Aprobat:

prin Ordinul Directorului

Europarc SRL

nr. **2** din **03 ianuarie 2023**

---

27 de pagini

REGULAMENTUL DE CERTIFICARE A CHEILOR PUBLICE

ALE EUROPARC

EUROPARC – prestator al serviciilor de încredere, (licență nr. 003926 din 30,12,2022), în conformitate cu Legea Nr. 124 din 19-05-2022 privind identificarea electronică și serviciile de încredere, cu respectarea prevederilor Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, publicat în Jurnalul Oficial al Uniunii Europene L 257 din 28 august 2014.

Prezentul Regulament descrie Procedura de lucru, Politica și Codul de Practici ale Centrului De Certificare A Cheilor Publice ale EUROPARC.

Regulamentul este elaborat în conformitate cu Legea Nr. 124 din 19-05-2022 privind identificarea electronică și serviciile de încredere.

Istoric document Ediție	**Versiune**	**Descriere**	**Data**	**Emitent**
1	0	Prima redactare:	**03 ian 2023**	CCC

EUROPARC SRL operează o infrastructură de chei publice (denumită în continuare PKI) în vederea furnizării de servicii de încredere.

În calitate de prestator al serviciilor de încredere, iar in speță - Autoritate de Certificare, EUROPARC SRL emite certificate atât persoanelor juridice, cât și persoanelor fizice din cadrul sectorului public, cât și celui privat, în conformitate cu regulile, principiile și practicile definite în acest document.

EUROPARC SRL urmărește să se afirme în calitate de unul din principalii Prestatori de Servicii de Încredere Calificate.

EUROPARC SRL garantează că:

- Activitatea sa comercială este asigurată pe baza unor echipamente și aplicații software fiabile,
- Activitățile și serviciile furnizate sunt conforme cu legislația aplicabilă și, în special, nu încalcă proprietatea intelectuală, licențele și alte drepturi conexe,
- Serviciile furnizate sunt conforme cu normele general acceptate,
- Menține o echipă competentă și experimentată care să asigure continuitatea serviciilor de marcare temporală,
- Asigură în permanență securitatea fizică și logică, precum și integritatea materialelor, software-urilor și bazelor de date necesare pentru funcționarea corectă, așa cum este descris în acest document,
- Va monitoriza și va controla infrastructura, pentru a preveni sau a limita orice perturbare sau indisponibilitate care rezultă din atacuri deliberate,
- Va lua toate măsurile necesare conform normelor general acceptate pentru a-și asigura serviciile,
- Va pune la dispoziție o infrastructură de rezervă care poate fi utilizată în cazul întreruperii serviciului infrastructurii principale.

1. Centrul de certificare a cheilor publice (în continuare *CCC*) – este subdiviziune a EUROPARC SRL, responsabilă de emiterea certificatelor și gestionarea ulterioară a acestora, responsabil de identificarea și autentificarea solicitanților, formarea cererii pentru certificare și executarea unor proceduri legate de gestionarea certificatelor (revocare, suspendare, reînnoire).

2. Centrul de certificare a cheilor publice este responsabilul de PKI (arhitectura, tehnicile, practicile și procedurile care contribuie la implementarea și funcționarea sistemelor criptografice cu chei publice și care constă din hardware și software, baze de date, resurse de rețea, proceduri și practici de securitate și obligații legale, legate împreună și care colaborează pentru a furniza și implementa atât servicii de certificare, cât și alte servicii asociate infrastructurii).

3. În cadrul CCC, sub aspect structural, sunt prevăzute următoarele funcții:

a) **conducătorul CCC**, având ca sarcină de bază organizarea tehnică a activității CCC;

b) **administratorul înregistrări** este responsabil de:

i) 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;

ii) înregistrarea și evidența titularilor certificatelor cheilor publice în procesul creării, suspendării sau restabilirii valabilității și revocării certificatelor cheilor publice;

iii) pregătirea solicitărilor titularilor certificatelor cheilor publice;

iv) eliberarea certificatelor cheilor publice titularilor acestora;

v) înștiințarea solicitantului certificatului cheii publice despre refuzul motivat de eliberare a certificatului cheii publice;

vi) înștiințarea titularului certificatului despre faptele care fac imposibilă utilizarea în continuare a cheii private, precum și despre revocarea certificatului cheii publice;

vii) asigurarea semnării actelor juridice cu solicitanții privind eliberarea semnăturii electronice.

viii) Alte obligații.

c) **administratorul certificare** (persoana împuternicită a CCC), este responsabil de crearea (generarea), suspendarea și restabilirea valabilității certificatelor cheilor publice;

d) **administratorul securitate**, este responsabil de:

i) controlul securității tuturor procedurilor și mecanismelor CCC;

ii) asigurarea securității componentelor complexului tehnic de program al CCC;

iii) elaborarea și implementarea politicii de securitate a CCC.

e) **administratorul sistem**, este responsabil de: instalarea, configurarea și întreținerea funcționării infrastructurii CCC.

