ORDINUL
DIRECTORULUI INSTITUȚIEI PUBLICE
SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ

ПРИКАЗ
ДИРЕКТОРА ПУБЛИЧНОГО УЧРЕЖДЕНИЯ СЛУЖБА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ

"20" februarie 2020 **Nr. 29** **mun. Chișinău**

Cu privire la aprobarea codului de practici și proceduri al centrului de certificare a cheilor publice

În vederea implementării prevederilor Legii nr.91 din 29 mai 2014, privind semnătura electronică și documentul electronic, în conformitate cu Hotărîrea Guvernului nr.1140 din 20 decembrie 2017 „Cu privire la activitatatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electrtonice", a Condițiilor speciale de activitate ale prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice, aprobate prin ordinal directorului Serviciului de Informații și Securitate al RM nr.70 din 15 iulie 2016, în temeiul punctului 26 subpct. 1) și 11) din Statutul Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică'':

ORDON:

1. A aproba, conform anexei, codul de practici și proceduri al centrului de certificare a cheilor publice.
2. Se abrogă subpct.1.1 din pct.1 a ordinului directorului Instituției nr. 50 din 01 august 2018 „Cu privire la aprobarea bazei normative a Centrului de certificare a cheilor publice" și ordinul directorului Instituției nr.98 din 03 decembrie 2018 „Cu privire la aprobarea codului de practici și proceduri al centrului de certificare a cheilor publice" .
3. Prezentul Ordin se aduce la cunoștința salariaților centrului de certificare a cheilor publice, salariaților secției vânzări și serviciului centrul de apel.
4. Controlul asupra executării prezentului Ordin mi-l asum personal.

Director **Serghei POPOVICI**

I.P. „SERVICIUL TEHNOLOGIA INFORMATIEI

SI SECURITATE CIBERNETICĂ"

Aprobat:
Prin ordinul Directorului
I.P. „Serviciul Tehnologia Informației
și Securitate Cibernetică"
nr. 29 din 20 februarie 2020

Clasificare de securitate:
C4 - PUBLIC

CODUL DE PRACTICI ŞI PROCEDURI
AL CENTRULUI DE CERTIFICARE A CHEILOR PUBLICE

Cod de referință: RG.0600.20

INFORMAȚIE DOCUMENT

Deținător	Centrul de certificare a cheilor publice
Data intrării în vigoare	20.02.2020
Versiune	3
Statut	APROBAT

FIŞA DE CONTROL A DOCUMENTULUI

ISTORIA MODIFICĂRILOR

Nr.	Versiune	Data	Autor	Comentarii modificare
1.	1.1	13.11.2013	Trifan Mariana	Versiune inițială.
2.	1.2	11.04.2014	Trifan Mariana	Adaptarea denumirii direcției tehnologii informaționale și servicii, din care face parte CC, și actualizarea listei persoanelor implicate.
3.	2.0	16.10.2016	Trifan Mariana	Ajustarea documentului conform RFC 3647 cu introducerea de noi secțiuni și a cap. 9.
4.	2.1	01.07.2018	Trifan Mariana	Ajustarea documentului ca urmare a reorganizării instituției.
5.	3.0	10.02.2020	Trifan Mariana	Completarea cap.7 cu tipurile de certificate, emise de Centrul de certificare a cheilor publice, adăugarea cap.10 Anexe.

DESTINATARII DOCUMENTULUI

Nr.	Organizație	Subdiviziuni / Funcții / roluri	Modalitate acces	Utilizare
1.	STISC	Secția resurse umane și documentare	Original, pe suport de hârtie	Păstrarea originalului în arhiva DNI.
2.	STISC	CC, secția centrul de apel, secția juridică, secția contabilitate	În formă electronică pe portalul intern.	Este interzisă copierea, tipărirea și distribuirea în orice formă a documentului.
3.	public	oricare persoană	În formă electronică pe site-ul www.stisc.gov.md	

Atenție! Conform Politicii de securitate a informației în cadrul IP STISC, sunteți autorizat să accesați acest document, doar în cazul în care faceți parte din lista Destinatarilor documentului mai sus. Accesarea neautorizată a acestui document este subiect al procesului disciplinar în cadrul Instituției.

PERSOANE IMPLICATE LA ELABORAREA DOCUMENTULUI

Nr.	Prenume, Nume	Organizație	Funcție	Responsabilitate	Semnătură
1.	Mariana Trifan	STISC	Administrator principal certificare, CC, DGTI	Elaborare	
2.	Ion Stati	STISC	Șef CC, DGTI	Coordonare	
3.	Gheorghe Pantaz	STISC	Șef DGTI	Coordonare	

CUPRINS

1. INTRODUCERE

Prezentul Cod de practici şi proceduri (în continuare *CPP* la cazul gramatical corespunzător) este elaborat în conformitate cu următoarele acte normative:

a) Legea nr.91 din 29 mai 2014 *privind semnătura electronică şi documentul electronic*,
b) Hotărârea Guvernului Nr.1140 din 20 decembrie 2017 *cu privire la activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice*,
c) Hotărârea Guvernului Nr. 1141 din 20 decembrie 2017 *pentru aprobarea Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcţionarii persoanelor juridice de drept public în cadrul circulaţiei electronice ale acestora*;
d) Hotărârea Guvernului Nr.414 din 08 mai 2018 *cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat*;
e) Normele tehnice în domeniul semnăturii electronice avansate calificate, aprobate prin Ordinul Serviciului de Informaţii şi Securitate nr. 69 din 15 iulie 2016,
f) Condiţiile speciale de activitate ale prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice, aprobate prin Ordinul Serviciului de Informaţii şi Securitate nr. 70 din 15 iulie 2016;
g) *Regulament privind procedura de acreditare a prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice*, aprobat prin Ordinul Serviciului de Informaţii şi Securitate nr. 70 din 15 iulie 2016,
h) Regulamentul privind procedura de avizare a dispozitivelor de creare şi/sau verificare a semnăturii electronice şi a produselor asociate semnăturii electronice, aprobat prin Ordinul Serviciului de Informaţii şi Securitate nr. 25 din 17 martie 2017,
i) *Regulamentul Prestatorului de servicii de certificare în domeniul aplicării semnăturii electronice avansate calificate*, aprobat prin Ordinul Serviciului de Informaţii şi Securitate nr. 70 din 15 iulie 2016,
j) *Regulamentul de soluţionare a situaţiilor litigioase în domeniul aplicării semnăturii electronice,* aprobat prin Ordinul Serviciului de Informaţii şi Securitate nr. 29 din 16 aprilie 2009,
k) recomandarea IETF (Internet Engineering Task Force) RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

1.1. REZUMAT

CPP stabileşte condiţiile generale de organizare a activităţii I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" (în continuare *Instituţie* sau *Prestator*) în calitate de prestator de servicii de certificare, şi determină:

- funcţiile, obligaţiile şi drepturile Prestatorului;
- procedurile şi mecanismele utilizate în procesul de prestare a serviciilor de certificare;
- obligaţiile utilizatorilor semnăturii electronice;
- modul de conlucrare cu reprezentanţii persoanelor juridice de drept public, de drept privat şi persoanele fizice (utilizatori ai semnăturii electronice avansate calificate, în continuare *utilizatori* la cazul gramatical);
- măsuri tehnico-organizatorice de bază pentru asigurarea securităţii;

- aplicarea CPP, inclusiv metodele de îmbunătăţire şi ordinea de introducere a modificărilor.

CPP se răsfrînge şi asupra:
- prestatorilor de servicii de certificare ce se află în relaţii comerciale cu Prestatorul;
- centrelor de înregistrări, cărora le-au fost delegate atribuţii;
- utilizatorilor semnăturii electronice.

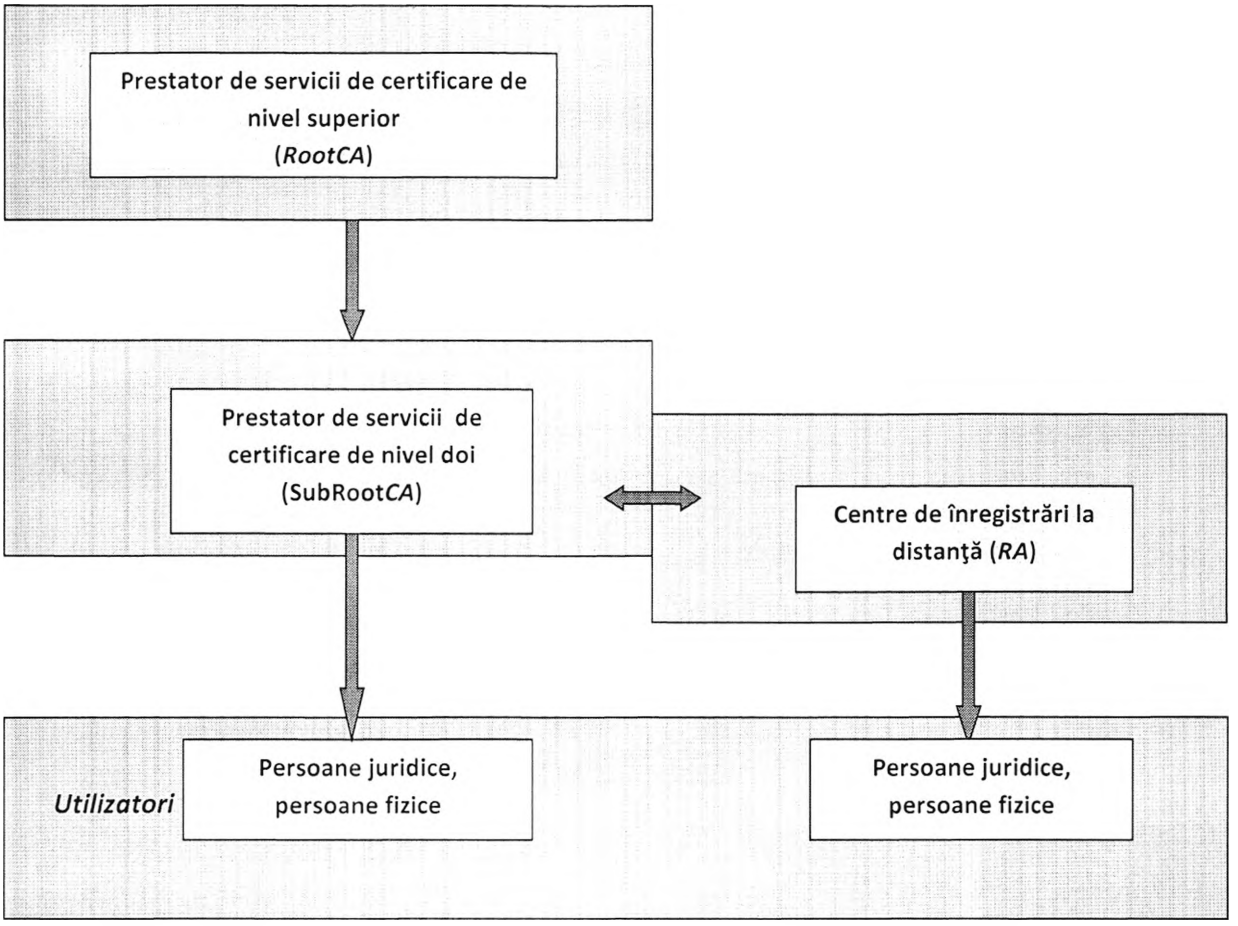
Infrastructura Prestatorului prevede 4 tipuri de certificate :
1. certificatele autorităţilor de certificare de nivel superior (RootCA),
2. certificatele autorităţilor de certificare de nivel doi (SubRootCA),
3. certificatele cheilor publice ale utilizatorilor semnăturii electronice şi
4. certificatele cheilor publice emise pentru sisteme informaţionale electronice ce urmează să interacţioneze cu serviciile electronice guvernamentale.

Infrastructura cheilor publice naţională este organizată în mod ierarhic.

În cazul semnăturii electronice avansată calificată/necalificată în vîrful ierarhiei se află prestatorul de servicii de certificare de nivel superior (RootCA) din cadrul Serviciului de Informaţii şi Securitate al RM, iar nivelul doi (SubRootCA) în această ierarhie îl ocupă prestatorul de servicii de certificare din cadrul I.P. „STISC".

În cazul certificatelor cheilor publice pentru autentificare şi servicii de securitate, al celor emise pentru sisteme informaţionale ce urmează a fi integrate cu serviciile electronice guvernamentale rolurile RootCA şi SubRootCA aparţin CC.

Reieşind din cele menţionate supra, avem următoarea schemă:



Prevederile prezentului CPP corespund cerinţelor din standardele unanim recunoscute, inclusiv ***AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework***, şi ale altor standarde din domeniul activităţii prestatorilor de servicii de certificare.

Structura acestuia corespunde standardului ***„Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework"***, cunoscut sub numele de **RFC 3647,** cu excepţia câtorva modificări în denumiri şi detalii ce corespund modelelor business ale Instituţiei. Corespunderea cu standardul dat simplifică dezvoltarea politicii de certificare, interacţiunea cu utilizatorii semnăturii electronice şi alţi prestatori de servicii de certificare.

NOTĂ: CPP presupune faptul că cititorul posedă cunoştinţe generale despre semnătura electronică şi infrastructura cheilor publice. În lipsa acestora, informaţie cu privire la criptografia cheii publice şi utilizarea infrastructurii cheilor publice se poate găsi pe site-ul www.stisc.gov.md.

1.2. DEFINIREA CODULUI DE PRACTICI ŞI PROCEDURI AL CENTRULUI DE CERTIFICARE A CHEILOR PUBLICE (DENUMIREA ŞI IDENTIFICAREA DOCUMENTULUI)

Prezentul CPP reprezintă un document de reglementare a activităţii Instituţiei în calitate de prestator de servicii de certificare.

CPP are denumiri în limbile de stat (**Codul de Practici şi Proceduri**), rusă (**Свод Правил и Процедур**) şi engleză (**Certification Practice Statement**).

Versiunile actualizate ale acestui document pot fi găsite după cum urmează:

- versiunea electronică -- în depozitul Prestatorului www.stisc.gov.md sau;
- versiunea pe suport de hârtie – la cerere, pe adresa Instituției (a se vedea Secţiunea 1.5).

1.3. PARTICIPANŢI AI INFRASTRUCTURII CHEILOR PUBLICE

1.3.1 AUTORITATEA DE CERTIFICARE (PRESTATORUL DE SERVICII DE CERTIFICARE)

1.3.1.1 *FUNCŢIILE PRESTATORULUI DE SERVICII DE CERTIFICARE*

Prestatorul îndeplinește următoarele funcţii:

a) certifică cheile publice ale utilizatorilor;

b) certifică cheile publice ale sistemelor informaționale ce urmează să interacționeze cu platformele guvernamentale;

c) suspendă şi restabilește valabilitatea, revocă certificatele cheilor publice emise;

d) întocmește şi gestionează Registrul certificatelor cheilor publice ale utilizatorilor (în continuare *Registru* la cazul gramatical corespunzător);

e) confirmă autenticitatea şi valabilitatea certificatelor cheilor publice ale titularilor certificatelor cheilor publice;

f) prestează şi alte servicii în domeniul semnăturii electronice (marcare temporală, actualizare a listei certificatelor revocate, de verificare a statutului certificatului cheii publice în regim de timp real, etc).

Pentru îndeplinirea funcţiilor sale, Prestatorul:

a) asigură crearea şi eliberarea certificatelor cheilor publice pe baza cererii depuse din partea utilizatorului în conformitate cu procedurile stabilite de prezentul CPP;

b) suspendă şi revocă certificatele cheilor publice ale utilizatorilor, precum şi restabilește valabilitatea certificatelor cheilor publice suspendate, în cazurile şi conform procedurilor stabilite de prezentul CPP;

c) gestionează Registrul certificatelor cheilor publice, asigură actualizarea acestuia şi accesul public la Registru;

d) conlucrează cu Prestatorul de servicii de certificare de nivel superior (în continuare *Prestator superior*) în cadrul infrastructurii cheilor publice;

e) acordă asistența metodică şi practică utilizatorilor;

f) creează sistemele informaționale şi de comunicaţii ale Prestatorului, asigură funcţionarea, securitatea, deservirea şi modernizarea lor, efectuează auditul intern permanent al securităţii şi funcționalității acestor sisteme.

1.3.1.2 *OBLIGAŢIILE PRESTATORULUI DE SERVICII DE CERTIFICARE*

Prestatorul este obligat:

a) să-şi desfăşoare activitatea în strictă conformitate cu legislația şi cerinţele stabilite de organul competent;

b) pe parcursul întregului termen de acreditare, să asigure respectarea cerinţelor în conformitate cu care a fost acreditat. În cazul apariţiei circumstanţelor care fac imposibilă asigurarea respectării

acestor cerinţe, prestatorul urmează să notifice organul competent despre acest fapt în decurs de 24 de ore;

c) să utilizeze dispozitivele de creare şi/sau de verificare a semnăturii şi produsele asociate semnăturii electronice ce deţin avizul organului competent;

d) să utilizeze dispozitivele de creare şi/sau de verificare a semnăturii şi produsele asociate semnăturii electronice în conformitate cu documentaţia de exploatare;

e) să organizeze regimul interior de funcţionare astfel încît să se excludă posibilitatea accesului persoanelor terţe la dispozitivele de creare şi/sau de verificare a semnăturii şi produsele asociate semnăturii electronice, la modificarea şi utilizarea lor neautorizată;

f) să genereze perechea de chei publică şi privată a Prestatorului (aferentă autorităţii de certificare);

g) să solicite certificarea cheii publice de către Prestatorul superior şi să creeze lista certificatelor revocate aferentă în conformitate cu cerinţele stabilite de organul competent şi de prezentul CPP;

h) să utilizeze cheia privată a CC numai la semnarea certificatelor cheilor publice eliberate de acesta şi a listelor certificatelor revocate;

i) să asigure securitatea cheilor private şi să creeze condiţiile necesare pentru excluderea accesului neautorizat la cheile private;

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

k) să solicite revocarea sau suspendarea imediată a valabilităţii certificatului cheii publice a CC în cazul în care are motiv să creadă că a fost încălcată confidenţialitatea cheii private, precum şi în cazul în care informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;

l) să primească cererile de certificare a cheilor publice de la utilizatori în conformitate cu procedurile stabilite de prezentul CPP;

m) să verifice autenticitatea datelor stipulate în cererea de certificare a cheii publice în baza documentelor ce confirmă aceste date, să asigure corespunderea informaţiilor din certificatul cheii publice cu informaţiile prezentate de către titularul certificatului cheii publice;

n) să asigure unicitatea informaţiei de înregistrare a utilizatorilor în Registrul certificatelor cheilor publice;

o) să nu divulge informaţiile cu accesibilitate limitată şi alte informaţii protejate de lege;

p) să verifice unicitatea cheilor publice certificate;

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

r) să creeze certificatul cheii publice a utilizatorilor conform cerinţelor stabilite de organul competent şi de prezentul CPP;

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

t) să elibereze certificatele cheilor publice utilizatorilor în conformitate cu procedurile stabilite de prezentul CPP;

u) să suspende şi să revoce certificatele cheilor publice, precum şi să restabilească valabilitatea certificatelor cheilor publice suspendate ale utilizatorilor în cazurile şi conform procedurilor stabilite de prezentul CPP;

v) să înscrie datele privind certificatul cheii publice revocat sau suspendat în lista certificatelor revocate în termen de trei ore lucrătoare, precizînd data, ora şi cauza revocării sau suspendării valabilităţii certificatului, efectuînd menţiunile respective în Registrul certificatelor cheilor publice;

w) să excludă din lista certificatelor revocate datele privind certificatul cheii publice suspendat în termen de trei ore lucrătoare din momentul restabilirii valabilităţii acestuia, efectuînd menţiunile respective în Registru:

x) să înştiinţeze utilizatorul despre suspendarea valabilităţii sau revocarea certificatului cheii publice, în cazurile şi conform procedurilor stabilite de prezentul CPP;

y) să înştiinţeze utilizatorul despre faptele de care a luat cunoştinţă Prestatorul sau Prestatorul superior şi care pot influenţa esenţial asupra posibilităţii utilizării ulterioare a certificatului cheii publice de către utilizator;

z) să înştiinţeze utilizatorul despre faptele care au devenit cunoscute Prestatorului şi care fac imposibilă utilizarea în continuare a cheii private, precum şi despre revocarea certificatului cheii publice, ce aparţine acestuia;

aa) să păstreze certificatul cheii publice a utilizatorului, precum şi alte informaţii despre acesta nu mai puţin de 15 ani de la data revocării sau expirării termenului de valabilitate a certificatului cheii publice;

bb) să asigure actualizarea Registrului şi posibilitatea accesului public la acesta, inclusiv în regimul timpului real, să întreprindă măsurile necesare pentru asigurarea securităţii Registrului;

cc) să pună la dispoziţia utilizatorilor datele din Registru privind certificatele cheilor publice revocate sau suspendate;

dd) să creeze şi să păstreze copia de rezervă a Registrului în conformitate cu cerinţele stabilite de organul competent;

ee) să asigure posibilitatea de stabilire cu exactitate a datei şi a orei eliberării, suspendării valabilităţii certificatului cheii publice sau revocării acestuia;

ff) să confirme autenticitatea şi valabilitatea certificatelor cheilor publice ale utilizatorilor la cererea acestora sau a organului competent;

gg) 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 şi să prezinte, pe suport de hîrtie, cererile de certificare a cheilor publice şi copiile actelor de identitate, iar electronic – certificatele cheilor publice incluse în Registru;

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

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

jj) să dispună de personal cu studii superioare în domeniul tehnologiei informaţiei şi/sau al securităţii informaţionale, cu nivel corespunzător de competenţe şi experienţă de gestionare şi expertizare în domeniul semnăturii electronice.

1.3.1.3 *DREPTURILE PRESTATORULUI DE SERVICII DE CERTIFICARE*

Prestatorul are dreptul:

a) doar în cazul apariţiei circumstanţelor care fac imposibilă conlucrarea cu prestatorul superior a persoanelor deja desemnaţi în procesul acreditării, să numească mai multe persoane-reprezentanţi ai Centrului de certificare a cheilor publice, responsabili de asigurarea colaborării cu Prestatorul superior în vederea obţinerii certificatelor cheilor publice pentru autorităţile de certificare, ale serviciilor de marcă temporală (TSP), ale serviciilor de verificare on-line a statutului certificatului (OCSP), revocarea acestora la necesitate, păstrarea în siguranţă a cheilor private corespunzătoare, cu informarea, în acest sens, a organului competent în raport cu modificările efectuate în decurs de 24 de ore,

b) să refuze eliberarea certificatului cheii publice solicitat de către utilizator, precizînd motivele refuzului, în următoarele cazuri:

- prezentarea în cererea de certificare a cheii publice a unor informaţii neveridice, ce nu corespund realităţii;
- încălcarea prevederilor legislaţiei în domeniul aplicării semnăturii electronice;
- încălcarea drepturilor unor terţi în procesul de întocmire sau de depunere a cererii de certificare a cheii publice;

c) să confirme autenticitatea şi valabilitatea certificatelor cheilor publice ale titularilor certificatelor cheilor publice;

d) să suspende valabilitatea sau să revoce certificatul cheii publice în cazurile şi în modul prevăzute de cadrul normativ şi de prezentul CPP.

1.3.2 AUTORITATEA DE ÎNREGISTRĂRI (RA)

Prestatorul oferă posibilitatea de a crea Autoritatea/Centru de înregistrări la distanţă, reprezentanţă a acestuia în interacţiunea cu utilizatorii.

Centrul de înregistrări activează în bază de contract şi regulament privind funcţionarea centrului de înregistrări. Crearea sau încetarea activităţii centrului de înregistrări, precum şi aprobarea regulamentului de funcţionare a acestuia, se efectuează doar după dispunerea avizului pozitiv de către organul competent, dacă actele normative nu prevăd altfel.

În Centrul de înregistrări au loc următoarele proceduri:

- identificarea şi înregistrarea solicitantului pentru certificarea cheii publice;
- recepţionarea şi prelucrarea cererilor de certificare a cheii publice, suspendare/restabilire a valabilităţii şi revocare a certificatului cheii publice;
- iniţierea procedurilor de certificare a cheii publice, suspendare/restabilire a valabilităţii şi revocare a certificatului cheii publice.

Orice persoană juridică poate fi Centru de înregistrări cu condiţia executării tuturor cerinţelor înaintate de Prestator şi fără încălcarea prevederilor cadrului normativ în domeniu.

Centrul de înregistrări la distanţă nu are dreptul de a deschide alte centre de înregistrări, nici de a delega funcţiile sale altei persoane juridice fără acordul în scris al Prestatorului.

Centrul de înregistrări la distanţă interacţionează doar cu solicitanţii pentru certificarea cheilor publice (persoanele de drept privat şi persoanele fizice). Persoanele juridice de drept public sunt deservite doar de către autoritatea de înregistrare din cadrul Instituţiei.

1.3.3 UTILIZATORI

În condiţiile cadrului normativ Instituţia prestează servicii oricărui tip de utilizatori ai semnăturii electronice (a se vedea mai jos).

Tipul certificatului	Eliberat	Serviciul pentru care se eliberează certificatul	Utilizatori
Certificatul cheii publice	Persoanei fizice	Corporativ	Colaboratorii Instituţiei, administratorii centrelor de înregistrări la distanţă
	Persoanei fizice	Vînzare	Orice utilizator al semnăturii electronice (angajaţi ai persoanelor juridice, cetăţeni)

Certificatul cheii publice pentru un sistem informațional	Persoanei juridice	Interacțiunea cu serviciile electronice guvernamentale	Administratorii sistemelor informaționale
Certificat SSL	Domenului ce aparține persoanei juridice, persoanei fizice	Securizarea tranzacțiilor	Persoană juridică, persoana fizică

1.3.3.1 *OBLIGAȚIILE TITULARILOR CERTIFICATELOR CHEILOR PUBLICE*

Titularul este obligat:

a) să asigure condiţiile necesare pentru excluderea accesului unei alte persoane la cheia sa privată;

b) să nu utilizeze cheia privată pentru crearea semnăturii electronice dacă are motive să presupună că este încălcată confidenţialitatea cheii private;

c) să solicite imediat suspendarea valabilităţii certificatului cheii publice sau revocarea acestuia în cazul în care:

– a pierdut cheia privată;

– are motive să creadă că a fost încălcată confidenţialitatea cheii private;

– informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;

d) să înştiinţeze Prestatorul, în decurs de 24 de ore, despre orice modificare a informaţiilor cuprinse în certificatul cheii publice;

e) să îndeplinească alte obligaţii prevăzute de cadrul normativ în domeniul semnăturii electronice şi de contractul/acordul încheiat cu Prestatorul.

1.3.3.2 *DREPTURILE TITULARILOR CERTIFICATELOR CHEILOR PUBLICE*

În cadrul interacțiunii cu Prestatorul titularul are dreptul:

a) să obțină lista certificatelor revocate;

b) să obțină accesul la Registru;

c) să aplice lista certificatelor revocate pentru verificarea valabilității certificatelor cheilor publice ale utilizatorilor;

d) să se adreseze către Prestator pentru confirmarea autenticității şi valabilității certificatelor cheilor publice ale acestuia şi ale utilizatorilor.

1.3.4 PĂRȚI DE ÎNCREDERE

Partea de încredere, ce foloseşte serviciile Prestatorului, poate fi reprezentată de orice persoană.

Aceasta este responsabilă de verificarea statutului certificatului cheii publice, de verificarea semnăturii electronice în scop de identificare a sursei sau autorului mesajului.

1.3.5 ALȚI PARTICIPANȚI

Nu se aplică.

