Politica de Certificare certSIGN

Versiunea 1.13
Data: 6 Iunie 2022

Notă importantă

Adresa: Bd. Tudor Vladimirescu, nr. 29 A,
AFI Tech Park 1, București 050881, România

Telefon: 004-021-31.19.901
Fax: 004-021-31.19.905

Web: www.certsign.ro

Istoria documentului

Versiune	Data efectivă	Motiv	Persoana care a făcut modificarea
1.0	Aprilie 2006	Publicarea primei versiuni	Manager Servicii Electronice
1.1	Iulie 2009	Schimbarea sediului firmei in Sos. Oltenitei 107A, Sector 4, Bucuresti.	Manager Servicii Electronice
1.2	Martie 2014	Adaugarea noului CA Class 3 Enterprise G2	Director Tehnic
1.3	Iulie 2015	Adaugarea noilor autoritati de certificare certSIGN CA Class 2 G2 certSIGN Qualified CA Class 3 G2 certSIGN Non-Repudiation CA Class 4 G2	Director Tehnic
1.4	10 Ianuarie 2016	Adaugarea noilor autoritati de certificare cu circuit inchis, certificate care sunt emise pentru Sistemul Electronic de Plati operat de Transfond S.A	Director Tehnic
1.5	25 Ianuarie 2016	S-a adaugat o noua autoritate de certificare destinata emiterii de certificate de semnare cod . In descrierea politicii de certificare a fost inclus si OIDul pt Non-EV Code Signing 2.23.140.1.4.1. De asemenea in politica de certificare asociata certificatelor SSL a fost inclus OIDul OV 2.23.140.1.2.2.	Director Tehnic
1.6	26 Noiembrie 2018	Actualizare determinata de schimbarea sediului	Manager Politici PKI
1.7	31 Ianuarie 2019	Revizuire anuala	Manager Politici PKI
1.8	31 Ianuarie 2020	Revizuire anuală	Manager Politici PKI
1.9	29 Ianuarie 2021	Revizuire anuală	Manager Politici PKI
1.10	23 Martie 2021	Actualizare cu SSL CA pentru DV și EV	Manager Politici PKI
1.11	23 Noiembrie 2021	Actualizări și corecții minore	Manager Politici PKI
1.12	31 Ianuarie 2022	Revizuire anuală	Manager Politici PKI
1.13	6 Iunie 2022	Corectie minoră	Manager Politici PKI

Acest document a fost creat si este proprietatea:

Proprietar	Autor	Data creării
Manager Servicii Electronice	Manager Servicii Electronice	27 Ianuarie 2006

Lista de Distribuție

Destinatar	Data distribuirii
Public-Internet	Aprilie 2006
Public-Internet	Iulie 2009
Public-Internet	Martie 2014
Public-Internet	Iunie 2015
Public-Internet	25 Ianuarie 2016
Public-Internet	26 Noiembrie 2018
Public-Internet	31 Ianuarie 2019
Public-Internet	31 Ianuarie 2020
Public-Internet	29 Ianuarie 2021
Public-Internet	23 Martie 2021
Public-Internet	23 Noiembrie 2021
Public-Internet	31 Ianuarie 2022
Public-Internet	6 Iunie 2022

Acest document a fost aprobat de

Versiune	Nume	Data
1.0	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Aprilie 2006
1.1	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Iulie 2009
1.2	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Martie 2014
1.3	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Iunie 2015
1.4	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Decembrie 2015
1.5	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Ianuarie 2016
1.6	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Noiembrie 2016
1.7	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Incredere	Ianuarie 2019
1.8	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Ianuarie 2020
1.9	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Ianuarie 2021
1.10	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Martie 2021
1.11	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Noiembrie 2021
1.12	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Ianuarie 2022
1.13	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Iunie 2022

Cuprins

1 Introducere

Politica de Certificare a certSIGN (CP) descrie regulile şi principiile generale aplicate de certSIGN în procesul de certificare a cheilor publice şi folosire a autorităţii de marcare a timpului (TSA), precum şi a altor servicii de ne-repudiere. Politica de certificare defineşte:
▪ entităţile implicate în procesele de certificare,
▪ responsabilităţile şi obligaţiile fiecărei entităţi,
▪ tipurile de certificate,
▪ tipurile de confirmări,
▪ procedurile de verificare a identităţii şi
▪ aria de aplicabilitate.

