Politica de Certificare certSIGN

Versiunea 1.20
Data: 15 Ianuarie 2026

Notă importantă

Acest document este proprietatea CERTSIGN SA

Distribuirea și reproducerea fără acordul CERTSIGN SA sunt interzise

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

Telefon: 004-021-31.19.901

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
1.14	31 Ianuarie 2023	Revizuire anuală	Manager Politici PKI
1.15	31 Iulie 2023	Adaugare tabel mapare cuprins RFC 3647	Manager Politici PKI
1.16	31 Ianuarie 2024	Revizuire anuală	Manager Politici PKI
1.17	18 Aprilie 2024	Adăugare certificat cross	Manager Politici PKI
1.18	15 Ianuarie 2025	Revizuire anuală	Manager Politici PKI
1.19	15 Aprilie 2025	Actualizare footer	Manager Politici PKI
1.20	15 Ianuarie 2026	Revizuire anuală	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
Public-Internet	31 Ianuarie 2023
Public-Internet	31 Iulie 2023
Public-Internet	31 Ianuarie 2024
Public-Internet	18 Aprilie 2024
Public-Internet	15 Ianuarie 2025
Public-Internet	15 Aprilie 2025
Public-Internet	15 Ianuarie 2026

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
1.14	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Ianuarie 2023
1.15	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Iulie 2023
1.16	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Ianuarie 2024
1.17	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Aprilie 2024
1.18	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Ianuarie 2025
1.19	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Aprilie 2025
1.20	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de Încredere	Ianuarie 2026

Cuprins

1 Introducere

Sistemul PKI certSIGN ROOT CA este la sfârșitul ciclului de viață, și nu mai emite certificate.

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.

CERTSIGN respectă cerințele celei mai recente versiuni publicate a Cerințelor de bază pentru emiterea și gestionarea certificatelor de încredere publică publicate la http://www.cabforum.org și versiunii actuale a Politicii Mozilla Root Store, a Programului Apple Root Certificate, a Programului Microsoft Trusted Root și a Politicii Chrome Root Program.

certSIGN respectă Legea Română nr.214/2024 - privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea.

Politica certSIGN Root este de a include Autorități de Certificare Emitente (Issuing CA), CA-uri Subordonate (prin CA Subordonată se înțelege o CA operată de o entitate diferită de cea care operează Root-ul) și certificări încrucișate.

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, în acord cu cerinţele din ETSI TS 119 312.

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 tranzacţiilor Web,
- Securizarea comunicaţiilor de reţea,

2.1 Certificate de Clasă 1

Certificatele de Clasă 1 sunt emise de Autoritatea de Certificare **certSIGN Demo CA Class 1.** Aceste certificate au fost folosite numai pentru scopuri demonstrative şi nu oferă nici o garanţie asupra identităţii subiectului. Certificatele demo au fost destinate în principal pentru testarea performanţei aplicaţiilor sau dispozitivelor înainte de cumpărarea certificatelor finale. Autoritatea de Certificare certSIGN Demo CA Class 1 a emis certificate pentru aproape toate scopurile. În majoritatea cazurilor, în timpul procesului de înregistrare se verifica 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}[1] 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. Nu se mai emit certificate cu această clasă.

2.2 Certificate de Clasă 2

Certificatele de Clasă 2 au fost emise de Autoritatea de Certificare **certSIGN CA Class 2 G2**.Toate autorităţile certSIGN de certificare de tip Class 2 au expirat.

[1] *{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 au fost emise de catre: **certSIGN SSL DV CA Class 3 G2**.
Certificatele emise în această clasă au fost certificate pentru securizarea obiectelor binare şi protecţia transmisiilor de date utilizând protocoalele IPSec, SSL şi TLS. Operatorii certSIGN au verificat datele furnizate de clienţi (organizaţii sau instituţii) în timpul procesului de înregistrare. Toate datele din certificat au fost verificate temeinic.
Pe baza unui certificat emis de certSIGN SSL DV CA Class 3 G2 se poate determina cu exactitate identitatea unei organizaţii.
Autoritatile de certificare certSIGN SSL DV CA Class 3 G2 au folosit certificate emise 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)

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).**

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.

2.4 Certificate de Clasă 4

Toate autoritățile certSIGN de certificare de tip Class 2 au expirat.

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 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

Sistemul PKI certSIGN ROOT CA este la sfârșitul ciclului de viață, și nu mai emite certificate.
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

Sistemul PKI certSIGN ROOT CA este la sfârșitul ciclului de viață, și nu mai emite certificate.
certSIGN a furnizat 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) 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 este revizuită și actualizată anual. 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).