Pentru îndeplinirea funcțiilor sale Centrul de certificare a cheilor publice:

- asigură înregistrarea persoanele fizice și juridice ce solicită eliberarea certificatelor cheii publice;

- asigură crearea și eliberarea certificatelor cheilor publice pe baza cererii persoanelor fizice și persoanelor împuternicite ale persoanelor juridice, sub formă de document pe suport de hârtie semnat cu semnătură olografă sau electronică, în conformitate cu procedurile stabilite de prezentul Regulament;

- suspendă și restabilește valabilitatea, revocă certificatele cheilor publice ale titularilor în cazurile și în conformitate cu procedurile stabilite de prezentul Regulament, actele juridice încheiate și legislația în vigoare;

- întocmește și gestionează Registrul certificatelor cheilor publice sub formă de documente electronice;

- publică și actualizează Registrul certificatelor cheilor publice revocate;

- acordă consultații și suport metodologic persoanelor fizice și juridice;

- confirmă autenticitatea și valabilitatea certificatelor cheilor publice ale persoanelor fizice și juridice;

- desfășoară activitatea în domeniul protecției criptografice și tehnice a informației;

- creează sistemele informaționale și de comunicații electronice ale CCC, asigură funcționarea, securitatea, deservirea și modernizarea lor, efectuează auditul intern permanent al securității și funcționalității acestor sisteme.

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

- 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 electronice (în continuare – organul competent);

- să asigure securitatea cheilor private, 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 CCC numai la semnarea certificatelor cheilor publice eliberate de acesta și a listelor certificatelor revocate;

- să creeze lista certificatelor revocate în conformitate cu cerințele stabilite de organul competent și de prezentul Regulament, conform modelului din Anexa nr. 2;

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

- să suspende imediat valabilitatea certificatului cheii publice 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 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 fizice și 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 informațiilor cuprinse în certificatul cheii publice cu informațiile prezentate de către persoanele fizice și juridice;

- să asigure unicitatea informației de înregistrare a titularilor 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 al persoanelor fizice și juridice, 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 titularilor în conformitate cu procedurile stabilite de prezentul Regulament;

- să suspende și să restabilească, să revoce certificatele cheii publice ale titularilor certificatelor cheii publice în cazurile și 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, precizând data, ora și 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 înștiințeze din timp titularii certificatelor cheilor publice despre suspendarea valabilității sau revocarea certificatului cheii publice, în cazurile și în conformitate cu procedurile stabilite de prezentul Regulament;

- să înștiințeze titularii certificatelor cheilor publice despre restabilirea valabilității certificatelor cheilor publice în conformitate cu procedurile stabilite de prezentul Regulament;

- să înștiințeze titularii certificatelor cheilor publice despre faptele de care a luat cunoștință CCC și care pot influenta esențial posibilitatea utilizării ulterioare a certificatului cheii publice;

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

- să păstreze toată informația cu privire la certificatul cheii publice al titularului, precum și alte informații despre acest certificat nu mai puțin de 15 ani din momentul revocării sau expirării termenului de valabilitate a certificatului;

- să asigure actualizarea Registrului certificatelor cheilor publice generate și revocate și posibilitatea accesului liber la acesta în vederea verificării autenticității semnăturii electronice și să întreprindă măsurile necesare pentru asigurarea securității datelor cu caracter personal conform legislației în domeniul protecției datelor cu caracter personal;

- 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 titularului semnăturii electronice, să confirme autenticitatea și valabilitatea certificatelor cheilor publice;

- 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 electronice, să confirme autenticitatea și valabilitatea certificatelor cheilor publice eliberate de CCC și să prezinte, pe suport de hârtie, copiile actelor în baza cărora a fost eliberată semnătura electronică;

- să sincronizeze activitatea serviciilor CCC, inclusiv a mijloacelor tehnice și de program conform destinației, cu Timpul Mondial Coordonat (UTC). Se permită sincronizarea serviciilor conform Timpului Greenwich (Greenwich Mean Team, GMT), fără trecerea la ora de vară conform NTP. Network Time Protocol: este un protocol de rețea pentru sincronizarea timpului sistemelor informatice prin rutarea pachetelor de rețea cu latență variabilă. Standardul de referință este IETF RFC 1305 (Network Time Protocol (NTP v3)

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

- să dispună de personal auxiliar care posedă calificarea necesară.

- alte obligații prevăzute de legislația în vigoare.

- să creeze certificatul cheii publice al persoanei împuternicite a CCC și 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, precizând motivele refuzului, în cazurile prevăzute de lege a) depunerii cererii de certificare a cheii publice cu încălcarea prevederilor art. 11 din Legea 124/2022; b) încălcării drepturilor unor terți în procesul de întocmire sau de depunere a cererii de certificare a cheii publice; c) prezentării în cererea de certificare a cheii publice a unor informații care nu sunt veridice.

- să revoce certificatul cheii publice al titularului în cazurile și în modul prevăzute de legislație și de prezentul Regulament.

Drepturile și obligațiile se ajustează conform legislației în vigoare și Conform condițiilor generale de furnizare a serviciilor, publicate pe www.europarc.md.

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

5.1 Titularul certificatului cheii publice este obligat:

- să prezinte referitor la sine informația necesară, prevăzută de procedura de identificare și să prezinte CCC documentele confirmative relevante;

- să prezinte informațiile în volumul determinat de prezentul Regulament;

- să comunice referitor la orice modificări, ce țin de informația personală, înregistrată în procesul de identificare; - să respecte cerințele legislației în domeniul aplicării semnăturii electronice;

- să aplice cheia sa privată în conformitate cu domeniile de aplicare a semnăturii electronice și alte restricții indicate în certificatul cheii publice;

- să asigure păstrarea cheii private în conformitate cu cerințele 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 CCC despre situațiile de compromitere a informației 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 CCC 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.