Descrierea detaliata a regulilor de mai sus este prezentata în **Codul de Practici şi Proceduri (CPP**).
Cunoaşterea Politicii de Certificare, precum şi al Codului de Practici şi Proceduri prezintă importanţă în mod special pentru abonaţii şi entităţile partener ale certSIGN.

2 Certificatele

Certificatul este un şir de date (mesaj) care conţine cel puţin numele şi identificatorul autorităţii, identificatorul abonatului, cheia sa publică, perioada de validitate, numărul serial şi semnatura autorităţii emitente.
Certificatele sunt utilizate pentru a lega datele personale ale abonatului de cheile publice specifice. Proprietarul certificatului este, de asemenea, şi proprietarul cheii private, corespunzătoare cheii publice conţinută în certificat. Datele de identificare conţinute în certificat permit altor părţi să determine cu exactitate proprietarul certificatului. Dacă cheia privată este utilizată în timpul semnarii electronice a unui mesaj, destinatarul mesajului poate fi sigur că mesajul a fost creat folosind cheia privată, corespunzătoare cheii publice conţinută în certificat (deci a fost creată de proprietarul certificatului) şi 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 căsuţei de poştă electronică;
- Cheia publică conţinută de certificat aparţine abonatului respectiv.

Datorită celor de mai sus, entităţile partener, după recepţia unui mesaj semnat, pot determina cine este proprietarul certificatului care a semnat mesajul şi, opţional, îl pot trage pe acesta la răspundere pentru acţiunile sale sau angajamentele luate.

certSIGN furnizează servicii în concordanţă cu legislaţia şi practicile în domeniu. Cheile autorităţii de certificare sunt protejate folosind module hardware de securitate (Hardware Security Module - HSM), certificate conform FIPS 140-2 nivel 3. certSIGN implementează controalele fizice şi procedurale ale sistemului. Semnăturile electronice sunt create prin intermediul algoritmului RSA în combinaţie cu algoritmul de hash SHA-2 si chei de minim 2048 biti.

Autoritatea de Certificare certSIGN emite certificate de diferite Clase, având nivele de credibilitate diferite. Credibilitatea certificatului depinde de procedura de verificare a identităţii abonatului şi 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 reţea pentru care se emite certificatul.

Specialiştii certSIGN pot verifica starea tehnică şi 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 şi furnizează servicii specifice unei infrastructuri de chei publice. Printre cele mai importante aplicaţii ale certificatelor emise de certSIGN CA, se numără (fără a se limita la):
- Semnarea documentelor electronice,
- Securizarea mesajelor de e-mail (poştă electronică),
- Securizarea tranzacţiilor Web,
- Securizarea comunicaţiilor de reţea,
- Semnarea codului pentru aplicaţii,
- 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 şi nu oferă nici o garanţie asupra identităţii subiectului. Certificatele demo sunt destinate în principal pentru testarea performanţei aplicaţiilor 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 căsuţei de mesagerie electronică şi/sau numele şi prenumele persoanei fizice sau al reprezentantului persoanei juridice.
Certificatele de Clasa 1 conţin următorul identificator de politică:
{certSIGN}* id-policy(1) id-cp(1)id-Class-1(1)
certSIGN nu îşi asumă nici o obligaţie financiară şi nu oferă nici o garanţie pentru certificatele (şi conţinutul acestora) emise în cadrul politicii de mai sus.

