndeplinește toate cerințele semnăturii electronice avansate necalificate și, suplimentar:

a) se bazează pe un certificat calificat al cheii publice emis de un prestator de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate;

b) este creată cu utilizarea dispozitivului securizat de creare a semnăturii electronice și se verifică securizat cu utilizarea dispozitivului de verificare a semnăturii electronice și/sau produsului asociat semnăturii electronice care dispun de confirmarea corespunderii cerințelor prevăzute de prezenta lege.

Articolul 5. Regimul juridic de utilizare a semnăturii electronice

(1) Semnătura electronică, indiferent de gradul de protecție de care dispune, produce efecte juridice și este acceptată ca probă, inclusiv în cadrul procedurilor judiciare, chiar dacă:

- a) se prezintă în formă electronică; sau
- b) nu se bazează pe un certificat eliberat de un prestator acreditat de servicii de certificare; sau
- c) nu se bazează pe un certificat calificat al cheii publice; sau
- d) nu este creată printr-un dispozitiv securizat de creare a semnăturii.

(2) Semnătura electronică avansată calificată dispune de aceeași valoare juridică ca și semnătura olografă.

(3) Modalitatea în care se va asigura gradul de protecție al semnăturii electronice avansate calificate pentru echivalarea acesteia cu semnătura olografă aplicată pe hîrtie se stabilește de organul competent, conform atribuțiilor prevăzute de articolul 36 alineatul (1) din prezenta lege.

(4) Pentru semnăturile electronice aplicate de către funcționarii autorităților publice, Guvernul aprobă modul de aplicare a acestora.. Subiecții de drept privat pot stabili condiții mai stricte față de semnăturile electronice aplicate pe documentele electronice pentru autentificare.

(5) Semnătura electronică nu constituie un mijloc de criptare a informației.

Articolul 6. Recunoașterea semnăturilor electronice străine

(1) Certificatul cheii publice eliberat de către un prestator de servicii de certificare cu domiciliul sau cu sediul într-un alt stat este recunoscut ca fiind echivalent din punct de vedere al efectelor juridice cu certificatul cheii publice eliberat de un prestator de servicii de certificare cu domiciliul sau cu sediul în Republica Moldova, dacă:

a) prestatorul de servicii de certificare cu domiciliul sau sediul în alt stat a fost acreditat în cadrul regimului de acreditare, în condițiile prevăzute de prezenta lege;

b) un prestator de servicii de certificare acreditat, cu domiciliul sau cu sediul în Republica Moldova, garantează recunoașterea certificatului;

c) certificatul sau prestatorul de servicii de certificare care l-a eliberat este recunoscut prin aplicarea unui acord bilateral sau multilateral între Republica Moldova și alte state sau organizații internaționale, pe baza de reciprocitate.

(2) Semnătura electronică și documentul electronic semnat prin intermediul acesteia nu pot fi considerate lipsite de putere juridică doar în baza faptului că certificatul cheii publice a fost eliberat în corespundere cu normele unui stat străin.

Articolul 7. Cheia privată și cheia publică

(1) Cheia privată și cheia publică care se folosesc pentru crearea semnăturii electronice avansate necalificate se creează de către persoana fizică. Acestea pot fi create de persoane terțe, prin acordul expres al persoanei fizice respective, cu condiția asigurării imposibilității de copiere a acestora.

(2) Cheia privată și cheia publică, care se folosesc pentru crearea semnăturii electronice avansate calificate, se creează de către prestatorul de servicii de certificare, cu utilizarea dispozitivului securizat de creare a semnăturii. În cazul utilizării dispozitivului securizat de creare a semnăturii în baza cartelei SIM, prestatorul de servicii de certificare asigură persoanei fizice inițierea procedurii de creare a cheii private și cheii publice.

(3) Cheia privată și cheia publică interdependente se creează concomitent.

(4) Persoana fizică poate fi titular al unui număr nelimitat de chei private și chei publice.

(5) Cheia privată este păstrată și utilizată exclusiv de către titular, într-un mod ce exclude accesul la ea al altei persoane.

(6) Cheia publică este certificată de către prestatorul de servicii de certificare și este accesibilă tuturor.

Articolul 8. Crearea semnăturii electronice

(1) Crearea semnăturii electronice se efectuează prin intermediul dispozitivului de creare a semnăturii electronice și/sau produsului asociat semnăturii electronice cu utilizarea datelor de creare a semnăturii electronice.

(2) La crearea semnăturii electronice simple părțile se bazează pe prevederile acordului încheiat.

(3) La crearea semnăturii electronice avansate necalificate și semnăturii electronice avansate calificate dispozitivul de creare a semnăturii electronice și/sau produsul asociat semnăturii electronice trebuie:

a) să ofere posibilitatea afișării conținutului documentului electronic semnat cu semnătură electronică sau să facă referința irevocabilă la documentul dat;

b) să creeze o semnătură electronică numai după confirmarea de către semnatar a operațiunii de creare a semnăturii electronice;

c) să confirme în mod univoc crearea semnăturii electronice.

(4) Dispozitivele securizate de creare a semnăturii electronice trebuie cel puțin să asigure, prin mijloace tehnice și proceduri corespunzătoare, că:

a) datele de creare a semnăturii utilizate pentru crearea semnăturii nu pot apărea decât o singură dată, iar confidențialitatea acestora este asigurată în conformitate cu prezenta lege;

b) datele de creare a semnăturii utilizate pentru crearea semnăturii electronice nu pot fi deduse și că semnătura este protejată împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată;

c) datele de creare a semnăturii utilizate la crearea semnăturii electronice trebuie să fie protejate în mod fiabil de semnatarul legitim împotriva utilizării de către alte persoane.

(5) Dispozitivele securizate de creare a semnăturii electronice nu trebuie să modifice datele care urmează să fie semnate sau să împiedice prezentarea lor semnatarului înainte de procesul de semnare.

Articolul 9. Verificarea autenticității semnăturii electronice

(1) Verificarea autenticității semnăturii electronice se efectuează prin intermediul dispozitivului de verificare a semnăturii electronice și/sau produsului asociat semnăturii electronice, cu utilizarea datelor de verificare a semnăturii electronice.

Articolul 11. Limitele utilizării unor tipuri de semnături electronice

(1) Nu se admite utilizarea semnăturii electronice simple și a semnăturii electronice avansate necalificate pentru:

a) semnarea documentelor electronice ce conțin informație atribuită la secretul de stat;

b) semnarea documentelor electronice în raporturile juridice ale autorităților și instituțiilor publice, inclusiv structurilor subordonate acestora, cu persoanele fizice și juridice de drept privat.

(2) Condițiile și modul de aplicare a semnăturii electronice în documentele electronice ale autorităților și instituțiilor publice, inclusiv structurilor subordonate acestora, se stabilesc de Guvern.

Articolul 12. Registrul împuternicirilor de reprezentare în baza semnăturii electronice

(1) Registrul împuternicirilor de reprezentare în baza semnăturii electronice conține date privind persoanele împuternicite, persoanele reprezentate, rolul și scopul împuternicirii, data acordării împuternicirilor, durata împuternicirilor, alte mențiuni privind acordarea, modificarea sau retragerea împuternicirilor.

(2) Orice modificare în Registrul împuternicirilor de reprezentare în baza semnăturii electronice privind delegarea împuternicirilor poate fi realizată doar de către persoana care acordă împuternicirile respective.

(3) Guvernul stabilește posesorul și deținătorul Registrului împuternicirilor de reprezentare în baza semnăturii electronice, precum și modul de creare și actualizare a acestuia.

Capitolul III

REGIMUL JURIDIC AL DOCUMENTULUI ELECTRONIC ȘI CIRCULAȚIA ELECTRONICĂ A DOCUMENTELOR

Articolul 13. Regimul juridic de utilizare a documentului electronic

(1) Documentul electronic care conține o semnătură electronică avansată calificată este asimilat, după efectele sale, cu documentul analogic pe suport de hârtie, autentificat cu semnătură olografă.

