REG-08
REGULAMENTUL CENTRULUI DE CERTIFICARE A CHEILOR PUBLICE

CUPRINS

ANEXE

- Anexa nr. 1 Structura certificatului cheii publice a centrului de certificare
- Anexa nr. 2 Structura certificatului cheii publice a utilizatorului semnăturii electronice
- Anexa nr. 3 Lista certificatelor revocate (CRL)
- Anexa nr. 4 Cerere pentru certificarea cheii publice - persoane fizice
- Anexa nr. 5 Cerere pentru certificarea cheii publice - persoane juridice
- Anexa nr. 6 Cererea de modificare a statutului certificatului cheii publice

1. DISPOZIŢII GENERALE

Regulamentul Prestatorului de servicii a cheilor publice este elaborat în conformitate următoarele acte normative:

- Legea nr. 91 din 29.05.2014 privind semnătura electronică şi documentul electronic (în vigoare din luna ianuarie, 2015, iar în partea ce ţine de procedurile judiciare – din luna ianuarie, 2016);
- Legea nr. 284 din 22.07.2004 privind comerţul electronic;
- Hotărîrea Guvernului nr. 945 din 05.09. 2005 „Cu privire la centrele de certificare a cheilor publice ";
- Hotărîrea Guvernului nr. 320 din 28.03.2006 „Pentru aprobarea Regulamentului privind ordinea de aplicare a semnăturii digitale în documentele electronice ale autorităţilor publice";
- Condiţiilor speciale de activitate a centrelor de certificare a cheilor publice, aprobate prin Ordinul Serviciului de Informaţii şi Securitate al Republicii Moldova nr. 13 din 03.04. 2006;
- Regulamentul privind procedura de înregistrare a Centrelor de certificare a cheilor publice, aprobat prin Ordinul Serviciului de Informaţii şi Securitate al Republicii Moldova nr. 13 din 03.04. 2006;
- Regulamentul CC a cheilor publice de nivel superior, aprobat prin Ordinul Serviciului de Informaţii şi Securitate al Republicii Moldova nr. 13 din 03.04. 2006;
- Normele tehnice in domeniul semnăturii digitale, aprobate prin Ordinul Serviciului de Informaţii şi Securitate al Republicii Moldova nr. 64 din 07.12.2006;
- Alte acte normative în vigoare stabilite de organul împuternicit.
- Regulamentul de soluționare a situațiilor litigioase în domeniul aplicării semnăturii digitale, aprobat prin Ordinul Serviciului de Informaţii şi Securitate al Republicii Moldova nr. 29 din 16.04.2009.

Pe lîngă documentul de bază cu privire la activitatea Centrul de Certificare a cheilor publice, mai există un şir de acte suplimentare de uz intern, și anume:

- Politica de certificare a cheilor publice;
- Politica de securitate și control al accesului în Centrul de certificare a cheilor publice;
- Instrucţiunea ce reglementează securitatea şi exploatarea MPCI;
- Ordinea de sincronizare a timpului după GMT.
- Plan de recuperare al activității Centrului de certificare a cheilor publice.

2. SCOP

REG-08 Regulamentul Centrului de Certificare a cheilor publice stabileşte condiţiile generale de organizare a activităţii Centrului de Certificare a cheilor publice a cheilor publice (*în continuare – CC*), precizează funcţiile, obligaţiile şi drepturile acestuia, mecanismul şi procedurile aplicate de către CC şi modul de conlucrare cu titularii certificatelor cheii publice, măsurile tehnico-organizatorice de bază pentru asigurarea securităţii.

Scopul acestui document este informarea și convingerea titularilor certificatelor cheilor publice în faptul că nivelul de încredere în certificatele publicate se datorează practicii de lucru în domeniul respectiv al CC.

3. DOMENIU DE APLICARE

Prezentul regulament este un act normativ intern în domeniul serviciilor de certificare în cadrul infrastructurii cheilor publice (PKI) unice în Republica Moldova. Acţiunea prevederilor

Regulamentului se extinde asupra tuturor participanţilor Centrului de certificare a Î.S. „Fiscservinform", independent de subordonarea sau locaţia acestora. Prezentul regulament intră în vigoare după aprobare, ulterior fiind plasat pe www.pki.fsi.md.

Centrul de Certificare a cheilor publice *(în continuare – CC)* este o subdiviziune structurală a Î.S. „Fiscservinform" care îşi desfăşoară activitatea în domeniul prestării serviciilor de certificare a cheilor publice şi a altor servicii în domeniul semnăturii electronice.

4. TERMINOLOGIE ŞI ABREVIERI

Centrul de certificare a cheilor publice – prestator de servicii de certificare a cheilor publice, responsabil de emiterea certificatelor şi gestionarea ulterioară a acestora.

Centrul de înregistrări - subiectul responsabil de identificarea şi autentificarea solicitanţilor, formarea cererii pentru certificare şi executarea unui şir de proceduri legate de gestionarea certificatelor (revocare, suspendare, reînnoire).

PKI – arhitectura, tehnicile, practicile şi procedurile care contribuie la implementarea şi funcţionarea sistemelor criptografice cu chei publice şi care constă din hardware şi software, baze de date, resurse de reţea, proceduri de securitate şi obligaţii legale, legate împreună şi care colaborează pentru a furniza şi implementa atît servicii de certificare cît şi alte servicii asociate infrastructurii;

Certificat al cheii publice - document electronic ce conţine cheia publică, este semnat cu semnătura electronică a prestatorului de servicii de certificare, atestă apartenenţa cheii respective titularului de certificat al cheii publice şi permite identificarea acestui titular;

Cheie privată – consecutivitate digitală unică, formată prin intermediul dispozitivului de creare a semnăturii electronice şi destinată a fi utilizată pentru crearea semnăturii electronice;

Cheie publică – consecutivitate digitală unică, formată prin intermediul dispozitivului de creare a semnăturii electronice, care corespunde cheii private interdependente şi este destinată a fi utilizată pentru verificarea autenticităţii semnăturii electronice;

Servicii de certificare – servicii de certificare a cheilor publice, de aplicare a mărcii temporale, alte servicii conexe în domeniul semnăturii electronice;

Semnătură electronică – date în formă electronică, care sunt ataşate la, sau logic asociate cu alte date în formă electronică şi care sunt utilizate ca metodă de autentificare;

Document electronic – informaţie în formă electronică, creată, structurată, prelucrată, păstrată şi/sau transmisă prin intermediul computerului sau al altor dispozitive electronice, semnată cu semnătură electronică în conformitate cu legislaţia cu privire la semnătura electronică şi documentul electronic;

Semnatar – persoană care deţine un dispozitiv de creare a semnăturii electronice şi care acţionează fie în nume propriu, fie în numele persoanei fizice, al persoanei juridice sau al entităţii pe care o reprezintă;

Titularul certificatului cheii publice – persoana pe numele căreia CC a eliberat certificatul cheii publice şi care deţine cheia privată corespunzătoare, ce permite semnarea documentului electronic;

Dispozitiv de creare a semnăturii electronice – mijloace tehnice şi/sau de program configurate, utilizate pentru punerea în aplicare a datelor de creare a semnăturii electronice;

Prestator de servicii de certificare – întreprinzător individual sau persoană juridică care prestează servicii de certificare;

repozitoriu - sursa informaţională de bază a Centrului de certificare ce reprezintă totalitatea bazelor de date, accesibile public, sub formă de documente pe suport de hârtie şi documente electronice, unde sunt stocate certificatele cheilor publice, emise de Centrul de certificare a cheilor publice, şi informaţia suplimentară cu privire la funcţionarea corectă a infrastructurii (CRL, prezentul Regulament, etc.);

Solicitant – subiectul (persoană fizică sau juridică), care depune cererea pentru primirea certificatului cheii publice;

Abonat - persoană fizică sau juridică căreia îi este eliberat certificatul cheii publice de către Centrul de certificare a cheilor publice a Î.S. „Fiscservinform”.

***Notă:** Prezentul regulament foloseşte termenii definiţi în Legea nr. 91 din 27.06.2014 privind semnătura electronică și documentul electronic.

Abrevieri:
CC – Centrul de Certificare a cheilor publice;
CÎ – Centrul de Înregistrări;
AÎ – Administrator înregistrare;
AC – Administrator certificare;
PKI – Infrastructură de chei publice (Public Key Infrastructure);
CRL –lista certificatelor revocate (Certificate Revocation List);
UTC – Timpul universal coordonat.

5. DESCRIERE ACTIVITĂŢI

5.1 Structura și funcţiile Centrului de Certificare a cheilor publice

5.1.1 Centrul de certificare a cheilor publice

Persoanele împuternicite ale CC se numesc prin ordinul administratorului Î.S. „Fiscservinform”, la propunerea conducătorului CC. Conducătorul CC se numeşte în funcţie prin ordinul administratorului Î.S. „Fiscservinform”.

Cerinţele de calificare şi obligaţiile de serviciu ale persoanelor împuternicite ale CC se stabilesc în conformitate cu fişa postului. Administratorul sistem şi administratorul securitate ai CC trebuie să aibă studii superioare tehnice de inginer. Accesul angajaţilor la documentele CC se organizează în conformitate cu sarcinile de serviciu aprobate de conducătorul CC.