2.2 Certificate de Clasă 2

Certificatele de Clasă 2 sunt emise de Autoritatile de Certificare **certSIGN CA Class 2** si **certSIGN CA Class 2 G2**. Acestea sunt certificate personale şi sunt destinate în principal pentru securizarea corespondenţei electronice sau autentificarea clienţilor în timpul sesiunilor online. Operatorii Autorităţilor de Certificare certSIGN CA Class 2 si certSIGN CA Class 2 G2 verifică datele furnizate de clienţi în timpul procesului de certificare. Identitatea persoanei fizice solicitante sau a reprezentantului persoanei juridice este supusă unei verificări. Autenticitatea adresei căsuţei de mesagerie electronică inclusă în certificat este de asemenea verificată.
Certificatele de Clasa 2 conţin următorul identificator de politică:
{certSIGN} .id-policy(1). id-cp(1).id-Class-2(2)
Certificatele emise în cadrul acestei politici oferă garanţii şi responsabilităţi 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)

Aditional, certificate de clasa 2 sunt emise cu 3 autoritati de certificare cu circuit inchis, certificate care sunt emise pentru Sistemul Electronic de Plati operat de Transfond S.A in baza unui protocol tehnic. Autoritatile care emit certificate pentru SEP sunt:

1. CERTSIGN FOR BANKING QUALIFIED DS TEST CA V3 cu identificatorul de politica: 1.3.6.1.4.1.25017.1.1.2.1.2
2. CERTSIGN FOR BANKING SIMPLE SSL PRODUCTION CA V3 cu identificatorul de politica: 1.3.6.1.4.1.25017.1.1.2.1.1
3. CERTSIGN FOR BANKING SIMPLE SSL TEST CA V3 cu identificatorul de politica: 1.3.6.1.4.1.25017.1.1.2.1.3

Certificatele de Clasa 2 pentru SEP refera următorul identificator de politică:
{certSIGN} .id-policy(1). id-cp(1).id-Class-2(2).id-Transfond(1)
Certificatele emise în cadrul acestei politici trebuie sa respecte protocolul tehnic incheiat intre certSIGN si Transfond.

2.3 Certificate de Clasă 3

Certificatele de Clasă 3 sunt emise de catre: **certSIGN Qualified CA Class 3, certSIGN Qualified CA Class 3 G2, certSIGN Enterprise CA Class 3**, **certSIGN Enterprise CA Class 3 G2, certSIGN SSL DV CA Class 3 G2, certSIGN SSL EV CA Class 3 G2 și certSIGN Code Signing CA Class 3 G2** . Certificatele emise în această clasă pot fi certificate calificate sau certificate pentru securizarea obiectelor binare şi protecţia transmisiilor de date utilizând protocoalele IPSec, SSL şi TLS. Operatorii certSIGN verifică datele furnizate de clienţi (organizaţii sau instituţii) în timpul procesului de înregistrare. Toate datele ce urmează a fi incluse în certificat sunt verificate.
Pe baza unui certificat emis de certSIGN Qualified CA Class 3, certSIGN Qualified CA Class 3 G2, certSIGN Enterprise CA Class 3, certSIGN SSL DV CA Class 3 G2, certSIGN SSL EV CA Class 3 G2 certSIGN Enterprise CA Class 3 G2 si certSIGN Enterprise CA Class 3 G2 se poate determina cu exactitate identitatea unui subiect sau autenticitatea unei organizaţii.
Certificatele calificate emise de certSIGN Qualified CA Class 3 si certSIGN Qualified CA Class 3 G2 pot fi utilizate pentru crearea de semnaturi electronice care să înlocuiască semnaturile olografe.
Certificatele calificate sunt emise de Autoritatile de Certificare **certSIGN Qualified CA Class 3 si certSIGN Qualified CA Class 3 G2**. Aceste certificate sunt conforme cu REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, Legea Semnaturii Electronice 455 / 2001 din România şi Hotărârea de Guvern 1259/Decembrie 2001 privind Normele de Aplicare ale Legii Semnaturii Electronice.
Autoritatile de certificare certSIGN Qualified CA Class 3 G2 , certSIGN Enterprise CA Class 3 G2, certSIGN SSL DV CA Class 3 G2, certSIGN SSL EV CA Class 3 G2 si certSIGN Code Siging CA Class 3 G2 folosesc un certificat emis cu algoritmul sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).
Certificatele de Clasa 3 conţin următorul identificator de politică:
{certSIGN} id-policy(1) id-cp(1)id-Class-3(3)