(2) Informația în forma electronică, semnată cu semnătura electronică simplă sau cu semnătura electronică avansată necalificată, este recunoscută în calitate de document electronic asimilat, după efectele sale, cu documentul analogic pe suport de hârtie, autentificat cu semnătură olografă doar în cazurile stabilite expres de actele normative sau de acordul părților privind aplicarea semnăturilor electronice, cu respectarea condițiilor stipulate la alineatul (1) articolul 16 din prezenta lege.

(3) Actele normative sau acordul părților privind aplicarea semnăturilor electronice care stabilesc cazurile de recunoaștere a documentelor electronice, semnate cu semnătura electronică simplă sau cu semnătura electronică avansată necalificată, asimilate, după efectele sale, cu documentul analogic pe suport de hârtie, autentificat cu semnătură olografă, trebuie să prevadă modalitatea de verificare a semnăturii electronice, precum și obligațiile părților privind confidențialitatea și răspunderea materială.

(4) În cazul în care, conform legislației, se cere ca documentul să fie perfectat sau prezentat pe suport de hârtie semnat cu semnătura olografă, documentul electronic se consideră corespunzând acestei cerințe.

(5) În cazul în care, conform legislației, se cere ca documentul pe suport de hârtie să fie autentificat cu ștampilă, documentul electronic se consideră corespunzând acestei cerințe.

(6) Cu o singură semnătură electronică pot fi semnate câteva documente electronice legate între ele (setul de documente electronice). În cazul semnării cu semnătura electronică a setului de documente electronice, fiecare document inclus în acest set se consideră semnat cu semnătura electronică de tipul corespunzător celui cu care este semnat tot setul.

(7) Modul de utilizare a documentelor electronice în cadrul procedurilor judiciare este reglementat de legislația procesuală.

(8) Documentul electronic este echivalat, după valoarea sa probantă, probelor scrise sau mijloacelor materiale de probă. Documentul electronic nu poate fi respins în calitate de probă pentru motivul că are o formă electronică.

(9) În cazul în care legislația prevede înregistrarea de stat a documentului, documentul electronic se supune înregistrării.

(10) Toate exemplarele identice ale documentului electronic sînt considerate originale și produc aceleași efecte juridice.

(11) În cazul în care o persoană creează un document electronic și un document pe suport de hârtie, identice după conținut, ambele se consideră documente de sine stătătoare și originale.

(12) Copie a documentului electronic se consideră reprezentarea (redarea) acestuia pe suport de hârtie, într-o formă perceptibilă. Copia documentului electronic se autentifică în modul prevăzut de legislație pentru autentificarea copiilor documentelor pe suport de hârtie și va conține mențiunea despre faptul că este copie a documentului electronic.

Articolul 14. Domeniile și scopul de utilizare a documentului electronic

(1) Documentul electronic poate fi utilizat de către persoanele fizice și juridice în toate domeniile de activitate în care este posibilă utilizarea dispozitivelor electronice și a mijloacelor tehnice și de program ce permit crearea, prelucrarea, expedierea, recepționarea, păstrarea, modificarea și/sau nimicirea informației în formă electronică.

(2) Documentul electronic poate fi utilizat în scopul expedierii datelor și comunicărilor, ținerii corespondenței, întocmirii actelor juridice, precum și în calitate de document care servește la reflectarea faptelor economice.

Articolul 15. Cerințele față de documentul electronic

Documentul electronic trebuie să corespundă următoarelor cerințe principale:

- a) să fie creat, prelucrat, expediat, recepționat, păstrat, modificat și/sau nimit cu ajutorul mijloacelor tehnice și/sau de program;
- b) să conțină, pentru confirmarea autenticității acestuia, una sau mai multe semnături electronice ce corespund condițiilor și cerințelor stabilite de prezenta lege;
- c) să fie creat și utilizat prin metode și într-o formă ce ar permite identificarea semnatarului documentului electronic;
- d) să fie afișat într-o formă perceptibilă;
- e) să permită utilizare repetată.

Articolul 16. Autenticitatea documentului electronic

(1) Documentul electronic este considerat autentic dacă întrunește următoarele condiții cumulativ:

- a) este semnat de persoana abilitată, în modul stabilit, să semneze cu semnătura olografă documentul echivalent pe suport de hîrtie;
- b) este semnat cu semnătura electronică autentică a semnatarului indicat în document.

(2) Verificarea autenticității documentului electronic se efectuează prin verificarea, cu dispozitive de verificare a semnăturii electronice și/sau produsul asociat semnăturii electronice, a autenticității acestei semnături.

Articolul 17. Organizarea circulației electronice a documentelor

(1) Circulația electronică a documentelor se efectuează conform prevederilor prezentei legi și regulilor stabilite de către proprietarul sistemului respectiv de circulație electronică a documentelor, precum și conform contractelor încheiate între subiecții circulației electronice a documentelor.

(2) Circulația electronică a documentelor poate include următoarele procese:

- a) crearea și prelucrarea documentului electronic;
- b) expedierea și recepționarea documentului electronic;
- c) verificarea autenticității documentului electronic;
- d) confirmarea recepționării documentului electronic;
- e) evidența documentelor electronice;
- f) păstrarea, modificarea și/sau nimitirea documentului electronic;
- g) crearea exemplarelor suplimentare ale documentului electronic,

h) crearea și autentificarea copiilor documentului electronic pe suport de hârtie;

i) aplicarea mărcii temporale.

(3) Modul de creare, prelucrare, expediere, recepționare, păstrare, modificare și/sau nimicire a documentului electronic pentru sistemele de circulație electronică a documentelor unităților de drept public se stabilește de Guvern, iar pentru sistemele de circulație electronică a documentelor unităților de drept privat – de către proprietarii acestora.

Articolul 18. Intermediarul în circulația electronică a documentelor

(1) La organizarea și efectuarea circulației electronice a documentelor pot participa intermediari în condițiile prezentei legi și în conformitate cu regulile stabilite de proprietarul sistemului corespunzător de circulație electronică a documentelor.

(2) Intermediarul în circulația electronică a documentelor este obligat:

a) să dispună de utilaje și mijloace tehnice și/sau de program ce asigură fiabilitatea și securitatea sistemelor informaționale utilizate;

b) să dispună de personal cu competență și/sau experiență în domeniul tehnologiei informației sau securității informaționale;

c) să asigure condițiile în vederea stabilirii exacte a timpului și sursei de expediere a documentului electronic, precum și a timpului recepționării și adresei electronice a destinatarului;

d) să asigure protecția și păstrarea documentelor electronice;

e) să păstreze documentele electronice conform contractului cu utilizatorii sistemului de circulație electronică a documentelor.

Articolul 19. Crearea documentului electronic

(1) Documentul electronic este creat de semnatarul acestuia și conține informație care constituie conținutul acestuia, precum și semnătura electronică a semnatarului.

(2) Crearea documentului electronic se finalizează prin aplicarea semnăturii electronice de către semnatarul documentului electronic, cu aplicarea mărcii temporale după caz.

Articolul 20. Expedierea și recepționarea documentului electronic

(1) Documentul electronic poate fi expedit și recepționat cu ajutorul sistemelor informaționale și de comunicații electronice, și/sau purtătorilor materiali.

(2) Documentul electronic se expediază într-o formă ce permite destinatarului păstrarea și utilizarea acestuia.

(3) În cazul în care semnatarul și destinatarul documentului electronic nu au convenit altfel, documentul electronic se consideră expedit dacă:

a) este expediat de către semnatar ori un intermediar ce acționează în numele semnatarului sau prin sistemul informațional, utilizat de către semnatar;

b) este adresat în mod corespunzător sau în alt mod direcționat în sistemul informațional indicat de destinatar;

c) este redat într-o formă ce permite prelucrarea lui în sistemul informațional indicat de destinatar;

d) intră într-un sistem informațional ce nu este controlat de semnatar sau de intermediarul care expediază documentul electronic în numele semnatarului.

