ÎS CENTRUL DE TELECOMUNICAȚII SPECIALE

CENTRUL DE CERTIFICARE A CHEILOR PUBLICE

POLITICA

de utilizare a certificatelor SSL

Iunie 2013

Chişinău 2013

CUPRINS

I. TERMENI ŞI ABREVIERI

1.1. ABREVIERI

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

CCCPAAP - Centrul de certificare a cheilor publice al autorităților administrației publice

CPP -- Codul de Practici şi Proceduri

SSL -- Secure Socket Layer

1.2. TERMENI

Certificat de server (certificate SSL) – certificat instalat pe serverul web prin care poate fi stabilită identitatea şi autenticitatea serverului web de către browserul utilizatorului,

SSL (Secure Sockets Layer) -- acronim ce reprezintă un protocol web pentru a transmite fără risc documente private prin Internet.

II. CONTEXT

2.1. SCOP DOCUMENT

Politica de utilizare a certificatelor SSL, eliberate de CCCPAAP, conține prevederile de bază, legate de aspectele normative şi operaționale în utilizarea certificatelor SSL.

Politica de utilizare a certificatelor SSL este un document de bază, ce stabileşte cerințe legale, operaționale şi tehnice în scopul de gestionare, utilizare, revocare şi de actualizăre a Politicii de utilizare a certificatelor SSL, eliberate de CCCPAAP, totodată se oferă posibilitatea de a evalua fiabilitatea utilizării certificatului SSL.

Cerințele sus-menționate sunt descrise detaliat în CPP, publicat pe site-ul http://pki.cts.md.

2.2. SFERA DE APLICARE

Certificatele SSL sunt utilizate în scopul creării canalelor securizate de transmitere a datelor prin intermediul protocoalelor TLS/SSL. Utilizarea certificatelor SSL asigură:

- **Autentificarea serverului.** În timp ce clientul se autentifică în dependență de algoritm, serverul se autentifică permanent.
- **Confidențialitatea mesajului.** Datele transmise nu pot fi vizualizate sau interceptate de terțe persoane.
- **Integritatea datelor.** Datele sunt transmise integral şi nu pot fi schimbate sau pierdute.

2.2.1. SARCINI PRINCIPALE

Principalele sarcini ale certificatului SSL sunt:

- determină dacă site-ul web aparține anumitei companii; certificatul SSL poate conține informații despre compania, căreia i-a fost eliberat certificatul, numele de domen, amplasarea, adresa juridică şi e-mail, numărul de înregistrare şi valabilitatea certificatului;
- criptează conexiunea între utilizator şi server; în timpul unei sesiuni de comunicare, are loc schimbul de chei cu scopul transmiterii informației criptate prin intermediul Internetului.

1.2.2. SARCINI SUPLIMENTARE

Certificatele SSL pot servi drept confirmare că terța parte independentă, şi anume CCCPAAP, confirmă faptul că site-ul web aparține anumitei companii. De fapt, certificatele SSL asigură integritatea, fiabilitatea şi transmiterea datelor, totodată:

- contribuie la prevenirea phishingului şi altor atacuri cibernetice;
- asigură asistență companiilor, care pot deveni țintă ale atacurilor de tip fishing şi a altor fraude on-line, oferind instrumente pentru a confirma apartenența site-lui web anumitei companii şi legalitatea lui;
- oferă ajutor organelor de drept în investigarea fraudelor cibernetice.

2.3. GARANȚII ŞI FIABILITATE

Asigurarea garanțiilor şi fiabilității certificatelor SSL intervine în momentul în care CCCPAAP eliberează certificatul şi parcurge toată perioadă valabilității certificatului. Procedura de eliberare şi transmitere a certificatului este descrisă detaliat în CPP şi în acordurile semnate cu solicitant. În momentul eliberării certificatului SSL, CCCPAAP confirmă faptul că solicitantul a depus pachetul de documente, necesare pentru eliberarea certificatului SSL, şi astfel a confirmat legalitatea activității sale şi existenței fizice (lista documentelor necesare pentru obținerea certificatului SSL sunt prezentate pe site-ul http://pki.cts.md/servicii/certificate-de-server). De asemenea:

- CCCPAAP garantează faptul că informația indicată în certificat corespunde documentelor oficiale prezentate de către solicitant;
- la momentul depunerii documentelor necesare solicitantul deține dreptul exclusiv asupra numelui de domen;
- CCCPAAP asigură accesul on-line 24/7 la lista certificatelor SSL revocate.

