ÎS CENTRUL DE TELECOMUNICAȚII SPECIALE

CENTRUL DE CERTIFICARE A CHEILOR PUBLICE

POLITICA

de certificare a cheilor publice

Iunie 2013

Chişinău 2013

CUPRINS

I. TERMENI ŞI ABREVIERI

1.1. ABREVIERI

CTS – Î.S. „Centrul de telecomunicaţii speciale”

CCCPAAP - Centrul de certificare a cheilor publice al autorităţilor administraţiei publice

CPP -- Codul de Practici şi Proceduri

CRL – lista certificatelor revocate (Certificate Revocation List)

1.2. TERMENI

Abonat -- titularul certificatului, datele căruia se conţin în cîmpul *Subject* al certificatului cheii publice,

certificat al cheii publice – document electronic conţinînd cheia publică, semnat cu semnătura digitală a persoanei împuternicite a CCCPAAP, document ce atestă apartenenţa cheii respective titularului certificatului cheii publice şi permite identificarea acestui titular.

II. CONTEXT

2.1. SCOP DOCUMENT

Politica de certificare a CCCPAAP descrie regulele generale folosite de acesta în procesul de certificare a cheilor publice pentru semnătura digitală cu forță juridică. În Politica de certificare sunt definite:

1. părțile implicate;
2. responsabilitățile şi obligațiile părților;
3. procedura de verificare a identității;
4. profilurile certificatelor;
5. domeniile de aplicabilitate.

Procedurile de mai sus sunt descrise detaliat în Codul de Practici şi Proceduri.

2.2. SFERA DE APLICARE

Certificatele cheilor publice pentru semnătura digitală cu forță juridică (*certificatul cheii publice*) sunt utilizate de autoritățile administrației publice, persoanele juridice cu diverse forme de activitate şi de persoanele fizice pentru aplicarea semnăturii digitale pe orice document în format electronic. Serviciile publice electronice disponibile în prezent utilizează cu succes aceste certificate.

2.3. CERTIFICATUL CHEII PUBLICE

Certificatele sunt conforme cu Directiva 1999/93/EC a Parlamentului European referitoare la Cadrul Comunitar privind Semnatura Electronică, ITU-T Recomandation X.509, versiunea 3, standardul SMV ISO CEI 9594-8:2007 *Information technology. Open Systems Interconnection. The Directory: Public-key and attribute certificate frameworks*, IETF RFC 3280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Legea cu privire la documentul electronic şi semnătura digitală nr. 264-XV din 15.07.04, Normele tehnice în domeniul semnăturii digitale (aprobate prin Ordinul directorului Serviciului de Informaţie şi Securitate nr. 64 din 07.12.2006). Certificatul cheii publice se utilizează, în mod obligator, cu programe specializate pentru aplicarea şi verificarea semnăturii digitale în documentele în format electronic ce corespund legislaţiei în vigoare (Legea nr. 264-XV din 15.07.04, cap. IV, art. 22), standardelor SMV CWA14170:2007 *Cerinţe de securitate pentru aplicaţiile de creare a semnăturii* şi SMV CWA 14171:2007 *Ghid general pentru verificarea semnăturii electronice*. În Republica Moldova acestea sunt MoldSign SmartSign, PKI Server, Signer Applet.

Certificatul leagă datele personale ale abonatului (titularul certificatului, datele căruia se conţin în cîmpul *Subject*) cu cheia publică. Titularul certificatului este şi posesorul cheii private, corespunzătoare cheii publice certificate. Datele de identificare din certificat permit constatarea titularului certificatului. Cheia privată utilizată în procesul de semnare a documentelor în format electronic asigură destinatarului convingerea că documentul a fost semnat cu cheia privată, corespunzătoare cheii publice din certificat.

Prin emiterea certificatului cheii publice Centrul de certificare confirmă:

- identitatea abonatului şi veridicitatea datelor prezentate de acesta,
- apartenenţa de către abonat a cheii publice certificate.

În baza celor menţionate, părţile parteneriale, după primirea documentului electronic, pot verifica semnăturile digitale aplicate documentului respectiv şi elaboratorii - titulari ai certificatelor cheilor publice. În plus, documentul electronic poate fi folosit în instanţa de judecată.

Identificatorul politicii de certificare este 1.2.498.3.3.1.

Centrul de certificare prestează servicii în baza legislaţiei şi a actelor normative din domeniul semnăturii digitale. Cheile autorităţii de certificare sunt protejate folosind module hardware de securitate (Hardware Security Module - HSM), certificate conform FIPS PUB140-2 *Security Requirements For Cryptographic Module nivelul 3*.