Maparea cuprinsului din RFC 3647 la Politica de Certificare

Cuprins RFC 3647	No	Cuprins Politica Certificare
1. INTRODUCTION	1.	Introducere
1.1 Overview	1.	Introducere
1.2 Document name and identification	1.	Introducere
1.3 PKI participants	1.	Introducere
1.3.1 Certification authorities	1.	Introducere
1.3.2 Registration authorities	1.	Introducere
1.3.3 Subscribers	8.	Abonatul
1.3.4 Relying parties	1.	Introducere
1.3.5 Other participants	7.	Entitatea Partener
1.4 Certificate usage	2.	Certificatele
1.4.1. Appropriate certificate uses	2.	Certificatele
1.4.2 Prohibited certificate uses	2.	Certificatele
1.5 Policy administration	1.	Introducere
1.5.1 Organization administering the document	1.	Introducere
1.5.2 Contact person	1.	In footer
1.5.3 Person determining CPS suitability for the policy	1.	Introducere
1.5.4 CPS approval procedures	9.	Actualizarea politicii de certificare
1.6 Definitions and acronyms	1.	Introducere
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	9.	Actualizarea politicii de certificare
2.1 Repositories	6.	Serviciul de certificare
2.2 Publication of certification information	9.	Actualizarea politicii de certificare
2.3 Time or frequency of publication	9.	Actualizarea politicii de certificare
2.4 Access controls on repositories	9.	Actualizarea politicii de certificare
3. IDENTIFICATION AND AUTHENTICATION (11)	1.	Introducere
3.1 Naming	1.	Introducere
3.1.1 Types of names	1.	Introducere
3.1.2 Need for names to be meaningful	1.	Introducere
3.1.3 Anonymity or pseudonymity of subscribers	1.	Introducere
3.1.4 Rules for interpreting various name forms	1.	Introducere
3.1.5 Uniqueness of names	1.	Introducere
3.1.6 Recognition, authentication, and role of trademarks	1.	Introducere
3.2 Initial identity validation	1.	Introducere
3.2.1 Method to prove possession of private key	1.	Introducere
3.2.2 Authentication of organization identity	1.	Introducere
3.2.3 Authentication of individual identity	1.	Introducere
3.2.4 Non-verified subscriber information	1.	Introducere
3.2.5 Validation of authority	1.	Introducere
3.2.6 Criteria for interoperation	1.	Introducere
3.3 Identification and authentication for re-key requests	1.	Introducere
3.3.1 Identification and authentication for routine re-key	1.	Introducere
3.3.2 Identification and authentication for re-key after revocation	1.	Introducere
3.4 Identification and authentication for revocation request	1.	Introducere
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)	1.	Introducere

Cuprins RFC 3647	No	Cuprins Politica Certificare
4.1 Certificate Application	1.	Introducere
4.1.1 Who can submit a certificate application	1.	Introducere
4.1.2 Enrollment process and responsibilities	1.	Introducere
4.2 Certificate application processing	1.	Introducere
4.2.1 Performing identification and authentication functions	1.	Introducere
4.2.2 Approval or rejection of certificate applications	1.	Introducere
4.2.3 Time to process certificate applications	1.	Introducere
4.3 Certificate issuance	1.	Introducere
4.3.1 CA actions during certificate issuance	1.	Introducere
4.3.2 Notification to subscriber by the CA of issuance of certificate	1.	Introducere
4.4 Certificate acceptance	5.	Certificate acceptance
4.4.1 Conduct constituting certificate acceptance	5.	Certificate acceptance
4.4.2 Publication of the certificate by the CA	5.	Certificate acceptance
4.4.3 Notification of certificate issuance by the CA to other entities	5.	Certificate acceptance
4.5 Key pair and certificate usage	1.	Introducere
4.5.1 Subscriber private key and certificate usage	1.	Introducere
4.5.2 Relying party public key and certificate usage	1.	Introducere
4.6 Certificate renewal	6.	Serviciul de certificare
4.6.1 Circumstance for certificate renewal	6.	Serviciul de certificare
4.6.2 Who may request renewal	6.	Serviciul de certificare
4.6.3 Processing certificate renewal requests	6.	Serviciul de certificare
4.6.4 Notification of new certificate issuance to subscriber	6.	Serviciul de certificare
4.6.5 Conduct constituting acceptance of a renewal certificate	6.	Serviciul de certificare
4.6.6 Publication of the renewal certificate by the CA	6.	Serviciul de certificare
4.6.7 Notification of certificate issuance by the CA to other entities	6.	Serviciul de certificare
4.7 Certificate re-key	6.	Serviciul de certificare
4.7.1 Circumstance for certificate re-key	6.	Serviciul de certificare
4.7.2 Who may request certification of a new public key	6.	Serviciul de certificare
4.7.3 Processing certificate re-keying requests	6.	Serviciul de certificare
4.7.4 Notification of new certificate issuance to subscriber	6.	Serviciul de certificare
4.7.5 Conduct constituting acceptance of a re-keyed certificate	6.	Serviciul de certificare
4.7.6 Publication of the re-keyed certificate by the CA	6.	Serviciul de certificare
4.7.7 Notification of certificate issuance by the CA to other entities	6.	Serviciul de certificare
4.8 Certificate modification	6.	Serviciul de certificare
4.8.1 Circumstance for certificate modification	6.	Serviciul de certificare
4.8.2 Who may request certificate modification	6.	Serviciul de certificare
4.8.3 Processing certificate modification requests	6.	Serviciul de certificare
4.8.4 Notification of new certificate issuance to subscriber	6.	Serviciul de certificare
4.8.5 Conduct constituting acceptance of modified certificate	6.	Serviciul de certificare
4.8.6 Publication of the modified certificate by the CA	6.	Serviciul de certificare