1.4. APLICABILITATE

1.4.1 APLICABILITATEA CERTIFICATULUI CHEII PUBLICE

Certificatele cheilor publice, emise de Prestator, permit părţilor terţe de încredere, participanţilor în procesul de comunicare electronică să verifice semnăturile electronice ale titularilor. Semnătura electronică sau orice tranzacţie, pe care a fost aplicată semnătura electronică prin utilizarea certificatului cheii publice emis de Prestator, va fi considerată validă, indiferent de locul unde a fost eliberat certificatul cheii publice sau a fost creată/utilizată semnătura electronică şi indiferent de locul unde utilizatorul îşi desfăşoară activitatea, cu condiţia respectării cadrului normativ.

Domeniul de aplicabilitate a certificatelor cheilor publice se determină de două elemente:

- aplicarea certificatului cheii publice (conform restricţiilor menţionate în acesta);
- aplicaţiile ce permit sau interzic utilizarea certificatului cheii publice.

Certificatele cheilor publice, emise de Prestator, pot fi utilizate în aplicaţii, ce deţin avizul pozitiv al organului competent.

1.4.2 RESTRICŢII DE APLICABILITATE A CERTIFICATELOR CHEILOR PUBLICE

Utilizarea certificatelor cheilor publice, emise de Prestator, nu este limitată la un anumit mediu, iar decizia, în raport cu domeniul de aplicare, aparţine titularului. Cu toate acestea, Prestatorul sau alţi participanţi la infrastructura cheilor publice nu poartă răspundere pentru monitorizarea sau stabilirea cărorva restricţii de aplicabilitate a certificatului cheii publice utilizatorului.

Unele certificate ale cheilor publice, emise de Prestator, au restricţii de utilizare. Certificatele cheilor publice ale Prestatorului nu pot fi utilizate decât pentru semnarea certificatelor cheilor publice ale utilizatorilor, a listei certificatelor revocate. Certificatele cheilor publice ale utilizatorilor se supun aplicaţiilor clienţilor şi nu sunt utilizate drept certificate pentru servicii.

În ce priveşte certificatele cheilor publice, emise de CC, ce corespund ***Normelor tehnice în domeniul semnăturii electronice avansate calificate*** (în continuare *Norme tehnice* la cazul gramatical corespunzător) şi recomandării **X.509 v3** ***The Directory: Public-key and attribute certificate framework***, utilizarea acestora este restricţionată de obiectivele urmărite de titular şi constrîngerile cu caracter tehnic a produselor asociate semnăturii electronice. Alte restricţii de aplicabilitate a certificatelor cheilor publice sunt determinate de însuşi utilizatori.

Certificatele cheilor publice se utilizează doar conform câmpurilor, stabilite la crearea lor, şi în conformitate cu cadrul normativ.

1.5. ADMINISTRAREA CODULUI DE PRACTICI ŞI PROCEDURI AL CENTRULUI DE CERTIFICARE A CHEILOR PUBLICE

1.5.1 INSTITUŢIA ADMINISTRATOARE

Instituţia este persoana juridică responsabilă pentru elaborarea, aplicarea şi modificarea ulterioară a CPP.

1.5.2 DATE DE CONTACT

Întrebări cu privire la prezentul CPP pot fi adresate la următoarea adresă:
I.P. "Serviciul Tehnologia Informației și Securitate Cibernetică"
Republica Moldova,
or. Chișinău,
Piața Marii Adunări Naționale, 1,
MD – 2033,
Telefon/fax: (+373) 22 250522
E-mail: pki@stisc.gov.md

1.5.3 PERSOANA CARE DETERMINĂ CORESPUNDEREA POLITICII DE CERTIFICARE CU CODUL DE PRACTICI ŞI PROCEDURI AL CENTRULUI DE CERTIFICARE A CHEILOR PUBLICE

Prestatorul este responsabil de a determina corespunderea politicii de certificare cu CPP.

1.5.4 PROCEDURA DE APROBARE A CODULUI DE PRACTICI ŞI PROCEDURI AL CENTRULUI DE CERTIFICARE A CHEILOR PUBLICE

Prezentul CPP este aprobat intern și publicat în formă electronică în Depozitul Prestatorului.

Modificarea prevederilor acestui CPP este rezultatul depistării erorilor, al actualizării sau al propunerilor parvenite de la utilizatorii semnăturii electronice. Propunerile cu privire la modificările CPP se primesc prin poșta electronică sau pe adresa instituției.

După fiecare modificare, introdusă în CPP, se schimbă versiunea documentului.

Modificările se fac de Prestator sub formă de documente ce conțin acele modificări sau actualizări.

Centrul de certificare își asumă dreptul de a introduce modificări în prezentul CPP fără notificarea utilizatorilor semnăturii electronice în compartimentele ce țin de greșeli de redactare, schimbarea URL-ului și a datelor de contact.

Prestatorul va introduce modificări în prezentul CPP cu notificarea persoanelor interesate.

Modificări esențiale, însoțite de notificări, sunt cele ce schimbă esența prevederilor prezentului CPP și sunt determinate de Prestator.

Toate actualizările și completările propuse în prezentul CPP pot fi solicitate prin scrisoare la adresa Instituției.

Prestatorul este deschis observațiilor utilizatorilor semnăturii electronice asupra CPP și, în caz că acestea sunt acceptabile, vor trece procedura de aprobare în conformitate cu secțiunea dată.

În cazuri excepționale, dacă Prestatorul consideră că modificările au un caracter urgent, în scop de prevenire sau de stopare a încălcării securității infrastructurii cheii publice, acesta are dreptul de a formula astfel de modificări, publicându-le în Depozitul Prestatorului.

Termenul pentru depunerea obiecțiilor și comentariilor cu privire la modificările propuse ale prevederilor prezentului CPP este de cincisprezece (15) zile din momentul publicării lor pe site-ul Prestatorului.

Vor fi luate în considerație toate obiecțiile și comentariile și:

- modificările propuse vor intra în vigoare fără rectificări,

- modificările vor fi supuse rectificărilor şi vor fi republicate ca rectificări noi, în conformitate cu prezenta secţiune,
- modificările propuse vor fi şterse.

Modificările propuse, cu excepţia celor şterse, intră în vigoare din momentul expirării termenului pentru depunerea obiecţiilor şi comentariilor.

Aprobarea CPP este o procedură internă a Instituţiei şi are loc conform regulilor stabilite în cadrul acesteia.

1.6. DEFINIŢII ŞI ABREVIERI

1.6.1 DEFINIŢII

Titular/utilizator (eng. End User) – persoana fizică pe numele căreia Prestatorul a eliberat certificatul cheii publice şi care deţine cheia privată corespunzătoare, ce permite crearea semnăturii electronice (identificatorul acestei persoane se conţine în cîmpul *Subject* al certificatului cheii publice),

Centrul de certificare a cheilor publice – subdiviziune din cadrul Direcţiei Generale Tehnologii Informaţionale, I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică",

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

prestator de servicii de certificare (*prestator*) - persoana juridică I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" ce prestează servicii de certificare,

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

partea de încredere – persoana fizică/juridică ce utilizează datele de verificare a semnăturii electronice,

persoana juridică – persoana juridică de drept public sau privat.

1.6.2 ABREVIERI

CPP – codul de practici şi proceduri,
CC – centrul de certificare a cheilor publice,
CRL – lista certificatelor revocate (Certificate Revocation List),
DGTI - Direcţia generală tehnologii informaţionale,
DJRU – Direcţia juridică şi resurse umane,
OCSP - Online Certificate Status Protocol,
PKI – infrastructura cheilor publice,
TSA – autoritate de marcare temporală (Time-Stamping Authority).

2. DEPOZITUL ŞI PUBLICAREA

2.1. DEPOZITUL PRESTATORULUI DE SERVICII DE CERTIFICARE

Depozitul Prestatorului este sursa informaţională de bază a acestuia şi reprezintă totalitatea datelor, accesibile public, sub formă de documente pe suport de hârtie şi documente electronice.

În Depozit sunt stocate Registrul, listele certificatelor revocate şi actele normative în domeniul semnăturii electronice, inclusiv baza normativă internă cu clasa de securitate corespunzătoare.

2.2. PUBLICAREA INFORMAŢIEI

Depozitul Prestatorului este o interfaţă publică ce conţine următoarea informaţie:

- versiunile actuale ale *Regulamentului prestatorului de servicii de certificare I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”*, ale *Codului de practici şi proceduri al Centrului de certificare a cheilor publice*, ale *Politicilor de certificare*, alte documente din domeniul semnăturii electronice;
- contracte-tip şi anexe, ce urmează a fi semnate cu utilizatorii semnăturii electronice;
- declaraţia cu privire la confidenţialitatea informaţiei primite şi prelucrate;
- lista centrelor de înregistrări împuternicite;
- Registrul în care se conţin:
  - certificatele cheilor publice ale autorităţilor de certificare;
  - listele certificatelor revocate;
- altă informaţie ce se modifică în timp real.

Cu conţinutul Depozitului a se lua cunoştinţă pe www.stisc.gov.md.

2.3. FRECVENŢA DE PUBLICARE

Informaţia, publicată în Depozitul Prestatorului, se actualizează în următorul mod:

- *Politicile de certificare*, *Codul de practici şi proceduri al Centrului de certificare a cheilor publice*, *Regulamentul prestatorului de servicii de certificare I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”*, alte documente interne – la introducerea modificărilor în caz de depistare a erorilor, modificare a standardelor corespunzătoare sau la propunerile utilizatorilor;
- certificatele cheilor publice ale Prestatorului – după primirea noilor certificate ale cheilor publice;
- certificatele cheilor publice ale titularilor – după eliberarea noului certificat în baza acordului în scris al titularului;
- lista certificatelor revocate – a se vedea pct. 4.9.7;
- informaţie suplimentară – la fiecare completare.

2.4. CONTROLUL ACCESULUI LA DEPOZIT

Informaţia, publicată în Depozitul Prestatorului, este informaţie publică. Instituţia a implementat măsuri de securitate fizică şi logică pentru a preveni adăugarea, ştergerea sau schimbarea informaţiei publicate în Depozit.

Nu se publică informaţia cu privire la rezultatele auditelor, ale controalelor în domeniul semnăturii electronice, informaţia confidenţială şi cea care ţine de secretul comercial.

3. IDENTIFICAREA ŞI AUTENTIFICAREA

3.1. NUME

3.1.1 TIPURI DE NUME

Certificatele cheilor publice, emise de Prestator, corespund cerinţelor standardului **ITU-T X.509, versiunea 3**, standardului **SMV ISO CEI 9594-8:2007** ***Information technology. Open Systems Interconnection. The Directory: Public-key and attribute certificate frameworks*** sau **IETF RFC 5280** ***Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile***.

Certificatele cheilor publice, emise de Prestator, conţin, în conformitate cu Recomandarea ITU-T X.501| ISO/IEC 9594-2, nume caracteristice în câmpurile emitentului şi subiectului.

Structurile certificatelor cheilor publice ale Prestatorului şi ale utilizatorilor semnăturii electronice sunt prezentate în cap. 10 al CPP.

3.1.2 NUMELE CARACTERISTICE

Numele ce se conţin în certificatele cheilor publice, emise de Prestator utilizatorilor, trebuie să fie cu sens şi să identifice persoana fizică drept subiect de certificare. Nu se acceptă utilizarea pseudonimelor.

Numele „distinguished name" (**DN**) constă din câmpuri obligatorii ce corespund Normelor tehnice, recomandărilor **RFC 5280** ***Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*** şi **X.520** ***The Directory: Selected attribute types***.

Numele, utilizate pentru crearea înscrierilor **DN** în certificatele cheilor publice ale utilizatorilor, se scriu în grafia latină cu utilizarea simbolurilor diacritice.

În cazul utilizatorilor din cadrul persoanelor juridice **DN** constă din următoarele câmpuri:

a) câmpul **SerialNumber** – IDNP-ul utilizatorului;
b) câmpul **CN** – numele, prenumele utilizatorului;
c) câmpul **L** – localitatea (în care este înregistrată persoana juridică);
d) câmpul **S** – statul;
e) câmpul **OU** – subdiviziunea persoanei juridice în care activează utilizatorul;
f) câmpul **O** – denumirea, IDNO-ul persoanei juridice, în care activează utilizatorul;
g) câmpul **Phone** – numărul de telefon al utilizatorului;
h) câmpul **T** – funcţia utilizatorului;
i) câmpul **C** – codul internaţional al statului (pentru Republica Moldova acesta este **MD**);
j) câmpul **E** – adresa de e-mail a utilizatorului;
k) câmpul **STREET** – adresa juridică a persoanei juridice.

NOTĂ: în anumite cazuri unele câmpuri din cele sus-menţionate pot lipsi. Acest fapt este coordonat cu organul competent.

În cazul persoanelor fizice **DN** constă din următoarele câmpuri:

a) câmpul **SerialNumber** – IDNP-ul utilizatorului;
b) câmpul **CN** – numele, prenumele utilizatorului;

c) câmpul **L** – localitatea de domiciliu;
d) câmpul **S** – statul;
e) câmpul **Phone** – numărul de telefon al utilizatorului;
f) câmpul **C** – codul internaţional al statului (pentru Republica Moldova acesta este **MD**);
g) câmpul **E** – adresa de e-mail a utilizatorului.

Datele indicate de utilizator sunt verificate şi identificate de administratorul de înregistrări. Prestatorul garantează unicitatea numelor în cadrul domenului său.

3.1.3 ANONIMATUL SAU PSEUDONIMELE UTILIZATORILOR

Anonimatul şi pseudonimele utilizatorilor nu se aplică.

3.1.4 REGULILE DE INTERPRETARE A DIFERITOR FORME DE NUME

Interpretarea diferitor forme de nume ale certificatelor cheilor publice se bazează pe profilurile certificatelor, expuse în cap. 7 al prezentului CPP. Pentru crearea şi interpretarea **DN** se folosesc recomandările expuse în pct. 3.1.2.

3.1.5 UNICITATEA NUMELOR

În scopul identificării utilizatorului certificatele cheilor publice, emise de Prestator, sunt distincte în conformitate cu **DN.**

Prestatorul asigură unicitatea certificatului utilizatorului în cadrul domenului Prestatorului prin intermediul unicităţii numărului de serie al fiecărui certificat şi a unicităţii codului numeric personal **IDNP** (după caz).

3.1.6 RECUNOAŞTEREA ŞI ROLUL MĂRCILOR COMERCIALE

Centrul de certificare posedă marca sa comercială înregistrată, ce constă din imaginea grafică şi inscripţie:

M LD SIGN

Imaginea grafică şi inscripţia reprezintă mărci comerciale înregistrate ale Instituţiei şi nu pot fi utilizate de nimeni fără permisiunea în scris a acesteia.

Marca comercială a Centrului de certificare este un element suplimentar al logotipului pentru fiecare Centru de înregistrări, ce intră în componenţa domenului Centrului de certificare; dreptul de utilizare a acestui logotip este permis automat noului Centru de înregistrări.

3.2. ÎNREGISTRAREA

Înregistrarea utilizatorului are loc în conformitate cu prevederile *Instrucţiunii de serviciu a administratorului înregistrare* şi presupune un şir de proceduri pentru colectarea datelor veridice necesare la identificarea persoanei utilizatorului.

Fiecare solicitant este supus procedurii de înregistrare. După verificarea datelor pentru certificare, prezentate de către solicitant, acesta este inclus în lista utilizatorilor Prestatorului.

Ținînd cont de faptul că Prestatorul furnizează produse și servicii de certificare în care verificarea informațiilor prezentate este obligatorie pentru a desfășura activitățile conform cadrului normativ în domeniul semnăturii electronice, Prestatorul verifică toate informațiile necesare emiterii certificatului.

Depunerea pachetului de documente pentru certificarea cheii publice este anticipată de executarea paşilor de pe portalul serviciilor electronice a Prestatorului.

3.2.1 DOVADA POSESIEI CHEII PRIVATE

Nu se aplică.

3.2.2 IDENTIFICAREA PERSOANELOR JURIDICE DE DREPT PUBLIC/PRIVAT

Identificarea persoanei juridice are drept scop:

- dovada că la momentul depunerii cererii de certificare a cheii publice persoana juridică, menţionată în cerere, există;
- dovada că solicitantul pentru certificarea cheii publice este persoană responsabilă din cadrul persoanei juridice menţionate.

Identificarea persoanei juridice are loc în prezenţa persoanei responsabile din cadrul acesteia în faţa administratorului de înregistrări. Pachetul de documente depus în acest scop are următorul conţinut:

- copia extrasului din Registrul de Stat al persoanelor juridice,
- copia actului ce confirmă identitatea persoanei responsabile (emis de o autoritate de încredere şi recunoscut pe teritoriul Republicii Moldova).

Administratorul de înregistrări identifică persoana juridică conform prevederilor *Instrucţiunii de serviciu a administratorului înregistrare*.

3.2.3 IDENTIFICAREA PERSOANELOR FIZICE

Identificarea persoanelor fizice are drept scop:

- dovada că informaţia, prezentată în cererea de certificare, se referă la persoana fizică în cauză;
- dovada că solicitantul pentru certificarea cheii publice este o persoană fizică, identificată în cerere.

Identificarea persoanelor fizice are la bază actele ce o identifică. Procedura de identificare, desfăşurată de administratorul de înregistrări, constă în:

- verificarea autenticităţii actelor prezentate de solicitant;
- verificarea autenticităţii cererii:
  - verificarea corespunderii datelor indicate în cerere cu cele din acte;
  - verificarea corespunderii numelui distinctiv.

Administratorul de înregistrări identifică persoana fizică conform prevederilor *Instrucţiunii de serviciu a administratorului înregistrare*.

3.2.4 IDENTIFICAREA ECHIPAMENTULUI

Identificarea echipamentului are loc similar procedurii de identificare a persoanei juridice.

3.2.5 INFORMAȚII NEVERIFICATE

Ținînd cont de faptul că Prestatorul furnizează produse și servicii de certificare în care verificarea informațiilor prezentate de către uilizator este obligatorie pentru a desfășura activitățile conform cadrului normativ în domeniul semnăturii electronice, Prestatorul verifică toate informațiile necesare emiterii fiecărui tip de certificat.

3.2.6 IDENTIFICAREA AUTORIZAȚIILOR

Atît Prestatorul, cît și Centrele de Înregistrări pot identifica autorizarea unei persoane fizice privind acționarea acesteia în numele pesoanei juridice sau a altei persoane fizice. Acest proces face parte din procedura de identificare a persoanei juridice/fizice.

3.2.7 CRITERII PENTRU INTEROPERARE

Nu se aplică.

3.3. IDENTIFICAREA ȘI AUTENTIFICAREA LA SOLICITAREA CERTIFICĂRII NOII PERECHI DE CHEI

Autentificarea identității utilizatorului care depune cererea pentru certificarea noii perechi de chei sau pentru modificarea cărorva date din certificatul cheii publice valid are loc conform prevederilor *Instrucțiunii de serviciu a administratorului înregistrare*.

3.3.1 IDENTIFICAREA ȘI AUTENTIFICAREA LA CERTIFICAREA NOII PERECHI DE CHEI ÎN CAZUL EXPIRĂRII PERIOADEI DE VALABILITATE A CERTIFICATULUI CHEII PUBLICE

Procedura de certificare a noii perechi de chei pentru utilizatorii, ale căror certificate valide expiră, are loc în momentul depunerii cererii de certificare a cheii publice cu cel puțin 30 zile (recomandat) pînă la expirarea perioadei de valabilitate.

Certificatul, emis de Prestator pentru noua pereche de chei, conține aceiași parametri ca și cel a cărui perioadă de valabilitate expiră, cu excepția numărului de serie, a perechii de chei și a perioadei de valabilitate a certificatului.

Titularii certificatelor cheilor publice emise de Prestator, care depun cererile de certificare a noilor perechi de chei sub formă de document electronic, sunt identificați în baza semnăturii electronice și a certificatului cheii publice valid.

3.3.2 IDENTIFICAREA ŞI AUTENTIFICAREA ÎN CAZUL INTRODUCERII MODIFICĂRILOR ÎN CERTIFICATUL CHEII PUBLICE VALID

Modificări în certificatul cheii publice valid al utilizatorului se fac în cazul necesităţii modificării măcar a unui câmp (e.g., la schimbarea funcţiei utilizatorului, a informaţiei de contact, a adresei electronice, a adresei juridice, a numelui la căsătorie, divorţ, etc.).

La fel se modifică perechea de chei certificată şi numărul de serie al certificatului cheii publice. Autentificarea titularului are loc în baza pachetului de documente depus anterior, iar introducerea modificărilor – în baza documentului ce atestă modificarea datelor. Procedura de identificare este similară celei descrise în Secţiunea 3.2 din CPP.

3.3.3 IDENTIFICAREA ŞI AUTENTIFICAREA ÎN CAZUL CERTIFICĂRII PERECHII NOI DE CHEI DUPĂ REVOCAREA CERTIFICATULUI CHEII PUBLICE

La schimbarea certificatelor cheilor publice revocate identificarea şi autentificarea au loc conform procedurilor respective la înregistrarea iniţială a utilizatorului (a se vedea Secţiunea 3.2 a CPP).

3.4. IDENTIFICAREA ŞI AUTENTIFICAREA LA DEPUNEREA CERERII DE REVOCARE A CERTIFICATULUI CHEII PUBLICE

În cazurile prevăzute de actele normative în domeniul semnăturii electronice privind revocarea certificatului cheii publice titularul este obligat, în modul stabilit de CPP, să solicite de la Prestator revocarea certificatului cheii publice (a se vedea Secţiunea 4.9 *Revocarea şi suspendarea valabilităţii certificatului cheii publice*).

Cererea de revocare se depune ca document pe suport de hârtie, semnată olograf de către titular şi/sau de către angajatorul acestuia sau ca document electronic (dacă este posibil).

În cazul persoanei fizice identitatea titularului se stabileşte prin propria prezenţă în faţa administratorului de înregistrări în baza buletinului de identitate, iar în cazul persoanei juridice – în baza documentelor parvenite din partea acesteia.

4. CERINŢE FAŢĂ DE GESTIONAREA CICLULUI DE VIAŢĂ AL CERTIFICATULUI CHEII PUBLICE

Ciclul de viaţa al certificatului cheii publice cuprinde înregistrarea, identificarea şi autentificarea solicitantului, emiterea certificatului cheii publice şi, după caz, suspendarea şi restabilirea validităţii certificatului cheii publice, dar şi revocarea certificatului cheii publice.

Fiecare procedură începe cu pregătirea pachetului de documente pentru prestarea unui anumit serviciu, stabilit de Prestator, şi depunerea acestuia de către solicitant la centrul de înregistrări sau direct la Prestator.

4.1. PACHETUL DE DOCUMENTE AFERENT CERTIFICĂRII CHEII PUBLICE

Pentru certificarea cheii publice a utilizatorului sunt prezentate următoarele documente şi informaţii, după caz:

A. Persoana juridică de drept public, angajaţii căreia sunt subiecţi ai declarării averii şi intereselor personale

Prestarea serviciilor de certificare a cheilor publice subiecţilor declarării averii şi intereselor personale are loc în conformitate cu prevederile *Regulamentului cu privire la modul de prestare a serviciilor de certificare a cheilor publice subiecţilor declarării averii şi intereselor personale.*

B. Persoana juridică de drept public, angajaţii căreia sunt utilizatori ai Sistemului informaţional automatizat „Asistenţa medicală primară"

Prestarea serviciilor de certificare a cheilor publice utilizatorilor SIA „Asistenţa medicală primară" are loc în conformitate cu prevederile *Regulamentului cu privire la modul de prestare a serviciilor de certificare a cheilor publice utilizatorilor Sistemului informaţional automatizat „Asistenţa medicală primară".*

C. Persoana juridică de drept public, angajaţii căreia nu sunt subiecţi ai declarării averii şi intereselor personale sau utilizatori ai Sistemului informaţional automatizat „Asistenţa medicală primară"

Prestarea serviciilor de certificare a cheilor publice angajaţilor din cadrul persoanelor juridice de drept public care nu sunt subiecţi ai declarării averii şi intereselor personale are loc în conformitate cu prevederile *Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcţionarii persoanelor juridice de drept public în cadrul circulaţiei electronice ale acestora*, aprobat prin HG 1141/2017, şi în baza următoarelor documente:

a) contractul de prestări servicii, semnat olograf de către conducător sau o persoană cu funcţie de răspundere şi ştampilat;
b) cererea ce conţine lista persoanelor pentru care se solicită prestarea serviciilor de certificare, semnată olograf de către conducător sau o persoană cu funcţie de răspundere (conform Anexei nr. 1A) şi ştampilată;

c) cererea de certificare a cheii publice, pentru persoana căreia i se solicită prestarea serviciilor de certificare, semnată olograf de către aceasta şi datată, conform Anexei nr. 2A;
d) copia lizibilă a actului de identitate, valabil la data solicitării, pentru fiecare persoană căreia i se solicită prestarea serviciilor de certificare;
e) copia lizibilă a extrasului din Registrul de Stat al unităților de drept cu mențiunea "*Confirm că datele înscrise sunt veridice și actuale*", datată și semnată olograf de către conducător sau o persoană cu funcție de răspundere;
f) dispozitivul securizat de creare a semnăturii electronice, după caz.

D. Persoana juridică de drept privat

a) contractul de prestări servicii, semnat olograf de către conducător sau o persoană cu funcție de răspundere;
b) cererea ce conține lista persoanelor pentru care se solicită prestarea serviciilor de certificare, semnată olograf de către conducător sau o persoană cu funcție de răspundere (conform Anexei nr. 1A);
c) cererea de certificare a cheii publice, pentru persoana căreia i se solicită prestarea serviciilor de certificare, semnată olograf de către aceasta și datată, conform Anexei nr. 2A;
d) copia lizibilă a actului de identitate, valabil la data solicitării, pentru fiecare persoană căreia i se solicită prestarea serviciilor de certificare;
e) copia lizibilă a extrasului din Registrul de Stat al unităților de drept cu mențiunea "*Confirm că datele înscrise sunt veridice și actuale*", datată și semnată olograf de către conducător sau o persoană cu funcție de răspundere;
f) dispozitivul securizat de creare a semnăturii electronice, după caz.

E. Persoana fizică

a) contractul de prestări servicii, semnată olograf de către persoana fizică;
b) cererea de certificare a cheii publice sub formă de document pe suport de hîrtie, semnată olograf (conform Anexei nr. 2B);
c) copia actului de identitate valabil la data solicitării;
d) în cazul delegării împuternicirilor se prezintă şi copia procurii autentificată notarial, eliberată pe numele persoanei cu drept de reprezentare, împreună cu copia lizibilă a actului de identitate, valabil la data solicitării,
e) dispozitivul securizat de creare a semnăturii electronice, după caz.

F. Sistemul informațional electronic

a) cererea pentru care se solicită prestarea serviciilor de certificare, semnată olograf de către conducător sau o persoană cu funcție de răspundere (conform Anexei nr. 1B) și ștampilată, după caz.
În coloana nume domen se înscrie: ***numesisteminformational.numeinstitutie.pki.gov.md***
b) cererea de certificare a cheii publice, semnată olograf de către persoana responsabilă (menționată în cererea de la lit. a), conform Anexei nr. 2A;
c) copia Extrasului din Registrul de stat al unităților de drept.

NOTĂ: în cazul depunerii pachetului de documente în format electronic, pe **fiecare document** în format electronic trebuie aplicată semnătura electronică avansată calificată de către persoanele respective în conformitate cu prevederile cadrului normativ în domeniul semnăturii electronice.

IMPORTANT!!! Nu se acceptă depunerea pachetului de documente parţial în format electronic, parţial pe suport de hîrtie.

Pachetul de documente se generează urmînd paşii de pe portalul serviciilor electronice STISC şi este depus la Prestator.

