

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

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

_____ Ion URSU

_____ Victoria IFTODI

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

REGULAMENTUL Centrului de certificare a cheilor publice de nivel superior

I. Dispoziții generale

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

2. Regulamentul stabilește condițiile generale de organizare a activității Centrului de certificare a cheilor publice de nivel superior (în continuare – Centrul de certificare), precizează funcțiile, obligațiile și drepturile acestuia, mecanismul și procedurile aplicate de către Centrul de certificare la administrarea infrastructurii ierarhice unice a cheilor publice (Public Key Infrastructure, PKI), precum și modul de conlucrare cu centrele de certificare și cu utilizatorii semnăturii digitale, măsurile tehnico-organizatorice de bază pentru asigurarea securității.

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 și juridice ce utilizează semnătura digitală sau desfășoară activități în domeniul semnăturii digitale.

4. Centrul de certificare este o subdiviziune structurală a Serviciului de Informații și Securitate care își desfășoară activitatea în domeniul protecției criptografice și tehnice a informației.

5. Conducătorul Centrului de certificare se numește în funcție prin ordinul directorului Serviciului de Informații și Securitate.

II. Funcțiile, obligațiile și drepturile Centrului de certificare

6. Centrul de certificare îndeplinește următoarele funcții:

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

b) suspendă și restabilește valabilitatea, revocă certificatele cheilor publice emise de către Centrul de certificare;

c) întocmește și gestionează registrul certificatelor cheilor publice ale persoanelor împuternicite ale Centrului de certificare și ale centrelor de certificare de nivelului al doilea (în continuare – Registrul certificatelor cheilor publice);

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

7. Pentru îndeplinirea funcțiilor sale, Centrul de certificare:

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

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

c) ține evidența centrelor de certificare de nivelului al doilea;

d) gestionează Registrul certificatelor cheilor publice sub formă de documente pe suport de hârtie și sub formă de documente electronice;

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

f) acordă consultații și suport metodologic persoanelor împuternicite ale centrelor de certificare de nivelului al doilea;

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

h) confirmă autenticitatea și valabilitatea certificatelor cheilor publice emise de către centrele de certificare de nivelului al doilea, în cazurile prevăzute de prezentul Regulament;

i) desfășoară activitatea în domeniul protecției criptografice și tehnice a informației;

j) creează sistemele informaționale și de telecomunicații ale Centrului de certificare, asigură funcționarea, securitatea, deservirea și modernizarea lor, efectuează auditul intern permanent al securității și funcționalității acestor sisteme.

8. Centrul de certificare este obligat:

să-și desfășoare activitatea în strictă conformitate cu legislația și cerințele stabilite de organul abilitat cu elaborarea și promovarea politicii de stat și 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 legislația în vigoare;

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

să organizeze regimul interior de funcționare a Centrului de certificare astfel încât să se excludă posibilitatea accesului persoanelor terțe la mijloacele semnăturii digitale, la modificarea și utilizarea lor neautorizată;

să asigure securitatea cheilor private ale persoanelor împuternicite ale Centrului de certificare și ale altor angajați, să creeze condițiile necesare pentru excluderea accesului neautorizat la cheile private;

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

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

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

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

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

să revoce certificatul cheii publice a persoanei împuternicite a Centrului de certificare în cazul constatat de încălcare a confidențialității cheii private sau de neconcordanță realității a informațiilor 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 informațiilor cuprinse în certificatul cheii publice cu informațiile prezentate de către persoana împuternicită a centrului de certificare de nivelul al doilea;

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

să nu divulge informațiile confidențiale și alte informații 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 cerințelor stabilite de organul competent și de prezentul Regulament;

să introducă certificatul cheii publice în Registrul certificatelor cheilor publice nu mai târziu de data și 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 și să restabilească valabilitatea, sau să revoce certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea în cazurile și 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, precizând data, ora și cauza revocării sau suspendării valabilității certificatului;

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

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

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

să înștiințeze persoana împuternicită a centrului de certificare de nivelul al doilea despre faptele de care a luat cunoștință Centrul de certificare și care pot influența esențial asupra posibilității utilizării ulterioare a certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;

să înștiințeze titularul certificatului cheii publice despre faptele de care a luat cunoștință Centrul de certificare, ce indică asupra imposibilității utilizării ulterioare a cheii private aparținând acestui titular;

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

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

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

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

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

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

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

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

să amplaseze mijloacele tehnice de program, destinate pentru certificarea cheilor publice, în încăperi speciale și 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 și 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, precizând motivele refuzului, în cazurile:

prezentării în cererea de certificare a cheilor publice a unor informații ce nu corespund realității;

încălțării prevederilor legislației în domeniul aplicării semnăturii digitale;

încălțării drepturilor persoanelor terțe în procesul întocmirii sau depunerii cererii;

d) să confirme autenticitatea și 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 și în modul prevăzute de legislație și de prezentul Regulament.

III. Organizarea activității Centrului de certificare

Secțiunea 1. Procedurile Centrului de certificare

10. Centrul de certificare îndeplinește următoarele proceduri:

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

b) suspendarea valabilității 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 valabilității 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 autenticității și valabilității 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 însuși Centrul de certificare, în temeiul împuternicirilor stabilite de legislația în domeniul aplicării semnăturii digitale.

12. Persoana împuternicită a Centrului de certificare creează cheia sa privată și cea publică conform cerințelor 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 Internaționale de Telecomunicații ITU-T X.509, versiunea 3, și 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 hârtie, cu următorul conținut:

- a) numărul de înregistrare a certificatului cheii publice;
- b) datele de identificare ale Centrului de certificare, numărul de identificare al unității de drept (IDNO);
- c) numele și 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 și funcția deținută 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 și ora la care începe și încetează termenul de valabilitate a certificatului cheii publice;
- h) datele despre algoritmul criptografic al semnăturii digitale și alte date tehnologice stabilite de Centrul de certificare;
- i) domeniile de aplicare a semnăturii digitale și alte restricții impuse;
- j) alte date, în conformitate cu standardele tehnice și cerințele 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 hârtie se semnează de persoana împuternicită a Centrului de certificare, de conducătorul Centrului de certificare, se aprobă de directorul Serviciului de Informații și Securitate și se autentifică cu ștampila Serviciului.

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

a) informațiile cuprinse în certificat corespund informațiilor 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 recunoașterii internaționale 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 internațional.

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 și sub formă de document electronic.