(4) În cazul în care semnatarul și destinatarul documentului electronic nu au convenit altfel, documentul electronic respectiv se consideră recepționat de către destinatar dacă acesta:

a) intră în sistemul informațional din care destinatarul poate să extragă documentele electronice;

b) intră în sistemul informațional indicat de destinatar, într-o formă accesibilă pentru utilizare în sistemul respectiv.

(5) Documentul electronic se consideră neexpediat în cazul în care destinatarul știa sau trebuia să știe că:

a) persoana indicată în document ca semnatar nu este semnatarul adevărat al acestuia;

b) semnatarul nu este inițiatorul expedierii documentului electronic;

c) documentul electronic este recepționat de către destinatar cu modificări sau fără semnătură electronică.

(6) Documentul electronic nu se consideră recepționat dacă persoana care l-a recepționat nu este destinatarul preconizat al acestuia.

Articolul 21. Momentul expedierii și primirii documentului electronic

(1) Dacă semnatarul și destinatarul documentului electronic nu au convenit altfel, moment al expedierii documentului electronic se consideră momentul intrării acestuia în sistemul informațional ce nu este controlat de semnatar sau de intermediarul care expediază documentul electronic în numele semnatarului.

(2) Dacă semnatarul și destinatarul documentului electronic nu au convenit altfel, moment al recepționării documentului electronic se consideră momentul intrării acestuia în sistemul informațional indicat de destinatar. În cazul în care destinatarul documentului electronic nu a indicat sistemul informațional respectiv, documentul electronic se consideră recepționat din momentul intrării acestuia în sistemul informațional al destinatarului, iar în cazul în care destinatarul nu dispune de un asemenea sistem – din momentul extragerii de către destinatar a documentului electronic din sistemul informațional prin care a fost transmis.

(3) Momentul expedierii documentului electronic în sistemele informaționale în caz de necesitate poate fi confirmat prin aplicarea mărcii temporale pe respectivul document electronic.

(4) Dacă semnatarul și destinatarul documentului electronic au convenit asupra confirmării recepționării documentului electronic, moment al recepționării acestuia se consideră momentul expedierii de către destinatar a confirmării privind recepționarea, cu aplicarea mărcii temporale după caz.

Articolul 22. Evidența documentelor electronice

(1) Evidența documentelor electronice ale persoanelor fizice și/sau juridice se efectuează în conformitate cu legislația, prin ținerea registrelor electronice și/sau pe suport de hîrtie.

(2) Ținerea registrelor electronice cuprinde procedurile tehnologice și de program de completare și administrare a acestora, precum și mijloacele de păstrare a documentelor electronice.

Articolul 23. Păstrarea documentelor electronice

(1) Subiecții circulației electronice a documentelor sînt obligați să păstreze originalele documentelor electronice pe suport material, într-o formă ce permite verificarea autenticității acestora.

(2) Termenul de păstrare a documentelor electronice este identic cu termenul prevăzut de legislație pentru documente echivalente pe suport de hîrtie.

(3) Subiecții circulației electronice a documentelor pot asigura păstrarea acestora, utilizînd serviciile intermediarului în circulația electronică a documentelor, cu condiția respectării prevederilor prezentei legi.

(4) Pentru păstrarea de arhivă a documentelor electronice se utilizează arhiva electronică. Guvernul stabilește categoriile de documente electronice pentru păstrarea cărora se utilizează arhiva electronică securizată.

Articolul 24. Protecția documentului electronic

(1) Documentul electronic beneficiază de protecție juridică egală cu cea a documentului pe suport de hîrtie.

(2) Informația ce constituie conținutul documentului electronic este utilizată și protejată, conform legislației, în funcție de statutul și gradul de protecție a acesteia.

(3) Crearea, prelucrarea, expedierea, recepționarea, păstrarea, modificarea și/sau nimicirea documentului electronic trebuie să corespundă cerințelor de securitate stabilite de Guvern pentru sistemele de circulație electronică a documentelor unităților de drept public. Pentru sistemele de circulație electronică a documentelor unităților de drept privat cerințele de securitate sînt stabilite de către proprietarii acestora.

(4) În procesul de creare, prelucrare, expediere, recepționare, păstrare, modificare și/sau nimicire a documentului electronic se impune păstrarea informației ce permite stabilirea originii, apartenenței și destinației documentului electronic, precum și a datei creării, expedierii și recepționării acestuia.

Capitolul IV

SERVICIILE DE CERTIFICARE

Articolul 25. Prestatorul de servicii de certificare

(1) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple și avansate necalificate dispun de dreptul de a trece procedura de acreditare. Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate se supun acreditării obligatorii în conformitate cu prevederile prezentei legi.

(2) Prestatorii de servicii de certificare sînt organizați în mod ierarhic. În fruntea ierarhiei se află prestatorul de servicii de certificare de nivel superior.

(3) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple și avansate necalificate își organizează ierarhia de sine stătător.

(4) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple pot să creeze un singur nivel ierarhic. Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate necalificate creează două niveluri ierarhice, inclusiv și de nivel superior.

(5) Organizarea activității prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, inclusiv ierarhia acestora, se stabilește de Guvern, în limitele prevederilor prezentei legi.

(6) Evidența prestatorilor de servicii de certificare acreditați se efectuează de către organul competent în cadrul registrului de evidență a prestatorilor de servicii de certificare, care se actualizează permanent și accesul la care este public.

(7) Înregistrarea în registrul de evidență a prestatorilor de servicii de certificare acreditați se efectuează la data acreditării acestora de către organul competent.

Articolul 26. Acreditarea prestatorului de servicii de certificare

(1) Acreditarea prestatorului de servicii de certificare se efectuează în baza cererii adresate organului competent. Acreditarea prestatorului de servicii de certificare se efectuează gratis, pentru un termen de 5 ani, dacă un termen mai mic nu este indicat în cererea de acreditare.

(2) Acreditarea în domeniul aplicării semnăturii electronice avansate calificate se acordă prestatorului de servicii de certificare, care întrunește următoarele cerințe:

a) dispunerea de resurse financiare (garanție bancară sau poliță de asigurare) în valoare de cel puțin 300 mii lei pentru recuperarea unor eventuale prejudicii aduse terților din cauza încrederii acestora în datele conținute în certificatul cheii publice, eliberat de către prestatorul de servicii de certificare,

sau în informația din registrul certificatelor eliberate de către prestatorul de servicii de certificare;

b) dispunerea pentru prestarea serviciilor de certificare de personal cu studii superioare în domeniul tehnologiei informației sau securității informaționale, cu competență și/sau experiență la nivel de gestionare, expertiză în domeniul tehnologiei semnăturilor electronice cu nivelul corespunzător de siguranță;

c) asigurarea securității, fiabilității și continuității de prestare a serviciilor de certificare;

d) asigurarea înregistrării informației în registrul certificatelor cheilor publice, în special prestarea operativă a serviciului de suspendare a valabilității și de revocare a certificatelor cheilor publice;

e) asigurarea posibilității de stabilire cu exactitate a datei și a orei eliberării, suspendării valabilității sau revocării certificatului cheii publice;

f) verificarea, în conformitate cu actele legislative, a identității persoanei pentru care se eliberează un certificat calificat al cheii publice;

g) utilizarea sistemelor și produselor care sînt protejate împotriva modificărilor și garantează siguranța tehnică și criptografică a funcțiilor pe care și le asumă;

h) crearea condițiilor de evitare a falsificării certificatelor și, în cazul în care prestatorul de servicii de certificare generează date de creare de semnături, garantarea confidențialității în decursul procesului de creare a respectivelor date;

i) utilizarea sistemelor care nu stochează sau copie datele de creare a semnăturii electronice ale persoanelor pentru care prestatorul de servicii de certificare a prestat servicii de gestionare a cheilor;

k) utilizarea sistemelor fiabile pentru stocarea certificatelor într-o formă care poate fi verificată, astfel încît:

numai persoanele autorizate să poată introduce și modifica date;

autenticitatea informației să poată fi controlată;

certIFICATELE să fie disponibile publicului pentru informare;

toate modificările tehnice care compromit cerințele de siguranță să fie vizibile pentru operator.