Cererea de certificare a cheii publice este semnată de către persoana menţionată în ea şi trebuie să conţină:

a) numele şi prenumele utilizatorului, IDNP, numărul documentului ce atestă identitatea;
b) informaţie de contact (numărul de telefon, adresa poştală, adresa poştei electronice);
c) denumirea persoanei juridice, al cărei angajat este, IDNO, funcţia deţinută (după caz);
d) alte date de identificare ale persoanei în dependenţă de scopurile pentru care este eliberat certificatul cheii publice.

4.1.1 ENTITĂŢI CARE POT DEPUNE CEREREA DE CERTIFICARE

Cererile pot fi depuse de diverşi solicitanţi şi pot conţine solicitări pentru diverse tipuri de certificate ale cheilor publice.

4.1.2 ÎNREGISTRAREA SOLICITĂRII DE CERTIFICARE A CHEII PUBLICE

Pachetul de documente al solicitantului, care satisface toate condiţiile prevăzute în CPP, este înregistrat de către administratorul de înregistrări. În caz contrar, administratorul de înregistrări refuză înregistrarea solicitantului pentru certificare şi restituie solicitantului pachetul de documente depus pentru înlăturarea cauzelor ce au servit temei de refuz.

După înregistrarea solicitantului pentru certificare administratorul de înregistrări transmite administratorului de certificare cererea de certificare a cheii publice pe suport de hîrtie, înregistrată şi semnată cu semnătura sa olografă, şi documentele ataşate acesteia.

4.2. PRELUCRAREA CERERII DE CERTIFICARE A CHEII PUBLICE

Fiecare cerere de certificare a cheii publice este prelucrată în următorul mod:

- administratorul de înregistrări primeşte cererea de certificare a cheii publice de la solicitant;
- administratorul de înregistrări verifică datele din cererea de certificare a cheii publice;
- ca urmare a verificării administratorul de înregistrări confirmă corespunderea datelor, conţinute în cererea de certificare a cheii publice, prin semnătura sa aplicată pe cerere;
- cererea de certificare a cheii publice confirmată şi documentele ataşate se transmit administratorului de certificare.

4.2.1 AUTENTIFICAREA ŞI IDENTIFICAREA

Administratorul de înregistrări identifică solicitantul în baza documentelor depuse şi realizează verificarea prealabilă în conformitate cu *Instrucţiunea de serviciu a administratorului înregistrare*.

În procesul verificării prealabile administratorul de înregistrări trebuie să constate respectarea următoarelor condiţii:

a) respectarea de către solicitant a cadrului normativ în domeniul semnăturii electronice la întocmirea şi depunerea cererii de certificare a cheii publice;

b) respectarea de către solicitant a drepturilor persoanelor terţe la întocmirea şi depunerea cererii de certificare a cheii publice;
c) autenticitatea informaţiei prezentate în cererea de certificare a cheii publice.

4.2.2 ACCEPTAREA SAU REFUZUL CERERII DE CERTIFICARE

La primirea pachetului de documente de la administratorul de înregistrări administratorul de certificare efectuează următoarele proceduri:
a) verifică autenticitatea cererii de certificare a chei publice (semnătura administratorului de înregistrări);
b) verifică corespunderea cererii de certificare a cheii publice (sintaxa şi conţinutul);
c) compară informaţia din cererea de certificare a cheii publice cu cea din copia actului de identitate prezentată;
d) verifică împuternicirile solicitantului de a depune cererea de certificare a cheii publice;
e) înscrie procedurile efectuate în baza de date şi în registrele de sistem.

După realizarea procedurilor menţionate supra administratorul de certificare ia decizia de certificare a cheii publice a solicitantului.

În cazul depistării încălcărilor legislaţiei în domeniul semnăturii electronice, încălcării drepturilor unor terţi în procesul de întocmire sau de depunere a cererii de certificare, prezentării în cererea de certificare a unor informaţii ce nu corespund realităţii administratorul de certificare ia decizia de refuz a certificării cheii publice, indicînd motivul refuzului.

Decizia de refuz a certificării cheii publice poate fi atacată în organul competent sau în instanţa de judecată şi nu serveşte temei pentru depunerea repetată a cererii după înlăturarea cauzelor ce au servit motiv pentru refuz.

4.2.3 TIMPUL DE PRELUCRARE A CERERII DE CERTIFICARE A CHEII PUBLICE

În dependenţă de solicitant distintigem următorii termeni de prelucrare a cererii de certificare a cheii publice:

1. persoană juridică de drept public angajaţii căreia sunt subiecţi ai declarării averii şi intereselor personale sau utilizatori ai Sistemului informaţional automatizat „Asistenţa medicală primară" – cel mult 15 zile lucrătoare de la recepţia pachetului de documente integral ce corespunde cerinţelor înaintate de Prestator,
2. persoană juridică de drept public angajaţii căreia nu sunt subiecţi ai declarării averii şi intereselor personale sau utilizatori ai Sistemului informaţional automatizat „Asistenţa medicală primară", persoană juridică de drept privat, persoană fizică – la momentul prezentării pachetului de documente integral ce corespunde cerinţelor înaintate de Prestator.

4.3. ELIBERAREA CERTIFICATULUI CHEII PUBLICE

După primirea şi prelucrarea cererii de certificare a cheii publice (a se vedea Secţiunile 4.1 şi 4.2), în cazul deciziei pozitive de certificare a cheii publice administratorul de certificare certifică cheia publică a utilizatorului sub formă de document electronic, în conformitate cu cap. 7 al CPP-ului.

Cererea de certificare a chei publice sub formă de document electronic se întocmeşte în conformitate cu cerinţele standardului IETF RFC 5967 *The application/pkcs10 Media Type*, IETF

RFC 4211 *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)* sau IETF RFC 6712 *Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP).*

Certificatul cheii publice a utilizatorului sub formă de document electronic corespunde cerinţelor standardului SM ISO CEI 9594-8:2014 Tehnologia informaţiei. Interconexiunea sistemelor deschise. Linii directoare: Structura certificatului cheii publice şi a atributului, ale standardului Uniunii Internaţionale a Telecomunicaţiilor ITU-T *X.509, versiunea 3*, sau recomandării IETF (Internet Engineering Task Force) RFC 5280 (RFC 2459) *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF RFC 6818 *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, şi IETF RFC 3739 *Qualified Certificates Profile.*

Titularului certificatului cheii publice (sau persoanei delegate ce deţine procură autentificată notarial) i se eliberează dispozitivul de creare a semnăturii electronice, ce conţine perechea de chei privată şi publică, generată şi, respectiv, certificată de Prestator. În cazul persoanelor juridice persoana responsabilă este cea căreia i se eliberează dispozitivul de creare a semnăturii electronice, ce conţine perechea de chei privată şi publică, generată şi, respectiv, certificată de Prestator.

Perioada de valabilitate a certificatului calificat al cheii publice a utilizatorului corespunde *Normelor tehnice*. Pentru celelalte tipuri de certificate în care Prestatorul are atît rolul de RootCA, cît şi SubRootCA, aceasta se determină prin ordine interne, iar pentru certificatele SSL – de către emitenţii acestora.

Ca document pe suport de hîrtie certificatul cheii publice se eliberează utilizatorului doar la solicitarea acestuia în două exemplare, este semnat cu semnăturile olografe de către conducătorul Prestatorului şi titular, şi autentificat cu ştampilele Prestatorului şi a persoanei juridice respectivă (după caz).

NOTĂ: La dorinţa titularului certificatul cheii publice poate fi transmis prin poşta electronică cu confirmarea recepţionării mesajului.

4.3.1 ACŢIUNILE ADMINISTRATORULUI DE CERTIFICARE ÎN PROCESUL DE GENERARE A CERTIFICATULUI CHEII PUBLICE

Fiecare certificat al cheii publice este eliberat în regim de timp real (on-line). Procedura de eliberare este următoarea:

- se iniţiază procedura de generare a perechii de chei;
- se generează cheile. Prin operaţii de testare şi determinare a corespunderii cheilor cu standardele PKI este verificată calitatea cheilor obţinute;
- se salvează cererea de certificare a cheii publice în format electronic (request);
- requestul este transmis către autoritatea de certificare;
- autoritatea de certificare certifică cheia publică;
- autoritatea de certificare pregăteşte răspunsul ce conţine certificatul cheii publice emis (în cazul emiterii lui) şi îl transmite administratorului de certificare.

4.3.2 NOTIFICAREA TITULARULUI DESPRE EMITEREA CERTIFICATULUI CHEII PUBLICE

Notificarea titularului despre emiterea certificatului cheii publice are loc în momentul transmiterii dispozitivului securizat de creare a semnăturii electronice. În cazul persoanei juridice notificarea se face prin intermediul persoanei responsabile, iar în cazul persoanei fizice -- fie

personal în timpul aflării titularului în sediul Prestatorului, fie prin intermediul persoanei împuternicite prin procură autentificată notarial.

4.4. ACCEPTAREA CERTIFICATULUI

4.4.1 ACŢIUNEA CE SEMNIFICĂ ACCEPTAREA CERTIFICATULUI CHEII PUBLICE

La primirea certificatului cheii publice titularul verifică conţinutul acestuia în raport cu corectitudinea prezentării datelor din cererea de certificare a cheii publice.

Dacă utilizatorul depistează necorespunderi, el trebuie să anunţe imediat Prestatorul.

Dacă în decursul a 3 (trei) zile din momentul primirii certificatului cheii publice de la titular nu parvin obiecţii, primirea şi instalarea certificatului cheii publice de către acesta se consideră realizată cu succes.

4.4.2 PUBLICAREA CERTIFICATULUI CHEII PUBLICE DE CĂTRE PRESTATOR

Fiecare certificat al cheii publice eliberat este stocat în Depozitul Prestatorului.

4.4.3 NOTIFICAREA ALTOR PERSOANE DESPRE ELIBERAREA CERTIFICATULUI CHEII PUBLICE UTILIZATORULUI

Publicarea certificatului cheii publice în Depozitul Prestatorului este echivalentă notificării părţilor interesate despre faptul că certificatul cheii publice al utilizatorului a fost emis de către Prestator.

4.5. PERECHEA DE CHEI PRIVATĂ ŞI PUBLICĂ ŞI UTILIZAREA CERTIFICATULUI CHEII PUBLICE

4.5.1 CHEIA PRIVATĂ A TITULARULUI ŞI UTILIZAREA CERTIFICATULUI CHEII PUBLICE

Titularul foloseşte cheia sa privată şi certificatul cheii publice:

- în conformitate cu destinaţia acestora, stabilită de prevederile CPP şi restricţiile stipulate în certificatul cheii publice (câmpurile *keyUsage* şi *enhancedKeyUsage*),
- în conformitate cu contractul de prestări servicii dintre persoana juridică sau persoana fizică şi Prestator,
- doar în perioadele valabilităţii lor.

În intervalul de timp cît perioada de valabilitate a certificatului cheii publice este **suspendată** utilizarea cheii private pentru crearea semnăturii electronice este **interzisă**.

4.5.2 CHEIA PUBLICĂ A TITULARULUI ŞI UTILIZAREA CERTIFICATULUI DE PARTEA DE ÎNCREDERE

Partea de încredere utilizează cheia publică şi certificatul cheii publice a utilizatorului:

- în conformitate cu destinaţia acestora, stabilită de prevederile CPP şi restricţiile stipulate în certificatul cheii publice (câmpurile *keyUsage* şi *enhancedKeyUsage*);
- doar după verificarea statutului certificatului şi verificarea semnăturii electronice a Prestatorului, emitentul certificatului utilizatorului;
- doar în perioadele de valabilitate ale acestora.

În intervalul de timp cît perioada de valabilitate a certificatului cheii publice este **suspendată** partea de încredere **nu poate utiliza** cheia publică şi certificatul cheii publice ale utilizatorului.

4.6. REÎNNOIREA CERTIFICATULUI

Conform legislaţiei în vigoare reînnoirea certificatului nu este permisă.

4.7. REÎNNOIREA CHEILOR

Nu se aplică.

4.8. MODIFICAREA DATELOR ÎN CERTIFICATUL CHEII PUBLICE

La modificarea datelor din cel puţin un cîmp al certificatului cheii publice valid titularul solicită revocarea acestuia. Acesta este trecut în Lista certificatelor revocate cu menţiunea *affiliationChanged*, ceea ce semnifică:

a) certificatul cheii publice a fost revocat ca rezultat al modificărilor datelor conţinute în el;
b) terţele părţi nu au motiv de a considera cheia privată corespunzătoare ca fiind compromisă.

Procedura de modificare a datelor din certificatul cheii publice, valabil la momentul solicitării, este echivalentă cu procedura de eliberare a unui nou certificat pentru o pereche de chei noi.

4.8.1 CAUZE PENTRU MODIFICAREA DATELOR DIN CERTIFICATUL CHEII PUBLICE

Drept temei pentru modificarea datelor din certificatul cheii publice valid poate fi: schimbarea numelui la căsătorie/divorţ, a subdiviziunii persoanei juridice sau a funcţiei (în cazul persoanelor juridice), schimbarea adresei, etc.

4.8.2 ENTITĂŢI CE POT SOLICITA MODIFICAREA CERTIFICATULUI CHEII PUBLICE

Ţinînd cont de faptul că procedura de modificare a datelor din certificatul cheii publice valid este echivalentă cu emiterea unui nou certificat cu datele schimbate, cererile de certificare a cheilor

publice pot fi depuse de diverşi solicitanţi şi pot conţine solicitări pentru diverse tipuri de certificate (în dependenţă de necesităţi).

4.8.3 PROCESAREA CERERII DE MODIFICARE A CERTIFICATULUI CHEII PUBLICE

A se vedea Secţiunea 4.2 , pct. 4.3.1.

4.8.1 NOTIFICAREA UTILIZATORULUI DESPRE EMITEREA NOULUI CERTIFICAT AL CHEII PUBLICE

A se vedea pct. 4.3.2.

4.8.2 ACŢIUNEA CE SEMNIFICĂ ACCEPTAREA CERTIFICATULUI CHEII PUBLICE MODIFICAT

A se vedea pct. 4.4.1.

4.8.3 PUBLICAREA CERTIFICATULUI CHEII PUBLICE MODIFICAT DE CĂTRE PRESTATORUL DE SERVICII DE CERTIFICARE

A se vedea pct. 4.4.2.

4.8.4 NOTIFICAREA ALTOR PERSOANE DESPRE ELIBERAREA CERTIFICATULUI UTILIZATORULUI

A se vedea pct. 4.4.3.

4.9. REVOCAREA ŞI SUSPENDAREA VALABILITĂŢII CERTIFICATULUI CHEII PUBLICE

4.9.1 CAUZE PENTRU REVOCARE

Certificatul cheii publice se revocă în următoarele cazuri:

a) la cererea titularului;

b) la încălcarea confidenţialităţii cheii private sau în cazul faptului constatat de compromitere a cheii private;

c) la depistarea unor informaţii neveridice în cererea de certificare a cheii publice sau 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 modificarea certificatului cheii publice;

f) în cazul decesului titularului sau al instituirii unei măsuri de ocrotire judiciară (ocrotire provizorie, curatelă sau tutelă) în privinţa acestuia;

g) la lichidarea Prestatorului. În acest caz toate certificatele eliberate şi publicate, cu perioada de valabilitate neexpirată, într-un termen specificat, sunt revocate împreună cu certificatul cheii publice al Prestatorului;
h) la solicitarea organului competent.

Prin compromiterea cheii private se subînţelege:
- pierderea dispozitivului securizat de creare a semnăturii electronice;
- apariţia suspiciunilor privind dezvăluirea informaţiei sau denaturarea ei în sistemul de legătură sau la locurile de utilizare a dispozitivului securizat de creare a semnăturii electronice;
- accesul persoanelor terţe la cheia privată sau la dispozitivul securizat de creare a semnăturii electronice;
- alte evenimente care dau temei de a presupune că a fost încălcată confidenţialitatea cheii private.

4.9.2 ENTITĂŢI CE POT SOLICITA REVOCAREA CERTIFICATULUI CHEII PUBLICE

Revocarea certificatului cheii publice poate fi solicitată:

a) de către titularul certificatului cheii publice;
b) de către persoana juridică – angajatorul titularului;
c) de către Centrul de înregistrări în cadrul prestării serviciului semnătură mobilă, în conformitate cu prevederile *Regulamentului privind funcţionarea Centrului de înregistrări al Centrului de certificare a cheilor publice al autorităţilor administraţiei publice în cadrul prestării serviciului semnătură digitală mobilă (serviciul mobile eID)*;
d) de către organul competent, în cazul încălcării Legii nr. 91 din 29.05.2014 privind semnătura electronică şi documentul electronic.

4.9.3 PROCEDURILE DE REVOCARE A CERTIFICATULUI CHEII PUBLICE

Cererea de revocare a certificatului se depune prin una din următoarele metode:
- în format electronic, semnată cu cheia privată valabilă a titularului, certificatul cheii publice al căruia urmează a fi revocat;
- sub formă de document pe suport de hîrtie personal de către titular/ persoana responsabilă direct la Prestator sau prin intermediul sistemului de schimb electronic de documente.

Cererea de revocare a certificatului cheii publice pe suport de hîrtie (conform Anexei nr. $3A_1$ sau Anexei nr.$3A_2$ la prezentul CPP) reprezintă un document semnat cu semnătura olografă a titularului şi/sau cu semnătura olografă a conducătorului persoanei juridice (sau a persoanei căreia i-au fost delegate împuterniciri, confirmate prin procură autentificată notarial sau ordin intern), cu aplicarea ştampilei (după caz). În cazul persoanei fizice modelul cererii corespunde cu Anexa nr. 3B şi aceasta este semnată olograf de către titular sau persoana împuternicită prin procură autentificată notarial.

Cererea de revocare a certificatului cheii publice a titularului trebuie să conţină:
a) datele de identificare ale titularului;
b) cauza revocării certificatului cheii publice;
c) tipul certificatului cheii publice ce urmează a fi revocat;
d) data semnării cererii, semnăturile titularului şi/sau a conducătorului persoanei juridice (sau a persoanei căreia i-au fost delegate împuterniciri, confirmate prin procură autentificată notarial sau ordin intern).

Procedura de revocare a certificatului cheii publice are loc astfel:
1. la primirea cererii de revocare a certificatului cheii publice administratorul de înregistrări identifică solicitantul, verifică corectitudinea completării cererii, verifică semnătura electronică – după caz, autentifică cererea de revocare a certificatului cheii publice;
2. dacă verificarea are loc cu succes administratorul de înregistrări o semnează, apoi transmite cererea de revocare a certificatului cheii publice administratorului de certificare care revocă certificatul cheii publice şi-l publică în Lista certificatelor revocate cu indicarea cauzei revocării;
3. administratorul de certificare contrasemnează cererea de revocare a certificatului cheii publice şi trimite notificare titularului despre revocarea certificatului deţinut;
4. notificare despre revocarea certificatului cheii publice primeşte şi solicitantul revocării (dacă acesta nu este titularul certificatului cheii publice).

4.9.4 PERIOADA DE GRAŢIE A CERERII DE REVOCARE

Nu se aplică.

4.9.5 TERMENUL DE PRELUCRARE A CERERII DE REVOCARE A CERTIFICATULUI CHEII PUBLICE DE CĂTRE PRESTATORUL DE SERVICII DE CERTIFICARE

Administratorul de certificare ia decizia cu privire la revocarea certificatului cheii publice timp de 1 (una) oră lucrătoare din momentul recepţionării cererii de revocare a certificatului cheii publice.

Prestatorul notifică utilizatorul despre decizia luată de acceptare sau refuz a revocării, cu indicarea motivului refuzului, în termen de 2 (două) ore lucrătoare din momentul recepţionării cererii de revocare a certificatului cheii publice.

Certificatul cheii publice revocat este inclus în lista certificatelor revocate timp de 3 (trei) ore lucrătoare din momentul recepţionării cererii de revocare a certificatului cheii publice, iar Prestatorul emite lista actualizată a certificatelor revocate.

Timpul de revocare a certificatului cheii publice se consideră timpul de emitere şi publicare a listei actualizate a certificatelor revocate (timpul indicat în cîmpul *ThisUpdate*).

4.9.6 VERIFICAREA CERTIFICATELOR CHEILOR PUBLICE REVOCATE DE CĂTRE PĂRŢILE DE ÎNCREDERE

La primirea documentului electronic semnat cu semnătura electronică partea de încredere este obligată să verifice dacă certificatul cheii publice, corespunzător cheii private cu ajutorul căreia a fost creată semnătura electronică, nu se află în Lista certificatelor revocate.

Verificarea statutului certificatului cheii publice doar în baza Listei certificatelor revocate este suficientă pentru a evita riscurile de a cauza prejudicii părţii de încredere. Există şi posibilitatea de a solicita de la Prestator confirmarea autenticităţii semnăturii electronice în documentul electronic sau de a verifica statutul certificatului în regim de timp real prin intermediul protocolului **OCSP**.

Prezenţa certificatului în Lista certificatelor revocate obligă partea de încredere să respingă documentul asociat cu acest certificat dacă motivul revocării a fost:

- **unspecified** – necunoscut;
- **keyCompromise** – încălcarea securităţii cheii private:
- **cACompromise** – încălcarea securităţii cheii private a Prestatorului;
- **cessationOfOperation** – suspendarea prestării serviciilor;
- **certificateHold** – suspendarea valabilităţii certificatului cheii publice.

Dacă certificatul cheii publice a fost revocat din unul din motivele

- **affiliationChanged** – modificarea informaţiei din certificat;
- **removeFromCRL** – restabilirea valabilităţii certificatului;
- **privilegeWithdrawn** – atribuţiile delegate titularului au fost anulate,

Partea de încredere decide singură despre plauzibilitatea semnăturii electronice corespunzătoare.

4.9.7 FRECVENŢA PUBLICĂRII LISTEI CERTIFICATELOR REVOCATE

Lista certificatelor revocate (CRL) este publicată (actualizată) cel puţin 1 dată la 10 zile şi la fiecare revocare, suspendare sau restabilire a valabilităţii certificatului cheii publice.

4.9.8 TIMPUL MAXIM DE LATENŢĂ PENTRU CRL

Nu se aplică.

4.9.9 UTILIZAREA SERVICE-ULUI OCSP

Prestatorul furnizează servicii de verificare a statutului certificatelor cheilor publice în regim de timp real pe baza protocolului OCSP, descris în RFC 6960 *X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol - OCSP*. Folosind OCSP, se poate obţine informaţie actualizată şi veridică despre statutul certificatului cheii publice.

OCSP funcţionează după principiul **întrebare-răspuns**. Ca răspuns la fiecare cerere serverul OCSP oferă următoarea informaţie despre statutul certificatului cheii publice:

- **good** – răspuns pozitiv la cerere (i.e. certificatul este valabil);
- **revoked** – certificatul cheii publice este revocat;
- **unknown** – certificatul verificat nu a fost eliberat de Prestator.

4.9.10 CERINŢE ÎNAINTATE LA VERIFICAREA CERTIFICATULUI PRIN OCSP

Părţile de încredere nu sunt obligate să verifice statutul certificatului cheii publice cu ajutorul service-ului OCSP, descris în pct. 4.9.9. Dar, necătînd la aceasta, se recomandă utilizarea service-ului OCSP pentru a minimiza riscul falsificării documentelor electronice cu utilizarea semnăturii electronice.

4.9.11 ALTE FORME DE NOTIFICARE PRIVIND STATUTUL CERTIFICATULUI

Nu se aplică.

4.9.12 CERINŢE SPECIALE FAŢĂ DE ÎNCĂLCAREA SECURITĂŢII CHEII PRIVATE

CPP nu defineşte cerinţe suplimentare faţă de încălcarea securităţii cheii private.

4.9.13 CIRCUMSTANŢE CE DETERMINĂ SUSPENDAREA VALABILITĂŢII CERTIFICATULUI CHEII PUBLICE

Suspendarea valabilităţii certificatului cheii publice are loc la solicitarea titularului (e.g., pentru un interval de timp cît lipseşte de la servici, dar nu mai mult de treizeci de zile calendaristice).

4.9.14 ENTITĂŢI CE POT SOLICITA SUSPENDAREA CERTIFICATULUI CHEII PUBLICE

Certificatul cheii publice se suspendă la cererea titularului.

4.9.15 PROCEDURA DE SUSPENDARE A VALABILITĂŢII CERTIFICATULUI CHEII PUBLICE

Cererea de suspendare a valabilităţii certificatului cheii publice se depune prin una din următoarele metode:

- în format electronic, semnată cu cheia privată valabilă a titularului, certificatul cheii publice al căruia urmează a fi suspendat;
- sub formă de document pe suport de hîrtie personal de către titular/persoana responsabilă din cadrul persoanei juridice direct la Prestator sau prin intermediul sistemului de schimb electronic de documente.

Cererea de suspendare a valabilităţii certificatului cheii publice pe suport de hîrtie (conform modelului din Anexa nr.4A) reprezintă un document semnat olograf atît de către titular, cît şi de către conducătorul persoanei juridice (sau o persoană căreia i-au fost delegate împuterniciri, confirmate prin procură autentificată notarial sau ordin intern), cu aplicarea ştampilei, după caz. În cazul persoanei fizice modelul cererii de suspendare a valabilităţii certificatului cheii publice corespunde cu Anexa nr. 4B şi aceasta este semnată olograf de către titular sau persoana împuternicită prin procură autentificată notarial.

Cererea de suspendare a valabilităţii certificatului cheii publice trebuie să conţină:

a) datele de identificare ale titularului;
b) termenul de suspendare a valabilităţii certificatului cheii publice;
c) cauza suspendării valabilităţii certificatului cheii publice;
d) data semnării cererii, semnăturile titularului şi/sau a conducătorului persoanei juridice (sau a persoanei căreia i-au fost delegate împuterniciri, confirmate prin procură autentificată notarial sau ordin intern).

Procedura de suspendare a valabilităţii certificatului cheii publice are loc în mod analog celei de revocare.

Certificatul cheii publice, valabilitatea căruia este suspendată, este publicat în Lista certificatelor revocate.

Timpul de suspendare a valabilităţii certificatului cheii publice se consideră timpul de emitere şi publicare a listei actualizate a certificatelor revocate (timpul indicat în cîmpul *ThisUpdate*).

4.9.16 RESTRICŢII PE PERIOADA SUSPENDĂRII VALABILITĂŢII CERTIFICATULUI

Valabilitatea certificatului cheii publice este suspendată pe o perioadă de pînă la 30 (treizeci) de zile calendaristice. În intervalul de timp cît perioada de valabilitate a certificatului cheii publice este **suspendată** utilizarea cheii private pentru crearea semnăturii electronice este **interzisă**.

4.9.17 RESTABILIREA VALABILITĂŢII CERTIFICATULUI

Valabilitatea certificatului cheii publice a utilizatorului este restabilită în următoarele cazuri:

a) la solicitarea titularului certificatului cheii publice;
b) la solicitarea persoanei juridice – angajatorul titularului.

Cererea de restabilire a valabilităţii certificatului cheii publice se depune sub formă de document pe suport de hîrtie personal de către titular/persoana împuternicită prin procură autentificată notarial/persoana responsabilă sau prin intermediul sistemului de schimb electronic de documente, şi 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 pe suport de hîrtie (conform modelului din Anexa nr.5A) reprezintă un document semnat olograf atît de către titular, cît şi de către conducătorul persoanei juridice (sau o persoană căreia i-au fost delegate împuterniciri, confirmate prin procură autentificată notarial sau ordin intern), cu aplicarea ştampilei, după caz. În cazul persoanei fizice modelul cererii corespunde cu Anexa nr. 5B şi aceasta este semnată olograf de către titular/ persoana împuternicită prin procură autentificată notarial.

