Proiect

PARLAMENTUL REPUBLICII MOLDOVA

LEGE
privind semnătura electronică şi documentul electronic

Parlamentul adoptă prezenta lege organică.

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

Capitolul I
DISPOZIŢII GENERALE

Articolul 1. Scopul legii şi domeniul de aplicare

(1) Prezenta lege stabileşte regimul juridic al semnăturii electronice şi al documentului electronic, inclusiv cerinţele principale faţă de valabilitatea acestora şi cerinţele principale faţă de serviciile de certificare.

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

(3) Recunoaşterea semnăturii electronice şi a documentului electronic în afara Republicii Moldova se stabileşte prin tratate internaţionale la care Republica Moldova este parte. În cazul în care tratatele internaţionale la care Republica Moldova este parte stabilesc alte norme decît cele stabilite de prezenta lege, se aplică normele tratatelor internaţionale.

Articolul 2. Noţiuni principale

În sensul prezentei legi, se definesc următoarele noţiuni:

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

b) **adresant al documentului electronic** - persoana fizică, persoana juridică sau statul căruia îi este adresat documentul electronic;

c) **autenticitate a documentului electronic** - calitate a documentului electronic care constă în faptul că acesta este semnat de persoana abilitată cu o semnătură electronică autentică;

d) **arhiva electronică securizată** – depozit structurat de documente electronice, care asigură confidenţialitatea, non-repudierea şi integritatea acestora, şi care garantează valoarea probantă a acestora în timp;

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

f) **certificat calificat al cheii publice** – certificat al cheii publice care întruneşte cerinţele prevăzute de articolul 32 din prezenta lege şi este eliberat de un prestator de servicii de certificare, care întruneşte cerinţele prevăzute de articolul 27 din prezenta lege;

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

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

i) **circulaţie electronică a documentelor** - totalitatea proceselor de creare, prelucrare, expediere, recepţionare, păstrare, modificare şi/sau nimicire a documentelor electronice;

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

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

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

m) **dispozitiv securizat de creare a semnăturii electronice** – dispozitiv de creare a semnăturii care întruneşte cerinţele prevăzute de aliniate 3) şi 4) din articolul 8 din prezenta lege;

n) **dispozitiv de verificare a semnăturii electronice** – unităţi de software şi (sau) hardware configurate, utilizate la aplicarea datelor de verificare a semnăturilor;

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

p) **destinatar al documentului electronic** - adresantul documentului electronic sau altă persoană care, în condiţiile legii sau ale contractului, recepţionează documentul electronic expediat adresantului;

q) **intermediar în circulaţia electronică a documentelor** – întreprinzător individual sau persoana juridică care, din însărcinarea alcătuitorului şi/sau a adresantului documentului electronic, organizează şi administrează sistemul de circulaţie electronică a documentelor şi/sau prestează servicii legate de circulaţia electronică a documentelor;

r) **marca temporală** – atribut al documentului electronic, care, prin intermediul semnăturii electronice, certifică faptul că informaţia a existat la un moment de timp determinat, cu păstrarea autenticităţii şi integrităţii documentului electronic;

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

t) **produs asociat semnăturii electronice** – unităţi 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;

u) **semnatar** – persoana care deţine un dispozitiv de creare a semnăturii electronice şi care acţionează fie în nume propriu, fie în numele persoanei fizice, al persoanei juridice sau al entităţii pe care o reprezintă;

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

w) **sistemul de circulaţie electronică a documentelor** - sistem tehnico-organizatoric ce asigură circulaţia 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) dreptul părţilor de a utiliza din propria dorinţă orice tip de semnătură electronică, dacă cerinţa 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 părţilor;

b) posibilitatea utilizării de către părţi, din propria dorinţă, a oricărei tehnologii şi (sau) a mijloacelor tehnice care permit utilizarea tipurilor concrete de semnătură electronică, în conformitate cu cerinţele prezentei legi;

c) neadmiterea recunoaşterii lipsei de putere juridică a semnăturii electronice şi (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 şi (sau) a produsului asociat semnăturii electronice.

Articolul 4. Tipuri de semnături electronice:

(1) Tipurile de semnături electronice, ale căror raporturi 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 reprezintă date în formă electronică, ataşate la sau logic asociate cu alte date în formă electronică, şi care sînt utilizate ca metodă de autentificare.

(3) Semnătura electronică avansată necalificată este o semnătură electronică ce îndeplineşte următoarele cerinţe:

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, şi

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 îndeplineşte toate cerinţele semnăturii electronice avansate necalificate şi, suplimentar:

a) se bazează pe un certificat calificat 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 şi se verifică securizat cu utilizarea dispozitivului de verificare a semnăturii electronice şi/sau produsului asociat semnăturii electronice care dispun de confirmarea corespunderii cerinţelor prevăzute de prezenta lege.

Articolul 5. Regimul juridic al semnăturii electronice

(1) Semnătura electronică, indiferent de gradul de protecţie, are efecte juridice şi este acceptată ca probă, inclusiv în justiţie, chiar dacă:

a) se prezintă în format electronic, 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, sau

d) nu este creată printr-un dispozitiv securizat de creare a semnăturii.

(2) Semnătura electronică avansată calificată dispune de aceeaşi valoare juridică ca şi semnătura olografă.

