Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr._____

din „__” _____ 2017

Chişinău

Pentru aprobarea Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcţionarii persoanelor juridice de drept public în cadrul circulaţiei electronice ale acestora

---

În scopul executării articolului 5 alineatul (4), al Legii nr. 91 din 29 mai 2014 privind semnătura electronică şi documentul electronic (Monitorul Oficial al Republicii Moldova, 2014, nr. 174-177, art. 397), Guvernul

HOTĂRĂŞTE:

1. Se aprobă Regulamentul privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcţionarii persoanelor juridice de drept public în cadrul circulaţiei electronice a acestora (se anexează).

2. Se pune în sarcina autorităţilor administraţiei publice centrale şi se recomandă autorităţilor administraţiei publice locale să creeze, în termen de trei luni, condiţiile necesare pentru aplicarea semnăturii electronice în conformitate cu Regulamentul aprobat.

3. Funcţionarii persoanelor juridice de drept public vor utiliza, în cadrul activităţii sale, certificatele cheilor publice emise de prestatorul de servicii de certificare din cadrul Întreprinderii de Stat „Centrul de telecomunicaţii speciale”.

4. Academia de Administrare Publică, în comun cu Întreprinderea de Stat „Centrul de telecomunicaţii speciale”, va organiza cursuri de instruire pentru angajaţii persoanelor juridice de drept public privind aplicarea semnăturii electronice.

5. Serviciile de certificare a cheilor publice şi alte servicii ce ţin de semnătura electronică vor fi prestate în conformitate cu prevederile capitolului III al Regulamentului cu privire la sistemele speciale de telecomunicaţii 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 şi completările ulterioare.

6. Întreprinderea de Stat „Centrul de telecomunicaţii speciale” va presta servicii de marcare temporală persoanelor juridice de drept public.

7. Se abrogă Hotărîrea Guvernului nr. 320 din 28.03.2006 „Pentru aprobarea Regulamentului privind ordinea de aplicare a semnăturii digitale în documentele electronice ale autorităţilor publice” (Monitorul Oficial al Republicii Moldova, 2006, nr.51-54, art. 350).

Prim-ministru **Pavel FILIP**

Contrasemnează:

Ministru al tehnologiei informaţiei şi comunicaţiilor **Vasile BOTNARI**

Aprobat
prin Hotărîrea Guvernului
nr_____din _____2017

Regulamentul
privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcţionarii persoanelor juridice de drept public în cadrul circulaţiei electronice a acestora

I. Dispoziţii generale

1. Prezentul Regulament determină condiţiile generale de aplicare a semnăturii electronice pe documentele electronice ale persoanelor juridice de drept public.

2. Persoana juridică de drept public recepţionează, pe bază de contract, serviciile de certificare a cheilor publice şi alte servicii ce ţin de semnătura electronică de la prestatorul de servicii de certificare a cheilor publice al autorităţilor administraţiei publice (*în continuare - prestatorul de servicii de certificare*) în conformitate cu regulamentul prestatorului de servicii de certificare şi efectuează schimbul de informaţii cu prestatorul de servicii de certificare prin intermediul Sistemului de telecomunicaţii al autorităţilor administraţiei publice.

3. Funcţionarii persoanelor juridice de drept public, la semnarea documentelor electronice în cadrul exercitării atribuţiilor de serviciu aplică semnătura electronică doar cu condiţia utilizării dispozitivelor de creare și/sau verificare a semnăturii electronice, produsului asociat semnăturii electronice ce dispun de avizul de conformitate, eliberat în conformitate cu procedura de avizare a dispozitivelor stabilită în Regulamentul privind avizarea dispozitivelor de creare şi/sau verificare a semnăturii electronice precum şi a produselor asociate semnăturii electronice, aprobat de Serviciul de Informaţii şi Securitate al Republicii Moldova, organul competent responsabil de elaborarea şi promovarea politicii de stat şi de exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice (*în continuare - organ competent*).

4. Responsabilitatea pentru organizarea aplicării semnăturii electronice pe documentele electronice ale persoanei juridice de drept public o poartă conducătorul acesteia.

II. Modalitatea de aplicare a semnăturii electronice

Secţiunea 1.
Condiţii generale la aplicarea semnăturii electronice

5. Aplicarea semnăturii electronice prevede:

1) crearea cheii publice şi a cheii private;
2) certificarea cheii publice la prestatorul de servicii de certificare;
3) semnarea documentului electronic, prin aplicarea semnăturii electronice;
4) verificarea autenticităţii semnăturii electronice aplicată pe documentul electronic.