În plus, pentru certificatele calificate se adaugă identificatorul de politică: **itu-t(0).identified-organization(4).etsi(0).qualified-certificate-policies(1456).policy-identifiers(1). qcp-public-with-sscd (1).**

Pentru certificatele emise de **certSIGN Enterprise CA Class 3 G2** se adaugă identificatorul de politica **{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline- requirements(2) subject-identity-validated(2)} (2.23.140.1.2.2)**.

Pentru certificatele emise de **certSIGN Code Signing CA Class 3 G2** se adaugă identificatorul de politică **{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) code-signing-requirements(4)code-signing(1)} (2.23.140.1.4.1)**

Pentru certificatele emise de **certSIGN SSL DV CA Class 3 G2** identificatorul de politică este: **{certSIGN} id-policy(1) id-cp(1) id-DV-CA(5)** la care se adaugă: **{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1).**

Pentru certificatele emise de **certSIGN SSL EV CA Class 3 G2** identificatorul de politică este: **{certSIGN} id-policy(1) id-cp(1)id-EV-CA(6)** la care se adaugă: **{joint - iso - itu - t(2) international - organizations(23) ca - browser - forum(140) certificate - policies(1) ev-guidelines (1) }(2.23.140.1.1).**

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

Aditional, certificate de clasa 3 sunt emise cu o autoritate de certificare cu circuit inchis, certificate care sunt emise pentru Sistemul Electronic de Plati operat de Transfond S.A in baza unui protocol tehnic. Autoritatea care emite certificate pentru SEP este:

1. CERTSIGN FOR BANKING QUALIFIED DS PRODUCTION CA V3 cu identificatorul de politica: 1.3.6.1.4.1.25017.1.1.3.1.1

Certificatele de Clasa 3 pentru SEP refera următorul identificator de politică:
{certSIGN} .id-policy(1). id-cp(1).id-Class-3(3).id-Transfond(1)

Certificatele emise în cadrul acestei politici trebuie sa respecte protocolul tehnic incheiat intre certSIGN si Transfond. Certificatele emise de aceasta autoritate nu includ identificatorul de certificat calificat.

2.4 Certificate de Clasă 4

Certificatele de Clasă 4 sunt emise de Autoritatile de Certificare **certSIGN Non-Repudiation CA Class 4 si certSIGN Non-Repudiation CA Class 4 G2**. Aceste certificate sunt destinate în principal Autorităţilor de Certificare intermediare sau altor furnizori de servicii de încredere (OCSP sau Autorităţi de Marcare Temporală). Operatorii certSIGN Non-Repudiation CA Class 4 si certSIGN Non-Repudiation CA Class 4 G2 verifică identitatea clienţilor care trebuie să se prezinte personal la unul din ghişeele certSIGN. Se vor verifica împuternicirea din partea firmei, autenticitatea şi corectitudinea documentelor de identitate furnizate precum şi actele organizaţiei. certSIGN Non-Repudiation CA Class 4 si certSIGN Non-Repudiation CA Class 4 G2 acceptă şi documente autentificate de către un

notar. Pe baza unui certificat emis de certSIGN Non-Repudiation CA Class 4 sau certSIGN Non-Repudiation CA Class 4 G2 se poate determina cu exactitate identitatea unui subiect, autenticitatea unei organizaţii sau credibilitatea unei Autorităţi de Certificare externe.
Perioada de valabilitate a unui certificat de Clasă 4 este de minim 2 ani. Cheile abonatului ce deţine un certificat de Clasă 4 trebuie protejate utilizând module hardware de securitate (HSM).
Certificatele de Clasă 4 conţin următorul identificator de politică:
{certSIGN} id-policy(1) id-cp(1)id-Class-4(4)