(3) Modalitatea în care se va asigura gradul de protecţie al semnăturii electronice avansate calificate pentru a fi echivalată cu cerinţele faţă de semnătura olografă aplicată pe hîrtie se stabileşte de organul competent, conform atribuţiilor prevăzute de articolul 37 alineatul (2) din prezenta lege.

(4) Pentru alte tipuri de semnături electronice, inclusiv pentru cele aplicate de funcţionarii autorităţilor publice, Guvernul adoptă tipurile de documente electronice pe care acestea se vor aplica. Subiecţii de drept privat pot stabili condiţii mai stricte faţă de semnăturile electronice aplicate pe documentele electronice pentru autentificare.

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

Articolul 6. Recunoaşterea semnăturilor electronice străine

(1) 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, 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 certificatul;

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 şi 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 şi cheia publică

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

(2) Cheia privată şi 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 iniţierea procedurii de creare a cheii private şi cheii publice.

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

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

(5) Cheia privată este păstrată şi 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 şi este accesibilă tuturor.

Articolul 8. Crearea semnăturii electronice

(1) Crearea semnăturii electronice se efectuează prin intermediul dispozitivului de creare a semnăturii electronice şi/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 şi semnăturii electronice avansate calificate dispozitivul de creare a semnăturii electronice şi/sau produsul asociat semnăturii electronice trebuie:

a) să afişeze semnatarului documentului electronic conţinutul informaţiei pe care o semnează;

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

c) să confirme în mod univoc crearea semnăturii electronice.

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

a) datele de creare a semnăturii utilizate pentru crearea semnăturii nu sînt aplicate decît o singură dată, iar confidenţialitatea acestora este asigurată în conformitate cu prezenta lege;

b) datele de creare a semnăturii utilizate pentru crearea semnăturii electronice nu pot fi deduse şi 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 autenticităţii semnăturii electronice

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

(2) La verificarea semnăturii electronice simple părțile se bazează pe prevederile acordului încheiat, care trebuie să prevadă modalitatea de confirmare a integrității documentului electronic semnat.

(3) La verificarea semnăturii electronice avansate necalificate și semnăturii electronice avansate calificate dispozitivul de verificare a semnăturii electronice şi/sau produsul asociat semnăturii electronice trebuie:

a) să ofere posibilitatea afişării conţinutului documentului electronic semnat cu semnătură electronică, sau, în cazul utilizării dispozitivului de creare a semnăturii electronice în baza cartelei SIM, să facă referinţa irevocabilă la documentul dat;

b) să afişeze faptul modificării documentului electronic semnat cu semnătură electronică, cu excepţia cazurilor de utilizare a dispozitivului de creare a semnăturii electronice în baza cartelei SIM;

c) să facă referinţă la persoana, cu utilizarea cheii private a semnăturii electronice căreia a fost semnat documentul electronic.

(4) La verificarea securizată a semnăturii electronice avansate necalificate și semnăturii electronice avansate calificate, trebuie să se garanteze, cu o siguranţă suficientă, că:

a) datele utilizate pentru verificarea semnăturii electronice corespund datelor afişate persoanei care verifică semnătura electronică;

b) semnătura electronică este verificată cu certitudine, rezultatul verificării şi identitatea semnatarului fiind corect afişate;

c) autenticitatea şi valabilitatea certificatului cheii publice solicitat în momentul verificării semnăturii sînt verificate cu certitudine;

d) redarea clară a pseudonimului (în caz de utilizare a acestuia); şi

e) orice modificări care pot influenţa securitatea semnăturii electronice pot fi detectate.

Articolul 10. Utilizarea semnăturii electronice simple

(1) Documentul electronic se consideră semnat cu semnătura electronică simplă dacă este întrunită una dintre următoarele condiţii:

a) semnătura electronică simplă se conţine nemijlocit în documentul electronic sau este logic asociată cu documentul electronic;

b) datele de creare a semnăturii electronice simple se aplică în corespundere cu regulile stabilite de către operatorul sistemului informatic prin intermediul căruia se efectuează crearea şi (sau) expedierea documentului electronic şi în documentul electronic se conţine informaţia care identifică persoana din numele căreia a fost creat (expediat) documentul electronic.

(2) Actele normative şi (sau) acordul părţilor, care stabilesc cazurile de recunoaştere a documentelor electronice, semnate cu semnătura electronică simplă, echivalente documentelor pe suport de hîrtie semnate cu semnătura olografă, trebuie să prevadă următoarele:

a) modalitatea de determinare a persoanei din numele căreia este semnat documentul electronic, în baza semnăturii electronice simple a acesteia;

b) obligaţia persoanei care creează şi (sau) utilizează date de creare a semnăturii electronice simple de a asigura confidenţialitatea acesteia.

Articolul 11. Limitele utilizării unor tipuri de semnături electronice

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

a) semnarea documentelor electronice ce conţin informaţie atribuită la secretul de stat;

b) semnarea documentelor electronice în raporturile juridice ale autorităţilor şi instituţiilor publice, inclusiv structurilor subordonate acestora, cu persoanele fizice şi juridice de drept privat.

(2) Condiţiile şi modul de aplicare a semnăturii electronice în documentele electronice ale autorităţilor şi instituţiilor 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 conţine date privind persoanele împuternicite, persoanele reprezentate, rolul împuternicirii, data acordării împuternicirilor, durata împuternicirilor, alte menţiuni privind acordarea, modificarea sau retragerea împuternicirilor.