(3) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate anexează la cerere documente care confirmă îndeplinirea cerințelor specificate în alineatul (2) al prezentului articol și anume ce atestă:

a) dispunerea de resurse financiare pentru recuperarea unor eventuale prejudicii;

b) dispunerea de o reglementare internă privind asigurarea activității prestatorului de servicii de certificare în conformitate cu cerințele prezentei legi;

c) corespunderea sistemelor și produselor utilizate cerințelor prezentei legi;

d) studiile și calificările persoanelor cu funcții de răspundere, ale căror obligații funcționale țin nemijlocit de prestarea serviciilor de certificare;

e) numirea angajaților responsabili de activitatea prestatorului de servicii de certificare și a persoanelor împuternicite să semneze certificatele cheilor publice, precum și actele de identitate ale acestora;

f) ordinea de sincronizare cu Timpul Mondial Coordonat (UTC);

g) licența eliberată de către Camera de Licențiere (numai pentru prestatorii ce prestează servicii de certificare terțelor persoane) ce atestă dreptul de import, export, proiectarea, producerea și comercializarea mijloacelor criptografice și tehnice de protecție a informației, mijloacelor tehnice speciale pentru obținerea ascunsă a informației; prestarea serviciilor în domeniul protecției criptografice și tehnice a informației (cu excepția activității desfășurate de autoritățile publice investite cu acest drept prin lege).

(4) Documentele menționate în alineatul (3) litera a) se prezintă în original. Documentele menționate în alineatul (3) literele b)-g) se prezintă în original, însoțite de copie, originalul fiind restituit după verificarea copiei la momentul prezentării.

(5) La depunerea cererii de acreditare, prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice simple și semnăturii electronice avansate necalificate este obligat să prezinte informațiile, în formatul stabilit de organul competent, referitoare la procedurile de securitate și de certificare utilizate, precum și datele sale de identificare.

(6) Organul competent, în baza documentelor prezentate și în termen de 30 de zile calendaristice, adoptă decizia privind acreditarea prestatorului de servicii de certificare sau privind refuzul de acreditare.

(7) În cazul adoptării deciziei de acreditare, organul competent, în termen de 10 zile calendaristice din momentul luării deciziei de acreditare, notifică prestatorului de servicii de certificare decizia luată și eliberează acestuia certificatul de acreditare de modelul stabilit și, în conformitate cu actele normative în domeniul semnăturii electronice, înregistrează titularul acreditării în registrul prestatorilor de servicii de certificare.

(8) În cazul refuzului de acreditare, organul competent, în termen de 10 zile calendaristice din momentul luării deciziei de refuz, notifică în scris prestatorului de servicii de certificare decizia luată, cu indicarea cauzelor refuzului.

(9) Temeiul pentru refuzul de acreditare constituie necorespunderea prestatorului de servicii de certificare cerințelor specificate în alineatul (2) al prezentului articol sau prezentarea informației neveridice în documentele ce se anexează la cererea de acreditare.

(10) Refuzul de acreditare nu poate împiedica depunerea repetată a documentelor în vederea acreditării, imediat după înlăturarea cauzelor care au servit temei pentru refuzul de acreditare.

(11) Decizia privind refuzul de acreditare poate fi atacată în instanța de judecată.

(12) Prestatorul de servicii de certificare se consideră acreditat din ziua emiterii certificatului de acreditare.

(13) În caz de deteriorare sau pierdere a certificatului de acreditare, în termen de 5 zile lucrătoare din ziua depunerii cererii corespunzătoare, prestatorul de servicii de certificare i se eliberează un duplicat al certificatului.

(14) Informația despre prestatorii de servicii de certificare, care au fost acreditați, precum și despre cei cu acreditarea retrasă, se publică de către organul competent pe pagina sa oficială în Internet.

(15) După primirea certificatului de acreditare pentru prestarea serviciilor de certificare în domeniul aplicării semnăturii electronice avansate calificate, cheia publică a prestatorului de servicii de certificare este certificată de către prestatorul de servicii de certificare de nivel superior, în conformitate cu regulamentul aprobat de organul competent.

(16) Acreditarea se consideră acordată sau, după caz, prelungită dacă organul competent nu răspunde solicitantului în termenul prevăzut de lege pentru acordarea sau prelungirea acesteia.

(17) După expirarea termenului stabilit de lege pentru acreditare și în lipsa unei notificări scrise din partea organului competent, acreditarea se consideră prelungită pentru un termen de 5 ani.

(18) Prestatorii de servicii de certificare acreditați în domeniul aplicării semnăturii electronice simple și semnăturii electronice avansate necalificate sînt obligați să comunice organului competent, cu cel puțin 10 zile înainte, orice intenție de modificare a procedurilor de securitate și de certificare, cu precizarea datei și orei la care modificarea intră în vigoare, precum și să confirme în termen de 24 de ore modificarea efectuată.

(19) În cazurile de urgență în care securitatea serviciilor de certificare este afectată, prestatorii de servicii de certificare acreditați în domeniul aplicării semnăturii electronice simple și semnăturii electronice avansate necalificate pot efectua modificări ale procedurilor de securitate și de certificare, urmînd să comunice, în termen de 24 de ore, organului competent modificările efectuate și justificarea deciziei luate.

(20) Prestatorul de servicii de certificare acreditat este obligat să asigure respectarea cerințelor, în conformitate cu care acesta a fost acreditat, pe parcursul întregului termen de acreditare. În cazul apariției circumstanțelor care fac imposibilă asigurarea acestora, prestatorul de servicii de certificare urmează să notifice organul competent despre acest fapt, în termen de 24 de ore.

(21) Prestatorul de servicii de certificare de nivel superior în domeniul aplicării semnăturii electronice avansate calificate nu este supus acreditării în conformitate cu prezenta lege.

Articolul 27. Activitatea prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare:

- a) creează și eliberează certificatele cheilor publice;
- b) suspendă și revocă certificatele cheilor publice, restabilește valabilitatea certificatelor suspendate;
- c) ține registrul certificatelor cheilor publice, asigură actualizarea acestuia și accesul liber la registru; și (sau)
- d) prestează, în bază de contract, alte tipuri de servicii ce țin de semnătura electronică.

(2) Activitatea prestatorului de servicii de certificare reprezintă o activitate în domeniul protecției criptografice și tehnice a informației și este supusă licențierii de către Camera de Licențiere, în conformitate cu Legea nr.451-XV din 30 iulie 2001 privind reglementarea prin licențiere a activității de întreprinzător.

Articolul 28. Obligațiile prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare este obligat:

- a) să verifice autenticitatea datelor indicate în cererea de certificare a cheii publice în baza documentelor ce confirmă datele în cauză;
- b) să asigure corespunderea informațiilor din certificatul cheii publice cu informațiile prezentate de către titularul certificatului cheii publice;
- c) să introducă certificatul cheii publice în registrul certificatelor cheilor publice nu mai târziu de data și ora când începe să curgă termenul de valabilitate a certificatului;
- d) să asigure accesul la registrul certificatelor cheilor publice, cu respectarea prevederilor articolului 43 al prezentei legi;
- e) să suspende valabilitatea sau să revoce certificatul cheii publice în cazurile prevăzute de lege și să facă mențiunea respectivă în registrul certificatelor cheilor publice, în termenele stabilite;
- f) să acopere prejudiciile aduse oricărei entități sau persoane fizice, care are încredere în mod rezonabil în datele conținute în certificatul cheii publice eliberat de către prestatorul de servicii de certificare, prin faptul că a omis să înregistreze revocarea certificatului;
- g) să înștiințeze titularul certificatului cheii publice despre faptele care au devenit cunoscute prestatorului de servicii de certificare și care fac imposibilă utilizarea în continuare a cheii private, precum și despre revocarea certificatului cheii publice;
- h) să prezinte informațiile necesare pentru autentificarea semnăturii electronice;
- i) să solicite eliberarea duplicatului certificatului de acreditare, în cazul pierderii sau deteriorării acestuia;
- k) să îndeplinească alte obligații stabilite de prezenta lege.

