Aprobat:
Serviciul de Informaţii şi Securitate
al Republicii Moldova
ordinul nr. 13 din 3 aprilie 2006

_____ Ion URSU

Înregistrat:
Ministerul Justiţiei
al Republicii Moldova
nr. de înregistrare 452 din 21 iunie 2006

_____ Victoria IFTODI

Anexa nr. 2
la Ordinul directorului Serviciului
de Informaţii şi Securitate
al Republicii Moldova
nr. 13 din 3 aprilie 2006

Condiţiile speciale de activitate a centrelor de certificare a cheilor publice

I. Noţiuni generale

1. Condiţiile speciale de activitate a centrelor de certificare a cheilor publice (în continuare – condiţii speciale) sînt elaborate în conformitate cu Legea nr. 264-XV din 15 iulie 2004 cu privire la documentul electronic şi semnătura digitală şi Hotărîrea Guvernului nr. 945 din 5 septembrie 2005 "Cu privire la centrele de certificare a cheilor publice".

2. Condiţiile speciale stabilesc cerinţele generale faţă de centrele de certificare şi infrastructura acestora, organizarea procedurilor de bază ale centrelor de certificare, faţă de sistemul de gestionare a securităţii informaţionale, precum şi măsuri specifice în procedura de înregistrare, organizare şi control al activităţii centrelor de certificare.

3. Condiţiile speciale reprezintă un document de reglementare în domeniul semnăturii digitale şi este obligatoriu pentru toate persoanele juridice care prestează servicii de certificare a cheilor publice şi alte servicii ce ţin de semnătura digitală.

4. În sensul prezentului document se definesc următoarele noţiuni:

utilizatorul semnăturii digitale – persoana fizică sau juridică, precum şi dispozitivul sau aplicaţia care utilizează serviciile centrului de certificare;

identificarea – atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

autentificarea – verificarea apartenenţei identificatorului atribuit subiectului de acces, confirmarea autenticităţii;

integritatea – certitudinea, necontradictorialitatea şi actualitatea informaţiei, protecţia ei de distrugere şi modificare neautorizată;

accesibilitatea – posibilitatea de a obţine informaţia solicitată sau a accesa serviciul de informare într-o perioadă satisfăcătoare de timp;

confidenţialitatea – protejarea informaţiei contra divulgării neautorizate;

mijloacele de protecţie criptografică a informaţiei (MPCI) – mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei, destinate să asigure integritatea şi confidenţialitatea informaţiei în procesul de prelucrare, depozitare şi transmitere a acesteia prin canalele de comunicaţii;

lista certificatelor revocate – lista certificatelor cheilor publice a căror valabilitate a fost suspendată sau a încetat înainte de expirarea termenului de valabilitate, întocmită de centrul de certificare;

protecția tehnică şi criptografica a informației – protecția informației cu aplicarea metodelor matematice (criptografice) speciale, a mijloacelor de program, tehnice, tehnico-aplicative sau de alt gen, precum şi a procedurilor tehnico-organizatorice;

protecția informației de scurgeri – ansamblu de măsuri îndreptate spre prevenirea răspîndirii neautorizate a informației protejate prin canalele tehnice sau prin canalele secundare cu ajutorul mijloacelor tehnice speciale;

protecția informației contra accesului neautorizat – ansamblu de măsuri orientate spre prevenirea obținerii informației protejate de către subiectul interesat, cu încălcarea drepturilor sau regulilor de acces la informația protejată stabilite de actele juridice sau de proprietarul (deținătorul) informației;

protecția informației contra acțiunilor neintenționate – ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care duc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum şi la pierderea, distrugerea acesteia sau la defectarea suportului material al informației;

politica de securitate – totalitatea deciziilor documentate de administrare, îndreptate spre protejarea informației, a mijloacelor tehnice şi de program ale sistemelor informaționale.

II. Serviciile şi procedurile centrului de certificare

5. Centrul de certificare prestează servicii obligatorii şi neobligatorii în domeniul semnăturii digitale.

6. Serviciul de certificare a cheilor publice ale persoanelor fizice este un serviciu obligatoriu.

7. Centrul de certificare poate presta următoarele servicii neobligatorii:

a) certificarea cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al treilea (numai pentru centrele de certificare de nivelul al doilea);

b) certificarea cheilor publice ale serviciilor prestate în sfera informațională [servicii informaționale e-mail, VPN (Virtual Private Network), web etc.];

c) fixarea timpului de inițiere a evenimentelor, inclusiv fixarea timpului de semnare a documentului electronic;

d) alte servicii în domeniul semnăturii digitale.

8. În procesul prestării serviciilor de certificare a cheilor publice ale persoanelor fizice, centrul de certificare trebuie să asigure realizarea următoarelor proceduri:

a) înregistrarea persoanei fizice;

b) crearea (emiterea) certificatului cheii publice a persoanei fizice;

c) suspendarea valabilității certificatului cheii publice a persoanei fizice;

d) restabilirea valabilității certificatului cheii publice a persoanei fizice;

e) revocarea certificatului cheii publice a persoanei fizice;

f) publicarea certificatelor cheilor publice;

g) distribuirea informației privind certificatele suspendate şi revocate (listelor certificatelor revocate).

9. Centrul de certificare asigură procesul de administrare (gestionare) a certificatelor cheilor publice prin realizarea complexă a procedurilor specificate.

III. Cerințele generale referitoare la centrul de certificare

10. Obiectele utilizate de către centrul de certificare trebuie să aparțină acestuia cu titlu de proprietate, arendă, administrare sau folosință.

11. Centrul de certificare trebuie să utilizeze mijloace de semnătură digitală care posedă certificat de conformitate, eliberat conform prevederilor legislației în vigoare.

12. Organizarea regimului intern de activitate al centrului de certificare trebuie să excludă posibilitatea accesului fizic neautorizat la mijloacele semnăturii digitale, utilizarea sau modificarea neautorizată a acestora.

13. Centrul de certificare trebuie să creeze condițiile necesare pentru asigurarea securității cheilor publice şi private ale persoanelor împuternicite ale centrului de certificare şi a registrului certificatelor cheilor publice.

14. Centrul de certificare trebuie să asigure utilizarea cheii private a persoanei împuternicite a centrului de certificare numai pentru semnarea certificatelor cheilor publice şi a listelor certificatelor revocate emise de către centrul de certificare.

15. Centrul de certificare trebuie să excludă posibilitatea de utilizare a cheii private a persoanei împuternicite a centrului de certificare dacă are motive să presupună că a fost încălcată confidențialitatea respectivei chei private.

16. Centrul de certificare trebuie să elaboreze şi să aprobe politica de certificare, care să includă un set de reguli ce stabilesc utilizarea certificatului emis de centrul de certificare conform cerințelor de securitate stabilite.

17. Centrul de certificare trebuie să elaboreze şi aprobe Regulamentul centrului de certificare, care să stabilească condițiile organizatorice, tehnice şi de alt nivel ale activității centrului de certificare în procesul de prestare a serviciilor de certificare a cheilor publice.

18. Regulamentul centrului de certificare trebuie să conțină:

a) lista serviciilor prestate de centrul de certificare şi modalitatea de prestare a acestora;

b) funcțiile, obligațiile şi drepturile centrului de certificare;

c) drepturile şi obligațiile utilizatorilor semnăturii digitale;

d) obligațiile financiare ale centrului de certificare;

e) responsabilitățile părților;

f) activitățile tehnico-organizatorice de bază de asigurare a securității centrului de certificare, inclusiv politica de confidențialitate;

g) procedurile centrului de certificare;

h) ordinea de publicare şi distribuire a informației;

i) modalitatea de accesare a resurselor informaționale ale centrului de certificare;

j) modul de arhivare a informației documentate;

k) procedurile de gestionare a cheilor persoanelor împuternicite ale centrului de certificare;

l) algoritmul acțiunilor în cazul compromiterii cheii private a persoanei împuternicite a centrului de certificare şi a utilizatorului semnăturii digitale;

m) descrierea formatelor de date aprobate de către centrul de certificare;

n) structura certificatului cheii publice a persoanei împuternicite a centrului de certificare;

o) structura certificatelor cheilor publice ale utilizatorilor semnăturii digitale;

p) structura listei certificatelor revocate;

q) ordinea de sincronizare a timpului;

r) modalitatea de soluționare a situațiilor litigioase în domeniul aplicării semnăturii digitale;

s) ordinea de înștiințare a utilizatorilor semnăturii digitale privind politica de certificare şi despre conținutul Regulamentului centrului de certificare.