(2) Guvernul stabilește autoritatea publică care este deținătorul Registrului prevăzut la alin.(1).

Capitolul III
REGIMUL JURIDIC AL DOCUMENTULUI ELECTRONIC

Articolul 13. Regimul juridic al documentului electronic

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

(2) Informaţia 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 hîrtie, autentificat cu semnătură olografă în cazurile stabilite de actele normative sau de acordul părţilor privind aplicarea semnăturilor electronice.

(3) Actele normative sau acordul părţilor privind aplicarea semnăturilor electronice care stabilesc cazurile de recunoaştere a documentelor electronice, semnate cu semnătura electronică simplă sau cu semnătura electronică avansată necalificată, asimilate, după efectele sale, cu documentul analogic pe suport de hîrtie, autentificat cu semnătură olografă, trebuie să prevadă modalitatea de verificare a semnăturii electronice, precum şi obligaţiile părţilor privind confidenţialitatea şi răspunderea materială

(4) În cazul în care, conform legislaţiei, se cere ca documentul să fie perfectat sau prezentat pe suport de hîrtie, documentul electronic se consideră corespunzînd acestei cerinţe.

(5) În cazul în care, conform legislaţiei, se cere ca documentul pe suport de hîrtie să fie autentificat cu ştampilă, documentul electronic se consideră corespunzînd acestei cerinţe.

(6) Cu o singură semnătură electronică pot fi semnate cîteva 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 aceluia cu care este semnat tot setul.

(7) Modul de utilizare a documentelor electronice în sistemul judecătoresc este reglementat de legislaţia procesuală.

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

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

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

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

(12) Copie a documentului electronic se consideră reprezentarea (redarea) acestuia pe suport de hîrtie, într-o formă perceptibilă. Copia documentului electronic se autentifică în modul prevăzut de legislaţie pentru autentificarea copiilor documentelor pe suport de hîrtie şi va conţine menţiunea despre faptul că este copie a documentului electronic.

Articolul 14. Utilizarea documentului electronic

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

(2) Documentul electronic poate fi utilizat în scopul expedierii datelor şi comunicărilor, ţinerii corespondenţei, întocmirii actelor juridice, precum şi în calitate de document de plată.

Articolul 15. Cerinţele faţă de documentul electronic

(1) Documentul electronic trebuie să corespundă următoarelor cerinţe principale:

a) să fie creat, prelucrat, expediat, recepționat, păstrat, modificat şi/sau nimicit cu ajutorul mijloacelor tehnice şi/sau de program;

b) să conţină, pentru confirmarea autenticităţii acestuia, una sau mai multe semnături electronice ce corespund condiţiilor şi cerinţelor stabilite de prezenta lege;

c) să fie creat şi utilizat prin metode şi 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:

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 autenticităţii documentului electronic se efectuează prin verificarea, cu dispozitive de verificare a semnăturii electronice şi/sau produsul asociat semnăturii electronice, a autenticităţii acestei semnături.

Articolul 17. Organizarea circulaţiei electronice a documentelor

(1) Circulaţia electronică a documentelor se efectuează conform prevederilor prezentei legi şi regulilor stabilite de către proprietarul sistemului respectiv de circulaţie electronică a documentelor, precum şi conform contractelor încheiate între subiecţii circulaţiei electronice a documentelor.

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

a) crearea şi prelucrarea documentului electronic;

b) expedierea şi recepţionarea documentului electronic;

c) verificarea autenticităţii documentului electronic;

d) confirmarea recepționării documentului electronic;

e) evidenţa documentelor electronice;

f) păstrarea, modificarea şi/sau nimicirea documentului electronic;

g) crearea exemplarelor suplimentare ale documentului electronic,

h) crearea şi autentificarea copiilor documentului electronic pe suport de hîrtie.

i) aplicarea mărcii temporale

(3) Modul de creare, prelucrare, expediere, recepționare, păstrare, modificare şi/sau nimicire a documentului electronic se stabileşte de Guvern şi/sau de către proprietarul sistemului corespunzător de circulaţie electronică a documentelor.

Articolul 18. Subiecţii circulaţiei electronice a documentelor

(1) Subiecţi ai circulaţiei electronice a documentelor pot fi:

a) cetăţenii Republicii Moldova, cetăţenii străini, apatrizii;

b) persoanele juridice, inclusiv cele străine, indiferent de tipul de proprietate şi forma juridică de organizare;

c) statul, în persoana autorităţilor publice;

d) organizaţiile internaţionale;

e) intermediarii în circulaţia electronică a documentelor;

f) prestatorii de servicii de certificare.

(2) Subiecţii circulaţiei electronice a documentelor sînt investiţi cu drepturi şi obligaţii stabilite de legislaţie şi de contractele corespunzătoare.

Articolul 19. Intermediarul în circulaţia electronică a documentelor

(1) La organizarea şi efectuarea circulaţiei electronice a documentelor pot participa intermediari în condiţiile prezentei legi şi în conformitate cu regulile stabilite de proprietarul sistemului corespunzător de circulaţie electronică a documentelor.