(2) Prestatorul de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate suplimentar este obligat:

a) să certifice, în modul stabilit de legislație, cheia publică a prestatorului de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate, destinată certificării cheilor publice;

b) să înregistreze, pe o perioadă corespunzătoare de timp, în conformitate cu articolul 32 din prezenta lege, toate informațiile pertinente referitoare la un certificat calificat al cheii publice, în special pentru a putea furniza dovezi de certificare în justiție. Înregistrările pot fi efectuate prin mijloace electronice;

c) înainte să stabilească o relație contractuală cu o persoană care solicită un certificat în sprijinul semnăturii sale electronice, să informeze respectiva persoană, prin mijloace de comunicare fiabile, cu privire la termenele și condițiile exacte de utilizare a certificatului, inclusiv cu privire la limitele impuse utilizării sale, la existența unui sistem de acreditare și la procedurile de contestare și soluționare a litigiilor. Aceste informații, care pot fi transmise pe cale electronică, trebuie comunicate în scris și într-un limbaj accesibil. Elementele pertinente ale informațiilor trebuie puse, de asemenea, la cerere, la dispoziția părților terțe care beneficiază de certificat;

d) să păstreze toată informația cu privire la certificatul cheii publice atașat semnăturilor electronice avansate calificate cel puțin 15 ani din momentul revocării sau expirării certificatului, în eventualitatea apariției unor litigii.

Articolul 29. Cererea de certificare a cheii publice

(1) Cererea de certificare a cheii publice se depune în formă electronică semnată cu semnătură electronică și/sau în formă de document pe suport de hârtie, semnat cu semnătura olografă a solicitantului.

(2) Cererea de certificare a cheii publice va conține:

a) numele și prenumele solicitantului și numărul actului de identitate;

b) alte date de identificare ale solicitantului, în funcție de scopul pentru care se eliberează certificatul cheii publice, precum și informațiile necesare pentru comunicarea cu acesta.

Articolul 30. Examinarea cererii de certificare a cheii publice

(1) Cererea de certificare a cheii publice este examinată de către prestatorul de servicii de certificare în termen de 3 zile lucrătoare de la data înregistrării cererii dacă părțile nu stabilesc altfel.

(2) În baza deciziei de certificare a cheii publice, prestatorul de servicii de certificare creează și eliberează certificatul respectiv al cheii publice. Modelul certificatului calificat al cheii publice este stabilit de organul competent.

(3) Decizia de refuz al certificării cheii publice se adoptă de prestatorul de servicii de certificare în următoarele cazuri:

a) încălcare a prevederilor prezentei legi;

b) încălcare a drepturilor unor terți în procesul de întocmire sau de depunere a cererii;

c) prezentare în cerere a unor informații ce nu corespund realității.

(4) Decizia de refuz a certificării cheii publice poate fi atacată în instanța de judecată competentă, în modul stabilit.

(5) Decizia de refuz a certificării cheii publice nu-l privează pe solicitant de dreptul de a depune o nouă cerere după înlăturarea tuturor încălcărilor admise.

Articolul 31. Certificatul cheii publice

(1) La crearea certificatului cheii publice, prestatorul de servicii de certificare este obligat să verifice unicitatea cheii publice.

(2) Certificatul cheii publice trebuie să conțină următoarele informații:

a) numărul unic de înregistrare a certificatului cheii publice;

b) datele de identificare ale prestatorului de servicii de certificare care a eliberat certificatul cheii publice;

c) date de identificare și alte date ale titularului certificatului cheii publice, în funcție de scopul pentru care se eliberează certificatul, precum și informațiile necesare pentru comunicarea cu acesta;

d) cheia publică;

e) data și ora la care începe și încetează termenul de valabilitate a certificatului cheii publice;

f) date despre algoritmul criptografic al semnăturii electronice;

g) după caz, restricțiile la utilizarea certificatului cheii publice sau limitele valorii operațiunilor în care acesta poate fi utilizat;

h) alte informații stabilite de prezenta lege.

(3) Certificatul calificat al cheii publice se emite de către prestatorul de servicii de certificare acreditat și suplimentar trebuie să conțină următoarele informații:

a) mențiunea care să indice că certificatul este eliberat ca certificat calificat al cheii publice;

b) posibilitatea includerii, atunci când este cazul, a unei calități speciale a semnatarului, în funcție de utilizarea pe care urmează să o aibă certificatul;

c) datele de verificare a semnăturii care corespund datelor de creare a semnăturii sub controlul semnatarului.

(4) În calitate de date de identificare ale titularului, în certificatul cheii publice servesc numele, prenumele și numărul de identificare a persoanei fizice (IDNP) și/sau pseudonimul, în caz de utilizare, iar în certificatul cheii publice al prestatorului de servicii de certificare – denumirea prestatorului și numărul de identificare a persoanei juridice (IDNO).

(5) În cazul semnăturii electronice simple și a semnăturii electronice avansate necalificate, structura certificatului cheii publice se stabilește de către prestatorul de servicii de certificare, în conformitate cu cerințele stabilite de prezenta lege. În cazul semnăturii electronice avansate calificate, structura

certificatului cheii publice se stabilește de către organul competent, în conformitate cu cerințele stabilite de prezenta lege.

(6) Certificatul cheii publice se semnează cu semnătura electronică a prestatorului de servicii de certificare, iar certificatul calificat al cheii publice – cu semnătură electronică avansată calificată a prestatorului de servicii de certificare.

(7) În cazurile stabilite de legislație sau prin acordul părților, prestatorul de servicii de certificare creează certificatul cheii publice și în formă de document pe suport de hârtie, în două exemplare. În acest caz, certificatul cheii publice sub formă de document pe suport de hârtie este semnat cu semnăturile olografe ale titularului certificatului cheii publice și ale persoanei împuternicite a prestatorului de servicii de certificare și se autentifică cu ștampila prestatorului de servicii de certificare. Un exemplar al certificatului cheii publice se transmite titularului, iar celălalt se păstrează la prestatorul de servicii de certificare.

(8) Prestatorul de servicii de certificare, de comun acord cu titularul certificatului cheii publice, poate indica în certificatul cheii publice unele restricții cu privire la utilizarea acestuia, precum și cazurile în care certificatul respectiv va putea fi utilizat.

(9) La cererea titularului certificatului cheii publice, prestatorul de servicii de certificare poate indica în certificatul cheii publice și alte informații decât cele specificate în alineatele (2) și (3), cu condiția ca acestea să nu contravină legislației și să nu pună în pericol securitatea națională sau ordinea publică, și numai după o prealabilă verificare a exactității informațiilor în cauză.

(10) Prestatorul de servicii de certificare introduce certificatul în registrul certificatelor cheilor publice nu mai târziu de data și ora la care începe termenul de valabilitate a certificatului.

Articolul 32. Termenul de valabilitate și termenul de păstrare a certificatului cheii publice

(1) Termenul de valabilitate a certificatului cheii publice a prestatorului de servicii de certificare de nivel superior constituie 20 de ani, termenul de valabilitate a certificatului cheii publice a prestatorului de servicii de certificare de nivelul II constituie 10 ani, termenul de valabilitate a certificatului cheii publice a utilizatorului se stabilește de către prestatorul de servicii de certificare, dar nu poate constitui mai mult de 1 an.

(2) Prestatorul de servicii de certificare este obligat să păstreze certificatul cheii publice cel puțin 15 ani de la data revocării sau expirării certificatului.

Articolul 33. Suspendarea și revocarea certificatului cheii publice

(1) Prestatorul de servicii de certificare suspendă certificatul cheii publice la cererea titularului certificatului cheii publice.

