

GVERNUL REPUBLICII MOLDOVA

**Hotărîre pentru aprobarea Regulamentului privind ordinea
de aplicare a semnăturii digitale în documentele electronice
ale autorităților publice**

Nr.320 din 28.03.2006

Monitorul Oficial al R.Moldova nr.51-54/350 din 31.03.2006

* * *

Întru executarea articolului 18 alineatul (3) al Legii 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), Guvernul HOTĂRĂȘTE:

1. Se aprobă Regulamentul privind ordinea de aplicare a semnăturii digitale în documentele electronice ale autorităților publice (se anexează).

2. Se pune în sarcina autorităților administrației publice centrale și se recomandă autorităților administrației publice locale să creeze, în termen de trei luni, condițiile necesare pentru aplicarea semnăturii digitale în conformitate cu Regulamentul aprobat.

3. Academia de Administrare Publică pe lângă Președintele Republicii Moldova, în comun cu Întreprinderea de Stat "Centrul de telecomunicații speciale" a Serviciului de Informații și Securitate, va organiza cursuri de instruire pentru angajații autorităților publice privind aplicarea semnăturii digitale.

4. Serviciile de certificare a cheilor publice și alte servicii ce țin de semnătura digitală vor fi prestate în conformitate cu prevederile capitolului III al Regulamentului cu privire la sistemele speciale de telecomunicații ale Republicii Moldova, aprobat prin Hotărîrea Guvernului nr.735 din 11 iunie 2002 (Monitorul Oficial al Republicii Moldova, 2002, nr.79-81, art.833), cu modificările și completările ulterioare.

Prim-ministru

Vasile TARLEV

Contrasemnează:
Ministrul dezvoltării
informaționale

Vladimir Molojen

Chișinău, 28 martie 2006.
Nr.320.

Aprobat
prin Hotărîrea Guvernului
nr.320 din 28 martie 2006

REGULAMENT

privind ordinea de aplicare a semnăturii digitale
în documentele electronice ale autorităților publice

I. Dispoziții generale

1. Presentul Regulament este elaborat în temeiul Legii nr.264-XV din 15 iulie 2004 cu privire la documentul electronic și semnătura digitală și determină condițiile generale de aplicare a semnăturii digitale în documentele electronice ale autorităților publice.

2. Autoritatea publică recepționează, pe bază de contract, serviciile de certificare a cheilor publice și alte servicii ce țin de semnătura digitală de la centrul de certificare a cheilor publice al autorităților administrației publice (în continuare - centrul de certificare) în conformitate cu regulamentul acestuia și efectuează schimbul de informații cu centrul de certificare prin intermediul Sistemului de telecomunicații al autorităților administrației publice.

3. Autoritatea publică aplică semnătura digitală doar cu condiția utilizării mijloacelor semnăturii digitale ce dispun de certificatul de conformitate, eliberat în corespundere cu legislația în vigoare. Până la crearea organismelor de evaluare a conformității mijloacelor semnăturii digitale, pot fi utilizate mijloacele semnăturii digitale ce dispun de avizul pozitiv al organului abilitat cu elaborarea și promovarea politicii de stat și cu exercitarea controlului în domeniul aplicării semnăturii digitale (în continuare - organ competent).

4. Angajații autorității publice aplică semnătura digitală în documentele electronice de plată sau de încheiere a tranzacțiilor în limitele valorilor indicate în certificatele cheilor publice.

5. Responsabilitatea pentru organizarea aplicării semnăturii digitale în documentele electronice ale autorității publice o poartă conducătorul acesteia.

II. Ordinea de aplicare a semnăturii digitale

6. Aplicarea semnăturii digitale prevede:

- a) crearea cheii publice și a cheii private;
- b) certificarea cheii publice în centrul de certificare;
- c) semnarea documentului electronic cu semnătura digitală;
- d) verificarea autenticității semnăturii digitale în documentul electronic.

7. Semnătura digitală se aplică în documentele electronice ale autorităților publice de către persoana abilitată, în modul stabilit, să semneze cu semnătura olografă documentele echivalente pe suport de hârtie (în continuare - angajatul).

8. Ordinea interioară de aplicare a semnăturii digitale în documentele electronice ale autorității publice, care prevede, în special, ordinea de creare, coordonare și semnare a documentelor electronice, de verificare a autenticității semnăturii digitale, regulile de ținere a evidenței, de păstrare și nimicire a cheilor private, ordinea de prezentare către centrul de certificare a informației necesare pentru crearea, suspendarea și restabilirea valabilității, revocarea certificatelor cheilor publice, se aprobă de conducătorul autorității publice, în conformitate cu cerințele stabilite în domeniul semnăturii digitale.

