Republica Moldova

SERVICIUL DE INFORMAŢII ŞI SECURITATE

ORDIN Nr. 13
din 03.04.2006

cu privire la aprobarea unor acte normative în domeniul organizării funcţionării centrelor de certificare a cheilor publice

Publicat : 07.07.2006 în Monitorul Oficial Nr. 102-105 art Nr : 367 Data intrarii in vigoare : 07.07.2006

Întru executarea Hotărîrii Guvernului nr. 945 din 5 septembrie 2005 cu privire la centrele de certificare a cheilor publice (Monitorul Oficial al Republicii Moldova, 2005, nr. 123-125, art. 1020), în temeiul art. 36 alin. (2) al Legii nr. 264-XV din 15 iulie 2004 cu privire la documentul electronic şi semnătura digitală (Monitorul Oficial al Republicii Moldova, 2004, nr. 132-137, art. 710),

ORDON:

1. Se aprobă:

Regulamentul privind procedura de înregistrare a centrelor de certificare a cheilor publice (anexa nr. 1);

Condiţiile speciale de activitate a centrelor de certificare a cheilor publice (anexa nr. 2);

Regulamentul Centrului de certificare a cheilor publice de nivel superior (anexa nr. 3).

2. Controlul executării prezentului Ordin se atribuie dlui Valentin Dediu, director-adjunct al Serviciului de Informaţii şi Securitate al Republicii Moldova.

3. Prezentul Ordin intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

Directorul
Serviciului de Informaţii
şi Securitate Ion URSU

Chişinău 3 aprilie 2006.
Nr. 13.

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 425 din 21 iunie 2006
_____ Victoria IFTODI

Anexa nr. 1
la Ordinul directorului Serviciului
de Informaţii şi Securitate
al Republicii Moldova
nr. 13 din 3 aprilie 2006

REGULAMENTUL
privind procedura de înregistrare a centrelor de certificare a cheilor publice

I. Dispoziţii generale

1. Prezentul Regulament este elaborat în conformitate cu Legea nr. 264-XV din 15 iulie 2004 cu privire la documentul electronic şi semnătura digitală, Hotărîrea Guvernului nr. 945 din 5 septembrie 2005 "Cu privire la centrele de certificare a cheilor publice" şi stabileşte procedura de înregistrare a centrelor de certificare a cheilor publice (în continuare - centre de certificare) la organul abilitat prin lege cu elaborarea şi promovarea politicii de stat şi cu exercitarea controlului în domeniul aplicării semnăturii digitale - Serviciul de Informaţii şi Securitate al Republicii Moldova (în continuare - organ competent).

2. Pentru prestarea serviciilor de certificare a cheilor publice şi altor servicii ce ţin de semnătura digitală, centrele de certificare urmează să treacă procedura de înregistrare la organul competent şi să certifice cheia publică a persoanei împuternicite a centrului în centrul de certificare ierarhic superior.

3. Evidenţa centrelor de certificare se efectuează în cadrul Registrului de stat al unităţilor de drept şi Registrului centrelor de certificare a cheilor publice.

II. Depunerea cererii de înregistrare a centrului de certificare

4. Pentru înregistrarea centrului de certificare se prezintă următoarele documente:

a) cererea de înregistrare conform modelului prevăzut în anexa nr. 1 la prezentul Regulament, în care se indică:

denumirea deplină a persoanei juridice, sediul şi forma juridică de organizare;

funcţia, numele şi prenumele conducătorului persoanei juridice, numărul buletinului de identitate, numărul de identificare al persoanei fizice (IDNP);

altă informaţie de contact (numărul de telefon, fax, adresa poştală, e-mail);

b) copia documentelor de constituire şi a certificatului de înregistrare de stat a persoanei juridice;

c) garanţia bancară sau poliţa de asigurare prevăzute la punctul 5 al prezentului Regulament (doar pentru centrele de certificare care prestează servicii de certificare a cheilor publice terţelor persoane);

d) regulamentul de funcţionare a centrului de certificare, aprobat de conducătorul persoanei juridice;

e) copia ordinului emis de conducătorul persoanei juridice cu privire la numirea angajaţilor centrului de certificare răspunzători de activitatea centrului de certificare şi a persoanelor împuternicite să semneze certificatele cheilor publice, precum şi copia actelor de identitate ale acestor persoane;

f) copia documentelor care certifică studiile şi calificările persoanelor cu funcţii de răspundere, obligaţiile funcţionale ale cărora ţin nemijlocit de prestarea serviciilor de certificare a cheilor publice;

g) planul schematic al încăperilor centrului de certificare şi ordinea de acces în încăperile cu regim special;

h) modul de păstrare a copiilor de rezervă ale registrului certificatelor cheilor publice;

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

j) copia licenţei ce atestă dreptul de a desfăşura activităţi în domeniul protecţiei criptografice a informaţiei (numai pentru centrele de certificare ce prestează servicii de certificare a cheilor publice terţelor persoane).

5. Centrul de certificare care prestează servicii de certificare a cheilor publice terţelor persoane

trebuie să dispună de resurse financiare necesare pentru repararea prejudiciului care ar putea fi cauzat titularilor certificatelor cheilor publice, utilizatorilor sau terţelor persoane în urma neîndeplinirii sau îndeplinirii neconforme de către centrul de certificare a obligaţiunilor sale.

În acest scop, centrul de certificare trebuie să prezinte în beneficiul organului competent o garanţie bancară sau o poliţă de asigurare, egală cu echivalentul în lei moldoveneşti a sumei de 20.000 euro.

6. Cererea de înregistrare şi documentele anexate la ea, redactate în limba moldovenească, se depun la sediul organului competent de către conducătorul persoanei juridice sau de către o altă persoană împuternicită. Documentele se depun în original sau în copii cu prezentarea originalelor spre verificare. Acestea pot fi însoţite şi de copii pe suport electronic.

7. Cererea de înregistrare şi documentele anexate la ea se primesc conform borderoului a cărui copie se expediază (înmînează) solicitantului, cu menţiunea privind data primirii documentelor, autentificată prin semnătura persoanei responsabile.

III. Examinarea cererii de înregistrare a centrului de certificare

8. Pe baza documentelor specificate la punctul 4 al prezentului Regulament, organul competent, în termen de pînă la 15 zile, efectuează un control privind respectarea de către centrul de certificare a cerinţelor în domeniul semnăturii digitale.

9. În cadrul examinării cererii de înregistrare, organul competent este abilitat să verifice autenticitatea documentelor anexate la cererea de înregistrare.

10. Interesele persoanei juridice care a depus cerere de înregistrare sînt reprezentate de către conducătorul persoanei juridice sau de către alte persoane împuternicite în modul stabilit.

11. Pe baza rezultatelor examinării cererii de înregistrare, organul competent întocmeşte un aviz.

IV. Luarea deciziei de înregistrare a centrului de certificare

12. În urma controlului privind respectarea cerinţelor în domeniul semnăturii digitale şi pe baza avizului întocmit, conducătorul organului competent adoptă decizia privind înregistrarea sau refuzul de a înregistra centrul de certificare.

13. În cazul adoptării deciziei privind înregistrarea, centrului de certificare i se eliberează, în termen de 5 zile lucrătoare, certificatul de înregistrare conform modelului prevăzut în anexa nr. 2 la prezentul Regulament.

14. Copia certificatului de înregistrare a centrului de certificare se transmite Ministerului Dezvoltării Informaţionale pentru înscrierea centrului de certificare în Registrul de stat al unităţilor de drept.

15. Decizia privind refuzul înregistrării trebuie să conţină motive întemeiate de refuz şi referinţe obligatorii la actele legislative şi normative care au fost încălcate. Decizia se comunică solicitantului înregistrării în termen de 5 zile lucrătoare.

16. Refuzul înregistrării nu poate împiedica depunerea repetată a documentelor în vederea înregistrării, dacă au fost înlăturate cauzele care au servit drept temei pentru refuzul înregistrării.

17. Decizia privind refuzul înregistrării poate fi atacată în instanţa de contencios administrativ competentă.

18. Centrul de certificare se consideră înregistrat din ziua emiterii certificatului de înregistrare.

19. În caz de modificare a documentelor specificate la punctul 4 al prezentului Regulament, centrul de certificare, în termen de 10 zile lucrătoare, prezintă documentele respective organului competent.

V. Examinarea cererii de eliberare a duplicatului certificatului de înregistrare

20. În caz de pierdere a certificatului de înregistrare, centrului de certificare i se eliberează un duplicat al certificatului în termen de 5 zile lucrătoare de la data depunerii cererii corespunzătoare.

21. Organul competent eliberează duplicatul certificatului de înregistrare după prezentarea următoarelor documente:

a) cererea de eliberare a duplicatului certificatului de înregistrare, semnată de către conducătorul persoanei juridice;

b) copia anunţului privind pierderea originalului certificatului de înregistrare, publicat în Monitorul Oficial al Republicii Moldova.

22. Cererea de eliberare a duplicatului certificatului de înregistrare se examinează în termen de 3 zile lucrătoare.

23. În urma examinării cererii de eliberare a duplicatului certificatului de înregistrare se întocmeşte un aviz, pe baza căruia conducătorul organului competent adoptă decizia privind eliberarea sau refuzul de eliberare a duplicatului.

24. Decizia motivată privind refuzul de eliberare a duplicatului certificatului se comunică solicitantului în scris.

25. La întocmirea duplicatului certificatului de înregistrare se face menţiunea "duplicat".

26. Copia duplicatului eliberat, precum şi materialele care au servit drept temei pentru eliberarea acestuia se anexează la dosarul de înregistrare.

VI. Păstrarea documentelor referitoare la înregistrarea centrelor de certificare

27. Materialele referitoare la înregistrarea centrelor de certificare se păstrează în dosare separate, care vor conţine documentele specificate la punctul 4 din prezentul Regulament, însoţite de copia certificatului de înregistrare.

28. În dosarele de înregistrare se anexează, de asemenea, toată corespondenţa ulterioară cu centrul de certificare în cauză, precum şi documente referitoare la controalele efectuate.

29. Dosarele de înregistrare se păstrează în arhiva organului competent pe o durată prevăzută de legislaţia în vigoare.

30. Organul competent eliberează, la solicitarea persoanelor abilitate şi în limitele prevăzute de legislaţie, informaţii şi copii de pe documentele din dosarul de înregistrare.

VII. Registrul centrelor de certificare a cheilor publice

31. Pe baza deciziei privind înregistrarea centrului de certificare, acestuia i se atribuie un număr de înregistrare şi este înscris în Registrul centrelor de certificare a cheilor publice.

32. Numărul de înregistrare este compus din 7 cifre, aabbccc, astfel:

aa - nivelul de ierarhie al centrului de certificare;

bb - anul înregistrării;

ccc - numărul de ordine.

33. Deţinător al Registrului centrelor de certificare a cheilor publice este organul competent, iar registrator al acestuia - Centrul de certificare a cheilor publice de nivel superior.

34. În Registrul centrelor de certificare a cheilor publice se efectuează stocarea şi actualizarea următoarelor date:

a) denumirea completă a persoanei juridice, numărul de identificare al unităţii de drept (IDNO), codul fiscal;

b) numele, prenumele şi telefonul conducătorului persoanei juridice;

c) denumirea, numărul şi data de înregistrare a centrului de certificare;

d) sediul, telefonul, faxul centrului de certificare;

e) numele, prenumele, telefonul, adresa poştală electronică a conducătorului şi persoanelor împuternicite ale centrului de certificare;

f) informaţii despre modificările şi completările operate în documentele specificate la punctul 4 al prezentului Regulament;

g) data şi cauza încetării activităţii centrului de certificare;

h) alte date tehnice.

35. Registrul centrelor de certificare a cheilor publice se ţine în conformitate cu cerinţele prevăzute de Legea cu privire la registre.

36. Centrele de certificare sînt obligate să informeze organul competent, în termen de 10 zile, despre modificările sau completările datelor ce se conţin în Registrul centrelor de certificare a cheilor publice.

37. Informaţia despre centrele de certificare înregistrate, precum şi despre cele a căror activitate a încetat se publică de către organul competent pe pagina sa oficială în reţeaua Internet.