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

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

a) încălcării legislației în domeniul aplicării semnăturii digitale;

b) existenței motivelor de a presupune că a fost încălcată confidențialitatea cheii private; sau

c) existenței motivelor de a presupune că informațiile cuprinse în certificatul cheii publice nu corespund realității.

22. Valabilitatea certificatului cheii publice a persoanei împuternicite a Centrului de certificare se suspendă prin dispoziția directorului Serviciului de Informații și 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 valabilității certificatului cheii publice a persoanei împuternicite a Centrului de certificare se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în câmpul This Update).

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

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

27. În cazul suspendării valabilității certificatului cheii publice a persoanei împuternicite a Centrului de certificare, prin dispoziția directorului Serviciului de Informații și Securitate, este creată comisia pentru efectuarea unei anchete de serviciu.

28. Din componența Comisiei fac parte:

- a) reprezentanții organului competent;
- b) conducătorul Centrului de certificare;
- c) alte persoane care posedă cunoștințe și experiența necesară în domeniul aplicării semnăturii digitale și întocmirii documentelor electronice.

29. Persoanele care fac parte din componența Comisiei trebuie să dispună de dreptul de acces la materialele documentare și la mijloacele tehnice și de program, necesare pentru desfășurarea activității comisiei.

30. Comisia examinează, la nivel tehnico-organizatoric, împrejurările ce au dus la suspendarea valabilității certificatului cheii publice a persoanei împuternicite a Centrului de certificare, stabilește cauzele și urmările situației create, identifică măsurile necesare pentru soluționarea acesteia.

31. Durata de activitate a comisiei nu poate depăși 30 de zile din ziua suspendării valabilității 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 întocmește un act, indicînd împrejurările ce au dus la suspendarea valabilității certificatului cheii publice, cauzele și urmările situației create, măsurile necesare pentru soluționarea acesteia și recomandările privind restabilirea valabilității 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 dispoziția directorului Serviciului de Informații și Securitate se adoptă decizia privind restabilirea valabilității 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 valabilității 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 valabilității certificatului cheii publice a persoanei împuternicite a Centrului de certificare se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în câmpul 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 informații neconforme realității 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 valabilității 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) și b) din prezentul Regulament se va face numai după suspendarea prealabilă a valabilității certificatului.

39. Decizia privind revocarea certificatului cheii publice a persoanei împuternicite a Centrului de certificare se perfectează prin dispoziția directorului Serviciului de Informații și 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 câmpul 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 funcție a persoanei împuternicite a Centrului de certificare, cheia sa privată se distruge, fără a fi încălcată confidențialitatea acesteia, de către o comisie numită prin dispoziția directorului Serviciului de Informații și Securitate, iar certificatul cheii publice corespunzător își păstrează valabilitatea până 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 și cea publică în conformitate cu cerințele 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 și informații:

a) cererea de certificare a cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea pe suport de hârtie, 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 cerințelor stabilite de organul competent.

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

- a) numele și prenumele persoanei împuternicite a centrului de certificare de nivelul al doilea, numărul buletinului de identitate al acesteia;
- b) informațiile necesare pentru comunicarea cu persoana împuternicită a centrului de certificare de nivelul al doilea (numărul de telefon, fax, adresa poștală, adresa poștei electronice);
- c) denumirea și datele de identificare ale persoanei juridice care a creat centrul de certificare de nivelul al doilea;
- d) denumirea și 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 și 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 înregistrării al Centrului de certificare identifică persoana împuternicită a centrului de certificare de nivelul al doilea pe baza documentelor prezentate și efectuează controlul prealabil.

51. La efectuarea controlului prealabil, administratorul înregistrării trebuie să urmărească îndeplinirea următoarelor condiții:

- a) respectarea de către solicitant a prevederilor legislației în vigoare în domeniul aplicării semnăturii digitale la întocmirea și înaintarea cererii de certificare a cheii publice;
- b) respectarea de către solicitant a drepturilor persoanelor terțe la întocmirea și înaintarea cererii de certificare a cheii publice;
- c) concordanța informațiilor cuprinse în cererea de certificare a cheii publice sub formă de document electronic cu informațiile cuprinse în cererea respectivă sub formă de document pe suport de hârtie;
- d) valabilitatea informațiilor prezentate în cererea de certificare a cheilor publice.

52. În cazul îndeplinirii de către solicitant a tuturor condițiilor prevăzute la punctul 51 al prezentului Regulament, administratorul înregistrării al Centrului de certificare înregistrează persoana împuternicită a centrului de certificare de nivelul al doilea. În caz contrar, administratorul înregistrării al Centrului de certificare refuză înregistrarea persoanei împuternicite a centrului de certificare de nivelul al doilea și 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 instanța de judecată competentă și 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 înregistrării 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 hârtie, înregistrată și autentificată cu semnătura olografă a administratorului înregistrării;

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

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

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

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

f) suportul material al certificatului cheii publice, ce trebuie să corespundă cerințelor 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 legislației în domeniul aplicării semnăturii digitale, persoana împuternicită a Centrului de certificare ia decizia privind refuzul certificării cheii publice, indicând obligatoriu motivele refuzului.

57. Decizia privind refuzul de certificare a cheii publice poate fi atacată la organul competent sau în instanța de judecată competentă și 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 hârtie, în două exemplare.

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

- a) numărul de înregistrare a certificatului cheii publice;
- b) datele de identificare ale centrului de certificare de nivelul al doilea, IDNO;
- c) numele și 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 și funcția deținută de către persoana împuternicită a centrului de certificare de nivelul al doilea;
- f) informațiile 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 și ora la care începe și încetează termenul de valabilitate a certificatului cheii publice;
- i) datele despre algoritmul criptografic al semnăturii digitale și alte date tehnologice stabilite de Centrul de certificare;
- j) domeniile de aplicare a semnăturii digitale și alte restricții impuse;
- k) semnătura digitală a persoanei împuternicite a Centrului de certificare;
- l) alte date, în conformitate cu standardele tehnice și cerințele 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 Internaționale de Telecomunicații ITU-T X.509, versiunea 3, și 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 hârtie, și 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 condiția că conține date ce corespund informațiilor cuprinse în certificatul corespunzător pe suport de hârtie.

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 înregistrării 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 hârtie, în două

exemplare, se semnează cu semnătura olografă a persoanei împuternicite a Centrului de certificare și a persoanei împuternicite a centrului de certificare de nivelul al doilea și se autentifică cu ștampila Centrului de certificare și cu ștampila 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 hârtie, semnat și autentificat cu ștampile;

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

c) suportul material ce conține 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 hârtie conținând datele de identitate ale persoanei împuternicite a centrului de certificare de nivelul al doilea și fraza-cheie pentru autentificarea la distanță 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 și document pe suport de hârtie.