9. Subdiviziunea tehnologiei informaționale din cadrul autorității publice, iar în cazul lipsei acesteia - subdiviziunea sau colaboratorul desemnat prin ordinul conducătorului acestei autorități (în continuare - subdiviziunea responsabilă):

- a) oferă consultații angajaților la crearea cheilor publice și

private, precum și la semnarea documentelor electronice și verificarea autenticității semnăturii digitale;

b) pregătește și prezintă centrului de certificare informația necesară pentru crearea certificatelor cheilor publice ale angajaților, precum și cererile de suspendare și restabilire a valabilității, de revocare a certificatelor;

c) asigură accesul angajaților la registrele certificatelor cheilor publice, ținute de centrele de certificare a cheilor publice;

d) ține evidența mijloacelor semnăturii digitale utilizate în autoritatea publică;

e) ține evidența purtătorilor materiali de chei private ale angajaților;

f) asigură păstrarea documentelor pe baza cărora au fost create certificatele cheilor publice ale angajaților;

g) exercită controlul intern asupra utilizării mijloacelor semnăturii digitale și păstrării purtătorilor materiali de chei private de către angajați în conformitate cu cerințele stabilite.

Secțiunea 1. Crearea cheii publice și a cheii private

10. Crearea cheii publice și a cheii private se efectuează personal de către angajat nemijlocit în autoritatea publică sau în centrul de certificare. În caz de necesitate, în timpul creării cheii publice și a cheii private, angajatului i se acordă ajutor de către subdiviziunea responsabilă sau de către personalul centrului de certificare, fără a se încălca confidențialitatea cheii private.

Secțiunea a 2-a. Certificarea cheii publice în centrul de certificare

11. Angajatul poate semna documentele electronice după primirea certificatului cheii publice de la centrul de certificare.

12. Conducătorul autorității publice sau o altă persoană desemnată de conducător remite centrului de certificare lista angajaților ale căror chei publice urmează a fi certificate, indicându-se numele și prenumele acestor persoane, funcțiile pe care le dețin, datele referitoare la subdiviziunea responsabilă, precum și, după caz, limitele valorice pentru care va fi valabilă aplicarea semnăturii digitale în documentele electronice de plată sau de încheiere a tranzacțiilor (în lei moldovenești).

13. În temeiul listei menționate la punctul 12 al prezentului Regulament, centrul de certificare recepționează cererile de certificare a cheilor publice în formă electronică, pe suport material sau prin canal de comunicații securizat, în conformitate cu cerințele organului competent.

14. Cererea de certificare a cheilor publice, întocmită de angajat, trebuie să conțină:

a) denumirea autorității publice și codul ei de identificare IDNO;

b) numele și prenumele angajatului, numărul buletinului de identitate și numărul de identificare al persoanei fizice IDNP, funcția pe care o deține;

c) informația necesară pentru comunicarea cu angajatul (numerele de telefon, fax, adresa poștei electronice);

d) cheia publică pentru care se solicită certificatul;

e) alte date stabilite de organul competent.

15. În conformitate cu lista prezentată de conducătorul autorității publice și în temeiul cererii parvenite de la angajat, centrul de certificare, în termen de trei zile lucrătoare de la data înregistrării cererii, adoptă decizia de certificare a cheii publice.

16. Pe baza deciziei de certificare a cheii publice, centrul de certificare creează și eliberează certificatul respectiv al cheii publice.

17. Examinarea cererilor de certificare a cheilor publice, adoptarea deciziilor de certificare a cheilor publice și crearea certificatelor cheilor publice se efectuează în conformitate cu procedura stabilită în regulamentul centrului de certificare.