Cererea de restabilire a valabilităţii certificatului cheii publice a titularului trebuie să conţină:

a) datele de identificare ale titularului;
b) data emiterii certificatului cheii publice a cărui valabilitate a fost suspendată;
c) termenul de suspendare a valabilităţii certificatului cheii publice;
d) cauza suspendării valabilităţii certificatului cheii publice;
e) cauza restabilirii valabilităţii certificatului cheii publice;
f) data semnării cererii, semnăturile titularului şi/sau a conducătorului persoanei juridice (sau a persoanei căreia i-au fost delegate împuterniciri, confirmate prin procură autentificată notarial sau ordin intern).

Procedura de restabilire a valabilităţii certificatului cheii publice are loc în următorul mod:

1. la primirea cererii, administratorul de înregistrări identifică solicitantul, verifică corectitudinea completării cererii, autentifică cererea de restabilire a valabilităţii certificatului cheii publice;
2. dacă verificarea are loc cu succes administratorul de înregistrări o semnează, apoi transmite cererea administratorului de certificare care restabileşte valabilitatea certificatului cheii publice şi îl elimină din Lista certificatelor revocate;
3. administratorul de certificare contrasemnează cererea şi trimite titularului certificatului cheii publice o notificare despre restabilirea valabilităţii certificatului deţinut.

Timpul de restabilire a valabilităţii certificatului cheii publice se consideră timpul de emitere şi publicare a listei actualizate a certificatelor revocate (timpul indicat în cîmpul *ThisUpdate*).

NOTĂ: în cazul expirării termenului pentru care a fost suspendată valabilitatea certificatului cheii publice şi în lipsa unei cereri din partea titularului sau şi a conducătorului persoanei juridice privind restabilirea valabilităţii certificatului cheii publice, conform prevederilor cadrului normativ, Prestatorul ia decizia de revocare a acestuia (Anexa nr.6).

4.10. SERVICIILE DE VERIFICARE A STATUTULUI CERTIFICATULUI

4.10.1 CARACTERISTICI OPERAŢIONALE

Conform recomandărilor definite în *Normele tehnice*.

4.10.2 DISPONIBILITATEA SERVICIULUI

Serviciile sunt disponibile 24x7.

4.10.3 CARACTERISTICI OPŢIONALE

Nu se specifică.

4.11. ÎNCETAREA RELAŢIEI DINTRE UTILIZATOR ŞI PRESTATOR

Utilizatorul poate încheia orice raport cu Prestatorul solicitînd revocarea certificatului sau din momentul expirării acestuia.

4.12. DEPOZITAREA CHEII ŞI RESTABILIREA EI

Nu se aplică.

4.13. ADMINISTRAREA CHEII PRIVATE ŞI PUBLICE A PRESTATORULUI

Termenul de valabilitate a cheii private a Prestatorului este de 5 ani, iar a cheii publice – 10 ani. Începutul perioadei de valabilitate a cheii private se consideră data şi ora la care începe termenul de valabilitate a certificatului cheii publice ce-i corespunde.

La expirarea termenului de valabilitate a cheii private a Prestatorului se creează o nouă pereche de chei şi este iniţiat procesul de certificare a cheii publice.

Schimbarea planificată a cheilor publice şi private ale Prestatorului se efectuează nu mai devreme de 14 zile înainte şi nu mai tîrziu de expirarea termenului de valabilitate a cheii private.

Schimbarea în afara acestui termen a cheilor se efectuează în cazul compromiterii sau pericolului de compromitere a cheii private a Prestatorului.

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

Cheia privată a Prestatorului se utilizează exclusiv pentru semnarea:

a) certificatelor cheilor publice ale utilizatorilor;
b) listelor certificatelor revocate.

Cheia privată a Prestatorului se păstrează şi se utilizează în condiţii ce exclud încălcarea confidenţialităţii acesteia şi în conformitate cu cadrul normativ.

5. RESURSE, GESTIONARE ŞI CONTROLUL OPERAŢIONAL

5.1. CONTROLUL FIZIC AL SECURITĂŢII

Sistemul de operare, terminalele operatorilor şi resursele informaţionale ale Prestatorului se află într-o încăpere special amenajată, protejată fizic de accesul nesancţionat, de deteriorări şi încălcarea activităţii acestuia. Fiecare intrare şi ieşire este controlată şi înscrisă în registru; este menţinută stabilitatea sursei de energie electrică, a izolaţiei hidrofuge şi a mediului înconjurător.

5.1.1 AMPLASARE

Prestatorul are sediul pe adresa juridică a instituţiei: or. Chişinău, Piaţa Marii Adunări Naţionale, 1, MD-2012, iar serviciile de certificare sunt furnizate de Prestator pe adresa: or. Chişinău, str. 31 august 1989, nr 82.

5.1.2 ACCESUL FIZIC

Accesul fizic în încăperea Prestatorului este controlat şi gestionat de sistemele de control al accesului şi de supraveghere video, de detectare a pătrunderii nesancţionate, de sistemul neîntrerupt de alimentare cu energie electrică, de sistemul antiincendiar. Toate sistemele funcţionează 24/24.

Atît utilizatorii, cît şi vizitatorii, au acces în sediul Prestatorului în fiecare zi lucrătoare de la 08:30 la 16:30. În rest (inclusiv zilele de odihnă), accesul este permis doar persoanelor abilitate şi administraţiei Prestatorului.

Vizitatorii Prestatorului de fiecare dată trebuie însoţiţi de persoanele abilitate ale acestuia.

Accesul fizic în încăperile Prestatorului este oferit după nivele. Descrierea şi cerinţele faţă de fiecare nivel sunt prezentate în tabel.

Nivel	Descriere	Mecanismul de control al accesului
Nivelul unu de securitate fizică	Se referă la bariera de acces primară. Este acordat utilizatorilor semnăturii electronice.	Accesul la acest nivel nu necesită însoţirea utilizatorului semnăturii electronice de către persoana abilitată – colaborator al Prestatorului. Accesul la acest nivel este monitorizat.
Nivelul doi de securitate fizică	Se răsfrînge asupra ariilor comune, inclusiv sala de şedinţe şi birourile. Este acordat colaboratorilor Centrului de certificare.	Nivelul doi impune controlul accesului individual al tuturor persoanelor. Accesul la nivelul doi este monitorizat automat.
Nivelul trei de securitate fizică	Se răsfrînge asupra încăperilor unde au loc procesele Centrului de certificare şi anume, autentificarea, verificarea şi eliberarea certificatelor. Este acordat administratorului de înregistrări şi administratorului de certificare.	Nivelul trei impune utilizarea autentificării multifactoriale a accesului individual. Accesul la nivelul trei este monitorizat automat.
Nivelul patru de securitate fizică	Se răsfrînge asupra încăperilor cu regim special unde au loc procesele Centrului de certificare şi anume, administrarea cheilor Prestatorului, crearea certificatelor cheilor publice.	Nivelul patru impune utilizarea autentificării multifactoriale a accesului individual. Accesul la nivelul patru este monitorizat automat.

Conţinutul acestei secţiuni corespunde *Politicii de acordare şi control a accesului la resursele Centrului de certificare a cheilor publice.*

5.1.3 ALIMENTAREA ELECTRICĂ ŞI CONDIŢIONAREA AERULUI

Toate zonele, cu prezenţă obligatorie a personalului, pe parcursul orelor de lucru sunt alimentate cu aer filtrat de temperatură şi umiditate necesare. Zona sistemelor computerizate totdeauna este alimentată cu un flux de aer condiţionat pentru asigurarea unui regim de temperatură adecvată pentru funcţionare, critic necesar pentru echipamentul computerizat.
Din momentul depistării de sistem a deconectării de avarie a alimentării cu energie timp de 120 minute funcţionarea echipamentului este asigurată pe baza energiei surselor neîntreruptibile de energie (UPS). Perioadele de funcţionalitate mai lungi sunt asigurate de generatoarele de energie diesel staţionare. În acest interval de timp este permisă deconectarea sistemului de condiţionare a aerului în zona sistemelor computerizate şi trecerea la iluminarea de servici. Monitorizarea şi gestionarea sistemelor din zona computerizată sunt realizate independent de alte zone şi încăperi şi fizic nu au nici o legătură între ele.

5.1.4 UMIDITATEA

În zona sistemelor computerizate sunt instalaţi senzori ce verifică automat nivelul umidităţii în aer şi a prezenţei apei. Aceşti senzori sunt integraţi în sistemul de control al securităţii clădirii Prestatorului. Colaboratorii responsabili, conform nomenclatorului şi atribuţiilor, vor fi înştiinţaţi la momentul oportun despre pericol, iar în cazuri excepţionale vor fi înştiinţate şi serviciile publice (civile).

5.1.5 SECURITATEA ANTIINCENDIARĂ ŞI MĂSURILE DE PREVENIRE

Prestatorul este dotat cu mijloace autonome şi sisteme de alarmă antiincendiară, stingere automată a incendiului şi înlăturare a fumului conform normativelor **NCM.E.03.03-2003** *"Dotarea clădirilor şi instalaţiilor cu sisteme autonome de semnalizare şi stingere a incendiilor"*, **NCM.E.03.05-2004** *"Instalaţii autonome de stingere şi semnalizare a incendiilor. Normativ pentru proiectare"*.

5.1.6 PĂSTRAREA PURTĂTORILOR DE INFORMAŢIE

În scop de asigurare a funcţionării şi integrităţii mediului informaţional al Prestatorului toţi purtătorii de informaţie, inclusiv copiile pe suport de hîrtie ale documentaţiei, ce au legătură cu datele critice, se păstrează în safeuri metalice ignifuge, accesul la care este limitat întru preîntîmpinarea posibilelor acţiuni nesancţionate chiar şi din partea persoanelor împuternicite.
Safeurile sunt amplasate într-o încăpere cu nivel înalt de securitate. Acces în încăpere şi la safeuri îl au doar persoanele împuternicite.

5.1.7 NIMICIREA PURTĂTORILOR DE INFORMAŢIE

La expirarea termenului de păstrare toţi purtătorii de informaţie (hîrtia ş.a.), ce conţin informaţie importantă din punct de vedere al securităţii Prestatorului, sunt nimiciţi în dispozitive speciale.

Sistemele operaţionale de securitate revin la starea iniţială şi se dezinstalează în conformitate cu recomandările producătorilor. Sistemele operaţionale sunt supuse acestor proceduri şi cînd purtătorii de informaţie sunt supuşi reparaţiei.

Cheile criptografice, codurile, purtătorii, folosiţi pentru păstrarea lor, sunt nimicite conform ***Instrucţiunii ce reglementează securitatea şi exploatarea mijloacelor de protecţie criptografică a informaţiei*** şi cu utilizarea dispozitivelor de clasă nu mai jos de **DIN-3** (aceste măsuri sunt aplicate dispozitivelor ce nu permit reutilizarea lor şi garantează nimicirea informaţiei).

Suporturile de hîrtie ce conţin informaţie cu caracter important pentru Prestator, după expirarea termenului stabilit de păstrare, sunt nimicite în dispozitive speciale.

5.1.8 COPIEREA DE REZERVĂ COMPLETĂ

Copiile parolelor, a codurilor se păstrează în containere speciale.

De asemenea, se efectuează rezervarea arhivelor, a copiilor şi a seturilor mijloacelor de program ale Prestatorului. Astfel, Prestatorul poate restabili orice disfuncţie în timp de 48 ore, iar restabilirea sistemului de distribuire a listei certificatelor revocate are loc în 10 minute.

5.2. ORGANIZAREA CONTROLULUI SECURITĂŢII

5.2.1 ROLURILE ŞI ATRIBUŢIILE FUNCŢIONALE

Prestatorul dispune de următoarele funcţii:

- **şeful Centrului de certificare a cheilor publice** -- responsabil de administrarea corectă şi conducerea CC;
- **administratorul de securitate** -- responsabil de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei, precum şi de elaborarea şi implementarea politicii de securitate a Prestatorului;
- **administratorul de certificare** -- responsabil pentru crearea, suspendarea sau restabilirea valabilităţii şi revocarea certificatelor cheilor publice, ţinerea registrului certificatelor cheilor publice, păstrarea şi utilizarea în siguranţă a cheii private;
- **administratorul de înregistrări** -- responsabil de corectitudinea (autenticitatea) informaţiei de completare a certificatului cheii publice şi înregistrarea titularilor certificatelor cheilor publice în procesul de creare, suspendare sau restabilire a valabilităţii şi revocare a certificatelor cheilor publice;
- **administratorul de sistem** -- responsabil de administrarea, funcţionarea corespunzătoare şi asigurarea securităţii complexului tehnic de program al Prestatorului.

În afara funcţiilor menţionate mai sus în cadrul Prestatorului mai pot activa:

- **manager** -- responsabil de primirea şi elaborarea răspunsurilor la petiţiile parvenite în cadrul Prestatorului, monitorizarea proceselor de prestare a serviciilor;
- **operatorii** care realizează activităţi de deservire zilnică a complexului tehnic de program al (copierea/restabilirea sistemului, gestionarea arhivelor, introducerea informaţiei etc.);
- **auditorul** este responsabil de corespunderea desfăşurării proceselor în conformitate cu clauzele actelor de reglementare. Auditorul efectuează auditul intern, are acces la toate arhivele şi înscrierile auditorilor sistemului;

- **juristul** este responsabil de elaborarea şi evidenţa documentelor juridice, elaborarea bazei normative a acestuia şi controlul asupra respectării cadrului normativ, studierea şi analiza întrebărilor juridice în domeniul semnăturii electronice.

5.2.2 NUMĂRUL PERSOANELOR CU FUNCŢII DE RĂSPUNDERE, NECESARE PENTRU REALIZAREA UNUI PROCES

Procedura creării perechii de chei a Prestatorului, necesară pentru semnarea certificatelor cheilor publice şi a Listei certificatelor revocate, solicită prezenţa a cel puţin două persoane: persoana împuternicită şi a administratorului de securitate.

Drept de acces logic şi fizic la modulul criptografic ce păstrează perechile de chei ale Prestatorului o deţin: administratorul de securitate, şeful CC, şeful DGTI.

Activarea modulului cu ajutorul cheilor de acces este urmată de aplicarea cheilor Prestatorului cu scop de desfăşurare a proceselor necesare, în particular, de creare şi semnare a certificatelor cheilor publice emise de Prestator.

Toate celelalte operaţii şi roluri, descrise mai sus în CPP, pot fi executate individual şi fără prezenţa altor colaboratori.

5.2.3 IDENTIFICAREA ŞI AUTENTIFICAREA ROLURILOR PERSOANELOR CU FUNCŢII DE RĂSPUNDERE

Persoanele cu funcţii de răspundere ale Prestatorului sunt supuse procedurilor de identificare şi autentificare în următoarele cazuri:

- includerea în lista persoanelor cu drept de acces în încăperile CC;
- includerea în lista persoanelor cu drept de acces la sistemele şi resursele de reţea ale CC;
- eliberarea confirmării cu privire la funcţia deţinută;
- asigurarea identificării în sistemul informaţional al CC.

Fiecare identificare:

- trebuie să fie unică şi să aparţină unei persoane;
- nu poate fi folosită împreună cu o altă persoană;
- trebuie să fie limitată în dependenţă de funcţie (reieşind din funcţiile executate) prin intermediul mijloacelor tehnice şi/sau de program ale sistemului Prestatorului.

Identificarea se realizează cu ajutorul prezenţei fizice a persoanei cu funcţie de răspundere în faţa persoanei împuternicite a Instituţiei, a colaboratorului serviciului securitate, care verifică actele ce confirmă identitatea (buletinul de identitate, paşaportul). Ulterior, confirmarea identităţii se efectuează prin procedurile de verificare, prevăzute în pct. 5.3.1 al CPP.

5.2.4 ROLURILE CE INTERZIC CUMULAREA FUNCŢIILOR

În conformitate cu cadrul normativ în domeniul semnăturii electronice nu se permite cumularea funcţiilor de administrator de înregistrări, administrator de certificare, administrator de sistem, administrator de securitate.

5.3. SECURITATEA PERSONALULUI

5.3.1 CERINŢE FAŢĂ DE CALIFICAREA ŞI EXPERIENŢA PERSONALULUI

Colaboratorul Prestatorului, care este persoană cu funcţie de răspundere, trebuie să treacă procedura de confirmare a corespunderii cu cerinţele înaintate funcţiei respective. Pentru aceasta el prezintă toate documentele de confirmare:

- a calificării: diploma de studii superioare, certificatele cursurilor absolvite, caracteristici profesionale;
- a experienţei de lucru;
- confirmarea credibilităţii: cazier juridic ce constată lipsa antecedentelor penale;
- să semneze acordul (contractul) de executare a atribuţiilor funcţionale pentru asigurarea nivelului corespunzător de responsabilitate;
- trebuie să semneze acordul de nedivulgare a datelor personale ale utilizatorului ce sunt sau pot fi cunoscute în procesul de executare a atribuţiilor funcţionale;
- este obligat să nu execute sarcini ce pot cauza daune sau duce la apariţia situaţiilor de conflict între Prestator şi alte persoane (fizice sau juridice).

Refuzul de numire în funcţie este motivat de:

- ducerea în eroare de către candidatul la funcţie;
- caracteristici nefavorabile sau necredibile despre candidat;
- semne de lipsă a responsabilităţii.

5.3.2 PROCEDURILE DE VERIFICARE A PERSONALULUI

Nu se aplică.

5.3.3 CERINŢE DE INSTRUIRE A PERSONALULUI

Personalul implicat în furnizarea serviciilor de certificare de către Prestator trece instruirea cu privire la:

- regulile de lucru cu informaţia clasificată şi de protecţie a acesteia;
- prevederile Regulamentului prestatorului de servicii de certificare I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică";
- prevederile Codului de practici şi proceduri al Centrului de certificare a cheilor publice;
- prevederile Politicii de certificare;
- procedurile şi controlul securităţii Prestatorului;
- utilizarea şi funcţionarea mijloacelor tehnice şi de program ale Prestatorului;
- atribuţiile funcţionale.

5.3.4 FRECVENŢA DESFĂŞURĂRII PERIOADELOR REPETATE DE INSTRUIRE ŞI CERINŢE

Pregătirea personalului are loc după necesitate sau după fiecare modificare esenţială în cadrul Prestatorului.

5.3.5 FRECVENŢA ŞI CONSECUTIVITATEA TRANSFERURILOR (ROTAŢIILOR) DE FUNCŢII

CPP nu stabileşte cerinţe faţă de transferurile colaboratorilor.

5.3.6 SANCŢIUNI ÎN CAZUL ACŢIUNILOR NEAUTORIZATE

În cazul acţiunilor neautorizate din partea persoanelor cu funcţii de răspundere ale Prestatorului se iau măsuri corespunzătoare de disciplină, pînă la eliberarea din funcţie, definite în documentele corespunzătoare ale Instituţiei şi sunt în conformitate cu legislaţia şi actele internaţionale.

În cazul acţiunilor neautorizate din partea terţelor persoane, administratorul de securitate împreună cu administratorul de sistem pot suspenda accesul respectivilor la sistemul Prestatorului.

5.3.7 CERINŢE DE ANGAJARE TEMPORARĂ A PERSONALULUI

Personalul, angajat pe un anumit interval de timp în bază de contract (servicii externe, elaborarea şi dezvoltarea subsistemelor şi ale aplicaţiilor, etc.) este supus aceleeaşi proceduri de verificare, ca şi colaboratorii Prestatorului. Mai mult ca atît, persoana angajată în bază de contract, cu excepţia celei care a primit aviz pozitiv din partea administratorului de securitate, în procesul efectuării lucrărilor în încăperile Prestatorului este însoţită de un colaborator împuternicit.

5.3.8 DOCUMENTAŢIE PUSĂ LA DISPOZIŢIA PERSONALULUI

Prestatorul pune la dispoziţia personalului documentaţia minimă necesară pentru executarea atribuţiilor sale funcţionale:

- baza normativă în domeniul semnăturii electronice,
- Regulamentul prestatorului de servicii de certificare I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică",
- Codul de practici şi proceduri al Centrului de certificare a cheilor publice,
- Politica de certificare,
- Instrucţiunile de serviciu,
- modelele cererilor şi ale altor documente necesare,
- extrasele din actele regulatorii cu privire la acţiunile întreprinse în situaţii critice.

5.4. EVENIMENTE SUPUSE ÎNREGISTRĂRII ŞI PROCEDURILE AUDITULUI

Cu scop de desfăşurare efectivă a procedurilor Prestatorului şi control al personalului şi al utilizatorilor, Prestatorul realizează protocolarea acţiunilor tuturor titularilor şi ale personalului de deservire, inclusiv şi a evenimentelor ce au loc în sistem.

Este necesar ca fiecare persoană, care are legătură cu prestarea serviciilor de certificare, să înscrie informaţia cu scop de a gestiona şi a reacţiona adecvat în conformitate cu atribuţiile sale funcţionale. Înscrierile informaţionale, ce alcătuiesc registrele evenimentelor, trebuie să fie accesibile persoanelor autorizate cu drept de acces la aceste date în caz de soluţionare a situaţiilor de conflict sau la depistarea încercărilor de a încălca securitatea Prestatorului.

În măsura posibilităţilor, registrele evenimentelor trebuie create în regim automatizat. Dacă înscrierile nu pot fi create în regim automatizat sau evenimentele nu pot fi ţinute la evidenţă cu ajutorul sistemelor automatizate atunci se folosesc registre corespunzătoare pe suport de hîrtie.

Fiecare registru, electronic sau pe suport de hîrtie, este supus controlului în procesul de audit al sistemelor.

În ce priveşte sistemele Prestatorului, auditorul (în cazul existenţei), la cererea administratorului de securitate, poate efectua controlul şi auditul regulat, poate verifica corespunderea mecanismelor şi a procedurilor aplicate în conformitate cu CPP, cu scop de ridicare a eficacităţii mecanismelor şi procedurilor existente.

5.4.1 TIPURILE DE EVENIMENTE SUPUSE ÎNSCRIERII

Fiecare eveniment, critic din punct de vedere al securităţii Prestatorului, este supus înscrierii şi păstrării în arhivă.

Registrele Prestatorului păstrează înscrierile fiecărei acţiuni realizate de componentele de program în cadrul sistemului. Toate datele sunt împărţite în trei categorii:

- **date de sistem** – înscrieri ce conţin informaţie despre cererile utilizatorilor şi răspunsurile serverului (sau invers), în conformitate cu nivelul protocoalelor de reţea (e.g., **http, https, tcp** etc.). În înscriere se indică adresa **IP** a serverului, operaţiile executate (e.g., căutare, redactare, înscriere) şi datele transmise (e.g., numărul înscrierilor în baza de date);
- **erori** – înscrieri ce conţin informaţie despre erori, în conformitate cu nivelul protocoalelor de reţea şi nivelul modulelor aplicaţiilor;
- **audite** – înscrieri ce conţin informaţie ce ţine de serviciile de certificare a cheilor publice (e.g., identificarea solicitantului, cereri de certificare, cereri de revocare a certificatelor, publicarea certificatului şi a **CRL** etc.).

Pentru fiecare componentă de program, critică din punct de vedere a securităţii Prestatorului, se foloseşte un registru separat. Registre separate se folosesc şi pentru fiecare server şi staţie de lucru. După completarea cu înscrieri, registrele se arhivează şi în locul lor se creează altele noi. Registrele anterioare, după arhivare şi copiere de rezervă, se şterg din sistem.

Fiecare înscriere, creată automat sau manual, conţine următoarea informaţie:

- tipul evenimentului;
- identificatorul evenimentului;
- data şi ora producerii evenimentului;
- identificatorul sau alte date, ce corespund indicatorului la colaboratorul responsabil;
- înscrierea despre decizia luată cu privire la eveniment (executat sau a dus la apariţia erorii).

Acces la registrele evenimentelor şi ale auditului au doar administratorul de securitate şi auditorul (a se vedea Secţiunea 5.2 al CPP).

5.4.2 FRECVENŢA DE VERIFICARE A REGISTRELOR EVENIMENTELOR

Înscrierile, conţinute în registrul evenimentelor, sunt analizate minuţios cel puţin o dată pe lună. Fiecare eveniment cu statut critic sau de importanţă primară este analizat şi descris în registrul corespunzător al evenimentelor.

Vizualizarea registrelor evenimentelor este însoţită de controlul modificării nesancţionate, cu verificarea fiecărei anomalii depistate sau a deranjamentelor reflectate în registre. Fiecare acţiune realizată ca urmare a deranjamentului depistat trebuie înscrisă în registru.

5.4.3 PERIOADA DE PĂSTRARE A REGISTRELOR EVENIMENTELOR

Înscrierile despre evenimentele înregistrate se păstrează în fişiere, amplasate pe purtători de informaţie de sistem, ce nu depăşesc dimensiunea spaţiului liber destinat acestor fişiere. În această perioadă registrele sunt considerate active şi accesibile fiecărui colaborator autorizat pentru efectuarea analizei.

Pentru a exclude cazurile de pierdere a datelor şi a menţine continuitatea lor registrele evenimentelor se păstrează în arhive, ce nu depăşesc dimensiunea spaţiului liber destinat acestor fişiere. Din acest moment ele sunt considerate inactive şi accesul la ele este posibil doar dintr-un sistem aparte.

Registrele se păstrează minim pentru perioada prevăzută de cadrul normativ.

5.4.4 PROTECŢIA REGISTRELOR EVENIMENTELOR

Registrele evenimentelor sunt arhivate şi stocate conform cerinţelor bazei normative în domeniul semnăturii electronice şi procedurilor interne ale Prestatorului.

Înainte de arhivare registrele evenimentelor sunt supuse vizualizării de către administratorul de securitate, administratorul de sistem sau auditor.

Accesul la registrele evenimentelor are loc astfel:

- doar persoanele care au legătură cu grupurile de utilizatori sus-menţionate au acces la conţinutul registrelor;
- doar administratorul de securitate poate arhiva sau şterge (după arhivare) registrele evenimentelor;
- este verificată, după posibilitate, integritatea registrelor, a înscrierilor conţinute în acestea cu privire la modificări şi anomalii;
- nici unul din ei nu are dreptul de a modifica înscrierile ce indică evenimentul ce a avut loc în sistem.

În plus, sunt prevăzute măsuri ce împiedică ştergerea copiilor de arhivă pînă la sfîrşitul perioadei lor de păstrare.

5.4.5 PROCEDURI APLICATE ÎN PROCESUL DE ARHIVARE A REGISTRELOR EVENIMENTELOR

Procedurile Prestatorului presupun anumite acţiuni în procesul de arhivare a registrelor evenimentelor. Aceste acţiuni trebuie reflectate în mod obligator în registre pe suport de hîrtie (sau alte suporturi) în prezenţa nemijlocită a administratorului de securitate, a administratorului de sistem şi a auditorului. Pe lîngă aceasta, este analizat conţinutul registrelor, sunt culese datele statistice despre evenimente şi analizate, sunt determinate locurile vulnerabile ale sistemului. Toate datele sunt formate ca raport şi sunt anexate la înscrieri în registru.

5.4.6 SISTEMUL AUDIT COLLECTION (INTERN VS EXTERN)

Datele de control automatizate sunt generate şi înregistrate în aplicaţii, la nivel de reţea şi sisteme de operare, iar cele generate manual sunt înregistrate de administratorul de securitate.

5.4.7 NOTIFICAREA PERSOANELOR RESPONSABILE DESPRE EVENIMENTE

Sistemul de analiză a evenimentelor funcţionează în regim automatizat, colectînd şi analizînd datele de intrare în regim de timp real şi, în caz de depistare a evenimentelor critice (depistarea intruziunii nesancţionate, defect al sistemului, refuz în deservire, deranjamente ale sistemului de alimentare cu energie electrică etc.), asigură notificarea automată a administratorului de securitate şi a altor persoane responsabile despre evenimentul ce a avut loc. Sistemul de notificări înştiinţează persoanele cu funcţii de răspundere conform participării şi atribuţiilor funcţionale. De exemplu, dacă a fost depistată o încercare de intruziune nesancţionată în sistem notificarea este trimisă administratorului de securitate, în cazul defecţiunii echipamentului sau a sistemului de alimentare cu energie electrică este notificat administratorul de sistem.