6. Semnătura electronică se aplică pe documentele electronice ale persoanelor juridice de drept public de către persoana abilitată, în modul stabilit, să semneze cu semnătura olografă documentele echivalente pe suport de hîrtie (*în continuare - angajatul*).

7. Subdiviziunea tehnologii informaţionale din cadrul persoanei juridice de drept public, iar în cazul lipsei acesteia - subdiviziunea sau colaboratorul desemnat prin ordinul conducătorului acestei persoane juridice (*în continuare - subdiviziunea responsabilă*):

1) oferă consultaţii angajaţilor la crearea cheilor publice şi private pentru crearea semnăturii electronice avansate necalificate, la semnarea documentelor electronice şi la verificarea autenticităţii semnăturii electronice;

2) pregăteşte şi prezintă prestatorului de servicii de certificare informaţia necesară pentru crearea certificatelor cheilor publice ale angajaţilor, precum şi cererile de suspendare şi restabilire a valabilităţii, de revocare a certificatelor;

3) asigură accesul angajaţilor la registrele certificatelor cheilor publice, ţinute de prestatorul de servicii de certificare;

4) ţine evidenţa dispozitivelor (în mod electronic şi/sau pe suport de hîrtie), inclusiv celor securizate, de creare a semnăturii electronice şi a celor de verificare a acesteia, precum şi produsului asociat semnăturii electronice, utilizate în cadrul persoanei juridice de drept public;

5) asigură păstrarea documentelor pe baza cărora au fost create certificatele cheilor publice ale angajaţilor cu respectarea cadrului legal privind protecţia datelor cu caracter personal;

6) exercită controlul intern asupra utilizării şi păstrării dispozitivelor de creare şi/sau de verificare a semnăturii electronice de către angajaţi, în conformitate cu cerinţele stabilite.

Secţiunea 2-a.
Crearea cheii publice şi a cheii private

8. Cheia privată şi cheia publică utilizate la crearea semnăturii electronice avansate necalificate se creează de către subdiviziunea responsabilă, nemijlocit în persoana juridică de drept public sau de către personalul prestatorului de servicii de certificare în sediul acestuia, fără a se încălca confidenţialitatea cheii private.

9. Cheia privată şi cheia publică utilizate la crearea semnăturii electronice avansate calificate se creează de către prestatorul de servicii de certificare prin intermediul dispozitivului securizat de creare a semnăturii.

Secţiunea a 3-a.
Certificarea cheii publice la prestatorul de servicii de certificare

10. Angajatul semnează electronic documentele prin aplicarea semnăturii electronice, după primirea certificatului cheii publice de la prestatorul de servicii de certificare.

11. Conducătorul persoanei juridice de drept public sau o altă persoană desemnată de conducător, remite prestatorului de servicii de certificare lista angajaţilor ale căror chei publice urmează a fi certificate, indicîndu-se numele,

prenumele şi IDNP-ul acestor persoane, funcţiile pe care le deţin, datele referitoare la subdiviziunea responsabilă.

12. În temeiul listei menţionate la punctul 13 al prezentului Regulament, prestatorul de servicii de certificare recepţionează cererile de certificare a cheilor publice în formă electronică semnată cu semnătură electronică şi/sau în formă de document pe suport de hîrtie, semnat cu semnătura olografă a solicitantului.

13. Cererea de certificare a cheilor publice, întocmită de angajat, trebuie să conţină:

1) denumirea persoanei juridice de drept public şi codul ei de identificare IDNO;

2) numele şi prenumele angajatului, numărul de identificare al persoanei fizice IDNP, funcţia pe care o deţine;

3) informaţia necesară pentru comunicarea cu angajatul (numerele de telefon, fax, adresa poştei electronice);

4) cheia publică pentru care se solicită certificatul, după caz;

5) alte date stabilite de organul competent.

14. În conformitate cu lista prezentată de conducătorul persoanei juridice de drept public şi în temeiul cererii recepţionate de la angajat, prestatorul de servicii de certificare, în termen de trei zile lucrătoare de la data înregistrării cererii, adoptă decizia de certificare a cheii publice.