Drepturile și obligațiile se ajustează conform legislației în vigoare și Conform condițiilor generale de furnizare a serviciilor, publicate pe www.europarc.md.

5.2 Titularul certificatului cheii publice are dreptul:

- să primească întregul spectru de servicii, prevăzute de Regulamentul CCC;

- să depună cererea de certificare a cheii publice;

- să aplice în mod repetat cererea pentru certificare cu condiția că toate observațiile prezentate cu referire la prima cerere au fost înlăturate;

- să depună cererile de suspendare valabilității certificatului cheii publice în perioada de valabilitate a cheii private corespunzătoare;

- să depună cererea de restabilire a valabilității certificatului cheii publice;

- să depună cererea pentru confirmarea autenticității și valabilității certificatului cheii publice; - să depună cererile de revocare a certificatului cheii publice în perioada de valabilitate a cheii private corespunzătoare;

- să obțină accesul la Registrul certificatelor cheilor publice și a Listei certificatelor revocate;

- să utilizeze certificatul cheii publice al persoanei împuternicite a CCC pentru verificarea autenticității semnăturii electronice în certificatele cheilor publice eliberate de către CCC;

- să utilizeze resursele informaționale puse la dispoziție de către CCC pentru confirmarea verificarea autenticității și valabilității certificatului cheii publice;

- să semneze și 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 depășirea limitelor valorice pentru care este valabilă în documentele electronice de plată sau de încheiere a tranzacțiilor;

- în cazul apariției situației litigioase ce ține de stabilirea autenticității și/sau a autorului documentului contestabil, să solicite soluționarea ei în modul stabilit de legislație;

- să primească consultații cu privire la aplicarea semnăturii electronice și verificarea autenticității documentului electronic de la personalul subdiviziunii responsabile și al prestatorului de servicii de certificare.

Drepturile și obligațiile se ajustează conform legislației în vigoare și Conform condițiilor generale de furnizare a serviciilor, publicate pe www.europarc.md.

6. Crearea și administrarea certificatului cheii publice a Centrului de certificare a cheilor publice

6.1 Certificarea cheii publice a Centrului de certificare a cheilor publice CCC creează cheia sa privată și cea publică în conformitate cu cerințele stabilite de organul competent. Crearea certificatului cheii publice a CCC se realizează de CCC de nivel superior conform cerințelor stabilite de legislație.

Generarea perechii de chei este un proces critic dat fiind faptul că modul în care este generată o pereche de chei este esențială pentru siguranța întregului sistem PKI. EUROPARC garantează că

orice cheie criptografică este generată în circumstanțe controlate și în conformitate cu cele mai bune practici din domeniu pentru ciclul de viață al cheii, lungimea cheii și algoritmii.

EUROPARC generează pereche de chei criptografice utilizate în serviciile sale de către personalul autorizat într-un mediu fizic securizat, într-un mod de securitate hardware (HSM) care este certificat ca fiind compatibil cu standardul FIPS 140-2 Level 3 sau cu standardul ISO 15408 Common Criteria EAL 4+.

Astfel, perechea de chei este generată și există pe toată durata vieții într-un mediu protejat fizic și electromagnetic. Cheia privată este păstrată permanent într-un format criptat și niciodată nu este lăsată într-un format necriptat.

Toate acțiunile întreprinse atunci când se generează perechea de chei sunt înregistratei.
Înregistrările sunt păstrate din motive de audit sau pentru verificări periodice ale sistemului.

După ce perechea cheilor este generată și cheia privată este activată în HSM, ea poate fi utilizată în operații criptografice până la expirarea perioadei de validitate.

6.2 Suspendarea valabilității certificatului cheii publice a Centrului de certificare a cheilor publice. Suspendarea valabilității certificatului cheii publice a CCC se realizează de CCC de nivel superior conform cerințelor stabilite de legislația în domeniul aplicării semnăturii electronice.
6.3 Revocarea certificatului cheii publice a Centrului de certificare a cheilor publice Certificatul cheii publice a CCC se revocă pe baza deciziei CCC de nivel superior conform cerințelor stabilite de legislație.
6.4 Administrarea cheii private și cheii publice a Centrului de certificare a cheilor publice

Valabilitatea cheii private: 10 ani - pentru prestatorul de nivel superior, 5 ani - pentru prestatorii de nivelul al doilea

Valabilitatea cheii publice: 20 ani - pentru prestatorul de nivel superior, 10 ani - pentru prestatorul de nivelul al doilea.

La expirarea termenului de valabilitate a cheii private a CCC, cheia privată se distruge, se creează din nou cheia privată și cea publică, precum și certificatul cheii publice. Procedurile de schimbare planificată a cheilor se realizează în conformitate cu regulamentul intern.

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

Cheia privată a CCC se păstrează și se utilizează în condiții ce exclud încălcarea confidențialității acestuia.