19. Politica de certificare şi Regulamentul centrului de certificare trebuie să corespundă recomandărilor IETF (Internet Engineering Task Force) RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

20. Centrul de certificare trebuie să excludă posibilitatea divulgării informației de înregistrare a utilizatorilor semnăturii digitale cu excepția informației ce se utilizează pentru identificarea certificatelor cheilor publice ale acestora şi care este publicată prin includerea acesteia în certificatele utilizatorilor semnăturii digitale.

21. Regimul de confidențialitate în cazul operării cu informația încredințată sau care a devenit cunoscută centrului de certificare în activitatea sa trebuie să asigure:

a) limitarea numărului persoanelor cu funcții de răspundere cu drept de acces la informația confidențială;

b) ordinea de admitere controlată a persoanelor cu funcții de răspundere la realizarea activităților legate de informația confidențială;

c) delimitarea funcțională a responsabilităților persoanelor cu funcții de răspundere;

d) identificarea şi autentificarea utilizatorilor semnăturii digitale cu utilizarea mijloacelor moderne de autentificare şi a protocoalelor criptografice;

e) delimitarea accesului subiecților la diferite obiecte şi/sau la funcțiile speciale ale centrului de certificare pe baza identificării subiecților şi a delimitării funcționale a acestora;

f) securitatea păstrării, prelucrării şi transmisiei informației confidențiale prin intermediul canalelor de comunicații.

22. Centrul de certificare trebuie sa asigure administrarea accesului subiecților la diferite obiecte şi/sau la funcțiile speciale ale centrului de certificare pe baza identificării subiecților şi a delimitării funcționale a acestora.

23. Centrul de certificare trebuie să asigure copierea de rezervă, păstrarea şi restabilirea informaţiei critice pentru activitatea sa, precum şi instalarea în caz de necesitate a resurselor tehnice suplimentare sau de rezervă.

24. Centrul de certificare trebuie să dispună de personal calificat suficient pentru funcţionarea şi asigurarea securităţii centrului de certificare.

25. Centrul de certificare trebuie să-şi realizeze funcţiile pe baza principiului delimitării privilegiilor (responsabilităţilor) persoanelor cu funcţii de răspundere: administratorul înregistrări, administratorul certificare, administratorul securitate şi administratorul sistem.

26. Administratorul înregistrări este responsabil de corectitudinea (autenticitatea) informaţiei de completare a certificatului cheii publice şi înregistrarea titularilor certificatelor cheilor publice în procesul creării, suspendării sau restabilirii valabilităţii şi revocării certificatelor cheilor publice.

27. Administratorul certificare (persoana împuternicită a centrului de certificare) este responsabil pentru crearea, suspendarea sau restabilirea valabilităţii şi revocarea certificatelor cheilor publice, ţinerea registrului certificatelor cheilor publice, păstrarea şi utilizarea în siguranţă a cheii sale private.

28. Administratorul securitate este responsabil de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei, precum şi de elaborarea şi implementarea politicii de securitate a centrului de certificare.

29. Administratorul sistem este responsabil de administrarea, funcţionarea corespunzătoare şi asigurarea securităţii complexului tehnic de program al centrului de certificare.

30. În caz de necesitate în centrul de certificare pot fi înfiinţate funcţii suplimentare, în special de operatori.

31. Operatorii realizează activităţi de deservire zilnică a complexului tehnic de program al centrului de certificare (copierea şi restabilirea sistemului, gestionarea arhivelor, introducerea informaţiei etc.).

32. Centrul de certificare trebuie să excludă cumularea funcţiilor de administrator înregistrări, administrator certificare, administrator securitate, administrator sistem şi operator.

33. Centrul de certificare trebuie să sincronizeze activitatea serviciilor sale, inclusiv a mijloacelor tehnice şi de program conform destinaţiei, cu Timpul Universal Coordonat (UTC). Se recomandă utilizarea a două surse independente UTC. Este permisă sincronizarea cu Greenwich Mean Time – GMT.

IV. Cerinţele referitoare la procedurile de bază ale centrului de certificare

Secţiunea 1. Cerinţele faţă de procedura de înregistrare a persoanei fizice

34. Persoanele fizice sînt înregistrate de către administratorul înregistrări, care administrează datele titularului certificatului cheii publice.

35. Administratorul înregistrări efectuează identificarea persoanei fizice ce a înaintat cererea de certificare a cheii sale publice în conformitate cu procedurile aprobate de către centrul de certificare.

36. Administratorul înregistrări trebuie să stabilească:

a) corespunderea procesului de completare şi înaintare a cererii cu prevederile Legii cu privire la documentul electronic şi semnătura digitală, ale Regulamentului centrului de certificare şi ale altor documente normative în domeniul semnăturii digitale;

b) autenticitatea şi valabilitatea informației prezentate în cerere;

c) corespunderea informației prezentate în cererea sub formă de document electronic şi a celei din cererea sub formă de document pe suport de hîrtie;

d) respectarea drepturilor persoanelor terțe.

37. Administratorul înregistrări trebuie să se asigure că persoana fizică ce a prezentat cererea de certificare a cheii publice este posesorul cheii private corespunzătoare.

38. Documentele electronice ale administratorului înregistrări trebuie să fie semnate cu semnătură digitală, să includă amprenta timpului, care stabileşte momentul creării documentului electronic, şi să fie transmise utilizînd sistemele ce asigură confidențialitatea mesajelor.

39. Centrul de certificare trebuie sa asigure protecția informației confidențiale a titularilor certificatelor cheilor publice.

Secțiunea a 2-a. Cerințele față de procedura de certificare a cheii publice

40. Centrul de certificare creează şi emite certificate ale cheilor publice în conformitate cu procedurile aprobate de centrul de certificare.

41. Centrul de certificare trebuie să elaboreze şi să aprobe politica şi procedurile de certificare a cheilor publice în conformitate cu normele tehnice stabilite în domeniul semnăturii digitale.

42. Certificatul cheii publice a persoanei fizice este creat de către administratorul certificare (persoana împuternicită a centrului de certificare).

43. Administratorul certificare trebuie să verifice integritatea şi autenticitatea datelor transmise de către administratorul înregistrări, precum şi corespunderea acestora cu standardul certificatelor cheilor publice stabilit.

44. Centrul trebuie să asigure autenticitatea informației care se conține în certificatul cheii publice, precum şi integritatea certificatului.

45. Certificatul cheii publice trebuie să corespundă profilurilor aprobate în centrul de certificare, corespunzătoare politicii de certificare.

46. Centrul de certificare trebuie să înscrie certificatul cheii publice în registrul certificatelor nu mai tîrziu de data şi ora începerii termenului de valabilitate a certificatului.

47. Cheia privată a administratorului certificare trebuie să fie utilizată numai pentru semnarea certificatelor cheilor publice şi a listelor certificatelor revocate (CRL) emise de acesta.

Secțiunea a 3-a. Cerințele față de procedurile de suspendare şi restabilire a valabilității şi de revocare a certificatului cheii publice

48. Centrul de certificare suspendă, restabileşte valabilitatea sau revocă certificatul cheii publice în cazurile stabilite de actele normative în domeniul semnăturii digitale.

49. Centrul de certificare trebuie să elaboreze şi să aprobe procedurile de suspendare, restabilire a valabilității şi revocare a certificatelor cheii publice în conformitate cu normele tehnice stabilite din domeniul semnăturii digitale.

50. Centrul de certificare trebuie să elaboreze şi să aprobe proceduri sigure de autentificare a persoanei ce a declarat intenția de a suspenda, restabili valabilitatea sau de a revoca certificatul său al cheii publice, precum şi proceduri de confirmare a valabilității cererii de suspendare, restabilire a valabilității sau revocare a certificatului cheii publice.

51. Centrul de certificare suspendă imediat valabilitatea certificatului cheii publice dacă are motive să presupună că a fost încălcată confidențialitatea cheii private a titularului certificatului sau informația înscrisă în certificatul cheii publice nu corespunde realității.

52. Centrul de certificare revocă certificatul cheii publice în cazul stabilirii încălcării confidențialității cheii private a titularului certificatului sau a neveridicității datelor incluse în certificatul cheii publice.

53. Suspendarea, restabilirea valabilității şi revocarea certificatului cheii publice se efectuează de către administratorul certificare sub supravegherea obligatorie a administratorului securitate sau a altei persoane cu funcții de răspundere, numită de conducătorul centrului de certificare.

54. Centrul de certificare trebuie să înscrie datele despre certificatul suspendat sau revocat în lista certificatelor revocate în decursul a 3 ore de lucru, indicînd data şi timpul includerii, cauza suspendării sau revocării acestuia.

55. Centrul de certificare trebuie să excludă posibilitatea restabilirii valabilității certificatului cheii publice revocat.

56. Certificatul cheii publice a cărui valabilitate a fost restabilită se exclude din lista certificatelor revocate în maxim 3 ore de lucru.

