

POLITICA DE CERTIFICARE





Cuprins

1. Introducere	3
2. Certificatele.....	3
2.1. Certificate de Clasă 1	5
2.2. Certificate de Clasă 2	5
2.3. Certificate de Clasă 3	6
2.4. Certificate de Clasă 4	7
3. Jetoane de ne-repudiere	7
3.1. Mărcile Temporale.....	8
3.2. Răspunsul de confirmare OCSP.....	8
4. Garanțiile oferite de certSIGN	9
5. Acceptarea certificatului	9
6. Serviciul de certificare	10
7. Entitatea Partener	11
8. Abonatul	11
9. Actualizarea politicii de certificare	11
10. Taxe.....	12

1. Introducere

Politica de Certificare a certSIGN (CP) descrie regulile și principiile generale aplicate de certSIGN în procesul de certificare a cheilor publice și folosire a autorității de marcare a timpului (TSA), precum și a altor servicii de ne-repudiere. Politica de certificare definește:

- entitățile implicate în procesele de certificare;
- responsabilitățile și obligațiile fiecărei entități;
- tipurile de certificate ;
- tipurile de confirmări;
- procedurile de verificare a identității și
- aria de aplicabilitate.

Descrierea detaliată a regulilor de mai sus este prezentată în **Codul de Practici și Proceduri (CPP)**. Cunoașterea Politicii de Certificare, precum și al Codului de Practici și Proceduri prezintă importanță în mod special pentru abonații și entitățile partenere ale certSIGN.

2. Certificatele

Certificatul este un șir de date (mesaj) care conține cel puțin numele și identificatorul autorității, identificatorul abonatului, cheia sa publică, perioada de validitate, numărul serial și semnătura autorității emitente.

Certificatele sunt utilizate pentru a lega datele personale ale abonatului de cheile publice specifice. Proprietarul certificatului este, de asemenea, și proprietarul cheii private, corespunzătoare cheii publice conținută în certificat. Datele de identificare conținute în certificat permit altor părți să determine cu exactitate proprietarul certificatului. Dacă cheia privată este utilizată în timpul semnării electronice a unui mesaj, destinatarul mesajului poate fi sigur că mesajul a fost creat folosind cheia privată, corespunzătoare cheii publice conținută în certificat (deci a fost creată de proprietarul certificatului) și mesajul nu a fost modificat de către altcineva.

Autoritatea de Certificare certSIGN CA confirmă prin emiterea unui certificat pentru un abonat:

- Identitatea acestuia sau credibilitatea altor date, ca de exemplu adresa căsuței de poștă electronică;

- Cheia publică conținută de certificat aparține abonatului respectiv.

Datorită celor de mai sus, entitățile partener, după recepția unui mesaj semnat, pot determina cine este proprietarul certificatului care a semnat mesajul și, opțional, îl pot trage pe acesta la răspundere pentru acțiunile sale sau angajamentele luate.

certSIGN furnizează servicii în concordanță cu legislația și practicile în domeniu. Cheile autorității de certificare sunt protejate folosind module hardware de securitate (Hardware Security Module - HSM), certificate conform FIPS 140-1 nivel 3. certSIGN implementează controalele fizice și procedurale ale sistemului.

Autoritatea de Certificare certSIGN emite certificate de diferite Clase, având nivele de credibilitate diferite. Credibilitatea certificatului depinde de procedura de verificare a identității abonatului și de efortul depus de operatorii certSIGN pentru a verifica datele trimise de către solicitant în cererea sa de înregistrare. Clasa certificatului poate, de asemenea să depindă de Clasa de securitate a serverului sau dispozitivului de rețea pentru care se emite certificatul. Specialiștii certSIGN pot verifica starea tehnică și Clasa de securitate a sistemului informatic al unui abonat

înainte de a emite un certificat din cea mai înaltă Clasă de credibilitate.

Autoritatea de Certificare certSIGN CA emite certificate pentru publicul larg și furnizează servicii specifice unei infrastructuri de chei publice. Printre cele mai importante aplicații ale certificatelor emise de certSIGN CA, se numără (fără a se limita la):

- Semnarea documentelor electronice;
- Securizarea mesajelor de e-mail (poștă electronică);
- Securizarea tranzacțiilor Web;
- Securizarea comunicațiilor de rețea;
- Semnarea codului pentru aplicații;
- Marcarea timpului.