Certificatele emise în cadrul acestei politici oferă garanţii şi responsabilităţi complete.
Abonatul certSIGN poate alege tipul de certificat potrivit nevoilor sale. Tipurile de certificate sunt descrise pe larg în Codul de Practici şi Proceduri (CPP) care poate fi consultat pe site-ul Web al certSIGN. De asemenea, aceste informaţii pot fi primite şi prin poştă electronica trimiţând un mesaj la adresa: office@certSIGN.ro.

3 Jetoane de ne-repudiere

Jetoanele de ne-repudiere sunt structuri de date (mesaje) conţinând cel puţin:

- informaţiile furnizate de către client (de exemplu, valoare hash, numărul serial al certificatului, numărul cererii etc.) unei autorităţi de ne-repudiere şi
- semnatura electronica a autorităţii respective.

Autorităţile de ne-repudiere care oferă servicii clienţilor sunt afiliate la certSIGN.
Prin emiterea unui jeton, o autoritate de ne-repudiere confirmă apariţia unui eveniment în momentul creării acestuia sau la un moment de timp anterior. Acest eveniment poate fi: transmiterea unui document, data creării semnaturii etc. Entitatea parteneră poate verifica, pe baza datelor recepţionate, corectitudinea semnaturii 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 şi celor aparţinând unei organizaţii. Mărcile temporale pot fi încorporate în:

- semnaturi electronice,
- acceptarea tranzacţiilor electronice,
- arhivarea datelor,
- notarizarea documentelor electronice etc.

Regulile ce stabilesc modul de operare al Autorităţii de Marcare Temporală precum şi alte informaţii suplimentare legate de acest sistem sunt descrise într-un document separat (a se vedea Politica certSIGN Time-Stamping Authority).
Jetonul de marcare temporală conţine următorul identificator de politică:
{certSIGN}[†].id-Time-Stamping(2).Id-Policy(1)
Responsabilitatea financiară a certSIGN pentru timpul, data şi alte informaţii 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}=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)

certSIGN Time-Stamping Authority oferă garanţii 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 şi reprezintă o alternativă la Listele de Certificate Revocate (Certificate Revocation List – CRL). certSIGN Validation Service oferă garanţii pentru răspunsurile OCSP emise, în limitele descrise în CPP. Modul de funcţionare al autorităţii OCSP şi informaţii suplimentare privind acest serviciu sunt prezentate pe pagina web (a se vedea http://www.certsign.ro) şi în CPP.

4 Garanţiile oferite de certSIGN

În funcţie de tipul de certificat emis, certSIGN garantează că va depune efortul necesar pentru a verifica în mod corespunzător informaţiile incluse în cadrul certificatelor (a se vedea Codul de Practici şi Proceduri - Capitolul 3.2). Verificarea informaţiilor este importantă în primul rând pentru entităţile partenere ce primesc mesaje de la un abonat care se identifică printr-un certificat digital calificat emis de certSIGN. În consecinţă, certSIGN este responsabilă din punct de vedere financiar pentru pagubele rezultate ca urmare a neglijenţei sau erorilor comise de certSIGN în ceea ce priveşte aceste tipuri de certificate. Responsabilităţile certSIGN depind de clasa certificatului abonatului, iar responsabilitatea este atât faţă de abonat cât şi faţă de entităţile partenere care au încredere în informaţiile din certificat (a se vedea Codul de Practici şi Proceduri – capitolul 2 şi capitolul 9).
Garanţiile certSIGN pot fi limitate de anumite restricţii. Aceste restricţii sunt aduse la cunoştinţă abonatului care confirmă acest lucru în cadrul unei declaraţii (a se vedea declaraţia de Acceptare a Certificatului). certSIGN garantează unicitatea semnaturilor electronice pentru abonaţii săi.