57. Centrul de certificare trebuie să asigure o procedură de emitere la timp a listei reînnoite a certificatelor revocate.

58. Centrul de certificare trebuie să elaboreze şi să aprobe procedura de informare a titularului certificatului cheii publice despre suspendarea, restabilirea valabilității sau revocarea certificatului.

Secțiunea a 4-a. Cerințele față de procedurile de publicare a certificatelor cheilor publice şi distribuire a informației referitoare la certificatele cheilor publice suspendate sau revocate

59. Distribuirea (publicarea) certificatelor cheilor publice se efectuează în conformitate cu procedurile stabilite de centrul de certificare, iar accesul persoanelor terțe poate fi limitat dacă acest fapt este solicitat de titularul certificatului.

60. Centrul de certificare trebuie să elaboreze şi să aprobe politica de control al accesului la certificatele cheilor publice emise de centrul de certificare.

61. Accesul la certificatele cheilor publice trebuie să fie acordat numai persoanelor ce au acest drept, conform regulilor stabilite de politica de securitate a centrului de certificare sau de către titularii certificatelor.

62. Centrul de certificare trebuie să ofere oricărei persoane informația referitoare la statutul certificatelor cheilor publice.

63. Centrul de certificare trebuie să prezinte informația referitoare la statutul certificatelor cheilor publice în regim de timp real (on-line), precum şi pe alte căi stabilite de centrul de certificare, inclusiv prin distribuirea listelor certificatelor revocate pentru abonați (off-line).

64. Centrul de certificare trebuie să asigure integritatea şi autenticitatea mesajelor în procesul de verificare a statutului certificatelor cheilor publice. Toate răspunsurile referitoare la starea certificatelor trebuie semnate cu semnătura digitală a persoanei împuternicite a centrului de certificare.

65. Centrul de certificare poate cere ca persoanele terțe să semneze cu semnătura digitală solicitările referitoare la statutul certificatelor cheilor publice.

66. Centrul de certificare poate răspunde solicitărilor referitoare la statutul certificatului cheii publice utilizînd datele reînnoite în timpul ultimei înştiințări a utilizatorilor.

67. Centrul de certificare trebuie să facă publice certificatele cheilor publice ale persoanelor împuternicite ale centrului.

68. Informația inclusă în registrul certificatelor cheilor publice trebuie să fie protejată contra accesului neautorizat, modificării sau distrugerii.

69. Centrul de certificare trebuie să stabilească modalitățile de acces cu drept de înregistrare sau modificare a registrului certificatelor cheilor publice pentru persoanele ce au acest drept conform obligațiilor sale de serviciu.

70. Centrul de certificare trebuie să utilizeze mecanisme de autentificare a subiecților, care au acces la informația corespunzătoare din registrul certificatelor cheilor publice.

V. Cerințele referitoare la infrastructura centrului de certificare

Secțiunea 1. Cerințele referitoare la încăperi

71. Încăperile centrului de certificare trebuie să asigure funcționarea stabilă a complexului tehnic de program, a sistemelor de telecomunicații şi a altor componente tehnice, a sistemelor de energie electrică, termică şi de apeduct, de aer condiționat, antiincendiare, să asigure protecția personalului şi să contribuie la prevenirea sustragerii, pierderii, modificării neautorizate a datelor, precum şi a distrugerii acestora sau a mijloacelor tehnico-aplicative.

72. Încăperile centrului de certificare trebuie să corespundă cerințelor normelor de igienă, securitate a muncii şi protecție a mediului înconjurător, stabilite de legislația în vigoare.

73. Încăperile centrului de certificare trebuie să fie amplasate în perimetrul de securitate (perimetru unde are drept de acces numai personalul organizației a cărei parte este centrul de certificare) şi să fie echipate corespunzător cu cerințele de asigurare a securității.

74. Din categoria încăperilor cu regim special (în continuare – încăperi speciale) ale centrului de certificare fac parte încăperile unde se instalează mijloacele tehnice de bază ale complexului tehnic de program (încăperi pentru servere), unde se păstrează suporturile materiale ce conțin: copiile de rezervă ale registrului certificatelor cheilor publice, copiile de rezervă ale resurselor de sistem şi de program, cheile private ale angajaților centrului de certificare sau cheile secrete ale altor sisteme criptografice ale centrului de certificare.

75. Încăperile speciale ale centrului de certificare trebuie:

a) să corespundă condițiilor de maximă securitate, stabilite de prezentele condiții speciale, pentru asigurarea securității fizice şi protecției tehnice a informației;

b) să fie dotate cu mijloace autonome şi sisteme automate de semnalizare antiincendiu, stingere a incendiului şi înlăturare a fumului conform normativelor NCM.E.03.03-2003 "Dotarea clădirilor şi instalațiilor cu sisteme autonome de semnalizare şi stingere a incendiilor" şi NCM.E.03.05-2004 "Instalații autonome de stingere şi semnalizare a incendiilor. Normativ pentru proiectare";

c) să corespundă cerințelor în vigoare în Republica Moldova privind proiectarea şi exploatarea rețelei electrice, conform normelor cuprinse în Regulile de instalare a dispozitivelor electrice, Regulile privind exploatarea tehnică a dispozitivelor electrice ale consumatorilor şi Regulile privind tehnici de securitate la exploatarea dispozitivelor electrice ale consumatorilor;

d) să asigure funcționarea mijloacelor tehnice principale pentru o perioada de cel puțin 30 minute din momentul stopării furnizării energiei electrice de la sursa de bază;

e) să fie echipate cu mijloace de ventilare şi condiționare a aerului care posedă certificat de conformitate, eliberat conform prevederilor legislației în vigoare.

76. În încăperile destinate pentru păstrarea documentației şi a copiilor de rezervă ale registrului certificatelor cheilor publice trebuie să fie instalate dulapuri metalice.

Secțiunea a 2-a. Cerințele referitoare la complexul tehnic de program

77. Complexul tehnic de program al centrului de certificare trebuie să asigure executarea de către centru a funcțiilor de certificare a cheilor publice şi să corespundă normelor tehnice în domeniul semnăturii digitale.

78. Exploatarea complexului tehnic de program al centrului de certificare trebuie efectuată conform cerințelor stabilite de asigurare a securității.

79. Mijloacele tehnice ale complexului tehnic de program, utilizate de centrul de certificare, trebuie să fie proprietate a centrului, fie închiriate sau primite în folosință pe baza unui contract scris.

80. Fiecare mijloc tehnic trebuie să fie înregistrat şi testat în privința posibilității de utilizare şi fiecare mijloc tehnic sau de program trebuie să fie însoțit de documentația tehnică.

81. Capacitatea de funcționare a mijloacelor tehnice trebuie verificată periodic pe parcursul întregului ciclu de exploatare, iar rezultatele verificării vor fi consemnate.

82. Toate mijloacele tehnice trebuie să fie asigurate cu posibilități de reparare. Pentru dispozitivele ce necesită deservire tehnică periodică trebuie elaborate instrucțiuni şi grafice de deservire tehnică. Toate echipamentele şi dispozitivele de control-măsurare trebuie întreținute în condiții ce asigură integritatea acestora.

83. Complexul tehnic de program al centrului de certificare trebuie să asigure posibilitatea copierii de rezervă şi păstrării informației critice pentru activitatea centrului de certificare, restabilirii operative şi complete a informației în caz de refuz al deservirii, de incidente sau erori în sisteme, precum şi instalării, în caz de necesitate, a resurselor tehnice suplimentare sau de rezervă.

84. În activitatea sa centrul de certificare trebuie să utilizeze numai soft licențiat sau liber distribuit.

85. Centrul de certificare este obligat să asigure administrarea complexului tehnic de program sau a subsistemelor acestuia numai de către persoane împuternicite să administreze, precum şi să excludă modificările neautorizate ale configurațiilor echipamentului, ale setărilor de sistem, ale algoritmilor de funcționare a mijloacelor de program, modificarea fluxurilor informaționale sau proceselor susținute.

Secțiunea a 3-a. Cerințele referitoare la personal

86. Centrul de certificare trebuie să dispună de un număr de angajați, cu calificare, experiență şi pregătire profesională care să permită realizarea întregului spectru de funcții privind prestarea serviciilor în domeniul semnăturii digitale.

87. Încadrarea personalului centrului de certificare trebuie să fie prezentată în structura organizatorică şi nomenclatorul de funcții, aprobate de conducătorul persoanei juridice. Nivelul de calificare a fiecărui specialist trebuie dovedit documentar.

88. Pentru fiecare specialist al centrului de certificare trebuie definite condițiile concrete privind nivelul de studii, de cunoştințe tehnice şi experiență de lucru. De asemenea vor fi stabilite obligațiile de serviciu, funcțiile, drepturile, responsabilitățile şi cerințele față de regimul de confidențialitate.