2.1. Certificate de Clasă 1

Certificatele de Clasă 1 sunt emise de Autoritatea de Certificare **certSIGN Demo CA Class 1**. Aceste certificate sunt folosite numai pentru scopuri demonstrative și nu oferă nici o garanție asupra identității subiectului. Certificatele demo sunt destinate în principal pentru testarea performanței aplicațiilor sau dispozitivelor înainte de cumpărarea certificatelor finale. Autoritatea de Certificare certSIGN Demo CA Class 1 emite certificate pentru aproape toate scopurile. În majoritatea cazurilor, în timpul procesului de înregistrare se verifică adresa căsuței de mesagerie electronică și/sau numele și prenumele persoanei fizice sau al reprezentantului persoanei juridice.

Certificatele de Clasa 1 conțin următorul identificator de politică:

{certSIGN}* id-policy(1) id-cp(1)id-Class-1(1)

certSIGN nu își asumă nici o obligație financiară și nu oferă nici o garanție pentru certificatele (și conținutul acestora) emise în cadrul politicii de mai sus.

2.2. Certificate de Clasă 2

Certificatele de Clasă 2 sunt emise de Autoritatea de Certificare **certSIGN Personal CA Class 2**. Acestea sunt certificate personale și sunt destinate în principal pentru securizarea corespondenței electronice sau autentificarea clienților în timpul sesiunilor online. Operatorii Autorității de Certificare certSIGN Personal CA Class 2 verifică datele furnizate de clienți în timpul procesului de certificare. Identitatea persoanei fizice solicitante sau a reprezentantului persoanei juridice este supusă unei verificări detaliate. Autenticitatea adresei căsuței de mesagerie electronică inclusă în certificat este de asemenea verificată.

Certificatele de Clasa 2 conțin următorul identificator de politică:

{certSIGN} .id-policy(1). id-cp(1).id-Class-2(2)

Certificatele emise în cadrul acestei politici oferă garanții și responsabilități limitate.

* {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN's IANNA assigned number (20715)

2.3. Certificate de Clasă 3

Certificatele de Clasă 3 sunt emise de Autoritatea de Certificare **certSIGN Enterprise CA Class 3**. Certificate emise în această clasă pot fi certificate calificate sau certificate pentru securizarea obiectelor binare și protecția transmisiilor de date utilizând protocoalele IPSec, SSL și TLS. Operatorii certSIGN Enterprise CA Class 3 verifică datele furnizate de clienți (organizații sau instituții) în timpul procesului de înregistrare. Toate datele ce urmează a fi incluse în certificat sunt verificate. Sunt necesare documente adiționale care să confirme autenticitatea organizației și dreptul de utilizare a domeniului Internet. Pe baza unui certificat emis de certSIGN Enterprise CA Class 3 se poate determina cu exactitate identitatea unui subiect sau autenticitatea unei organizații.

Certificatele calificate emise de certSIGN tot în Clasa 3 pot fi utilizate pentru crearea de semnături electronice care să înlocuiască semnăturile olografe.

Certificatele calificate sunt emise de Autoritatea de Certificare **certSIGN Qualified CA Class 3**. Aceste certificate sunt conforme cu Directiva 1999/93/EC a Parlamentului European referitoare la Cadrul Comunitar privind Semnatura Electronica, Legea Semnaturii Electronice 455/2001 din România și Hotărârea de Guvern 1259/Decembrie 2001 privind Normele de Aplicare ale Legii Semnăturii Electronice.

Certificatele de Clasa 3 conțin următorul identificator de politică:

{certSIGN} id-policy(1) id-cp(1)id-Class-3(3)

În plus, pentru certificatele calificate se adaugă următorul identificator de politică:

itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1).qcp-public-with-sscd (1)

Responsabilitatea financiară a certSIGN pentru datele din certificatele emise în cadrul politicii de mai sus este prezentată în Codul de Practici și Proceduri (CPP) (a se vedea <http://www.certSIGN.ro/repository>). Certificatele emise în cadrul acestei politici oferă garanții și responsabilități complete.

2.4. Certificate de Clasă 4

Certificatele de Clasă 4 sunt emise de Autoritatea de Certificare **certSIGN Non-Repudiation CA Class 4**. Aceste certificate sunt destinate în principal Autorităților de Certificare subordonate sau altor furnizori de servicii de încredere (OCSP sau Autorități de Marcare Temporală). Operatorii certSIGN Non-Repudiation CA Class 4 verifică identitatea clienților care trebuie să se prezinte personal la unul din ghișeele certSIGN. Se vor verifica împuternicirea din partea firmei, autenticitatea și corectitudinea documentelor de identitate furnizate precum și actele organizației. certSIGN Non-Repudiation CA Class 4 acceptă și documente autentificate de către un notar. Pe baza unui certificat emis de certSIGN Non-Repudiation CA Class 4 se poate determina cu exactitate identitatea unui subiect, autenticitatea unei organizații sau credibilitatea unei Autorități de Certificare externe. Perioada de valabilitate a unui certificat de Clasă 4 este de minim 2 ani. Cheile abonatului ce deține un certificat de Clasă 4 trebuie protejate utilizând module hardware de securitate (HSM).