2.4. PROFILUL CERTIFICATULUI

2.4.1. PROFILUL CERTIFICATULUI CHEII PUBLICE A ABONATULUI

Certificatul cheii publice constă din următoarele cîmpuri şi extensii (determinate de actele normative în vigoare şi de CCCPAAP).

Denumire (în eng.)	Descriere	Conținut
Cîmpurile de bază		
Version	Versiunea	V3
Serial number	Numărul de înregistrare a certificatului	Număr aleator
Issuer	Datele de identificare ale emitentului	CN = Denumirea Centrului de certificare OU = Subdiviziunea persoanei juridice, numele, prenumele, IDNP-ul persoanei împuternicite a Centrului de certificare O = Denumirea persoanei juridice, IDNO L = Localitatea S = Statul C = Codul statului
Valid from	Perioada de valabilitate	Valabil de la: «__» _____ 20__ hh:mm:ss GMT
Valid to	Perioada de valabilitate	Valabil pînă la: «__» _____ 20__ hh :mm:ss GMT
Subject	Datele de identificare ale titularului certificatului	SERIALNUMBER=IDNP-ul titularului Phone = Numărul de telefon al titularului T = Funcția titularului CN = Numele, prenumele titularului PostalCode=Codul poştal STREET=Adresa juridică a persoanei juridice OU = Subdiviziunea persoanei juridice O = Denumirea persoanei juridice, IDNO L = Localitatea S = Statul C = Codul statului
Public Key	Cheia publică	Cheia publică a titularului
Signature Algorithm	Algoritmul de semnare a emitentului certificatului	Denumirea algoritmului semnăturii digitale a emitentului certificatului

Cîmpurile alternative		
Key Usage	Utilizarea cheii	Non-repudiere
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a titularului certificatului, corespunzătoare cheii publice
Authority Key Identifier	Identificatorul cheii Centrului de certificare	Identificatorul cheii private a persoanei împuternicite a Centrului de certificare, corespunzătoare cheii publice certificate
CRL Distribution Point	Punctul de distribuție a listei certificatelor revocate	Sursa de publicare a listei certificatelor revocate
Certificate Policies	Politici de certificare	Identificatorul politicii de certificare şi calificatorul (http://www.ca.cts.md)
1.3.6.1.5.5.7.1.3	Valoarea OID	Valoare ce confirmă emiterea certificatului cheii publice pentru semnătura digitală cu forță juridică conform legislației şi actelor normative în vigoare
Thumbprint algorithm	Algoritmul „amprentei”	Algoritmul „amprentei”
Thumbprint	„Amprenta”	„Amprenta”
IssuerAlternativeName	URL	URL emitentului
Subject Alternative Name	E-mail	Adresa de e-mail a titularului

2.4.2. PROFILUL CERTIFICATULUI CHEII PUBLICE A CCCPAAP

Denumire (în eng.)	Descriere	Conținut
Cîmpurile de bază		
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Număr aleator
Issuer	Datele de identificare ale emitentului	CN = Denumirea Centrului de certificare de nivel superior OU = Subdiviziunea persoanei juridice, numele, prenumele, IDNP-ul persoanei împuternicite a Centrului de certificare de nivel superior O = Denumirea persoanei juridice, IDNO L = Localitatea S = Statul C = Codul statului
Valid from	Perioada de valabilitate	Valabil de la: «__» _____ 20__ hh:mm:ss GMT
Valid to	Perioada de valabilitate	Valabil pînă la: «__» _____ 20__ hh :mm:ss GMT
Subject	Datele de identificare ale persoanei împuternicite	CN = Denumirea Centrului de certificare OU = Subdiviziunea persoanei juridice, numele, prenumele, IDNP-ul persoanei împuternicite a Centrului de certificare O = Denumirea persoanei juridice, IDNO L = Localitatea S = Statul C = Codul statului
Public Key	Cheia publică	Cheia publică
Signature Algorithm	Algoritmul de semnare a emitentului certificatului	Denumirea algoritmului semnăturii digitale a emitentului certificatului