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

69. Suspendarea valabilității 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 valabilității certificatului cheii publice ce-i aparține dacă are motive să presupună că a fost încălcată confidențialitatea cheii private, precum și în cazul în care informațiile cuprinse în certificatul cheii publice nu corespund realității.

71. Cererea de suspendare a valabilității 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 hârtie sau document electronic.

72. În cazuri excepționale, în care este necesară suspendarea urgentă a valabilității 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 hârtie sau document electronic, în termen de o zi de lucru.

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

- 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 valabilității certificatului cheii publice;
- e) data semnării cererii, semnătura persoanei împuternicite și a conducătorului centrului de certificare de nivelul al doilea.

74. Cererea de suspendare a valabilității certificatului cheii publice sub formă de document pe suport de hârtie 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 valabilității 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 valabilității certificatului cheii publice ce-i aparține. Autentificarea se realizează conform:

- a) datelor din buletinul de identitate al solicitantului;
- b) certificatului cheii publice, prin confirmarea autenticității cererii de suspendare a valabilității certificatului cheii publice sub formă de document electronic;
- c) frazei-cheie pentru autentificarea la distanță, 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 valabilității certificatului în termen de 3 ore de lucru din momentul primirii cererii de suspendare a valabilității certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea.

78. Ora suspendării valabilității 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 câmpul This Update).

79. Centrul de certificare comunică în scris centrului de certificare de nivelul al doilea despre decizia privind suspendarea valabilității 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 dispoziție a directorului Serviciului de Informații și Securitate.

81. Dacă Centrul de certificare are motive să presupună că a fost încălcată confidențialitatea cheii private a persoanei împuternicite a centrului de certificare de nivelul al doilea sau informațiile cuprinse în certificatul cheii publice nu corespund realității, Centrul de certificare este în drept să ia unilateral decizia privind suspendarea valabilității certificatului cheii publice corespunzător.

82. În cazul suspendării valabilității 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 valabilității 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 valabilității acestuia, certificatul cheii publice se revocă.

86. Restabilirea valabilității 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 valabilității 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 și a conducătorului centrului de certificare de nivelul al doilea.

88. Cererea de restabilire a valabilității 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 valabilității certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea trebuie să conțină:

- 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 valabilității certificatului cheii publice;
- e) justificarea restabilirii valabilității certificatului cheii publice;
- f) data semnării cererii, semnătura persoanei împuternicite și a conducătorului centrului de certificare de nivelul al doilea.

90. Persoana împuternicită a Centrului de certificare ia decizia de restabilire a valabilității certificatului în termen de 5 zile lucrătoare din data primirii cererii de restabilire a valabilității 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 valabilității certificatului cheii publice, indicând 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 restabilește prin decizia organului competent, perfectată sub formă de dispoziție a directorului Serviciului de Informații și 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 valabilității certificatului cheii publice corespunzător.

94. În cazul restabilirii valabilității 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 valabilității 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 valabilității 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 câmpul 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 constat de compromitere a cheii private;
- d) la depistarea unor informații neconforme realității 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 valabilității 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 aparține în cazul faptelor constatate de încălcare a confidențialității cheii sale private sau în cazul în care informațiile cuprinse în certificat nu corespund realității, precum și 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 hârtie semnat cu semnătura olografă a persoanei împuternicite și 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 conțină:

- 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 și 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, indicând 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 dispoziție a directorului Serviciului de Informații și 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 constat de compromitere a cheii private;
- b) la depistarea unor informații neconforme realității 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 valabilității 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 câmpul 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 funcție a persoanei împuternicite a centrului de certificare de nivelul al doilea, cheia sa privată se distruge în conformitate cu cerințele stabilite de organul competent, iar certificatul cheii publice corespunzător își păstrează valabilitatea pînă la expirarea termenului.

1.7. Confirmarea autenticității și valabilității certificatului cheii publice

111. Centrul de certificare confirmă autenticitatea și 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 instanței de judecată, a altor persoane și organe care au acest drept în temeiul legii sau în alte cazuri prevăzute de legislația în domeniul aplicării semnăturii digitale.

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

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

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

113. Cererea utilizatorului semnăturii digitale de confirmare a autenticității și valabilității 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 conținînd certificatul cheii publice sub formă de document electronic a cărui autenticitate și valabilitate trebuie confirmată.

115. Centrul de certificare transmite solicitantului, în termen de 3 zile lucrătoare, un proces-verbal privind rezultatele verificării autenticității și valabilității certificatului cheii publice, care va conține:

- a) timpul și locul verificării;
- b) cauza verificării;
- c) datele despre angajatul Centrului de certificare care a efectuat verificarea (numele, prenumele, funcția);
- d) conținutul și rezultatele verificării;
- e) evaluarea rezultatelor verificării și concluziile corespunzătoare;
- f) alte date stabilite de Centrul de certificare.

116. Centrul de certificare poate refuza solicitantului să verifice autenticitatea și 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.

Secțiunea 2. Administrarea cheii private și 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 și 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 și cea publică, precum și certificatul cheii publice.

120. Schimbarea planificată a cheii private și a cheii publice corespunzătoare, ce aparțin persoanei împuternicite a Centrului de certificare, se efectuează nu mai devreme de 2 ani și 5 luni și nu mai târziu de 2 ani și 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 cerințele 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 și se utilizează în condiții ce exclud încălcarea confidențialității 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 prezența persoanei împuternicite a Centrului de certificare (administratorului certificare), administratorului securitate al Centrului de certificare și a conducătorului Centrului de certificare în așa mod încât în cazul absenței cel puțin a uneia dintre aceste persoane accesul la cheia privată să fie imposibil de realizat. În cazul absenței temporare a administratorului securitate și a conducătorului Centrului de certificare accesul se realizează în prezența persoanelor care îi înlocuiesc.

126. Persoana împuternicită a Centrului de certificare utilizează cheia sa privată în prezența administratorului securitate evitând încălcarea confidențialității cheii private.