15. Pe baza deciziei de certificare a cheii publice, prestatorul de servicii de certificare creează şi eliberează certificatul respectiv al cheii publice.

16. Examinarea cererilor de certificare a cheilor publice, adoptarea deciziilor de certificare a cheilor publice şi crearea certificatelor cheilor publice sau privind refuzul de certificare a cheii publice se efectuează în conformitate cu procedura stabilită în regulamentul prestatorului de servicii de certificare.

17. Certificatul cheii publice trebuie să conţină:

1) numărul unic de înregistrare al certificatului cheii publice;

2) datele de identificare ale prestatorului de servicii de certificare;

3) denumirea persoanei juridice de drept public şi codul ei de identificare IDNO;

4) numele şi prenumele angajatului, numărul de identificare al persoanei fizice IDNP, funcţia pe care o deţine;

5) informaţia necesară pentru comunicarea cu angajatul (numerele de telefon, fax, adresa poştei electronice);

6) cheia publică a angajatului;

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

8) datele despre algoritmul criptografic al semnăturii electronice şi alte date tehnologice determinate de prestatorul de servicii de certificare;

9) restricţiile privind utilizarea certificatului cheii publice şi/sau limitele valorii operaţiunilor în care acesta poate fi utilizat, dacă acestea se aplică;

10) semnătura electronică a prestatorului de servicii de certificare;

11) alte date, în conformitate cu standardele şi cerinţele tehnice stabilite de organul competent.

18. Certificatul calificat al cheii publice trebuie să conţină, suplimentar:

1) menţiunea care să indice că certificatul este eliberat ca certificat calificat al cheii publice;

2) informaţia, atunci cînd este cazul, privind o calitate specială a angajatului, în funcţie de utilizarea pe care urmează să o aibă certificatul;

3) datele de verificare a semnăturii electronice care corespund datelor de creare a semnăturii electronice controlate de angajat.

19. La cererea conducătorului persoanei juridice de drept public, prestatorul de servicii de certificare poate indica în certificatele cheilor publice ale angajaţilor şi alte informaţii decît cele specificate la punctul 17 al prezentului Regulament, în condiţiile legislaţiei.

20. Angajatul este obligat să înştiinţeze la timp subdiviziunea responsabilă şi prestatorul de servicii de certificare despre orice modificare a informaţiilor cuprinse în certificatul cheii publice.

21. Certificatul cheii publice se revocă:

1) la cererea titularului certificatului cheii publice sau persoanei juridice de drept public în care acesta activează;

2) la depistarea unor informaţii neveridice în cererea de certificare a cheii publice sau în certificatul cheii publice;

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

4) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice şi în lipsa unei cereri din partea titularului certificatului cheii publice sau persoanei juridice de drept public în care acesta activează privind restabilirea valabilităţii acestuia;

5) la modificarea certificatului cheii publice;

6) în cazul decesului titularului certificatului cheii publice sau la recunoaşterea lui ca fiind incapabil;

7) la solicitarea organului competent, în cazul încălcării prevederilor Legii nr. 91 din 29 mai 2014 privind semnătura electronică și documentul electronic.

22. Suspendarea, restabilirea valabilităţii şi revocarea certificatelor cheilor publice ale angajaţilor se efectuează în conformitate cu procedurile stabilite de organul competent.

23. Prestatorul de servicii de certificare determină modalitatea legăturii de urgenţă cu titularul certificatului cheii publice şi subdiviziunea responsabilă în caz de compromitere a cheii private.

24. Modul de creare a cheilor publice şi private ale angajaţilor este stabilit de normele tehnice aprobate de organul competent.

25. În caz de concediere a angajatului, cheia privată ce aparţine acestei persoane se nimiceşte printr-o metodă ce nu admite posibilitatea restabilirii ei, iar certificatul cheii publice, corespunzător, se revocă.

Secţiunea a 4-a.

Aplicarea semnăturii electronice pe documentul electronic

26. Documentele electronice se semnează de către angajat cu ajutorul dispozitivului de creare a semnăturii electronice, utilizînd datele de creare a semnăturii electronice.

27. În timpul îndeplinirii atribuţiilor funcţionale, angajatul utilizează cheia sa privată creată în acest scop. Se interzice utilizarea cheii private în scopuri ce nu ţin de îndeplinirea atribuţiilor funcţionale.