În cadrul CC, sub aspect structural, sunt prevăzute următoarele funcţii:

a) conducătorul CC, avînd ca sarcină de bază organizarea activităţii CC;

b) administratorul înregistrări (persoana împuternicită a CC), este responsabil de:

- verificarea corespunderii datelor indicate în cererea de certificare a cheii publice în baza documentelor ce confirmă datele în cauză prezentate de către solicitantul certificatului cheii publice;
- înregistrarea şi evidenţa titularilor certificatelor cheilor publice în procesul creării, suspendării sau restabilirii valabilităţii şi revocării certificatelor cheilor publice;
- pregătirea solicitărilor titularilor certificatelor cheilor publice;
- eliberarea certificatelor cheilor publice titularilor acestora;
- înştiinţarea solicitantului certificatului cheii publice despre refuzul motivat de eliberare a certificatului cheii publice;
- înştiinţarea titularului certificatului despre faptele care fac imposibilă utilizarea în continuare a cheii private, precum şi despre revocarea certificatului cheii publice;
- asigurarea semnării actelor juridice cu solicitanţii privind eliberarea semnăturii electronice.

c) administratorul certificare (persoana împuternicită a CC), este responsabil de:

- crearea (generarea), suspendarea şi restabilirea valabilităţii certificatelor cheilor publice;

- verificarea corespunderii informaţiilor din certificatul cheii publice cu informaţiile prezentate de către titularul certificatului cheii publice;
- revocarea certificatelor cheilor publice;
- ţinerea registrelor de evidenţă a certificatelor cheilor publice generate şi revocate;
- întocmirea actelor juridice privind eliberarea semnăturilor electronice;
- întocmirea şi publicarea (emiterea) listei certificatelor cheilor publice revocate.

d) administratorul securitate, este responsabil de:
- controlul securităţii tuturor procedurilor şi mecanismelor CC;
- asigurarea securităţii componentelor complexului tehnic de program al CC;
- elaborarea şi implementarea politicii de securitate a CC.

e) administratorul sistem, este responsabil de: instalarea, configurarea şi întreţinerea funcţionării infrastructurii CC

Centrul de certificare a cheilor publice îndeplineşte următoarele funcţii:

a) creează infrastructura PKI ca platformă pentru toate serviciile electronice, prestate de către Î.S. „Fiscservinform", în care se aplică semnătură electronică în baza certificatului cheii publice, eliberat de CC.
b) creează (generează) şi eliberează certificatul cheii publice pentru persoane fizice şi juridice;
c) suspendă şi restabileşte valabilitatea, revocă certificatele cheilor publice ale persoanelor fizice şi juridice emise de către CC;
d) întocmeşte, gestionează şi actualizează registrul certificatelor cheilor publice generate şi revocate;
e) confirmă autenticitatea şi valabilitatea certificatelor cheilor publice ale persoanelor fizice şi juridice;

Pentru îndeplinirea funcţiilor sale Centrul de certificare a cheilor publice:

- asigură înregistrarea persoanele fizice şi juridice ce solicită eliberarea certificatelor cheii publice;
- asigură crearea şi eliberarea certificatelor cheilor publice pe baza cererii persoanelor fizice şi persoanelor împuternicite ale persoanelor juridice, sub formă de document pe suport de hîrtie, semnat cu semnătură olografă, în conformitate cu procedurile stabilite de prezentul Regulament;
- suspendă şi restabileşte valabilitatea, revocă certificatele cheilor publice ale titularilor în cazurile şi în conformitate cu procedurile stabilite de prezentul Regulament, actele juridice încheiate şi legislaţia în vigoare;
- întocmeşte şi gestionează Registrul certificatelor cheilor publice sub formă de documente electronice;
- publică şi actualizează Registrul certificatelor cheilor publice revocate;
- acordă consultaţii şi suport metodologic persoanelor fizice şi juridice;
- confirmă autenticitatea şi valabilitatea certificatelor cheilor publice ale persoanelor fizice şi juridice;
- desfăşoară activitatea în domeniul protecţiei criptografice şi tehnice a informaţiei;
- creează sistemele informaţionale şi de comunicaţii electronice ale CC, asigură funcţionarea, securitatea, deservirea şi modernizarea lor, efectuează auditul intern permanent al securităţii şi funcţionalităţii acestor sisteme.

5.1.2 Centrul de înregistrare

CC are posibilitatea de a crea Centre de înregistrări de la distanţă (*în continuare - CÎ*), pentru optimizarea şi comoditatea interacţiunii cu persoanele fizice şi juridice, potenţiali titulari

ale certificatelor cheii publice. CÎ îndeplinesc unele funcții ale AÎ (*în continuare - AÎ*), cu condiția executării tuturor condițiilor înaintate de către CC.

CÎ sunt subdiviziuni ale Î.S. „Fiscservinform", sau persoane juridice distincte, exercitînd activitatea în bază de contract, care au drept scop executarea funcţiilor AÎ în conformitate cu prezentul Regulament.

În cadrul CÎ au loc următoarele proceduri:

a) identificarea şi înregistrarea solicitantului pentru certificarea cheii publice;
b) primirea şi prelucrarea documentelor cererilor pentru certificare, suspendare, restabilire a validităţii şi revocare a certificatului cheii publice;
c) eliberarea şi actualizarea certificatelor cheilor publice titularilor.

5.2 Drepturile și obligațiile Centrului de certificare a cheilor publice și ale titularilor certificatelor cheilor publice.

5.2.1 Drepturile și obligațiile Centrului de Certificare a cheilor publice

Centrul de Certificare a cheilor publice este obligat:

- să-şi desfăşoare activitatea în strictă conformitate cu legislaţia şi cerinţele stabilite de organul abilitat cu elaborarea şi promovarea politicii de stat şi cu exercitarea controlului în domeniul aplicării semnăturii electronice (în continuare – organul competent);
- să utilizeze dispozitive securizate ce dispun de certificatul de conformitate eliberat în conformitate cu legislaţia în vigoare;
- să utilizeze dispozitive securizate în conformitate cu documentaţia de exploatare;
- să organizeze regimul interior de funcţionare a CC astfel încît să se excludă posibilitatea accesului persoanelor terţe la dispozitivele securizate, la modificarea şi utilizarea lor neautorizată;
- să asigure securitatea cheilor private, să creeze condiţiile necesare pentru excluderea accesului neautorizat la cheile private;
- să administreze suporturile materiale de chei private în conformitate cu cerinţele stabilite de organul competent;
- să utilizeze cheia privată a persoanei împuternicite a CC numai la semnarea certificatelor cheilor publice eliberate de acesta şi a listelor certificatelor revocate;
- să creeze lista certificatelor revocate în conformitate cu cerinţele stabilite de organul competent şi de prezentul Regulament, conform Anexei nr. 2;
- să nu utilizeze cheia privată pentru crearea semnăturii electronice dacă există dovezi (suspiciuni) că a fost încălcată confidenţialitatea cheii private;
- să suspende imediat valabilitatea certificatului cheii publice dacă există dovezi (suspiciuni) că a fost încălcată confidenţialitatea cheii private, precum şi în cazul în care informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;
- să revoce certificatul cheii publice în cazul constatat de încălcare a confidenţialităţii cheii private sau de neconcordanţă realităţii a informaţiilor cuprinse în certificatul cheii publice;
- să primească cererile de certificare a cheilor publice de la persoanele fizice şi juridice în conformitate cu procedurile stabilite de prezentul Regulament;
- să verifice autenticitatea datelor stipulate în cererea de certificare a cheii publice pe baza documentelor ce confirmă aceste date, să asigure conformitatea informaţiilor cuprinse în certificatul cheii publice cu informaţiile prezentate de către persoanele fizice şi juridice;
- să asigure corespunderea informațiilor din certificatul cheii publice cu informaţiile prezentate de către titularul certificatului cheii publice;

- să asigure unicitatea informaţiei de înregistrare a titularilor în Registrul certificatelor cheilor publice;
- să nu divulge informaţiile confidenţiale şi alte informaţii protejate de lege;
- să verifice unicitatea cheilor publice certificate;
- să asigure unicitatea numerelor de înregistrare ale certificatelor cheilor publice eliberate;
- să creeze certificatul cheii publice al persoanelor fizice şi juridice, conform cerinţelor stabilite de organul competent şi de prezentul Regulament;
- să introducă certificatul cheii publice în Registrul certificatelor cheilor publice nu mai tîrziu de data şi ora la care începe termenul de valabilitate a certificatului;
- să elibereze certificatele cheilor publice titularilor în conformitate cu procedurile stabilite de prezentul Regulament;să suspende şi să restabilească, să revoce certificatele cheii publice ale titularilor certificatelor cheii publice în cazurile şi în conformitate cu procedurile stabilite de prezentul Regulament;
- să înscrie datele privind certificatul cheii publice revocat în lista certificatelor revocate în termen de 3 (trei) ore de lucru, precizînd data, ora şi cauza revocării certificatului;
- să excludă din lista certificatelor revocate datele privind certificatul cheii publice suspendat în termen de 3 (trei) ore de lucru din momentul restabilirii valabilității acestuia;
- să înştiinţeze din timp titularii certificatelor cheilor publice despre suspendarea valabilităţii sau revocarea certificatului cheii publice, în cazurile şi în conformitate cu procedurile stabilite de prezentul Regulament;
- să înştiinţeze titularii certificatelor cheilor publice despre restabilirea valabilităţii certificatelor cheilor publice în conformitate cu procedurile stabilite de prezentul Regulament;
- să înştiinţeze titularii certificatelor cheilor publice despre faptele de care a luat cunoştinţă CC şi care pot influenţa esenţial posibilitatea utilizării ulterioare a certificatului cheii publice;
- să înştiinţeze titularul certificatului cheii publice despre faptele de care a luat cunoştinţă CC, ce indică asupra imposibilităţii utilizării ulterioare a cheii private aparţinînd acestui titular;
- să păstreze toată informaţia cu privire la certificatul cheii publice al titularului, precum şi alte informaţii despre acest certificat nu mai puţin de 15 ani din momentul revocării sau expirării termenului de valabilitate a certificatului;
- să asigure actualizarea Registrului certificatelor cheilor publice generate şi revocate şi posibilitatea accesului liber la acesta în vederea verificării autenticităţii semnăturii electronice şi să întreprindă măsurile necesare pentru asigurarea securităţii datelor cu caracter personal conform legislaţiei în domeniul protecţiei datelor cu caracter personal;
- să creeze şi să păstreze copia de rezervă a Registrului certificatelor cheilor publice în conformitate cu cerinţele stabilite de organul competent;
- să asigure posibilitatea de a se determina ora şi data eliberării, suspendării valabilităţii şi revocării certificatului cheii publice;
- la cererea titularului semnăturii electronice, să confirme autenticitatea şi valabilitatea certificatelor cheilor publice;
- la cererea instanţei de judecată, a altor persoane şi organe ce dispun de acest drept în temeiul legii sau în alte cazuri prevăzute de legislaţia în domeniul aplicării semnăturii electronice, să confirme autenticitatea şi valabilitatea certificatelor cheilor publice eliberate de CC şi să prezinte, pe suport de hîrtie, copiile actelor în baza cărora a fost eliberată semnătura electronică;