Accesul la suportul material al cheii private a CCC se efectuează cu autorizarea scrisă a CCC, Conducătorul CCC, administratorul certificare și administratorul securitate poartă răspundere personală pentru utilizarea sigură a cheii private a CCC.

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

CCC prestează servicii de certificare a cheilor publice atât persoanelor fizice, cât și persoanelor juridice, conform prezentului Regulament, 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 valabilității 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 autenticității și valabilității certificatului cheii publice.

CCC prestează servicii conform politicii sale comerciale reflectate în contracte, oferte publice.

Înregistrarea și autentificarea identității

Înregistrarea constă din proceduri ce permit verificarea veridicității datelor prezentate și presupune proceduri pentru colectarea datelor veridice necesare la identificarea solicitantului de certificat al cheii publice. Verificarea identității unui utilizator este făcută în mod obligatoriu în etapa de înregistrare a datelor.

Depunerea pachetului de documente se face conform art. 11 din Legea 124/2022 sau în alt mod care va asigura respectarea art. 11 din Legea 124/2022.

Pentru certificarea cheii publice a persoanei fizice, aceasta adresează un demers (pe hârtie sau electronic, conform modelului anexat sau in format liber) cu indicarea datelor de identificare.

Pentru certificarea cheii publice a persoanei juridice, este nevoie de un demers (pe hârtie sau electronic, conform modelului anexat sau in formă liberă) cu indicarea datelor de identificare, semnat de către administratorul, sau persoana împuternicită (împuternicirile trebuie confirmate prin procură/mandat).

Autentificarea identității asigură că datele din cererea creată corespund entității respective.

Procedura de identificare constă în verificarea setului de date care permite stabilirea identității unei persoane fizice sau a datelor de identificare ale unei persoane juridice ori a identității persoanei fizice care reprezintă o persoană juridică. Verificarea se efectuează fizic și/sau electronic (la distanța) conform prevederilor legale.

După verificarea datelor prezentate pentru certificare, acesta este inclus în lista abonaților CCC.

CCC înregistrează solicitantul și sau refuză cu indicarea motivelor. Refuzul nu împiedică depunerea repetată a cererii.

În cazul înregistrării solicitantului, **CCC eliberează certificatele cheii publice solicitantului**, în termenii și condițiile tehnice acceptate de către solicitant conform contractul sau ofertei publice.

Certificatul cheii publice al titularului conține datele conform Anexei nr. 1 și/sau alte date prevăzute sau neinterzise de legislația în vigoare.

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

Suspendarea valabilității certificatului cheii publice al titularului se efectuează:

a) la cererea titularului certificatului cheii publice.

b) conform contractului și/sau ofertei publice, de către CCC;

c) în baza hotărârii/deciziei instanței de judecată

d) alte cazuri prevăzute de lege.

Cererea de suspendare a valabilității certificatului cheii publice va fi completată și prezentată conform modelului din Anexa nr. 6 al prezentului Regulament (sau in formă liberă cu indicarea datelor de identificare).

Cererea de suspendare a valabilității certificatului cheii publice poate fi depusă și în formă verbală prin mijloacele de comunicare.

CCC efectuează autentificarea titularului care solicită suspendarea valabilității certificatului cheii publice ce-i aparține. Autentificarea se realizează conform:

a) datelor din buletinul de identitate al solicitantului;

b) frazei-cheie sau cuvântului-cheie pentru autentificarea la distanță, comunicată la telefon de către titular.

Autentificarea la distanță poate avea loc și prin alte metode prevăzute de lege și/sau aprobate de către CCC.

CCC ia decizia privind suspendarea valabilității certificatului în termen de 3 (trei) ore lucrătoare și comunică titularului despre decizia privind suspendarea valabilității certificatului cheii publice sau despre refuzul de suspendare, în termen de 3 (trei) zile lucrătoare.

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

Dacă CCC are motive să presupună că a fost încălcată confidențialitatea cheii private a titularului sau informațiile cuprinse în certificatul cheii publice nu corespund realității, CCC este în drept să ia unilateral decizia privind suspendarea valabilității certificatului cheii publice corespunzător. În cazul suspendării valabilității certificatului cheii publice al titularului pe baza deciziei organului competent sau a CCC, CCC informează imediat, prin mijloacele legăturii telefonice, titularul despre suspendarea valabilității certificatului cheii publice comunicând 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 până 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, până 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.

Restabilirea valabilității certificatului cheii publice al titularului se efectuează:

a) la cererea titularului certificatului cheii publice;

b) pe baza deciziei CCC.

c) în baza hotărârii instanței de judecată.

d) în alte cazuri prevăzute de lege.

Cererea de restabilire a valabilității certificatului cheii publice al titularului se depune nu mai târziu de 5 (cinci) zile lucrătoare până la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice. Cererea de restabilire a valabilității certificatului cheii publice va fi completată și prezentată conform Anexei nr. 5 sau 6 al prezentului Regulament. CCC ia decizia de restabilire a valabilității certificatului, în termen de 3 (trei) zile lucrătoare din data primirii cererii de restabilire a valabilității certificatului cheii publice. CCC comunică titularului despre decizia privind restabilirea sau privind refuzul de restabilire a valabilității certificatului cheii publice, indicând motivele refuzului, în termen de 3 (trei) zile lucrătoare.