Certificatele de Clasă 4 conțin următorul identificator de politică:

{certSIGN} id-policy(1) id-cp(1)id-Class-4(4)

Certificatele emise în cadrul acestei politici oferă garanții și responsabilități complete.

Abonatul certSIGN poate alege tipul de certificat potrivit nevoilor sale. Tipurile de certificate sunt descrise pe larg în Codul de Practici și Proceduri (CPP) care poate fi consultat pe site-ul Web al certSIGN. De asemenea, aceste informații pot fi primite și prin poștă electronică trimițând un mesaj la adresa: office@certSIGN.ro.

3. Jetoane de ne-repudiere

Jetoanele de ne-repudiere sunt structuri de date (mesaje) conținând cel puțin:

- informațiile furnizate de către client (de exemplu, valoare hash, numărul serial al certificatului, numărul cererii etc.) unei autorități de ne-repudiere și
- semnătura electronică a autorității respective.

Autoritățile de ne-repudiere care oferă servicii clienților sunt afiliate la certSIGN.

Prin emiterea unui jeton, o autoritate de ne-repudiere confirmă apariția unui eveniment în momentul creării acestuia sau la un moment de timp anterior. Acest eveniment poate fi: transmiterea unui document, data creării semnăturii etc. Entitatea parteneră poate verifica, pe baza datelor recepționate, corectitudinea semnăturii bazându-se pe încrederea în certSIGN CA.

3.1. Mărcile Temporale

Mărcile temporale sunt emise de Autoritatea **certSIGN Time-Stamping Authority**. Mărcile temporale, ca element de bază în asigurarea ne-repudierii, sunt emise atât persoanelor private cât și celor aparținând unei organizații. Mărcile temporale pot fi încorporate în:

- semnături electronice;
- acceptarea tranzacțiilor electronice;
- arhivarea datelor;
- notarizarea documentelor electronice etc.

Regulile ce stabilesc modul de operare al Autorității de Marcare Temporală precum și alte informații suplimentare legate de acest sistem sunt descrise într-un document separat (**a se vedea Politica certSIGN Time-Stamping Authority**).

Jetonul de marcă temporală conține următorul identificator de politică:

{certSIGN}* .id-Time-Stamping(2).Id-Policy(1)

Responsabilitatea financiară a certSIGN pentru timpul, data și alte informații suplimentare incluse în mărcile temporale emise în cadrul politicii de mai sus este prezentată în Politica certSIGN Time-Stamping Authority (**a se vedea <http://www.certSIGN.ro/repository>**). certSIGN Time-Stamping Authority oferă garanții pentru mărcile temporale emise în limitele specificate în Politica certSIGN Time-Stamping Authority.

3.2. Răspunsul de confirmare OCSP

Răspunsurile OCSP (*Online Certificate Status Protocol*) sunt emise de Autoritatea **certSIGN Validation Service**. Răspunsurile OCSP sunt utilizate în principal pentru determinarea stării



certificatelor. Aceste servicii sunt disponibile public și reprezintă o alternativă la Listele de Certificate Revocate (Certificate Revocation List – CRL). certSIGN Validation Service oferă garanții pentru răspunsurile OCSP emise, în limitele descrise în CPP. Modul de funcționare al autorității OCSP și informații suplimentare privind acest serviciu sunt prezentate pe pagina web (a se vedea <http://www.certSIGN.ro>) și în CPP.

4. Garanțiile oferite de certSIGN

În funcție de tipul de certificat emis, certSIGN garantează că va depune efortul necesar pentru a verifica în mod corespunzător informațiile incluse în cadrul certificatelor (a se vedea Codul de Practici și Proceduri - Capitolul 2.1: Obligații). Verificarea informațiilor este importantă în primul rând pentru entitățile partenere ce primesc mesaje de la un abonat care se identifică printr-un certificat digital calificat emis de certSIGN. În consecință, certSIGN este responsabilă din punct de vedere financiar pentru pagubele rezultate ca urmare a neglijenței sau erorilor comise de certSIGN în ceea ce privește aceste tipuri de certificate. Responsabilitățile certSIGN depind de clasa certificatului abonatului, iar responsabilitatea este atât față de abonat cât și față de entitățile partenere care au încredere în informațiile din certificat (a se vedea Codul de Practici și Proceduri – Capitolul 2.2 Responsabilități Juridice și 2.3 Responsabilități de natură financiară).

Garanțiile certSIGN pot fi limitate de anumite restricții. Aceste restricții sunt aduse la cunoștință abonatului care confirmă acest lucru în cadrul unei declarații (a se vedea declarația de Acceptare a Certificatului). certSIGN garantează unicitatea semnăturilor electronice pentru abonații săi.