18. Certificatul cheii publice trebuie să conțină:

- a) numărul unic de înregistrare al certificatului cheii publice;
- b) datele de identificare ale centrului de certificare;
- c) denumirea autorității publice și codul ei de identificare IDNO;
- d) numele și prenumele angajatului, numărul de identificare al persoanei fizice IDNP, funcția pe care o deține;
- e) informația necesară pentru comunicarea cu angajatul (numerele de telefon, fax, adresa poștei electronice);
- f) cheia publică a angajatului;
- g) data și ora la care începe și încetează să curgă termenul de valabilitate a certificatului cheii publice;
- h) datele despre algoritmul criptografic al semnăturii digitale și alte date tehnologice determinate de centrul de certificare;
- i) sferele de aplicare a semnăturii digitale, precum și, după caz, limitele valorice pentru care este valabilă aplicarea semnăturii digitale în documentele electronice de plată sau de încheiere a tranzacțiilor (în lei moldovenești);
- j) semnătura digitală a persoanei abilitate a centrului de certificare;
- k) alte date, în conformitate cu standardele și cerințele tehnice stabilite de organul competent.

19. La cererea conducătorului autorității publice, centrul de certificare poate indica în certificatele cheilor publice ale angajaților și alte informații decât cele specificate la punctul 18 al prezentului Regulament, în condițiile legislației.

20. Angajatul este obligat să înștiințeze la timp subdiviziunea responsabilă și centrul de certificare despre orice modificare a informațiilor cuprinse în certificatul cheii publice.

21. Valabilitatea certificatului cheii publice se suspendă:

- a) pe baza deciziei organului competent;
- b) pe baza deciziei autorității publice;
- c) la apariția presupunerilor că a fost încălcată confidențialitatea cheii private;
- d) la apariția presupunerilor că informațiile cuprinse în certificatul cheii publice nu corespund realității.

22. Certificatul cheii publice se revocă:

- a) pe baza deciziei organului competent;
- b) pe baza deciziei autorității publice;
- c) la cererea titularului certificatului cheii publice;
- d) în cazul stabilirii faptului de compromitere a cheii private;
- e) la depistarea unor informații neveridice în cererea de certificare a cheii publice sau în certificatul cheii publice;

f) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice, dacă nu a fost luată decizia de restabilire a valabilității certificatului;

g) la necesitatea operării modificărilor în certificatul cheii publice;

h) la expirarea termenului de valabilitate a certificatului cheii publice;

i) la concedierea sau la decesul titularului certificatului cheii publice.

23. Suspendarea, restabilirea valabilității și revocarea certificatelor cheilor publice ale angajaților se efectuează în conformitate cu procedurile stabilite de regulamentul centrului de certificare.

24. Centrul de certificare determină modalitatea legăturii de urgență cu titularul certificatului cheii publice și subdiviziunea responsabilă în caz de compromitere a cheii private.

25. Modul de schimbare a cheilor publice și private ale angajaților la expirarea termenelor de valabilitate a cheilor este stabilit de normele tehnice aprobate de organul competent.

26. În caz de concediere a angajatului, cheia privată ce aparține acestei persoane se nimicește printr-o metodă ce nu admite posibilitatea restabilirii ei, iar certificatul cheii publice corespunzător funcționează pînă la expirarea termenului de valabilitate a certificatului.

Secțiunea a 3-a. Semnarea documentului electronic

27. Documentele electronice se semnează de către angajat cu ajutorul mijloacelor semnăturii digitale, utilizînd cheia sa privată.

28. În timpul îndeplinirii atribuțiilor funcționale, angajatul utilizează cheia sa privată creată în acest scop. Se interzice utilizarea cheii private în scopuri ce nu țin de îndeplinirea atribuțiilor funcționale.

29. Subdiviziunea responsabilă asigură accesul angajaților la informația actualizată privind certificatele cheilor publice valabile, suspendate și revocate sau în alt mod asigură posibilitatea verificării valabilității certificatelor cheilor publice eliberate de centrul de certificare, inclusiv prin distribuirea către angajați a listei modificate a certificatelor cheilor publice revocate, furnizată de centrul de certificare.

Secțiunea a 4-a. Verificarea autenticității semnăturii digitale

30. Verificarea autenticității semnăturilor digitale în documentele electronice se efectuează de către persoana care verifică autenticitatea documentului electronic cu utilizarea mijloacelor semnăturii digitale și certificatului cheii publice al elaboratorului documentului.

III. Obligațiile și drepturile angajatului

31. Angajatul are obligația:

a) să asigure condițiile necesare pentru a exclude accesul unei alte persoane la cheia sa privată;

b) să utilizeze mijloacele semnăturii digitale în conformitate cu documentația de exploatare și regimul de utilizare a mijloacelor semnăturii digitale, stabilit de autoritatea publică;

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

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

a) pierdut cheia privată;

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

informațiile cuprinse în certificatul cheii publice nu corespund realității;

e) la soluționarea situațiilor litigioase ce țin de stabilirea autenticității și/sau a autorului documentului contestabil, să ofere informațiile necesare;

f) să îndeplinească alte obligații stabilite de legislația în vigoare.