Valabilitatea certificatului cheii publice, suspendată pe baza deciziei organului competent, se restabilește prin decizia organului competent sau a instanței de judecată.

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

În cazul restabilirii valabilității certificatului cheii publice al titularului pe baza deciziei organului competent sau a CCC, CCC informează titularul despre restabilirea valabilității 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 valabilității certificatului cheii publice al titularului se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în câmpul This Update).

Revocarea certificatului cheii publice al titularului se face:

a) la cererea titularului certificatului cheii publice conform Anexei 5 sau 6;

b) la cererea conducătorului persoanei juridice în care activează titularul certificatului cheii publice, în cazul certificatelor eliberate titularilor acestora pentru reprezentarea persoanei juridice;

c) la depistarea unor informații neveridice în cererea de certificare a cheii publice sau în certificatul cheii publice;

d) la încălcarea confidențialității cheii private (compromiterea cheii private);

e) la expirarea termenului pentru care a fost suspendată valabilitatea certificatului cheii publice și în lipsa unei cereri din partea titularului certificatului cheii publice privind restabilirea valabilității acestuia;

f) la modificarea informației cuprinse în certificatul cheii publice;

g) în cazul decesului titularului certificatului cheii publice sau al instituirii unei măsuri de ocrotire judiciare (ocrotire provizorie, curatelă sau tutelă) în privința titularului;

h) la solicitarea organului de supraveghere și control, în cazul încălcării prezentei legi.

i) în alte cazuri prevăzute de legislația în vigoare.

Certificatul cheii publice revocat al titularului, în termen de 3 (trei) ore de lucru se înscrie în lista certificatelor revocate, iar CCC 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 câmpul This Update). În cazul revocării certificatului cheii publice pe motivul expirării termenului de valabilitate a acestuia, certificatul nu se înscrie în lista certificatelor revocate.

Confirmarea autenticității și valabilității certificatului cheii publice

CCC confirmă autenticitatea și valabilitatea certificatelor cheilor publice:

a) la solicitarea titularului certificatului cheii publice;

b) la cererea instanței de judecată,

c) în alte cazuri neinterzise de lege.

CCC asigură titularilor semnăturii electronice, precum și terților, posibilitatea de a stabili, de regulă contra plată, de sine stătător, autenticitatea și valabilitatea certificatului cheii publice al titularului prin:

a) acordarea accesului la Registrul certificatelor cheilor publice și Listei certificatelor revocate în baza numărului de serie a certificatului cheii publice, sau

b) oferirea serviciului online de verificare a certificatului cheii publice în baza numărului de serie a acestuia.

La solicitarea titularului certificatului cheii publice, în condițiile de plată stabilite de prestator, CCC oferă titularului acces la următoarele date privind **rezultatele verificării autenticității** și valabilității certificatului cheii publice, care va conține:

a) timpul și locul verificării;

b) cauza verificării;

c) datele despre angajatul CCC care a efectuat verificarea (numele, prenumele, funcția);

d) conținutul și rezultatele verificării;

e) evaluarea rezultatelor verificării și concluziile corespunzătoare;

f) alte date stabilite de CCC.

CCC poate refuza solicitantului să verifice autenticitatea și valabilitatea certificatului cheii publice al titularului, dacă nu au fost respectate cerințele Prezentului Regulament.

7 Registrul certificatelor cheilor publice.

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

a) certificatele cheilor publice ale persoanelor împuternicite ale CCC;

b) cererile de certificare a cheilor publice ale solicitanților;

c) certificatele cheilor publice ale titularilor;

d) cererile de revocare a certificatelor cheilor publice ale titularilor;

e) listele certificatelor revocate.

În arhiva CCC se păstrează următoarele resurse informaționale:

a) registrul certificatelor cheilor publice;

b) registrele de audit al complexului tehnic de program al CCC;

c) documentele de serviciu ale CCC, conform criteriilor stabilite de conducătorul Centrului. Termenul de păstrare a documentelor de arhivă ale CCC este de 15 (cincisprezece) ani.

Pregătirea pentru distrugere și distrugerea documentelor de arhivă se efectuează de către o comisie formată din angajați ai CCC. Pregătirea pentru distrugere și distrugerea documentelor care nu necesită a fi păstrate în arhivă se efectuează de către CCC.

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

Accesul utilizatorilor semnăturii electronice la versiunea electronică a Registrului certificatelor cheilor publice (lista certificatelor) se efectuează prin intermediul resursei informaționale electronice.

Mijloacele de asigurare a activității Centrului de certificare a cheilor publice

CCC 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 electronice.

Serviciul certificare reprezintă componentul tehnologic de bază al complexului tehnic de program al CCC 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 și administratorul sistem.

Serviciul înregistrare reprezintă componentul tehnologic al complexului tehnic de program al CCC care asigură înregistrarea utilizatorilor. Responsabilitatea pentru exploatarea serviciului înregistrare o poartă AÎ.

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

a) păstrarea certificatelor cheilor publice ale persoanelor împuternicite ale CCC;

b) păstrarea certificatelor cheilor publice ale titularilor;

c) păstrarea cererilor de certificare a cheilor publice;

d) păstrarea informației de înregistrare a titularilor certificatelor cheilor publice;

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 CCC.