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

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

b) să dispună de personal cu competență și/sau experiență în domeniul tehnologiei informaţiei sau securităţii informaţionale;

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

d) să asigure protecţia şi păstrarea documentelor electronice;

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

Articolul 20. Crearea documentului electronic

(1) Documentul electronic este creat de semnatarul acestuia şi conţine informaţie care constituie conţinutul acestuia, precum şi 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 21. Expedierea şi recepționarea documentului electronic

(1) Documentul electronic poate fi expediat şi recepţionat cu ajutorul sistemelor informaţionale şi de comunicaţii electronice, şi/sau purtătorilor materiali.

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

(3) În cazul în care semnatarul şi adresantul documentului electronic nu au convenit altfel, documentul electronic se consideră expediat dacă:

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

b) este adresat în mod corespunzător sau în alt mod direcţionat în sistemul informaţional indicat de adresant;

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

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

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

a) intră în sistemul informaţional din care adresantul poate să extragă documentele electronice;

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

(5) Documentul electronic se consideră neexpediat în cazul în care adresantul ştia sau trebuia să ştie că:

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

b) semnatarul nu este iniţiatorul expedierii documentului electronic;

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

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

Articolul 22. Momentul expedierii şi primirii documentului electronic

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

(2) Dacă semnatarul şi adresantul documentului electronic nu au convenit altfel, moment al recepționării documentului electronic se consideră momentul intrării acestuia în sistemul informaţional indicat de adresant. În cazul în care adresantul documentului electronic nu a indicat sistemul informaţional respectiv, documentul electronic se consideră recepționat din momentul intrării acestuia în sistemul informaţional al adresantului, iar în cazul în care adresantul nu dispune de un asemenea sistem - din momentul extragerii de către adresant a documentului electronic din sistemul informaţional prin care a fost transmis.

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

(4) Dacă semnatarul şi adresantul documentului electronic au convenit asupra confirmării recepţionării documentului electronic, moment al recepţionării acestuia se consideră momentul expedierii de către adresant a confirmării privind recepţionarea, cu aplicarea mărcii temporale după caz.

Articolul 23. Evidenţa documentelor electronice

(1) Evidenţa documentelor electronice ale persoanelor fizice şi/sau juridice se efectuează în conformitate cu legislaţia, prin ţinerea registrelor electronice şi/sau pe suport de hîrtie.

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

Articolul 24. Păstrarea documentelor electronice

(1) Subiecţii circulaţiei electronice a documentelor sînt obligaţi să păstreze originalele documentelor electronice pe suport material, într-o formă ce permite verificarea autenticităţii acestora.

(2) Termenul de păstrare a documentelor electronice nu poate fi mai mic decît termenul prevăzut de legislaţie pentru documente echivalente pe suport de hîrtie.

(3) Subiecţii circulaţiei electronice a documentelor pot asigura păstrarea acestora, utilizînd serviciile intermediarului în circulaţia electronică a documentelor, cu condiţia respectării prevederilor prezentei legi.

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

Articolul 25. Protecţia documentului electronic

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

(2) Informaţia ce constituie conţinutul documentului electronic este utilizată şi protejată, conform legislaţiei, în funcţie de statutul juridic a acesteia.

(3) Crearea, prelucrarea, expedierea, recepționarea, păstrarea, modificarea şi/sau nimicirea documentului electronic trebuie să corespundă cerinţelor de securitate stabilite faţă de un sistem informaţional concret de către Guvernul şi/sau proprietarul acestuia.

(4) În procesul de creare, prelucrare, expediere, recepționare, păstrare, modificare şi/sau nimicirea documentului electronic se impune păstrarea informaţiei ce permite stabilirea originii, apartenenţei şi destinaţiei documentului electronic, precum şi a datei creării, expedierii și recepționării acestuia.

Capitolul IV
SERVICIILE DE CERTIFICARE

Articolul 26. Prestatorul de servicii de certificare

(1) Prestatorii de servicii de certificare dispun de dreptul de a trece procedura de acreditare.

(2) Prestatorii de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate sînt organizaţi în mod ierarhic. În fruntea ierarhiei se află prestatorul de servicii de certificare de nivel superior.

(3) Organizarea activităţii prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate se stabileşte de Guvern, în limitele prevederilor prezentei legi.

(4) Evidenţa prestatorilor de servicii de certificare acreditaţi se efectuează de către organul competent în cadrul registrului de evidenţă a prestatorilor de servicii de certificare, accesul la care este public.

(5) Înregistrarea în registrul de evidenţă a prestatorilor de servicii de certificare acreditaţi se efectuează la data acreditării acestora de către organul competent.

Articolul 27. 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 întruneşte următoarele cerinţe:

a) dispunerea de resurse financiare (garanţie bancară sau poliţă de asigurare) în valoare de cel puţin 300 mii lei pentru recuperarea unor eventuale prejudicii aduse terţilor din cauza încrederii acestora în datele conţinute în certificatul cheii publice, eliberat de către prestatorul de servicii de certificare, sau în informaţia 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 informaţiei sau securităţii informaţionale, cu competenţă şi/sau experienţă la nivel de gestionare, expertiză în domeniul tehnologiei semnăturilor electronice cu nivelul corespunzător de siguranţă;

c) asigurarea securităţii, fiabilităţii şi continuităţii de prestare a serviciilor de certificare;

d) asigurarea înregistrării informaţiei în registrul certificatelor cheilor publice, în special prestarea operativă a serviciului de suspendare a valabilităţii şi de revocare a certificatelor cheilor publice;