5. Acceptarea certificatului

Responsabilitățile și garanțiile certSIGN se aplică din momentul acceptării certificatului de către abonat. Modalitatea de furnizare a certificatului și acceptanța certificatului sunt descrise în Codul de Practici și Proceduri (a se vedea capitolul 4.4 Acceptarea Certificatului) și sunt detaliate în acordurile încheiate cu abonații.

* {certSIGN}=1.3.6.1.4.1.25017= iso(1). identified-organization(3). dod(6). internet(1). private(4). enterprise(1). certSIGN's IANNA assigned number (25017)

6. Serviciul de certificare

certSIGN furnizează **patru servicii de bază**:

- (1) înregistrarea;
- (2) emiterea unui certificat digital;
- (3) reînnoirea unui certificat;
- (4) revocarea unui certificat ;
- (5) verificarea stării unui certificat.

În plus, certSIGN oferă și următoarele servicii de ne-repudiere:

- (6) Autoritate de Marcare Temporală;
- (7) Serviciu de validare on-line a stării certificatelor digitale.

Înregistrarea are ca scop verificarea identității unui abonat și precedă operațiunea de emitere a certificatului (a se vedea Codul de Practici și Proceduri, capitolul 4.1 Trimiterea cererii și Capitolul 4.3 Emiterea certificatului digital).

Reînnoirea unui certificat are loc atunci când un abonat înregistrat deja dorește să obțină un certificat pentru o aceeași cheie publică cu modificarea perioadei de valabilitate (a se vedea Codul de Practici și Proceduri, Capitolul 4.7 Certificarea cheii și schimbarea cheii certificatului).

Revocarea unui certificat are loc atunci când cheia privată corespunzătoare cheii publice din certificatul digital a fost compromisă sau este susceptibilă că ar putea fi compromisă (a se vedea Codul de Practici și Proceduri, Capitolul 4.9 Revocarea și suspendarea certificatelor).

Verificarea stării unui certificat este un serviciu prin care certSIGN confirmă validitatea unui certificat digital, folosind Listele de Certificate Revocate (CRL) emise de autoritățile afiliate. Verificarea stării unui certificat se poate realiza și prin intermediul serviciului de validare on-line a stării certificatelor (a se vedea Codul de Practici și Proceduri, Capitolul 4.9.7 Verificarea on-line a stării certificatelor).

certSIGN permite ca fiecare pereche de chei (privată-publică) să fie generată de către abonat. certSIGN poate face recomandări cu privire la dispozitivele pentru generarea cheilor. În anumite condiții specifice, certSIGN poate genera perechi de chei unice și livra aceste chei abonaților.

7. Entitatea Partener

Entitatea partener este obligată să verifice în mod corespunzător fiecare semnătură electronică de pe documentele recepționate (inclusiv certificatul digital). Pe timpul procesului de verificare, entitatea partener trebuie să utilizeze procedurile și resursele puse la dispoziție de certSIGN. Acestea specifică, printre altele, faptul că trebuie verificată lista de certificate revocate publicată de certSIGN și căile de certificare permise (**a se vedea Codul de Practici și Proceduri, Capitolul 2.1.4 Obligațiile entităților partener**).

Fiecare document pentru care există probleme la verificarea semnăturii digitale trebuie să fie respins și trebuie să fie verificat prin alte modalități sau proceduri, de exemplu verificarea documentului la un notar.

8. Abonatul

Abonatul este obligat să păstreze în siguranță cheia sa privată, pentru a preveni accesul neautorizat la aceasta al unei terțe părți. În cazul în care există bănuiala că a fost accesată de o terță parte, abonatul este obligat să anunțe imediat autoritatea care a emis certificatul sau digital. Informațiile furnizate autorității trebuie să fie suficiente pentru a determina cu exactitate identitatea persoanei căreia i se va revoca certificatul digital.

9. Actualizarea politicii de certificare

Politica de certificare a certSIGN se poate modifica periodic. Aceste modificări vor fi disponibile tuturor abonaților prin intermediul site-lui Web al certSIGN. Abonații care nu acceptă modificările aduse politicii de certificare trebuie să trimită către certSIGN o declarație în acest sens și să renunțe la serviciile oferite de certSIGN.



10. Taxe

Serviciile de certificare furnizate de certSIGN sunt disponibile comercial. Tarifele pentru aceste servicii depind de clasa certificatelor emise sau deținute de un abonat și de tipul de serviciu cerut. Tarifele sunt prezentate în listele de prețuri, disponibile pe site-ul certSIGN (<http://www.certSIGN.ro>).