Serviciul control etalonat al semnăturii electronice reprezintă componentul tehnologic al complexului tehnic de program al CCC care asigură confirmarea autenticității certificatelor cheilor publice și a altor documente electronice.

Mijloacele tehnice de asigurare a funcționării complexului tehnic de program al CCC includ:

a) echipamentul de server;

b) echipamentul de comunicații electronice;

c) locurile de muncă computerizate ale administratorilor CCC;

d) dispozitivele de imprimare pe suport de hârtie;

e) alte echipamente auxiliare.

Responsabilitatea pentru exploatarea mijloacelor tehnice de asigurare a funcționării complexului tehnic de program al CCC o poartă administratorul sistem. În componența complexului tehnic de program al CCC funcționează mijloacele de protecție criptografică a informației, inclusiv complexele tehnice de program de protejare contra accesului neautorizat și de asigurare a integrității mijloacelor tehnice de program.

Responsabilitatea pentru exploatarea mijloacelor de protecție a informației o poartă administratorul sistem și administratorul securitate. Complexul tehnic de program trebuie să corespundă cerințelor stabilite de organul competent și actele normative în domeniu.

Repozitoriu și publicarea

Publicarea informației despre certificatele cheilor publice

Repozitoriul CCC este o interfață publică ce poate conține următoarea informație:

- versiunile actuale și anterioare ale prezentului Regulamentul și ale Politicilor de certificare (extrase)

- contracte-tip / Oferte publice, ce urmează a fi semnate cu titularii certificatelor cheilor publice;

- formulare de cereri-tip de creare, de suspendare și reînnoire a valabilității, de revocare a certificatului cheii publice;

- lista centrelor de înregistrare împuternicite sau partenerilor împuterniciți;

- lista certificatelor cheilor publice ale titularilor;

- lista certificatelor revocate;

- altă informație ce se modifică în timp real.

Volumul și conținut informației poate fi modificat la discreția CCC.

Interacțiunea titularilor certificatelor cheilor publice cu Centrul de certificare a cheilor publice

Interacțiunea titularilor certificatelor cheilor publice cu CCC se efectuează în conformitate cu procedurile stabilite de prezentul Regulament și cu cerințele în domeniul semnăturii electronice.

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

Sunt supuse soluționării în conformitate cu prezentul Regulament situațiile litigioase care apar în legătură cu:

a) contestarea integrității documentului electronic;

b) contestarea identificării persoanei care a semnat documentul electronic;

c) contestarea împuternicirilor persoanei care a semnat documentul electronic;

d) contestarea valabilității și autenticității certificatului cheii publice a CCC și utilizatorului semnăturii electronice;

e) alte situații litigioase în legătură cu aplicarea semnăturii electronice.

Situațiile litigioase, în dependență de natura și complexitatea lor, se soluționează în regim de lucru și/sau de către Comisia de soluționare a situațiilor litigioase în domeniul aplicării semnăturii electronice (în continuare – Comisia) creată de către prestator, în condițiile prevăzute de contract sau oferta publică sau de către arbitraj sau instanţa de judecată.

8 Responsabilitatea financiară

În scopul garantării reparării prejudiciilor, care ar putea fi cauzate titularilor certificatelor cheilor publice, utilizatorilor sau terților persoane în urma neîndeplinirii sau îndeplinirii neconforme de către CCC a deține o garanție bancară sau o poliță de asigurare, conform exigențelor legale, care stabilesc și limitele financiare de răspundere de **300.000 lei**.

9 Asigurarea securității și protecția informațiilor confidențiale

Informațiile care se prelucrează și se păstrează în CCC sunt protejate prin lege. Informațiile care se păstrează în registrele de audit ale CCC sunt confidențiale. Nu sunt confidențiale informațiile ce se conțin în registrul certificatelor cheilor publice și în listele certificatelor revocate. CCC asigură integritatea și controlul accesului la informațiile protejate de lege în conformitate cu legislația Republicii Moldova. Activitățile de prelucrare a datelor cu caracter personal în cadrul CCC sunt notificate în condițiile legii și sunt reglementate prin Politica de securitate a datelor cu caracter personal.

Măsurile tehnico-inginereşti de protecție a informației

Măsurile tehnico-inginereşti de protecție a informației trebuie să asigure posibilitatea funcționării neîntrerupte, pe o durată îndelungată, a complexului tehnic de program al CCC.

EUROPARC va dispune sau contracta serviciile de server care corespund exigențelor cerute de legislație și/sau celor mai bune practici din domeniu.

Măsurile de protecție a informației cu mijloacele de program

Complexul tehnic de program al CCC trebuie să asigure controlul integrității mijloacelor tehnice și de program. Responsabilitatea pentru îndeplinirea măsurilor de verificare a integrității

mijloacelor tehnice și de program ale complexului tehnic de program al CCC o poartă administratorul sistem și administratorul securitate.

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

Măsurile organizatorice de protecție a informației

Măsurile organizatorice, destinate prevenirii situațiilor de compromitere a securității resurselor CCC, sunt în conformitate cu Politica de Securitate aprobate de EUROPARC și se bazează pe următoarele:

- evidența resurselor care necesită a fi protejate;

- prevenirea accesului, modificării și/sau distrugerii neautorizate a datelor;

- prevenirea divulgării sau transmiterii nesancționate a informațiilor confidențiale unor terți;

- depistarea oportună a accesului nesancționat la informațiile confidențiale;

- prevenirea influențelor externe asupra mijloacelor tehnice de prelucrare a datelor;

- controlul nivelului de protecție a datelor;

- managementul incidentelor de securitate;

- conștientizarea asigurării securității datelor prelucrate în cadrul CCC.