e) asigurarea posibilităţii de stabilire cu exactitate a datei şi a orei eliberării, suspendării valabilităţii sau revocării certificatului cheii publice;

f) verificarea, în conformitate cu actele legislative, a identităţii persoanei pentru care se eliberează un certificat calificat;

g) utilizarea sistemelor şi produselor care sînt protejate împotriva modificărilor şi garantează siguranţa tehnică şi criptografică a funcţiilor pe care şi le asumă;

h) crearea condiţiilor de evitare a falsificării certificatelor şi, în cazul în care prestatorul de servicii de certificare generează date de creare de semnături, garantarea confidenţialităţii 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 şi modifica date;

autenticitatea informaţiei să poată fi controlată;

certificatele să fie disponibile publicului pentru informare;

toate modificările tehnice care compromit cerinţele de siguranţă să fie vizibile pentru operator.

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

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

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

c) corespunderea sistemelor şi produselor utilizate cerinţelor prezentei legi;

d) studiile şi calificările persoanelor cu funcţii de răspundere, ale căror obligaţii funcţionale ţin nemijlocit de prestarea serviciilor de certificare;

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

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

g) licenţa eliberată de către Camera de Licenţiere ce atestă dreptul de prestare a serviciilor în domeniul protecţiei criptografice şi tehnice a informaţiei (numai pentru prestatorii ce prestează servicii de certificare a terţelor persoane).

(4) Documentele menţionate în alineatul (3) litera a) se prezintă în original. Documentele menţionate în alineatul (3) literele b)-h) se prezintă în original, însoţite 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 şi semnăturii electronice avansate necalificate este obligat să prezinte informaţiile, în formatul stabilit de organul competent, referitoare la procedurile de securitate şi de certificare utilizate, precum şi datele sale de identificare.

(6) Organul competent, în baza documentelor prezentate şi 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 şi eliberează acestuia certificatul de acreditare de modelul stabilit şi, 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 cerinţelor specificate în alineatul (2) al prezentului articol sau prezentarea informaţiei neveridice în documentele ce se anexează la cererea de acreditare.

(10) Refuzul de acreditare nu poate împiedica depunerea repetată a documentelor în vederea acreditării, dacă au fost înlăturate cauzele care au servit temei pentru refuzul de acreditare.

(11) Decizia privind refuzul de acreditare poate fi atacată în instanţa 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, prestatorului de servicii de certificare i se eliberează un duplicat al certificatului.

(14) Informaţia despre prestatorii de servicii de certificare, care au fost acreditaţi, precum şi 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 şi 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 acreditaţi în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate sînt obligaţi să comunice organului competent, cu cel puţin 10 zile înainte, orice intenţie de modificare a procedurilor de securitate şi de certificare, cu precizarea datei şi orei la care modificarea intră în vigoare, precum şi să confirme în termen de 24 de ore modificarea efectuată.

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

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

(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 28. Activitatea prestatorului de servicii de certificare

(1) Prestatorul de servicii de certificare:

a) creează şi eliberează certificatele cheilor publice;

b) suspendă şi revocă certificatele cheilor publice, restabileşte valabilitatea certificatelor suspendate;

c) ţine registrul certificatelor cheilor publice, asigură actualizarea acestuia şi accesul liber la registru; şi (sau)

d) prestează, în bază de contract, alte tipuri de servicii ce ţin de semnătura electronică.

(2) Activitatea prestatorului de servicii de certificare reprezintă o activitate în domeniul protecţiei criptografice şi tehnice a informaţiei şi este supusă licenţierii de către Camera de Licenţiere, în conformitate cu actele legislative.

Articolul 29. Obligaţiile 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 informaţiilor din certificatul cheii publice cu informaţiile prezentate de către titularul certificatului cheii publice;

c) să introducă certificatul cheii publice în registrul certificatelor cheilor publice nu mai tîrziu de data şi ora cînd începe să curgă termenul de valabilitate a certificatului;

d) să asigure accesul liber la registrul certificatelor cheilor publice;

e) să suspende valabilitatea sau să revoce certificatul cheii publice în cazurile prevăzute de lege şi să facă menţiunea respectivă în registrul certificatelor cheilor publice, în termenele stabilite;

f) să acopere prejudiciile aduse oricărei entităţi sau persoane fizice, care are încredere în mod rezonabil în datele conţinute în certificatul cheii publice eliberat de către prestatorul de servicii de certificare, prin faptul că a omis să înregistreze revocarea certificatului;

g) să înştiinţeze titularul certificatului cheii publice despre faptele care au devenit cunoscute prestatorului de servicii de certificare şi care fac imposibilă utilizarea în continuare a cheii private, precum şi despre revocarea certificatului cheii publice;

h) să prezinte informaţiile necesare pentru autentificarea semnăturii electronice;

i) să solicite eliberarea duplicatului certificatului de acreditare, în cazul pierderii sau deteriorării acestuia;

k) să îndeplinească alte obligaţii 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 legislaţie, 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 33 din prezenta lege, toate informaţiile pertinente referitoare la un certificat calificat, în special pentru a putea furniza dovezi de certificare în justiţie. Înregistrările pot fi efectuate prin mijloace electronice;

c) înainte să stabilească o relaţie 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 şi condiţiile exacte de utilizare a certificatului, inclusiv cu privire la limitele impuse utilizării sale, la existenţa unui sistem de acreditare şi la procedurile de contestare şi soluţionare a litigiilor. Aceste informaţii, care pot fi transmise pe cale electronică, trebuie comunicate în scris şi într-un limbaj accesibil. Elementele pertinente ale informaţiilor trebuie puse, de asemenea, la cerere, la dispoziţia părţilor terţe care beneficiază de certificat;

d) să păstreze toată informaţia cu privire la certificatul cheii publice ataşat semnăturilor electronice avansate calificate cel puţin 15 ani din momentul revocării sau expirării certificatului, în eventualitatea apariţiei unor litigii.