89. Fiecare angajat al centrului de certificare este obligat să cunoască şi să îndeplinească obligațiile sale de serviciu, periodic să-şi sporească nivelul de calificare, să studieze profesiile complementare profilului activității de bază.

90. Centrul de certificare trebuie să verifice şi să evalueze periodic nivelul de calificare a specialiştilor săi şi să asigure sporirea acestuia.

91. În cazul lipsei specialiştilor proprii pentru realizarea activităților specifice, centrul de certificare poate implica angajați ai altor organizații, cu asigurarea cerințelor de securitate stabilite.

92. Angajaţii centrului de certificare trebuie să semneze clauze de confidenţialitate, în condiţiile articolului 53 al Codului muncii al Republicii Moldova, precum şi, după caz, angajamente de nedivulgare a secretului comercial, valabile atît pentru perioada contractului individual de muncă încheiat, cît şi pentru perioada stabilită în contract după expirarea acţiunii acestuia.

VI. Cerinţele referitoare la gestionarea resurselor informaţionale ale centrului de certificare

Secţiunea 1. Cerinţele referitoare la resursele informaţionale

93. Resursele informaţionale ale centrului de certificare sînt registrul certificatelor cheilor publice şi documentele de serviciu ale centrului de certificare.

94. Resursele informaţionale ale centrului de certificare sînt ţinute sub formă de documente pe suport de hîrtie şi sub formă de documente electronice, păstrate pe suporturi materiale.

95. Resursa informaţională principală a centrului de certificare este registrul certificatelor cheilor publice, care reprezintă un ansamblu de documente electronice şi documente pe suport de hîrtie incluzînd:

a) cereri de certificare a cheilor publice ale utilizatorilor semnăturii digitale;

b) certificatele cheilor publice ale utilizatorilor semnăturii digitale;

c) decizii de suspendare, restabilire a valabilităţii sau revocare a certificatelor cheilor publice ale utilizatorilor semnăturii digitale;

d) certificatele cheilor publice ale persoanelor împuternicite ale centrului de certificare de nivelul al treilea (numai pentru centrele de certificare de nivelul al doilea);

e) cereri de suspendare, restabilire a valabilităţii sau revocare a certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al treilea (numai pentru centrele de certificare de nivelul al doilea);

f) listele certificatelor revocate.

96. Documentaţia centrului de certificare trebuie să corespundă standardului internaţional ISO 15489 "Informaţia şi documentaţia – gestionarea documentaţiei".

Secţiunea a 2-a. Cerinţele faţă de păstrarea, în formă arhivată, a resurselor informaţionale

97. În formă arhivată vor fi păstrate următoarele resurse informaţionale ale centrului de certificare:

a) registrul certificatelor cheilor publice;

b) jurnale de audit al complexului tehnic de program;

c) alte tipuri de documente stabilite de centrul de certificare.

98. Termenul de păstrare în formă arhivată a registrului certificatelor cheilor publice va fi de cel puţin 10 ani din momentul revocării ultimului certificat inclus în registru.

99. Pregătirea pentru distrugere şi efectuarea distrugerii documentelor arhivate se realizează de o comisie, formată din angajaţii centrului de certificare, în conformitate cu legislaţia în vigoare.

100. Lucrările de pregătire pentru distrugere şi de distrugere a documentelor ce nu sînt supuse arhivării se efectuează de către angajaţii centrului de certificare ce gestionează documentele, în modul stabilit de conducătorul centrului de certificare.

Secţiunea a 3-a. Cerinţele faţă de asigurarea accesului la resursele informaţionale

101. Centrul de certificare asigură accesul utilizatorilor semnăturii digitale la registrul certificatelor cheilor publice prin intermediul:

a) resurselor electronice oficiale ale centrului de certificare (portalul web);

b) poştei electronice;

c) rezolvării solicitărilor utilizatorilor semnăturii digitale conform procedurilor aprobate de centrul de certificare.

102. Accesul la documentele din arhivă ale centrului de certificare se realizează în conformitate cu legislaţia în vigoare.

VII. Cerinţele referitoare la asigurarea securităţii centrului de certificare

Secţiunea 1. Cerinţele referitoare la sistemul de securitate

103. Obiectivele de bază privind asigurarea securităţii centrului de securitate sînt:

a) protecţia informaţiei confidenţiale la depozitarea, prelucrarea şi transmiterea acesteia (chei criptografice, mijloace de protecţie criptografică a informaţiei, date personale protejate conform legislaţiei în vigoare, informaţie despre parole etc.);

b) verificarea integrităţii informaţiei confidenţiale şi publice (informaţia despre titulari inclusă în certificatele cheilor publice, informaţia despre certificatele cheilor publice suspendate sau revocate, componentele aplicative distribuite liber şi documentele aferente etc.);

c) verificarea integrităţii componentelor de program şi de aparataj ale complexului tehnic de program;

d) asigurarea continuităţii în activitate;

e) asigurarea securităţii fizice a centrului de certificare.

104. Sistemul de securitate a centrului de certificare trebuie:

a) să protejeze informaţia referitor la titularii certificatelor cheilor publice prin intermediul asigurării confidenţialităţii, integrităţii şi asigurării accesului securizat la registrul certificatelor cheilor publice;

b) să asigure securitatea infrastructurii şi a resurselor informaţionale ale centrului de certificare;

c) să stabilească responsabilităţi referitor la securitatea informaţională în centrul de certificare;

d) să minimizeze riscurile referitoare la utilizarea tehnologiilor informaționale;

e) să asigure capacitatea centrului de certificare de a continua activitatea în cazuri excepționale sau alte situații critice (asigurarea continuității activității centrului de certificare).

105. Ansamblul măsurilor şi al mijloacelor de protecție a informației în centrul de certificare trebuie să includă următoarele subsisteme:

a) subsistemul de protecție criptografică a informației, care include mijloacele de protecție criptografică a informației;

b) subsistemul de protecție a informației contra accesului neautorizat;

c) subsistemul de audit activ al securității informaționale a centrului;

d) subsistemul de detectare a intruziunilor;

e) subsistemul de protecție a informației contra acțiunilor neintenționate, inclusiv subsistemul de copiere de rezervă şi arhivare a datelor;

f) subsistemul de asigurare a integrității informației, componentelor de program şi de aparataj ale complexului tehnic de program al centrului de certificare, inclusiv prin metode criptografice;

g) subsistemul de asigurare a accesibilității, inclusiv subsistemul de asigurare a continuității funcționării complexului tehnic de program al centrului de certificare;

h) subsistemul de protecție a echipamentului complexului tehnic de program al centrului de certificare contra scurgerii de informații prin canalele tehnice şi cele auxiliare;

i) subsistemul securității fizice.

106. Centrul de certificare trebuie să elaboreze condițiile de asigurare a securității proprii, criteriile şi indicatorii de evaluare a nivelului de securitate, în concordanță cu care realizează activități şi implementează mijloace concrete de protecție a informației.

107. Orice funcție a centrului de certificare poate fi delegată persoanelor terțe numai în condițiile cînd se respectă activitatea securizată a centrului de certificare.

108. Centrul de certificare trebuie să elaboreze şi să aprobe procedurile interne de activitate, care să asigure funcționarea securizată a centrului de certificare.

109. Orice situație de forță majoră care poate influența în mod negativ realizarea procedurilor obligatorii ale centrului de certificare trebuie adusă la cunoştința titularilor certificatelor cheilor publice.

110. Centrul de certificare trebuie să elaboreze şi să aprobe politica de securitate a centrului de certificare, care va reflecta viziunea asupra problemei securității informaționale a centrului de certificare, ansamblul de măsuri pentru asigurarea acesteia, responsabilitățile angajaților şi mecanismele de control al stării securității informaționale.

111. Politica de securitate trebuie să asigure respectarea regulilor, standardelor şi normelor general acceptate în domeniul securității informaționale şi trebuie să includă:

a) categoriile resurselor centrului de certificare cu indicarea nivelului necesar de securitate pentru fiecare categorie;

b) analiza riscurilor centrului de certificare, ce pot apărea la utilizarea tehnologiilor informaționale şi de telecomunicații;

c) modelul de securitate a centrului de certificare;

d) alegerea unui sistem complex de asigurare a securității centrului de certificare;

e) principalele măsuri tehnico-organizatorice necesare pentru asigurarea securității centrului de certificare;

f) condiții impuse mijloacelor tehnice de protecție a informației;

g) enumerarea mijloacelor tehnice de protecție a informației;

h) planul de acțiuni privind menținerea regimului de securitate a centrului de certificare, inclusiv planurile de continuitate în activitate;

i) responsabilitățile personalului centrului de certificare privind asigurarea securității;

j) proceduri de control al centrului de certificare privind respectarea condițiilor de securitate;

k) procedura de aducere la cunoştința utilizatorilor semnăturii digitale a Regulamentului centrului de certificare şi a politicii de securitate, de acceptare şi asumare a obligațiilor de respectare a prevederilor Regulamentului şi a politicii de securitate de către utilizatori;

l) înştiințarea utilizatorilor semnăturii digitale despre nivelul de securitate a centrului de certificare.