- să sincronizeze activitatea serviciilor CC, inclusiv a mijloacelor tehnice şi de program conform destinaţiei, cu Timpul Mondial Coordonat (UTC). Se permită sincronizarea serviciilor conform Timpului Greenwich (Greenwich Mean Team, GMT), fără trecerea la ora de vară;
- să amplaseze mijloacele tehnice de program, destinate pentru certificarea cheilor publice, în încăperi speciale şi să asigure securitatea acestora;
- să dispună de personal auxiliar care posedă calificarea necesară.

Centrul de certificare a cheilor publice are dreptul:

- să creeze certificatul cheii publice al persoanei împuternicite a CC şi să îndeplinească procedura de eliberare către sine a certificatului cheii publice;
- să numească mai multe persoane împuternicite cu drepturi egale pentru semnarea certificatelor cheilor publice ale titularilor;
- să refuze eliberarea certificatului cheii publice solicitantului, precizînd motivele refuzului, în cazurile:
  - prezentării în cererea de certificare a cheilor publice a unor informaţii ce nu corespund realităţii;
  - încălcării prevederilor legislaţiei în domeniul aplicării semnăturii electronice;
  - încălcării drepturilor persoanelor terţe în procesul întocmirii sau depunerii cererii.
- să confirme autenticitatea şi valabilitatea certificatelor cheilor publice ale utilizatorilor semnăturii electronice;
- să suspende certificatul cheii publice al titularului în cazurile şi în modul prevăzute de legislaţie şi de prezentul Regulament;
- să revoce certificatul cheii publice al titularului în cazurile şi în modul prevăzute de legislaţie şi de prezentul Regulament.

5.2.2 Drepturile și obligațiile titularilor certificatelor cheilor publice

Titularul certificatului cheii publice este obligat:

- să prezinte referitor la sine informaţia necesară, prevăzută de procedura de identificare şi să prezinte CC documentele confirmative relevante;
- să prezinte informaţiile în volumul determinat de prezentul Regulament;
- să comunice referitor la orice modificări, ce ţin de informaţia personală, înregistrată în procesul de identificare;
- să respecte cerinţele legislaţiei în domeniul aplicării semnăturii electronice;
- să aplice cheia sa privată în conformitate cu domeniile de aplicare a semnăturii electronice şi alte restricţii indicate în certificatul cheii publice;
- să asigure păstrarea cheii private în conformitate cu cerinţele de securitate, stabilite de către organul împuternicit;
- să asigure condițiile necesare pentru a exclude accesul unei alte persoane la certificatul cheii private ce îl deține;
- în mod prompt să comunice CC despre situaţiile de compromitere a informaţiei sau suspiciuni cu privire la o asemenea compromitere;
- să nu utilizeze cheile, care au fost compromise sau cheile, termenul de validitate al cărora a expirat;
- să solicite imediat CC suspendarea valabilității certificatului cheii publice sau revocarea acestuia în cazul în care:
  - a pierdut cheia privată;
  - are motive să presupună că a fost încălcată confidențialitatea cheii private;

- informațiile cuprinse în certificatul cheii publice nu corespund realității.

- să îndeplinească alte obligațiuni stabilite de legislația în vigoare.

Titularul certificatului cheii publice are dreptul:

- să primească întregul spectru de servicii, prevăzute de Regulamentul CC;
- să depună cererea de certificare a cheii publice;
- să aplice în mod repetat cererea pentru certificare cu condiţia că toate observaţiile prezentate cu referire la prima cerere au fost înlăturate;
- să depună cererile de suspendare valabilităţii certificatului cheii publice în perioada de valabilitate a cheii private corespunzătoare;
- să depună cererea de restabilire a valabilităţii certificatului cheii publice;
- să depună cererea pentru confirmarea autenticităţii şi valabilităţii certificatului cheii publice;
- să depună cererile de revocare a certificatului cheii publice în perioada de valabilitate a cheii private corespunzătoare;
- să obţină accesul la Registrul certificatelor cheilor publice şi a Listei certificatelor revocate;
- să utilizeze certificatul cheii publice al persoanei împuternicite a CC pentru verificarea autenticităţii semnăturii electronice în certificatele cheilor publice eliberate de către CC;
- să utilizeze resursele informaţionale puse la dispoziţie de către CC pentru confirmarea verificarea autenticităţii şi valabilităţii certificatului cheii publice;
- să semneze şi să verifice semnătura electronică aplicată pe documentele electronice;
- să nu primească spre executare documentele electronice semnate cu semnătură electronică dacă:
  - certificatul cheii publice al persoanei care a semnat documentul electronic se află în lista certificatelor cheilor publice revocate sau nu era valabil la momentul semnării documentului electronic;
  - nu este confirmată autenticitatea semnăturii electronice în documentul electronic;
  - semnătura electronică se utilizează cu încălcarea sferei de aplicare sau cu depăşirea limitelor valorice pentru care este valabilă în documentele electronice de plată sau de încheiere a tranzacţiilor;
- în cazul apariţiei situaţiei litigioase ce ţine de stabilirea autenticităţii şi/sau a autorului documentului contestabil, să solicite soluţionarea ei în modul stabilit de legislaţie;
- să primească consultaţii cu privire la aplicarea semnăturii electronice şi verificarea autenticităţii documentului electronic de la personalul subdiviziunii responsabile şi al prestatorului de servicii de certificare.

5.3 Crearea şi administrarea certificatului cheii publice a Centrului de certificare a cheilor publice

5.3.1 Certificarea cheii publice a Centrului de certificare a cheilor publice

CC creează cheia sa privată şi cea publică în conformitate cu cerinţele stabilite de organul competent.

Crearea certificatului cheii publice a CC se realizează de CC de nivel superior conform cerinţelor stabilite de legislaţia în domeniul aplicării semnăturii electronice.

5.3.2 Suspendarea valabilităţii certificatului cheii publice a Centrului de certificare a cheilor publice

Suspendarea valabilităţii certificatului cheii publice a CC se realizează de CC de nivel superior conform cerinţelor stabilite de legislaţia în domeniul aplicării semnăturii electronice.

5.3.3 Revocarea certificatului cheii publice a Centrului de certificare a cheilor publice

Certificatul cheii publice a CC se revocă pe baza deciziei CC de nivel superior conform cerinţelor stabilite de legislaţia în domeniul aplicării semnăturii electronice.

5.3.4 Administrarea cheii private şi cheii publice a Centrului de certificare a cheilor publice

Termenul de valabilitate a certificatului cheii publice, al prestatorului de servicii de certificare este de 10 (zece) ani.

La expirarea termenului de valabilitate a cheii private a CC, cheia privată se distruge, se creează din nou cheia privată şi cea publică, precum şi certificatul cheii publice.

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

Cheia privată a CC se utilizează exclusiv pentru semnarea cu semnătura electronică a certificatului cheii publice al titularului.

Cheia privată a CC se păstrează şi se utilizează în condiţii ce exclud încălcarea confidenţialităţii acestuia.

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

CC utilizează cheia sa privată în prezenţa administratorului securitate, evitînd încălcarea confidenţialităţii cheii private.

Conducătorul CC poartă răspundere pentru organizarea accesului sigur la suportul material al cheii private şi utilizării autorizate a cheii.

Conducătorul CC, administratorul certificare şi administratorul securitate poartă răspundere personală pentru utilizarea sigură a cheii private a CC.

5.4 Serviciile prestate de către Centrul de Certificare a cheilor publice și modalitatea de prestare ale acestora

CC prestează servicii de certificare a cheilor publice atît persoanelor fizice, cît şi persoanelor juridice, reglînd aceste corelaţii prin prezentul Regulament.

CC a cheilor publice prestează servicii de certificare în cadrul infrastructurii cheilor publice (PKI), și anume:

a) înregistrarea și autentificarea identității persoanelor fizice și juridice;
b) crearea și eliberarea certificatului cheii publice a persoanelor fizice și juridice;
c) suspendarea valabilităţii certificatului cheii publice al persoanelor fizice și juridice;
d) restabilirea valabilității certificatului cheii publice a persoanelor fizice și juridice;
e) revocarea certificatului cheii publice al persoanelor fizice și juridice;
f) publicarea și actualizează registrul certificatelor cheilor publice;
g) confirmarea autenticităţii și valabilităţii certificatului cheii publice.

5.4.1 Înregistrarea şi autentificarea identităţii

Înregistrarea constă din proceduri ce permit CC primirea şi verificarea veridicităţii datelor prezentate şi presupune un şir de proceduri pentru colectarea datelor veridice necesare la identificarea solicitantului de certificat al cheii publice. Verificarea identităţii unui utilizator este făcută în mod obligatoriu în etapa de înregistrare a datelor.