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

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

Secțiunea 3. Resursele informaționale ale Centrului de certificare

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

130. Registrul certificatelor cheilor publice reprezintă totalitatea documentelor pe suport de hârtie și a documentelor electronice, cuprinzând:

- a) certificatele cheilor publice ale persoanelor împuternicite ale Centrului de certificare;
- b) deciziile privind suspendarea și restabilirea valabilității, 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 și restabilire a valabilității, 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 informaționale:

- 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 și distrugerea documentelor de arhivă se efectuează de către o comisie formată din angajați ai Centrului de certificare și colaboratori ai organului competent.

134. Pregătirea pentru distrugere și distrugerea documentelor care nu necesită a fi păstrate în arhivă se efectuează de către angajații Centrului de certificare, desemnați de conducătorul Centrului.

135. Protecția resurselor informaționale ale Centrului de certificare se efectuează în conformitate cu legislația în vigoare și cerințele stabilite de organul competent.

136. Modul de realizare a accesului la resursele informaționale ale Centrului de certificare, inclusiv a accesului la documentele de arhivă, se reglementează de prevederile legislației în vigoare, de cerințele stabilite de organul competent și de prezentul Regulament.

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

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

b) poștei electronice: pki@sis.md;

c) cererii scrise a utilizatorului semnăturii digitale în conformitate cu procedurile stabilite de prezentul Regulament. Adresa poștală: MD-2004, Republica Moldova, mun. Chișinău, bd. Ștefan cel Mare și Sfânt, nr. 166, Centrul de certificare al cheilor publice de nivel superior.

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

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

b) copiile electronice ale certificatelor cheilor publice, pe suport de hârtie, ale persoanelor împuternicite ale Centrului de certificare și 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 și 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 poștei electronice.

Secțiunea 4. Mijloacele de asigurare a activității Centrului de certificare

140. Centrul de certificare creează și 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) și 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 înregistrării.

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 informației de înregistrare a persoanelor împuternicite ale centrelor de certificare de nivelul al doilea;
- e) publicarea și difuzarea listelor certificatelor revocate;
- f) accesul la certificatele cheilor publice valabile și la listele certificatelor revocate;
- g) păstrarea altor informații ce țin 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 autenticității certificatelor cheilor publice și a altor documente electronice.

147. Mijloacele tehnice de asigurare a funcționării complexului tehnic de program al Centrului de certificare includ:

- a) echipamentul de server;
- b) echipamentul de telecomunicații;
- c) locurile de muncă computerizate ale administratorilor Centrului de certificare;
- d) dispozitivele de imprimare pe suport de hârtie;
- e) alte echipamente auxiliare.

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

149. În componența complexului tehnic de program al Centrului de certificare funcționează mijloacele de protecție criptografică a informației, inclusiv:

- a) mijloacele semnăturii digitale;
- b) complexe tehnice de program de protejare contra accesului neautorizat și de asigurare a integrității mijloacelor tehnice de program.

150. Responsabilitatea pentru exploatarea mijloacelor de protecție a informației o poartă administratorul sistem și administratorului securitate.

151. Complexul tehnic de program trebuie să corespundă cerințelor stabilite de organul competent și parametrilor tehnici indicați în anexa nr. 10 la prezentul Regulament.

IV. Asigurarea securității și protecția informațiilor confidențiale

Secțiunea 1. Confidențialitatea informației

152. Informațiile care se prelucrează și se păstrează în Centrul de certificare sînt protejate prin lege.

153. Informațiile care se păstrează în registrele de audit ale Centrului de certificare sînt confidențiale.

154. Nu sînt confidențiale informațiile ce se conțin 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 și controlul accesului la informațiile protejate de lege în conformitate cu legislația Republicii Moldova.

Secțiunea 2. Măsurile tehnico-inginerești de protecție a informației

156. Măsurile tehnico-inginerești de protecție a informației trebuie să asigure posibilitatea funcționării neîntrerupte, pe o durată îndelungată, a complexului tehnic de program al Centrului de certificare.

157. Serverele serviciului certificare, serviciului înregistrare și 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 cerințele 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 și de serviciu trebuie să fie dotate cu mijloace de ventilare și de condiționare a aerului care să asigure respectarea parametrilor optimi ai regimului de temperatură și umiditate.

162. Securitatea antiincendiară a încăperilor Centrului de certificare se asigură în conformitate cu normele și cerințele stabilite de legislația în vigoare.

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

Secțiunea 3. Măsurile de protecție a informației cu mijloacele de program și de aparataj

164. Complexul tehnic de program al Centrului de certificare trebuie să asigure controlul integrității mijloacelor tehnice și de program.

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

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

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

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

169. Accesul personalului de ingineri și al administratorilor sistem la serverele serviciului certificare, serviciului înregistrare și serviciului registru pentru îndeplinirea lucrărilor reglementare se efectuează în prezența 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.

Secțiunea 4. Măsurile organizatorice de protecție a informației

171. Măsurile organizatorice de protecție a informației trebuie să asigure:

- a) integritatea documentelor și a bunurilor materiale;
- b) depistarea și reținerea contraveniențelor care încearcă să pătrundă în clădirea (încăperile) Centrului de certificare.

172. În Centrul de certificare sînt prevăzute următoarele funcții:

- a) administratorul înregistrări, avînd ca sarcini de bază: înregistrarea și evidența 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 și restabilirea valabilității,

revocarea certificatelor cheilor publice, întocmirea și publicarea (emiterea) listei certificatelor revocate;

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

d) administratorul sistem, avînd ca sarcini de bază: instalarea, configurarea și întreținerea funcționării serviciului de certificare, serviciului de înregistrare și serviciului de registru.

173. Persoana împuternicită a Centrului de certificare se numește prin ordinul directorului Serviciului de Informații și Securitate, la propunerea conducătorului Centrului de certificare. Cerințele de calificare și obligațiile de serviciu ale persoanei împuternicite a Centrului de certificare se stabilesc în conformitate cu fișa postului.

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

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

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

Secțiunea 1. Modul de interacțiune a persoanelor împuternicite ale centrelor de certificare de nivelul al doilea și a utilizatorilor semnăturii digitale cu Centrul de certificare

176. Interacțiunea centrelor de certificare de nivelul al doilea și a utilizatorilor semnăturii digitale cu Centrul de certificare se efectuează în conformitate cu procedurile stabilite de prezentul Regulament și cu cerințele în domeniul semnăturii digitale.

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

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

179. În vederea interacțiunii, 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 poștală, adresa poștei electronice).

180. În cazul revocării certificatului cheii publice a persoanei împuternicite a Centrului de certificare, se revocă concomitent și 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 autenticității semnăturii digitale în documentul electronic.