(2) Prestatorul de servicii de certificare revocă certificatul cheii publice:

a) la cererea titularului certificatului cheii publice;

b) la depistarea unor informații neveridice în cererea de certificare a cheii publice sau în certificatul cheii publice;

c) la încălcarea confidențialității cheii private (compromiterea cheii private);

d) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice și în lipsa unei cereri din partea titularului certificatului cheii publice de restabilire a valabilității acestuia;

e) la modificarea certificatului cheii publice;

f) la decesul titularului certificatului cheii publice sau la recunoașterea lui ca fiind incapabil;

g) la solicitarea organului competent, în cazul încălcării prezentei legi.

(3) În cazul primirii informațiilor ce impun revocarea certificatului cheii publice, prestatorul de servicii de certificare este obligat, în termen de 3 ore de lucru, să facă înscrierile respective în registrul certificatelor cheilor publice.

(4) Prestatorul de servicii de certificare este obligat să înștiințeze titularul certificatului cheii publice despre motivele revocării certificatului acestuia.

Articolul 34. Obligațiile titularului certificatului cheii publice

Titularul certificatului cheii publice este obligat:

a) să asigure condițiile necesare pentru excluderea accesului unei alte persoane la cheia sa privată;

b) să nu utilizeze cheia privată pentru crearea semnăturii electronice dacă are motive să presupună că este încălcată confidențialitatea cheii private;

c) să solicite imediat suspendarea valabilității certificatului cheii publice sau revocarea acestuia în cazul în care:

a) pierdut cheia privată;

are motive să creadă că a fost încălcată confidențialitatea cheii private;

informațiile cuprinse în certificatul cheii publice nu corespund realității;

d) să înștiințeze, în timp de 24 de ore, prestatorul de servicii de certificare despre orice modificare a informațiilor cuprinse în certificatul cheii publice;

e) să îndeplinească alte obligații stabilite de prezenta lege și de acordul încheiat cu prestatorul de servicii de certificare.

Articolul 35. Registrul certificatelor cheilor publice

(1) Prestatorul de servicii de certificare este obligat să țină registrul certificatelor cheilor publice.

(2) Registrul certificatelor cheilor publice va conține:

a) certificatele valabile ale cheilor publice;

b) certificatele revocate și suspendate ale cheilor publice;

c) data și ora eliberării certificatelor cheilor publice;

d) data și ora revocării certificatelor cheilor publice;

e) altă informație în conformitate cu actele normative în domeniul semnăturii electronice.

(3) În vederea verificării autenticității semnăturii electronice, prestatorul de servicii de certificare este obligat să asigure accesul la registrul certificatelor cheilor publice, inclusiv în regimul timpului real.

Capitolul V

MONITORIZARE ȘI CONTROL

Articolul 36. Atribuțiile autorităților publice în domeniul aplicării semnăturii electronice

(1) Organul competent de elaborarea și promovarea politicii de stat și cu exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice este Serviciul de Informații și Securitate, care exercită următoarele atribuții:

a) efectuează acreditarea, inclusiv voluntară, a prestatorilor de servicii de certificare;

b) exercită funcția prestatorului de servicii de certificare de nivel superior pentru prestatorii de servicii de certificare acreditați în domeniul aplicării semnăturii electronice avansate calificate;

c) asigură ținerea, actualizarea și accesul liber la datele registrului de evidență a prestatorilor de servicii de certificare acreditați;

d) elaborează și aprobă, prin acte normative, cerințele în domeniul aplicării tuturor tipurilor de semnături electronice;

e) monitorizează și controlează asigurarea cerințelor la prestarea serviciilor de certificare în domeniul aplicării tuturor tipurilor de semnături electronice;

f) participă la elaborarea și aprobarea reglementărilor tehnice și a standardelor în domeniul semnăturii electronice;

g) acordă, la solicitare, asistență metodică și practică autorităților publice la aplicarea mecanismelor semnăturii electronice;

h) realizează colaborarea internațională în domeniul semnăturii electronice.

(2) Guvernul stabilește autoritatea sau instituția publică responsabilă pentru prestarea serviciului de sursă unică de sincronizare cu Timpul Mondial Coordonat (UTC).

Articolul 37. Controlul în domeniul aplicării semnăturii electronice

(1) Organul competent controlează respectarea obligațiilor prevăzute de prezenta lege la prestarea serviciilor de certificare de către prestatorii acreditați și la acordarea sau prelungirea acreditării.

(2) Controlul se efectuează de către Comisia de control în domeniul semnăturii electronice (în continuare – Comisia) în baza Regulamentului aprobat de organul competent.

(3) Comisia se creează în cadrul organului competent în baza ordinului privind efectuarea controlului, emis de conducătorul acestui organ.

(4) Componenta nominală a Comisiei se stabilește pentru fiecare caz în parte.

(5) Comisia are dreptul:

a) la acces liber la materialele documentare, necesare pentru desfășurarea lucrărilor, pe suport de hârtie și în mod electronic, ce țin de prestarea serviciilor de certificare, precum și la sistemele de distribuție de aplicații soft, aplicațiile soft și mijloacele tehnice instalate;

b) să obțină informații complete despre condițiile și modul de exploatare a mijloacelor tehnice și de program;

c) să obțină informații de la persoanele responsabile și personalul prestatorului de servicii de certificare în privința presării serviciilor de certificare și care țin de obiectul controlului;

d) la acces, în decursul zilei lucrătoare (în termenul efectuării controlului), în încăperile prestatorului de servicii de certificare.

(6) Comisia nu are dreptul să efectueze controlul fără prezentarea ordinului privind efectuarea controlului și fără documentele de identitate ale membrilor.

(7) La efectuarea controlului privind respectarea condițiilor prevăzute de prezenta lege, Comisia va ține cont de următoarele principii:

a) legalitatea și respectarea competenței stabilite de lege;

b) neadmiterea aplicării sancțiunilor care nu sînt stabilite de lege;

c) tratarea dubiilor, apărute la aplicarea legislației, în favoarea prestatorului de servicii de certificare;

d) efectuarea cheltuielilor de control din contul statului;

e) prescrierea recomandărilor pentru înlăturarea încălcărilor constatate în urma controlului;

f) dreptul prestatorului de servicii de certificare de a ataca acțiunile organului competent, inclusiv în instanța judecătorească.

(8) Controalele planificate asupra respectării de către prestatorul de servicii de certificare a obligațiilor prevăzute de prezenta lege se efectuează de către organul competent cel mult o dată în decursul anului calendaristic, cu cooptarea, după caz, a reprezentanților instituțiilor cu funcții de reglementare și de control, conform competenței.

(9) Planurile controalelor, elaborate de organul competent și aprobate în modul stabilit, se coordonează, în privința termenelor de efectuare, cu conducerea prestatorului de servicii de certificare, cel puțin cu 5 de zile lucrătoare pînă la începerea acestor controale.

(10) Controalele inopinate se efectuează la decizia organului competent, numai în temeiul:

a) depistării și confirmării, de organul competent, a faptelor de încălcare a prezentei legi; și (sau)

b) recepționării cererilor și reclamațiilor scrise argumentate în adresa organului competent referitor la încălcările și la îndeplinirea necorespunzătoare a obligațiilor stabilite de prezenta lege de către prestatorul de servicii de certificare.

(11) Prestatorul de servicii de certificare se informează despre efectuarea controlului inopinat în ziua demarării.

(12) Controalele repetate se efectuează numai în scopul verificării executării prescripției privind lichidarea încălcărilor prezentei legi, indicate în actul de control precedent (planificat sau inopinat). Controlul repetat se consideră parte componentă a controlului precedent.

(13) Controlul se efectuează strict în termenul stabilit în ordinul privind efectuarea controlului.

(14) Termenul de efectuare a controlului planificat și a controlului inopinat nu poate depăși 10 zile lucrătoare, iar a celui repetat – nu mai mult de 5 zile lucrătoare. În cazul controalelor inopinate, termenul de 10 zile poate fi prelungit cu încă 10 zile de către conducătorul organului competent în baza unei decizii motivate, aduse la cunoștința prestatorului de servicii de certificare supus controlului, care poate fi contestată de către prestatorul de servicii de certificare.