Anexa nr. 1
la Regulamentul privind procedura
de înregistrare a centrelor
de certificare a cheilor publice

Model
Serviciului de Informaţii şi
Securitate al Republicii Moldova

CERERE
de înregistrare a centrului de certificare a cheilor publice

Prin prezenta, în conformitate cu pct. 7 al Regulamentului cu privire la modul de creare şi organizare a activităţii centrelor de certificare a cheilor publice, aprobat prin Hotărîrea Guvernului nr. 945 din 5 septembrie 2005,

_____
_____,
(denumirea completă a persoanei juridice, IDNO)
în persoana _____
_____
(funcţia, numele, prenumele conducătorului persoanei juridice,
_____,
numărul buletinului de identitate, IDNP)
solicită înregistrarea centrului de certificare a cheilor publice cu următoarele date:
Denumirea centrului de certificare: _____
Nivelul în structura ierarhică a centrelor de certificare: _____
Sediul: _____
Informaţiile de contact ale persoanei juridice:
telefon _____
fax _____
adresa poştală _____
e-mail _____
"____"_____ 200_ _____
(semnătura)

Anexa nr. 2
la Regulamentul privind procedura
de înregistrare a centrelor
de certificare a cheilor publice

Modelul certificatului de înregistrare
a centrului de certificare a cheilor publice

OSIS13A2.doc

Aprobat:
Serviciul de Informaţii şi
Securitate al Republicii Moldova
Ordinul nr. 13 din 3 aprilie 2006
din 21 iunie 2006
_____ Ion URSU

Înregistrat:
Ministerul Justiţiei
al Republicii Moldova
nr. de înregistrare 452

_____ 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;

protecţia tehnică şi criptografică a informaţiei - protecţia informaţiei cu aplicarea metodelor matematice (criptografice) speciale, a mijloacelor de program, tehnice, tehnico-aplicative sau de alt gen, precum şi a procedurilor tehnico-organizatorice;

protecţia informaţiei de scurgeri - ansamblu de măsuri îndreptate spre prevenirea răspîndirii neautorizate a informaţiei protejate prin canalele tehnice sau prin canalele secundare cu ajutorul mijloacelor tehnice speciale;

protecţia informaţiei contra accesului neautorizat - ansamblu de măsuri orientate spre prevenirea obţinerii informaţiei protejate de către subiectul interesat, cu încălcarea drepturilor sau regulilor de acces la informaţia protejată stabilite de actele juridice sau de proprietarul (deţinătorul) informaţiei;

protecţia informaţiei contra acţiunilor neintenţionate - ansamblu de măsuri orientate spre prevenirea acţiunilor neintenţionate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informaţiei, dar care duc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie,

precum şi la pierderea, distrugerea acesteia sau la defectarea suportului material al informaţiei;

politica de securitate - totalitatea deciziilor documentate de administrare, îndreptate spre protejarea informaţiei, a mijloacelor tehnice şi de program ale sistemelor informaţionale.

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 informaţională şservicii informaţionale e-mail, VPN (Virtual Private Network), web etc.î;

c) fixarea timpului de iniţiere 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 valabilităţii certificatului cheii publice a persoanei fizice;

d) restabilirea valabilităţii certificatului cheii publice a persoanei fizice;

e) revocarea certificatului cheii publice a persoanei fizice;

f) publicarea certificatelor cheilor publice;

g) distribuirea informaţiei 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. Cerinţele generale referitoare la centrul de certificare

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

11. Centrul de certificare trebuie să utilizeze mijloace de semnătură digitală care posedă certificat de conformitate, eliberat conform prevederilor legislaţiei 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 condiţiile necesare pentru asigurarea securităţii 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 confidenţialitatea 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 cerinţelor de securitate stabilite.

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

18. Regulamentul centrului de certificare trebuie să conţină:

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

b) funcţiile, obligaţiile şi drepturile centrului de certificare;

c) drepturile şi obligaţiile utilizatorilor semnăturii digitale;
d) obligaţiile financiare ale centrului de certificare;
e) responsabilităţile părţilor;
f) activităţile tehnico-organizatorice de bază de asigurare a securităţii centrului de certificare, inclusiv politica de confidenţialitate;
g) procedurile centrului de certificare;
h) ordinea de publicare şi distribuire a informaţiei;
i) modalitatea de accesare a resurselor informaţionale ale centrului de certificare;
j) modul de arhivare a informaţiei documentate;
k) procedurile de gestionare a cheilor persoanelor împuternicite ale centrului de certificare;
l) algoritmul acţiunilor 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 soluţionare a situaţiilor litigioase în domeniul aplicării semnăturii digitale;
s) ordinea de înştiinţare a utilizatorilor semnăturii digitale privind politica de certificare şi despre conţinutul 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 informaţiei de înregistrare a utilizatorilor semnăturii digitale cu excepţia informaţiei 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 confidenţialitate în cazul operării cu informaţia încredinţată sau care a devenit cunoscută centrului de certificare în activitatea sa trebuie să asigure:
a) limitarea numărului persoanelor cu funcţii de răspundere cu drept de acces la informaţia confidenţială;
b) ordinea de admitere controlată a persoanelor cu funcţii de răspundere la realizarea activităţilor legate de informaţia confidenţială;
c) delimitarea funcţională a responsabilităţilor persoanelor cu funcţii de răspundere;
d) identificarea şi autentificarea utilizatorilor semnăturii digitale cu utilizarea mijloacelor moderne de autentificare şi a protocoalelor criptografice;
e) delimitarea accesului subiecţilor la diferite obiecte şi/sau la funcţiile speciale ale centrului de certificare pe baza identificării subiecţilor şi a delimitării funcţionale a acestora;
f) securitatea păstrării, prelucrării şi transmisiei informaţiei confidenţiale prin intermediul canalelor de comunicaţii.

22. Centrul de certificare trebuie sa asigure administrarea accesului subiecţilor la diferite obiecte şi/sau la funcţiile speciale ale centrului de certificare pe baza identificării subiecţilor şi a delimitării funcţionale 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 informaţiei prezentate în cerere;

c) corespunderea informaţiei 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 terţe.

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 confidenţialitatea mesajelor.

39. Centrul de certificare trebuie sa asigure protecţia informaţiei confidenţiale a titularilor certificatelor cheilor publice.

Secţiunea a 2-a. Cerinţele faţă 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 informaţiei care se conţine 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.

Secţiunea a 3-a. Cerinţele faţă de procedurile de suspendare şi restabilire a valabilităţii 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 valabilităţii 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 intenţia de a suspenda, restabili valabilitatea sau de a revoca certificatul său al cheii publice, precum şi proceduri de confirmare a valabilităţii cererii de suspendare, restabilire a valabilităţii 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 confidenţialitatea cheii private a titularului certificatului sau informaţia înscrisă în certificatul cheii publice nu corespunde realităţii.

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

53. Suspendarea, restabilirea valabilităţii şi revocarea certificatului cheii publice se efectuează de către administratorul certificare sub supravegherea obligatorie a administratorului securitate sau a altei persoane cu funcţii 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 valabilităţii 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 valabilităţii sau revocarea certificatului.

Secţiunea a 4-a. Cerinţele faţă de procedurile de publicare a certificatelor cheilor publice şi distribuire a informaţiei 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 terţe 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 informaţia referitoare la statutul certificatelor cheilor publice.

63. Centrul de certificare trebuie să prezinte informaţia 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 abonaţi (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 terţe 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 înştiinţări a utilizatorilor.

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

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

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

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

V. Cerinţele referitoare la infrastructura centrului de certificare

Secţiunea 1. Cerinţele referitoare la încăperi

71. Încăperile centrului de certificare trebuie să asigure funcţionarea stabilă a complexului tehnic de program, a sistemelor de telecomunicaţii şi a altor componente tehnice, a sistemelor de energie electrică, termică şi de apeduct, de aer condiţionat, antiincendiare, să asigure protecţia 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 cerinţelor normelor de igienă, securitate a muncii şi protecţie a mediului înconjurător, stabilite de legislaţia în vigoare.

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

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 conţin: copiile de rezervă ale registrului certificatelor cheilor publice, copiile de rezervă ale resurselor de sistem şi de program, cheile private ale angajaţilor 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 condiţiilor de maximă securitate, stabilite de prezentele condiţii speciale, pentru asigurarea securităţii fizice şi protecţiei tehnice a informaţiei;

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 instalaţiilor cu sisteme autonome de semnalizare şi stingere a incendiilor" şi NCM.E.03.05-2004 "Instalaţii autonome de stingere şi semnalizare a incendiilor. Normativ pentru proiectare";

c) să corespundă cerinţelor în vigoare în Republica Moldova privind proiectarea şi exploatarea reţelei 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 funcţionarea mijloacelor tehnice principale pentru o perioadă de cel puţin 30

minute din momentul stopării furnizării energiei electrice de la sursa de bază;

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

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

Secţiunea a 2-a. Cerinţele referitoare la complexul tehnic de program

77. Complexul tehnic de program al centrului de certificare trebuie să asigure executarea de către centru a funcţiilor 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 cerinţelor stabilite de asigurare a securităţii.

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

80. Fiecare mijloc tehnic trebuie să fie înregistrat şi testat în privinţa posibilităţii de utilizare şi fiecare mijloc tehnic sau de program trebuie să fie însoţit de documentaţia tehnică.

81. Capacitatea de funcţionare 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 posibilităţi de reparare. Pentru dispozitivele ce necesită deservire tehnică periodică trebuie elaborate instrucţiuni şi grafice de deservire tehnică. Toate echipamentele şi dispozitivele de control-măsurare trebuie întreţinute în condiţii ce asigură integritatea acestora.

83. Complexul tehnic de program al centrului de certificare trebuie să asigure posibilitatea copierii de rezervă şi păstrării informaţiei critice pentru activitatea centrului de certificare, restabilirii operative şi complete a informaţiei 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 licenţiat 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 configuraţiilor echipamentului, ale setărilor de sistem, ale algoritmilor de funcţionare a mijloacelor de program, modificarea fluxurilor informaţionale sau proceselor susţinute.

Secţiunea a 3-a. Cerinţele referitoare la personal

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

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

88. Pentru fiecare specialist al centrului de certificare trebuie definite condiţiile concrete privind nivelul de studii, de cunoştinţe tehnice şi experienţă de lucru. De asemenea vor fi stabilite obligaţiile de serviciu, funcţiile, drepturile, responsabilităţile şi cerinţele faţă de regimul de confidenţialitate.

89. Fiecare angajat al centrului de certificare este obligat să cunoască şi să îndeplinească obligaţiile sale de serviciu, periodic să-şi sporească nivelul de calificare, să studieze profesiile complementare profilului activităţii 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 activităţilor specifice, centrul de certificare poate implica angajaţi ai altor organizaţii, cu asigurarea cerinţelor 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 informaţionale;

e) să asigure capacitatea centrului de certificare de a continua activitatea în cazuri excepţionale sau alte situaţii critice (asigurarea continuităţii activităţii centrului de certificare).

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

a) subsistemul de protecţie criptografică a informaţiei, care include mijloacele de protecţie criptografică a informaţiei;

b) subsistemul de protecţie a informaţiei contra accesului neautorizat;

c) subsistemul de audit activ al securităţii informaţionale a centrului;

d) subsistemul de detectare a intruziunilor;

e) subsistemul de protecţie a informaţiei contra acţiunilor neintenţionate, inclusiv subsistemul de copiere de rezervă şi arhivare a datelor;

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

g) subsistemul de asigurare a accesibilităţii, inclusiv subsistemul de asigurare a continuităţii funcţionării complexului tehnic de program al centrului de certificare;

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

i) subsistemul securităţii fizice.

106. Centrul de certificare trebuie să elaboreze condiţiile de asigurare a securităţii proprii, criteriile şi indicatorii de evaluare a nivelului de securitate, în concordanţă cu care realizează activităţi şi implementează mijloace concrete de protecţie a informaţiei.

107. Orice funcţie a centrului de certificare poate fi delegată persoanelor terţe numai în condiţiile 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 funcţionarea securizată a centrului de certificare.

109. Orice situaţie de forţă majoră care poate influenţa în mod negativ realizarea procedurilor obligatorii ale centrului de certificare trebuie adusă la cunoştinţa 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 securităţii informaţionale a centrului de certificare, ansamblul de măsuri pentru asigurarea acesteia, responsabilităţile angajaţilor şi mecanismele de control al stării securităţii informaţionale.

111. Politica de securitate trebuie să asigure respectarea regulilor, standardelor şi normelor general acceptate în domeniul securităţii informaţionale 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 informaţionale şi de telecomunicaţii;

c) modelul de securitate a centrului de certificare;

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

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

f) condiţii impuse mijloacelor tehnice de protecţie a informaţiei;

g) enumerarea mijloacelor tehnice de protecţie a informaţiei;

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

i) responsabilităţile personalului centrului de certificare privind asigurarea securităţii;

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

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

l) înştiinţarea 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 protecţie a informaţiei etc.) din punctul de vedere al riscurilor, să planifice şi să realizeze activităţi de minimizare şi evitare a riscurilor depistate.

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

115. Centrul de certificare trebuie să elaboreze şi să aprobe planul de acţiuni pentru asigurarea continuităţii activităţii, plan care va fi analizat şi revizuit periodic pe baza analizei activităţii curente şi rezultatelor testării în diferite situaţii excepţionale posibile.

Secţiunea a 2-a. Cerinţele de asigurare a securităţii fizice

116. Centrul de certificare trebuie să creeze şi să menţină sistemul de securitate fizică care să asigure protecţia infrastructurii, a resurselor informaţionale şi a personalului centrului, să fie flexibil în cazul modificării cerinţelor de securitate înaintate, să permită adăugarea de noi funcţionalităţi 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 informaţiei;

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

e) înştiinţarea şi asigurarea conexiunii în caz de situaţii excepţionale.

118. Centrul de certificare trebuie să stabilească şi să precizeze responsabilităţile angajaţilor legate de asigurarea securităţii fizice.

119. Informaţia privind amplasarea subsistemelor complexului tehnic de program al centrului de certificare este confidenţială.