Fiecare solicitant pentru certificarea cheii publice este supus procedurii de înregistrare o singură dată. După verificarea datelor prezentate pentru certificare, acesta este inclus în lista abonaţilor CC. Depunerea pachetului de documente pentru certificarea cheii publice este anticipată de consultarea şi executarea paşilor expuşi în instrucţiunea de pe site-ul CC http://pki.fsi.md.

Autentificarea identităţii asigură că datele din cererea creată corespund entităţii respective. Procedura de identificare constă în:

- verificarea documentelor furnizate de către solicitant;
- verificarea exactităţii datelor indicate de către solicitant în cererea de certificare a cheii publice cu cele din documentele furnizate;
- verificarea informaţiilor din cerere folosind alte surse informaţionale;
- verificarea adresei de e-mail etc;

5.4.2 Certificarea cheii publice a persoanei fizice

Pentru certificarea cheii publice a persoanei fizice, aceasta prezintă CC următoarele documente şi informaţii:

a) cererea de certificare a cheii publice pe suport de hîrtie, semnată cu semnătură olografă, conform reglementărilor interne şi formularelor plasate pe www.pki.fsi.md (Anexa nr. 4);

b) copia buletinului de identitate, însoţită de original;

5.4.3 Certificarea cheii publice a persoanei juridice

Pentru certificarea cheii publice a persoanei juridice, aceasta prezintă CC următoarele documente şi informaţii:

a) copia buletinului de identitate al persoanei responsabile a persoanei juridice (conducător şi contabil-şef sau altă persoană împuternicită în modul stabilit), însoţită de original;

b) copia procurii autentificate notarial privind împuternicirea persoanei cu dreptul exclusiv de a ridica, transmite semnătura electronică şi/sau de a semna documentele din numele persoanei juridice (însoţită de original);

c) cererea de certificare a cheii publice pe suport de hîrtie de la persoana responsabilă a persoanei juridice se semnează cu semnătură olografă conform reglementărilor interne şi formularelor plasate pe www.pki.fsi.md *(Anexa nr. 5)*.

Cererea de certificare a cheii publice a titularului sub formă de document electronic trebuie să corespundă standardului IETF RFC 5967 The application/pkcs10 Media Type sau IETF RFC 4211 Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF).AÎ al CC identifică solicitantul certificatului cheii publice pe baza documentelor prezentate şi efectuează controlul prealabil.

La efectuarea controlului prealabil, AÎ trebuie să urmărească îndeplinirea următoarelor condiţii:

a) respectarea de către solicitant a prevederilor legislaţiei în vigoare în domeniul aplicării semnăturii electronice la întocmirea şi înaintarea cererii de certificare a cheii publice;
b) respectarea de către solicitant a drepturilor persoanelor terţe la întocmirea şi înaintarea cererii de certificare a cheii publice;

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

În cazul îndeplinirii de către solicitant a tuturor condiţiilor prevăzute la punctul 5.4.3 al prezentului Regulament, AÎ al CC înregistrează solicitantul. În caz contrar, AÎ al CC refuză înregistrarea solicitantului şi restituie solicitantului documentele prezentate.

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

În cazul înregistrării solicitantului, AÎ al CC transmite AC următoarele documente:

a) cererea de certificare a cheii publice sub formă de document pe suport de hîrtie, înregistrată şi autentificată cu semnătura ologrfă a AÎ;

b) pachetul de documente necesar eliberării certificatului cheii publice;

AC ia decizia despre certificarea cheii publice a solicitantului în termen de cel mult 3 (trei) zile lucrătoare din data înregistrării cererii.

În cazul depistării unor încălcări ale legislaţiei în domeniul aplicării semnăturii electronice, AC ia decizia privind refuzul certificării cheii publice, indicînd obligatoriu motivele refuzului.

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

În cazul deciziei de aprobare privind certificarea cheii publice, AC creează certificatul cheii publice al solicitantului.

Certificatul cheii publice al titularului, în calitate de persoană fizică, trebuie să conţină datele conform Anexei nr. 1, şi anume:

a) numărul de înregistrare al certificatului cheii publice;
c) numele şi prenumele titularului certificatului cheii publice;
d) numărul de identificare al persoanei fizice (IDNP);
g) cheia publică a persoanei – titular al certificatului cheii publice;
h) data şi ora la care începe şi încetează termenul de valabilitate a certificatului cheii publice;
i) datele despre algoritmul criptografic al semnăturii electronice şi alte date tehnologice stabilite de CC;
k) semnătura electronică a titularului;
l) alte date, în conformitate cu standardele tehnice şi cerinţele stabilite de organul competent.

Certificatul cheii publice al titularului, în calitate de persoană juridică, trebuie să conţină datele conform Anexei nr. 1, şi anume:

a) numărul de înregistrare al certificatului cheii publice;
b) datele de identificare ale persoanei juridice (IDNO);
c) numele şi prenumele titularului certificatului cheii publice;
d) numărul de identificare al persoanei fizice (IDNP);
e) denumirea persoanei juridice şi funcţia deţinută de către persoana fizică în cadrul acesteia;
g) cheia publică a persoanei – titular al certificatului cheii publice;
h) data şi ora la care începe şi încetează termenul de valabilitate a certificatului cheii publice;
i) datele despre algoritmul criptografic al semnăturii electronice şi alte date tehnologice stabilite de CC;
k) semnătura electronică a titularului;

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

Certificatul cheii publice sub formă de document electronic trebuie să corespundă standardului ITU-T X.509, versiunea 3, standardului SM ISO CEI 9594-8:2014 Tehnologia informaţiei, Linii directoare: Structura certificatului cheii publice şi a atributului sau recomandării ETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profil, ETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profil şi IETF RFC 3739 Qualified Certificates ProfileTermenul de valabilitate a certificatului cheii publice este de 1 (un) an.

AÎ al CC informează titularul despre crearea certificatului cheii publice şi o eliberează acestuia.

Certificatul cheii publice al titularului se păstrează în Registrul certificatelor cheilor publice sub formă de document electronic.

5.4.4 Suspendarea valabilităţii certificatului cheii publice al titularului

Suspendarea valabilităţii certificatului cheii publice al titularului se efectuează:

a) la cererea titularului certificatului cheii publice;
b) pe baza deciziei organului competent;
c) pe baza deciziei CC;
d) în baza hotărîrii/deciziei instanţei de judecată definitive.

Titularul poate cere suspendarea valabilităţii certificatului cheii publice ce-i aparţine dacă are motive să presupună că a fost încălcată confidenţialitatea cheii private, precum şi în cazul în care informaţiile cuprinse în certificatul cheii publice nu corespund realităţii.

Cererea de suspendare a valabilităţii certificatului cheii publice al titularului (conform reglementărilor interne şi formularelor plasate pe www.pki.fsi.md) poate fi prezentată sub formă de document pe suport de hîrtie la CC sau CÎ personal de către titular, sub formă de document pe suport de hîrtie care urmează să fie semnat olograf în cadrul CC sau CÎ de către titular şi/sau conducătorului entităţii (în cazul persoanelor juridice), precum şi generată direct în cadrul CC sau CÎ la prezentarea titularului şi/sau conducătorului entităţii (în cazul persoanelor juridice).

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

Cererea de suspendare a valabilităţii certificatului cheii publice va fi completată şi prezentată conform Anexei nr. 6 al prezentului Regulament.

Cererea de suspendare a valabilităţii certificatului cheii publice în formă verbală se transmite de către titular prin mijloacele legăturii telefonice.

AÎ efectuează autentificarea titularului care solicită suspendarea valabilităţii certificatului cheii publice ce-i aparţine. Autentificarea se realizează conform:

a) datelor din buletinul de identitate al solicitantului;
b) certificatului cheii publice, prin confirmarea autenticităţii cererii de suspendare a valabilităţii certificatului cheii publice sub formă de document electronic;
c) frazei-cheie sau cuvîntului-cheie pentru autentificarea la distanţă, comunicată la telefon de către titular.

AC ia decizia privind suspendarea valabilităţii certificatului în termen de 3 (trei) ore de lucru din momentul primirii cererii de suspendare a valabilităţii certificatului cheii publice.

CC comunică titularului despre decizia privind suspendarea valabilităţii certificatului cheii publice sau despre refuzul de suspendare, indicînd motivele refuzului, în termen de 3 (trei) zile lucrătoare.

Ora suspendării valabilităţii certificatului cheii publice a titularului se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în cîmpul This Update).

Dacă CC are motive să presupună că a fost încălcată confidenţialitatea cheii private a titularului sau informaţiile cuprinse în certificatul cheii publice nu corespund realităţii, CC este în drept să ia unilateral decizia privind suspendarea valabilităţii certificatului cheii publice corespunzător.

În cazul suspendării valabilităţii certificatului cheii publice al titularului pe baza deciziei organului competent sau a CC, CC informează imediat, prin mijloacele legăturii telefonice, titularul despre suspendarea valabilităţii certificatului cheii publice comunicînd ulterior în scris, prin e-mail, asupra acestei decizii, în termen de 5 (cinci) zile lucrătoare.

Valabilitatea certificatului cheii publice al titularului se suspendă pentru o perioadă de pînă la 30 de zile calendaristice.

Certificatul cheii publice al titularului a cărui valabilitate a fost suspendată, în termen de 3 (trei) ore de lucru, va fi înscris în lista certificatelor revocate.

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

Restabilirea valabilităţii certificatului cheii publice al titularului se efectuează:

a) la cererea titularului certificatului cheii publice;
b) pe baza deciziei organului competent;
c) pe baza deciziei CC.
d) Cererea de restabilire a valabilităţii certificatului cheii publice al titularului (conform reglementărilor interne şi formularelor plasate pe www.pki.fsi.md) reprezintă un document pe suport de hîrtie semnat cu semnătura olografă a titularului.