Asigurarea măsurilor organizatorice de protecție a informației este pusă în sarcina administratorului securitate.

10 Arhivarea informațiilor aferente Centrului de certificare a cheilor publice. Politica de Arhivare (backup)

Arhivarea informației pe hârtie se realizează în spații special amenajate care să asigure condițiile specifice de păstrare.

Durata de arhivare a informației și documentelor, în format electronic și pe hârtie, retrase din uz (originalele) este minim cel prevăzut de lege.

Pentru a se exclude posibilitatea utilizării documentelor depășite sau anulate, acestea vor fi periodic revizuite și, în caz de necesitate – prompt retrase din uz.

Datele arhivate electronic sunt protejate de vizualizarea nesancționată, modificări sau ștergerea prin intermediul controlorilor de acces fizic și logic.

Pentru verificarea integrității și a posibilității de restabilire a datelor copiile de arhivă și de rezervă sunt supuse verificării periodice și comparării cu originalul (dacă este posibil). Acest tip de verificare este accesibil doar administratorului securitate.

Tipurile de informații supuse arhivării:

CCC gestionează două tipuri de arhive:

1) arhiva documentelor pe suport de hârtie:

- documente și date folosite în procesul de identificare a identității;

- cererile și datele primite de la solicitant pe suport de hârtie;

- actele juridice încheiate și semnate dintre CCC și titularii certificatelor cheilor publice;

- corespondența internă și externă dintre CCC și titulari etc.

2) arhiva electronică:

- istoria cheilor titularilor din momentul generării lor și până la nimicire;

- istoria cheilor CCC din momentul generării și până la momentul nimicirii;

- baza de date a titularilor certificatelor cheilor publice;

- baza de date a certificatelor cheilor publice;

- listele certificatelor revocate publicate;

- cererile și datele primite în format electronic de la solicitant;

- informație despre efectuarea controalelor mijloacelor ce asigură securitatea (primită din rapoartele auditului) etc.

Copiile arhivei

Copiile de arhivă permit restabilirea completă (e.g., după căderea sistemului) a tuturor datelor necesare pentru funcționarea corectă a CCC. Metodele de creare a copiilor de rezervă trebuie să asigure posibilitatea de restabilire rapidă a datelor și sistemelor în cazul pierderii sau deteriorării lor.

În CCC se aplică următoarele două metode:

- copierea de rezervă ce are loc zilnic și poate fi utilizată în cazul restabilirii rapide a datelor pierdute;

- copierea de rezervă pentru asigurarea restabilirii rapide a configurațiilor și setărilor echipamentului și mijloacelor de program.

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

11 Procedura/Algoritmul de restabilire a sistemului în caz de compromitere și defecțiuni

Compromiterea Centrului de certificare a cheilor publice

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

- CCC generează o pereche nouă de chei și obține un nou certificat de cheie publică;

- titularii certificatelor cheilor publice sunt notificați imediat despre compromiterea cheilor prin intermediul mass-media și al poștei electronice;

- certificatul cheii publice, corespunzător cheii compromise lichidate, se revocă și se plasează în lista certificatelor revocate;

- toate certificatele din lanțul certificatelor în care se află certificatul compromis, se înregistrează în lista de certificate revocate cu indicarea motivului respective („CA compromise”);

- abonaților le sunt eliberate certificate noi de chei publice;

- se execută livrarea noilor certificate către abonați fără perceperea unei taxe suplimentare.

Caz de deteriorare a resurselor informaționale

Normele de siguranță care se aplică în cadrul CCC stipulează diverse situații, la apariția cărora trebuie să fie păstrată operaționalitatea CCC și garantat nivelul prestării serviciilor:

- deteriorarea fizică a sistemelor informatice, inclusiv deteriorarea infrastructurii rețelei și a cablurilor

- ca urmare a unei situații de avarie;

- defecțiuni ale complexului de programe, incapacitatea de a accesa datele

- ca rezultat al deteriorării spațiului sistemelor de operare, aplicațiilor utilizatorilor, sau al rulării altor programe, cum ar fi „virușii", „troienii", „viermii";

- pierdere (oprire, lipsă de acces) a serviciilor importante de rețea, oferite de către CCC, în primul rând se referă la pierderea alimentării cu energie electrică sau deteriorarea conexiunilor de rețea;

- deteriorare a unei părți a rețelei interne, utilizată de către CCC pentru furnizarea serviciilor sale - poate conduce la indisponibilitatea deservirii titularilor.

Restabilirea securității după o situație de avarie

La finalul procedurilor de restabilire a sistemului după o situație de avarie, administratorii CCC sunt obligați să:

- înlocuiască toate parolele utilizate anterior;

- elimine drepturile utilizate anterior de acces la sistem și la resursele acestuia;

- înlocuiască toate codurile și PIN-urile, asociate cu accesul fizic la componentele CCC;

- în conformitate cu Politica de securitate si control al accesului în CCC, toate componentele de rețea și regulile accesului fizic trebuie să fie revizuite;

- informeze conducerii despre restabilirea funcționării sistemului.