Articolul 30. Cererea de certificare a cheii publice

(1) Cererea de certificare a cheii publice se depune în format electronic şi/sau în formă de document pe suport de hîrtie, semnat cu semnătura olografă a solicitantului.

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

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

b) alte date de identificare ale solicitantului, în funcţie de scopul pentru care se eliberează certificatul cheii publice, precum şi informaţiile necesare pentru comunicarea cu acesta;

c) alte informaţii stabilite de prezenta lege.

Articolul 31. 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 de la data înregistrării cererii dacă părţile nu stabilesc altfel, luîndu-se decizia de certificare sau de refuz al certificării cheii publice.

(2) În baza deciziei de certificare a cheii publice, prestatorul de servicii de certificare creează şi eliberează certificatul respectiv al cheii publice de modelul 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 terţi în procesul de întocmire sau de depunere a cererii;

c) prezentare în cerere a unor informaţii ce nu corespund realităţii.

(4) Decizia de refuz a certificării cheii publice poate fi atacată în instanţa 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 32. 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 conţină următoarele informaţii:

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 şi alte date ale titularului certificatului cheii publice, în funcţie de scopul pentru care se eliberează certificatul, precum şi informaţiile necesare pentru comunicarea cu acesta;

d) cheia publică;

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

f) date despre algoritmul criptografic al semnăturii electronice;

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

h) alte informaţii stabilite de prezenta lege.

(3) Certificatul calificat al cheii publice se emite de către prestatorul de servicii de certificare acreditat şi suplimentar trebuie să conţină următoarele informaţii:

a) menţiunea care să indice că certificatul este eliberat ca certificat calificat;

b) posibilitatea includerii, atunci cînd este cazul, a unei calităţi speciale a semnatarului, în funcţie 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 necalificat al cheii publice servesc numele şi prenumele acestuia şi/sau pseudonimul, după caz, în certificatul calificat al cheii publice – numele şi prenumele, iar în certificatul cheii publice al prestatorului de servicii de certificare – denumirea prestatorului.

(5) În cazul semnăturii electronice simple şi a semnăturii electronice avansate necalificate, structura certificatului cheii publice se stabileşte de către prestatorul de servicii de certificare, în conformitate cu cerinţele stabilite de prezenta lege. În cazul semnăturii electronice avansate calificate, structura certificatului cheii publice se stabileşte de către organul competent, în conformitate cu cerinţele stabilite de prezenta lege.

(6) Certificatul cheii publice se semnează cu semnătura electronică avansată necalificată 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 legislaţie sau prin acordul părţilor, prestatorul de servicii de certificare creează certificatul cheii publice şi în formă de document pe suport de hîrtie, în două exemplare. În acest caz, certificatul cheii publice sub formă de document pe suport de hîrtie este semnat cu semnăturile olografe ale titularului certificatului cheii publice şi ale persoanei abilitate a prestatorului de servicii de certificare şi se autentifică cu ştampila 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 restricţii cu privire la utilizarea acestuia, precum şi 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 şi alte informaţii decît cele specificate în alineatele (2) şi (3), cu condiţia ca acestea să nu contravină

legislaţiei şi să nu pună în pericol securitatea naţională sau ordinea publică, şi numai după o prealabilă verificare a exactităţii informaţiilor în cauză.

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

Articolul 33. Termenul de valabilitate şi 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 stabileşte de către prestatorul de servicii de certificare, dar nu poate constitui mai mult de 5 ani.

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

Articolul 34. Suspendarea şi 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 informaţii neveridice în cererea de certificare a cheii publice sau în certificatul cheii publice;

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

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

e) la modificarea certificatului cheii publice;

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

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

(3) În cazul primirii informaţiilor 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 înştiinţeze titularul certificatului cheii publice, la cerere, despre motivele revocării certificatului acestuia.

Articolul 35. Obligaţiile titularului certificatului cheii publice

Titularul certificatului cheii publice este obligat:

a) să asigure condiţiile 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 confidenţialitatea cheii private;

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

a pierdut cheia privată;

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

informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;

d) să înştiinţeze la timp prestatorul de servicii de certificare despre orice modificare a informaţiilor cuprinse în certificatul cheii publice;

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

Articolul 36. Registrul certificatelor cheilor publice

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

(2) Registrul certificatelor cheilor publice va conţine:

a) certificatele valabile ale cheilor publice;

b) certificatele revocate şi suspendate ale cheilor publice;

c) data şi ora eliberării certificatelor cheilor publice;

d) data şi ora revocării certificatelor cheilor publice;

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

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

Capitolul V
MONITORIZARE ŞI CONTROL

Articolul 37. Atribuţiile autorităţilor publice în domeniul aplicării semnăturii electronice