112. Centrul de certificare trebuie să elaboreze şi să aprobe sistemul de acordare a drepturilor de acces la resursele centrului de certificare, conform procedurilor de acces stabilite.

113. Centrul de certificare trebuie să analizeze toate componentele infrastructurii proprii (resurse aplicative şi tehnice, mijloace de protecție a informației etc.) din punctul de vedere al riscurilor, să planifice şi să realizeze activități de minimizare şi evitare a riscurilor depistate.

114. Centrul de certificare trebuie să implementeze instrumente automatizate de analiză a sistemelor informaționale şi de telecomunicații, precum şi a proceselor de afaceri ale centrului de certificare, pentru depistarea vulnerabilităților în sistemul de securitate.

115. Centrul de certificare trebuie să elaboreze şi să aprobe planul de acțiuni pentru asigurarea continuității activității, plan care va fi analizat şi revizuit periodic pe baza analizei activității curente şi rezultatelor testării în diferite situații excepționale posibile.

Secțiunea a 2-a. Cerințele de asigurare a securității fizice

116. Centrul de certificare trebuie să creeze şi să mențină sistemul de securitate fizică care să asigure protecția infrastructurii, a resurselor informaționale şi a personalului centrului, să fie flexibil în cazul modificării cerințelor de securitate înaintate, să permită adăugarea de noi funcționalități şi să fie simplu în utilizare.

117. Sistemul de securitate fizică a centrului de certificare trebuie să includă următoarele subsisteme:

a) gestionarea accesului la diferite obiecte fizice;

b) depistarea intruziunilor neautorizate la obiectele fizice;

c) gestionarea, analiza şi înregistrarea informației;

d) protecția tehnică şi de inginerie (protecția pasivă);

e) înştiințarea şi asigurarea conexiunii în caz de situații excepționale.

118. Centrul de certificare trebuie să stabilească şi să precizeze responsabilitățile angajaților legate de asigurarea securității fizice.

119. Informația privind amplasarea subsistemelor complexului tehnic de program al centrului de certificare este confidențială.

120. Echipamentul special şi tehnic de inginerie, protecția şi regimul de acces în încăperile speciale ale centrului de certificare trebuie să asigure securitatea informației confidențiale şi a cheilor criptografice, accesul controlat în aceste încăperi, precum şi accesul la mijloacele tehnice şi cheile criptografice.

121. Centrul de certificare trebuie să-şi clasifice încăperile cu regim special de acces, să stabilească reguli de acces şi să aprobe lista persoanelor cărora le este permis accesul în aceste încăperi.

122. Accesul angajaților centrului de certificare în încăperile speciale se efectuează conform instrucțiunilor şi ordinelor în vigoare în centrul de certificare.

123. Accesul fizic în încăperile speciale ale centrului de certificare trebuie să fie posibil numai în urma controlului dublu şi conform drepturilor de acces stabilite.

124. Angajații centrului de certificare care au acces în încăperile speciale poartă răspundere personală pentru permiterea accesului persoanelor terțe în aceste încăperi.

125. Încăperile speciale vor fi dotate în mod obligatoriu cu sisteme de control al accesului şi monitorizare video, care trebuie să permită supravegherea accesului persoanelor în aceste încăperi.

126. Încăperile speciale se dotează în mod obligatoriu cu sisteme de pază pe mai multe linii şi semnalizare de alarmă, în conformitate cu normele metodologice şi tehnice de proiectare şi montare a sistemelor de alarmare împotriva efracției, aprobate prin Hotărîrea Guvernului nr. 667 din 8 iulie 2005 "Cu privire la măsurile de realizare a Legii nr. 283-XV din 4 iulie 2003 privind activitatea particulară de detectiv şi de pază".

127. La amplasarea mijloacelor tehnice, centrul de certificare trebuie să asigure protecția lor contra accesului neautorizat, furt, incendii, inundații, cîmpuri electromagnetice puternice şi alte riscuri posibile.

128. Încăperile destinate pentru amplasarea personalului centrului de certificare, precum şi alte încăperi de serviciu trebuie să fie echipate cu:

a) sisteme de pază, alarmă şi semnalizare antiincendiară;

b) sisteme de control al accesului, care să permită supravegherea accesului personalului centrului de certificare în anumite încăperi.

129. În cazul amplasării încăperilor de serviciu sau a altor încăperi la parter şi la ultimul etaj, precum şi în cazul existenței balcoanelor, scărilor antiincendiare etc., la ferestrele încăperilor respective trebuie să fie instalate gratii din interior.

Secțiunea a 3-a. Cerințele referitoare la asigurarea securității sistemelor informaționale şi de telecomunicații

130. Pentru micşorarea riscurilor legate de utilizarea tehnologiilor informaționale şi de telecomunicații, centrul de certificare elaborează şi implementează un set de măsuri de asigurare a securității sistemelor sale informaționale şi de telecomunicații (mijloace de program şi tehnice, canale de telecomunicații, echipament de rețea, informații prelucrate, depozitate şi transmise), prin funcționarea următoarelor subsisteme de securitate:

a) subsistemul de gestiune a accesului;

b) subsistemul de înregistrare şi evidență (audit);

c) subsistemul de asigurare a integrității;

d) subsistemul de asigurare a accesibilității;

e) subsistemul de protecție criptografică.

131. Subsistemul de gestiune a accesului:

a) asigură delimitarea accesului la obiectele informaționale şi la funcțiile sistemelor informaționale corespunzător cu regulile de acces, bazate pe atributele de acces;

b) efectuează verificarea identității subiecților ce obțin acces la componentele sistemelor informaționale;

c) verifică accesul subiecților la resursele protejate corespunzător cu nivelurile de acces stabilite;

d) gestionează fluxurile informaționale şi aplică sigla de confidențialitate;

e) fixează cazurile de acces cu succes sau cu eşec.

132. Subsistemul de înregistrare şi evidență:

a) înregistrează evenimentele de accesare (părăsire) a sistemului de către subiect conform următorilor parametri:

data şi timpul tentativei de accesare (părăsire);

identificatorul subiectului de acces;

rezultatul tentativei de accesare (părăsire) – succes sau eşec;

b) înregistrează tentativele de lansare (stopare) a aplicațiilor şi a proceselor destinate să prelucreze resursele protejate conform următorilor parametri:

data şi timpul tentativei de lansare;

denumirea (identificatorul) aplicației sau procesului;

identificatorul subiectului de acces;

rezultatul tentativei de lansare – succes sau eşec;

c) înregistrează tentativele de obținere a drepturilor de acces (de executare a operațiilor) pentru aplicații şi procese la resursele protejate conform următorilor parametri:

data şi timpul tentativei de obținere a accesului (executare a operației);

denumirea (identificatorul) aplicației sau procesului;

identificatorul subiectului de acces;

specificațiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);

tipul operației solicitate (citire, înregistrare, ştergere, montare etc.);

rezultatul tentativei de obținere a accesului (executare a operației) – succes sau eşec;

d) înregistrează tentativele de acces neautorizat al subiecților în sistem, tentativele de lansare neautorizată a aplicațiilor (proceselor) sau de executare a operațiilor, asigurînd blocarea tuturor operațiunilor neautorizate şi înştiințînd despre acest fapt administratorul securitate;

e) înregistrează modificările drepturilor de acces al subiecților şi statutul obiectelor de acces conform următorilor parametri:

data şi timpul modificării drepturilor;

identificatorul administratorului care a operat modificările;

identificatorul subiectului de acces şi noile drepturi sau specificațiile obiectului de acces şi noul său statut;

f) înregistrează toate ieşirile de informație din sistem (documente electronice, date etc.) conform următorilor parametri:

data şi timpul ieşirilor de date;

denumirea informației şi calea spre ea;

specificațiile dispozitivului ce a eliberat informația (numele logic);

identificatorul subiectului de acces care a solicitat informația;

volumul documentului eliberat (număr de pagini, foi, copii) şi rezultatul eliberării de informație (succes, eşec);

g) ține evidența resurselor protejate ale centrului de certificare, înregistrează intrarea/ieşirea suporturilor materiale ce conțin informație confidențială;

h) protejează datele "protocolate" (jurnalul de înregistrări, fişiere log etc.) contra modificărilor;

i) identifică şi arată evenimentele curente.