(15) La efectuarea controlului asupra respectării obligațiilor prevăzute de prezenta lege, prestatorul de servicii de certificare prezintă informația și documentele relevante scopului controlului și nu împiedică efectuarea acestuia.

(16) În baza rezultatelor controlului, se întocmește un act în 2 exemplare, unul dintre care se expediază (înmînează), în termen de cel mult 5 zile lucrătoare după încheierea controlului efectuat, prestatorului de servicii de certificare, iar al doilea se păstrează la organul competent. În caz de dezacord cu rezultatele controlului efectuat, prestatorul de servicii de certificare, în termen de 10 zile lucrătoare de la data primirii actului de control, poate prezenta în scris argumentarea dezacordului, anexînd documentele de rigoare.

(17) În cazul în care se depistează încălcări ale respectării obligațiilor prevăzute de prezenta lege, organul competent, la întocmirea actului de control, emite prescripția privind lichidarea încălcărilor, cuprinzînd recomandările privind modul de remediere a tuturor deficiențelor identificate, precum și avertizarea despre posibila suspendare sau retragere a acreditării, dacă încălcările depistate nu vor fi lichidate în termenul stabilit.

(18) Termenul minim stabilit de organul de control pentru lichidarea încălcărilor depistate constituie 10 zile lucrătoare, iar cel maxim – 30 zile lucrătoare după primirea prescripției expediate (înmînate) împreună cu actul de control.

(19) În cazuri excepționale și la solicitarea oficială a prestatorului de servicii de certificare, termenul pentru lichidarea încălcărilor poate fi prelungit cu cel mult 20 de zile lucrătoare.

(20) Prestatorul de servicii de certificare acreditat, primind prescripția privind lichidarea încălcărilor obligațiilor prevăzute de prezenta lege, este

obligat, în termenul indicat în prescripție, să comunice organului competent informația privind lichidarea încălcărilor.

(21) În cazul constatării semnelor de compromitere a cheilor private ale prestatorului de servicii de certificare acreditat, încălcării obligațiilor prevăzute de prezenta lege, neînlăturării, în termenul stabilit, a datelor eronate în certificatele cheilor publice, organul competent poate aplica măsuri de suspendare sau retragere a acreditării prestatorului de servicii de certificare în conformitate cu prezenta lege.

(22) Informațiile despre rezultatele efectuării controlului se publică de către organul competent pe pagina sa oficială în rețeaua Internet.

(23) Prestatorul de servicii de certificare are dreptul să depună la organul competent reclamații în scris despre încălcarea prezentei legi, admise de Comisie, sau să conteste acțiunile acesteia în instanța judecătorească.

Articolul 38. Suspendarea și reluarea valabilității acreditării

(1) Acreditarea poate fi suspendată în conformitate cu prevederile Legii nr.235-XVI din 20 iulie 2006 cu privire la principiile de bază de reglementare a activității de întreprinzător.

(2) Temei pentru realizarea acțiunilor prevăzute de lege pentru suspendarea acreditării servesc:

a) cererea prestatorului de servicii de certificare privind suspendarea acesteia;

b) încălcarea de către prestatorul de servicii de certificare a obligațiilor stabilite de prezenta lege;

c) nevalabilitatea garanției bancare sau a poliței de asigurare pentru prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, prevăzute de articolul 26 alineatul (2) litera a) din prezenta lege;

d) nerespectarea de către prestatorul de servicii de certificare a prescripției privind lichidarea încălcării obligațiilor stabilite de prezenta lege, depistate în cadrul controlului efectuat de organul competent.

(3) Decizia privind suspendarea acreditării se aduce la cunoștință prestatorului de servicii de certificare în termen de 3 zile lucrătoare de la data emiterii acesteia. Termenul de suspendare a acreditării nu poate depăși 2 luni, dacă actele normative în domeniul semnăturii electronice nu prevăd altfel.

(4) Prestatorul de servicii de certificare este obligat să înștiințeze în scris organul competent despre înlăturarea circumstanțelor care au condus la suspendarea acreditării.

(5) Decizia privind reluarea valabilității acreditării se adoptă de către organul competent în temeiul hotărârii instanței de judecată care a emis hotărârea de suspendare a acesteia, în termen de 3 zile lucrătoare de la data primirii înștiințării. Decizia se aduce la cunoștință prestatorului de servicii de certificare în termen de 3 zile lucrătoare de la data adoptării acesteia.

(6) Termenul de valabilitate a acreditării nu se prelungește pe perioada de suspendare a acesteia.

Articolul 39. Retragera acreditării

(1) Acreditarea poate fi retrasă în conformitate cu prevederile Legii nr.235-XVI din 20 iulie 2006 cu privire la principiile de bază de reglementare a activității de întreprinzător.

(2) Temei pentru realizarea acțiunilor prevăzute de lege în vederea retragerii acreditării servesc:

a) cererea prestatorului de servicii de certificare privind încetarea activității, depusă cu 30 de zile calendaristice înainte de încetarea planificată;

b) decizia cu privire la anularea înregistrării de stat a persoanei juridice în cadrul căreia activează prestatorul de servicii de certificare;

c) depistarea unor date neautentice în documentele prezentate organului competent;

d) stabilirea faptului de transmitere a certificatului de acreditare sau a copiei de pe acesta altei persoane, în scopul desfășurării genului de activitate acreditată;

e) neînălăturarea, în termenul stabilit, a circumstanțelor care au condus la suspendarea acreditării;

f) nerespectarea a doua oară a prescripțiilor privind lichidarea încălcărilor ce țin de obligațiile stabilite de prezenta lege.

(3) Mențiunea referitoare la data și numărul deciziei privind retragerea acreditării se înscrie în registrul de evidență a prestatorilor de servicii de certificare, nu mai târziu de ziua lucrătoare imediat următoare adoptării deciziei.

(4) Toate certificatele cheilor publice emise de către prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate care și-a încetat activitatea se revocă și se transmit spre păstrare altui prestator de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, în modul stabilit de organul competent, din contul prestatorului de servicii de certificare care își încetează activitatea.

(5) Prestatorul de servicii de certificare este obligat, în decurs de 10 zile lucrătoare de la data adoptării deciziei de retragere a acreditării, să depună la organul competent certificatul de acreditare retras.

Capitolul VI RĂSPUNDEREA

Articolul 40. Răspunderea persoanelor fizice și juridice care cad sub incidența prezentei legi

(1) Persoanele fizice și juridice poartă răspundere, stabilită de actele legislative, pentru neîndeplinirea cerințelor din prezenta lege.

(2) Intermediarul, în circulația electronică a documentelor, poartă răspundere, stabilită de actele legislative, pentru neexecutarea sau executarea necorespunzătoare a obligațiilor și pentru calitatea necorespunzătoare a serviciilor prestate, precum și pentru prejudiciul cauzat de aceste acțiuni (inacțiuni).

(3) Pentru acces ilegal la informația cuprinsă în documentele electronice, persoanele poartă răspundere civilă, contravențională sau penală, după caz, conform actelor legislative.

(4) Litigiile care apar în cadrul circulației electronice a documentelor, precum și cele legate de utilizarea documentelor electronice și de aplicarea semnăturii electronice, se soluționează de către subiecții circulației electronice a documentelor, în conformitate cu actele legislative și contractele încheiate.

Articolul 41. Răspunderea prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare poartă răspundere civilă, contravențională sau penală, după caz, conform actelor legislative în vigoare.

(2) Prestatorul de servicii de certificare poartă răspundere civilă pentru prejudiciul cauzat urmare a neîndeplinirii obligațiilor prevăzute de prezenta lege, cu excepția cazurilor în care prestatorul de servicii de certificare aduce probe pertinente că nu a putut împiedica cauzarea prejudiciului.