Cererea de restabilire a valabilităţii certificatului cheii publice al titularului se depune la CC sau CÎ personal de către titular, nu mai tîrziu de 5 (cinci) zile lucrătoare pînă la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice.

Cererea de restabilire a valabilităţii certificatului cheii publice va fi completată şi prezentată conform Anexei nr. 6 al prezentului Regulament.

CC ia decizia de restabilire a valabilităţii certificatului, în termen de 3 (trei) zile lucrătoare din data primirii cererii de restabilire a valabilităţii certificatului cheii publice.

CC comunică titularului despre decizia privind restabilirea sau privind refuzul de restabilire a valabilităţii certificatului cheii publice, indicînd motivele refuzului, în termen de 3 (trei) zile lucrătoare.

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

În cazul în care valabilitatea certificatului cheii publice al titularului a fost suspendată pe baza deciziei CC, CC este în drept să ia unilateral decizia privind restabilirea valabilităţii certificatului cheii publice corespunzător.

În cazul restabilirii valabilităţii certificatului cheii publice al titularului pe baza deciziei organului competent sau a CC, CC informează titularul despre restabilirea valabilităţii certificatului, în termen de 3 (trei) zile lucrătoare.

Certificatul cheii publice al titularului a cărui valabilitate a fost restabilită, în termen de 3 (trei) ore de lucru, va fi radiat din lista certificatelor revocate.

Ora restabilirii valabilităţii certificatului cheii publice al titularului se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în cîmpul This Update).

5.4.5 Revocarea certificatului cheii publice al titularului

Certificatul cheii publice se revocă în următoarele cazuri:

a) la cererea titularului certificatului cheii publice;
b) în baza deciziei organului competent (organului de drept, instanţei de judecată, etc.);
c) în cazul faptului constatat de compromitere a cheii private;
d) la depistarea unor informaţii neconforme realităţii în cererea de certificare a cheii publice sau în certificatul cheii publice;
e) la introducerea unor modificări în certificatul cheii publice;
f) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice, dacă nu a fost adoptată decizia de restabilire a valabilităţii acestuia;
g) la expirarea termenului de valabilitate a certificatului cheii publice.

Titularul certificatului cheii publice poate cere revocarea certificatului cheii publice ce-i aparţine în cazul faptelor constatate de încălcare a confidenţialităţii cheii sale private sau în cazul în care informaţiile cuprinse în certificat nu corespund realităţii, precum şi în alte cazuri prevăzute de Regulamentul CC.

Cererea de revocare a certificatului cheii publice al titularului (conform reglementărilor interne și formularelor plasate pe www.pki.fsi.md) reprezintă un document pe suport de hîrtie semnat cu semnătură olografă, conform Anexei nr. 5 al prezentului regulament

Cererea de revocare a certificatului cheii publice poate fi prezentată sub formă de document pe suport de hîrtie la CC sau CÎ personal de către titular, sub formă de document electronic care urmează să fie semnat olograf în cadrul CC sau CÎ de către titular şi/sau conducătorului entităţii (în cazul persoanelor juridice), precum şi generată direct în cadrul CC sau CÎ la prezentarea titularului şi/sau conducătorului entităţii (în cazul persoanelor juridice).

Cererea de revocare a certificatului cheii publice va fi completată și prezentată conform Anexei nr. 6 al prezentului Regulament.

CC ia decizia privind revocarea certificatului, în termen de 3 (trei) zile lucrătoare din momentul primirii cererii de revocare a certificatului cheii publice.

CC comunică titularului despre decizia de revocare a certificatului cheii publice sau despre refuzul revocării certificatului, indicînd motivele refuzului, în termen de 3 (trei) zile lucrătoare.

CC este în drept să ia unilateral decizia privind revocarea certificatului cheii private:

a) în cazul faptului constatat de compromitere a cheii private;
b) la depistarea unor informaţii neconforme realităţii în cererea de certificare a cheii publice sau în certificatul cheii publice;
c) la introducerea unor modificări în certificatul cheii publice;
d) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice, dacă nu a fost adoptată decizia de restabilire a valabilităţii acestuia;
e) la expirarea termenului de valabilitate a certificatului cheii publice.

Certificatul cheii publice revocat al titularului, în termen de 3 (trei) ore de lucru se înscrie în lista certificatelor revocate, iar CC emite lista actualizată a certificatelor revocate.

Ora revocării certificatului cheii publice al titularului se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în cîmpul This Update).

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

5.4.6 Confirmarea autenticităţii şi valabilităţii certificatului cheii publice

CC confirmă autenticitatea şi valabilitatea certificatelor cheilor publice:

a) la solicitarea titularului certificatului cheii publice;
b) la cererea instanţei de judecată, a altor persoane şi organe care au acest drept în temeiul legii sau în alte cazuri prevăzute de legislaţia în domeniul aplicării semnăturii electronice.

CC asigură titularilor semnăturii electronice, precum şi terţilor, posibilitatea de a stabili de sine stătător autenticitatea şi valabilitatea certificatului cheii publice al titularului prin:

a) acordarea accesului la Registrul certificatelor cheilor publice şi Listei certificatelor revocate în baza numărului de serie a certificatului cheii publice;
b) oferirea serviciului online de verificare a certificatului cheii publice în baza numărului de serie a acestuia.

Cererea titularului semnăturii electronice de confirmare a autenticităţii şi valabilităţii certificatului cheii publice reprezintă un document pe suport de hîrtie semnat cu semnătura olografă a solicitantului.

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

CC transmite solicitantului, în termen de 3 (trei) zile lucrătoare, un proces-verbal privind rezultatele verificării autenticităţii şi valabilităţii certificatului cheii publice, care va conţine:

a) timpul şi locul verificării;
b) cauza verificării;
c) datele despre angajatul CC care a efectuat verificarea (numele, prenumele, funcţia);
d) conţinutul şi rezultatele verificării;
e) evaluarea rezultatelor verificării şi concluziile corespunzătoare;
f) alte date stabilite de CC.

CC poate refuza solicitantului să verifice autenticitatea şi valabilitatea certificatului cheii publice al titularului, dacă nu au fost respectate cerinţele Prezentului Regulament.

5.4.7 Resursele informaţionale ale Centrului de certificare a cheilor publice

Resursa informaţională de bază a CC este Registrul certificatelor cheilor publice.

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

a) certificatele cheilor publice ale persoanelor împuternicite ale CC;
b) cererile de certificare a cheilor publice ale solicitanţilor;
c) certificatele cheilor publice ale titularilor;
d) cererile de revocare a certificatelor cheilor publice ale titularilor;
e) listele certificatelor revocate.

În arhiva CC se păstrează următoarele resurse informaţionale:

a) registrul certificatelor cheilor publice;
b) registrele de audit al complexului tehnic de program al CC;
c) documentele de serviciu ale CC, conform criteriilor stabilite de conducătorul Centrului.

Termenul de păstrare a documentelor de arhivă ale CC este de 15 (cincisprezece) ani.

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

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

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

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

Accesul utilizatorilor semnăturii electronice la versiunea electronică a Registrului certificatelor cheilor publice (lista certificatelor) se efectuează prin intermediul resursei informaţionale electronice oficiale a CC pe adresa: www.pki.fsi.md.

CC publică pe paginile resursei informaţionale electronice www.pki.fsi.md pune la dispoziţie utilizatorilor Lista certificatelor revocate.

5.4.8 Mijloacele de asigurare a activităţii Centrului de certificare a cheilor publice

CC creează şi exploatează complexul tehnic de program care include următoarele componente:

a) serviciul certificare;
b) serviciul înregistrare;
c) serviciul registru;
d) serviciul control etalonat al semnăturii electronice.

Serviciul certificare reprezintă componentul tehnologic de bază al complexului tehnic de program al CC care asigură:

a) generarea cheilor;
b) Crearea certificatului cheii publice al utilizatorului sub formă de document electronic;
c) crearea listei certificatelor revocate.

Responsabilitatea pentru exploatarea serviciului certificare o poartă AC şi administratorul sistem.

Serviciul înregistrare reprezintă componentul tehnologic al complexului tehnic de program al CC care asigură înregistrarea utilizatorilor.

Responsabilitatea pentru exploatarea serviciului înregistrare o poartă AÎ.

Serviciul registru reprezintă componentul tehnologic al complexului tehnic de program al CC care asigură:

a) păstrarea certificatelor cheilor publice ale persoanelor împuternicite ale CC;
b) păstrarea certificatelor cheilor publice ale titularilor;
c) păstrarea cererilor de certificare a cheilor publice;
d) păstrarea informaţiei de înregistrare a titularilor certificatelor cheilor publice;
e) publicarea şi difuzarea listelor certificatelor revocate;
f) accesul la certificatele cheilor publice valabile şi la listele certificatelor revocate;
g) păstrarea altor informaţii ce ţin de activitatea CC.

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

Mijloacele tehnice de asigurare a funcţionării complexului tehnic de program al CC includ:

a) echipamentul de server;
b) echipamentul de comunicaţii electronice;
c) locurile de muncă computerizate ale administratorilor CC;
d) dispozitivele de imprimare pe suport de hîrtie;
e) alte echipamente auxiliare.

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

În componenţa complexului tehnic de program al CC funcţionează mijloacele de protecţie criptografică a informaţiei, inclusiv:

a) dispozitive securizate;

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

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

Complexul tehnic de program trebuie să corespundă cerinţelor stabilite de organul competent şi actele normative în domeniu.