133. Subsistemul de asigurare a integrității menține stabilitatea mediului aplicativ, integritatea informației prelucrate, a mijloacelor tehnico-aplicative şi a mijloacelor de protecție a informației.

134. Subsistemul de asigurare a accesibilității:

a) asigură funcționarea continuă a sistemelor informaționale şi de telecomunicații ale centrului de certificare;

b) asigură păstrarea garantată a resurselor informaționale ale centrului de certificare, precum şi posibilitatea de restabilire a lor în caz de necesitate sau în cazul situațiilor de forță majoră;

c) asigură utilizatorilor sistemului acces permanent la resursele informaționale ale centrului de certificare, corespunzător cu normele stabilite de acces la informație.

135. Subsistemul de protecție criptografică:

a) realizează criptarea informației confidențiale în sistemul informațional şi în canalele de telecomunicații;

b) asigură controlul accesului subiecților la operațiile de criptare şi la cheile criptografice, corespunzător cu regulile de acces stabilite.

136. Arhitectura sistemelor informaționale şi de telecomunicații ale centrului de certificare şi a subsistemelor acestora trebuie să fie destul de flexibilă, să permită dezvoltarea simplă, fără modificări structurale, a configurațiilor mijloacelor utilizate şi completarea de noi funcții şi resurse.

137. Sistemele informaționale şi de telecomunicații ale centrului de certificare trebuie să fie însoțite de documentație care să asigure exploatarea lor calificată.

138. Componentele critice ale sistemelor informaționale şi de telecomunicații ale centrului de certificare trebuie să includă sisteme de rezervă şi de repornire în cazul încălcării regimului de securitate sau refuzului (deficienței) de deservire.

139. Sistemele informaționale şi de telecomunicații, componentele lor, mijloacele tehnice şi de program ale centrului de certificare trebuie să corespundă normelor stabilite de politica de securitate informațională, iar prestatorii de servicii (producătorii, furnizorii etc.) trebuie să asigure suportul tehnic necesar.

140. Centrul de certificare trebuie să asigure protecția sistemelor informaționale şi de telecomunicații proprii contra acțiunilor aplicațiilor malefice (sistemul de protecție antivirus).

141. Centrul de certificare trebuie să-şi clasifice resursele sistemului informațional, să stabilească procedurile de acces şi să aprobe lista persoanelor cu drept de acces la resursele specifice ale sistemului informațional şi de telecomunicații.

142. Centrul de certificare trebuie să elaboreze, să aprobe şi să implementeze mecanismele şi procedurile necesare de delimitare şi control al accesului logic şi fizic la echipamentele sistemelor informaționale şi de telecomunicații.

143. Accesul angajaților centrului de certificare la resursele sistemelor informaționale şi de telecomunicații trebuie să fie acordat pe baza instrucțiunilor şi ordinelor aprobate în centrul de certificare corespunzător drepturilor de acces.

144. Centrul de certificare trebuie să stabilească şi să documenteze procedurile privind administrarea şi utilizarea resurselor de program şi de sistem.

145. Sistemele informaționale şi de telecomunicații noi sau modernizate, componentele acestora, mijloacele tehnice şi de program trebuie să fie implementate numai în conformitate cu procedurile stabilite, cu respectarea cerințelor privind asigurarea securității informaționale.

146. Centrul de certificare trebuie să elaboreze şi să aprobe instrucțiuni de implementare a sistemelor informaționale şi de telecomunicații noi sau de modificare a celor existente, a componentelor acestora, a mijloacelor tehnice şi de program.

147. Personalul responsabil al centrului de certificare trebuie să fie instruit privind funcționalitatea şi regulile de administrare (exploatare) a sistemelor informaționale şi de telecomunicații, a componentelor, a mijloacelor tehnice şi de program noi sau modernizate.

148. Toate modificările de configurare a sistemelor informaționale şi de telecomunicații în ansamblu, a componentelor acestora, a mijloacelor tehnice şi de program trebuie să fie testate pînă la implementarea acestora în mediul operațional. Decizia despre modificare trebuie luată numai după realizarea unei evaluări a riscurilor referitoare la implementarea modificărilor respective.

149. Centrul de certificare trebuie să elaboreze şi să aprobe proceduri formale de control al modificărilor în sistemul informațional şi de telecomunicații, al modificărilor componentelor acestuia, al mijloacelor tehnice şi de program.

150. Centrul de certificare trebuie să utilizeze conexiuni şi mecanisme securizate şi controlabile, care să asigure integritatea şi confidenţialitatea informaţiei la transmiterea prin intermediul reţelelor publice.

151. Centrul de certificare trebuie să implementeze mecanisme de ecranare a reţelelor, pentru a proteja sistemele informaţionale şi de telecomunicaţii interne, precum şi resursele centrului de certificare în general.

152. Personalul responsabil al centrului de certificare (administratorii sistem) este obligat să efectueze controlul zilnic al stării sistemelor informaţionale şi de telecomunicaţii, al componentelor acestora, sistemelor operaţionale şi aplicative, precum şi al instrumentelor de securitate.

Secţiunea a 4-a. Condiţiile de utilizare a mijloacelor de protecţie criptografică a informaţiei

153. Centrul de certificare asigură securitatea informaţiei confidenţiale la depozitare, prelucrare şi transmitere prin canalele de comunicaţii, aplicînd tehnologiile de criptare a informaţiei cu utilizarea mijloacelor de protecţie criptografică a informaţiei (MPCI).

154. În scopul elaborării şi realizării măsurilor de asigurare a securităţii informaţiei şi utilizării MPCI, centrul de certificare trebuie să creeze o subdiviziune pentru protecţia criptografică a informaţiei (să numească un angajat), să elaboreze şi să aprobe instrucţiuni care să reglementeze procesele de pregătire, introducere, prelucrare, păstrare şi transmitere a informaţiei confidenţiale protejate cu MPCI.

155. Subdiviziunea de protecţie criptografică:

a) elaborează şi implementează sistemul de protecţie criptografică a informaţiei confidenţiale a centrului de certificare;

b) elaborează instrucţiunile şi măsurile de asigurare a funcţionării şi securităţii MPCI utilizate;

c) asigură păstrarea şi evidenţa purtătorilor materiali de informaţie confidenţială, MPCI şi documentaţiei aferente, purtătorilor materiali de informaţie-cheie, precum şi evidenţa utilizatorilor ce folosesc nemijlocit MPCI;

d) instruieşte utilizatorii MPCI privind regulile de lucru cu MPCI;

e) controlează modalitatea de respectare de către utilizatori a normelor de utilizare a MPCI stabilite, precum şi a documentaţiei de exploatare şi tehnice aferente MPCI;

f) verifică integritatea resurselor de program şi de sistem ale mijloacelor tehnice unde au fost instalate MPCI, precum şi integritatea MPCI;

g) depistează faptele de încălcare a normelor de utilizare a MPCI şi întreprinde măsurile necesare de evitare a urmărilor acestor încălcări.

156. Angajaţii subdiviziunii de protecţie criptografică sînt obligaţi:

a) să respecte regimul de confidenţialitate în procesul de îndeplinire a obligaţiilor de serviciu;

b) să depisteze la timp tentativele persoanelor terţe de a obţine date privind informaţia confidenţială, MPCI utilizate şi suporturile-cheie;

c) să ia măsuri urgente de prevenire a cazurilor de divulgare a informației confidențiale şi de scurgere a informației la utilizarea MPCI.

157. Angajații subdiviziunii de protecție criptografică trebuie să posede un nivel de calificare corespunzător şi să activeze conform fişei de post.

158. Centrul de certificare implementează şi exploatează MPCI conform documentației tehnice şi de exploatare aferentă acestor mijloace, pe baza instrucțiunilor aprobate, precum şi în conformitate cu prezentele condiții speciale.

159. Instrucțiunile ce reglementează modul de exploatare în siguranță a MPCI trebuie să prevadă:

a) drepturile şi obligațiile angajaților centrului de certificare ce exploatează MPCI;

b) ordinea de amplasare, instalare, păstrare şi utilizare a MPCI şi a documentației privind exploatarea acestora;

c) ordinea de creare, evidență, distribuire, păstrare şi distrugere a cheilor criptografice;

d) ordinea de cercetare a faptelor de încălcare a regulilor stabilite la utilizarea MPCI, a cheilor criptografice, precum şi măsurile de înlăturare a consecințelor;

e) ordinea de control al respectării cerințelor de asigurare a protecției informației cu ajutorul MPCI.

160. Condițiile de implementare şi exploatare a MPCI trebuie să excludă posibilitatea accesului neautorizat la ele, modificarea, furtul şi difuzarea necontrolată a acestora.