120. Echipamentul special şi tehnic de inginerie, protecţia şi regimul de acces în încăperile speciale ale centrului de certificare trebuie să asigure securitatea informaţiei confidenţiale 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 angajaţilor centrului de certificare în încăperile speciale se efectuează conform instrucţiunilor 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. Angajaţii centrului de certificare care au acces în încăperile speciale poartă răspundere personală pentru permiterea accesului persoanelor terţe 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 efracţiei, 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 protecţia lor contra accesului neautorizat, furt, incendii, inundaţii, 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 existenţei balcoanelor, scărilor antiincendiare etc., la ferestrele încăperilor respective trebuie să fie instalate gratii din interior.

Secţiunea a 3-a. Cerinţele referitoare la asigurarea securităţii sistemelor informaţionale şi de telecomunicaţii

130. Pentru micşorarea riscurilor legate de utilizarea tehnologiilor informaţionale şi de telecomunicaţii, centrul de certificare elaborează şi implementează un set de măsuri de asigurare a securităţii sistemelor sale informaţionale şi de telecomunicaţii (mijloace de program şi tehnice, canale de telecomunicaţii, echipament de reţea, informaţii prelucrate, depozitate şi transmise), prin funcţionarea următoarelor subsisteme de securitate:

a) subsistemul de gestiune a accesului;

b) subsistemul de înregistrare şi evidenţă (audit);

c) subsistemul de asigurare a integrităţii;

d) subsistemul de asigurare a accesibilităţii;

e) subsistemul de protecţie criptografică.

131. Subsistemul de gestiune a accesului:

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

b) efectuează verificarea identităţii subiecţilor ce obţin acces la componentele sistemelor informaţionale;

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

d) gestionează fluxurile informaţionale şi aplică sigla de confidenţialitate;

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

132. Subsistemul de înregistrare şi evidenţă:

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 aplicaţiilor şi a proceselor destinate să prelucreze resursele protejate conform următorilor parametri:

data şi timpul tentativei de lansare;

denumirea (identificatorul) aplicaţiei sau procesului;

identificatorul subiectului de acces;

rezultatul tentativei de lansare - succes sau eşec;

c) înregistrează tentativele de obţinere a drepturilor de acces (de executare a operaţiilor) pentru aplicaţii şi procese la resursele protejate conform următorilor parametri:

data şi timpul tentativei de obţinere a accesului (executare a operaţiei);

denumirea (identificatorul) aplicaţiei sau procesului;

identificatorul subiectului de acces;

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

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

rezultatul tentativei de obţinere a accesului (executare a operaţiei) - succes sau eşec;

d) înregistrează tentativele de acces neautorizat al subiecţilor în sistem, tentativele de lansare neautorizată a aplicaţiilor (proceselor) sau de executare a operaţiilor, asigurînd blocarea tuturor operaţiunilor neautorizate şi înştiinţînd despre acest fapt administratorul securitate;

e) înregistrează modificările drepturilor de acces al subiecţilor 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 specificaţiile obiectului de acces şi noul său statut;

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

data şi timpul ieşirilor de date;

denumirea informaţiei şi calea spre ea;

specificaţiile dispozitivului ce a eliberat informaţia (numele logic);

identificatorul subiectului de acces care a solicitat informaţia;

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

g) ţine evidenţa resurselor protejate ale centrului de certificare, înregistrează intrarea/ieşirea suporturilor materiale ce conţin informaţie confidenţială;

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

i) identifică şi arată evenimentele curente.

133. Subsistemul de asigurare a integrităţii menţine stabilitatea mediului aplicativ, integritatea informaţiei prelucrate, a mijloacelor tehnico-aplicative şi a mijloacelor de protecţie a informaţiei.

134. Subsistemul de asigurare a accesibilităţii:

a) asigură funcţionarea continuă a sistemelor informaţionale şi de telecomunicaţii ale centrului de certificare;

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

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

135. Subsistemul de protecţie criptografică:

a) realizează criptarea informaţiei confidenţiale în sistemul informaţional şi în canalele de telecomunicaţii;

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

136. Arhitectura sistemelor informaţionale şi de telecomunicaţii ale centrului de certificare şi a subsistemelor acestora trebuie să fie destul de flexibilă, să permită dezvoltarea simplă, fără

modificări structurale, a configuraţiilor mijloacelor utilizate şi completarea de noi funcţii şi resurse.

137. Sistemele informaţionale şi de telecomunicaţii ale centrului de certificare trebuie să fie însoţite de documentaţie care să asigure exploatarea lor calificată.

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

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

140. Centrul de certificare trebuie să asigure protecţia sistemelor informaţionale şi de telecomunicaţii proprii contra acţiunilor aplicaţiilor malefice (sistemul de protecţie antivirus).

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

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 informaţionale şi de telecomunicaţii.

143. Accesul angajaţilor centrului de certificare la resursele sistemelor informaţionale şi de telecomunicaţii trebuie să fie acordat pe baza instrucţiunilor 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 informaţionale şi de telecomunicaţii noi sau modernizate, componentele acestora, mijloacele tehnice şi de program trebuie să fie implementate numai în conformitate cu procedurile stabilite, cu respectarea cerinţelor privind asigurarea securităţii informaţionale.

146. Centrul de certificare trebuie să elaboreze şi să aprobe instrucţiuni de implementare a sistemelor informaţionale şi de telecomunicaţii 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 funcţionalitatea şi regulile de administrare (exploatare) a sistemelor informaţionale şi de telecomunicaţii, a componentelor, a mijloacelor tehnice şi de program noi sau modernizate.

148. Toate modificările de configurare a sistemelor informaţionale şi de telecomunicaţii în ansamblu, a componentelor acestora, a mijloacelor tehnice şi de program trebuie să fie testate pînă la implementarea acestora în mediul operaţional. 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 informaţional şi de telecomunicaţii, 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 informaţiei confidenţiale şi de scurgere a informaţiei la utilizarea MPCI.

157. Angajaţii subdiviziunii de protecţie 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 documentaţiei tehnice şi de exploatare aferentă acestor mijloace, pe baza instrucţiunilor aprobate, precum şi în conformitate cu prezentele condiţii speciale.

159. Instrucţiunile ce reglementează modul de exploatare în siguranţă a MPCI trebuie să prevadă:

a) drepturile şi obligaţiile angajaţilor centrului de certificare ce exploatează MPCI;

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

c) ordinea de creare, evidenţă, 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 consecinţelor;

e) ordinea de control al respectării cerinţelor de asigurare a protecţiei informaţiei cu ajutorul MPCI.

160. Condiţiile 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 funcţionare.

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

163. În caz de necesitate, pentru asigurarea integrităţii cheilor criptografice pot fi create copii de rezervă, care se păstrează conform normelor stabilite de asigurare a protecţiei contra accesului neautorizat şi acţiunilor neintenţionate.

164. Angajaţii centrului de certificare poartă răspundere personală pentru integritatea şi

securitatea cheilor criptografice.

165. Subdiviziunea de protecţie criptografică ţine evidenţa suporturilor materiale de chei criptografice.

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

167. Distrugerea cheilor criptografice se efectuează prin distrugerea fizică a suportului material sau prin distrugerea garantată a informaţiei-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 protecţie criptografică efectuează toate acţiunile de verificare a acestui fapt şi înlăturare a urmărilor.

Secţiunea a 5-a. Condiţiile de protecţie tehnică a informaţiei

170. Centrul de certificare asigură protecţia informaţiei confidenţiale prin utilizarea tehnologiilor şi a mijloacelor speciale de prevenire a scurgerii informaţiei prin canalele tehnice.

171. Centrul de certificare trebuie să excludă prezenţa 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 informaţiei 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 părţilor ecranului: pereţi, tavan, podea, ferestre şi uşi. Materialul pentru uşi trebuie să posede un contact electric sigur cu ecranul încăperii pe toată suprafaţa, construcţiile de ecranare trebuie să posede prize de pămînt care să fie amplasate în regiunea controlată.

174. Centrul de certificare trebuie să asigure protecţia informaţiei contra scurgerii prin intermediul reţelei electrice şîncrucişarea reţelelor electrice ale obiectului cu instalarea filtrelor de protecţie care să blocheze (bruieze) semnalulî.

175. În încăperile centrului de certificare unde sînt amplasate mijloacele tehnice ce prelucrează informaţie confidenţială 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 distanţă de cel puţin de 3 metri de la mijloacele tehnice principale ale complexului tehnic de program al centrului de certificare.

177. Suficienţa măsurilor de protecţie 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.

Secţiunea a 6-a. Condiţiile referitoare la asigurarea securităţii resurselor informaţionale

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

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

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

181. Centrul de certificare trebuie să ia măsuri de protecţie a datelor personale conform legislaţiei Republicii Moldova.

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

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

Secţiunea 1. Condiţiile 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 condiţii:

a) să creeze (numească) o subdiviziune pentru realizarea funcţiilor 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 condiţiilor referitoare la încăperile centrului de certificare stabilite în prezentele condiţii speciale;

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

g) să creeze o subdiviziune (să numească un angajat) responsabilă de protecţia criptografică a informaţiei 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 continuităţii activităţii centrului de certificare;

procedurile de restabilire a activităţii centrului de certificare;

instrucţiuni ce reglementează securitatea şi exploatarea MPCI;

regulamentul privind efectuarea auditului intern al centrului de certificare.

i) să obţină o garanţie bancară la o bancă înregistrată pe teritoriul Republicii Moldova sau o poliţă 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 termenului 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 iniţiativa persoanei juridice care a creat centrul de certificare;

b) la iniţiativa 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 anunţe organul competent şi centrul de certificare ierarhic superior despre decizia de lichidare a centrului de certificare în termen de cel puţin de 30 de zile pînă la momentul lichidării.

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

218. Procedura de lichidare a centrului de certificare la iniţiativa persoanei juridice care a creat centrul de certificare se iniţiază 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 iniţiativa organului competent este efectuată pe cale judiciară în baza încheierii organului competent privind încălcarea legislaţiei în domeniul semnăturii digitale. După pronunţarea hotărîrii instanţei de judecată, prin ordinul conducătorului organului competent, se creează comisia de lichidare.

221. În componenţa 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 confidenţialitatea în conformitate cu cerinţele 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 legislaţia în vigoare.

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

Aprobat:	Înregistrat:
Serviciul de Informaţii şi	Ministerul Justiţiei
Securitate al Republicii Moldova	al Republicii Moldova
Ordinul nr. 13 din 3 aprilie 2006	nr. de înregistrare 452
din 21 iunie 2006	
_____ Ion URSU	_____ Victoria IFTODI

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

REGULAMENTUL
Centrului de certificare a cheilor publice de nivel superior
I. Dispoziţii generale

1. Prezentul Regulament este elaborat în temeiul Legii nr. 264-XV din 15 iulie 2004 cu privire la documentul electronic şi semnătura digitală şi al Hotărîrii Guvernului nr. 945 din 5 septembrie 2005 "Cu privire la centrele de certificare a cheilor publice".

2. Regulamentul stabileşte condiţiile generale de organizare a activităţii Centrului de certificare a cheilor publice de nivel superior (în continuare - Centrul de certificare), precizează funcţiile, obligaţiile şi drepturile acestuia, mecanismul şi procedurile aplicate de către Centrul de certificare la administrarea infrastructurii ierarhice unice a cheilor publice (Public Key Infrastructure, PKI), precum şi modul de conlucrare cu centrele de certificare şi cu utilizatorii semnăturii digitale, măsurile tehnico-organizatorice de bază pentru asigurarea securităţii.

3. Regulamentul Centrului de certificare a cheilor publice de nivel superior este un act normativ în domeniul aplicării semnăturii digitale, obligatoriu pentru toate persoanele fizice şi juridice ce utilizează semnătura digitală sau desfăşoară activităţi în domeniul semnăturii digitale.

4. Centrul de certificare este o subdiviziune structurală a Serviciului de Informaţii şi Securitate care îşi desfăşoară activitatea în domeniul protecţiei criptografice şi tehnice a informaţiei.

5. Conducătorul Centrului de certificare se numeşte în funcţie prin ordinul directorului Serviciului de Informaţii şi Securitate.

II. Funcţiile, obligaţiile şi drepturile Centrului de certificare

6. Centrul de certificare îndeplineşte următoarele funcţii:

a) certifică cheile publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

b) suspendă şi restabileşte valabilitatea, revocă certificatele cheilor publice emise de către Centrul de certificare;

c) întocmeşte şi gestionează registrul certificatelor cheilor publice ale persoanelor împuternicite ale Centrului de certificare şi ale centrelor de certificare de nivelul al doilea (în continuare - Registrul certificatelor cheilor publice);

d) confirmă autenticitatea şi valabilitatea certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea.