Informaţia despre evenimentele critice este transmisă persoanelor responsabile prin intermediul mijloacelor de comunicaţii securizate, a telefonului mobil, a poştei electronice.

Colaboratorii care au primit astfel de notificări sunt obligaţi să întreprindă măsurile corespunzătoare pentru a soluţiona problema creată.

5.4.8 EVALUAREA PUNCTELOR VULNERABILE ALE SISTEMULUI

Evaluarea punctelor vulnerabile ale sistemului este necesară pentru a asigura funcţionarea completă a tuturor sistemelor Prestatorului, a avertiza intrarea nesancţionată în sistem şi utilizarea resurselor lui în scopuri ilegale. Astfel sunt necesare măsuri de evaluare pentru a determina punctele cu un grad ridicat de risc, ce apar în sistem, în dependenţă de configurarea echipamentului, a tipurilor mijloacelor de program aplicate. Aceste măsuri pot fi efectuate pentru toate procedurile şi configuraţiile interne şi externe, aplicate de Prestator. Pentru desfăşurarea acestor măsuri pot fi implicaţi colaboratori autorizaţi de Prestator pentru a efectua auditul şi analiza punctelor vulnerabile ale sistemului.

Auditorul este responsabil de realizarea auditului intern cu scop de control a stării sistemelor şi corespunderea cu cerinţele CPP şi alte documente interne, realizînd operaţii de creare a copiilor de rezervă ale registrelor.

Desfăşurarea auditului sistemelor de securitate are loc în conformitate cu cerinţele stabilite în **ISO/IEC 13355** ***Guidelines for Management of IT Security*** şi **ISO/IEC 17799** ***Code of Practice for Information Security Management***.

5.5. ARHIVAREA ÎNSCRIERILOR

Toate datele ce au legătură cu buna funcţionare a Prestatorului, securitatea sistemelor, cererile parvenite din partea utilizatorilor, informaţia despre titulari, publicarea certificatelor, listele certificatelor revocate, cheile utilizate, cît şi toată corespondenţa Prestatorului cu utilizatorii sunt supuse copierii de rezervă şi arhivării.

Prestatorul realizează gestiunea a două tipuri de arhive: arhive accesibile în regim on-line (arhive on-line) şi arhive accesibile în regim off-line (arhive off-line).

Certificatele valide ale titularilor (publicate cu cel mult 15 ani înainte de data curentă) sunt păstrate în arhive on-line ale certificatelor active şi pot fi folosite pentru realizarea anumitor tipuri de operaţii interne, de exemplu, pentru verificarea valabilităţii certificatului.

Arhivele off-line se folosesc pentru păstrarea certificatelor (inclusiv certificatele revocate), publicate în perioada de la **15** la **20 ani** înainte de data curentă. Arhivele conţin documentele corespunzătoare certificatelor, semnate (în trecut) de către utilizator (în format electronic).

Datele de arhivă sunt criptate şi asupra acestora se aplică marca temporală. Cheile, folosite pentru criptarea şi semnarea acestor date, sunt gestionate şi accesibile administratorului de securitate.

5.5.1 TIPURILE DE DATE SUPUSE ARHIVĂRII

Arhivării şi păstrării obligatorii sunt supuse următoarele date:
a) informaţia despre efectuarea controalelor mijloacelor ce asigură securitatea (primită din rapoartele auditului), protecţia logică şi fizică a Prestatorului şi informaţia ce se păstrează în Depozit;
b) cererile şi datele primite în format electronic de la utilizator sau trimise acestuia sub formă de fişiere sau mesaje electronice;
c) baza de date a certificatelor;
d) listele certificatelor revocate publicate;
e) istoria cheilor Prestatorului din momentul generării şi pînă la momentul nimicirii;
f) corespondenţa internă şi externă (pe suport de hîrtie şi/sau în format electronic, după caz) între Prestator, utilizatori şi părţile de încredere în ce priveşte suspendarea valabilităţii certificatelor şi activarea repetată a lor;
g) documente şi date folosite în procesul de identificare a identităţii, parte componentă a pachetului de documente depus pentru prestarea serviciilor de certificare.

5.5.2 FRECVENŢA DE ARHIVARE A DATELOR

Arhivarea bazei de date a certificatelor, a listelor certificatelor revocate, a corespondenţei electronice şi cererile titularilor, la fel şi răspunsurile la cereri, se păstrează la Prestator şi sunt arhivate cu o frecvenţă recomandată de bunele practici şi care nu contravin prevederilor cadrului normativ.

5.5.3 TERMENELE DE PĂSTRARE A DATELOR DE ARHIVĂ

Datele de arhivă (în format electronic şi/sau pe hîrtie) se păstrează pentru o perioadă de cel puţin 15 ani de la data revocării sau expirării certificatului cheii publice, în eventualitatea unor litigii.

La expirarea perioadei de păstrare datele de arhivă trebuie nimicite prin distrugere fizică, elaborînd actul corespunzător, şi în prezenţa comisiei, în componenţa căreia obligatoriu intră administratorul de certificare şi administratorul de securitate.

5.5.4 PROTECŢIA ARHIVELOR

Protecţia arhivelor Prestatorului are loc prin accesul la arhive doar a colaboratorilor autorizaţi. Datele arhivate electronic sunt protejate de acces fizic şi logic, de vizualizarea nesancţionată, de modificarea sau ştergerea prin intermediul controalelor. Purtătorii, pe care sunt arhivate datele şi aplicaţiile corespunzătoare de prelucrare a datelor, sunt menţinuţi încît să fie accesibili în intervalul de timp stabilit în pct. 5.5.3.

5.5.5 PROCEDURILE COPIERII DE REZERVĂ

Copiile de arhivă permit restabilirea completă (e.g., după căderea sistemului) a tuturor datelor necesare pentru funcţionarea corectă a Prestatorului. Întru asigurarea acestor scopuri sunt supuse copierii de rezervă următoarele aplicaţii şi fişiere:

a) purtătorii de informaţie ce conţin pachete de instalare a aplicaţiilor de sistem şi ale sistemelor;
b) purtătorii de informaţie ce conţin mijloacele de program ale Prestatorului;
c) serverele web;
d) certificatele şi Listele certificatelor revocate;
e) datele despre utilizatorii şi colaboratorii Prestatorului;
f) registrele evenimentelor.

Metodele de creare a copiilor de rezervă trebuie să asigure posibilitatea de restabilire rapidă a datelor şi sistemelor în cazul pierderii sau deteriorării lor. Prestatorul aplică următoarele două metode:

A. copierea de rezervă ce are loc zilnic şi poate fi utilizată în cazul restabilirii rapide a datelor pierdute;

B. copierea de rezervă pentru asigurarea restabilirii rapide a configuraţiilor şi setărilor echipamentului şi a mijloacelor de program. Aceste copii permit protejarea şi restabilirea funcţionalităţii serverelor de bază. 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.

Descrierea detaliată a procedurilor de creare a copiilor de rezervă şi de restabilire a sistemelor după deteriorare se găseşte în documentele Prestatorului cu clasa de securitate C2.

5.5.6 CERINŢE DE APLICARE A MĂRCII TEMPORALE PE ÎNSCRIERE

Prezentul CPP recomandă aplicarea mărcii temporale în procesul de creare a arhivei sau a copiei de rezervă. Marca temporală se creează cu ajutorul Serviciului de marcare temporală (**Time Stamp Authority - TSA**). Pentru aceasta este nevoie de certificatul emis în aceste scopuri.

5.5.7 SISTEMUL ARCHIVE COLLECTION

Nu se aplică.

5.5.8 PROCEDURILE DE ACCES ŞI DE VERIFICARE A INFORMAŢIEI DE ARHIVĂ

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 de securitate.

5.6. ARHIVAREA DOCUMENTAŢIEI PE SUPORT DE HÎRTIE

Documentele pe suport de hîrtie, obţinute ca rezultat al prestării serviciilor de certificare, urmează a fi arhivate în conformitate cu prevederile cadrului normativ despre arhivarea documentelor.

Perfectarea dosarelor trebuie să corespundă următoarelor cerinţe:

- documentele din dosar sunt sortate în ordine cronologică;
- completarea datelor pe prima copertă a dosarului;
- dosarele conţin sechestrul intern al documentelor supuse arhivării;
- dosarele nu conţin duplicate, maculatoare, file nescrise, ace, agrafe, clame;
- numerotarea filelor dosarelor se începe cu numărul „1";

- se numerotează în colţul din dreapta, jos, cu pix negru;
- fiecare dosar conţine nu mai mult de 250 file;
- coaserea dosarelor trebuie să asigure citirea completă a textului şi datelor.

Certificarea dosarului: pe o filă nescrisă, adăugată la sfârşitul dosarului se face următoarea certificare: "*Prezentul dosar conţine ..... file (în cifre şi, în paranteze, în litere)*". Se indică data când a fost efectuată certificarea şi semnătura executantului.

Documentele arhivate sunt transmise în arhiva Instituţiei, termenul de păstrare al acestora fiind reglementat de cadrul normativ.

5.7. SCHIMBAREA CHEILOR

Schimbarea cheilor publice şi private ale Prestatorului are loc conform pp. 18-22 din *Normele tehnice*.

5.8. ÎNCĂLCAREA SECURITĂŢII CHEILOR ŞI RESTABILIREA DUPĂ AVARIE

5.8.1 PROCEDURI ÎN CAZ DE COMPROMITERE A CHEILOR SAU DE SUSPICIUNE DE COMPROMITERE A CHEILOR PRESTATORULUI DE SERVICII DE CERTIFICARE

La depistarea sau existenţa suspiciunilor de compromitere a cheilor private ale Prestatorului, trebuie efectuate următoarele acţiuni:

- toţi utilizatorii semnăturii electronice sunt notificaţi imediat despre compromiterea cheilor prin mijloace de informare în masă şi prin poşta electronică;
- toate certificatele cheilor publice emise de Prestator, prin intermediul certificatului cheii publice compromis, corespunzător cheii private compromise, sunt revocate cu indicarea cauzei compromiterii;
- Prestatorul generează o nouă pereche de chei şi primeşte un nou certificat al cheii publice;
- titularilor le sunt emise noi certificate ale cheilor publice;
- distribuirea noilor certificate ale titularilor are loc fără perceperea unei sume de bani suplimentare.

5.8.2 DETERIORAREA RESURSELOR INFORMAŢIONALE, A MIJLOACELOR DE PROGRAM SAU A DATELOR

Regulile de securitate, aplicate de Prestator, prevăd diferite situaţii la apariţia cărora trebuie menţinută funcţionarea acestuia şi nivelul garantat de prestare a serviciilor:

- *deteriorare fizică a sistemelor de computer, inclusiv infrastructura de reţea şi de cablu* – ca rezultat al apariţiei situaţiei de avarie;
- *deranjamente ale mijloacelor de program, imposibilitatea accesului la date* – ca rezultat al deteriorării mediului sistemelor informaţionale, a aplicaţiilor utilizatorilor sau a executării altor programe, cum ar fi viruşii, „troianul";
- *pierderea (stoparea, inaccesibilitatea) serviciilor de reţea importante prestate*– în primul rînd aceasta ţine de alimentarea cu energie sau deteriorări ale conexiunilor de reţea;

- *deteriorarea parţială a reţelei interne, utilizată de Prestator cu scop de prestare a serviciilor* – poate servi obstacol pentru utilizatori şi duce la refuz în deservire.

O listă mai completă se conţine în documentul *Planul de gestionare a riscurilor*.

Pentru prevenirea şi reducerea la minim a ameninţărilor sus-menţionate sunt prevăzute următoarele măsuri:

- **Planul de restabilire în cazul calamităţilor şi a situaţiilor de avarie**

Toţi titularii şi părţile de încredere sunt notificaţi, în perioade de timp minime şi în corespundere cu gravitatea situaţiei apărute, despre fiecare caz de deteriorare sau refuz în deservire, asociată cu sistemul informaţional corespunzător. Planul de restabilire descrie un şir de proceduri, ce previn compromiterea sistemului (defectarea, modificarea etc.), şi implică întreprinderea următoarelor măsuri:

- periodic, conform procedurilor, sunt create copii de rezervă a bazelor de date. Copiile includ toate cererile primite, certificatele publicate, revocate şi restabilite. Ultimele copii se păstrează atît la Prestator, cît şi în afara amplasării lui;
- periodic, urmînd procedurile, sunt create copii de rezervă ale datelor din fiecare resursă informaţională. Aceste copii conţin toate cererile primite, înscrierile din registrele evenimentelor, toate tipurile de certificate, inclusiv cele revocate. Ultimele copii se păstrează atît la Prestator, cît şi în afara amplasării lui;
- cheile private ale Prestatorului, în conformitate cu procedurile de asigurare a confidenţialităţii, sunt împărţite cîtorva persoane de încredere care le păstrează;
- sistemele de restabilire după avarie sunt testate pe fiecare componentă de sistem cel puţin o dată pe an. Aceste teste sunt parte a auditului intern al sistemului.

- **Verificarea modificărilor**

Instalarea sau reînnoirea mijloacelor de program pînă la cele mai actuale versiuni este posibilă doar în cazul testărilor intensive, în strictă corespundere cu procedurile stabilite în documentaţia aferentă mijloacelor de program. Fiecare modificare a sistemului necesită permisiunea şi confirmarea administratorului de securitate. În cazul pierderii datelor după instalarea unei noi componente a sistemului se aplică planul de restabilire după avarie a sistemului deteriorat pînă la starea anterioară deteriorării.

- **Situaţii de avarie**

În cazul situaţiilor de avarie şi nefuncţionalitate a sistemelor Prestatorului timp de 24 ore din momentul pornirii programului de restabilire după avarie toate sistemele trebuie restabilite şi accesibile pentru verificare completă pentru a fi lansate. Respectarea strictă şi cu regularitate a *Procedurilor de restabilire a activităţii Centrului de certificare a cheilor publice* permite restabilirea sistemului după starea la momentul apariţiei acestei situaţii. Cererile parvenite în perioada nefuncţionalităţii sistemelor de bază sunt prelucrate şi păstrate pe serverele de rezervă ajutătoare, ce funcţionează în regim de "schimb fierbinte". În scop de evitare a situaţiilor de acest gen Prestatorul întreprinde următoarele măsuri:

- includerea automată (posibil şi un control manual) în lucru a sistemelor de înlocuire;
- prelucrarea şi acumularea cererilor parvenite în regimul de timp real pînă la restabilirea sistemului de bază;
- prelucrarea cererilor parvenite si acumulate, dar neprelucrate în perioada situaţiei critice.

- **Posibilităţi suplimentare**

Pentru a preveni deteriorarea sistemului din cauza alimentării cu energie şi continuarea funcţionării se folosesc sistemele UPS şi electrogeneratoarele Diesel, ce se află în stare de disponibilitate de a ieşi în regim de lucru timp de 30 secunde. În plus, serverele de bază ale Prestatorului se alimentează cu energie electrică de la cîteva substaţii, fizic amplasate în diferite raioane administrative ale oraşului. Tot echipamentul de alimentare cu energie de rezervă este testat cel puţin o data la şase luni, fapt ce se înregistrează în registrul evenimentelor.

5.8.3 PROCEDURI ÎN CAZ DE COMPROMITERE A CHEILOR SAU DE SUSPICIUNE DE COMPROMITERE A CHEILOR UTILIZATORILOR

În cazul compromiterii cheilor sau de suspiciune de compromitere a cheilor utilizatorilor se aplică procedurile descrise în secţiunea 4.9 *Revocarea şi suspendarea valabilităţii certificatului cheii publice* a CPP.

5.8.4 RESTABILIREA SECURITĂŢII DUPĂ STAREA DE AVARIE

La finisarea procedurilor de restabilire a sistemului după avarie administratorul de securitate, administratorul de sistem, administratorul de certificare sau administratorul de înregistrări trebuie:

- să schimbe toate parolele utilizate anterior;
- să şteargă drepturile de acces la sistem şi la resursele lui, utilizate anterior;
- să schimbe toate codurile şi PIN, asociate cu accesul fizic la componentele sistemului;
- conform regulilor de securitate în reţea a Prestatorului toate componentele de reţea şi regulile de acces fizic trebuie revizuite;
- să informeze despre restabilirea funcţionalităţii sistemului.

5.9. ÎNCETAREA ACTIVITĂŢII PRESTATORULUI DE SERVICII DE CERTIFICARE

Procedura privind încetarea activităţii Prestatorului este prevăzută de cadrul normativ.

6. CONTROLUL TEHNIC AL SECURITĂŢII

6.1. GENERAREA ŞI UTILIZAREA PERECHII DE CHEI

În procesul de administrare a cheilor se aplică proceduri ce asigură păstrarea lor securizată şi utilizarea de către titular.

O atenţie deosebită se acordă proceselor de generare şi protecţie a cheilor private ale Prestatorului, compromiterea cărora poate influenţa tot domenul de certificare.

Prestatorul este titularul certificatului cheii publice emis de Prestatorul superior. Cheia privată, corespunzătoare cheii publice certificate, este folosită doar în scopuri de semnare a certificatelor cheilor publice ale utilizatorilor şi a Listei certificatelor revocate.

Crearea şi verificarea semnăturii electronice avansate calificate are loc în conformitate cu Capitolul IV al *Normelor tehnice*.

În restul cazurilor Centrul de certificare are atît rolul de Prestator de servicii de certificare de nivel superior, cît şi de Prestator de servicii de certificare de nivelul doi.

6.1.1 CREAREA PERECHII DE CHEI PRIVATĂ ŞI PUBLICĂ

Cheile privată şi publică ale Prestatorului sunt create în încăperile şi pe echipamentul acestuia în prezenţa persoanelor împuternicite, dintre care una este în mod obligator administratorul de securitate.

Cheile Prestatorului sunt păstrate pe dispozitivul securizat de creare şi verificare a semnăturii electronice (module de securitate hardware Hardware Security Module - HSM) corespunzătoare cerinţelor FIPS 140-2 nivelul 3 şi deţin avizul pozitiv al organului competent.

Paşii realizaţi în procesul de creare a cheilor sunt înscrişi obligator în registrul evenimentelor, se indică data creării şi se semnează toate persoanele prezente. Înscrierile se păstrează pentru auditul sistemului şi al certificatelor cheilor publice.

În cazul semnăturii electronice avansate calificate cheia privată a utilizatorului este generată de Prestator pe un dispozitiv securizat de creare a semnăturii electronice. Cheia publică corespunzătoare cheii private a utilizatorului este certificată de către Prestator. Procedurile respective au loc în conformitate cu cerinţele standardului *FIPS 140-2 Security Requirements For Cryptographic Modules, nivelele 3 sau 4*, sau *SMV CWA 14169:2008 Dispozitive de siguranţă pentru crearea semnăturilor „EAL4+"* sau *SM ISO/CEI 19790:2014 Tehnologia informaţiei. Tehnici de securitate. Cerinţe de securitate pentru module criptografice*.

În cazul semnăturii electronice avansate necalificate cheia privată a utilizatorului este generată fie de Prestator, fie de utilizator pe un dispozitiv securizat de creare a semnăturii electronice. Cheia publică corespunzătoare cheii private a utilizatorului este certificată de către Prestator. Procedurile respective au loc în conformitate cu cerinţele standardului *FIPS 140-2 Security Requirements For Cryptographic Modules, nivelele 3 sau 4*, sau *SMV CWA 14169:2008 Dispozitive de siguranţă pentru crearea semnăturilor „EAL4–"* sau *SM ISO/CEI 19790:2014 Tehnologia informaţiei. Tehnici de securitate. Cerinţe de securitate pentru module criptografice*.

În celelalte situaţii Prestatorul este cel care generează perechea de chei publică şi privată, certifică cheia publică şi transmite utilizatorului fişierul în format PKCS#12.

6.1.2 TRANSMITEREA CHEII PRIVATE UTILIZATORULUI

În dependenţă de domeniul de utilizare a cheii private, aceasta se transmite utilizatorului personal sau prin intermediul persoanei responsabile, după cum urmează:

- în format PKCS#11 pentru semnătura electronică avansată calificată,
- în format PKCS#11 pentru semnătura electronică avansată necalificată,
- în format PKCS#11 sau PKCS#12 pentru semnătura electronică simplă (autentificare şi servicii de securitate),
- în format PKCS#12 în cazul sistemelor informaţionale ce urmează a fi integrate cu serviciile electronice guvernamentale (MSign, MPass, MLog etc.)

6.1.3 TRANSMITEREA CHEII PUBLICE CĂTRE PRESTATORUL DE SERVICII DE CERTIFICARE

În cazul în care utilizatorul îşi generează singur perechea de chei publică şi privată, cu excepţia perechii de chei pentru semnătura electronică avansată calificată, acesta prezintă spre certificare cheia publică în format PKCS#10.

6.1.4 RĂSPÎNDIREA CHEILOR PUBLICE DE CĂTRE PRESTATORUL DE SERVICII DE CERTIFICARE

Cheile publice certificate de Prestator se răspîndesc ca certificate conform recomandărilor ITU-T X.509 v.3.

Prestatorul răspîndeşte cheile sale publice pe două căi diferite:

– publicînd certificatele în Depozit;
– împreună cu mijloacele de program (browsere, clienţi de poştă electronică etc.), ce permit utilizarea serviciilor prestate de Prestator.

Prestatorul realizează transmiterea lanţului de certificare integru către titular.

6.1.5 LUNGIMEA CHEILOR

În cazul semnăturii electronice avansată calificată lungimea cheilor este determinată de *Normele tehnice*, în celelalte cazuri aceasta se determină de actele normative interne ale Prestatorului.

6.1.6 PARAMETRII CHEILOR PUBLICE ŞI VERIFICAREA CALITĂŢII PARAMETRILOR

În prezentul CPP nu sunt stipulate cerinţe faţă de parametrii cheilor publice. În acest sens Prestatorul utilizează recomandările minimale posibile pentru cheile **RSA**, descrise în "***Algorithms and Parameters for Secure Electronic Signatures***". Stabilirea parametrilor în procesul de creare a cheilor are loc conform standardului ***FIPS PUB 140-2 Security Requirements For Cryptographic Module, nivelele 3 sau 4***, sau ***SMV CWA 14169:2008 Dispozitive de siguranţă pentru crearea semnăturilor „EAL4+"*** sau ***SM ISO/CEI 19790:2014 Tehnologia informaţiei. Tehnici de securitate. Cerinţe de securitate pentru module criptografice.***

6.1.7 SCOPURILE DE UTILIZARE A CHEILOR (ÎN CONFORMITATE CU X.509 V3)

Pentru certificatele X.509, versiunea 3, Prestatorul completează cîmpul *KeyUsage* (utilizarea cheii) din certificate în conformitate cu ***RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile***, mai 2008.

*Utilizarea valorilor cîmpului **KeyUsage** trebuie să corespundă următoarelor:*

a) **digitalSignature** certificatul cheii publice este destinat pentru verificarea semnăturii electronice, creată în scopuri diferite de pct. b), g) şi h);
b) **nonRepudiation** certificatul cheii publice este destinat pentru utilizarea mijloacelor de non-repudiere pentru persoane fizice şi în alte scopuri, indicate în pct. f) şi g);
c) **keyEncipherment** certificatul cheii publice este destinat pentru criptarea cheilor simetrice, asigurînd confidenţialitatea datelor;
d) **dataEncipherment** certificatul cheii publice este destinat pentru criptarea datelor utilizatorului, excluzînd pct. c) şi e);
e) **keyAgreement** certificatul cheii publice este destinat pentru utilizarea cu protocoalele de verificare a cheilor;
f) **keyCertSign** cheia publică a certificatului poate fi utilizată pentru verificarea semnăturii în certificatele emise de Prestator;
g) **cRLSign** cheia publică a certificatului poate fi utilizată pentru verificarea certificatelor revocate şi suspendate şi a listelor certificatelor revocate, emise de Prestator;
h) **encipherOnly** certificatul poate fi folosit în conformitate cu pct. e), indicînd posibilitatea criptării datelor utilizînd protocolul de verificare a cheilor;
i) **decipherOnly** certificatul poate fi folosit în conformitate cu pct. e), indicînd posibilitatea decriptării datelor prin utilizarea protocolului de verificare a cheilor.

6.1.8 METODELE SOFTWARE ŞI/SAU HARDWARE DE CREARE A CHEILOR

Cheile privată şi publică ale Prestatorului sunt create prin metoda hardware.

Cheile privată şi publică ale utilizatorului, utilizate la crearea semnăturii electronice avansate ne-/calificate, sunt create prin metoda hardware; cheile privată şi publică ale utilizatorului, utilizate pentru autentificare şi servicii de securitate sau pentru sisteme informaţionale, sunt create prin metoda software.

6.2. PROTECŢIA CHEILOR PRIVATE ŞI CONTROLUL INGINERESC AL MODULILOR CRIPTOGRAFICI

Pentru asigurarea securităţii cheilor publice ale Prestatorului a aplicat totalitatea măsurilor de control fizic, logic şi procedural.

Utilizatorii trebuie să respecte regimul de exploatare a mijloacelor de program stabilit de *Ghidul utilizatorului semnăturii electronice.*

6.2.1 STANDARDE PENTRU MODULELE CRIPTOGRAFICE

Pentru crearea cheilor Prestatorului, dar şi crearea cheilor utilizatorului se foloseşte modulul criptografic corespunzător cerinţelor prevăzute în *Normele tehnice* şi care deţine avizul pozitiv al organului competent.

6.2.2 PARTAJAREA ŞI DISTRIBUIREA CHEII PRIVATE

În cazul rolurilor concomitente ale Prestatorului de RootCA şi SubRootCA acesta practică partajarea şi distribuirea cheii private mai multor persoane de încredere, astfel încît pentru restabilirea acesteia este necesară prezenţa a cel puţin două persoane de încredere care deţin părţi din cheie. Dacă numărul părţilor este prea mic cheia privată nu poate fi restabilită.

6.2.3 DEPOZITAREA CHEII PRIVATE

Nu se aplică.

6.2.4 ARHIVAREA CHEII PRIVATE

La expirarea perioadei de valabilitate cheile private ale autorităţilor de certificare sunt arhivate pe o perioadă de 20 ani, fiind stocate pe module criptografice hardware, după care sunt nimicite.

6.2.5 TRANSFERUL CHEII PRIVATE ÎN SAU DIN MODULUL CRIPTOGRAFIC

Cheile privată şi publică ale Prestatorului sunt create pe modulul de securitate hardware.

6.2.6 METODE DE ACTIVARE A CHEII PRIVATE

Datele de activare a cheii private se folosesc pentru autorizarea utilizatorului semnăturii electronice şi pentru controlul accesului la cheia privată.

Datele de activare sunt folosite în două cazuri:

- ca element al procedurii de autentificare ce se bazează pe unul sau mai mulţi factori (parola, cod PIN etc);
- ca parte a cheii private distribuite.

Cheile private ale Prestatorului sunt activate după crearea lor sau repunerea în funcţiune în modulul criptografic. Activarea cheilor private este realizată de administratorul de securitate sau persoana împuternicită, după caz.

Autentificarea întotdeauna se bazează pe verificarea împuternicirilor indicate pe cartela de identificare, aflată permanent la administratorul de securitate. După introducerea cartelei în cititorul de cartelă se cere codul **PIN**; în acest caz se subînţelege că pînă la scoaterea cartelei din cititor cheile private sunt în stare activă.

Alte chei private, de exemplu, folosite cu scop de autentificare sau creare a conexiunii securizate, pot fi automat activate pe perioada de creare a sesiunii securizate, imediat după autentificarea utilizatorului. Închiderea sesiunii duce la dezactivarea imediată a tuturor cheilor activate mai devreme.