182. În procesul interacțiunii persoanelor împuternicite ale centrelor de certificare de nivelul al doilea și a utilizatorilor semnăturii digitale cu Centrul de certificare pot apărea situații litigioase. Sînt supuse soluționării în conformitate cu prezentul Regulament situațiile 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 valabilității și autenticității certificatului cheii publice a persoanei împuternicite a Centrului de certificare;

b) contestarea de către utilizatorul semnăturii digitale a valabilității și autenticității 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 și a altor restricții indicate în certificatele cheilor publice eliberate de către Centrul de certificare;

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

g) alte cazuri de apariție a situațiilor litigioase în legătură cu aplicarea semnăturii digitale.

183. Situația litigioasă se soluționează în regim de lucru de către părțile interesate în conformitate cu Regulamentul de soluționare a situațiilor litigioase în domeniul aplicării semnăturii digitale, aprobat de organul competent.

184. În cazul în care situația litigioasă este considerată de către părți ca fiind soluționată, se întocmește un proces-verbal privind soluționarea situației litigioase, care se semnează de către părți.

185. În cazul imposibilității de soluționare a situației litigioase în regim de lucru, părțile se pot adresa în instanța de judecată, conform procedurilor prevăzute de legislație.

Secțiunea 2. Drepturile și obligațiile persoanei împuternicite a centrului de certificare de nivelul al doilea în interacțiunea cu Centrul de certificare

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

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

b) să depună cererea de certificare a cheii publice;

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

d) să obțină accesul la Registrul certificatelor cheilor publice;

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

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

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

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

i) să se adreseze la Centrul de certificare pentru confirmarea autenticității și valabilității certificatului cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea;

j) să obțină asistență metodică de la persoana împuternicită a Centrului de certificare.

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

a) să respecte cerințele legislației în domeniul aplicării semnăturii digitale;

b) să prezinte informațiile 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 și alte restricții 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 valabilității 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.

Secțiunea 3. Drepturile utilizatorului semnăturii digitale în cadrul interacțiunii cu Centrul de certificare

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

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

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

c) să obțină accesul la Registrul certificatelor cheilor publice;

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

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

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

VI. Reorganizarea și lichidarea Centrului de certificare

189. Reorganizarea și lichidarea Centrului de certificare se efectuează în conformitate cu legislația.

190. La reorganizarea Centrului de certificare și transmiterea funcțiilor lui la o altă instituție, prin decizia comună a conducătorilor instituțiilor interesate se creează o comisie de transmitere a Centrului de certificare.

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

- a) reprezentanții părților;
- b) conducătorul Centrului de certificare sau persoana care îl înlocuiește;
- c) reprezentantul organului competent;
- d) alte persoane desemnate de către părți.

192. La încheierea lucrărilor, comisia întocmește actul de predare-primire, în conformitate cu care instituției succesoare i se transmite Registrul certificatelor cheilor publice, precum și drepturile și obligațiile Centrului de certificare. Actul se semnează de către toți membrii comisiei și se aprobă de către conducătorii instituțiilor 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 hârtie se transmite sub formă de arhivă a documentelor pe suporturi de hârtie.

194. La transmiterea Centrului de certificare, cheile private ale persoanelor împuternicite ale Centrului de certificare se distrug, fără a se încălca confidențialitatea lor, în conformitate cu cerințele 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 Informații și Securitate se creează comisia de lichidare, în sarcina căreia se pune realizarea procedurii de lichidare în conformitate cu legislația în vigoare și cerințele stabilite de organul competent.

196. În componența comisiei de lichidare se includ:

- a) conducătorul Centrului de certificare sau persoana care îl înlocuiește;
- b) reprezentantul organului competent;
- c) alte persoane indicate în ordin.

197. La încheierea lucrărilor, comisia întocmește actul de lichidare, potrivit căruia Centrul de certificare își încetează activitatea, iar Registrul certificatelor

cheilor publice se transmite organului competent și se păstrează în arhivă conform legislației.

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 hârtie se transmite sub formă de arhivă a documentelor pe suporturi de hârtie, pe baza actului de primire-predare. Actul se semnează de către conducătorul Centrului de certificare, reprezentantul organului competent responsabil de păstrare și se aprobă de către directorul Serviciului de Informații și Securitate.

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

Anexa nr. 1
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

**Structura certificatului cheii publice
a persoanei împuternicite a Centrului de certificare de nivel superior**

Certificatul cheii publice a persoanei împuternicite a Centrului de certificare de nivel superior conține următoarele câmpuri:

Denumirea (în engleză)	Descrierea	Conținutul
<i>Câmpurile de bază</i>		
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Numărul
Issuer	Datele de identificare ale Centrului de certificare de nivel superior	<p>N = Numele, prenumele persoanei împuternicite a Centrului de certificare de nivel superior, IDNP</p> <p>CN = MoldovaCA</p> <p>L = Chișinău</p> <p>S = Republica Moldova</p> <p>OU = Centrul de certificare de nivel superior</p> <p>O = Serviciul de Informații și Securitate al Republicii Moldova, IDNO</p> <p>P = Telefonul persoanei împuternicite</p> <p>T = Funcția persoanei împuternicite a Centrului de certificare de nivel superior</p> <p>C = MD</p> <p>E = pki@sis.md</p>
Validity Period	Termenul de valabilitate a certificatului	<p>Valabil de la: " __ " _____ 20__ oo:mm:ss GMT</p> <p>Valabil pînă la: " __ " _____ 20__ oo:mm:ss GMT</p>

Subject	Datele de identificare ale Centrului de certificare de nivel superior	<p>N = Numele, prenumele persoanei împuternicite a Centrului de certificare de nivel superior, IDNP</p> <p>CN = MoldovaCA</p> <p>L = Chișinău</p> <p>S = Republica Moldova</p> <p>OU = Centrul de certificare de nivel superior</p> <p>O = Serviciul de Informații și Securitate al Republicii Moldova, IDNO</p> <p>P = Telefonul persoanei împuternicite</p> <p>T = Funcția persoanei împuternicite a Centrului de certificare de nivel superior</p> <p>C = MD</p> <p>E = pki@sis.md</p>
FriendlyName	Nume în clar	MoldovaCA
Public Key	Cheia publică	Cheia publică (algoritmul RSA)
Issuer Signature Algorithm	Algoritmul semnăturii emitentului certificatului	SHA-1/RSA
Issuer Sign	Semnătura digitală a emitentului certificatului	Semnătura emitentului în conformitate cu SHA-1/RSA
<i>Cîmpurile auxiliare</i>		
Key Usage	Utilizarea cheii	Irevocabilitatea, Semnătura digitală în certificatele persoanelor împuternicite ale centrelor de certificare de nivel al doilea, Semnătura digitală în lista certificatelor revocate (CRL)
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a persoanei împuternicite a Centrului de certificare de nivel superior, corespunzătoare prezentului certificat