(3) Prestatorul de servicii de certificare nu poartă răspundere civilă pentru prejudiciul cauzat urmare a utilizării certificatului cheii publice cu încălcarea restricțiilor de utilizare a acestuia sau a restricțiilor privind limitele valorii operațiunilor în care acesta poate fi utilizat.

Articolul 42. Răspunderea titularului certificatului cheii publice

(1) Titularul certificatului cheii publice poartă răspundere civilă, contravențională sau penală, după caz, conform actelor legislative în vigoare.

(2) Titularul certificatului cheii publice poartă răspundere civilă pentru prejudiciul cauzat de:

a) neîndeplinirea sau îndeplinirea defectuoasă a obligațiilor stabilite de prezenta lege;

b) semnarea documentelor electronice cu utilizarea cheii private, inclusiv în perioada de la solicitarea suspendării valabilității sau revocării certificatului cheii publice până la înscrierea, în termenul stabilit, a mențiunii respective în registrul certificatelor cheilor publice, cu excepția cazurilor în care titularul certificatului va aduce probe pertinente că documentul electronic a fost semnat de o altă persoană.

Capitolul VII

PROTECȚIA DATELOR CU CARACTER PERSONAL

Articolul 43. Protecția datelor cu caracter personal

(1) Prestatorii de servicii de certificare și autoritatea responsabilă de supraveghere vor asigura ca prevederile Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal să fie respectate în procesul de prestare a serviciilor de certificare.

(2) Datele cu caracter personal se colectează de către prestatorul de servicii de certificare, exclusiv cu acordul prealabil al persoanei care solicită certificatul, și numai atunci când acestea sînt necesare pentru eliberarea și menținerea certificatului. Datele personale nu pot fi colectate sau prelucrate în alte scopuri fără consimțămîntul prealabil și expres al persoanei interesate.

Capitolul VIII

DISPOZIȚII FINALE

Articolul 44. Dispoziții finale

(1) Prezenta lege intră în vigoare la 6 luni de la data publicării.

(2) La data intrării în vigoare a prezentei legi se abrogă Legea nr.264-XV din 15 iulie 2004 cu privire la documentul electronic și semnătura digitală (Monitorul Oficial al Republicii Moldova, 2004, nr. 132-137, art. 710).

(3) Guvernul, în termen de 12 luni de la data publicării prezentei legi:

a) va prezenta propuneri privind aducerea legislației în concordanță cu prezenta lege;

b) va aduce actele sale normative în concordanță cu prezenta lege;

c) va elabora și va adopta actele normative necesare executării legii.

(4) Prevederile articolului 5 alineatul (1) în partea ce ține de procedurile judiciare intră în vigoare începînd cu 1 ianuarie 2016.

Președintele Parlamentului

Nota informativă la proiectul legii privind semnătura electronică și documentul electronic

Prezenta notă informativă descrie cadrul în care a fost elaborat proiectul de lege privind semnătura electronică și documentul electronic (în continuare proiect de lege) și oportunitatea proiectului de lege.

Proiectul de lege creează cadrul necesar pentru transpunerea în legislația națională a prevederilor Directivei nr. 1999/93/CE a Parlamentului European și a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice, publicat în Jurnalul Oficial al Comunităților Europene nr. L 13 din 19 ianuarie 2000.

Scopul proiectului de lege este stabilirea regimului juridic al semnăturii electronice și al documentului electronic, inclusiv cerințelor principale față de valabilitatea acestora și cerințelor principale față de serviciile de certificare. Totodată, proiectul de lege urmărește crearea condițiilor juridice pentru utilizarea eficientă, sigură și fără costuri nejustificate a formelor alternative de autentificare a semnăturii olografe.

Intervenția prin intermediul proiectului de lege este dictată de ineficiența cadrului juridic actual instituit pentru semnătura digitală – cea mai complexă formă a semnăturii electronice. Pentru a simplifica procedurile de certificare, eliberare și utilizare a semnăturii electronice se stabilesc mai multe tipuri de semnături electronice cu valoare juridică și gradul de protecție diferit și caracterul oportun pentru diverse acte juridice.

Prin intermediul proiectului de lege se instituie tipurile de semnături electronice, principiile de utilizare a acestora, efectele juridice ale utilizării semnăturii electronice, precum și cerințele care se vor impune față de prestatorii de servicii de certificare. Proiectul de lege nu schimbă cadrul juridic deja existent privind cerințele de valabilitate ale actelor juridice civile, ci asigură cadrul juridic pentru utilizarea autentificării alternative semnăturii olografe, care ține de cerința de formă pentru valabilitatea actelor juridice civile.

În contextul utilizării transnaționale a semnăturilor electronice proiectul de lege stabilește condițiile în care un certificat al cheii publice eliberat de către un prestator de servicii de certificare cu domiciliul sau cu sediul într-un alt stat este recunoscut ca fiind echivalent din punct de vedere al efectelor juridice cu certificat al cheii publice eliberat de un prestator de servicii de certificare cu domiciliul sau cu sediul în Republica Moldova, inclusiv prin acorduri bilaterale și multilaterale pentru recunoașterea semnăturilor electronice naționale în alte state și recunoașterea semnăturilor electronice străine în Republica Moldova.

La capitolul definiții, pentru a se asigura corespunderea proiectului de lege cu prevederile Directivei nr. 1999/93/CE se oferă definiții ale semnăturii electronice simple, semnăturii electronice avansate necalificate și semnăturii electronice avansate calificate. În textul proiectului de lege au fost importate definițiile oferite de Directivă ce

țin de dispozitive de creare a semnăturii, dispozitive securizate de creare a semnăturilor, certificate calificate, prestator de servicii de certificare etc.

Pentru a se asigura o protecție suficientă a actelor care sunt semnate cu semnătură electronică, se stabilește regula generală conform căreia semnătura electronică avansată calificată se echivalează după valoare juridică cu semnătura olografă. Totodată, Guvernul este investit cu competențe de stabilire a modului de aplicare a semnăturilor electronice de către funcționarii autorităților publice. În același timp, subiecții de drept privat pot stabili condiții mai stricte față de semnăturile electronice aplicate pe documente electronice pentru autentificare.

Domeniile de aplicare a semnăturii electronice pentru recunoașterea lor în procedurile judiciare au fost lăsate la latitudinea reglementărilor speciale - legislația procesual civilă. Urmare adoptării acestui proiect de lege vor fi necesare modificări și completări ale domeniului de aplicare a semnăturii electronice în acest sector special. Se propune intrarea în vigoare a prevederilor ce țin de recunoașterea semnăturii electronice pentru procedurile judiciare la începutul anului 2016.

Condițiile pentru serviciile de certificare, certificatele calificate și dispozitivele securizate de creare a semnăturilor au fost preluate în totalitate din Directiva nr. 1999/93/CE.

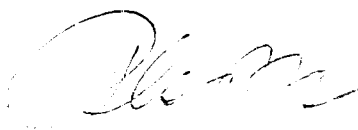
Proiectul de lege instituie procedura de acreditare obligatorie a prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, iar prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice simple și avansate necalificate nu vor fi supuse acreditării obligatorii, dar vor putea trece procedura de acreditare la propria inițiativă.

Termenul de valabilitate a certificatului cheii publice a utilizatorului se stabilește de către prestatorul de servicii de certificare, dar nu poate constitui mai mult de 1 an. De asemenea, s-a impus obligația față de prestatorii de servicii de certificare să păstreze cel puțin 15 ani informația despre semnătura electronică pentru a permite organelor de urmărire penală să dispună de probele necesare – în conformitate cu prevederile Codului Penal, termenul de prescripție pentru infracțiunile grave constituie 15 ani.

Proiectul de lege stabilește competențele Serviciului de Informații și Securitate privind elaborarea și promovarea politicii de stat și exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice.

Implementarea legii nu necesită cheltuieli financiare suplimentare din bugetul de stat și se va efectua în limita alocațiilor curente pentru organele competente.

Ministru



Pavel FILIP