7. Pentru îndeplinirea funcţiilor sale, Centrul de certificare:

a) asigură crearea şi eliberarea certificatelor cheilor publice pe baza cererii persoanelor împuternicite ale centrelor de certificare de nivelul al doilea, sub formă de document electronic şi sub formă de document pe suport de hîrtie, în conformitate cu procedurile stabilite de prezentul Regulament;

b) suspendă şi restabileşte valabilitatea, revocă certificatele cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea în cazurile şi în conformitate cu procedurile stabilite de prezentul Regulament;

c) ţine evidenţa centrelor de certificare de nivelul al doilea;

d) gestionează Registrul certificatelor cheilor publice sub formă de documente pe suport de hîrtie şi sub formă de documente electronice;

e) asigură conlucrarea cu centrele de certificare de nivelul al doilea în cadrul infrastructurii ierarhice unice a cheilor publice;

f) acordă consultaţii şi suport metodologic persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

g) confirmă autenticitatea şi valabilitatea certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

h) confirmă autenticitatea şi valabilitatea certificatelor cheilor publice emise de către centrele

de certificare de nivelul al doilea, în cazurile prevăzute de prezentul Regulament;

i) desfăşoară activitatea în domeniul protecţiei criptografice şi tehnice a informaţiei;

j) creează sistemele informaţionale şi de telecomunicaţii ale Centrului de certificare, asigură funcţionarea, securitatea, deservirea şi modernizarea lor, efectuează auditul intern permanent al securităţii şi funcţionalităţii acestor sisteme.

8. Centrul de certificare este obligat:

să-şi desfăşoare activitatea în strictă conformitate cu legislaţia şi cerinţele stabilite de organul abilitat cu elabo-rarea şi promovarea politicii de stat şi cu exercitarea controlului în domeniul aplicării semnăturii digitale (în continuare - organul competent);

să utilizeze mijloacele semnăturii digitale ce dispun de certificatul de conformitate eliberat în conformitate cu legislaţia în vigoare;

să utilizeze mijloacele semnăturii digitale în conformitate cu documentaţia de exploatare;

să organizeze regimul interior de funcţionare a Centrului de certificare astfel încît să se excludă posibilitatea accesului persoanelor terţe la mijloacele semnăturii digitale, la modificarea şi utilizarea lor neautorizată;

să asigure securitatea cheilor private ale persoanelor împuternicite ale Centrului de certificare şi ale altor angajaţi, să creeze condiţiile necesare pentru excluderea accesului neautorizat la cheile private;

să administreze suporturile materiale de chei private în conformitate cu cerinţele stabilite de organul competent;

să utilizeze cheia privată a persoanei împuternicite a Centrului de certificare numai la semnarea certificatelor cheilor publice eliberate de acesta şi a listelor certificatelor revocate;

să creeze certificatul cheii publice a persoanei împuternicite a Centrului de certificare şi lista certificatelor revocate în conformitate cu cerinţele stabilite de organul competent şi de prezentul Regulament;

să nu utilizeze cheia privată pentru crearea semnăturii digitale dacă există dovezi (suspiciuni) că a fost încălcată confidenţialitatea cheii private;

să suspende imediat valabilitatea certificatului cheii publice a persoanei împuternicite a Centrului de certificare dacă există dovezi (suspiciuni) că a fost încălcată confidenţialitatea cheii private, precum şi în cazul în care informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;

să revoce certificatul cheii publice a persoanei împuternicite a Centrului de certificare în cazul constatat de încălcare a confidenţialităţii cheii private sau de neconcordanţă realităţii a informaţiilor cuprinse în certificatul cheii publice;

să primească cererile de certificare a cheilor publice de la persoanele împuternicite ale centrelor de certificare de nivelul al doilea în conformitate cu procedurile stabilite de prezentul Regulament;

să verifice autenticitatea datelor stipulate în cererea de certificare a cheii publice pe baza documentelor ce confirmă aceste date, să asigure conformitatea informaţiilor cuprinse în certificatul cheii publice cu informaţiile prezentate de către persoana împuternicită a centrului de certificare de nivelul al doilea;

să asigure unicitatea informaţiei de înregistrare a persoanelor împuternicite ale centrelor de certificare de nivelul al doilea în Registrul certificatelor cheilor publice;

să nu divulge informaţiile confidenţiale şi alte informaţii protejate de lege;

să verifice unicitatea cheilor publice certificate;

să asigure unicitatea numerelor de înregistrare ale certificatelor cheilor publice eliberate;

să creeze certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea, conform cerinţelor stabilite de organul competent şi de prezentul Regulament;

să introducă certificatul cheii publice în Registrul certificatelor cheilor publice nu mai tîrziu de data şi ora la care începe termenul de valabilitate a certificatului;

să elibereze certificatele cheilor publice către persoanele împuternicite ale centrelor de certificare de nivelul al doilea în conformitate cu procedurile stabilite de prezentul Regulament;

să suspende şi să restabilească valabilitatea, sau să revoce certificatul cheii publice a persoanei

împuternicite a centrului de certificare de nivelul al doilea în cazurile şi în conformitate cu procedurile stabilite de prezentul Regulament;

să înscrie datele privind certificatul cheii publice revocat sau suspendat în lista certificatelor revocate în termen de 3 ore de lucru, precizînd data, ora şi cauza revocării sau suspendării valabilităţii certificatului;

să excludă din lista certificatelor revocate datele privind certificatul cheii publice suspendat în termen de 3 ore de lucru din momentul restabilirii valabilităţii acestuia;

să înştiinţeze din timp persoana împuternicită a centrului de certificare de nivelul al doilea despre suspendarea valabilităţii sau revocarea certificatului cheii publice, în cazurile şi în conformitate cu procedurile stabilite de prezentul Regulament;

să înştiinţeze persoana împuternicită a centrului de certificare de nivelul al doilea despre suspendarea şi restabilirea valabilităţii sau revocarea certificatului cheii publice în conformitate cu procedurile stabilite de prezentul Regulament;

să înştiinţeze persoana împuternicită a centrului de certificare de nivelul al doilea despre faptele de care a luat cunoştinţă Centrul de certificare şi care pot influenţa esenţial asupra posibilităţii utilizării ulterioare a certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;

să înştiinţeze titularul certificatului cheii publice despre faptele de care a luat cunoştinţă Centrul de certificare, ce indică asupra imposibilităţii utilizării ulterioare a cheii private aparţinînd acestui titular;

să păstreze certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea, precum şi alte informaţii despre acest certificat nu mai puţin de 10 ani din momentul revocării sau expirării termenului de valabilitate a certificatului;

să asigure actualizarea Registrului certificatelor cheilor publice şi posibilitatea accesului liber la acesta al persoanelor împuternicite ale centrelor de certificare de nivelul al doilea şi utilizatorilor semnăturii digitale, să întreprindă măsurile necesare pentru asigurarea securităţii Registrului;

să pună la dispoziţia persoanelor împuternicite ale centrelor de certificare de nivelul al doilea şi utilizatorilor semnăturii digitale datele din Registrul certificatelor cheilor publice privind certificatele revocate sau suspendate;

să creeze şi să păstreze copia de rezervă a Registrului certificatelor cheilor publice în conformitate cu cerinţele stabilite de organul competent;

să asigure posibilitatea de a se determina ora şi data eliberării, suspendării valabilităţii şi revocării certificatului cheii publice;

la cererea utilizatorilor semnăturii digitale, să confirme autenticitatea şi valabilitatea certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

la cererea instanţei de judecată, a altor persoane şi organe ce dispun de acest drept în temeiul legii sau în alte cazuri prevăzute de legislaţia în domeniul aplicării semnăturii digitale, să confirme autenticitatea şi valabilitatea certificatelor cheilor publice eliberate de centrele de certificare de nivelul al doilea şi să prezinte, pe suport de hîrtie, copiile certificatelor cheilor publice incluse în Registrul certificatelor cheilor publice;

să sincronizeze activitatea serviciilor Centrului de certificare, inclusiv a mijloacelor tehnice şi de program conform destinaţiei, cu Timpul Mondial Coordonat (UTC). Se permite sincronizarea serviciilor conform Timpului Greenwich (Greenwich Mean Team, GMT), fără trecerea la ora de vară;

să amplaseze mijloacele tehnice de program, destinate pentru certificarea cheilor publice, în încăperi speciale şi să asigure securitatea acestora;

să dispună de personal care posedă calificarea necesară.

9. Centrul de certificare are dreptul:

a) să creeze certificatul cheii publice a persoanei împuternicite a Centrului de certificare şi să îndeplinească procedura de eliberare către sine a certificatului cheii publice;

b) să numească mai multe persoane împuternicite cu drepturi egale pentru semnarea

certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

c) să refuze eliberarea certificatului cheii publice către persoana împuternicită a centrului de certificare de nivelul al doilea, precizînd motivele refuzului, în cazurile:

prezentării în cererea de certificare a cheilor publice a unor informaţii ce nu corespund realităţii;

încălcării prevederilor legislaţiei în domeniul aplicării semnăturii digitale;

încălcării drepturilor persoanelor terţe în procesul întocmirii sau depunerii cererii;

d) să confirme autenticitatea şi valabilitatea certificatelor cheilor publice ale utilizatorilor semnăturii digitale;

e) să suspende valabilitatea sau să revoce certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea în cazurile şi în modul prevăzute de legislaţie şi de prezentul Regulament.

III. Organizarea activităţii Centrului de certificare

Secţiunea 1. Procedurile Centrului de certificare

10. Centrul de certificare îndeplineşte următoarele proceduri:

a) certificarea cheii publice a persoanei împuternicite a Centrului de certificare;

b) suspendarea valabilităţii certificatului cheii publice a persoanei împuternicite a Centrului de certificare;

c) revocarea certificatului cheii publice a persoanei împuternicite a Centrului de certificare;

d) certificarea cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;

e) suspendarea valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;

f) revocarea certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;

g) confirmarea autenticităţii şi valabilităţii certificatului cheii publice.

1.1. Certificarea cheii publice a persoanei împuternicite a Centrului de certificare

11. Crearea certificatului cheii publice a persoanei împuternicite a Centrului de certificare se realizează de însuşi Centrul de certificare, în temeiul împuternicirilor stabilite de legislaţia în domeniul aplicării semnăturii digitale.

12. Persoana împuternicită a Centrului de certificare creează cheia sa privată şi cea publică conform cerinţelor stabilite de organul competent.

13. Persoana împuternicită a Centrului de certificare creează certificatul cheii publice sub formă de document electronic pe care îl semnează cu cheia sa privată.

14. Certificatul cheii publice a persoanei împuternicite a Centrului de certificare sub formă de document electronic trebuie să corespundă standardului ISO/IEC 9594/8 Directory Services, standardului Uniunii Internaţionale de Telecomunicaţii ITU-T X.509, versiunea 3, şi recomandării IETF (Internet Engineering Task Force) RFC 3280 (RFC 2459).

15. După crearea certificatului cheii publice sub formă de document electronic persoana împuternicită a Centrului de certificare creează certificatul cheii sale publice sub formă de document pe suport de hîrtie, cu următorul conţinut:

a) numărul de înregistrare a certificatului cheii publice;

b) datele de identificare ale Centrului de certificare, numărul de identificare al unităţii de drept (IDNO);

c) numele şi prenumele persoanei împuternicite a Centrului de certificare - titular al certificatului cheii publice;

d) numărul de identificare al persoanei fizice - persoanei împuternicite a Centrului de certificare (IDNP);

e) denumirea Centrului de certificare şi funcţia deţinută de către persoana împuternicită a Centrului de certificare;

f) cheia publică a persoanei împuternicite a Centrului de certificare - titular al certificatului cheii publice;

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

h) datele despre algoritmul criptografic al semnăturii digitale şi alte date tehnologice stabilite de Centrul de certificare;

i) domeniile de aplicare a semnăturii digitale şi alte restricţii impuse;

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

16. Structura certificatului cheii publice a persoanei împuternicite a Centrului de certificare este prezentată în anexa nr. 1 la prezentul Regulament.

17. Certificatul cheii publice a persoanei împuternicite a Centrului de certificare pe suport de hîrtie se semnează de persoana împuternicită a Centrului de certificare, de conducătorul Centrului de certificare, se aprobă de directorul Serviciului de Informaţii şi Securitate şi se autentifică cu ştampila Serviciului.

18. Certificatul cheii publice a persoanei împuternicite a Centrului de certificare sub formă de document electronic este valabil în următoarele condiţii:

a) informaţiile cuprinse în certificat corespund informaţiilor precizate în certificatul aprobat al cheii publice pe suport de hîrtie;

b) certificatul este semnat cu cheia privată a persoanei împuternicite a Centrului de certificare, care corespunde cheii publice precizate în certificat.

19. În scopul recunoaşterii internaţionale a certificatelor cheilor publice eliberate în cadrul infrastructurii cheilor publice din Republica Moldova, se admite certificarea cheii publice a persoanei împuternicite a Centrului de certificare într-un centru de certificare de nivel internaţional.

20. Certificatul cheii publice a persoanei împuternicite a Centrului de certificare se păstrează în Registrul certificatelor cheilor publice sub formă de document pe suport de hîrtie şi sub formă de document electronic.

1.2. Suspendarea valabilităţii certificatului cheii publice a persoanei împuternicite a Centrului de certificare

21. Suspendarea valabilităţii certificatului cheii publice a persoanei împuternicite a Centrului de certificare se realizează prin decizia organului competent în cazul:

a) încălcării legislaţiei în domeniul aplicării semnăturii digitale;

b) existenţei motivelor de a presupune că a fost încălcată confidenţialitatea cheii private; sau

c) existenţei motivelor de a presupune că informaţiile cuprinse în certificatul cheii publice nu corespund realităţii.