Cîmpurile alternative		
Key Usage	Utilizarea cheii	Semnarea certificatelor, semnarea automată a listei certificatelor revocate, semnarea listei

		certificatelor revocate
Subject Key Identifier	Identificatorul cheii Centrului de certificare	Identificatorul cheii private a persoanei împuternicite a Centrului de certificare, corespunzătoare cheii publice certificate
Authority Key Identifier	Identificatorul cheii Centrului de certificare de nivel superior	Identificatorul cheii private a persoanei împuternicite a Centrului de certificare de nivel superior, corespunzătoare cheii publice certificate
CRL Distribution Point	Punctul de distribuție a listei certificatelor revocate	Sursa de publicare a listei certificatelor revocate
Certificate Policies	Politici de certificare	Identificatorul politicii de certificare şi calificatorul (http://www.pki.sis.md)
Private Key Usage Period	Perioada de utilizare a cheii private	Perioada de utilizare a cheii private aa.ll.dd hh.mm.ss
BasicConstraints	Constrîngeri de bază	Determină tipul subiectului şi constrîngerea la lungimea lanțului de certificare
Thumbprint algorithm	Algoritmul „amprentei”	Algoritmul „amprentei”
Thumbprint	„Amprenta”	„Amprenta”
IssuerAlternativeName	URL	URL emitentului

2.4.3. PROFILUL LISTEI CERTIFICATELOR REVOCATE

Lista certificatelor revocate, emisă de CCCPAAP, conține următoarele cîmpuri de bază şi alternative:

Denumire (în eng.)	Descriere	Conținut
Cîmpurile de bază		
Version	Versiunea	V2
Issuer	Emitentul CRL	CN = Denumirea Centrului de certificare OU = Subdiviziunea persoanei juridice, numele, prenumele, IDNP-ul persoanei împuternicite a Centrului de certificare O = Denumirea persoanei juridice, IDNO L = Localitatea S = Statul C = Codul statului
thisUpdate	Timpul emiterii CRL	«__» _____ 20__ hh:mm:ss GMT
nextUpdate	Timpul actualizării CRL	«__» _____ 20__ hh:mm:ss GMT
Issuer Signature Algorithm	Algoritmul de semnare a emitentului listei CRL	Denumirea algoritmului semnăturii digitale a emitentului listei CRL
Revoked Certificates	Lista certificatelor revocate	Numărul de serie al certificatului (CertificateSerialNumber) Data şi ora revocării
Cîmpurile alternative		
CRLNumber	Numărul CRL	Numărul de serie al CRL
Reason Code	Codul cauzei revocării certificatului	"0" nu este indicat "1" compromiterea cheii private "2" compromiterea cheii private a Centrului de certificare "3" schimbarea apartenenței "4" modificarea certificatului

		"5" stoparea activității "6" suspendarea certificatului
Authority Key Identifier	Identificatorul cheii emitentului	Identificatorul cheii private a persoanei împuternicite a Centrului de certificare, cu care este semnată lista CRL

2.5. GARANȚIILE OFERITE

Centrul de certificare va depune efortul necesar pentru a verifica informațiile incluse în certificate şi este responsabil, din punct de vedere financiar, pentru pagubele rezultate ca urmare a neglijenței sau erorilor comise ce țin de certificat. Responsabilitatea este atît față de abonați, cît şi față de entitățile partenere ce au încredere în datele din certificate. Centrul de certificare garantează unicitatea semnăturilor digitale pentru abonații săi.

2.6. ACCEPTAREA CERTIFICATULUI

Responsabilitatea şi garanţiile Centrului de certificare intră în vigoare odată cu acceptarea certificatului de către abonat. Furnizarea certificatului către abonat are loc prin intermediul persoanei responsabile din cadrul persoanei juridice. În cazul persoanelor fizice este obligatorie prezența personală la Centrul de certificare.

2.7. ENTITATEA PARTENER

Entitatea partener este obligată să verifice autenticitatea semnăturii digitale în documentele electronice, utilizînd mijloacele tehinice şi de program specializate, certificatul cheii publice al elaboratorului documentului.

2.8. ABONATUL

Abonatul este obligat să excludă accesul unei alte persoane la cheia sa privată, să utilizaze mijloacele semnăturii digitale şi programul specializat conform documentaţiei de exploatare, să nu utilizeze cheia sa privată dacă are motive să presupună că este încălcată confidenţialitatea cheii private, să solicite revocarea certificatului cheii publice. Pentru revocarea certificatului informaţiile furnizate trebuie să fie suficiente pentru a determina cu exactitate identitatea persoanei.

2.9. ACTUALIZAREA POLITICII DE CERTIFICARE

Politica de certificare se poate modifica periodic. Versiunile acestui document sunt disponibile abonaților prin intermediul site-ului http://pki.cts.md.

2.10. TAXE

Serviciile prestate de Centrul de certificare a cheilor publice (identificarea şi înregistrarea abonatului, eliberarea/revocarea certificatului) sunt disponibile contra cost. Pentru detalii contactați prestatorul.