28. Subdiviziunea responsabilă asigură accesul angajaţilor la informaţia actualizată privind certificatele cheilor publice valabile, suspendate şi revocate sau în alt mod asigură posibilitatea verificării valabilităţii certificatelor cheilor publice eliberate de prestatorul de servicii de certificare, inclusiv prin distribuirea către angajaţi a listei actualizate a certificatelor cheilor publice revocate, furnizată de prestatorul de servicii de certificare.

Secţiunea a 5-a.

Verificarea autenticităţii semnăturii electronice

29. Verificarea autenticităţii semnăturilor electronice pe documentele electronice se efectuează de către persoana care verifică autenticitatea documentului electronic cu utilizarea dispozitivului de verificare a semnăturii electronice și/sau al produsului asociat semnăturii electronice, cu utilizarea datelor de verificare a semnăturii electronice.

30. Persoanele juridice de drept public utilizează, în sisteme informaționale proprii, serviciul de sursă unică de sincronizare cu Timpul Mondial Coordonat (UTC) oferit de prestatorul de servicii de certificare.

III. Obligațiile și drepturile angajatului

31. Angajatul are obligaţia:

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

2) să utilizeze dispozitivele (dispozitivele securizate în cazul utilizării semnăturii electronice avansate calificate) de creare și/sau verificare a semnăturii electronice, produsul asociat semnăturii electronice în conformitate cu documentaţia de exploatare şi regimul de utilizare a acestora, stabilit de persoana juridică de drept public;

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

4) să nu primească spre executare documentele electronice semnate cu semnătură electronică dacă:

a) 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;

b) nu este confirmată autenticitatea semnăturii electronice în documentul electronic;

c) semnătura electronică se utilizează cu încălcarea sferei de aplicare sau cu depăşirea limitelor valorice pentru care este valabilă în documentele electronice de plată sau de încheiere a tranzacţiilor;

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

a) a pierdut cheia privată;

b) are motive să presupună că a fost încălcată confidenţialitatea cheii private;

c) informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;

6) la soluţionarea situaţiilor litigioase ce ţin de stabilirea autenticităţii şi/sau a autorului documentului contestabil, să ofere informaţiile necesare;

7) să îndeplinească alte obligaţii stabilite de legislaţia în vigoare.

32. Angajatul are dreptul:

1) să semneze şi să verifice semnătura electronică aplicată pe documentele electronice;

2) în cazul apariţiei situaţiei litigioase ce ţine de stabilirea autenticităţii şi/sau a autorului documentului contestabil, să solicite soluţionarea ei în modul stabilit de legislaţie;

3) să primească consultaţii cu privire la aplicarea semnăturii electronice şi verificarea autenticităţii documentului electronic de la personalul subdiviziunii responsabile şi al prestatorului de servicii de certificare.

IV. Asigurarea securităţii

33. Evidenţa dispozitivelor (dispozitivelor securizate în cazul utilizării semnăturii electronice avansate calificate) de creare a semnăturilor electronice este ţinută de subdiviziunea responsabilă pe exemplare, în conformitate cu prevederile legislaţiei în domeniu, ordinea interioară de aplicare a semnăturii electronice pe documentele electronice ale persoanelor juridice de drept public.

34. Păstrarea dispozitivelor de creare a semnăturilor electronice se efectuează în condiţii care să excludă pierderea şi utilizarea lor neautorizată.

35. La transportarea dispozitivelor (dispozitivelor securizate în cazul utilizării semnăturii electronice avansate calificate) de creare a semnăturilor electronice se asigură protecţia lor contra deteriorării fizice şi influenţei din exterior.

36. Cheia privată ce se utilizează pentru crearea semnăturii electronice avansate necalificate se păstrează cu asigurarea condiţiilor în care compromiterea cheii nu este posibilă.

37. Dispozitivele (dispozitivele securizate în cazul utilizării semnăturii electronice avansate calificate) de creare și/sau verificare a semnăturii electronice, produsul asociat semnăturii electronice utilizate în persoana juridică de drept public sînt supuse evidenţei şi controlului integrităţii de către subdiviziunea responsabilă. Se interzice utilizarea dispozitivelor (dispozitivelor securizate în cazul utilizării semnăturii electronice avansate calificate) de creare și/sau verificare a semnăturii electronice în cazul încălcării integrităţii lor.