PrivateKeyUsagePeriod	Termenul de valabilitate a cheii private	Valabil de la: " __ " _____ 20__ oo:mm:ss GMT Valabil pînă la: " __ " _____ 20__ oo:mm:ss GMT
CRL Distribution Point	Punctul de distribuție a listei certificatelor revocate (CRL)	URL= http://www.pki.sis.md/cert/rootca.crl
Certificate Template	Modelul certificatului	CA

Anexa nr. 2
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

Structura listei certificatelor revocate (CRL)

Lista certificatelor revocate a Centrului de certificare de nivel superior conține următoarele câmpuri:

Denumirea (în engleză)	Descrierea	Conținutul
<i>Câmpurile de bază</i>		
Version	Versiunea	V2
Issuer	Emitentul CRL	<p>N= Numele, prenumele persoanei împuternicite a Centrului de certificare de nivel superior, IDNP</p> <p>CN = MoldovaCA</p> <p>L = Chișinău</p> <p>S = Republica Moldova</p> <p>OU = Centrul de certificare de nivel superior</p> <p>O = Serviciul de Informații și Securitate al Republicii Moldova, IDNO</p> <p>P = Telefonul persoanei împuternicite</p> <p>T = Funcția persoanei împuternicite a Centrului de certificare de nivel superior</p> <p>C = MD</p> <p>E = pki@sis.md</p>
thisUpdate	Data emiterii CRL	" __ " _____ an. 20__ oo:mm:ss GMT
nextUpdate	Termenul pentru care este valabilă CRL	« __ » _____ an. 20__ oo:mm:ss GMT
RevokedCertificates	Lista certificatelor revocate	<p>Numărul certificatului (CertificateSerialNumber)</p> <p>Data revocării sau suspendării valabilității certificatului (Time)</p>

Issuer Signature Algorithm	Algoritmul semnăturii emitentului certificatului	SHA-1/RSA
Issuer Sign	Semnătura digitală a emitentului certificatului	Semnătura emitentului în conformitate cu SHA-1/RSA
<i>Cîmpurile auxiliare</i>		
Reason Code	Codul cauzei revocării certificatului	"0" Nu este indicată "1" Compromiterea cheii private "2" Compromiterea Centrului de certificare "3" Schimbarea apartenenței "4" Certificatul a fost schimbat "5" Încetarea activității "6" Suspendarea valabilității
holdInstructionCode	Codul cauzei de suspendare temporară a valabilității certificatului	Codul cauzei de suspendare temporară a valabilității certificatului (OID)
Authority Key Identifier	Identificatorul cheii emitentului	Identificatorul cheii private a persoanei împuternicite a Centrului de certificare de nivel superior cu utilizarea căreia este semnată CRL
CRLNumber	Numărul de serie	Numărul de serie CRL

Anexa nr. 3
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

**Cerere-model de certificare a cheii publice
a persoanei împuternicite a centrului de certificare de nivelul al doilea**

**Centrului de certificare a cheii publice
de nivel superior**

**Cerere
pentru certificarea cheii publice**

Prin prezenta _____
(numele și prenumele persoanei împuternicite)

Numărul buletinului de identitate: _____

IDNP: _____, e-mail: _____,

adresa poștală: _____

telefon/fax: _____,

fiind persoană împuternicită _____

(denumirea centrului de certificare de nivelul al doilea)

certificatul de înregistrare nr. _____ din " ____ " _____ 200__,

eliberat _____

(numele persoanei juridice care a creat centrul de certificare de nivelul al doilea)

(adresa juridică)

Rog eliberarea certificatului cheii publice

_____ în conformitate cu datele indicate în prezenta cerere și includerea în certificat a următoarelor informații:

N (Name) = _____

(numele, prenumele persoanei împuternicite)

IDNP = _____

(numărul de identificare al persoanei fizice – persoana împuternicită)

CN (Common Name) = _____

(denumirea centrului de certificare)

L (Locality) = _____

(localitatea)

S (State) = _____

(statul)

OU (Organizational Unit) = _____

(denumirea subdiviziunii persoanei juridice)

O (Organization) = _____

(denumirea persoanei juridice)

T (Title) = _____

(funcția persoanei împuternicite)

C (Country) = _____
(codul statului)

E (Email) = _____
(adresa poștei electronice)

Modelele certificatului:

- _____;
- _____.

Mijlocul semnăturii digitale (CryptoProvider): _____

Cheia publică certificată: _____

Numele fișierului cererii de certificare a cheii publice în corespundere cu PKCS#10 _____

Codul poștal și adresa persoanei juridice _____

Telefonul de contact al persoanei juridice _____

Telefonul de contact al persoanei împuternicite _____,
inclusiv următoarele date despre domeniile de aplicare a semnăturii digitale și alte restricții impuse:

_____.

Obligațiile funcționale ale _____
(funcția, numele, prenumele)

sînt confirmate _____
(mențiunile documentului privind numirea persoanei împuternicite)

L.Ș.

Funcția _____

(semnătura)

" " _____ 200__

(numele, prenumele)

Prin prezenta confirm că cererea de certificare a cheii publice pe numele

(numele și prenumele)

persoana _____
(numele și prenumele)

este identificată. Datele indicate în cerere sînt verificate.

" " _____ 200__

Administratorul înregistrări

L.Ș.