161. MPCI utilizate de centrul de certificare trebuie să fie verificate periodic pe parcursul întregului ciclu de funcționare.

162. MPCI trebuie să fie inventariate. MPCI de tip aplicativ sînt supuse evidenței împreună cu mijloacele tehnice pe care le rulează.

163. În caz de necesitate, pentru asigurarea integrității cheilor criptografice pot fi create copii de rezervă, care se păstrează conform normelor stabilite de asigurare a protecției contra accesului neautorizat şi acțiunilor neintenționate.

164. Angajații centrului de certificare poartă răspundere personală pentru integritatea şi securitatea cheilor criptografice.

165. Subdiviziunea de protecție criptografică ține evidența suporturilor materiale de chei criptografice.

166. Suporturile materiale de chei criptografice neutilizate sau scoase din uz sînt distruse de subdiviziunea de protecție criptografică.

167. Distrugerea cheilor criptografice se efectuează prin distrugerea fizică a suportului material sau prin distrugerea garantată a informației-cheie fără deteriorarea suportului (pentru utilizarea repetată a acestuia).

168. Cheile criptografice ale MPCI trebuie schimbate periodic. Procedura de schimbare a cheilor criptografice se stabileşte de către centrul de certificare.

169. Dacă există suspiciuni privitoare la compromiterea cheilor criptografice sau MPCI, acestea sînt scoase imediat din uz, iar subdiviziunea de protecție criptografică efectuează toate acțiunile de verificare a acestui fapt şi înlăturare a urmărilor.

Secțiunea a 5-a. Condițiile de protecție tehnică a informației

170. Centrul de certificare asigură protecția informației confidențiale prin utilizarea tehnologiilor şi a mijloacelor speciale de prevenire a scurgerii informației prin canalele tehnice.

171. Centrul de certificare trebuie să excludă prezența necontrolată a persoanelor sau a mijloacelor de transport, precum şi instalarea întîmplătoare a antenelor, într-o zonă de 15 metri de la locul amplasării mijloacelor tehnice principale ale complexului tehnic de program (în continuare – perimetru controlat).

172. Încăperile pentru servere ale centrului de certificare trebuie să fie protejate contra scurgerii informației din cauza emisiilor electromagnetice prin ecranarea încăperilor sau instalarea sistemelor de bruiaj electromagnetic.

173. În cazul ecranării încăperilor trebuie asigurată continuitatea conexiunii electrice a materialului tuturor părților ecranului: pereți, tavan, podea, ferestre şi uşi. Materialul pentru uşi trebuie să posede un contact electric sigur cu ecranul încăperii pe toată suprafața, construcțiile de ecranare trebuie să posede prize de pămînt care să fie amplasate în regiunea controlată.

174. Centrul de certificare trebuie să asigure protecția informației contra scurgerii prin intermediul rețelei electrice [încrucişarea rețelelor electrice ale obiectului cu instalarea filtrelor de protecție care să blocheze (bruieze) semnalul].

175. În încăperile centrului de certificare unde sînt amplasate mijloacele tehnice ce prelucrează informație confidențială trebuie exclusă sau limitată instalarea altor dispozitive electrice, radio sau de alt gen.

176. Utilajul pe liniile care au ieşire în afara regiunii controlate trebuie instalate la o distanță de cel puțin de 3 metri de la mijloacele tehnice principale ale complexului tehnic de program al centrului de certificare.

177. Suficiența măsurilor de protecție tehnică realizate, precum şi necesitatea instalării mijloacelor tehnice speciale suplimentare se stabilesc conform rezultatului cercetărilor speciale şi de evaluare a nivelului de protejare al obiectului.

Secțiunea a 6-a. Condițiile referitoare la asigurarea securității resurselor informaționale

178. Resursele informaționale ale centrului de certificare trebuie să fie clasificate şi definite pe categorii în funcție de nivelul de securitate al acestora.

179. Toată informația, datele şi documentele trebuie să fie prelucrate şi păstrate conform nivelului de clasificare şi categoriei acestei informații.

180. Toata informația, datele şi documentele, clasificate ca fiind confidențiale, trebuie păstrate într-un mediu sigur separat.

181. Centrul de certificare trebuie să ia măsuri de protecție a datelor personale conform legislației Republicii Moldova.

182. Registrul certificatelor cheilor publice trebuie păstrat şi gestionat în condiții care îi vor asigura integritatea, accesibilitatea şi confidențialitatea.

183. Centrul de certificare trebuie să creeze copii de rezervă ale registrului certificatelor cheilor publice, precum şi pentru altă informație critică.

184. Copiile de rezervă se păstrează în încăperi speciale ale centrului de certificare.

185. Documentele centrului de certificare trebuie să fie protejate contra pierderii, distrugerii şi falsificării.

186. Centrul de certificare trebuie să fixeze termenele de utilizare şi păstrare a documentelor şi a informaţiei, să elaboreze nomenclatorul dosarelor, în care vor fi specificate tipurile documentelor principale şi perioada de păstrare a acestora.

187. Utilizarea resurselor informaţionale ale centrului de certificare în scopuri personale de către angajaţii centrului este interzisă.

188. Angajaţii centrului de certificare sînt obligaţi să cunoască riscurile legate de încălcarea securităţii informaţiei cu care lucrează.

Secţiunea a 7-a. Condiţiile referitoare la sistemul de administrare a securităţii informaţionale

189. Centrul de certificare trebuie să creeze sistemul de administrare a securităţii informaţionale, să realizeze monitorizarea permanentă a sistemului de securitate informaţională şi să gestioneze riscurile.

190. Pentru administrarea securităţii informaţionale se recomandă standardul internaţional ISO/IEC 17799-2005 "Tehnologii informaţionale. Cod de practici privind administrarea securităţii informaţionale".

VIII. Controlul activităţii centrului de certificare

191. Centrul de certificare este obligat să efectueze o dată în doi ani un control complex al activităţii sale.

192. Controlul complex al activităţii centrului de certificare se efectuează de către organului abilitat cu elaborarea şi promovarea politicii de stat şi cu exercitarea controlului în domeniul aplicării semnăturii digitale – Serviciului de Informaţii şi Securitate al Republicii Moldova (în continuare – organ competent), cu atragerea, după caz, a specialiştilor în domeniu.

193. La iniţiativa centrului de certificare, controlul complex al activităţii acestuia poate fi realizat de către organizaţii specializate de audit şi de consultare în domeniul tehnologiilor informaţionale, cu atragerea reprezentantului organului competent, din contul centrului de certificare.

194. Se recomandă ca organizaţia ce realizează controlul complex al activităţii centrului de certificare să corespundă următoarelor cerinţe:

a) să posede personal cu calificare atestată prin certificate de auditori în domeniul sistemelor informaţionale (standarde internaţionale CISA sau CISM);

b) să posede experienţă de audit în domeniul tehnologiilor informaţionale de minim 2 ani.

195. Organizaţia ce realizează controlul complex al activităţii centrului de certificare trebuie:

a) să asigure independenţa controlului efectuat;

b) să efectueze controlul în conformitate cu normele şi standardele de audit în domeniul tehnologiilor informaţionale şi de securitate a sistemelor informaţionale;

c) să utilizeze o metodologie de audit bazată pe evaluarea riscurilor şi pe procedurile corespunzătoare de evaluare a măsurilor de gestionare a riscurilor;

d) să asigure confidenţialitatea informaţiei obţinute în urma controlului.

196. Organizaţia ce realizează controlul complex al activităţii centrului de certificare trebuie să întocmească un act de verificare şi o încheiere.

197. Actul de verificare se semnează de către persoana responsabilă care a efectuat controlul activităţii centrului de certificare, reprezentantul organului competent şi conducătorul persoanei juridice în cadrul căreia îşi desfăşoară activitatea centrul de certificare.

198. Încheierea se întocmeşte pe baza actului de verificare şi reprezintă documentul care atestă (infirmă) concordanţa activităţii centrului de certificare cu normele stabilite în domeniul semnăturii digitale.

199. Încheierea trebuie să cuprindă:

a) evaluarea calităţii şi continuităţii serviciilor în domeniul semnăturii digitale prestate de către centrul de certificare;

b) corespunderea activităţii centrului de certificare cu standardele, normele tehnice şi alte documente normative din domeniul semnăturii digitale;

c) corespunderea activităţii centrului de certificare cu prevederile Regulamentului centrului de certificare, politicii de certificare şi politicii de securitate;

d) corespunderea activităţii centrului de certificare cu funcţiile şi obligaţiile stabilite;

e) concordanţa procedurilor principale ale centrului de certificare cu cerinţele înaintate;

f) concordanţa activităţii centrului de certificare cu cerinţele de asigurare a securităţii centrului de certificare;

g) concluzii privind suficienţa măsurilor de asigurare a confidenţialităţii, a integrităţii şi accesibilităţii informaţiei şi a serviciilor informaţionale;

h) evaluarea calităţii şi complexităţii procedurilor interne ale centrului de certificare;

i) analiza funcţiilor de gestionare a riscurilor centrului de certificare;

j) respectarea procedurilor de asigurare a continuităţii în activitate a centrului de certificare;

k) corespunderea complexului tehnic de program al centrului de certificare cu cerinţele înaintate;

l) evaluarea măsurilor întreprinse pentru remedierea celor constatate în urma auditului precedent.