2.4. CONDIȚII DE CERTIFICARE

2.4.1. ELIBERAREA CERTIFICATULUI SSL

CCCPAAP este organul abilitat să elibereze certificatul SSL la cererea solicitantului. Solicitantul generează perechea de chei şi se adresează la CCCPAAP. După verificarea şi aprobarea documentelor depuse CCCPAAP eliberează certificatul SSL.

Notificarea oficială cu privire la faptul că a fost eliberat certificatul SSL este publicarea acestui certificat în Repozitoriu. În cazul verificării pozitive a cererii pentru certificatul SSL, solicitantul primeşte răspunsul pozitiv prin emiterea certificatului SSL. CCCPAAP poate expedia solicitantului un aviz de eliberare a certificatului SSL prin intermediul poştei electronice sau prin telefon.

2.5. STRUCTURA CERTIFICATULUI SSL

2.5.1. CÎMPURILE DE BAZĂ ALE CERTIFICATULUI

Certificatele, eliberate de CCCPAAP, au următoarele cîmpuri de bază, semnificația cărora este stabilită în conformitate cu normele, prezentate în tabelul de mai jos:

Cîmpurile de bază		
Version	Versiunea	V3
Serial Number	Numărul de înregistrare a certificatului	Număr aleator
Issuer	Datele de identificare a centrului de certificare, emitentul certificatului	N = Numele, prenumele persoanei împuternicite a centrului de certificare, IDNP CN = Denumirea centrului de certificare L = Localitate S = Stat OU = Subdiviziunea emitentului O = Denumirea emitentului, IDNO P = Telefonul de contact a persoanei împuternicite a centrului de certificare PostalCode = Codul poştal al emitentului STREET= Adresa juridică emitentului T = Funcția persoanei împuternicite a centrului de certificare C = Codul statului E = Poşta electronică a persoanei împuternicite a centrului de certificare
Valid from	Perioada de valabilitate a certificatului	Valabil din: «__» _____ 20__ hh:mm:ss GMT
Valid to	Perioada de valabilitate a certificatului	Valabil pînă la: «__» _____ 20__ hh:mm:ss GMT
Subject	Datele de identificare a titularului certificatului	E = Poşta electronică persoanei responsabile a persoanei juridice P = Telefonul de contact a persoanei responsabile a persoanei juridice CN = Denumirea numelui de domen PostalCode= Codul poştal a adresei juridice a persoanei juridice STREET= Adresa juridică a persoanei juridice OU = Subdiviziunea persoanei juridice O = Denumirea persoanei juridice, IDNO

		L = Localitate S = Stat C = Codul statului
Public Key	Cheia publică	Cheia publică
Signature Algorithm	Algoritmul de semnare a emitentului certificatului	Denumirea algoritmului semnăturii digitale a emitentului certificatului

2.5.2. CÎMPURILE ALTERNATIVE ALE CERTIFICATULUI

Certificatele, eliberate de CCCPAAP, pentru autentificarea serverului şi domenuri de rețea (inclusiv Wildcard), au următoarele cîmpuri alternative:

Cîmpuri alternative		
Issuer Alternative Name	Numele alternativ al emitentului	URL emitentului
Authority Information Access	Acces la informațiile centrului de certificare	URL pentru stabilirea statutului certificatului
Key Usage	Utilizarea cheii	Non-repudierea, semnătura digitală, criptarea cheilor, key agreement
Extended Key Usage	Utilizarea extinsă a cheii	Autentificarea serverului
Netscape Cert Type	Tipul certificatului Netscape	SSL-autentificarea serverului
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private, corespunzătoare cheii publice certificate
CRL Distribution Point	Punctul distribuiție a listei certificatelor revocate	Sursa de publicare a listei certificatelor revocate
Basic Constraints	Constrîngeri de bază	Determină tipul subiectului şi constrîngerea la lungimea lanțului de certificare
Thumbprint algorithm	Algoritmul „amprentei”	Denumirea algoritmului
Thumbprint	„Amprenta”	„Amprenta”

2.6. PROCEDURA DE REVOCARE A CERTIFICATULUI SSL

Revocarea certificatului SSL se efectuează prin depunerea cererii de revocare la CCCPAAP. Din momentul primirii şi aprobării cererii de revocare a certificatului SSL, CCCPAAP este obligat în termen de 3 ore lucrătoare să efectueze procedura dată. Notificarea oficială cu privire la revocarea certificatului SSL se consideră publicarea în lista certificatelor revocate.