5.5 Repozitoriul şi publicarea

5.5.1 Publicarea informaţiei despre certificatele cheilor publice

Repozitoriul CC este o interfaţă publică ce conţine următoarea informaţie:

- versiunile actuale şi anterioare ale prezentului Regulamentul şi ale Politicilor de certificare;
- contracte-tip şi anexe, ce urmează a fi semnate cu titularii certificatelor cheilor publice;
- formulare de cereri-tip de creare, de suspendare şi reînnoire a valabilităţii, de revocare a certificatului cheii publice;
- lista centrelor de înregistrare împuternicite;
- lista certificatelor cheilor publice ale titularilor;
- lista certificatelor revocate (CRL);
- altă informaţie ce se modifică în timp real.

Cu conţinutul Repozitoriului a se lua cunoştinţă pe http://pki.fsi.md.

5.5.2 Cauzele şi frecvenţa de publicare

Informaţia, publicată în Repozitoriul C, se actualizează în următorul mod:

- Politicile de certificare şi Regulamentul Centrului de certificare a cheilor publice - la introducerea modificărilor în caz de depistare a erorilor, modificare a standardelor corespunzătoare sau la propunerile titularilor;
- contractele-tip şi anexele - după introducerea modificărilor;
- formulare de cereri-tip - după introducerea modificărilor;
- certificatele abonaţilor - după eliberarea noului certificat titularului;
- lista certificatelor revocate (CRL) – cel puţin o dată în zi şi la fiecare revocare, suspendare sau restabilire a valabilităţii certificatului cheii publice;
- informaţie suplimentară – la fiecare completare.

5.5.3 Controlul accesului la Repozitoriu

Informaţia, publicată în Repozitoriul CC, este informaţie publică. Întreprinderea a implementat măsuri de securitate fizică şi logică pentru a preveni adăugarea, ştergerea sau schimbarea informaţiei publicate în Repozitoriul CC.

5.6 Interacţiunea titularilor certificatelor cheilor publice cu Centrul de certificare a cheilor publice

5.6.1 Modul de interacţiune a titularilor certificatelor cheilor publice cu Centrul de certificare a cheilor publice

Interacţiunea titularilor certificatelor cheilor publice cu CC se efectuează în conformitate cu procedurile stabilite de prezentul Regulament şi cu cerinţele în domeniul semnăturii electronice.

CC asigură accesul titularilor certificatelor cheilor publice la Registrul certificatelor cheilor publice şi Listei certificatelor revocate în conformitate cu prezentul Regulament.

În vederea interacţiunii, persoana împuternicită a CC prezintă titularilor datele ei de contact (numărul de telefon, fax, adresa poştală, adresa poştei electronice).

În cazul revocării certificatului cheii publice a persoanei împuternicite a CC, se revocă concomitent şi certificatele titularilor.

Titularii certificatelor cheilor publice folosesc certificatul cheii publice al persoanei împuternicite a CC în procesul verificării autenticităţii semnăturii electronice în documentul electronic.

În procesul interacţiunii titularilor semnăturii electronice cu CC pot apărea situaţii litigioase. Sunt supuse soluţionării în conformitate cu prezentul Regulament situaţiile litigioase care apar în legătură cu:

a) contestarea integrităţii documentului electronic;
b) contestarea identificării persoanei care a semnat documentul electronic;
c) contestarea împuternicirilor persoanei care a semnat documentul electronic;
d) contestarea valabilităţii şi autenticităţii certificatului cheii publice a CC şi utilizatorului semnăturii electronice;
e) contestarea sferei de aplicare a semnăturii electronice şi a altor restricţii indicate în certificatele cheilor publice, emise de CC;
f) neîncrederea în dispozitivele securizate, utilizate de către CC, şi utilizatorul semnăturii electronice;
g) neîncrederea în CC;
h) contestarea împuternicirilor CC;
i) alte situaţii litigioase în legătură cu aplicarea semnăturii electronice.

Situaţiile litigioase, în dependenţă de natura şi complexitatea lor, se soluţionează în regim de lucru şi/sau de către Comisia de soluţionare a situaţiilor litigioase în domeniul aplicării semnăturii electronice (*în continuare – Comisia*).

Partea (CC sau titularul) care depistează împrejurări ce indică prezenţa unei situaţii litigioase, are obligaţia să înştiinţeze imediat cealaltă parte despre aceasta, în termen de cel mult o zi lucrătoare. Ulterior, părţile implicate în litigiu au obligaţia să verifice prezenţa acestor împrejurări şi să întreprindă măsuri pentru soluţionarea situaţiei litigioase, înştiinţîndu-se reciproc despre rezultatele verificării şi acţiunile întreprinse.

În cazul în care situaţia litigioasă nu a fost soluţionată în regim de lucru, partea-iniţiator are dreptul, în termen de cel mult 3 (trei) zile lucrătoare după apariţia situaţiei litigioase, de a înainta un aviz despre situaţia litigioasă cu propunere de a forma Comisia. În componenţa Comisiei se include conducătorul CC şi membrii CC, precum şi titularul certificatului cheii publice, în caz de necesitate.

CC va întruni Comisia în termen de 5 (cinci) zile lucrătoare din data parvenirii avizului despre situaţia litigioasă din partea titularului certificatului cheii publice. Persoanele care se includ în componenţa Comisiei trebuie să posede cunoştinţele necesare şi experienţă de lucru în domeniul aplicării semnăturii electronice şi întocmirii de documente electronice, să dispună de dreptul de acces la materialele documentare şi la mijloacele tehnice şi de program necesare pentru desfăşurarea activităţii Comisiei.

În sarcinile Comisiei intră examinarea, la nivel legal şi tehnico-organizaţional, a circumstanţelor situaţiei litigioase, stabilirea cauzelor şi urmărilor acestei situaţii, determinarea măsurilor necesare pentru soluţionarea ei şi prezentarea conducerii Î.S. „Fiscservinform” a propunerilor şi proiectului deciziei pe marginea situaţiei litigioase.

În cazul în care situaţia litigioasă este considerată de către părţi ca fiind soluţionată, în termen de cel mult 5 (cinci) zile lucrătoare după încheierea lucrărilor Comisiei, se întocmeşte un act privind soluţionarea situaţiei litigioase, care este semnat de membrii Comisiei şi aprobat de către administratorul Î.S. „Fiscservinform”.

În cazul imposibilităţii de a soluţiona situaţia litigioasă pe cale amiabilă, părţile se pot adresa în instanţa de judecată.

5.6.2 Responsabilitatea financiară

În scopul garantării reparării prejudiciilor, care ar putea fi cauzate titularilor certificatelor cheilor publice, utilizatorilor sau terţelor persoane în urma neîndeplinirii sau îndeplinirii neconforme de către CC a obligaţiunilor sale, acesta este obligat de a obţine o garanţie bancară sau o poliţă de asigurare, egală cu suma de 300 000 lei.

5.7 Asigurarea securităţii şi protecţia informaţiilor confidenţiale

5.7.1 Confidenţialitatea informaţiei

Informaţiile care se prelucrează şi se păstrează în CC sunt protejate prin lege.

Informaţiile care se păstrează în registrele de audit ale CC sunt confidenţiale.

Nu sunt confidenţiale informaţiile ce se conţin în registrul certificatelor cheilor publice şi în listele certificatelor revocate.

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

Activităţile de prelucrare a datelor cu caracter personal în cadrul CC sunt notificate în condiţiile legii şi sunt reglementate prin Politica de securitate a datelor cu caracter personal.

5.7.2 Măsurile tehnico-inginereşti de protecţie a informaţiei

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

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

Încăperile pentru servere ale CC se dotează cu sisteme de control al accesului.

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

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

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

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

Mijloacele tehnice ale CC trebuie sa fie conectate la reţeaua de alimentare cu electricitate garantată.

Modul de evidenţă, păstrare, comercializare, transmitere şi distrugere a mijloacelor tehnice speciale şi documentaţiei tehnice este reglementat în Instrucţiunea privind manipularea mijloacelor tehnice speciale.

5.7.3 Măsurile de protecţie a informaţiei cu mijloacele de program şi de aparataj

Complexul tehnic de program al CC trebuie să asigure controlul integrităţii mijloacelor tehnice şi de program.

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

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

În cadrul accesului la procedurile CC se utilizează separarea funcţională a membrilor grupului de administratori care deservesc complexul tehnic de program al CC.

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

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

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

5.7.4 Măsurile organizatorice de protecţie a informaţiei

Măsurile organizatorice, destinate prevenirii situaţiilor de compromitere a securităţii resurselor CC, sunt următoarele:

- evidenţa strictă a resurselor care necesită a fi protejate;
- prevenirea accesului, modificării şi/sau distrugerii neautorizate a datelor;
- prevenirea divulgării sau transmiterii nesancţionate a informaţiilor confidenţiale unor terţi;
- depistarea oportună a accesului nesancţionat la informaţiile confidenţiale;
- prevenirea influenţelor externe asupra mijloacelor tehnice de prelucrare a datelor;
- controlul nivelului de protecţie a datelor;
- managementul incidentelor de securitate;
- conştientizarea asigurării securităţii datelor prelucrate în cadrul CC.

Asigurarea măsurilor organizatorice de protecţie a informaţiei este pusă în sarcina administratorului securitate.

5.8 Arhivarea informaţiilor aferente Centrului de certificare a cheilor publice

5.8.1 Arhivarea informațiilor

Informația aferentă CC, actele juridice încheiate cu titularii cheilor publice, cererile titularilor, solicitările adresate de titulari, informaţiile despre titulari, certificatele cheilor publice publicate, listele certificatelor cheilor publice revocate, cheile folosite în CC, securitatea sistemelor, precum şi toată corespondenţa CC cu titularii, sunt supuse copierii de rezervă şi arhivării obligatorii.