6.2.7 METODE DE DEZACTIVARE A CHEII PRIVATE

Metodele de dezactivare a cheilor private sunt folosite ca urmare a terminării sesiunii de utilizare a cheilor private. Cheile private pot fi dezactivate după fiecare procedură prin închiderea sesiunii de lucru sau scoaterea cartelei din cititorul de cartelă, în dependenţă de mecanismul de autentificare utilizat.

Cheile private ale Prestatorului sunt dezactivate în momentul scoaterii cartelei din cititor de către administratorul de certificare.

În caz că perioada de valabilitate a cheilor a expirat sau cheile au fost revocate, sau este necesară suspendarea tehnologică a sistemului, dezactivarea este efectuată doar de către administratorul de securitate.

Fiecare procedură de dezactivare a cheilor private trebuie să se reflecte în registrul evenimentelor.

6.2.8 METODE DE DISTRUGERE (NIMICIRE) A CHEII PRIVATE

Prestatorul nimiceşte cheile sale private prin metoda ce garantează inexistenţa părţilor de cheie ce ar putea permite restabilirea ei. Nimicirea cheilor private implică ştergerea lor completă de pe purtător sau distrugerea completă a purtătorului în cazul defectării cartelei şi a imposibilităţii nimicirii datelor prin metode obişnuite, cu scop de prevenire a accesului la date chiar şi pe cartela deteriorată.

Procesul este realizat de o comisie în componenţa căreia intră colaboratori ai Prestatorului şi, după caz, ai organului competent.

Fiecare procedură de nimicire a cheilor private este înscrisă în registrul evenimentelor.

6.2.9 EVALUAREA MODULULUI CRIPTOGRAFIC

Modulele criptografice din cadrul Prestatorului sunt în conformitate cu cerinţele standardului *FIPS 140-2 Security Requirements For Cryptographic Modules, nivelele 3 sau 4*, sau *SMV CWA 14169:2008 Dispozitive de siguranţă pentru crearea semnăturilor „EAL4+"* sau *SM ISO/CEI 19790:2014 Tehnologia informaţiei. Tehnici de securitate. Cerinţe de securitate pentru module criptografice*.

Evaluarea conformităţii modulelor criptografice cu cerinţele prevăzute de cadrul normativ se realizează de organul competent.

6.3. ALTE ASPECTE DE ADMINISTRARE A CHEILOR

6.3.1 ARHIVELE CHEILOR PUBLICE

Certificatele cheilor publice ale Prestatorului şi certificatele utilizatorilor sunt supuse stocării şi arhivării.

Destinaţia de bază a arhivelor cheilor publice o reprezintă posibilitatea de a verifica semnătura electronică după ştergerea certificatului din Registru. Această operaţie este foarte importantă în prestarea serviciului de non-repudiere, de exemplu, marcarea temporală, sau a serviciului de verificare a statutului certificatului cheii publice.

Prestatorul realizează arhivarea certificatelor cheilor publice în baza certificatelor emise utilizatorilor. Cheile publice ale Prestatorului sunt arhivate împreună cu cheile private corespunzătoare.

Certificatele mai pot fi arhivate local de către utilizatori, dacă aplicaţia ce le utilizează permite (necesită) aceasta. De exemplu, clienţii de e-mail ai utilizatorilor.

Arhivele cheilor publice trebuie protejate de adăugarea, modificarea sau extragerea nesancţionată a cheilor din arhiva creată. Asigurarea integrităţii acestora are loc prin intermediul semnării arhivelor şi controlul accesului la acestea.

În cadrul domenului Prestatorului sunt arhivate certificatele utilizate pentru verificarea semnăturii electronice, celelalte tipuri de certificate fiind păstrate cel puţin 15 ani de la data revocării sau expirării.

Administratorul de securitate verifică integritatea arhivelor cheilor publice lunar. Această procedură se efectuează cu scop de verificare a funcţionalităţii, integrităţii arhivelor şi a faptului că certificatele, stocate în arhivă, nu sunt modificate.

Cheile publice, stocate în arhivele cheilor publice, sunt păstrate **20 ani** (conform Secţiunii 5.5 din CPP). Fiecare procedură de nimicire a arhivelor cheilor publice este înscrisă în registrele evenimentelor respective.

6.3.2 TERMENUL DE VALABILITATE A CERTIFICATULUI ŞI PERIOADA DE UTILIZARE A CHEILOR PRIVATĂ ŞI PUBLICĂ

Termenul de valabilitate a certificatului cheii publice ia sfîrşit la expirarea perioadei de valabilitate a acestuia sau la revocarea certificatului.

Termenul de valabilitate a certificatului cheii publice, corespunzătoare cheii private, constituie:

20 ani – pentru Prestatorul de nivel superior;

10 ani – pentru Prestator;

până la 2 ani inclusiv – pentru utilizatori (lungimea cheii publice minimum de 2048 biţi, pentru algoritmul RSA);

până la 3 ani inclusiv – pentru lungimea cheilor publice şi private minimum de 3072 biţi, pentru algoritmul RSA;

până la 5 ani – pentru lungimea cheilor publice şi private minimum de 4096 biţi, pentru algoritmul RSA.

Termenul de valabilitate a cheii private constituie:

10 ani -- pentru Prestatorul de nivel superior;

5 ani – pentru Prestator;

până la 2 ani inclusiv – pentru utilizatori (lungimea cheii private minimum de 2048 biţi, pentru algoritmul RSA);

până la 3 ani inclusiv – pentru lungimea cheilor publice şi private minimum de 3072 biţi, pentru algoritmul RSA;

până la 5 ani – pentru lungimea cheilor publice şi private minimum de 4096 biţi, pentru algoritmul RSA.

Începutul termenului de valabilitate a cheii private se consideră data şi ora începutului termenului de valabilitate a certificatului cheii publice corespunzătoare.

6.4. ACTIVAREA DATELOR

Datele de activare se folosesc pentru activarea cheilor private. Deasemenea sunt folosite pentru intensificarea controlului şi a nivelului garantat de autentificare a utilizatorului la accesarea cheilor private.

6.4.1 CREAREA ŞI UTILIZAREA DATELOR DE ACTIVARE

Datele de activare, folosite pentru protecţia purtătorilor ce conţin cheile private, inclusiv în cazul cheilor private distribuite, sunt create conform ***FIPS-112 Password Usage***.

Principiile de bază de alegere a parolelor prevăd că parolele trebuie:

- să fie create de utilizator;
- să aibă lungimea minimă de 8 caractere;
- să conţină cel puţin 1 caracter alfabetic şi 1 caracter cifric;
- să conţină măcar o minusculă;
- să nu conţină acelaşi caracter decît o singură dată;
- să nu coincidă cu parola profilului administratorului;
- să nu conţină o parte a profilului utilizatorului.

Prestatorul recomandă utilizarea a doi şi mai mulţi factori de autentificare (cartelă şi parolă, biometrie şi parolă sau biometrie şi cartelă).

6.4.2 PROTECŢIA DATELOR DE ACTIVARE

Metodele de protecţie a datelor de activare depind de scopul de utilizare a datelor: pentru autentificare şi controlul accesului la cheia privată sau pentru restabilirea cheii private „distribuite".

În cazul autentificării, datele de activare sunt protejate conform ***FIPS-112 Password Usage***. În cazul cheii private „distribuite" datele de activare sunt protejate conform ***FIPS 140 Computer Security standards that specify requirements for cryptographic modules.***

Utilizatorii de sine stătător trebuie să-şi păstreze datele de activare şi să semneze actul de luare la cunoştinţă a obligaţiunilor (responsabilităţilor) sale.

Prestatorul recomandă ca stocarea datelor de activare ale administratorilor şi ale utilizatorilor să se realizeze prin metode criptografice şi controlul accesului fizic, iar protecţia cheilor private să se realizeze prin utilizarea purtătorilor materiali şi a parolelor sigure. Tentativele de acces neautorizat la aceste dispozitive de păstrare trebuie să ducă la blocarea temporară a purtătorului de date. Datele de activare nu trebuie transmise niciodată împreună cu datele activate.

Prestatorul recomandă utilizarea a doi şi mai mulţi factori de autentificare (cartelă şi parolă, biometrie şi parolă sau biometrie şi cartelă).

6.4.3 ALTE ASPECTE ALE PROCESULUI DE ACTIVARE A DATELOR

Datele de activare protejază accesul la cheile private, păstrate pe dispozitive, şi trebuie modificate periodic.

Datele de activare pot fi arhivate.

6.5. CONTROLUL DE SECURITATE A COMPUTERELOR

Prestatorul îşi îndeplineşte funcţiile folosind sistemele de încredere (Trustworthy Systems).

6.5.1 CERINŢE TEHNICE SPECIFICE A SECURITĂŢII COMPUTERELOR

Prestatorul garantează că sistemele ce susţin mijloacele de program şi fişierele cu date ale Prestatorului sunt sisteme de încredere pentru prevenirea accesului nesancţionat. În plus, Prestatorul limitează accesul la servere pînă la persoanele care au temei pentru acces. Utilizatorii aplicaţiilor comune nu au drept de acces la serverul în stare de lucru.

Reţeaua de lucru a Prestatorului este separată logic de la alte componente. Această separare previne accesul la reţea, cu excepţia accesului prin intermediul anumitor aplicaţii.

Pentru protecţia reţelei de lucru de accesele intern şi extern şi pentru limitarea sferei şi sursei de activitate în reţea se foloseşte firewall. Prestatorul impune utilizarea parolei cu număr minim de caractere, cu combinarea caracterelor speciale, alfabetice şi cifrice.

Prestatorul schimbă periodic parolele.

Accesul direct la baza de date a Depozitului Prestatorului este limitat pînă la persoanele care au temei pentru acces.

6.5.2 EVALUAREA SECURITĂŢII COMPUTERELOR

Nivelele de securitate ale calculatoarelor corespund cerinţelor EAL 4 stipulate în ***ISO/IEC 15408-3:1999, Information technology – security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements***, prevederilor standardelor ***ISO 27001***, ***ETSI TS 101456 – Electronic Signatures and Infrastructures (ESI): Policy requirements for certification authorities issuing qualified certificates***; sistemele de calculatoare ale Prestatorului corespund cerinţelor descrise în ***Information Technology Security Evalution Criteria (ITSEC)***.

6.6. CONTROALE TEHNICE ALE CICLULUI DE VIAŢĂ

Destinaţia principală a acestui tip de control este urmărirea stării sistemului şi asigurarea integrităţii complexului tehnic de program.

6.6.1 CONTROALE SPECIFICE DEZVOLTĂRII SISTEMULUI

Implementarea sistemelor în cadrul Prestatorului are loc în conformitate cu standardele în vigoare. În procesul de implementare sunt implicaţi: platforma de test (cu lansarea ulterioară pe platforma de producere), personalul Prestatorului, utilizatori finali care vor folosi sistemul. Testele au loc după un scenariu predefinit. Datele de testare nu vor fi folosite în producere şi invers.

6.6.2 CONTROALE DE MANAGEMENT A SECURITĂŢII

Managementul securităţii se bazează pe anumite reguli şi/sau sisteme elaborate şi implementate de către Prestator în cadrul infrastructurii cheilor publice.

Sistemele şi regulile de control stabilite şi aplicate de Prestator urmăresc scopul de a asigura funcţionalitatea stabilită iniţial şi conformitatea nivelului de încredere cerut.

Administrarea sistemului de securitate presupune controlul direct şi verificarea corespunderii stării sistemului şi a integrităţii lui, controlul numerelor versiunilor şi verificarea originalităţii mijloacelor tehnice.

6.6.3 CONTROALE DE SECURITATE A CICLULUI DE VIAŢĂ

Nu se menţionează.

6.7. ADMINISTRAREA SECURITĂŢII DE REŢEA

Serverele şi staţiile de lucru de încredere, exploatate de Prestator, funcţionează în reţea locală multinivel.

Accesul, venit din Internet, la orice segment al reţelei este protejat prin software şi/sau hardware specializat, ce realizează funcţii de control a traficului, conform cerinţelor Instituţiei, de asemenea se realizează controlul accesului la anumite porturi (în aceste scopuri este activat sistemul de depistare a intruziunilor).

6.8. MARCA TEMPORALĂ

În cazul mesajelor între Prestator, centrele de înregistrări şi utilizatori se recomandă utilizarea mărcii temporale certificate.

Marca temporală, creată în sistemul Prestatorului, corespunde recomandărilor ***RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).***

7. PROFILURILE CERTIFICATULUI, A LISTEI CERTIFICATELOR REVOCATE ŞI OCSP

Profilurile certificatelor şi a listei certificatelor revocate (CRL) se creează conform formatului determinat în standardul ITU-T X509 v.3. Profilul OCSP este creat conform cerinţelor **RFC 6960** ***X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP***. Mai jos sunt analizate valorile cîmpurilor Certificatului, a Listei certificatelor revocate şi a răspunsurilor serverului OCSP, extensiile de bază şi alternative, elaborate pentru necesităţile Prestatorului.

7.1. PROFILUL CERTIFICATELOR

În conformitate cu standardul *ITU-T X509 v.3* certificatul cheii publice prezintă consecutivitatea următoarelor cîmpuri: primul – conţine corpul certificatului (**tbsCertificate**), al doilea – informaţie despre algoritmii utilizaţi pentru semnarea certificatelor (**signatureAlgorithm**) şi al treilea – semnătura electronică, creată în certificat de către Prestator (**signatureValue**).

7.1.1 VERSIUNEA CERTIFICATULUI

Certificatele cheilor publice sub formă de document electronic trebuie să corespundă cerinţelor standardului ***ITU-T X.509 versiunea 3***, standardului ***SMV ISO CEI 9594-8:2014 Information technology. Open Systems Interconnection. The Directory: Public-key and attribute certificate frameworks*** sau recomandării ***IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*** şi ***IETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile şi IETF RFC 3739 Qualified Certificates Profile***.

Structurile certificatelor cheilor publice ale Prestatorului şi ale utilizatorilor sunt prezentate în cap. 10 **Anexe**.

7.1.2 CÎMPURILE CERTIFICATULUI CHEII PUBLICE

7.1.2.1 CÎMPURILE DE BAZĂ ALE CERTIFICATULUI CHEII PUBLICE

Certificatul cheii publice constă din **cîmpuri** şi **extensii** (de bază – determinate de actele normative, şi alternative – determinate de Prestator).

Toate certificatele, emise de Prestator, au următoarele cîmpuri de bază, semnificaţiile cărora sunt stabilite corespunzător regulilor, indicate în tabelul de mai jos:

Cîmpurile de bază		
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Număr aleator
Issuer	Datele de identificare ale prestatorului de servicii de certificare, emitent al certificatului	CN = Denumirea certificatului prestatorului de servicii de certificare L = Localitatea S = Statul OU = Prestatorul de servicii de certificare, subdiviziunea persoanei juridice

		O = Denumirea persoanei juridice, IDNO C = Codul statului
Validity Period	Termen de valabilitate	Valabil de pe: "__" _____ 20__ oo:mm:ss GMT Valabil pînă la: "__" _____ 20__ oo:mm:ss GMT
Subject	Datele de identificare ale titularului certificatului	SERIALNUMBER = IDNP-ul utilizatorului Phone= Telefonul utilizatorului (după caz) T = Funcţia utilizatorului (după caz) CN = Numele, prenumele abonatului OU = Subdiviziunea persoanei juridice în care activează utilizatorul (după caz) O = Denumirea persoanei juridice, IDNO, în care activează utilizatorul (după caz) L = Localitatea de domiciliu S = Statul C = Codul statului
Public Key	Cheia publică	Cheia publică a utilizatorului
Signature Algorithm	Algoritmul de semnare a emitentului certificatului	Denumirea algoritmului semnăturii electronice a emitentului certificatului
Signature value	Semnătura electronică a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat

7.1.2.2 CÎMPURILE AUXILIARE ALE CERTIFICATULUI CHEII PUBLICE

Toate certificatele, emise de Prestator, au următoarele cîmpuri auxiliare, semnificaţiile cărora sunt stabilite corespunzător regulilor, indicate în tabelul de mai jos:

Cîmpurile auxiliare		
Key Usage	Utilizarea cheii	Irevocabilitate şi alte restricţii stabilite
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii privatea utilizatorului, corespunzătoare prezentului certificat
CRL Distribution Points	Punctul de distribuţie a listei certificatelor revocate	Sursa de publicare a listei certificatelor revocate
Subject AltName	Numele alternativ al titularului	RFC822=Poşta electronică a utilizatorului
Certificate Policies	Politica de certificare a prestatorului de servicii de certificare	Identificatorul politicii Informaţiile calificatorului politicii

Prestatorul susţine următoarele tipuri de extensii:

- ✓ **AuthorityKeyIdentifier**: identificatorul cheii Prestatorului, corespunzătoare cheii private, folosită pentru semnarea certificatului cheii publice – extensia este marcată ca **non-critical**,
- ✓ **SubjectKeyIdentifier:** identificatorul abonatului **(non-critical)**,
- ✓ **KeyUsage**: valori permise de utilizare a cheilor – această extensie este marcată ca **critical**. Cîmpul descrie scopurile de utilizare a cheilor, de exemplu pentru criptarea datelor, schimbul de chei etc. (*a se vedea mai jos*).

digitalSignature (0)	-- cheie pentru crearea semnăturii,
nonRepudiation (1)	– cheie asociată cu serviciile de non-repudiere,
keyEncipherment (2)	-- cheie pentru schimbul de chei,
dataEncipherment (3)	-- cheie pentru criptarea datelor,
keyAgreement (4)	-- cheie pentru negocierea de chei,
keyCertSign (5)	-- cheie pentru semnarea de certificate,
cRLSign (6)	-- cheie pentru semnarea de CRL-uri,
encipherOnly (7)	-- cheie numai pentru criptare,
decipherOnly (8)	-- cheie numai pentru decriptare

- ✓ **ExtKeyUSage:** restricţia de utilizare a cheii – extensia este marcată ca **non-critical**. Acest cîmp defineşte unul sau mai multe domenii de utilizare a cheii în conformitate cu domeniile standard, definite în cîmpul **keyUsage**, şi indică posibilităţile de utilizare a certificatului. Obligator, cîmpul trebuie înteles ca **RESTRICŢIE** a valorilor permise de utilizare a cheii definite în **keyUsage**. Prestatorul emite certificate, ce pot conţine una sau o combinaţie dintre următoarele valori:

serverAuth	- autentificarea serverului Web TLS; cîmpul keyUsage are setaţi biţii pentru: digitalSignature, keyEncipherments sau keyAgreement;
clientAuth	- autentificarea clientului Web TLS: cîmpul keyUsage are setaţi biţii pentru: digitalSignature şi/sau keyAgreement;
codeSigning	- semnarea codurilor executabile; cîmpul keyUsage are setat bitul pentru: digitalSignature;
emailProtection	- protecţia e-mail-ului; cîmpul keyUsage are setaţii biţii pentru: digitalSignature; nonRepudiation şi/sau (keyEncipherment sau keyAgreement);
dvcs	- emiterea confirmărilor de către notariate; cîmpul keyUsage are setaţi biţii pentru: digitalSignature, nonRepudiation, keyCertSign, cRLSign.

- ✓ **CertificatePolicies** – extensia prezintă informaţie (identificatori, adrese electronice), ce indică politicile de certificare aplicate de Prestator. Extensia este marcată ca **non-critical**.

Certificatele, emise de Prestator, conţin extensii în conformitate cu recomandările definite în **RFC 5280** ***Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.***

PolicyMapping	Cîmp marcat ca **non-critical**. El conţine unul sau mai multe identificatoare ale obiectelor, definind echivalenţa între politicile de certificare ale Prestatorului şi ale prestatorului de servicii de certificare supus acreditării (de obicei, se utilizează în scop de cross-certificare între prestatorii de servicii de certificare).
IssuerAlternativeName	Extensia conţine atribute ne incluse ca componente ale **DN**. Cîmpul este marcat ca **non-critical.**
SubjectAlternativeName	Defineşte numele alternativ al subiectului certificatului. Cîmpul este

marcat ca **non-critical.**

BasicConstraints — Constrîngeri de bază. Cîmpul totdeauna este marcat ca **critical** pentru Autoritatea de certificare şi **non-critical** pentru certificatul utilizatorului. Valoarea acestui cîmp permite definirea Prestatorului în calitate de utilizator (cîmpul **CA**) şi lungimea maximală (reieşind din ierarhia prestatorilor de servicii de certificare) a prestatorilor de servicii de certificare intermediare între prestatorul respectiv şi utilizator (cîmpul **pathLength**).

CRLDistributionPoints — Punctul de distribuire a listei certificatelor revocate. Cîmpul nu este marcat ca **critical**, extensia defineşte adresa de reţea la care se află **CRL**-ul curent, emis de **CRLIssuer.**

SubjectDirectoryAttributes — Atribute ce indică la directoria utilizatorului. Cîmpul este marcat ca **non-critical**. Extensia conţine atribute auxiliare, asociate cu utilizatorul, şi include informaţie indicată în cîmpul **Subject** şi **SubjectAlternativeName**. Această extensie nu este inclusă în componenţa **DN.**

7.1.3 EXTENSIILE CERTIFICATULUI CHEII PUBLICE ŞI TIPURI DE CERTIFICATE ALE CHEILOR PUBLICE

Certificatele, emise de Prestator, pot conţine diverse extensii, definite în § 7.1.1 al CPP. Prezenţa unor sau altor extensii în corpul certificatului cheii publice este determinată de destinaţia corespunzătoare a acestuia. La cererea utilizatorului are loc certificarea cheii publice.

7.1.3.1 EXTENSIILE CERTIFICATELOR CHEILOR PUBLICE ALE PRESTATORULUI DE SERVICII DE CERTIFICARE

Certificatul cheii publice al Prestatorului poate conţine următoarele extensii:

EXTENSIE	VALOARE	STATUT
Basic Constraints	**Subject Type** = CA Path length constraint = {none,1}	**critical**

7.1.3.2 EXTENSIILE CERTIFICATULUI CHEII PUBLICE PENTRU SEMNĂTURA ELECTRONICĂ AVANSATĂ CALIFICATĂ

Certificatul cheii publice pentru semnătura electronică avansată calificată conform **RFC 3739** ***Qualified Certificates Profile***, emis de Prestator utilizatorului, poate conţine următoarele extensii:

EXTENSIE	VALOARE	STATUT
Basic Constraints	**Subject Type** = end entity Path length constraint = none	**critical** **(dacă există)**
Key Usage	**non-repudiation**	**critical**

Subject Alternative Name	**RFC822Name**	**non-critical**
CRL Distribution Points	**URI:**	**non-critical**
Authority Information Access	**OCSP:**	**non-critical**
Certificate Policies	**Policies:** **CPS:**	**non-critical**

7.1.3.3 EXTENSIILE CERTIFICATELOR CHEILOR PUBLICE PENTRU SEMNĂTURA ELECTRONICĂ AVANSATĂ NECALIFICATĂ

Certificatul cheii publice pentru semnătura electronică avansată necalificată, pentru criptarea sistemelor de fișiere (**EFS**), pentru schimbul electronic de date (**EDI**), emis de Prestator utilizatorului, poate conține următoarele extensii:

EXTENSIE	VALOARE	STATUT
Key Usage	**digital signature** **non=-repudiation** **key encipherment** **key agreement**	**critical**
Extended Key Usage	**Secure email**	**non-critical**
Netscape Cert Type	**SMIME**	**non-critical**
Subject Alternative Name	**RFC822Name**	**non-critical**
CRL Distribution Points	**URI:**	**non-critical**
Authority Information Access	**OCSP:**	**non-critical**
Certificate Policies	**Policies:** **CPS:**	**non-critical**

7.1.3.4 EXTENSIILE CERTIFICATELOR CHEILOR PUBLICE PENTRU AUTENTIFICARE ȘI SERVICII DE SECURITATE

Certificatul cheii publice pentru autentificare și servicii de securitate, emis de Prestator utilizatorului, poate conține următoarele extensii:

EXTENSIE	VALOARE	STATUT
Key Usage	**digital signature** **key encipherment**	**critical**
Extended Key Usage	**Client Authentication**	**non-critical**
Netscape Cert Type	**SSL Client Authentication**	**non-critical**
Subject Alternative Name	**RFC822Name**	**non-critical**

CRL Distribution Point	**URI:**	**non-critical**
Authority Information Access	**OCSP:**	**non-critical**
Certificate Policies	**Policies:** **CPS:**	**non-critical**

7.1.3.5 EXTENSIILE CERTIFICATELOR CHEILOR PUBLICE PENTRU AUTENTIFICARE BIFACTORIALĂ SECURIZATĂ

Certificatul cheii publice pentru autentificare bifactorială securizată, emis de Prestator utilizatorului, poate conține următoarele extensii:

EXTENSIE	VALOARE	STATUT
Key Usage	**digital signature** **key encipherment**	**critical**
Extended Key Usage	**Client Authentication** **Server Authentication**	**non-critical**
Netscape Cert Type	**SSL Client Authentication, SSL Server Authentication**	**non-critical**
CRL Distribution Points	**URI:**	**non-critical**
Authority Information Access	**OCSP:**	**non-critical**
Certificate Policies	**Policies:** **CPS:**	**non-critical**

7.1.3.6 EXTENSIILE CERTIFICATELOR CHEILOR PUBLICE PENTRU SISTEMELE INFORMAȚIONALE ELECTRONICE

Certificatul cheii publice, emis de Prestator utilizatorului, pentru sistemele informaționale electronice, ce urmează să interacționeze cu serviciile electronice guvernamentale, poate conține următoarele extensii:

EXTENSIE	VALOARE	STATUT
Basic Constraints	**Subject Type** = empty (end entity) Path length constraint = none	**non-critical**
Key Usage	digital signature key encipherment data encipherment	**critical**
Extended Key Usage	Client Authentication	**non-critical**
Netscape Cert Type	SSL Client Authentication	**non-critical**
CRL Distribution Point	**URI:**	**non-critical**
Authority Information	**OCSP:**	**non-critical**

Access		
Certificate Policies	**Policies:** **CPS:**	**non-critical**

7.1.4 IDENTIFICATORUL ALGORITMULUI SEMNĂTURII ELECTRONICE

Cîmpul **signatureAlgorithm** conţine identificatorul algoritmului criptografic, descriind algoritmul pentru crearea semnăturii electronice, aplicat de Prestator în certificatul cheii publice.

De exemplu, Prestatorul utilizează algoritmul **RSA** în combinaţie cu funcţiile hash **SHA-1** sau **SHA-2**.

7.1.5 CÎMPUL SEMNĂTURII ELECTRONICE

Valoarea cîmpului **signatureValue** reprezintă rezultatul execuţiei funcţiei hash pentru toate cîmpurile certificatului, marcate ca cîmpuri ale corpului certificatului (**tbsCertificate**) şi criptarea ulterioară a digest-ului cu ajutorul cheii private a utilizatorului.

7.1.6 TIPURI DE NUME

A se vedea pct. 3.1

7.1.7 CONSTRÎNGERI DE NUME

A se vedea pct. 3.1

7.1.8 IDENTIFICATORUL POLITICII DE CERTIFICARE

În domeniul semnăturii electronice sub-arcul {iso(1) member-body(2) md(498)CA(3)}, din cadrul arcului de ţară {iso(1) member-body(2) md(498)}, este alocat I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" cu scop de gestionare şi utilizare a acestuia în prestarea serviciilor de certificare a cheilor publice. Identificatoarele de obiecte utilizate sunt descrise în *Politica de gestionare a identificatorilor de obiecte.*

7.1.9 UTILIZAREA POLITICII CONSTRÎNGERILOR

Prestatorul foloseşte extensia **Basic Constraints** - constrîngeri de bază. Cîmpul totdeauna este marcat ca **critical** pentru Autoritatea de certificare şi **critical** pentru certificatul calificat al utilizatorului (dacă apare. În celelalte tipuri de certificate ale cheilor publice aceasta este non-critical sau lipseşte). Valoarea acestui cîmp permite definirea Autorităţii de certificare drept utilizator (cîmpul **CA**) şi lungimea maximală (reieşind din ierarhia prestatorilor de servicii de certificare) a autorităţilor de certificare intermediare între autoritatea respectivă şi utilizator (cîmpul **pathLength**).