(semnătura)

(numele, prenumele)

Anexa nr. 4
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

**Structura cererii de certificare a cheii publice a persoanei împuternicite
a centrului de certificare de nivelul al doilea sub formă de document electronic**

Cererea de certificare a cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea sub formă de document electronic conține următoarele câmpuri de bază:

Denumirea (în engleză)	Descrierea
N (Name)	Numele, prenumele persoanei împuternicite a centrului de certificare
IDNP	Numărul de identificare al persoanei fizice – persoana împuternicită a centrului de certificare
CN (Common Name)	Denumirea centrului de certificare
L (Locality)	Localitatea
S (State)	Statul
OU (Organizational Unit)	Subdiviziunea persoanei juridice
O (Organization)	Denumirea persoanei juridice
T (Title)	Funcția persoanei împuternicite a centrului de certificare
C (Country)	Codul statului
E (Email address)	Adresa poștei electronice a persoanei împuternicite a centrului de certificare
OID (Certificate Template)	Modelul certificatului
CryptoProvider	Mijloacele semnăturii digitale
Public Key	Cheia publică certificată
FileName	Numele fișierului în care este înscrisă cererea de certificare
Street address	Adresa centrului de certificare
Postal code	Codul poștal al centrului de certificare
Phone, Fax	Telefonul, faxul centrului de certificare
Celelalte proceduri de generare a cererii de certificare se efectuează conform RFC 2986	

Anexa nr. 5
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

**Structura certificatului cheii publice a persoanei împuternicite
a centrului de certificare de nivelul al doilea**

Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivelul al doilea include următoarele câmpuri:

Denumirea (în engleză)	Descrierea	Conținutul
<i>Câmpurile de bază</i>		
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Numărul
Issuer	Datele de identificare ale Centrului de certificare de nivel superior	N= Numele, prenumele persoanei împuternicite a Centrului de certificare de nivel superior, IDNP CN = MoldovaCA L = Chișinău S = Republica Moldova OU = Centrul de certificare de nivel superior O = Serviciul de Informații și Securitate al Republicii Moldova, IDNO P = Telefonul persoanei împuternicite T = Funcția persoanei împuternicite a Centrului de certificare de nivel superior C = MD E = pki@sis.md
Validity Period	Termenul de valabilitate a certificatului	Valabil de la: " __ " _____ 20__ oo:mm:ss GMT Valabil pînă la: " __ " _____ 20__ oo:mm:ss GMT

Subject	Datele de identificare ale centrului de certificare de nivelul al doilea	<p>N = Numele, prenumele persoanei împuternicite a centrului de certificare de nivelul al doilea, IDNP</p> <p>CN = Denumirea centrului de certificare de nivelul al doilea</p> <p>L = Chișinău</p> <p>S = Republica Moldova</p> <p>OU = Subdiviziunea persoanei juridice ce administrează centrul de certificare de nivelul al doilea</p> <p>O = Denumirea persoanei juridice ce administrează centrul de certificare de nivelul al doilea</p> <p>P = Telefonul</p> <p>T = Funcția persoanei împuternicite a centrului de certificare de nivelul al doilea</p> <p>C = MD</p> <p>E = ___@____.____</p>
FriendlyName	Numele în clar	Denumirea centrului de certificare de nivelul al doilea (la alegerea centrului de certificare de nivelul al doilea)
Public Key	Cheia publică a persoanei împuternicite a centrului de certificare de nivelul al doilea	Cheia publică (algoritmul ____)
Subject Signature Algorithm	Algoritmul semnăturii titularului certificatului	Funcția hash/algoritmul semnăturii
Issuer Signature Algorithm	Algoritmul semnăturii emitentului certificatului	SHA-1/RSA
Issuer Sign	Semnătura digitală a emitentului certificatului	Semnătura emitentului în conformitate cu SHA-1/RSA
<i>Cîmpurile auxiliare</i>		
Key Usage	Utilizarea cheii	Irevocabilitatea, Semnătura digitală în

		certificatul persoanei împuternicite a centrului de certificare de nivelul al doilea, Semnătura digitală în lista certificatelor revocate (CRL)
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a persoanei împuternicite a Centrului de certificare de nivel superior corespunzător certificatului dat
PrivateKeyUsagePeriod	Perioada de valabilitate a cheii private	Valabilă de la: " __ " _____ 20__ oo:mm:ss GMT Valabilă pînă la: " __ " _____ 20__ oo:mm:ss GMT
CRL Distribution Point	Punctul de distribuire a listei certificatelor revocate (CRL)	URL= http://www.pki.sis.md/cert/rootca.crl
Certificate Template	Modelul certificatului	SubCA

Anexa nr. 6
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

**Cerere-model de suspendare a valabilității certificatului cheii publice
a persoanei împuternicite a centrului de certificare de nivelul al doilea**

**Centrului de certificare a cheilor publice
de nivel superior**

**Cerere
de suspendare a valabilității certificatului cheii publice**

Prin prezenta _____
(numele, prenumele persoanei împuternicite)

Numărul buletinului de identitate: _____

IDNP: _____

Numărul de înregistrare în centrul de certificare _____,
fiind persoană împuternicită a _____

(denumirea centrului de certificare de nivelul al doilea)

certificatul de înregistrare nr. _____ din " ____ " _____ 200__

rog să suspendați valabilitatea certificatului cheii publice emis pe numele meu

nr. _____

pe o durată de _____ zile,
(numărul de zile cu litere)

în legătură cu _____
(motivul suspendării)

Persoana împuternicită a centrului de certificare

(semnătura) / _____
(numele, prenume)

Conducătorul centrului de certificare

(semnătura) / _____
(numele, prenumele)

L.Ș.

" ____ " _____ 200__

Anexa nr. 7
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

**Cerere-model de restabilire a valabilității certificatului cheii publice
a persoanei împuternicite a centrului de certificare de nivelul al doilea**

**Centrului de certificare a cheilor publice
de nivel superior**

**Cerere
de restabilire a valabilității certificatului cheii publice**

Prin prezenta _____
(numele, prenumele persoanei împuternicite)

Numărul buletinului de identitate: _____

IDNP: _____

Numărul de înregistrare în centrul de certificare _____,

fiind persoană împuternicită a _____,

(denumirea centrului de certificare de nivelul al doilea)

certificatul de înregistrare nr. _____ din " ____ " _____ 200 __,

rog să restabiliți valabilitatea certificatului cheii publice emis pe numele meu

nr. _____

suspendat pe o durată de _____ zile,

(numărul de zile cu litere)

în legătură cu _____.

(motivul suspendării)

Motivul de restabilire a valabilității certificatului cheii publice _____

_____.

" ____ " _____ 200 __

Persoana împuternicită a centrului de certificare

_____/_____
(semnătura) / (numele, prenumele)

Conducătorului centrului de certificare

_____/_____
(semnătura) / (numele, prenumele)

L.Ș.