(1) Organul competent de elaborarea şi promovarea politicii de stat şi cu exercitarea controlului în domeniul aplicării semnăturii electronice simple şi avansate necalificate este Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, care exercită următoarele atribuţii:

a) efectuează acreditarea voluntară a prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate, la iniţiativa acestora;

b) asigură ţinerea, actualizarea şi accesul liber la datele registrului de evidenţă a prestatorilor de servicii de certificare acreditaţi în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate;

c) elaborează şi aprobă, prin acte normative, cerinţele în domeniul aplicării semnăturii electronice simple şi a semnăturii electronice avansate necalificate;

d) monitorizează şi controlează respectarea cerinţelor la prestarea serviciilor de certificare în domeniul aplicării semnăturii electronice simple şi semnăturii electronice avansate necalificate;

e) participă la elaborarea şi aprobarea reglementărilor tehnice şi standardelor în domeniul semnăturii electronice simple şi semnăturii electronice avansate necalificate;

f) acordă, la solicitare, asistenţă metodică şi practică autorităţilor publice la aplicarea mecanismelor semnăturii electronice simple şi semnăturii electronice avansate necalificate;

g) realizează colaborarea internaţională în domeniul semnăturii electronice simple şi semnăturii electronice avansate necalificate.

(2) Organul competent de elaborarea şi promovarea politicii de stat şi cu exercitarea controlului în domeniul aplicării semnăturii electronice avansate calificate este Serviciul de Informaţii şi Securitate, care exercită următoarele atribuţii:

a) efectuează acreditarea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate;

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

c) asigură ţinerea, actualizarea şi accesul liber la datele registrului de evidenţă a prestatorilor de servicii de certificare acreditaţi în domeniul aplicării semnăturii electronice avansate calificate;

d) elaborează şi aprobă, prin acte normative, cerinţele în domeniul aplicării semnăturii electronice avansate calificate;

e) monitorizează şi controlează asigurarea cerinţelor la prestarea serviciilor de certificare în domeniul aplicării semnăturii electronice avansate calificate;

f) participă la elaborarea şi aprobarea reglementărilor tehnice şi a standardelor în domeniul semnăturilor electronice avansate calificate;

g) acordă, la solicitare, asistenţă metodică şi practică autorităţilor publice la aplicarea mecanismelor semnăturii electronice avansate calificate;

h) realizează colaborarea internaţională în domeniul semnăturii electronice avansate calificate.

(3) Autoritatea publică menţionată în alineatul (1) poate delega atribuţiile sale de acreditare, control, evidenţă şi asistenţă unei instituţii publice aflate în subordine.

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

Articolul 38. Controlul în domeniul aplicării semnăturii electronice

(1) Organul competent are obligaţia să controleze respectarea obligaţiilor prevăzute de prezenta lege la prestarea serviciilor de certificare de către prestatorii acreditaţi şi la acordarea/prelungirea acreditării.

(2) Controlul se efectuează de către Comisia de control în domeniul semnăturii electronice (în continuare – Comisia).

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

(4) Componenţa nominală a Comisiei se stabileşte pentru fiecare caz în parte.

(5) Comisia are dreptul:

a) la acces liber la materialele documentare, necesare pentru desfăşurarea lucrărilor, pe suport de hîrtie şi în mod electronic, ce ţin de prestarea serviciilor de certificare, precum şi la sistemele de distribuţie de aplicaţii soft, aplicaţiile soft şi mijloacele tehnice instalate;

b) să obţină informaţii complete despre condiţiile şi modul de exploatare a mijloacelor tehnice şi de program;

c) să obţină informaţii de la persoanele responsabile şi personalul prestatorului de servicii de certificare în privinţa presării serviciilor de certificare şi care ţin de obiectul controlului;

d) la acces liber, 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 şi fără documentele de identitate ale membrilor.

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

a) legalitatea şi respectarea competenţei stabilite de lege;

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

c) tratarea dubiilor, apărute la aplicarea legislaţiei, 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 acţiunile organului competent, inclusiv în instanţa judecătorească.

(8) Controalele planificate asupra respectării de către prestatorul de servicii de certificare a obligaţiilor prevăzute de prezenta lege se efectuează de către organul competent cel mult o dată în decursul anului calendaristic, cu cooptarea, după caz, a reprezentanţilor instituţiilor cu funcţii de reglementare şi de control, conform competenţei.

(9) Planurile controalelor, elaborate de organul competent şi aprobate în modul stabilit, se coordonează, în privinţa termenelor de efectuare, cu conducerea prestatorului de servicii de certificare, cel puţin cu 30 de zile lucrătoare pînă la începerea acestor controale.

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

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

b) recepţionării cererilor şi reclamaţiilor scrise argumentate în adresa organului competent referitor la încălcările şi la îndeplinirea necorespunzătoare a obligaţiunilor stabilite de prezenta lege de către prestatorul de servicii de certificare;

c) cererii instanţei judecătoreşti.

(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 prescripţiei 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 nu poate depăşi 15 zile lucrătoare, a controlului inopinat – nu mai mult de 10 zile lucrătoare, iar a celui repetat – nu mai mult de 5 zile lucrătoare. Prelungirea termenului de efectuare a controlului nu se admite.

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

(16) În baza rezultatelor controlului, se întocmeşte 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 3 zile lucrătoare de la data întocmirii actului de control, poate prezenta în scris argumentarea dezacordului, anexînd documentele de rigoare.