Continuitatea activității Centrului de certificare a cheilor publice în cazuri excepționale

Auditarea Centrului de certificare a cheilor publice

Activitățile desfășurate în cadrul CCC sunt supuse auditării, în conformitate cu reglementările interne ale Europarc sau de către instituții independente competente (audit extern).

A
nexa nr. 1
Regulamentul
Centruluide
certificare a cheilor
publice

1. 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 și Securitate Republicii Moldova, IDNO C = MD	
Validity	Termenul de valabilitate a certificatului	Valabil de la: «_»_____20_____oo:mm:ss GMT Valabil până 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 publiceO = IS Fiscservinform C = MD	
Subject PublicKey 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 KeyIdentifier	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

CertificatePolicies	Politica de certificare a centrului de certificare	Identificatorul politicii = toate politicile deemitere. 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 până la: DD: MM:YY HH:MM:SS GMT	
Basic Constraints	Restricţii de bază	Tipul subiectului = CA Limitarea lungimii lanţului de certificate = 1	CRITIC
CRL DistributionPoint	Punctul de distribuţie a listei certificatelor revocate	URL= http://www.pki. sis.md/ certmd.crl	
Authority Information Access	Accesul la informațiile 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
Regulamentul Centrului de certificare a cheilor publice

2. 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 decertificare OU = Subdiviziunea persoanei juridice O = Denumirea persoanei juridice, IDNOC = Codul statului	
Validity	Termenul de valabilitate a certificatului	Valabil de la: «_»_____20___oo:mm:ss GMT Valabil până la: «_»___20___oo:mm:ss GMT	
Subject	Datele de identificare ale utilizatorului semnăturii electronice, titular al certificatului	Serialnumber = IDNP a utilizatorului semnăturiielectronice CN = Numele, prenumele utilizatorului semnăturii electronice L = Localitatea de domiciliu a utilizatoruluisemnăturii electronice S = Statul OU = Subdiviziunea persoanei juridice, în careactivează 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 aemitentului certificatului	
Signature Value	Semnătura electronică a	Semnătura emitentului în conformitate cualgoritmul utilizat	

	emitentului certificatului		
Cîmpurile auxiliare			
Authority KeyIdentifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a centrului decertificare, 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 și poate fi

		Limitarea lungimii lanţului de certificate =lipseşte	CRITIC
CRL Distribution Point	Punctul de distribuţie a listei certificatelor revocate	Sursa publicării listei certificatelor revocate	
Authority Information Access	Accesul la informațiile despre centrul de certificare	Modalitatea de acces la informațiile 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 conține restricții cu privire la aplicarea acestui certificat.	

Anexa nr. 3
Regulamentul Centrului de certificare a cheilor publice

3. 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 aemitentului 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 actualizăria CRL	«_»_____20_oo:mm:ss GMT	
Revoked Certificates	Lista certificatelor revocate	userCertificate Numărul de serie a certificatului(CertificateSerialNumber) revocationDate Data revocării sau suspendării valabilității certificatului (Time)	
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii electronice aemitentului certificatului	
Signature Value	Semnătura electronică a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat	
Cîmpurile auxiliare			
Authority KeyIdentifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a centrului de certificare, care a fost utilizat pentru semnareaCRL	
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 valabilității	

Anexa nr. 4
Regulamentul Centrului de certificare a cheilor publice

Către "EUROPARC" SRL

Cererea **PENTRU CERTIFICAREA CHEII PUBLICE-PERSOANE FIZICE**

Datele Solicitantului:

Nume	
Prenume	
IDNP/IDNO (13 cifre)	
Email. de corespondență/user	
Telefon mobil	
Adresa de domiciliu (orașul, strada, bloc, nr. apartamentului)	

Data _____ Semnătura _____

Anexa 5

Către "EUROPARC" SRL

Cererea **PENTRU CERTIFICAREA CHEII PUBLICE-PERSOANE JURIDICE**

Datele Solicitantului:

Nume	
Prenume	
IDNP (13 cifre)	
Care activează în baza	
IDNO	
Denumirea Instituției	
Email. de corespondență/user	
Telefon mobil	
Adresa de domiciliu (orașul, strada, bloc, nr. apartamentului)	

Data _____ Semnătura _____

Anexa nr. 6
Regulamentul Centrului de certificare a cheilor publice

Cererea **PRIVIND MODIFICAREA STATUTULUI CERTIFICATULUI CHEII PUBLICE**

Se solicită Modificarea prin:
1) REVOCARE

2) SUSPENDARE de la _____ până la _____

3) RESTABILIRE

Datele Solicitantului:

Nume	
Prenume	
IDNP (13 cifre)	
Care activează în baza	
IDNO	
Denumirea Instituției	
Email. de corespondență/user	
Telefon mobil	
Adresa de domiciliu (orașul, strada, bloc, nr. apartamentului)	

Data _____ Semnătura _____

"EUROPARC" S.R.L.,
IDNO 1005600004639;
mun. Chişinău, Calea Iesilor, 10B

"EUROPARC" S.R.L.,
IDNO 1005600004639;
mun. Chişinău, Calea Iesilor, 10B