7.2. PROFILUL CRL

Listele certificatelor revocate (**CRL**) constau din trei cîmpuri. Primul cîmp (**tbsCertList**) conţine informaţie despre certificatele revocate, al doilea şi al treilea – **signatureAlgorithm** şi

signatureValue conţin informaţie despre identificatorul algoritmului, folosit pentru semnarea listei certificatelor revocate, şi despre semnătura electronică a Prestatorului. În acest mod, ultimele două cîmpuri sunt identice cu cîmpurile certificatului cheii publice. Cîmpul **tbsCertList** reprezintă o secvenţă de cîmpuri de bază şi auxiliare. Cîmpurile de bază identifică autoritatea de certificare, ce a semnat Lista certificatelor revocate, iar cele auxiliare conţin informaţie despre certificatele revocate şi extensiile **CRL**-ului.

Cîmpurile de bază şi auxiliare, ce se conţin în Lista certificatelor revocate, sunt:

Denumirea (în engleză)	Descrierea	Conţinutul
	Cîmpuri de bază	
Version	Versiunea	V2
Issuer	Emitentul CRL	CN = Denumirea prestatorului de servicii de certificare L = Localitatea S = Statul OU = Prestatorul de servicii de certificare, subdiviziunea persoanei juridice O = Denumirea persoanei juridice, IDNO C = Codul statului
thisUpdate	Data emiterii CRL	„__” _____ 20__ oo:mm:ss GMT
nextUpdate	Termenul pentru care este valabilă CRL	„__” _____ 20__ oo:mm:ss GMT
Revoked Certificates	Lista certificatelor revocate	Numărul de serie al certificatului (CertificateSerialNumber) Data revocării sau suspendării valabilităţii certificatului (Time)
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii electronice a emitentului certificatului
Issuer Sign	Semnătura electronică a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat
	Cîmpuri auxiliare	
Reason Code	Codul cauzei revocării certificatului	"0" nu este indicată "1" compromiterea cheii private "2"compromiterea prestatorului de servicii de certificare "3" schimbarea apartenenţei "4" certificatul a fost schimbat "5" încetarea activităţii "6" suspendarea valabilităţii "9" revocarea atribuţiilor

Hold Instruction Code	Codul cauzei de suspendare temporară a valabilităţii certificatului	Codul cauzei de suspendare temporară a valabilităţii (OID)
Authority Key Identifier	Identificatorul cheii emitentului	Identificatorul cheii private a centrului de certificare cu utilizarea căreia este semnată CRL
CRLNumber	Numărul de serie	Numărul de serie al CRL

7.2.1 VERSIUNEA

Listele certificatelor revocate trebuie să corespundă cerinţelor standardului ITU-T X.509, versiunea 2, standardului SM ISO/CEI 9594-8:2014 *Tehnologia informaţiei. Interconexiunea sistemelor deschise. Linii directoare: Structura certificatului cheii publice şi a atributului* sau recomandării IETF RFC 5280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF RFC 6818 *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*

7.2.2 EXTENSIILE ACCEPTATE

Extensiile Listei certificatelor revocate ale Prestatorului (**crlEntryExtensions**) conţin următoarele cîmpuri:

✓ **ReasonCode**: codul cauzei revocării certificatului. Valoarea acestui cîmp este marcată ca extensie **non-critical** şi permite determinarea cauzei revocării certificatului şi, ca urmare, determină gradul final de încredere. Prestatorul acceptă următoarele cauze de revocare:

unspecified - nespecificat;

keyCompromise - pierderea sau compromiterea cheii;

cACompromise - pierderea sau compromiterea cheii Prestatorului;

affilationChanged - datele utilizatorului au fost modificate;

superseded - certificatul a fost schimbat;

cessationOfOperation - sistarea utilizării certificatului;

certificateHold - suspendarea valabilităţii certificatului;

removeFromCRL - eliminarea certificatului din CRL;

privilegeWithdrawn - atributiile delegate titularului au fost anulate.

✓ **HoldInstructionCode:** codul operaţiei de suspendare a valabilităţii certificatului. Cîmp marcat ca **non-critical** şi determină identificatorul înregistrat al comenzii, folosit în procesul de căutare a certificatului printre cele revocate cu definirea cauzei de suspendare a valabilităţii certificatului (**certificateHold**). Dacă aplicaţia utilizatorului în procesul de analiză a CRL-ului găseşte valoarea **id-holdinstruction-callissuer**, abonatul trebuie înştiinţat să ia legătura cu Prestatorul pentru a concretiza cauzele de suspendare a valabilităţii certificatului şi a determina acţiunile ulterioare conform cauzei indicate (a accepta sau a respinge). Dacă aplicaţia utilizatorului

găseşte valoarea **id-holdinstruction-reject**, certificatul trebuie respins în mod obligator. Comanda **id-holdinstruction-none** se echivalează cu absenţa **holdInstructionCode**.

7.3. PROFILUL RĂSPUNSULUI OCSP

Protocolul de verificare a statutului certificatului (**OCSP**) este folosit de Prestator şi permite verificarea statutului certificatului în regim de timp real.

Informaţia despre statutul certificatului cheii publice este definită în cîmpurile **certStatus** ale structurii **SingleResponse**. Ea trebuie să conţină una din cele trei valori, definite în secţiunea 4.9.9 al CPP.

7.3.1 VERSIUNEA

Serverul **OCSP** al Prestatorului confirmă statutul certificatului cheii publice în conformitate cu recomandările **RFC 6960** ***X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP***.

7.3.2 EXTENSIILE RĂSPUNSULUI OCSP

Certificatul serverului **OCSP** conţine extensia **extKeyUsage**, conform **RFC 5280**. Extensia trebuie marcată ca necritică (**non-critical**) şi semnifică faptul că Prestatorul, semnînd certificatul serverului **OCSP**, îi deleghează acestuia împuterniciri de confirmare a statutului certificatului cheii publice, pentru care a fost primită cererea din partea utilizatorului final.

De asemenea, certificatul serverului **OCSP** trebuie să conţină informaţie despre metodele de contact cu serverul. Această informaţie este inclusă în cîmpul **AuthorityInfoAccessSyntax**.

8. AUDITUL ŞI ALTE EVALUĂRI

Funcţiile auditului sunt necesare pentru controlul integrităţii activităţii Prestatorului, a serviciilor prestate.

Scopul auditului este de a verifica echivalenţa acţiunilor Prestatorului cu cerinţele şi procedurile stabilite.

Auditul, efectuat de Prestator, se răsfrînge asupra centrelor de prelucrare a datelor şi asupra procedurilor de administrare a cheilor. Acest audit se desfăşoară în cadrul Prestatorului şi în alte componente ale infrastructurii cheilor publice, de exemplu, serverele OCSP.

Auditul poate fi efectuat de angajaţii Prestatorului (audit intern) sau de instituţii independente (audit extern). Indiferent de tip, auditul se desfăşoară la cererea şi sub supravegherea administratorului de securitate.

8.1. FRECVENŢA EFECTUĂRII AUDITULUI

Auditul extern verifică integritatea şi conformitatea procedurilor aplicabile cu legislaţia în vigoare (în corelaţie cu prezentul CPP şi Politica de certificare) şi trebuie efectuat cel puţin o dată în patru ani. Auditul intern al activităţii Prestatorului se efectuează anual.

8.2. IDENTIFICAREA ŞI CALIFICAREA AUDITORULUI

Auditul extern este efectuat de o instituţie licenţiată, independentă, înregistrată în Republica Moldova sau de o instituţie internaţională cu reprezentanţă în Republica Moldova ce satisface următoarele condiţii:

- dispune de personal cu studii tehnice corespunzătoare şi experienţă de lucru (cu acte ce o atestă) în domeniul infrastructurii cheilor publice, a tehnologiilor şi a echipamentului de securitate informaţională şi a auditului sistemelor de securitate;
- este înregistrată, licenţiată şi recunoscută la nivel internaţional.

Auditul intern este efectuat de angajaţi calificaţi ai Instituţiei.

8.3. CONTROALE DE AUDIT ŞI INTERCORELAŢIA CU SUPERVIZAŢII

A se vedea secţiunile 8.1 şi 8.2 din CPP.

8.4. ÎNTREBĂRI CU SPECIFIC DE AUDIT

Procedurile interne şi externe ale auditului sunt efectuate în conformitate cu regulile stabilite de **American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA) Web Trust Principles and Criteria for Certification Authorities** (în continuare - **Web Trust**).

Auditul se desfăşoară conform regulilor stabilite în *Regulamentul de efectuare a auditului intern al Centrului de certificare a cheilor publice* şi se răsfrînge asupra:

- securităţii fizice a Prestatorului:
- procedurii de verificare a identităţii utilizatorului:
- serviciilor de certificare şi a procedurilor de prestare a acestora;
- securităţii mijloacelor de program şi a accesului la reţea;
- securităţii personalului Prestatorului;
- registrelor evenimentelor şi a proceselor de monitorizare a sistemului;
- arhivării şi restabilirii datelor;
- procedurii de arhivare:
- înscrierilor de modificare a parametrilor de configurare a Autorităţii de certificare;
- înscrierilor despre analiza şi verificările aplicaţiilor de program şi a dispozitivelor tehnice.

8.5. ACŢIUNI DESFĂŞURATE ÎN CAZ DE DEPISTARE A DISCREPANŢELOR

Rapoartele controalelor de audit efectuate sunt transmise conducerii Prestatorului. Timp de 15 zile de la primirea rezultatelor auditului conducerea pregăteşte un rezumat cu privire la neajunsurile depistate şi elaborează planul de acţiuni pentru înlăturarea acestora. Aceste acţiuni trebuie direcţionate spre înlăturarea discrepanţelor depistate şi a situaţiilor critice. După înlăturarea discrepanţelor şi a necorespunderilor, acestea sunt şterse din raportul auditorului prin alcătuirea raportului de înlăturare a discrepanţelor depistate, copia căruia este trimisă instituţiei ce efectuează auditul în caz de audit extern.

În caz de defecte ce prezintă risc direct pentru procesul de certificare a cheilor publice administratorul de securitate poate lua decizia de suspendare temporară a procesului dat. Toţi utilizatorii vor fi înştiinţaţi despre decizia luată şi despre termenele de suspendare.

8.6. NOTIFICARE DESPRE REZULTATELE AUDITULUI

Rapoartele auditorului(-ilor) (cu cele mai mici detalii posibile) şi opinia generală a auditorului despre starea şi funcţionalitatea Prestatorului sunt elaborate în conformitate cu cerinţele indicate în ***WebTrust*** şi sunt aduse la cunoştinţa administraţiei Instituţiei. Aceste rapoarte nu se fac publice.

9. ALTE ASPECTE FINANCIARE ŞI LEGALE

9.1. TARIFUL SERVICIILOR

9.1.1 TARIFUL SERVICIILOR DE CERTIFICARE

Serviciile de certificare sunt prestate în baza tarifelor aprobate în cadrul Instituției şi sunt publicate pe portalul www.stisc.gov.md. Politica tarifară este periodic revizuită.

Modalităţi de achitare: pe bază de factură fiscală, ordin de plată conform prevederilor legale.

9.1.2 TARIFUL PENTRU ACCES LA CERTIFICATE

Certificatele cheilor publice sunt publicate într-un registru, accesul la care se face în baza anumitor parametri, astfel încît să nu fie încălcate prevederile Legii nr. 133 din 08.07.2011 *privind protecţia datelor cu caracter personal*. Prestatorul nu percepe careva taxe pentru acest servici.

9.1.3 TARIFUL PENTRU ACCES LA INFORMAŢIA DESPRE STATUTUL CERTIFICATULUI CHEII PUBLICE

Nu se percepe.

9.1.4 TARIFELE SERVICIILOR ADIŢIONALE

Prestatorul este în drept de a percepe taxe suplimentare pentru orice serviciu suplimentar, cum ar fi:

- serviciul de marcare temporală (Time-Stamping Authority);
- serviciul de aplicare a semnăturii electronice prin intermediul aplicaţiei web,
- serviciul de aplicare şi/sau verificare automatizată a semnăturii electronice;
- serviciul MobileSignature,

în bază contractuală.

9.1.5 POLITICA DE RESTITUIRE

Persoana juridică sau persoana fizică poate solicita, în formă scrisă, restituirea sumei achitată pentru serviciile de certificare doar dacă solicitarea dată survine pînă la prestarea serviciilor de certificare.

După examinarea solicitării şi verificarea sumelor, Prestatorul îşi onorează obligaţiunea de a restitui banii.

9.2. RESPONSABILITĂŢI FINANCIARE

9.2.1 ASIGURAREA FINANCIARĂ

În conformitate cu cadrul normativ Prestatorul dispune de resurse financiare pentru recuperarea eventualelor prejudicii (garanţia financiară constituie 300000 mdl).

9.2.2 ALTE ACTIVE

Nu se aplică.

9.2.3 ASIGURAREA SAU GARANŢIA FINANCIARĂ PENTRU ENTITĂŢI FINALE

A se vedea pct. 9.2.1.

9.3. CONFIDENŢIALITATEA INFORMAŢIEI

În procesul de colectare şi prelucrare a informaţiei Prestatorul asigură respectarea prevederilor cadrului normativ privind protecţia datelor cu caracter personal. Informaţia este preluată direct de la solicitantul unui certificat al cheii publice sau de la persoana împuternicită, cu posibila validare a datelor în registrele de stat.

9.3.1 INFORMAŢIE CONFIDENŢIALĂ

Următoarea informaţie este considerată confidenţială sau cu caracter privat:

- informaţiile oferite de solicitant în cererea de certificare a cheii publice,
- înregistrarile din sistem,
- rezultatele de audit,
- informaţii privind măsurile luate pentru protecţia mijloacelor hardware şi software ale Prestatorului,
- informaţiile referitoare la evenimentele ce ţin de serviciile prestate de Prestator,
- documentaţia internă a Prestatorului cu clasa de securitate C1 şi C2.

Acest tip de informaţie este oferită autorităţilor legale doar cu respectarea cadrului normativ.

9.3.2 INFORMAŢIE NECONFIDENŢIALĂ

Următoarea informaţie nu este considerată confidenţială sau cu caracter privat:

- informaţiile incluse în certificatele cheilor publice ale Prestatorului,
- cuprinsul Depozitului,
- instrucţiunile elaborate pentru utilizatori,
- oferta comercială şi tehnică a produselor şi serviciilor,
- lista certificatelor revocate.

9.3.3 RESPONSABILITATEA DE A PROTEJA INFORMAŢIA CONFIDENŢIALĂ

Angajaţii Prestatorului sunt obligaţi să păstreze secretul informaţiilor la care au acces atît pe parcursul executării atribuţiilor sale în cadrul Instituţiei, cît şi după expirarea contractului de muncă.

9.4. INFORMAŢIA PERSONALĂ PRIVATĂ

9.4.1 POLITICA DE CONFIDENŢIALITATE

Prestatorul a implementat *Politica de confidențialitate*, disponibilă pe www.stisc.gov.md.

9.4.2 INFORMAȚIA PRIVATĂ

A se vedea pct. 9.3.1.

9.4.3 INFORMAȚIA NEPRIVATĂ

A se vedea pct. 9.3.2.

9.4.4 RESPONSABILITATEA DE A PROTEJA INFORMAȚIA PRIVATĂ

Angajații Prestatorului sunt obligați să păstreze secretul informațiilor la care au acces atît pe parcursul executării atribuțiilor sale în cadrul Instituției, cît și după expirarea contractului de muncă.

9.4.5 NOTIFICAREA ȘI CONSIMȚĂMÎNTUL DE A UTILIZA INFORMAȚIA PRIVATĂ

Prestatorul utilizează și prelucrează, cu acordul solicitantului, doar informația privată prezentată de către solicitant.

9.4.6 DIVULGAREA INFORMAȚIEI CA URMARE A PROCESELOR JUDICIARE SAU ADMINISTRATIVE

Atît Prestatorul, cît și utilizatorul se obligă să nu divulge conținutul prevederilor contractuale decît în cazurile prevăzute de cadrul normativ.

9.4.7 ALTE CIRCUMSTANȚE DE DIVULGARE A INFORMAȚIEI

Nu se aplică.

9.5. DREPTURILE DE PROPRIETATE INTELECTUALĂ

Prestatorul deține drepturile de proprietate intelectuală asupra mijlocelor de program și a documentației elaborate. Reproducerea acestora este strict interzisă.

Perechile de chei corespunzătoare certificatelor cheilor publice ale utilizatorilor sunt proprietatea titularilor menționați în cîmpul Subject.

Perechile de chei corespunzătoare certificatelor cheilor publice ale Prestatorului sunt proprietatea Prestatorului.

Mărcile, siglele, patentele, imaginile grafice etc folosite de Prestator (pe pagina sa oficială sau în alte mijloace de comunicare) sunt proprietatea deținătorilor acestora și Prestatorul specifică acest lucru conform cerințelor înaintate de către deținători.

Mărcile, siglele, patentele, licențele, imaginile grafice etc ce aparțin Prestatorului sunt proprietatea acestuia și nu pot fi reproduse sau utilizate de către terți decît cu acordul scris al Prestatorului.

9.6. AUTORITĂŢI ŞI GARANŢII

9.6.1 AUTORITATEA DE CERTIFICARE

Prestatorul îşi onorează obligaţiile sale faţă de titulari şi terţe părţi, participanţi ai infrastructurii cheilor publice din Republica Moldova, conform cadrului normativ.

9.6.2 AUTORITATEA DE ÎNREGISTRĂRI

Autoritatea de înregistrări, reprezentanţii Prestatorului în interacţiunea cu utilizatorul, îşi onorează obligaţiile faţă de utilizatori în baza prevederilor contractuale şi ale cadrului normativ.

9.6.3 UTILIZATORUL

Titularul certificatului cheii publice este obligat:
a. să prezinte informaţie veridică în cererile depuse către Prestator;
b. să asigure condiţiile necesare pentru excluderea accesului unei alte persoane la cheia sa privată;
c. să nu utilizeze cheia privată pentru crearea semnăturii electronice dacă are motive să presupună că este încălcată confidenţialitatea cheii private;
d. să solicite imediat suspendarea valabilităţii certificatului cheii publice sau revocarea acestuia în cazul în care: a pierdut cheia privată, are motive să creadă că a fost încălcată confidenţialitatea cheii private, informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;
e. să înştiinţeze, în decurs de 24 de ore, Prestatorul despre orice modificare a informaţiilor cuprinse în certificatul cheii publice;
f. să îndeplinească alte obligaţii prevăzute de lege şi de contractul încheiat cu Prestatorul.

9.6.4 PĂRŢI DE ÎNCREDERE ŞI GARANŢII

A se vedea pct. 1.3.4.

9.6.5 GARANŢII ALE ALTOR PARTICIPANŢI

REGISTRUL ŞI GARANŢII

Prestatorul este responsabil de funcţionarea corectă a Registrelor aferente autorităţilor sale de certificare. După revocarea certificatului cheii publice, acesta este notificat despre faptul dat, certificatul cheii publice este trecut în CRL, actualizarea căreia se face automat şi CRL este accesibilă pe www.stisc.gov.md.

9.7. NEGAREA GARANŢIILOR

Nu se aplică.

9.8. LIMITĂRI ALE RĂSPUNDERII

Prestatorul nu este responsabil de acţiunile titularilor, entităţilor partenere şi a altor părţi. Prestatorul nu este responsabil pentru:

- utilizarea aplicaţiilor şi a dispozitivelor ce nu satisfac condiţiile minime stipulate în CPP sau în documentele destinate utilizatorilor, puse la dispoziţie pe www.stisc.gov.md,
- daunele cauzate de utilizarea incorectă a certificatului (revocat/suspendat),
- stocarea datelor eronate şi includerea acestora în certificatul cheii publice ca urmare a declarării acestora, de către utilizator, drept corecte,
- daunele cauzate de neglijenţa păstrării dispozitivelor de către utilizator.

9.9. DESPĂGUBIRI

A se vedea pct. 9.2.1.

9.10. VALABILITATE ŞI ÎNCHEIEREA PREVEDERILOR

9.10.1 VALABILITATE

Prevederile CPP sunt aplicabile din momentul aprobării acestuia. Publicul poate lua cunoştinţă cu CPP pe www.stisc.gov.md.

9.10.2 ÎNCHEIEREA PREVEDERILOR

CPP este actualizat periodic şi prevederile lui sunt aplicabile pînă la apariţia unei noi versiuni.

9.10.3 EFECTELE ÎNCHEIERII PREVEDERILOR

Nu se aplică.

9.11. NOTIFICAREA ŞI COMUNICAREA CU PARTICIPANŢII

Comunicarea cu participanţii la infrastructura cheilor publice se face în formă scrisă sau verbală şi poate avea loc prin intermediul scrisorilor oficiale, email, telefon, fax. La notificarea şi comunicarea cu participanţii se folosesc datele de contact furnizate de către aceştia. Totodată, se ţine cont şi de nedivulgarea informaţiei critice.

9.12. AMENDAMENTE

9.12.1 PROCEDURI

A se vedea pct.1.5.4.

9.12.2 MECANISMUL ŞI PERIOADA DE NOTIFICARE

A se vedea pct. 1.5.4, 2.3.

9.12.3 CIRCUMSTANŢE CE DUC LA SCHIMBAREA OID

Nu se aplică.

9.13. SOLUŢIONAREA LITIGIILOR

Situaţiile litigioase, apărute între Prestator şi utilizator, vor fi soluţionate pe cale amiabilă şi, după caz, conform prevederilor *Regulamentului de soluţionare a situaţiilor litigioase în domeniul aplicării semnăturii electronice*, aprobat prin Ordinul Serviciului de Informaţii şi Securitate nr. 29 din 16 aprilie 2009.

În cazul în care părţile nu vor ajunge la un numitor comun, oricare dintre părţi este în drept să solicite soluţionarea situaţiei apărute de către instanţa judecătorească.

9.14. CADRUL NORMATIV APLICABIL

Prestatorul îşi desfăşoară activitatea în conformitate cu actele normative în domeniul semnăturii electronice.

9.15. CONCORDANŢA CU CADRUL NORMATIV APLICAT

CPP este subiectul de aplicare practică a legilor, a hotărîrilor de guvern, a ordinelor, a standardelor naţionale şi internaţionale în domeniu.

9.16. ALTE PREVEDERI

9.16.1 ACORD INTEGRAL

Nu se aplică.

9.16.2 DECLARAŢII

Nu se aplică.

9.16.3 SEPARABILITATE

Nu se aplică.

9.16.4 CONSTRÎNGERI

Nu se aplică.

9.16.5 CIRCUMSTANȚE CARE JUSTIFICĂ NEEXECUTAREA OBLIGAȚIUNILOR

În afară de cazurile prevăzute de Codul Civil al Republicii Moldova, neexecutarea obligației este justificată în măsura în care partea care invocă neexecutarea demonstrează faptul că aceasta se datorează unui impediment în afara controlului acesteia și dacă părții nu i se putea cere în mod rezonabil să evite sau să depășească impedimentul ori consecințele acestuia.

În cazul în care obligația a apărut dintr-un contract sau alt act juridic, neexecutarea nu este justificată dacă partea care invocă neexecutarea ar fi putut în mod rezonabil să ia în considerare impedimentul la data încheierii.

În cazul în care impedimentul justificator este doar temporar, justificarea produce efecte pe durata existenței impedimentului. Totuși, dacă întârzierea capătă trăsăturile neexecutării esențiale, cealaltă parte poate să recurgă la mijloacele juridice de apărare întemeiate pe o asemenea neexecutare.

Partea care invocă neexecutarea are obligația de a asigura ca cealaltă parte să primească o notificare despre impediment și efectele lui asupra capacității de a executa, într-un termen rezonabil după ce prima parte a cunoscut sau trebuia să cunoască aceste circumstanțe. Partea Informată despre neexecutare are dreptul la despăgubiri pentru orice prejudiciu rezultat din neprimirea respectivei notificări.

Impedimentul justificator nu exonerează partea care invocă neexecutarea de plata despăgubirilor dacă impedimentul a apărut după neexecutarea obligației, cu excepția cazului când cealaltă parte nu ar fi putut, oricum, din cauza impedimentului, să beneficieze de executarea obligației.

9.17. ALTELE

Nu se aplică.

10. ANEXE

Acest capitol conține modelele cererilor, depuse de către utilizatori în scop de prestare a serviciilor de certificare. Totodată, aici descriem și structurile certificatelor cheilor publice ale utilizatorilor, emise de Prestator, și ale Prestatorului.

Anexa nr.1A
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică

CERERE

Prin prezenta. _____, în baza Hotărârii Guvernului Nr. 1140/2017 „Cu privire la activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice", a Hotărârii Guvernului Nr. 1141/2017 „Pentru aprobarea Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcţionarii persoanelor juridice de drept public în cadrul circulaţiei electronice ale acestora" (după caz), şi a Hotărârii Guvernului Nr. 414/2018 „Cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat", solicită eliberarea certificatelor cheilor publice următorilor angajaţi:

Nr.	Nume, Prenume	Funcţia	extrasIDNP	Nr. cererii de certificare

Persoana responsabilă de colaborare cu I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" în domeniul semnăturii electronice este:

Nr.	Nume, Prenume	extrasIDNP	Email	Telefon

Conducătorul persoanei juridice

_____/_____
(semnătura) (numele, prenumele)

L.Ş.

Anexa nr.1B
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică

CERERE

Prin prezenta _____, în baza Hotărârii Guvernului Nr. 1140/2017
(denumirea persoanei juridice)

„Cu privire la activitatea prestatorilor de servicii de certficare în domeniul aplicării semnăturii electronice" şi a Hotărârii Guvernului Nr. 414/2018 „Cu privire la măsurile de consolidare a centrelor de date în sectorul public şi de raţionalizare a administrării sistemelor informaţionale de stat", solicită eliberarea certificatului SSL pentru următorul domen

Nr.	Nume domen
1	
2	

Persoana responsabilă de colaborare cu I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică" în domeniul semnăturii electronice este:

Nr.	Nume, Prenume	extrasIDNP	Email	Telefon

Conducătorul persoanei juridice

_____/_____
(semnătura) (numele, prenumele)

L. Ş.

Anexa nr.2A

la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

Cerere de certificare a cheii publice nr.

Prin prezenta, subsemnatul/a _____,
(numele, prenumele utilizatorului)
IDNP _____, e-mail: _____,
fiind angajat al _____
(denumirea persoanei juridice)

rog eliberarea certificatului cheii publice în conformitate cu datele indicate în prezenta cerere şi includerea în certificat a următoarelor informaţii:

Numele, Prenumele _____
IDNP _____
Organizaţia, IDNO _____
Adresa juridică _____
Secţia _____
Funcţia _____
Oraşul _____
Statul _____
Codul poştal _____
Email _____
Telefon _____

Subsemnatul/a, subiect al datelor cu caracter personal, în conformitate cu ***Legea nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal***, sunt de acord ca datele mele personale să fie prelucrate în contextul prestării serviciilor de certificare a cheii publice şi declar că informaţia furnizată este corectă.

Nume, Prenume _____
Semnătura _____
Data _____

..... *Se completează de Prestatorul de servicii de certificare*.....