Anexa nr. 8
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

**Cerere-model de revocare a certificatului cheii publice
a persoanei împuternicite a centrului de certificare de nivelul al doilea**

**Centrului de certificare a cheilor publice
de nivel superior**

**Cerere
de revocare a certificatului cheii publice**

Prin prezenta _____
(numele, prenumele persoanei împuternicite)

Numărul actului de identitate: _____

IDNP: _____

Numărul de înregistrare în centrul de certificare _____,

fiind persoană împuternicită a _____

(denumirea centrului de certificare de nivelul al doilea)

certificatul de înregistrare nr. _____ din " ____ " _____ 200__

rog să revocați certificatul cheii publice emis pe numele meu

nr. _____

în legătură cu _____

(motivul revocării)

" ____ " _____ 200__

Persoana împuternicită a centrului de certificare

(semnătura) / _____
(numele, prenumele)

Conducătorul centrului de certificare

(semnătura) / _____
(numele, prenumele)

L.Ș.

Anexa nr. 9
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

**Cerere-model de confirmare a autenticității și valabilității
certificatului cheii publice**

**Centrului de certificare a cheilor publice
de nivel superior**

**Cerere
de confirmare a autenticității și valabilității certificatului cheii publice**

Prin prezenta, _____,
(numele și prenumele solicitantului)

Numărul buletinului de identitate: _____

Datele de contact _____

rog să confirmați autenticitatea și valabilitatea certificatului cheii publice

numărul de înregistrare _____

eliberat pe numele _____
(numele și prenumele)

La prezenta cerere se anexează certificatul cheii publice

numărul de înregistrare _____

eliberat pe numele _____
(numele și prenumele)

Sub formă de document electronic pe suportul material

(tipul și numărul suportului material)

"__" _____ 200__

(semnătura) / _____
(numele, prenumele)

Anexa nr. 10
la Regulamentul Centrului de certificare
a cheilor publice de nivel superior

**Parametrii tehnici ai complexului tehnic de program
al Centrului de certificare de nivel superior**

Nr. d/o	Criteriul	Parametrii tehnici
1.	Metodele de certificare	Prin rețea, ierarhică
2.	Ansamblul serviciilor de certificare	Fără restricții
3.	Ansamblul serviciilor de înregistrare	Fără restricții
4.	Proporționarea	Cantitatea certificatelor eliberate fără restricții
5.	Formatul certificatului și al listei certificatelor revocate	În conformitate cu ISO/IEC 9594/8 Directory Services (X.509 v3) RFC 3280 (fostul RFC 2459) Certificate and Certificate Revocation List (CRL) Profile
6.	Suplimentele certificatului	X.509 v 3, PKIX, FPKX, Web, SET, VPN, stabilite de utilizator
7.	Formatul certificatului de utilizare limitată	În conformitate cu RFC 3039
8.	Formatul certificatului pentru autorizare	În conformitate cu RFC 3281
9.	Politica de aplicare a certificatelor și structura regulamentului	În conformitate cu RFC 2527 Certificate Policy and Certification Practices Framework
10.	Protocoalele de administrare a certificatelor	În conformitate cu RFC 2510 Certificate Management Protocols (CMP)
11.	Cererea de certificare	În conformitate cu RFC 2986 Certification Request Syntax Specification
12.	Protocolul de determinare a statutului certificatului	În conformitate cu RFC 2560 Online Certificate Status Protocol (OCSP)
13.	Metodele de revocare a certificatului	Prin distribuirea listelor certificatelor revocate, protocolul OCSP
14.	Obținerea din registrul certificatelor și a listei certificatelor revocate	În conformitate cu RFC 2585 HTTP/FTP Operations

		Distribuirea automatizată a listelor certificatelor revocate prin poșta electronică
15.	Administrarea certificatelor pe baza mesajelor de administrare a certificatelor	În conformitate cu RFC 2797 Certificate Management Messages over CMS (CMC)
16.	Algoritmele și identificatoarele pentru profilurile certificatelor și listelor certificatelor revocate CAC PKIX	În conformitate cu RFC 3279 (fostul RFC 2528) Algorithms and Identifiers for Internet X.509 Public Key Infrastructure Certificate and CRL Profile
17.	Algoritmele semnăturii digitale	RFC3447 – Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1; GOST P 34.10-94 GOST P 34.10-2001
18.	Algoritmele de calculare a funcțiilor hash	RFC3174 – US Secure Hash Algorithm 1(SHA1) GOST P 34.11-94
19.	Protocoalele serverului de certificare și verificare a autenticității datelor	În conformitate cu RFC 3029 Data Validation and Certification Server Protocols
20.	Protocoalele de exploatare a infrastructurii cheilor publice	În conformitate cu RFC 2559 LDAP v2
21.	Schema de susținere PKIX în LDAP v2	În conformitate cu RFC 2587 LDAP v2 Schema
22.	Comunicarea cu clientul (subsistemul de recepționare a certificatelor)	PKCS#10/7, PKCS#12, cu ajutorul citirii codului PIN, prin poșta electronică, SSL, PKIX-CMP
23.	Comunicarea între subsistemele de certificare și de înregistrare	Mesajele semnate, PKIX-CMP
24.	Mecanismele de înregistrare	Prezența personală a utilizatorului, prin intermediul web, poștei electronice, conexiunii VPN
25.	Susținerea cataloagelor	Catalogul propriu sau susținerea altui catalog LDAP v2 și v3
26.	Susținerea smart-cardurilor	Standardele: ISO 7816-1/2/3, PKCS#11, PC/SC, alte standarde legate de smart-card
27.	Restabilirea cheilor	Posibilitatea de rezervare a cheilor administratorilor și ai utilizatorilor

28.	Protocoalele de înregistrare a marcajelor de timp	În conformitate cu RFC 3161 Time-Stamp Protocol (TSP)
29.	Administrarea siguranței ciclului vital al procesului de certificare	Fiabilitatea în timpul verificării statutului certificatului Deservirea garantată a utilizatorilor Crearea sistemului de control al tuturor acțiunilor administratorului în legătură cu certificatul, controlul integrității certificatului
30.	Asigurarea integrității bazelor de date ale certificatelor, titularilor certificatelor etc.	Utilizarea concepției de bază de date sigură, administrarea discretă și mandatară a accesului, marcajele, utilizarea repetată a obiectului, calea veridică; crearea sistemului de copiere de rezervă
31.	Asigurarea securității cheilor private	Crearea, păstrarea și utilizarea sigură, sistemul multifactorial de autentificare
32.	Controlul securității	Înregistrarea și controlul evenimentelor în subsisteme Ținerea, prelucrarea și verificarea registrelor de control Asigurarea securității registrelor de control împotriva modificării și distrugerii neautorizate