2.6.1. CAUZELE REVOCĂRII CERTIFICATULUI SSL

CCCPAAP revocă certificatul în următoarelor cazuri:

- la cererea titularului certificatului,
- în cazul compromiterii cheii private,
- efectuarea modificărilor în certificatul cheii publice,
- la decizia CCCPAAP (în cazul în care solicitantul încalcă prevederile CPP şi Politicii de utilizare a certificatelor SSL sau cerinţele altor documente de reglementare, publicate de CCCPAAP),
- în momentul în care CCCPAAP îşi suspendă activitatea în domeniul semnăturii digitale, toate certificatele valabile eliberate şi publicate, într-un termen determinat vor fi revocate paralel cu certificatul CCCPAAP,
- atunci cînd solicitantul reţine sau ignoră achitarea serviciilor de certificare,
- în cazul în care încrederea faţă de gradul de fiabilitate a cheii private a CCCPAAP a fost subminată,
- dacă s-a depistat că există erori în datele indicate în cererea de certificare sau în certificat.

2.7. PERECHEA DE CHEI ŞI UTILIZAREA CERTIFICATULUI SSL

2.7.1. CHEIA PRIVATĂ A CERTIFICATULUI SSL ŞI UTILIZAREA EI

Utilizarea certificatelor trebuie să fie în strictă conformitate cu prevederile prezentei Politici de utilizare a certificatelor SSL şi conținutului extensiei cîmpurilor KeyUsage („Utilizarea cheii") (e.g., în caz dacă nu este bifat „Criptarea cheilor", utilizarea certificatului pentru autentificare nu este admisă).

2.7.2. CHEIA PUBLICĂ A CERTIFICATULUI SSL ŞI UTILIZAREA EI

Titularii certificatelor SSL au dreptul să le utilizeze în orice aplicații, dar strict în limitele stabilite în prezenta Politică de utilizare a certificatelor SSL.

Pentru a avea încredere în certificatul SSL şi înainte de utilizarea acestuia, titularul certificatului trebuie să stabilească:

- aplicabilitatea şi oportunitatea utilizării certificatului SSL cu un anumit scop. Totodată titularul certificatului SSL trebuie să fie sigur că va fi utilizat în scopuri ce nu contrazic cerințelor Politicii de utilizare a certificatelor SSL. CCCPAAP nu poartă răspundere pentru determinarea aplicabilității şi oportunității de utilizare a certificatului SSL,
- faptul că certificatul SSL va fi utilizat în conformitate cu extensiile cîmpurilor sale KeyUsage („Utilizarea cheii").

2.8. CERTIFICATELE SSL EMISE DE ALTE AUTORITĂȚI DE CERTIFICARE

CCCPAAP eliberează, în bază contractuală, certificate SSL emise de alte autorități de certificare, recunoscute implicit în browsere. Astfel, orice solicitant poate beneficia de o gamă largă de certificate SSL.

2.8.1. CERTIFICATE SSL EMISE DE UNIZETO TECHNOLOGIES S.A.

Autoritatea de încredere Unizeto Technologies S.A. emite următoarele tipuri de certificate: Commercial SSL, Trusted SSL, Premium EV SSL. Informație detaliată despre acestea, inclusiv descrierea şi asigurarea oferită, se găseşte în „Certification Policy of CERTUM's Certification Services" şi „Certification Practice Statement of CERTUM's Certification Services", accesibile pe http://www.certum.eu/certum/cert,expertise_certyfication_policy.xml şi, respectiv, http://www.certum.eu/certum/cert,expertise_practice_statement.xml.

2.8.2. CERTIFICATE SSL EMISE DE SYMANTEC

Autoritatea de Certificare şi Înregistrare Symantec administrează procesul de emitere al certificatelor SSL, ce au ca şi autorități de rădăcină (ROOT) VeriSign, Thawte si GeoTrust. Informație detaliată despre acestea este accesibilă pe http://www.symantec.com/about/profile/policies/repository.jsp.

2.9. ACTUALIZAREA POLITICII DE UTILIZARE A CERTIFICATELOR SSL

Politica de utilizare a certificatelor SSL se poate modifica periodic. Versiunile acestui document sunt disponibile prin intermediul site-ului http://pki.cts.md.