Arhivarea informației se realizează în spaţii special amenajate care să asigure condiţiile specifice de păstrare, protecţia împotriva pierderii, dispariţiei, deteriorării sau nimicirii acestora (foc, condens, inundaţii, furturi, insecte şi rozătoare, acte de vandalism etc.). Durata de arhivare a informației şi documentelor, în format electronic şi pe hîrtie, retrase din uz (originalele) este minim 20 (douăzeci) de ani. Pentru a se exclude posibilitatea utilizării documentelor depăşite sau anulate, acestea vor fi periodic revizuite şi, în caz de necesitate – prompt retrase din uz.

Protecţia arhivelor CC are loc prin accesul la arhive doar a colaboratorilor autorizaţi. Datele arhivate electronic sunt protejate de vizualizarea nesancţionată, modificări sau ştergerea prin intermediul controlorilor de acces fizic şi logic.

Arhiva informației aferente CC se va cripta cu cheile gestionate și accesibile administratorului de securitate. Pentru verificarea integrităţii şi a posibilităţii de restabilire a datelor copiile de arhivă şi de rezervă sunt supuse verificării periodice şi comparării cu originalul (dacă este posibil). Acest tip de verificare este accesibil doar administratorului securitate.

5.8.2 Tipurile de informații supuse arhivării

CC gestionează două tipuri de arhive:

1) arhiva documentelor pe suport de hîrtie:
   - documente şi date folosite în procesul de identificare a identităţii;
   - cererile şi datele primite de la solicitant pe suport de hîrtie;
   - actele juridice încheiate şi semnate dintre CC şi titularii certificatelor cheilor publice;
   - corespondenţa internă şi externă dintre CC şi titulari etc.
2) arhiva electronică:
   - istoria cheilor titularilor din momentul generării lor şi pînă la nimicire;
   - istoria cheilor CC din momentul generării şi pînă la momentul nimicirii;
   - baza de date a titularilor certificatelor cheilor publice;
   - baza de date a certificatelor cheilor publice;
   - listele certificatelor revocate publicate;
   - cererile şi datele primite în format electronic de la solicitant;
   - informaţie despre efectuarea controalelor mijloacelor ce asigură securitatea (primită din rapoartele auditului) etc.

5.8.3 Copiile arhivei

Copiile de arhivă permit restabilirea completă (e.g., după căderea sistemului) a tuturor datelor necesare pentru funcţionarea corectă a CC. Metodele de creare a copiilor de rezervă trebuie să asigure posibilitatea de restabilire rapidă a datelor şi sistemelor în cazul pierderii sau deteriorării lor. În CC se aplică următoarele două metode:

- copierea de rezervă ce are loc zilnic şi poate fi utilizată în cazul restabilirii rapide a datelor pierdute;
- copierea de rezervă pentru asigurarea restabilirii rapide a configuraţiilor şi setărilor echipamentului şi mijloacelor de program.

Aceste copii permit protejarea şi restabilirea funcţionalităţii serverelor de bază şi se păstrează pe o perioadă de 30 de zile. Arhivarea de rezervă trebuie să cuprindă starea curentă a sistemelor şi să permită restabilirea completă a sistemului funcţionabil în decurs de 48 ore din momentul depistării deteriorării și vor fi păstrate în safeul CC.

5.9 Algoritmul de restabilire a sistemului în caz de compromitere și defecțiuni

5.9.1 Compromiterea Centrului de certificare a cheilor publice

În cazul în care cheile CC sunt compromise sau există o suspiciune de compromitere a acestora, se efectuează următorii paşi:

- CC generează o pereche nouă de chei şi obţine un nou certificat de cheie publică;
- titularii certificatelor cheilor publice sunt notificaţi imediat despre compromiterea cheilor prin intermediul mass-media şi al poştei electronice;
- certificatul cheii publice, corespunzător cheii compromise lichidate, se revocă şi se plasează în lista certificatelor revocate;

- toate certificatele din lanţul certificatelor în care se află certificatul compromis, se înregistrează în lista de certificate revocate cu indicarea motivului respective *(„CA compromise”)*;
- abonaţilor le sunt eliberate certificate noi de chei publice;
- se execută livrarea noilor certificate către abonaţi fără perceperea unei taxe suplimentare.

5.9.2 Caz de deteriorare a resurselor informaţionale

Normele de siguranţă care se aplică în cadrul CC stipulează diverse situaţii, la apariţia cărora trebuie să fie păstrată operaţionalitatea CC şi garantat nivelul prestării serviciilor:

- deteriorarea fizică a sistemelor informatice, inclusiv deteriorarea infrastructurii reţelei şi a cablurilor - ca urmare a unei situaţii de avarie;
- defecţiuni ale complexului de programe, incapacitatea de a accesa datele - ca rezultat al deteriorării spaţiului sistemelor de operare, aplicaţiilor utilizatorilor, sau al rulării altor programe, cum ar fi „viruşii”, „troienii”, „viermii”;
- pierdere (oprire, lipsă de acces) a serviciilor importante de reţea, oferite de către CC, în primul rând se referă la pierderea alimentării cu energie electrică sau deteriorarea conexiunilor de reţea;
- deteriorare a unei părţi a reţelei interne, utilizată de către CC pentru furnizarea serviciilor sale - poate conduce la indisponibilitatea deservirii titularilor.

5.9.3 Restabilirea securităţii după o situaţie de avarie

La finalul procedurilor de restabilire a sistemului după o situaţie de avarie, administratorii CC sunt obligaţi să:

- înlocuiască toate parolele utilizate anterior;
- elimine drepturile utilizate anterior de acces la sistem şi la resursele acestuia;
- înlocuiască toate codurile şi PIN-urile, asociate cu accesul fizic la componentele CC;
- în conformitate cu Politica de securitate si control al accesului în CC, toate componentele de reţea şi regulile accesului fizic trebuie să fie revizuite;
- informeze conducerii despre restabilirea funcţionării sistemului.

5.9.4 Continuitatea activităţii Centrului de certificare a cheilor publice în cazuri excepţionale

În cazul situaţiilor excepţionale, CC asigură continuitatea activităţii în conformitate cu „*Planul de recuperare al activităţii Centrului de certificare a cheilor publice”*.

5.10 Auditarea Centrului de certificare a cheilor publice

Activităţile desfăşurate în cadrul CC sunt supuse auditării, în conformitate cu reglementările interne ale Î.S. „Fiscservinform” sau de către instituţii independente competente (audit extern).

5.11 Reorganizarea şi lichidarea Centrului de certificare a cheilor publice

Reorganizarea şi lichidarea CC se efectuează în conformitate cu legislaţia.

La reorganizarea CC şi transmiterea funcţiilor lui la o altă unitate de drept, prin decizia comună a conducătorilor entităţilor interesate se creează o comisie de transmitere a CC.

În componenţa comisiei de transmitere a CC se includ:

a) reprezentanţii părţilor;
b) conducătorul CC sau persoana care îl înlocuieşte;

c) reprezentantul organului competent;
d) alte persoane desemnate de către părţi.

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

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

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

La lichidarea CC prin ordinul administratorului Î.S. „Fiscservinform” se creează comisia de lichidare, în sarcina căreia se pune realizarea procedurii de lichidare în conformitate cu legislaţia în vigoare şi cerinţele stabilite de organul competent.

În componenţa comisiei de lichidare se includ:
a) conducătorul CC sau persoana care îl înlocuieşte;
b) reprezentantul organului competent;
c) alte persoane indicate în ordin.

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

Registrul certificatelor cheilor publice al CC lichidat, sub formă de documente electronice, se transmite organului competent pe suporturi materiale, pe baza actului de primire-predare. Actul se semnează de către conducătorul CC, reprezentantul organului competent responsabil de păstrare şi se aprobă de către administratorul Î.S. „Fiscservinform”.

În cazul lichidării CC, cheile private ale CC se distrug, fără a se încălca confidenţialitatea cheilor, iar certificatele cheilor publice corespunzătoare se revocă.

Anexa nr. 1
la REG-08 Regulamentul Centrului
de certificare a cheilor publice

Structura certificatului cheii publice a Centrului de certificare a cheilor publice

Denumirea (în engleză)	Descrierea	Conţinutul	NOTĂ
Cîmpurile de bază			
Version	Versiunea	V3	
Serial Number	Numărul de înregistrare a certificatului	Numărul	
Issuer	Datele de identificare ale centrului de certificare, emitent al certificatului	CN = RootCASIS2 L = Chişinău S = Republica Moldova OU = Centrul de certificare de nivel superior O = Serviciul de Informaţie şi Securitate Republicii Moldova, IDNO C = MD	
Validity	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 utilizatorului semnăturii electronice, titular al certificatului	CN = FiscservinformCA OU = Centrul de certificare a cheilor publice O = IS Fiscservinform C = MD	
Subject Public Key Info	Cheia publică	Cheia publică (algoritmul RSA)	
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	SHA256RSA	
Signature Value	Semnătura electronică a emitentului certificatului	Semnătura autorului în acord cu SHA256RSA	
Cîmpurile auxiliare			
Authority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a centrului de certificare, corespunzătoare prezentului certificat	
Key Usage	Utilizarea cheii	Semnătura electronică în certificate, semnătura electronică în lista a certificatelor revocate	CRITIC
Certificate Policies	Politica de certificare a centrului de certificare	Identificatorul politicii = toate politicile de emitere. Informaţiile calificatorului politicii = CPS Informaţiile calificatorului politicii = http://www.pki.sis.md	Poate fi CRITIC
Private Key Usage Period	Termenul de valabilitate a cheii private	Valabil pînă la: DD: MM:YY HH:MM:SS GMT	
Basic Constraints	Restricţii de bază	Tipul subiectului = CA Limitarea lungimii lanţului de certificate = 1	CRITIC
CRL Distribution Point	Punctul de distribuţie a listei certificatelor revocate	URL= http://www.pki. sis.md/ certmd.crl	
Authority Information Access	Accesul la informaţiile despre centrul de certificare	Modalitatea de acces = Furnizorul centrului de certificare (1.3.6.1.5.5.7.48.2) Nume suplimentar: URL=http://www.pki.sis.md/cert/certmd.cer	