Prin prezenta confirm că persoana _____
(nume, prenume)
este identificată. Datele indicate în cerere au fost verificate.
„____" _____ 20___

Administrator de înregistrări
_____/_____
(semnătură) (nume, prenume)

Administrator de certificare
_____/_____
(semnătură) (nume, prenume)

Anexa nr.2B
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

Cerere de certificare a cheii publice nr.

Prin prezenta, subsemnatul/a_____,
(numele, prenumele utilizatorului)
IDNP _____, e-mail: _____,

rog eliberarea certificatului cheii publice în conformitate cu datele indicate în prezenta cerere şi includerea în certificat a următoarelor informaţii:

Numele, Prenumele _____
IDNP _____
Adresa _____
Oraşul _____
Statul _____
Codul poştal _____
Email _____
Telefon _____

Subsemnatul/a, subiect al datelor cu caracter personal, în conformitate cu ***Legea nr. 133 din 08.07. 2011 privind protecţia datelor cu caracter personal***, sunt de acord ca datele mele personale să fie prelucrate în contextul prestării serviciilor de certificare a cheii publice şi declar că informaţia furnizată este corectă.

Nume, Prenume _____
Semnătura _____
Data _____

..... *Se completează de Prestatorul de servicii de certificare*.....

Prin prezenta confirm că persoana_____
(nume, prenume)
este identificată. Datele indicate în cerere au fost verificate.

„____" _____20___

Administrator de înregistrări
_____/_____
(semnătură) (nume, prenume)

Administrator de certificare
_____/_____
(semnătură) (nume, prenume)

Anexa nr. $3A_1$
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică"

Cerere de revocare a certificatului cheii publice

Prin prezenta, _____,
(numele, prenumele utilizatorului)
IDNP: _____, fiind angajat al _____.
(denumirea persoanei juridice)
Rog să revocaţi certificatul cheii publice emis pe numele meu în data de _____, în legătură cu:

_ cererea titularului;
_ încălcarea confidenţialităţii cheii private (compromiterea cheii private), şi anume:
◊ pierderea dispozitivului securizat de creare a semnăturii electronice;
◊ apariţia suspiciunilor privind dezvăluirea informaţiei sau denaturarea ei în sistemul de legătură sau la locurile de utilizare a dispozitivului securizat de creare a semnăturii electronice;
◊ accesul persoanelor terţe la cheia privată sau la dispozitivul securizat de creare a semnăturii electronice;
◊ alte evenimente care dau temei de a presupune că a fost încălcată confidenţialitatea cheii private;
_ modificarea informaţiei cuprinsă în certificat;
_ informaţiile cuprinse în certificatul cheii publice nu corespund realităţii.

Tipul certificatului cheii publice:
_ pentru semnătura electronică avansată calificată.
_ pentru semnătura electronică avansată necalificată.
_ pentru autentificare şi servicii de securitate.

Funcţia _____
_____ / _____
(semnătura) (nume, prenume)
Conducătorul persoanei juridice
"__" _____ 20__ _____ / _____
(semnătura) (nume, prenume)
L.Ş.

..... *Se completează de Prestatorul de servicii de certificare* .....

Prin prezenta confirm că cererea a fost prezentată pe data de *zz.ll.aaaa* la ora *hh.mm* şi transmisă administratorului de certificare pe data de *zz.ll.aaaa* la ora *hh:mm*.

Administrator de înregistrări
_____ / _____
(semnătură) (nume, prenume)

Cererea a fost recepţionată de la administratorul de înregistrări pe data de *zz.ll.aaaa* la ora *hh.mm*. Certificatul cheii publice emis dnei/dlui _____ a fost revocat pe data de *zz.ll.aaaa* la ora *hh:mm*.
(nume, prenume)

Administrator de certificare
_____ / _____
(semnătură) (nume, prenume)

Anexa nr.3A$_2$
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică"

Cerere de revocare a certificatului cheii publice

Prin prezenta, _____,
(denumirea persoanei juridice)
solicităm revocarea certificatului cheii publice emis pentru dl/dna _____,
(numele, prenumele utilizatorului)
IDNP: _____, pe data de _____, în legătură cu:

- ☐ încălcarea confidenţialităţii cheii private (compromiterea cheii private), şi anume:
  - ◊ pierderea dispozitivului securizat de creare a semnăturii electronice;
  - ◊ apariţia suspiciunilor privind dezvăluirea informaţiei sau denaturarea ei în sistemul de legătură sau la locurile de utilizare a dispozitivului securizat de creare a semnăturii electronice;
  - ◊ accesul persoanelor terţe la cheia privată sau la dispozitivul securizat de creare a semnăturii electronice;
  - ◊ alte evenimente care dau temei de a presupune că a fost încălcată confidenţialitatea cheii private;
- ☐ instituirea unei măsuri de ocrotire judiciare (ocrotire provizorie, curatelă sau tutelă) în privinţa titularului;
- ☐ decesul titularului;
- ☐ încetarea raporturilor de muncă ale titularului la persoana juridică;
- ☐ lichidarea Beneficiarului.

Tipul certificatului cheii publice:
- ☐ pentru semnătura electronică avansată calificată.
- ☐ pentru semnătura electronică avansată necalificată.
- ☐ pentru autentificare şi servicii de securitate.

Conducătorul persoanei juridice

"__"_____ 20__ _____ / _____
(semnătura) (nume, prenume)
L.Ş.

..... *Se completează de Prestatorul de servicii de certificare* .....

Prin prezenta confirm că cererea a fost prezentată pe data de *zz.ll.aaaa* la ora *hh:mm* şi transmisă administratorului de certificare pe data de *zz.ll.aaaa* la ora *hh:mm.*

Administrator de înregistrări

_____ / _____
(semnătură) (nume, prenume)

Cererea a fost recepţionată de la administratorul de înregistrări pe data de *zz.ll.aaaa* la ora *hh:mm.* Certificatul cheii publice emis dnei/dlui_____ a fost revocat pe data de *zz.ll.aaaa* la ora *hh:mm.*
(nume, prenume)

Administrator de certificare

_____ / _____
(semnătură) (nume, prenume)

Anexa nr.3B
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică"

Cerere de revocare a certificatului cheii publice

Prin prezenta, _____.
(numele, prenumele utilizatorului)

IDNP: _____.

Rog să revocaţi certificatul cheii publice emis pe numele meu în data de _____, în legătură cu:

- ☐ cererea titularului;
- ☐ încălcarea confidenţialităţii cheii private (compromiterea cheii private), şi anume:
  - ◊ pierderea dispozitivului securizat de creare a semnăturii electronice;
  - ◊ apariţia suspiciunilor privind dezvăluirea informaţiei sau denaturarea ei în sistemul de legătură sau la locurile de utilizare a dispozitivului securizat de creare a semnăturii electronice;
  - ◊ accesul persoanelor terţe la cheia privată sau la dispozitivul securizat de creare a semnăturii electronice;
  - ◊ alte evenimente care dau temei de a presupune că a fost încălcată confidenţialitatea cheii private;
- ☐ modificarea informaţiei cuprinsă în certificat;
- ☐ informaţiile cuprinse în certificatul cheii publice nu corespund realităţii;
- ☐ instituirea unei măsuri de ocrotire judiciare (ocrotire provizorie, curatelă sau tutelă) în privinţa titularului.

Tipul certificatului cheii publice:
- ☐ pentru semnătura electronică avansată calificată;
- ☐ pentru semnătura electronică avansată necalificată;
- ☐ pentru autentificare şi servicii de securitate.

Utilizator final

"___" _____ 20___ _____/_____
(semnătura) (nume, prenume)

..... *Se completează de Prestatorul de servicii de certificare* .....

Prin prezenta confirm că cererea a fost prezentată pe data de *zz.ll.aaaa* la ora *hh:mm* şi transmisă administratorului de certificare pe data de *zz.ll.aaaa* la ora *hh:mm*.

Administrator de înregistrări

_____/_____
(semnătură) (nume, prenume)

Cererea a fost recepţionată de la administratorul de înregistrări pe data de *zz.ll.aaaa* la ora *hh:mm*. Certificatul cheii publice emis dnei/dlui _____ a fost revocat pe data de *zz.ll.aaaa* la ora *hh:mm*.
(nume, prenume)

Administrator de certificare

_____/_____
(semnătură) (nume, prenume)

Anexa nr. 4A
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică"

Cerere de suspendare a valabilității certificatului cheii publice

Prin prezenta, _____.
(numele, prenumele utilizatorului)
IDNP:_____, fiind angajat al _____.
(denumirea persoanei juridice)
rog să suspendați valabilitatea certificatului cheii publice emis pe numele meu pe data de _____
pe o durată de _____zile
(numărul de zile cu litere)
în legătură cu_____.
(motivul suspendării)

Tipul certificatului cheii publice:
- pentru semnătura electronică avansată calificată.
- pentru semnătura electronică avansată necalificată.
- pentru autentificare și servicii de securitate.

Funcția _____
_____ / _____
(semnătura) (nume, prenume)

Conducătorul persoanei juridice
_____ / _____
(semnătura) (nume, prenume)
L.Ş.

"___" _____ 20___

..... *Se completează de Prestatorul de servicii de certificare* .....

Prin prezenta confirm că cererea a fost prezentată pe data de *zz.ll.aaaa* la ora *hh:mm* şi transmisă administratorului de certificare pe data de *zz.ll.aaaa* la ora *hh:mm.*

Administrator de înregistrări
_____ / _____
(semnătură) (nume, prenume)

Cererea a fost recepționată de la administratorul de înregistrări pe data de *zz.ll.aaaa* la ora *hh:mm.* Certificatul cheii publice emis dnei/dlui_____ a fost suspendat pe data de *zz.ll.aaaa* la ora *hh:mm.*
(nume, prenume)

Administrator de certificare
_____ / _____
(semnătură) (nume, prenume)

Anexa nr. 4B
la Codul de practici și proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică"

Cerere de suspendare a valabilității certificatului cheii publice

Prin prezenta, _____.
(numele, prenumele utilizatorului)
IDNP:_____,

rog să suspendați valabilitatea certificatului cheii publice emis pe numele meu pe data de _____

pe o durată de _____zile
(numărul de zile cu litere)
în legătură cu_____.
(motivul suspendării)

Tipul certificatului cheii publice:
- ☐ pentru semnătura electronică avansată calificată.
- ☐ pentru semnătura electronică avansată necalificată.
- ☐ pentru autentificare și servicii de securitate.

"___" _____ 20___

Utilizator
_____ / _____
(semnătura) (nume, prenume)

..... *Se completează de Prestatorul de servicii de certificare* .....

Prin prezenta confirm că cererea a fost prezentată pe data de *zz.ll.aaaa* la ora *hh:mm* și transmisă administratorului de certificare pe data de *zz.ll.aaaa* la ora *hh:mm.*

Administrator de înregistrări
_____ / _____
(semnătură) (nume, prenume)

Cererea a fost recepționată de la administratorul de înregistrări pe data de *zz.ll.aaaa* la ora *hh:mm.* Certificatul cheii publice emis dnei/dlui _____ a fost suspendat pe data de *zz.ll.aaaa* la ora *hh:mm.*
(nume, prenume)

Administrator de certificare
_____ / _____
(semnătură) (nume, prenume)

Anexa nr.5A
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică"

Cerere de restabilire a valabilităţii certificatului cheii publice

Prin prezenta, _____,
(numele, prenumele utilizatorului)
IDNP _____, fiind angajat al _____,
(denumirea persoanei juridice)
rog să restabiliţi valabilitatea certificatului cheii publice emis pe numele meu pe data de_____,
suspendat pe o durată de _____zile
(numărul de zile cu litere)
în legătură cu _____.
(motivul suspendării)
Motivul de restabilire a valabilităţii certificatului cheii publice constituie _____
_____.

Tipul certificatului cheii publice:
- ☐ pentru semnătura electronică avansată calificată.
- ☐ pentru semnătura electronică avansată necalificată.
- ☐ pentru autentificare şi servicii de securitate.

Funcţia _____
_____ / _____
(semnătura) (nume, prenume)

Conducătorul persoanei juridice
_____ / _____
(semnătura) (nume, prenume)

"__"_____20__

L.Ş.

..... *Se completează de Prestatorul de servicii de certificare* .....

Prin prezenta confirm că cererea a fost prezentată pe data de *zz.ll.aaaa* la ora *hh:mm* şi transmisă administratorului de certificare pe data de *zz.ll.aaaa* la ora *hh:mm.*

Administrator de înregistrări
_____ / _____
(semnătură) (nume, prenume)

Cererea a fost recepţionată de la administratorul de înregistrări pe data de *zz.ll.aaaa* la ora *hh:mm.* Certificatul cheii publice emis dnei/dlui_____ a fost restabilit pe data de *zz.ll.aaaa* la ora *hh:mm.*
(nume, prenume)

Administrator de certificare
_____ / _____
(semnătură) (nume, prenume)

Anexa nr.5B
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică"

Cerere de restabilire a valabilității certificatului cheii publice

Prin prezenta, _____,
(numele, prenumele utilizatorului)
IDNP _____,
rog să restabiliți valabilitatea certificatului cheii publice emis pe numele meu pe data de _____,
suspendat pe o durată de _____ zile
(numărul de zile cu litere)
în legătură cu _____,
(motivul suspendării)
Motivul de restabilire a valabilității certificatului cheii publice constituie _____
_____.

Tipul certificatului cheii publice:
- ☐ pentru semnătura electronică avansată calificată.
- ☐ pentru semnătura electronică avansată necalificată.
- ☐ pentru autentificare și servicii de securitate.

"___" _____ 20___

Utilizator final
_____ / _____
(semnătura) (nume, prenume)

..... *Se completează de Prestatorul de servicii de certificare* .....

Prin prezenta confirm că cererea a fost prezentată pe data de *zz.ll.aaaa* la ora *hh:mm* şi transmisă administratorului de certificare pe data de *zz.ll.aaaa* la ora *hh:mm.*

Administrator de înregistrări
_____ / _____
(semnătură) (nume, prenume)

Cererea a fost recepționată de la administratorul de înregistrări pe data de *zz.ll.aaaa* la ora *hh:mm.* Certificatul cheii publice emis dnei/dlui _____ a fost restabilit pe data de *zz.ll.aaaa* la ora *hh:mm.*
(nume prenume)

Administrator de certificare
_____ / _____
(semnătură) (nume, prenume)

Anexa nr.6
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

I.P. „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică"

Decizie privind revocarea
certificatului cheii publice
(după suspendarea valabilităţii acestuia)

Ţinînd cont de faptul că la data de _____ a fost depusă cererea de suspendare a valabilităţii certificatului cheii publice emis dlui/dnei _____, IDNP _____, pe data de _____, angajat/-ă în cadrul _____.
(denumirea persoanei juridice)
pe o durată de _____zile
(numărul de zile cu litere)
în legătură cu_____.
(motivul suspendării)

şi în lipsa unei cereri privind restabilirea valabilităţii certificatului cheii publice, conform prevederilor cadrului normativ, Prestatorul de servicii de certificare decide revocarea certificatului cheii publice menţionat.

Tipul certificatului cheii publice:
- ☐ pentru semnătura electronică avansată calificată.
- ☐ pentru semnătura electronică avansată necalificată.
- ☐ pentru autentificare şi servicii de securitate.

Administrator de certificare
_____/_____
(semnătură) (nume, prenume)

Şef al Centrului de certificare a cheilor publice

"__" _____ 20__

_____/_____
(semnătura) (nume, prenume)

Certificatul cheii publice emis dlui dnei_____ a fost revocat pe data de *zz.ll.aaaa* la
(nume, prenume)
ora *hh:mm*.

Administrator de certificare
_____/_____
(semnătură) (nume, prenume)

Anexa nr.7
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

Structura certificatului cheii publice a Prestatorului (I.P. STISC) în calitate de prestator de nivel superior şi de nivel doi

Certificatul cheii publice a Prestatorului în calitate de prestator de nivel superior şi inferior include următoarele cîmpuri:

Denumirea (în engleză)	Descrierea	Conţinutul
Cîmpurile de bază		
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Numărul
Issuer	Datele de identificare ale Prestatorului superior	CN = Denumirea prestatorului de servicii de certificare L = Localitatea S = Statul OU = Prestatorul de servicii de certificare, 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 prestatorului	CN = Denumirea certificatului prestatorului de servicii de certificare L = Chişinău S = Republica Moldova OU = Subdiviziunea prestatorului O = Denumirea persoanei juridice, IDNO C = MD
Subject Public Key Info	Cheia publică	Cheia publică a prestatorului
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		
Autority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a prestatorului de servicii de certificare, emitentului certificatului (doar în certificatul prestatorului de servicii de certificare de nivel inferior)
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a prestatorului de servicii de certificare, corespunzătoare prezentului certificat
Key Usage	Utilizarea cheii	Semnătura electronică în certificate, semnătura electronică în lista certificatelor revocate
Private Key Usage Period	Perioada de valabilitate a cheii private	Valabilă de la: "__" _____ 20__ oo:mm:ss GMT Valabilă pînă la: "__" _____ 20__ oo:mm:ss GMT
Certificate Policies	Politica de certificare a	Identificatorul politicii = toate politicile de emitere.

	prestatorului de servicii de certificare	Informațiile calificatorului politicii
Basic Constraints	Restricții de bază	Tipul subiectului = CA Limitarea lungimii lanțului de certificate = {none sau 1}
CRL Distribution Points	Punctul de distribuire a listei certificatelor revocate (CRL)	Sursa publicării listei certificatelor revocate
Authority Information Access	Accesul la informațiile despre prestatorii de servicii de certificare	Modalitatea de acces la informațiile despre prestatorul de servicii de certificare

Anexa nr.8
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

Structura certificatului cheii publice a utilizatorului pentru semnătura electronică avansată calificată

Certificatul cheii publice a utilizatorului semnăturii electronice conţine următoarele cîmpuri:

Denumirea (în engleză)	**Descrierea**	**Conţinutul**
	Cîmpurile de bază	
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Numărul
Issuer	Datele de identificare ale prestatorului de servicii de certificare, emitent al certificatului	CN = Denumirea certificatului prestatorului de servicii de certificare L = Localitatea S = Statul OU = Prestatorul de servicii de certificare, 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 CN = Numele, prenumele utilizatorului L = Localitatea de domiciliu a utilizatorului S = Statul OU = Subdiviziunea persoanei juridice, în care activează utilizatorul, după caz O = Denumirea persoanei juridice, IDNO, în care activează utilizatorul, după caz P = Telefonul utilizatorului T = Funcţia deţinută de către utilizator, după caz C = Codul statului
Subject Public Key Info	Cheia publică	Cheia publică a utilizatorului
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii electronice a emitentului certificatului
Signature Value	Semnătura electronice a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat
	Cîmpurile auxiliare	
Authority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a prestatorului de servicii de certificare, emitentului certificatului
Subject Key Identifier	Identificatorul cheii titularului	Identificatorul cheii private a utilizatorului,

	certificatului	corespunzătoare prezentului certificat
Key Usage	Utilizarea cheii	Irevocabilitatea
Certificate Policies	Politica de certificare a prestatorului de servicii de certificare	Identificatorul politicii Informaţiile calificatorului politicii
Subject Alternative Name	Numele alternativ al titularului certificatului	RFC822 Name = Poşta electronică a utilizatorului
CRL Distribution Points	Punctul de distribuţie a listei certificatelor revocate	Sursa publicării listei certificatelor revocate
Authority Information Access	Accesul la informaţiile despre prestatorul de servicii de certificare	Modalitatea de acces la informaţiile despre prestatorul de servicii 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.9
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

Structura certificatului cheii publice a utilizatorului pentru semnătura electronică avansată necalificată

Certificatul cheii publice a utilizatorului conţine următoarele cîmpuri:

Denumirea (în engleză)	Descrierea	Conţinutul
	Cîmpurile de bază	
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Numărul
Issuer	Datele de identificare ale prestatorului de servicii de certificare, emitent al certificatului	CN = Denumirea certificatului prestatorului de servicii de certificare L = Localitatea S = Statul OU = Prestatorul de servicii de certificare, 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 CN = Numele, prenumele utilizatorului L = Localitatea de domiciliu a utilizatorului S = Statul OU = Subdiviziunea persoanei juridice, în care activează utilizatorul, după caz O = Denumirea persoanei juridice, IDNO, în care activează utilizatorul, după caz P = Telefonul utilizatorului T = Funcţia deţinută de către utilizator, după caz Street = Adresa juridică PostalCode = Codul poştal corespunzător adresei juridice C = Codul statului
Subject Public Key Info	Cheia publică	Cheia publică a utilizatorului
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii electronice a emitentului certificatului
Signature Value	Semnătura electronice a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat
	Cîmpurile auxiliare	
Authority Key Identifier	Identificatorul cheii emitentului	Identificatorul cheii private a prestatorului de

	certificatului	servicii de certificare, emitentului certificatului
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a utilizatorului, corespunzătoare prezentului certificat
Key Usage	Utilizarea cheii	Digital Signature, Non-Repudiation, Key Encipherment, Key Agreement
Certificate Policies	Politica de certificare a prestatorului de servicii de certificare	Identificatorul politicii Informațiile calificatorului politicii
Subject Alternative Name	Numele alternativ al titularului certificatului	RFC822 Name = Poșta electronică a utilizatorului
CRL Distribution Points	Punctul de distribuție a listei certificatelor revocate	Sursa publicării listei certificatelor revocate
Authority Information Access	Accesul la informațiile despre prestatorul de servicii de certificare	Modalitatea de acces la informațiile despre prestatorul de servicii de certificare

Anexa nr.10
la Codul de practici și proceduri
al Centrului de certificare a cheilor publice

Structura certificatului cheii publice a utilizatorului pentru autentificare și servicii de securitate

Certificatul cheii publice a utilizatorului conține următoarele cîmpuri:

Denumirea (în engleză)	Descrierea	Conținutul
Cîmpurile de bază		
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Numărul
Issuer	Datele de identificare ale prestatorului de servicii de certificare, emitent al certificatului	CN = Denumirea certificatului prestatorului de servicii de certificare L = Localitatea S = Statul OU = Prestatorul de servicii de certificare, 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 CN = Numele, prenumele utilizatorului L = Localitatea de domiciliu a utilizatorului S = Statul OU = Subdiviziunea persoanei juridice, în care activează utilizatorul, după caz O = Denumirea persoanei juridice, IDNO, în care activează utilizatorul, după caz P = Telefonul utilizatorului T = Funcția deținută de către utilizator, după caz Street = Adresa juridică PostalCode = Codul poștal corespunzător adresei juridice C = Codul statului
Subject Public Key Info	Cheia publică	Cheia publică a utilizatorului
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii electronice a emitentului certificatului
Signature Value	Semnătura electronice a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat
Cîmpurile auxiliare		
Authority Key Identifier	Identificatorul cheii emitentului	Identificatorul cheii private a prestatorului de

	certificatului	servicii de certificare, emitentului certificatului
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a utilizatorului, corespunzătoare prezentului certificat
Key Usage	Utilizarea cheii	Digital Signature, Key Encipherment
Enhanced key Usage	Utilizarea extinsă a cheii	Client Authentication
Netscape Cert Type		SSL Client Authentication
Certificate Policies	Politica de certificare a prestatorului de servicii de certificare	Identificatorul politicii Informațiile calificatorului politicii
Subject Alternative Name	Numele alternativ al titularului certificatului	RFC822 Name = Poșta electronică a utilizatorului
CRL Distribution Points	Punctul de distribuție a listei certificatelor revocate	Sursa publicării listei certificatelor revocate
Authority Information Access	Accesul la informațiile despre prestatorul de servicii de certificare	Modalitatea de acces la informațiile despre prestatorul de servicii de certificare

Anexa nr.11
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

Structura certificatului cheii publice a utilizatorului pentru autentificare bifactorială securizată

Certificatul cheii publice a utilizatorului conţine următoarele cîmpuri:

Denumirea (în engleză)	Descrierea	Conţinutul
Cîmpurile de bază		
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Numărul
Issuer	Datele de identificare ale prestatorului de servicii de certificare, emitent al certificatului	CN = Denumirea certificatului prestatorului de servicii de certificare L = Localitatea S = Statul OU = Prestatorul de servicii de certificare, 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 = nume.prenume utilizator CN = Numele, prenumele utilizatorului L = LocalitateaS = Statul OU = Subdiviziunea persoanei juridice, în care activează utilizatorul, după caz O = Denumirea persoanei juridice, IDNO, în care activează utilizatorul, după caz P = Telefonul utilizatorului T = Funcţia deţinută de către utilizator, după caz Street = adresa juridică PostalCode – Codul poştal corespunzător adresei juridice C = Codul statului E = adresa de email a utilizatorului
Subject Public Key Info	Cheia publică	Cheia publică a utilizatorului
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii electronice a emitentului certificatului
Signature Value	Semnătura electronice a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat
Cîmpurile auxiliare		
Key Usage	Utilizarea cheii	Digital Signature, Key Encipherment

Enhanced key Usage	Utilizarea extinsă a cheii	Client Authentication Server Authentication
Netscape Cert Type		SSL Client Authentication, SSL Server Authentication
Certificate Policies	Politica de certificare a prestatorului de servicii de certificare	Identificatorul politicii Informațiile calificatorului politicii
CRL Distribution Points	Punctul de distribuție a listei certificatelor revocate	Sursa publicării listei certificatelor revocate
Authority Information Access	Accesul la informațiile despre prestatorul de servicii de certificare	Modalitatea de acces la informațiile despre prestatorul de servicii de certificare

Anexa nr.12
la Codul de practici şi proceduri
al Centrului de certificare a cheilor publice

Structura certificatului cheii publice a sistemului informaţional electronic

Certificatul cheii publice conţine următoarele cîmpuri:

Denumirea (în engleză)	Descrierea	Conţinutul
Cîmpurile de bază		
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Numărul
Issuer	Datele de identificare ale prestatorului de servicii de certificare, emitent al certificatului	CN = Denumirea certificatului prestatorului de servicii de certificare L = Localitatea S = Statul OU = Prestatorul de servicii de certificare, subdiviziunea persoanei juridice O = Denumirea persoanei juridice 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	CN = Fully Qualified Name* L = Localitatea S = Statul OU = Subdiviziunea persoanei juridice, responsabilă de utilizarea certificatului chei publice, după caz O = Denumirea persoanei juridice, IDNO, după caz C = Codul statului
Subject Public Key Info	Cheia publică	Cheia publică
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii electronice a emitentului certificatului
Signature hash algorithm	Algoritmul hash al semnăturii emitentului certificatului	Denumirea algoritmului hash al semnăturii electronice a emitentului certificatului
Cîmpurile auxiliare		
Authority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a prestatorului de servicii 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	Semnătura digitală (Digital Signature), criptarea cheilor (Key Encipherment)
Enhanced Key Usage	Utilizarea extinsă a cheii	Autentificarea clientului (Client Authentication)
Netscape Cert Type		Autentificarea SSL a clientului (SSL Client Authentication)
Certificate Policies	Politica de certificare a prestatorului de servicii de certificare	Identificatorul politicii Informaţiile calificatorului politicii
Basic Constraints	Restricţii de bază	Tipul subiectului = utilizatorul final Limitarea lungimii lanţului de certificate = lipseşte
CRL Distribution Points	Punctul de distribuţie a listei certificatelor revocate	Sursa publicării listei certificatelor revocate
Authority Information Access	Accesul la informaţiile despre prestatorul de servicii de certificare	Modalitatea de acces la informaţiile despre prestatorul de servicii de certificare

* în calitate de CN va fi folosit FQN (Fully Qualified Name) cu urmatoarea structură:

DenumireaSistemuluiInformational.DenumireaOrganizatiei.pki.gov.md

NOTĂ: în CN nu se acceptă spaţii libere.

Denumirea organizaţiei şi a sistemului informativ se indică prescurtat.