200. Rezultatele controlului complex al activităţii centrului de certificare (copia actului şi încheierii), efectuat de către o organizaţie specializată de audit şi de consultare în domeniul tehnologiilor informaţionale, se prezintă organului competent.

201. Centrul de certificare trebuie să efectueze periodic auditul intern al activităţii sale, în conformitate cu Regulamentul privind efectuarea auditului intern aprobat de către acest centru.

IX. Crearea, reorganizarea şi lichidarea centrului de certificare

Secțiunea 1. Condițiile la crearea centrului de certificare

202. Pentru prestarea serviciilor de certificare a cheilor publice, centrul de certificare trebuie să îndeplinească procedura de înregistrare conform normelor stabilite şi să certifice cheia publică a persoanei împuternicite a centrului de certificare la centrul de certificare ierarhic superior.

203. Pentru înregistrarea centrului de certificare, persoana juridică care creează centrul de certificare este obligată să asigure îndeplinirea următoarelor condiții:

a) să creeze (numească) o subdiviziune pentru realizarea funcțiilor centrului de certificare;

b) să formeze un stat de personal, cu calificarea necesară pentru prestarea serviciilor de certificare a cheilor publice şi a altor servicii în domeniul semnăturii digitale;

c) să amenajeze încăperi speciale, precum şi alte încăperi de lucru ale centrului de certificare conform condițiilor referitoare la încăperile centrului de certificare stabilite în prezentele condiții speciale;

d) să creeze complexul tehnic de program al centrului de certificare în conformitate cu normele tehnice din domeniul semnăturii digitale şi conform prezentelor condiții speciale;

e) să numească persoana împuternicită a centrului de certificare (administratorul certificare), administratorul înregistrări, administratorul securitate şi administratorul sistem;

f) să creeze sistemul de securitate al centrului de certificare în conformitate cu prezentele condițiile speciale;

g) să creeze o subdiviziune (să numească un angajat) responsabilă de protecția criptografică a informației în centrul de certificare;

h) să elaboreze şi să aprobe baza normativă a centrului de certificare necesară pentru prestarea serviciilor de certificare a cheilor publice, care include următoarele documente obligatorii:

politica de certificare a centrului de certificare;
Regulamentul centrului de certificare;
politica de securitate a centrului de certificare;
politica de acordare şi control al accesului la resursele centrului de certificare;
planul de gestionare a riscurilor;
planul de asigurare a continuității activității centrului de certificare;
procedurile de restabilire a activității centrului de certificare;
instrucțiuni ce reglementează securitatea şi exploatarea MPCI;
regulamentul privind efectuarea auditului intern al centrului de certificare.

i) să obțină o garanție bancară la o bancă înregistrată pe teritoriul Republicii Moldova sau o poliță de asigurare la o companie de asigurări înregistrată în Republica Moldova în favoarea organului competent pentru o sumă în lei echivalentă a 20.000 euro.

204. În procesul înregistrării, centrul de certificare trebuie să treacă procedura unui control complex în conformitate cu cerinţele de control al activităţii centrului de certificare, stabilite în prezentele condiţii speciale.

Secţiunea a 2-a. Condiţiile referitoare la reorganizarea centrului de certificare

205. Reorganizarea centrului de certificare se efectuează prin formele prevăzute de legislaţie, funcţiile acestuia fiind transmise unei alte persoane juridice.

206. Transmiterea centrului de certificare se efectuează:

a) pe baza contractului de transmitere a centrului de certificare;

b) pe baza deciziei de reorganizare a persoanei juridice.

207. Persoana juridică trebuie să anunţe organul competent şi centrul de certificare ierarhic superior despre decizia privind transmiterea centrului de certificare în termen de cel puţin de 30 de zile pînă la momentul transmiterii.

208. Persoana juridică trebuie să anunţe toate centrele de certificare ierarhic inferioare şi utilizatorii semnăturii digitale despre decizia privind transmiterea centrului de certificare şi despre necesitatea reîncheierii contractelor de deservire cu noul centru de certificare în termen de cel puţin de 30 zile pînă la momentul transmiterii.

209. Prin decizia persoanelor juridice interesate se creează comisia de transmitere a centrului de certificare.

210. În componenţa comisiei de transmitere a centrului de certificare trebuie să intre:

a) reprezentanţii persoanelor juridice;

b) reprezentantul organului competent;

c) alte persoane, stabilite de părţi.

211. În procesul de transmitere, centrul de certificare trebuie:

a) să distrugă cheile private ale persoanelor împuternicite ale centrului de certificare fără a le atinge confidenţialitatea, în conformitate cu cerinţele stabilite de organul competent;

b) să transmită registrul certificatelor cheilor publice.

212. Registrul certificatelor cheilor publice sub formă de documente electronice se transmite pe suporturi materiale, iar registrul certificatelor cheilor publice sub formă de documente pe suport de hîrtie se transmite sub formă de arhivă a documentelor pe suporturi de hîrtie.

213. Certificatele cheilor publice eliberate de către centrul de certificare continuă să fie valabile pînă la expirarea termenul de valabilitate.

214. La încheierea lucrărilor comisiei se întocmeşte actul de primire-predare, conform căruia persoana juridică căreia i-a fost transmis centrul de certificare devine succesorul de drepturi al centrului. Actul se semnează de membrii comisiei şi se aprobă de către conducătorii persoanelor juridice interesate.

Secţiunea a 3-a. Condiţiile referitoare la lichidarea centrului de certificare

215. Centrul de certificare poate fi lichidat:

a) la inițiativa persoanei juridice care a creat centrul de certificare;

b) la inițiativa organului competent în cazul încălcării normelor în domeniul semnăturii digitale;

c) în cazul lichidării persoanei juridice care a creat centrul de certificare.

216. Persoana juridică trebuie să anunțe organul competent şi centrul de certificare ierarhic superior despre decizia de lichidare a centrului de certificare în termen de cel puțin de 30 de zile pînă la momentul lichidării.

217. Utilizatorii semnăturii digitale vor fi înştiințați despre decizia de lichidare a centrului de certificare într-o perioadă de cel puțin 30 de zile pînă la momentul lichidării.

218. Procedura de lichidare a centrului de certificare la inițiativa persoanei juridice care a creat centrul de certificare se inițiază prin ordinul conducătorului persoanei juridice.

219. Prin ordinul conducătorului persoanei juridice care lichidează centrul de certificare se creează comisia de lichidare, în sarcina căreia intră desfăşurarea procedurii de lichidare.

220. Lichidarea centrului de certificare la inițiativa organului competent este efectuată pe cale judiciară în baza încheierii organului competent privind încălcarea legislației în domeniul semnăturii digitale. După pronunțarea hotărîrii instanței de judecată, prin ordinul conducătorului organului competent, se creează comisia de lichidare.

221. În componența comisiei de lichidare trebuie să intre:

a) conducătorul persoanei juridice ce a creat centrul de certificare;

b) reprezentantul organului competent;

c) alte persoane, numite prin ordin.

222. În procesul de lichidare, centrul de certificare trebuie:

a) să distrugă cheile private ale persoanelor împuternicite ale centrului de certificare fără a le atinge confidențialitatea în conformitate cu cerințele stabilite de către organul competent;

b) să revoce certificatele cheilor publice ale utilizatorilor semnăturii digitale eliberate de centrul de certificare aflat în curs de lichidare;

c) să publice statutul certificatelor cheilor publice;

d) să transmită spre păstrare organului competent registrul certificatelor cheilor publice.

223. Registrul certificatelor cheilor publice sub formă de documente electronice se transmite pe suporturi materiale, iar registrul certificatelor cheilor publice sub formă de documente pe suport de hîrtie se transmite sub formă de arhivă a documentelor pe suporturi de hîrtie, fapt ce se consemnează în actul de primire-predare, semnat de către conducătorul persoanei juridice şi reprezentantul organului competent, responsabil pentru păstrare. Registrul certificatelor cheilor publice se păstrează în formă arhivată în conformitate cu legislația în vigoare.

224. Comisia de lichidare întocmeşte un act, în urma căruia centrul de certificare îşi încetează existența.