5 Acceptarea certificatului

Responsabilităţile şi garanţiile certSIGN se aplică din momentul acceptării certificatului de către abonat. Modalitatea de furnizare a certificatului şi acceptanţa certificatului sunt descrise în Codul de Practici şi Proceduri (a se vedea capitolul 4.4 Acceptarea Certificatului) şi sunt detaliate în acordurile încheiate cu abonaţii.

6 Serviciul de certificare

certSIGN furnizează cinci servicii de bază:
(1) înregistrarea,
(2) emiterea unui certificat digital,
(3) reînnoirea unui certificat,
(4) revocarea unui certificat şi
(5) verificarea stării unui certificat.
În plus, certSIGN oferă şi 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 identităţii unui abonat şi precedă operaţiunea de emitere a certificatului (a se vedea Codul de Practici şi Proceduri, Capitolul 3 Identificarea și autentificarea și Capitolul 4.1 Trimiterea cererii).

Reînnoirea unui certificat are loc atunci când un abonat înregistrat deja doreşte să obţină un certificat pentru o aceeaşi cheie publică cu modificarea perioadei de valabilitate (a se vedea Codul de Practici şi Proceduri, Capitolul 4.6 Reînnoirea certificatului și Capitolul 4.7 Re-Key-ul 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 şi Proceduri, Capitolul 4.9 Revocarea şi 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 autorităţile afiliate. Verificarea stării unui certificat se poate realiza şi prin intermediul serviciului de validare on-line a stării certificatelor (a se vedea Codul de Practici şi Proceduri, Capitolul 4.10 Servicii privind starea 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 condiţii specifice, certSIGN poate genera perechi de chei unice şi livra aceste chei abonaţilor.

7 Entitatea Partener

Entitatea partener este obligată să verifice în mod corespunzător fiecare semnatură electronică de pe documentele recepţionate (inclusiv certificatul digital). Pe timpul procesului de verificare, entitatea partener trebuie să utilizeze procedurile şi resursele puse la dispoziţie de certSIGN. Acestea specifică, printre altele, faptul că trebuie verificată lista de certificate revocate publicată de certSIGN şi căile de certificare permise (a se vedea Codul de Practici şi Proceduri, Capitolul 4.5 Utilizarea perechii de chei și a certificatelor).
Fiecare document pentru care există probleme la verificarea semnaturii digitale trebuie să fie respins şi trebuie să fie verificat prin alte modalităţi sau proceduri, de exemplu verificarea documentului la un notar.

8 Abonatul

Abonatul este obligat să păstreze în siguranţă cheia sa privată, pentru a preveni accesul neautorizat la aceasta al unei terţe părţi. În cazul în care există bănuiala că a fost accesată de o terţă parte, abonatul este obligat să anunţe imediat autoritatea care a emis certificatul sau digital. Informaţiile furnizate autorităţii trebuie să fie suficiente pentru a determina cu exactitate identitatea persoanei căreia i se va revoca certificatul digital.

9 Actualizarea politicii de certificare

Comitetul de Management al Politicilor și Procedurilor certSIGN este responsabil de aprobarea acestui document. Politica de certificare a certSIGN se poate modifica periodic. Aceste modificări vor fi disponibile tuturor abonaţilor prin intermediul site-lui Web al certSIGN. Abonaţii care nu acceptă modificările aduse politicii de certificare trebuie să trimită către certSIGN o declaraţie în acest sens şi să renunţe 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 deţinute de un abonat şi de tipul de serviciu cerut. Tarifele sunt prezentate în listele de preţuri, disponibile pe site-ul certSIGN (http://www.certsign.ro).