(17) În cazul în care se depistează încălcări ale respectării obligaţiilor prevăzute de prezenta lege, organul competent, în termen de 15 zile lucrătoare de la data întocmirii actului de control, emite prescripţia privind lichidarea încălcărilor, cuprinzînd recomandările privind modul de remediere a tuturor deficienţelor identificate, precum şi avertizarea despre posibila suspendare sau retragere a acreditării, dacă încălcările depistate nu vor fi lichidate în termenul stabilit.

(18) Termenul minim pentru lichidarea încălcărilor depistate constituie 5 zile lucrătoare, iar cel maxim – 15 zile lucrătoare.

(19) În cazuri excepţionale şi 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 prescripţia privind lichidarea încălcărilor obligaţiilor prevăzute de prezenta lege, este obligat, în termenul indicat în prescripţie, să comunice organului competent informaţia privind lichidarea încălcărilor.

(21) În cazul constatării semnelor de compromitere a cheilor private ale prestatorului de servicii de certificare acreditat, încălcării obligaţiilor 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) Informaţiile despre rezultatele efectuării controlului se publică de către organul competent pe pagina sa oficială în reţeaua Internet.

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

Articolul 39. Suspendarea şi reluarea valabilităţii 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 activităţii de întreprinzător.

(2) Temei pentru realizarea acţiunilor 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 obligaţiilor stabilite de prezenta lege;

c) nevalabilitatea garanţiei bancare sau a poliţei de asigurare pentru prestatorul de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate, prevăzute de articolul 27 alineatul (2) lit.a) din prezenta lege;

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

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

(4) Prestatorul de servicii de certificare este obligat să înştiinţeze în scris organul competent despre înlăturarea circumstanţelor care au dus la suspendarea acreditării.

(5) Decizia privind reluarea valabilităţii acreditării se adoptă de către organul competent în temeiul hotărîrii instanţei de judecată care a emis hotărîrea de suspendare a acesteia, în termen de 3 zile lucrătoare de la data primirii înştiinţării. Decizia se aduce la cunoştinţă prestatorului de servicii de certificare în termen de 3 zile lucrătoare de la data adoptării acesteia.

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

Articolul 40. Retragerea 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 activităţii de întreprinzător.

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

a) cererea prestatorului de servicii de certificare privind încetarea activităţii, 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 desfăşurării genului de activitate acreditată;

e) neînlăturarea, în termenul stabilit, a circumstanţelor care au dus la suspendarea acreditării;

f) nerespectarea a doua oară a prescripţiilor privind lichidarea încălcărilor ce ţin de obligaţiile stabilite de prezenta lege.

(3) Menţiunea referitoare la data şi numărul deciziei privind retragerea acreditării se înscrie în registrul de evidenţă a prestatorilor de servicii de certificare, nu mai tîrziu 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 şi-a încetat activitatea se revocă şi 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 îşi 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 41. Răspunderea persoanelor fizice şi juridice

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

(2) Intermediarul, în circulaţia electronică a documentelor, poartă răspundere, stabilită de actele legislative, pentru neexecutarea sau executarea necorespunzătoare a obligaţiilor şi pentru calitatea necorespunzătoare a serviciilor prestate, precum şi pentru prejudiciul cauzat de aceste acţiuni (inacţiuni).

(3) Pentru acces ilegal la informaţia cuprinsă în documentele electronice, persoanele poartă răspundere conform legislaţiei cu privire la accesul la informaţie şi protecţia datelor cu caracter personal.

(4) Litigiile care apar în cadrul circulaţiei electronice a documentelor, precum şi cele legate de utilizarea documentelor electronice şi de aplicarea semnăturii electronice, se soluţionează de către subiecţii circulaţiei electronice a documentelor, în conformitate cu actele legislative şi contractele încheiate.

Articolul 42. Răspunderea prestatorului de servicii de certificare

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

(2) Prestatorul de servicii de certificare poartă răspundere civilă pentru prejudiciul cauzat urmare a neîndeplinirii obligaţiilor prevăzute de prezenta lege, cu excepţia 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 restricţiilor de utilizare a acestuia sau a restricţiilor privind limitele valorii operaţiunilor în care acesta poate fi utilizat.

Articolul 43. Răspunderea titularului certificatului cheii publice

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

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

a) neîndeplinirea obligaţiilor stabilite de prezenta lege;

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

Capitolul VII
PROTECŢIA DATELOR CU CARACTER PERSONAL

Articolul 44. Protecţia datelor cu caracter personal

(1) Prestatorii de servicii de certificare şi autoritatea responsabilă de supraveghere vor asigura ca prevederile Legii nr.17-XVI din 15 februarie 2007 cu privire la protecţia 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, şi numai atunci cînd acestea sînt necesare pentru eliberarea şi menţinerea certificatului. Datele personale nu pot fi colectate sau prelucrate în alte scopuri fără consimţămîntul prealabil şi expres al persoanei interesate.

Capitolul VIII
DISPOZIŢII FINALE

Articolul 45. Dispoziţii finale şi tranzitorii

(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 şi 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 legislaţiei în concordanţă cu prezenta lege;

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

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

(4) Prevederile articolului 5 alineatul 1 în partea ce ţine de justiţie intră în vigoare începînd cu 1 ianuarie 2015.

Preşedintele Parlamentului