38. Regimul de utilizare a dispozitivelor (dispozitivelor securizate în cazul utilizării semnăturii electronice avansate calificate) de creare și/sau verificare a semnăturii electronice, a produsului asociat semnăturii electronice în persoana juridică de drept public trebuie să excludă posibilitatea accesului persoanelor terţe la aceste mijloace, modificării şi utilizării lor neautorizate.

V. Acţiunile în caz de compromitere a cheii private

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

1) pierderea dispozitivului (dispozitivului securizat în cazul utilizării semnăturii electronice avansate calificate) de creare a semnăturii electronice, indiferent de faptul dacă a fost sau nu găsit ulterior;

2) apariţia suspiciunilor privind dezvăluirea informaţiei sau denaturarea ei în sistemul de legătură sau la locurile de utilizare a dispozitivelor (dispozitivelor securizate în cazul utilizării semnăturii electronice avansate calificate) de creare şi/sau verificare a semnăturii electronice, a produsului asociat semnăturii electronice;

3) încălcarea integrităţii ştampilei la locul de păstrare a dispozitivelor (dispozitivelor securizate în cazul utilizării semnăturii electronice avansate calificate) de creare a semnăturii electronice;

4) pierderea cheii de la locul de păstrare în momentul aflării în acesta a dispozitivelor (dispozitivelor securizate în cazul utilizării semnăturii electronice avansate calificate) de creare a semnăturii electronice, indiferent de faptul dacă a fost sau nu găsită ulterior cheia;

5) accesul persoanelor terţe la cheia privată sau la dispozitivele (dispozitivele securizate în cazul utilizării semnăturii electronice avansate calificate) de creare şi/sau verificare a semnăturii electronice, la produsul asociat semnăturii electronice;

6) alte evenimente care dau temei de a presupune că a fost încălcată confidenţialitatea cheii private.

40. În cazul apariţiei unei împrejurări legate de compromiterea cheii private, titularul ei şi/sau subdiviziunea responsabilă au obligaţia să informeze imediat, în modul stabilit, prestatorul de servicii de certificare despre compromiterea cheii private.

41. Prestatorul de servicii de certificare, primind informaţia cu privire la compromiterea cheii private a angajatului, trebuie să se convingă, în modul stabilit, de autenticitatea acesteia şi imediat, dar nu mai tîrziu de trei ore de lucru, să suspende valabilitatea sau să revoce certificatul cheii publice respective.

42. Valabilitatea certificatului cheii publice se suspendă în cazurile prevăzute de prezentul Regulament pe un termen stabilit de organul competent, de pînă la 30 de zile. În cazul în care la expirarea termenului de suspendare a valabilităţii certificatului cheii publice nu parvine cererea de restabilire a valabilităţii certificatului, certificatul cheii publice se revocă.

43. După suspendarea valabilităţii sau revocarea certificatului cheii publice, prestatorul de servicii de certificare anunţă în scris, în modul stabilit, subdiviziunea responsabilă despre acest fapt.

44. Referitor la faptul compromiterii cheii private se desfăşoară o investigaţie de serviciu, la încheierea căreia, potrivit deciziei comisiei, cheia privată care a fost compromisă se nimiceşte.

45. Crearea cheilor publice şi private noi se face după investigarea şi înlăturarea cauzelor de compromitere a cheii private anterioare.

VI. Ordinea de soluţionare a situaţiilor litigioase în domeniul aplicării semnăturii electronice

46. Situaţiile litigioase se soluţionează în conformitate cu prevederile Regulamentului de soluționare a situațiilor litigioase în domeniul semnăturii electronice.

47. Regulamentul de soluționare a situațiilor litigioase în domeniul semnăturii electronice se aprobă de organul competent.

VII. Responsabilităţi

48. Angajatul poartă răspundere personală pentru asigurarea confidenţialităţii cheii sale private şi pentru integritatea dispozitivelor utilizate.

49. La semnarea documentelor electronice în cadrul exercitării atribuţiilor de serviciu, angajatul persoanei juridice de drept public poartă răspundere identică cu cea stabilită pentru cazurile de semnare cu semnătura olografă a documentelor pe suport de hîrtie.

50. Pentru neîndeplinirea sau îndeplinirea neconformă a obligaţiilor stabilite de prezentul Regulament, angajaţii, colaboratorii subdiviziunii responsabile şi prestatorul de servicii de certificare poartă răspundere în conformitate cu prevederile legislaţiei în vigoare.