32. Angajatul are dreptul:

a) să semneze și să verifice semnătura digitală în documentele electronice;

b) să nu primească spre executare documentele electronice semnate cu semnătură digitală dacă:

certificatul cheii publice al persoanei care a semnat documentul electronic se află în lista certificatelor cheilor publice revocate sau nu era valabil la momentul semnării documentului electronic;

nu este confirmată autenticitatea semnăturii digitale în documentul electronic;

semnătura digitală se utilizează cu încălcarea sferei de aplicare sau cu depășirea limitelor valorice pentru care este valabilă în documentele electronice de plată sau de încheiere a tranzacțiilor;

c) în cazul apariției situației litigioase ce ține de stabilirea autenticității și/sau a autorului documentului contestabil, să solicite soluționarea ei în modul stabilit;

d) să primească consultații cu privire la aplicarea semnăturii digitale și verificarea autenticității documentului electronic de la personalul subdiviziunii responsabile și al centrului de certificare.

IV. Asigurarea securității

33. Evidența purtătorilor materiali de chei private este ținută de subdiviziunea responsabilă pe exemplare, în conformitate cu ordinea interioară de aplicare a semnăturii digitale în documentele electronice ale autorității publice.

34. Păstrarea purtătorilor materiali de chei private se efectuează în condiții care să excludă pierderea și utilizarea lor neautorizată.

35. La transportarea purtătorilor materiali de chei private se asigură protecția lor contra deteriorării fizice și influenței din exterior.

36. Cheia privată și, dacă este prevăzut, duplicatul ei se păstrează separat, cu asigurarea condițiilor în care compromiterea lor concomitentă nu este posibilă.

37. Mijloacele semnăturii digitale utilizate în autoritatea publică

sînt supuse evidenței și controlului integrității de către subdiviziunea responsabilă. Se interzice utilizarea mijloacelor semnăturii digitale în cazul încălcării integrității lor.

38. Regimul de utilizare a mijloacelor semnăturii digitale în autoritatea publică trebuie să excludă posibilitatea accesului persoanelor terțe la aceste mijloace, modificării și utilizării lor neautorizate.

V. Acțiunile în caz de compromitere a cheii private

39. La împrejurări legate de compromiterea cheii private se atribuie următoarele situații:

a) pierderea purtătorului material de cheie privată, indiferent de găsirea lui ulterioară;

b) apariția suspiciunilor privind dezvăluirea informației sau denaturarea ei în sistemul de legătură sau la locurile de utilizare a mijloacelor semnăturii digitale;

c) încălcarea integrității ștampilei la locul de păstrare a purtătorilor materiali de chei private;

d) pierderea cheii de la locul de păstrare în momentul aflării în acesta a purtătorilor materiali de chei private, indiferent de găsirea ulterioară a cheii;

e) accesul persoanelor terțe la cheia privată sau la mijloacele semnăturii digitale;

f) alte evenimente care dau temei de a presupune că a fost încălcată confidențialitatea cheii private.

40. În cazul apariției unei împrejurări legate de compromiterea cheii private, titularul ei și/sau subdiviziunea responsabilă au obligația să informeze imediat, în modul stabilit, centrul de certificare despre compromiterea cheii private.

41. În termen de trei zile lucrătoare, subdiviziunea responsabilă înștiințează în scris centrul de certificare despre compromiterea cheii private.

42. Centrul de certificare, primind informația cu privire la compromiterea cheii private a angajatului, trebuie să se convingă, în modul stabilit, de autenticitatea acesteia și imediat, dar nu mai târziu de trei ore de lucru, să suspende valabilitatea sau să revoce certificatul cheii publice respective.

43. Valabilitatea certificatului cheii publice se suspendă în cazurile prevăzute de prezentul Regulament pe un termen stabilit de organul competent. În cazul în care la expirarea termenului de suspendare a valabilității certificatului cheii publice nu parvine cererea de restabilire a valabilității certificatului, certificatul cheii publice se revocă.

44. După suspendarea valabilității sau revocarea certificatului cheii publice, centrul de certificare anunță în scris, în modul stabilit, subdiviziunea responsabilă despre acest fapt.