22. Valabilitatea certificatului cheii publice a persoanei împuternicite a Centrului de certificare se suspendă prin dispoziţia directorului Serviciului de Informaţii şi Securitate, pe o durată de pînă la 30 de zile.

23. Certificatul cheii publice a persoanei împuternicite a Centrului de certificare a cărui valabilitate a fost suspendată, în termen de 3 ore de lucru, se înscrie în lista certificatelor revocate a Centrului de certificare, iar Centrul de certificare emite lista actualizată a certificatelor revocate.

24. Ora suspendării valabilităţii certificatului cheii publice a persoanei împuternicite a Centrului de certificare se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în cîmpul This Update).

25. Lista certificatelor revocate a Centrului de certificare este un document electronic şi trebuie să corespundă standardului ISO/IEC 9594/8 Directory Services, standardului Uniunii Internaţionale de Telecomunicaţii ITU-T X.509, versiunea 2, şi recomandării IETF RFC 3280 (RFC 2459).

26. Structura listei certificatelor revocate este prezentată în anexa nr. 2 la prezentul Regulament.

27. În cazul suspendării valabilităţii certificatului cheii publice a persoanei împuternicite a Centrului de certificare, prin dispoziţia directorului Serviciului de Informaţii şi Securitate, este creată comisia pentru efectuarea unei anchete de serviciu.

28. Din componenţa Comisiei fac parte:

a) reprezentanţii organului competent;

b) conducătorul Centrului de certificare;

c) alte persoane care posedă cunoştinţe şi experienţa necesară în domeniul aplicării semnăturii digitale şi întocmirii documentelor electronice.

29. Persoanele care fac parte din componenţa Comisiei trebuie să dispună de dreptul de acces la materialele documentare şi la mijloacele tehnice şi de program, necesare pentru desfăşurarea activităţii comisiei.

30. Comisia examinează, la nivel tehnico-organizatoric, împrejurările ce au dus la suspendarea valabilităţii certificatului cheii publice a persoanei împuternicite a Centrului de certificare, stabileşte cauzele şi urmările situaţiei create, identifică măsurile necesare pentru soluţionarea acesteia.

31. Durata de activitate a comisiei nu poate depăşi 30 de zile din ziua suspendării valabilităţii certificatului cheii publice a persoanei împuternicite a Centrului de certificare.

32. În termen de 5 zile pînă la expirarea termenului pe care a fost suspendată valabilitatea certificatului cheii publice a persoanei împuternicite a Centrului de certificare, comisia întocmeşte un act, indicînd împrejurările ce au dus la suspendarea valabilităţii certificatului cheii publice, cauzele şi urmările situaţiei create, măsurile necesare pentru soluţionarea acesteia şi recomandările privind restabilirea valabilităţii sau revocarea certificatului cheii publice a persoanei împuternicite a Centrului de certificare.

33. Pe baza rezultatelor stabilite de comisie, în termen de 5 zile pînă la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice a persoanei împuternicite a Centrului de certificare, prin dispoziţia directorului Serviciului de Informaţii şi Securitate se adoptă decizia privind restabilirea valabilităţii sau revocarea cheii publice a persoanei împuternicite a Centrului de certificare.

34. În cazul în care pînă la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice nu se adoptă decizia privind restabilirea valabilităţii acestuia, certificatul cheii publice se revocă.

35. Certificatul cheii publice a persoanei împuternicite a Centrului de certificare a cărui valabilitate a fost restabilită, în termen de 3 ore de lucru, va fi radiat din lista certificatelor revocate, iar Centrul de certificare va emite lista actualizată a certificatelor revocate.

36. Ora restabilirii valabilităţii certificatului cheii publice a persoanei împuternicite a Centrului de certificare se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în cîmpul This Update).

1.3. Revocarea certificatului cheii publice a persoanei împuternicite a Centrului de certificare

37. Certificatul cheii publice a persoanei împuternicite a Centrului de certificare se revocă pe baza deciziei organului competent în următoarele cazuri:

a) în cazul faptului constatat de compromitere a cheii private;

b) la depistarea unor informaţii neconforme realităţii în cererea de certificare a cheii publice sau în certificatul cheii publice;

c) la introducerea unor modificări în certificatul cheii publice;

d) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice, dacă nu a fost adoptată decizia de restabilire a valabilităţii acestuia;

e) la expirarea termenului de valabilitate a certificatului cheii publice.

38. Revocarea certificatului cheii publice a persoanei împuternicite a Centrului de certificare din motivele indicate la punctul 37 literele a) şi b) din prezentul Regulament se va face numai după suspendarea prealabilă a valabilităţii certificatului.

39. Decizia privind revocarea certificatului cheii publice a persoanei împuternicite a Centrului de certificare se perfectează prin dispoziţia directorului Serviciului de Informaţii şi Securitate.

40. Certificatul revocat al cheii publice a persoanei împuternicite a Centrului de certificare, în termen de 3 ore de lucru, se înscrie în lista certificatelor revocate, iar Centrul de certificare emite lista actualizată a certificatelor revocate.

41. Ora revocării certificatului cheii publice a persoanei împuternicite a Centrului de certificare se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în cîmpul This Update).

42. În cazul revocării certificatului cheii publice din motivul expirării termenului de valabilitate, certificatul dat nu se înscrie în lista certificatelor revocate.

43. În cazul eliberării din funcţie a persoanei împuternicite a Centrului de certificare, cheia sa privată se distruge, fără a fi încălcată confidenţialitatea acesteia, de către o comisie numită prin dispoziţia directorului Serviciului de Informaţii şi Securitate, iar certificatul cheii publice corespunzător îşi păstrează valabilitatea pînă la expirarea termenului.

1.4. Certificarea cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea

44. După primirea certificatului de înregistrare a centrului de certificare de nivelul al doilea, persoana împuternicită a acestui centru creează cheia sa privată şi cea publică în conformitate cu cerinţele stabilite de organul competent.

45. Cheia publică a persoanei împuternicite a centrului de certificare de nivelul al doilea se certifică de către Centrul de certificare în conformitate cu prezentul Regulament.

46. Pentru certificarea cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea, aceasta prezintă personal Centrului de certificare următoarele documente şi informaţii:

a) cererea de certificare a cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea pe suport de hîrtie, semnată cu semnătura olografă (anexa nr. 3 la prezentul Regulament);

b) cererea de certificare a cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document electronic semnat cu semnătura digitală a persoanei împuternicite a centrului de certificare de nivelul al doilea cu utilizarea cheii private ce corespunde cheii publice supuse certificării - pe suport material;

c) certificatul de înregistrare a centrului de certificare de nivelul al doilea;

d) ordinul conducătorului centrului de certificare de nivelul al doilea cu privire la numirea persoanei împuternicite a acestui centru;

e) buletinul de identitate al persoanei împuternicite a centrului de certificare de nivelul al doilea;

f) suportul material al certificatului cheii publice sub formă de document electronic, ce trebuie să corespundă cerinţelor stabilite de organul competent.

47. Cererea de certificare a cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea trebuie să conţină:

a) numele şi prenumele persoanei împuternicite a centrului de certificare de nivelul al doilea, numărul buletinului de identitate al acesteia;

b) informaţiile necesare pentru comunicarea cu persoana împuternicită a centrului de certificare de nivelul al doilea (numărul de telefon, fax, adresa poştală, adresa poştei electronice);

c) denumirea şi datele de identificare ale persoanei juridice care a creat centrul de certificare de nivelul al doilea;

d) denumirea şi alte date despre centrul de certificare de nivelul al doilea;

e) cheia publică ce urmează a fi certificată.

48. Cererea de certificare a cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document electronic trebuie să corespundă standardului PKCS=10: Certification Request Syntax Specification Version 1.7 şi recomandării IETF (Internet Engineering Task Force) RFC 2986 Certification Request Syntax Specification.

49. Structura cererii de certificare a cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document electronic este prezentată în anexa nr. 4 la prezentul Regulament.

50. Administratorul înregistrări al Centrului de certificare identifică persoana împuternicită a centrului de certificare de nivelul al doilea pe baza documentelor prezentate şi efectuează controlul prealabil.

51. La efectuarea controlului prealabil, administratorul înregistrări trebuie să urmărească îndeplinirea următoarelor condiţii:

a) respectarea de către solicitant a prevederilor legislaţiei în vigoare în domeniul aplicării

semnăturii digitale la întocmirea şi înaintarea cererii de certificare a cheii publice;

b) respectarea de către solicitant a drepturilor persoanelor terţe la întocmirea şi înaintarea cererii de certificare a cheii publice;

c) concordanţa informaţiilor cuprinse în cererea de certificare a cheii publice sub formă de document electronic cu informaţiile cuprinse în cererea respectivă sub formă de document pe suport de hîrtie;

d) valabilitatea informaţiilor prezentate în cererea de certificare a cheilor publice.

52. În cazul îndeplinirii de către solicitant a tuturor condiţiilor prevăzute la punctul 51 al prezentului Regulament, administratorul înregistrări al Centrului de certificare înregistrează persoana împuternicită a centrului de certificare de nivelul al doilea. În caz contrar, administratorul înregistrări al Centrului de certificare refuză înregistrarea persoanei împuternicite a centrului de certificare de nivelul al doilea şi restituie solicitantului documentele prezentate.

53. Decizia privind refuzul de înregistrare a persoanei împuternicite a centrului de certificare de nivelul al doilea poate fi atacată la organul competent sau în instanţa de judecată competentă şi nu împiedică depunerea repetată a cererii, dacă au fost înlăturate cauzele care au servit drept temei pentru refuzul înregistrării.

54. În cazul înregistrării persoanei împuternicite a centrului de certificare de nivelul al doilea, administratorul înregistrări al Centrului de certificare transmite persoanei împuternicite a Centrului de certificare (administratorului certificare) următoarele documente:

a) cererea de certificare a cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea, sub formă de document pe suport de hîrtie, înregistrată şi autentificată cu semnătura ologrfă a administratorului înregistrări;

b) cererea de certificare a cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea, sub formă de document electronic, înregistrată şi autentificată cu semnătura digitală a administratorului înregistrări;

c) copia ordinului conducătorului centrului de certificare de nivelul al doilea privind numirea persoanei împuternicite a acestui centru, înregistrată de către administratorul înregistrări;

d) copia certificatului de înregistrare a centrului de certificare de nivelul al doilea, înregistrată de către administratorul înregistrări;

e) copia buletinului de identitate a persoanei împuternicite a centrului de certificare de nivelul al doilea, înregistrată de către administratorul înregistrări;

f) suportul material al certificatului cheii publice, ce trebuie să corespundă cerinţelor stabilite de organul competent.

55. Persoana împuternicită a Centrului de certificare (administratorul certificare) ia decizia despre certificarea cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea în termen de 3 zile lucrătoare din data înregistrării cererii.

56. În cazul depistării unor încălcări ale legislaţiei în domeniul aplicării semnăturii digitale, persoana împuternicită a Centrului de certificare ia decizia privind refuzul certificării cheii publice, indicînd obligatoriu motivele refuzului.

57. Decizia privind refuzul de certificare a cheii publice poate fi atacată la organul competent sau în instanţa de judecată competentă şi nu împiedică depunerea repetată a cererii, dacă au fost înlăturate cauzele care au servit drept temei pentru refuz.

58. În cazul deciziei de aprobare privind certificarea cheii publice, persoana împuternicită a Centrului de certificare creează certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document pe suport de hîrtie, în două exemplare.

59. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea trebuie să conţină:

a) numărul de înregistrare a certificatului cheii publice;

b) datele de identificare ale centrului de certificare de nivelul al doilea, IDNO;

c) numele şi prenumele persoanei împuternicite a centrului de certificare de nivelul al doilea - titular al certificatului cheii publice;

d) numărul de identificare al persoanei fizice - persoanei împuternicite a centrului de certificare de nivelul al doilea (IDNP);

e) denumirea centrului de certificare şi funcţia deţinută de către persoana împuternicită a centrului de certificare de nivelul al doilea;

f) informaţiile necesare pentru comunicarea cu persoana împuternicită a centrului de certificare de nivelul al doilea - titular al certificatului cheii publice;

g) cheia publică a persoanei împuternicite a centrului de certificare de nivelul al doilea - titular al certificatului cheii publice;

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

i) datele despre algoritmul criptografic al semnăturii digitale şi alte date tehnologice stabilite de Centrul de certificare;

j) domeniile de aplicare a semnăturii digitale şi alte restricţii impuse;

k) semnătura digitală a persoanei împuternicite a Centrului de certificare;

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

60. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document electronic trebuie să corespundă standardului ISO/IEC 9594/8 Directory Services, standardului Uniunii Internaţionale de Telecomunicaţii ITU-T X.509, versiunea 3, şi recomandării IETF (Internet Engineering Task Force) RFC 3280 (RFC 2459).

61. Structura certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea este prezentată în anexa nr. 5 la prezentul Regulament.

62. Persoana împuternicită a Centrului de certificare creează certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document electronic, corespunzător certificatului pe suport de hîrtie, şi îl semnează cu semnătura sa digitală.

63. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document electronic este valabil cu condiţia că conţine date ce corespund informaţiilor cuprinse în certificatul corespunzător pe suport de hîrtie.

64. Termenul de valabilitate a certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea este de 5 ani.

65. Administratorul înregistrări al Centrului de certificare informează persoana împuternicită a centrului de certificare de nivelul al doilea despre crearea certificatului cheii publice.

66. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document pe suport de hîrtie, în două exemplare, se semnează cu semnătura olografă a persoanei împuternicite a Centrului de certificare şi a persoanei împuternicite a centrului de certificare de nivelul al doilea şi se autentifică cu ştampila Centrului de certificare şi cu ştampila centrului de certificare de nivelul al doilea.

67. Persoanei împuternicite a centrului de certificare de nivelul al doilea i se eliberează:

a) un exemplar al certificatului cheii publice a persoanei împuternicite a centrului de certificare sub formă de document pe suport de hîrtie, semnat şi autentificat cu ştampile;

b) copia certificatului cheii publice a persoanei împuternicite a Centrului de certificare sub formă de document pe suport de hîrtie;

c) suportul material ce conţine următoarele documente electronice:
certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;
certificatul cheii publice a persoanei împuternicite a Centrului de certificare;
lista actualizată a certificatelor revocate;

d) documentul pe suport de hîrtie conţinînd datele de identitate ale persoanei împuternicite a centrului de certificare de nivelul al doilea şi fraza-cheie pentru autentificarea la distanţă a acestei persoane.

68. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se păstrează în Registrul certificatelor cheilor publice sub formă de document electronic şi document pe suport de hîrtie.

1.5. Suspendarea valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea

69. Suspendarea valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare se efectuează:

a) la cererea persoanei împuternicite a centrului de certificare de nivelul al doilea - titular al certificatului cheii publice;

b) pe baza deciziei organului competent;

c) pe baza deciziei Centrului de certificare.

70. Persoana împuternicită a centrului de certificare de nivelul al doilea poate cere suspendarea valabilităţii certificatului cheii publice ce-i aparţine dacă are motive să presupună că a fost încălcată confidenţialitatea cheii private, precum şi în cazul în care informaţiile cuprinse în certificatul cheii publice nu corespund realităţii.

71. Cererea de suspendare a valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea (anexa nr. 6 la prezentul Regulament) se depune de către această persoană la Centrul de certificare sub formă de document pe suport de hîrtie sau document electronic.

72. În cazuri excepţionale, în care este necesară suspendarea urgentă a valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea, cererea poate fi prezentată verbal, cu confirmarea ulterioară a acesteia sub formă de document pe suport de hîrtie sau document electronic, în termen de o zi de lucru.

73. Cererea de suspendare a valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea trebuie să conţină:

a) datele de identitate ale persoanei împuternicite a centrului de certificare de nivelul al doilea;

b) numărul certificatului cheii publice a cărui valabilitate se suspendă;

c) termenul pentru care se suspendă valabilitatea certificatului cheii publice;

d) motivul suspendării valabilităţii certificatului cheii publice;

e) data semnării cererii, semnătura persoanei împuternicite şi a conducătorului centrului de certificare de nivelul al doilea.

74. Cererea de suspendare a valabilităţii certificatului cheii publice sub formă de document pe suport de hîrtie se depune la Centrul de certificare personal de către persoana împuternicită a centrului de certificare de nivelul al doilea, iar sub formă de document electronic - prin intermediul sistemului de schimb electronic de documente.

75. Cererea de suspendare a valabilităţii certificatului cheii publice în formă verbală se transmite de către persoana împuternicită a centrului de certificare de nivelul al doilea prin mijloacele legăturii telefonice.

76. Persoana împuternicită a Centrului de certificare efectuează autentificarea persoanei împuternicite a centrului de certificare de nivelul al doilea care solicită suspendarea valabilităţii certificatului cheii publice ce-i aparţine. Autentificarea se realizează conform:

a) datelor din buletinul de identitate al solicitantului;

b) certificatului cheii publice, prin confirmarea autenticităţii cererii de suspendare a valabilităţii certificatului cheii publice sub formă de document electronic;

c) frazei-cheie pentru autentificarea la distanţă, comunicată la telefon de către persoana împuternicită a centrului de certificare de nivelul al doilea.

77. Persoana împuternicită a Centrului de certificare ia decizia privind suspendarea valabilităţii certificatului în termen de 3 ore de lucru din momentul primirii cererii de suspendare a valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea.

78. Ora suspendării valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în cîmpul This Update).

79. Centrul de certificare comunică în scris centrului de certificare de nivelul al doilea despre decizia privind suspendarea valabilităţii certificatului cheii publice sau despre refuzul de suspendare, cu precizarea motivelor refuzului, în termen de 3 zile lucrătoare.

80. Valabilitatea certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se suspendă prin decizia organului competent, perfectată sub formă de dispoziţie a directorului Serviciului de Informaţii şi Securitate.

81. Dacă Centrul de certificare are motive să presupună că a fost încălcată confidenţialitatea

cheii private a persoanei împuternicite a centrului de certificare de nivelul al doilea sau informaţiile cuprinse în certificatul cheii publice nu corespund realităţii, Centrul de certificare este în drept să ia unilateral decizia privind suspendarea valabilităţii certificatului cheii publice corespunzător.

82. În cazul suspendării valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea pe baza deciziei organului competent sau a Centrului de certificare, Centrul de certificare informează imediat, prin mijloacele legăturii telefonice, centrul de certificare de nivelul al doilea despre suspendarea valabilităţii certificatului cheii publice a persoanei împuternicite a acestui centru, comunicînd ulterior în scris asupra acestei decizii în termen de 3 zile lucrătoare.

83. Valabilitatea certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se suspendă pentru o perioadă de pînă la 30 de zile.

84. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea al cărui valabilitate a fost suspendată, în termen de 3 ore de lucru, va fi înscris în lista certificatelor revocate, iar Centrul de certificare va emite lista actualizată a certificatelor revocate.

85. În cazul în care pînă la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice nu a fost luată decizia privind restabilirea valabilităţii acestuia, certificatul cheii publice se revocă.

86. Restabilirea valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se efectuează:

a) la cererea persoanei împuternicite a centrului de certificare de nivelul al doilea - titular al certificatului cheii publice;

b) pe baza deciziei organului competent;

c) pe baza deciziei Centrului de certificare.

87. Cererea de restabilire a valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea (anexa nr. 7 la prezentul Regulament) reprezintă un document pe suport de hîrtie semnat cu semnătura olografă a persoanei împuternicite şi a conducătorului centrului de certificare de nivelul al doilea.

88. Cererea de restabilire a valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se depune la Centrul de certificare personal de către persoana împuternicită a centrului de certificare de nivelul al doilea, nu mai tîrziu de 5 zile lucrătoare pînă la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice.

89. Cererea de restabilire a valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea trebuie să conţină:

a) datele de identitate ale persoanei împuternicite a centrului de certificare de nivelul al doilea;

b) numărul certificatului cheii publice a cărui valabilitate a fost suspendată;

c) termenul pentru care a fost suspendată valabilitatea certificatului cheii publice;

d) motivul suspendării valabilităţii certificatului cheii publice;

e) justificarea restabilirii valabilităţii certificatului cheii publice;

f) data semnării cererii, semnătura persoanei împuternicite şi a conducătorului centrului de certificare de nivelul al doilea.

90. Persoana împuternicită a Centrului de certificare ia decizia de restabilire a valabilităţii certificatului în termen de 5 zile lucrătoare din data primirii cererii de restabilire a valabilităţii certificatului cheii publice.

91. Centrul de certificare comunică în scris centrului de certificare de nivelul al doilea despre decizia privind restabilirea sau privind refuzul de restabilire a valabilităţii certificatului cheii publice, indicînd motivele refuzului, în termen de 3 zile lucrătoare.

92. Valabilitatea certificatului cheii publice a centrului de certificare de nivelul al doilea, suspendată pe baza deciziei organului competent, se restabileşte prin decizia organului competent, perfectată sub formă de dispoziţie a directorului Serviciului de Informaţii şi Securitate.

93. În cazul în care valabilitatea certificatului cheii publice a centrului de certificare de nivelul al doilea a fost suspendată pe baza deciziei Centrului de certificare, Centrul de certificare este în drept să ia unilateral decizia privind restabilirea valabilităţii certificatului cheii publice corespunzător.

94. În cazul restabilirii valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea pe baza deciziei organului competent sau a Centrului de certificare, Centrul de certificare informează în scris centrul de certificare de nivelul al doilea despre restabilirea valabilităţii certificatului în termen de 3 zile lucrătoare.

95. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea a cărui valabilitate a fost restabilită, în termen de 3 ore de lucru, va fi radiat din lista certificatelor revocate, iar Centrul de certificare va emite lista actualizată a certificatelor revocate.

96. Ora restabilirii valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în cîmpul This Update).

1.6. Revocarea certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea

97. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se revocă:

a) la cererea persoanei împuternicite a centrului de certificare de nivelul al doilea - titular al certificatului cheii publice;

b) pe baza deciziei organului competent;

c) în cazul faptului constatat de compromitere a cheii private;

d) la depistarea unor informaţii neconforme realităţii în cererea de certificare a cheii publice sau în certificatul cheii publice;

e) la introducerea unor modificări în certificatul cheii publice;

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

g) la expirarea termenului de valabilitate a certificatului cheii publice.

98. Persoana împuternicită a centrului de certificare de nivelul al doilea poate cere revocarea certificatului cheii publice ce-i aparţine în cazul faptelor constatate de încălcare a confidenţialităţii cheii sale private sau în cazul în care informaţiile cuprinse în certificat nu corespund realităţii, precum şi în alte cazuri prevăzute de Regulamentul centrului de certificare de nivelul al doilea.

99. Cererea de revocare a certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea (anexa nr. 8 la prezentul Regulament) reprezintă un document pe suport de hîrtie semnat cu semnătura olografă a persoanei împuternicite şi a conducătorului centrului de certificare de nivelul al doilea.

100. Cererea de revocare a certificatului cheii publice se depune la Centrul de certificare personal de către persoana împuternicită a centrului de certificare de nivelul al doilea.

101. Cererea de revocare a certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea trebuie să conţină:

a) datele de identitate ale persoanei împuternicite a centrului de certificare de nivelul al doilea;

b) numărul certificatului cheii publice care se cere a fi revocat;

c) motivul revocării certificatului cheii publice;

d) data semnării cererii, semnătura persoanei împuternicite şi a conducătorului centrului de certificare de nivelul al doilea.

102. Persoana împuternicită a Centrului de certificare ia decizia privind revocarea certificatului în termen de 3 zile lucrătoare din momentul primirii cererii de revocare a certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea.

103. Centrul de certificare comunică în scris centrului de certificare de nivelul al doilea despre decizia de revocare a certificatului cheii publice sau despre refuzul revocării certificatului,

indicînd motivele refuzului, în termen de 3 zile lucrătoare.

104. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se revocă pe baza deciziei organului competent, perfectată sub formă de dispoziţie a directorului Serviciului de Informaţii şi Securitate.

105. Centrul de certificare este în drept să ia unilateral decizia privind revocarea certificatului cheii private a persoanei împuternicite a centrului de certificare de nivelul al doilea:

a) în cazul faptului constatat de compromitere a cheii private;

b) la depistarea unor informaţii neconforme realităţii în cererea de certificare a cheii publice sau în certificatul cheii publice;

c) la introducerea unor modificări în certificatul cheii publice;

d) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice, dacă nu a fost adoptată decizia de restabilire a valabilităţii acestuia;

e) la expirarea termenului de valabilitate a certificatului cheii publice.

106. În cazul revocării certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea pe baza deciziei organului competent sau a Centrului de certificare, Centrul de certificare informează imediat, prin mijloacele legăturii telefonice, centrul de certificare de nivelul al doilea despre revocarea certificatului cheii publice a persoanei împuternicite a acestui centru, comunicînd ulterior în scris despre această decizie în termen de 3 zile lucrătoare.

107. Certificatul cheii publice revocat a persoanei împuternicite a centrului de certificare de nivelul al doilea în termen de 3 ore de lucru se înscrie în lista certificatelor revocate, iar Centrul de certificare emite lista actualizată a certificatelor revocate.

108. Ora revocării certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în cîmpul This Update).

109. În cazul revocării certificatului cheii publice pe motivul expirării termenului de valabilitate a acestuia, certificatul nu se înscrie în lista certificatelor revocate.

110. În cazul eliberării din funcţie a persoanei împuternicite a centrului de certificare de nivelul al doilea, cheia sa privată se distruge în conformitate cu cerinţele stabilite de organul competent, iar certificatul cheii publice corespunzător îşi păstrează valabilitatea pînă la expirarea termenului.

1.7. Confirmarea autenticităţii şi valabilităţii certificatului cheii publice

111. Centrul de certificare confirmă autenticitatea şi valabilitatea certificatelor cheilor publice:

a) ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea - la cererea utilizatorilor semnăturii digitale;

b) eliberate de către centrele de certificare de nivelul al doilea - la cererea instanţei de judecată, a altor persoane şi organe care au acest drept în temeiul legii sau în alte cazuri prevăzute de legislaţia în domeniul aplicării semnăturii digitale.