Anexa nr. 2
la REG-08 Regulamentul Centrului
de certificare a cheilor publice

Structura certificatului cheii publice a utilizatorului semnăturii electronice

Denumirea (în engleză)	Descrierea	Conţinutul	NOTĂ
Cîmpurile de bază			
Version	Versiunea	V3	
Serial Number	Numărul de înregistrare a certificatului	Numărul	
Issuer	Datele de identificare ale centrului de certificare, emitent al certificatului	CN = Denumirea certificatului centrului de certificare OU = Subdiviziunea persoanei juridice O = Denumirea persoanei juridice, IDNO C = Codul statului	
Validity	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 utilizatorului semnăturii electronice, titular al certificatului	Serialnumber = IDNP a utilizatorului semnăturii electronice CN = Numele, prenumele utilizatorului semnăturii electronice L = Localitatea de domiciliu a utilizatorului semnăturii electronice S = Statul OU = Subdiviziunea persoanei juridice, în care activează utilizatorul semnăturii electronice, după caz O = Denumirea persoanei juridice, IDNO, în care activează utilizatorul semnăturii electronice, după caz P = Telefonul utilizatorului semnăturii electronice, după caz T = Funcţia deţinută de către utilizatorul semnăturii electronice, după caz C = Codul statului	
Subject Public Key Info	Cheia publică	Cheia publică a utilizatorului semnăturii electronice	
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii electronice a emitentului certificatului	
Signature Value	Semnătura electronică a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat	
Cîmpurile auxiliare			
Authority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a centrului de certificare, emitentului certificatului	
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a utilizatorului semnăturii electronice, corespunzătoare prezentului certificat	
Key Usage	Utilizarea cheii	Irevocabilitatea	CRITIC
Certificate Policies	Politica de certificare a centrului de certificare	Identificatorul politicii Informaţiile calificatorului politicii	Poate fi CRITIC
Subject Alternative Name	Numele alternativ al titularului certificatului	RFC822 Name = Poşta electronică a utilizatorului semnăturii electronice	
Basic Constraints	Restricţii de bază	Tipul subiectului = utilizatorul final	Poate fi şi poate fi

		Limitarea lungimii lanţului de certificate = lipsește	CRITIC
CRL Distribution Point	Punctul de distribuţie a listei certificatelor revocate	Sursa publicării listei certificatelor revocate	
Authority Information Access	Accesul la informaţiile despre centrul de certificare	Modalitatea de acces la informaţiile despre centrul de certificare	
Qualified certificate Statements	Criteriu ce determină că certificatul este destinat pentru formarea semnăturii cu putere juridică	Identificatorul certificatului, ce determină că certificatul este destinat pentru formarea semnăturii cu putere juridică în conformitate cu actele normative în domeniul semnăturii electronice, poate conţine restricţii cu privire la aplicarea acestui certificat.	

Anexa nr. 3
la REG-08 Regulamentul Centrului
de certificare a cheilor publice

Lista certificatelor revocate (CRL)

Denumirea (în engleză)	Descrierea	Conţinutul	NOTĂ
Cîmpurile de bază			
Version	Versiunea	V2	
Signature	Algoritmul semnăturii emitentului CRL	Denumirea algoritmului semnăturii electronice a emitentului CRL	
Issuer	Emitentul CRL	CN = Denumirea centrului de certificare OU = Subdiviziunea persoanei juridice O = Denumirea persoanei juridice, IDNO C = Codul statului	
This Update	Data emiterii CRL	«__» _____ 20__ oo:mm:ss GMT	
Next Update	Data următoarei actualizări a CRL	«__» _____ 20__ oo:mm:ss GMT	
Revoked Certificates	Lista certificatelor revocate	userCertificate Numărul de serie a certificatului (CertificateSerialNumber) revocationDate Data revocării sau suspendării valabilităţii certificatului (Time)	
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii electronice a emitentului certificatului	
Signature Value	Semnătura electronică a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat	
Cîmpurile auxiliare			
Authority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a centrului de certificare, care a fost utilizat pentru semnarea CRL	
CRL Number	Numărul de ordine	Numărul de ordine a CRL	
Reason Code	Codul cauzei revocării certificatului	"0" Nu este indicată "1" Compromiterea cheii private "2" Compromiterea centrului de certificare "3" Schimbarea apartenenţei "4" Certificatul a fost schimbat "5" Încetarea activităţii "6" Suspendarea valabilităţii	

Anexa nr. 4
la REG-08 Regulamentul Centrului
de certificare a cheilor publice

CERERE NR._____
PENTRU CERTIFICAREA CHEII PUBLICE-PERSOANE FIZICE

Prin prezenta, _____,
(Nume/Prenume)

în baza Legii nr. 91 din 27.06.2014 privind semnătura electronică şi documentul electronic, rog eliberarea certificatului cheii publice în conformitate cu datele indicate în prezenta cerere şi includerea în certificat a următoarelor informaţii:

Numele, prenumele: _____
IDNP: _____
Adresa de domiciliu: _____
Localitatea: _____
Statul: _____
Codul poştal: _____
Telefon: _____
E-mail: _____

.

Numele Prenumele: _____
Semnătura: _____
Data: _____

Prin aplicarea semnăturii, semnatarul confirmă consimţământul utilizării datelor cu caracter personal în scopul prelucrării cererii respective, iar declararea datelor ce nu corespund realităţii constituie infracţiune şi se pedepseşte conform prevederilor Codului penal

Se completează de către administratorul de înregistrare al Centrului de certificare

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

_____este identificată.

Datele indicate în cerere sunt verificate.

„___” _____20__ administratorul de înregistrare
_____/_____

„___” _____20__ administratorul de certificare
_____/_____

Documentul conţine date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condiţiile prevăzute de legislaţie. Î.S.„Fiscservinform” operator de date cu caracter personal nr.0000072.

Anexa nr. 5
la REG-08 Regulamentul Centrului
de certificare a cheilor publice

CERERE NR._____
PENTRU CERTIFICAREA CHEII PUBLICE-PERSOANE JURIDICE

Prin prezenta, _____
(numele/prenumele conducătorului instituției)

IDNP	
Care activează în baza	
IDNO	
Denumirea instituției	

în baza Legii nr. 91 din 27.06.2014 privind semnătura electronică şi documentul electronic, rog eliberarea certificatului cheii publice în conformitate cu datele indicate în prezenta cerere şi includerea în certificat a următoarelor informaţii:

Numele Prenumele titularului: _____
IDNP: _____
Adresa de domiciliu: _____
Localitate: _____
Ţara: _____
Codul poştal: _____
IDNO: _____
Denumirea instituției: _____
Subdiviziunea: _____
Funcţia: _____
E-mail: _____

Titularul certificatului cheii publice
_____ / _____
(semnătura) (numele, prenumele)

„__” _____ 20__

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

L.Ş.

Prin aplicarea semnăturii, semnatarul confirmă consimțământul utilizării datelor cu caracter personal în scopul prelucrării cererii respective, iar declararea datelor ce nu corespund realității constituie infracțiune și se pedepsește conform prevederilor Codului penal.

Se completează de către administratorul de înregistrare al Centrului de certificare

Prin prezenta confirm că cheia publică pe numele_____,
este identificată. Datele indicate în cerere sunt verificate.

„___” _____20__ administratorul de înregistrare
_____/_____

„___” _____20__ administratorul de certificare
_____/_____

Documentul conține date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de legislație. Î.S.„Fiscservinform” operator de date cu caracter personal nr.0000072.

Anexa nr. 6
la REG-08 Regulamentul Centrului
de certificare a cheilor publice

CERERE NR._____
PRIVIND MODIFICAREA STATUTULUI CERTIFICATULUI CHEII PUBLICE

Subsemnatul_____, solicit
(Numele/Prenumele solicitantului)

☐ **REVOCARE** ☐ **SUSPENDARE: de la_____pînă la_____** ☐ **RESTABILIRE**

Datele personale ale titularului certificatului cheii publice:
Nume/Prenume: _____
IDNP: _____
e-mail _____
fiind angajat al (denumirea instituției) : _____
IDNO: _____
în legătură cu: _____
(motivul)

* Titularul certificatului cheii publice
_____ / _____
(semnătura) (numele, prenumele)

„__” _____ 20__

**Conducătorul instituției
_____ / _____
(semnătura) (numele, prenumele)

**L.Ş.

*se va completa în cazul în care solicitarea parvine din partea titularului certificatului cheii publice
**se va completa în cazul în care solicitarea parvine din partea conducătorului instituției

Prin aplicarea semnăturii, semnatarul confirmă consimțământul utilizării datelor cu caracter personal în scopul prelucrării cererii respective, iar declararea datelor ce nu corespund realității constituie infracțiune și se pedepsește conform prevederilor Codului penal.

Se completează de către administratorul de înregistrare al Centrului de certificare

Prin prezenta confirm că solicitarea privind certificatul cheii publice emis pe numele/prenumele

_____,

cu nr.certificatului_____,

a fost verificată și executată. Datele indicate în cerere sunt verificate.

„___” _____20__ administratorul de înregistrare
_____/_____

„___” _____20__ administratorul de certificare
_____/_____

Documentul conține date cu caracter personal. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de legislație. Î.S.„Fiscservinform” operator de date cu caracter personal nr.0000072.