45. Referitor la faptul compromiterii cheii private se desfășoară o investigație de serviciu, la încheierea căreia, potrivit deciziei comisiei, cheia privată care a fost compromisă se nimicește.

46. Crearea cheilor publice și private noi se face după investigarea și înlăturarea cauzelor de compromitere a cheii private.

VI. Ordinea de soluționare a situațiilor litigioase

în domeniul aplicării semnăturii digitale

47. În conformitate cu prezentul Regulament, se soluționează situațiile litigioase care apar în legătură cu:

- a) contestarea integrității documentului electronic;
- b) contestarea identificării persoanei care a semnat documentul electronic;
- c) contestarea împuternicirilor persoanei care a semnat documentul electronic;
- d) contestarea valabilității certificatului cheii publice;
- e) contestarea sferei de aplicare a semnăturii digitale și altor restricții;
- f) neîncrederea în mijloacele semnăturii digitale;
- g) neîncrederea în centrul de certificare;
- h) alte cazuri de apariție a situațiilor litigioase în legătură cu aplicarea semnăturii digitale.

48. Situațiile litigioase se soluționează în regim de lucru și/sau de către Comisia de soluționare a situațiilor litigioase în domeniul aplicării semnăturii digitale.

49. În cazul apariției unor împrejurări ce indică prezența unei situații litigioase, părțile implicate în litigiu (în continuare - părți) au obligația, în termen de cel mult o zi lucrătoare, să verifice prezența acestor împrejurări și să întreprindă măsuri pentru soluționarea situației litigioase, înștiințându-se reciproc despre rezultatele verificării și acțiunile întreprinse.

50. Situația litigioasă se consideră soluționată în regim de lucru dacă nici una dintre părți nu are pretenții.

51. În cazul în care situația litigioasă nu a fost soluționată în regim de lucru, se creează Comisia de soluționare a situațiilor litigioase în domeniul aplicării semnăturii digitale (în c

ontinuare -
Comisia).

52. În cadrul autorității publice, Comisia se creează pe baza deciziei conducătorului acestei autorități, iar în cazul situației litigioase între câteva autorități publice - pe baza deciziei comune a conducătorilor autorităților publice interesate.

53. În componența Comisiei se includ:

- a) reprezentanții părților;
- b) angajații subdiviziunilor responsabile ale autorităților publice interesate;
- c) reprezentantul centrului de certificare;
- d) reprezentantul organului competent;
- e) alte persoane desemnate de părți.

54. Persoanele care se includ în componența Comisiei trebuie să posede cunoștințele necesare și experiență de lucru în domeniul aplicării semnăturii digitale și întocmirii de documente electronice, să dispună de dreptul de acces la materialele documentare și la mijloacele tehnice și de program necesare pentru desfășurarea activității Comisiei.

55. Comisia își desfășoară lucrările în conformitate cu regulamentul de soluționare a situațiilor litigioase în domeniul aplicării semnăturii digitale, aprobat de organul competent.

56. În sarcinile Comisiei intră examinarea, la nivel tehnico-organizațional, a împrejurărilor ce indică prezența situației de

conflict, stabilirea cauzelor și urmărilor acestei situații, determinarea măsurilor necesare pentru soluționarea ei.

57. În cazul în care situația litigioasă este considerată de către părți ca fiind soluționată, în termen de cel mult cinci zile lucrătoare după încheierea lucrărilor Comisiei se întocmește un act privind soluționarea situației litigioase, care se aprobă de către conducătorii autorităților publice interesate.

58. În cazul imposibilității de a soluționa situația litigioasă în regim de lucru sau după încheierea lucrărilor Comisiei, părțile se pot adresa în instanța de judecată.

VII. Responsabilități

59. Angajatul poartă răspundere personală pentru asigurarea confidențialității cheii sale private și pentru integritatea mijloacelor semnăturii digitale utilizate.

60. Angajatul poartă răspundere personală în aceeași măsură ca și în cazul aplicării semnăturii olografe.

61. Pentru neîndeplinirea sau îndeplinirea neconformă a obligațiilor stabilite de prezentul Regulament, angajații, colaboratorii subdiviziunii responsabile și centrul de certificare poartă răspundere în conformitate cu prevederile legislației în vigoare.

Hotărârile Guvernului

320/28.03.2006 Hotărîre pentru aprobarea Regulamentului privind ordinea de aplicare a semnăturii digitale în documentele electronice ale autorităților publice

Monitorul Oficial 51-54/350, 31.03.2006