112. Centrul de certificare asigură utilizatorilor semnăturii digitale posibilitatea de a stabili de sine stătător autenticitatea şi valabilitatea certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea prin:

acordarea accesului liber la documentele electronice conţinute în Registrul certificatelor cheilor publice;

difuzarea liberă şi publicarea listei certificatelor revocate, sub formă de document electronic.

113. Cererea utilizatorului semnăturii digitale de confirmare a autenticităţii şi valabilităţii certificatului cheii publice reprezintă un document pe suport de hîrtie semnat cu semnătura olografă a solicitantului (anexa nr. 9 la prezentul Regulament).

114. Cererea se depune la Centrul de certificare împreună cu suportul material conţinînd certificatul cheii publice sub formă de document electronic a cărui autenticitate şi valabilitate trebuie confirmată.

115. Centrul de certificare transmite solicitantului, în termen de 3 zile lucrătoare, un proces-verbal privind rezultatele verificării autenticităţii şi valabilităţii certificatului cheii publice, care va conţine:

a) timpul şi locul verificării;

b) cauza verificării;

c) datele despre angajatul Centrului de certificare care a efectuat verificarea (numele, prenumele, funcţia);

d) conţinutul şi rezultatele verificării;

e) evaluarea rezultatelor verificării şi concluziile corespunzătoare;

f) alte date stabilite de Centrul de certificare.

116. Centrul de certificare poate refuza solicitantului să verifice autenticitatea şi valabilitatea certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea dacă nu au fost prezentate toate documentele electronice necesare sau dacă suportul material este deteriorat.

Secţiunea 2. Administrarea cheii private şi cheii publice a persoanei împuternicite a Centrului de certificare

117. Termenul de valabilitate a cheii private a persoanei împuternicite a Centrului de certificare este de 2,5 ani. Începutul perioadei de valabilitate a cheii private se consideră data şi ora la care începe termenul de valabilitate a certificatului cheii publice ce-i corespunde.

118. Termenul de valabilitate a certificatului cheii publice, ce corespunde cheii private a persoanei împuternicite a Centrului de certificare, este de 5 ani.

119. La expirarea termenului de valabilitate a cheii private a persoanei împuternicite a Centrului de certificare cheia privată se distruge, se creează din nou cheia privată şi cea publică, precum şi certificatul cheii publice.

120. Schimbarea planificată a cheii private şi a cheii publice corespunzătoare, ce aparţin persoanei împuternicite a Centrului de certificare, se efectuează nu mai devreme de 2 ani şi 5 luni şi nu mai tîrziu de 2 ani şi 6 luni de la data la care începe termenul de valabilitate a cheii private a persoanei împuternicite a Centrului de certificare.

121. Schimbarea în afara acestui termen a cheilor se efectuează în cazul compromiterii sau pericolului de compromitere a cheii private a persoanei împuternicite a Centrului de certificare.

122. Procedurile de schimbare planificată a cheilor se realizează în conformitate cu cerinţele stabilite de organul competent.

123. Cheia privată a persoanei împuternicite a Centrului de certificare se utilizează exclusiv pentru semnarea cu semnătura digitală a:

a) certificatului cheii publice a persoanei împuternicite a Centrului de certificare;

b) certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

c) listelor certificatelor revocate.

124. Cheia privată a persoanei împuternicite a Centrului de certificare se păstrează şi se utilizează în condiţii ce exclud încălcarea confidenţialităţii acestuia.

125. Accesul la suportul material al cheii private a persoanei împuternicite a Centrului de certificare se efectuează cu autorizarea scrisă a conducătorului Centrului de certificare, în prezenţa persoanei împuternicite a Centrului de certificare (administratorului certificare), administratorului securitate al Centrului de certificare şi a conducătorului Centrului de certificare în aşa mod încît în cazul absenţei cel puţin a uneia dintre aceste persoane accesul la cheia privată să fie imposibil de realizat. În cazul absenţei temporare a administratorului securitate şi a conducătorului Centrului de certificare accesul se realizează în prezenţa persoanelor care îi înlocuiesc.

126. Persoana împuternicită a Centrului de certificare utilizează cheia sa privată în prezenţa administratorului securitate evitînd încălcarea confidenţialităţii cheii private.

127. Conducătorul Centrului de certificare poartă răspundere pentru organizarea accesului sigur la suportul material al cheii private şi utilizării autorizate a cheii.

128. Conducătorul Centrului de certificare, persoana împuternicită a Centrului de certificare (administratorul certificare) şi administratorul securitate poartă răspundere personală pentru utilizarea sigură de către persoana împuternicită a cheii sale private.

Secţiunea 3. Resursele informaţionale ale Centrului de certificare

129. Resursa informaţională de bază a Centrului de certificare este Registrul certificatelor cheilor publice.

130. Registrul certificatelor cheilor publice reprezintă totalitatea documentelor pe suport de hîrtie şi a documentelor electronice, cuprinzînd:

a) certificatele cheilor publice ale persoanelor împuternicite ale Centrului de certificare;

b) deciziile privind suspendarea şi restabilirea valabilităţii, revocarea certificatelor cheilor publice ale persoanelor împuternicite ale Centrului de certificare;

c) cererile de certificare a cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

d) certificatele cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

e) cererile de suspendare şi restabilire a valabilităţii, de revocare a certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

f) listele certificatelor revocate.

131. În arhiva Centrului de certificare se păstrează următoarele resurse informaţionale:

a) Registrul certificatelor cheilor publice;

b) registrele de audit al complexului tehnic de program al Centrului de certificare;

c) documentele de serviciu ale Centrului de certificare, conform criteriilor stabilite de conducătorul Centrului.

132. Termenul de păstrare a documentelor de arhivă ale Centrului de certificare este de 20 de ani.

133. Pregătirea pentru distrugere şi distrugerea documentelor de arhivă se efectuează de către o comisie formată din angajaţi ai Centrului de certificare şi colaboratori ai organului competent.

134. Pregătirea pentru distrugere şi distrugerea documentelor care nu necesită a fi păstrate în arhivă se efectuează de către angajaţii Centrului de certificare, desemnaţi de conducătorul Centrului.

135. Protecţia resurselor informaţionale ale Centrului de certificare se efectuează în conformitate cu legislaţia în vigoare şi cerinţele stabilite de organul competent.

136. Modul de realizare a accesului la resursele informaţionale ale Centrului de certificare, inclusiv a accesului la documentele de arhivă, se reglementează de prevederile legislaţiei în vigoare, de cerinţele stabilite de organul competent şi de prezentul Regulament.

137. Accesul utilizatorilor semnăturii digitale la Registrul certificatelor cheilor publice se efectuează prin intermediul:

a) resursei informaţionale electronice oficiale a Centrului de certificare pe adresa: www.pki.sis.md;

b) poştei electronice: pki+sis.md;

c) cererii scrise a utilizatorului semnăturii digitale în conformitate cu procedurile stabilite de prezentul Regulament. Adresa poştală: MD-2004, Republica Moldova, mun. Chişinău, bd. Ştefan cel Mare şi Sfînt, nr. 166, Centrul de certificare al cheilor publice de nivel superior.

138. Centrul de certificare publică pe paginile resursei informaţionale electronice:

a) lista actualizată a certificatelor revocate sub formă de document electronic;

b) copiile electronice ale certificatelor cheilor publice, pe suport de hîrtie, ale persoanelor împuternicite ale Centrului de certificare şi ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea, în format PDF;

c) certificatele cheilor publice ale persoanelor împuternicite ale Centrului de certificare şi ale persoanelor împuternicite ale centrului de certificare de nivelul al doilea sub formă de documente electronice.

139. Centrul de certificare efectuează expedierea automată a listei actualizate a certificatelor revocate către centrele de certificare de nivelul al doilea, prin intermediul poştei electronice.

Secţiunea 4. Mijloacele de asigurare a activităţii Centrului de certificare

140. Centrul de certificare creează şi exploatează complexul tehnic de program care include următoarele componente:

a) serviciul certificare;

b) serviciul înregistrare;
c) serviciul registru;
d) serviciul control etalonat al semnăturii digitale.

141. Serviciul certificare reprezintă componentul tehnologic de bază al complexului tehnic de program al Centrului de certificare care asigură:

a) crearea certificatului cheii publice a persoanei împuternicite a Centrului de certificare sub formă de document electronic;

b) crearea certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document electronic;

c) crearea listei certificatelor revocate.

142. Responsabilitatea pentru exploatarea serviciului certificare o poartă persoana împuternicită a Centrului de certificare (administratorul certificare) şi administratorul sistem.

143. Serviciul înregistrare reprezintă componentul tehnologic al complexului tehnic de program al Centrului de certificare care asigură înregistrarea persoanelor împuternicite ale centrelor de certificare de nivelul al doilea.

144. Responsabilitatea pentru exploatarea serviciului înregistrare o poartă administratorul înregistrări.

145. Serviciul registru reprezintă componentul tehnologic al complexului tehnic de program al Centrului de certificare care asigură:

a) păstrarea certificatelor cheilor publice ale persoanelor împuternicite ale Centrului de certificare;

b) păstrarea certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

c) păstrarea cererilor de certificare a cheilor publice;

d) păstrarea informaţiei de înregistrare a persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

e) publicarea şi difuzarea listelor certificatelor revocate;

f) accesul la certificatele cheilor publice valabile şi la listele certificatelor revocate;

g) păstrarea altor informaţii ce ţin de activitatea Centrului de certificare.

146. Serviciul control etalonat al semnăturii digitale reprezintă componentul tehnologic al complexului tehnic de program al Centrului de certificare care asigură confirmarea autenticităţii certificatelor cheilor publice şi a altor documente electronice.

147. Mijloacele tehnice de asigurare a funcţionării com-plexului tehnic de program al Centrului de certificare includ:

a) echipamentul de server;

b) echipamentul de telecomunicaţii;

c) locurile de muncă computerizate ale administratorilor Centrului de certificare;

d) dispozitivele de imprimare pe suport de hîrtie;

e) alte echipamente auxiliare.

148. Responsabilitatea pentru exploatarea mijloacelor tehnice de asigurare a funcţionării complexului tehnic de program al Centrului de certificare o poartă administratorul sistem.

149. În componenţa complexului tehnic de program al Centrului de certificare funcţionează mijloacele de protecţie criptografică a informaţiei, inclusiv:

a) mijloacele semnăturii digitale;

b) complexele tehnice de program de protejare contra accesului neautorizat şi de asigurare a integrităţii mijloacelor tehnice de program.

150. Responsabilitatea pentru exploatarea mijloacelor de protecţie a informaţiei o poartă administratorul sistem şi administratorul securitate.

151. Complexul tehnic de program trebuie să corespundă cerinţelor stabilite de organul competent şi parametrilor tehnici indicaţi în anexa nr. 10 la prezentul Regulament.

IV. Asigurarea securităţii şi protecţia informaţiilor confidenţiale

Secţiunea 1. Confidenţialitatea informaţiei

152. Informaţiile care se prelucrează şi se păstrează în Centrul de certificare sînt protejate prin

lege.

153. Informaţiile care se păstrează în registrele de audit ale Centrului de certificare sînt confidenţiale.

154. Nu sînt confidenţiale informaţiile ce se conţin în:

a) certificatele cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;

b) listele certificatelor revocate.

155. Centrul de certificare asigură integritatea şi controlul accesului la informaţiile protejate de lege în conformitate cu legislaţia Republicii Moldova.

Secţiunea 2. Măsurile tehnico-inginereşti de protecţie a informaţiei

156. Măsurile tehnico-inginereşti de protecţie a informaţiei trebuie să asigure posibilitatea funcţionării neîntrerupte, pe o durată îndelungată, a complexului tehnic de program al Centrului de certificare.

157. Serverele serviciului certificare, serviciului înregistrare şi serviciului registru se instalează în încăperi pentru servere, pe suporturi speciale.

158. Încăperile pentru servere ale Centrului de certificare se dotează cu sisteme de control al accesului.

159. Accesul în încăperile pentru servere ale Centrului de certificare se efectuează în conformitate cu cerinţele stabilite de organul competent.

160. Alte mijloace tehnice din complexul tehnic de program al Centrului de certificare se instalează în încăperile de serviciu ale Centrului.

161. Încăperile pentru servere şi de serviciu trebuie să fie dotate cu mijloace de ventilare şi de condiţionare a aerului care să asigure respectarea parametrilor optimi ai regimului de temperatură şi umiditate.

162. Securitatea antiincendiară a încăperilor Centrului de certificare se asigură în conformitate cu normele şi cerinţele stabilite de legislaţia în vigoare.

163. Mijloacele tehnice ale Centrului de certificare trebuie să fie conectate la reţeaua de alimentare cu electricitate garantată.

Secţiunea 3. Măsurile de protecţie a informaţiei cu mijloacele de program şi de aparataj

164. Complexul tehnic de program al Centrului de certificare trebuie să asigure controlul integrităţii mijloacelor tehnice şi de program.

165. Responsabilitatea pentru îndeplinirea măsurilor de verificare a integrităţii mijloacelor tehnice şi de program ale complexului tehnic de program al Centrului de certificare o poartă administratorul sistem şi administratorul securitate.

166. Mijloacele complexului tehnic de program al Centrului de certificare trebuie să asigure copierea de rezervă a informaţiei critic importante, pe măsura necesităţii.

167. În cadrul accesului la procedurile Centrului de certificare se utilizează separarea funcţională a membrilor grupului de administratorii care deservesc complexul tehnic de program al Centrului de certificare.

168. Serverele serviciului certificare, serviciului înregistrare şi serviciului registru, precum şi locurile de lucru ale administratorilor Centrului de certificare se echipează cu mijloacele de program şi de aparataj de protecţie contra accesului neautorizat.

169. Accesul personalului de ingineri şi al administratorilor sistem la serverele serviciului certificare, serviciului înregistrare şi serviciului registru pentru îndeplinirea lucrărilor reglementare se efectuează în prezenţa administratorilor responsabili de exploatarea complexului de program corespunzător.

170. Organizarea accesului la mijloacele tehnice din complexul tehnic de program al Centrului de certificare care se află în încăperile de serviciu este pus în sarcina administratorilor Centrului de certificare responsabili pentru exploatarea acestor mijloace tehnice.

Secţiunea 4. Măsurile organizatorice de protecţie a informaţiei

171. Măsurile organizatorice de protecţie a informaţiei trebuie să asigure:

a) integritatea documentelor şi a bunurilor materiale;

b) depistarea şi reţinerea contravenienţilor care încearcă să pătrundă în clădirea (încăperile) Centrului de certificare.

172. În Centrul de certificare sînt prevăzute următoarele funcţii:

a) administratorul înregistrări, avînd ca sarcini de bază: înregistrarea şi evidenţa persoanelor împuternicite ale centrelor de certificare de nivelul al doilea, pregătirea solicitărilor pentru crearea certificatelor cheilor publice, eliberarea certificatelor cheilor publice către persoanele împuternicite ale centrelor de certificare de nivelul al doilea;

b) administratorul certificare (persoana împuternicită a Centrului de certificare), avînd ca sarcini de bază: crearea, suspendarea şi restabilirea valabilităţii, revocarea certificatelor cheilor publice, întocmirea şi publicarea (emiterea) listei certificatelor revocate;

c) administratorul securitate, avînd ca sarcini de bază: controlul securităţii tuturor procedurilor şi mecanismelor Centrului de certificare, asigurarea securităţii componentelor complexului tehnic de program al Centrului de certificare;

d) administratorul sistem, avînd ca sarcini de bază: instalarea, configurarea şi întreţinerea funcţionării serviciului certificare, serviciului înregistrare şi serviciului registru.

173. Persoana împuternicită a Centrului de certificare se numeşte prin ordinul directorului Serviciului de Informaţii şi Securitate, la propunerea conducătorului Centrului de certificare. Cerinţele de calificare şi obligaţiile de serviciu ale persoanei împuternicite a Centrului de certificare se stabilesc în conformitate cu fişa postului.

174. Administratorul sistem şi administratorul securitate ai Centrului de certificare trebuie să aibă studii superioare tehnice de inginer.

175. Accesul angajaţilor la documentele Centrului de certificare se organizează în conformitate cu sarcinile de serviciu aprobate de conducătorul Centrului de certificare.

V. Interacţiunea persoanelor împuternicite ale centrelor de certificare de nivelul al doilea şi a utilizatorilor semnăturii digitale cu Centrul de certificare

Secţiunea 1. Modul de interacţiune a persoanelor împuternicite ale centrelor de certificare de nivelul al doilea şi a utilizatorilor semnăturii digitale cu Centrul de certificare

176. Interacţiunea centrelor de certificare de nivelul al doilea şi a utilizatorilor semnăturii digitale cu Centrul de certificare se efectuează în conformitate cu procedurile stabilite de prezentul Regulament şi cu cerinţele în domeniul semnăturii digitale.

177. Centrul de certificare asigură accesul centrelor de certificare de nivelul al doilea şi al utilizatorilor semnăturii digitale la Registrul certificatelor cheilor publice în conformitate cu prezentul Regulament.

178. Centrul de certificare publică lista actualizată a certificatelor revocate şi o transmite în mod automatizat centrelor de certificare de nivelul al doilea.

179. În vederea interacţiunii, persoana împuternicită a Centrului de certificare prezintă persoanelor împuternicite ale centrelor de certificare de nivelul al doilea datele ei de contact (numărul de telefon, fax, adresa poştală, adresa poştei electronice).

180. În cazul revocării certificatului cheii publice a persoanei împuternicite a Centrului de certificare, se revocă concomitent şi certificatele persoanelor împuternicite ale centrelor de certificare de nivelul al doilea.

181. Utilizatorii semnăturii digitale folosesc certificatul cheii publice a persoanei împuternicite a Centrului de certificare în procesul verificării autenticităţii semnăturii digitale în documentul electronic.

182. În procesul interacţiunii persoanelor împuternicite ale centrelor de certificare de nivelul al doilea şi a utilizatorilor semnăturii digitale cu Centrul de certificare pot apărea situaţii litigioase. Sînt supuse soluţionării în conformitate cu prezentul Regulament situaţiile litigioase care apar în legătură cu:

a) contestarea de către persoana împuternicită a centrului de certificare de nivelul al doilea sau de către utilizatorul semnăturii digitale a valabilităţii şi autenticităţii certificatului cheii publice a

persoanei împuternicite a Centrului de certificare;

b) contestarea de către utilizatorul semnăturii digitale a valabilităţii şi autenticităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;

c) contestarea împuternicirilor persoanei împuternicite a Centrului de certificare;

d) contestarea împuternicirilor persoanei împuternicite a centrului de certificare de nivelul al doilea;

e) contestarea domeniului de aplicare a semnăturii digitale şi a altor restricţii indicate în certificatele cheilor publice eliberate de către Centrul de certificare;

f) neîncrederea faţă de mijloacele semnăturii digitale utilizate de către Centrul de certificare;

g) alte cazuri de apariţie a situaţiilor litigioase în legătură cu aplicarea semnăturii digitale.

183. Situaţia litigioasă se soluţionează în regim de lucru de către părţile interesate în conformitate cu Regulamentul de soluţionare a situaţiilor litigioase în domeniul aplicării semnăturii digitale, aprobat de organul competent.

184. În cazul în care situaţia litigioasă este considerată de către părţi ca fiind soluţionată, se întocmeşte un proces-verbal privind soluţionarea situaţiei litigioase, care se semnează de către părţi.

185. În cazul imposibilităţii de soluţionare a situaţiei litigioase în regim de lucru, părţile se pot adresa în instanţa de judecată, conform procedurilor prevăzute de legislaţie.

Secţiunea 2. Drepturile şi obligaţiile persoanei împuternicite a centrului de certificare de nivelul al doilea în interacţiunea cu Centrul de certificare

186. În cadrul interacţiunii cu Centrul de certificare, persoana împuternicită a centrului de certificare de nivelul al doilea are dreptul:

a) să creeze cheia privată şi cheia publică folosind mijloacele certificate ale semnăturii digitale;

b) să depună cererea de certificare a cheii publice;

c) să depună cererile de revocare, suspendare şi restabilire a valabilităţii certificatului cheii publice în perioada de valabilitate a cheii private corespunzătoare;

d) să obţină accesul la Registrul certificatelor cheilor publice;

e) să utilizeze certificatul cheii publice a persoanei împuternicite a Centrului de certificare pentru verificarea autenticităţii semnăturii digitale în certificatele cheilor publice eliberate de către Centrul de certificare;

f) să obţină lista certificatelor revocate a Centrului de certificare;

g) să aplice lista certificatelor revocate a Centrului de certificare pentru determinarea valabilităţii certificatului cheii publice a persoanei împuternicite a Centrului de certificare;

h) să obţină copia certificatului cheii publice a persoanei împuternicite a Centrului de certificare pe suport de hîrtie;

i) să se adreseze la Centrul de certificare pentru confirmarea autenticităţii şi valabilităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;

j) să obţină asistenţă metodică de la persoana împuternicită a Centrului de certificare.

187. În cadrul interacţiunii cu Centrul de certificare, persoana împuternicită a centrului de certificare de nivelul al doilea are obligaţia:

a) să respecte cerinţele legislaţiei în domeniul aplicării semnăturii digitale;

b) să prezinte informaţiile în volumul determinat de prezentul Regulament;

c) să excludă accesul unei alte persoane la cheia sa privată, să întreprindă măsuri pentru prevenirea compromiterii cheii private;

d) să aplice cheia sa privată în conformitate cu domeniile de aplicare a semnăturii digitale şi alte restricţii indicate în certificatul cheii publice;

e) să comunice imediat Centrului de certificare despre compromiterea propriei chei private;

f) să nu utilizeze cheia sa privată dacă are motive să presupună că aceasta a fost compromisă;

g) să nu utilizeze cheia sa privată în perioada examinării cererii de certificare a cheii publice

corespunzătoare, a cererilor de revocare, suspendare sau restabilire a valabilităţii certificatului cheii publice corespunzătoare;

h) să nu utilizeze cheia sa privată dacă valabilitatea certificatului cheii publice ce-i corespunde este suspendată sau dacă certificatul a fost revocat.

Secţiunea 3. Drepturile utilizatorului semnăturii digitale în cadrul interacţiunii cu Centrul de certificare

188. În cadrul interacţiunii cu Centrului de certificare utilizatorul semnăturii digitale are dreptul:

a) să creeze cheia privată şi cheia publică folosind mijloacele certificate ale semnăturii digitale;

b) să obţină lista certificatelor revocate a Centrului de certificare;

c) să obţină accesul la Registrul certificatelor cheilor publice;

d) să aplice lista certificatelor revocate a Centrului de certificate pentru verificarea valabilităţii certificatelor cheilor publice ale persoanelor împuternicite ale Centrului de certificare şi ale centrelor de certificare de nivelul al doilea;

e) să aplice certificatul cheii publice a persoanei împuternicite a Centrului de certificare pentru confirmarea autenticităţii certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;

f) să se adreseze la Centrul de certificare pentru confirmarea autenticităţii şi valabilităţii certificatelor cheilor publice ale persoanei împuternicite a Centrului de certificare şi ale persoanelor împuternicite ale centrelor de certificare de nivelul al doilea.

VI. Reorganizarea şi lichidarea Centrului de certificare

189. Reorganizarea şi lichidarea Centrului de certificare se efectuează în conformitate cu legislaţia.

190. La reorganizarea Centrului de certificare şi transmiterea funcţiilor lui la o altă instituţie, prin decizia comună a conducătorilor instituţiilor interesate se creează o comisie de transmitere a Centrului de certificare.

191. În componenţa comisiei de transmitere a Centrului de certificare se includ:

a) reprezentanţii părţilor;

b) conducătorul Centrului de certificare sau persoana care îl înlocuieşte;

c) reprezentantul organului competent;

d) alte persoane desemnate de către părţi.

192. La încheierea lucrărilor, comisia întocmeşte actul de predare-primire, în conformitate cu care instituţiei succesoare i se transmite Registrul certificatelor cheilor publice, precum şi drepturile şi obligaţiile Centrului de certificare. Actul se semnează de către toţi membrii comisiei şi se aprobă de către conducătorii instituţiilor implicate.

193. 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.

194. La transmiterea Centrului de certificare, cheile private ale persoanelor împuternicite ale Centrului de certificare se distrug, fără a se încălca confidenţialitatea lor, în conformitate cu cerinţele stabilite de organul competent, iar certificatele cheilor publice corespunzătoare, transmise unui alt centru de certificare, continuă să fie valabile pînă la expirarea termenului lor.

195. La lichidarea Centrului de certificare prin ordinul directorului Serviciului de Informaţii şi Securitate se creează comisia de lichidare, în sarcina căreia se pune realizarea procedurii de lichidare în conformitate cu legislaţia în vigoare şi cerinţele stabilite de organul competent.

196. În componenţa comisiei de lichidare se includ:

a) conducătorul Centrului de certificare sau persoana care îl înlocuieşte;

b) reprezentantul organului competent;

c) alte persoane indicate în ordin.

197. La încheierea lucrărilor, comisia întocmeşte actul de lichidare, potrivit căruia Centrul de certificare îşi încetează activitatea, iar Registrul certificatelor cheilor publice se transmite organului competent şi se păstrează în arhivă conform legislaţiei.

198. Registrul certificatelor cheilor publice al Centrului de certificare lichidat, sub formă de documente electronice, se transmite organului competent pe suporturi materiale, iar Registrul certificatelor cheilor publice pe suport de hîrtie se transmite sub formă de arhivă a documentelor pe suporturi de hîrtie, pe baza actului de primire-predare. Actul se semnează de către conducătorul Centrului de certificare, reprezentantul organului competent responsabil de păstrare şi se aprobă de către directorul Serviciului de Informaţii şi Securitate.

199. În cazul lichidării Centrului de certificare, cheile private ale persoanelor împuternicite ale Centrului de certificare se distrug, fără a se încălca confidenţialitatea cheilor, iar certificatele cheilor publice corespunzătoare se revocă.