Cuprins RFC 3647	No	Cuprins Politica Certificare
4.8.7 Notification of certificate issuance by the CA to other entities	6.	Serviciul de certificare
4.9 Certificate revocation and suspension	6.	Serviciul de certificare
4.9.1 Circumstances for revocation	6.	Serviciul de certificare
4.9.2 Who can request revocation	6.	Serviciul de certificare
4.9.3 Procedure for revocation request	6.	Serviciul de certificare
4.9.4 Revocation request grace period	6.	Serviciul de certificare
4.9.5 Time within which CA must process the revocation request	6.	Serviciul de certificare
4.9.6 Revocation checking requirement for relying parties	6.	Serviciul de certificare
4.9.7 CRL issuance frequency (if applicable)	6.	Serviciul de certificare
4.9.8 Maximum latency for CRLs (if applicable)	6.	Serviciul de certificare
4.9.9 On-line revocation/status checking availability	6.	Serviciul de certificare
4.9.10 On-line revocation checking requirements	6.	Serviciul de certificare
4.9.11 Other forms of revocation advertisements available	6.	Serviciul de certificare
4.9.12 Special requirements re key compromise	6.	Serviciul de certificare
4.9.13 Circumstances for suspension	6.	Serviciul de certificare
4.9.14 Who can request suspension	6.	Serviciul de certificare
4.9.15 Procedure for suspension request	6.	Serviciul de certificare
4.9.16 Limits on suspension period	6.	Serviciul de certificare
4.10 Certificate status services	1.	Introducere
4.10.1 Operational characteristics	1.	Introducere
4.10.2 Service availability	3.2	Raspunsul de confirmare OCSP
4.10.3 Optional features	1.	Introducere
4.11 End of subscription	6.	Serviciul de certificare
4.12 Key escrow and recovery	6.	Serviciul de certificare
4.12.1 Key escrow and recovery policy and practices	6.	Serviciul de certificare
4.12.2 Session key encapsulation and recovery policy and practices	6.	Serviciul de certificare
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS (11)	1.	Introducere
5.1 Physical controls	1.	Introducere
5.1.1 Site location and construction	1.	Introducere
5.1.2 Physical access	1.	Introducere
5.1.3 Power and air conditioning	1.	Introducere
5.1.4 Water exposures	1.	Introducere
5.1.5 Fire prevention and protection	1.	Introducere
5.1.6 Media storage	1.	Introducere
5.1.7 Waste disposal	1.	Introducere
5.1.8 Off-site backup	1.	Introducere
5.2 Procedural controls	1.	Introducere
5.2.1 Trusted roles	1.	Introducere
5.2.2 Number of persons required per task	1.	Introducere
5.2.3 Identification and authentication for each role	1.	Introducere
5.2.4 Roles requiring separation of duties	1.	Introducere
5.3 Personnel controls	1.	Introducere
5.3.1 Qualifications, experience, and clearance requirements	1.	Introducere
5.3.2 Background check procedures	1.	Introducere

Cuprins RFC 3647	No	Cuprins Politica Certificare
5.3.3 Training requirements	1.	Introducere
5.3.4 Retraining frequency and requirements	1.	Introducere
5.3.5 Job rotation frequency and sequence	1.	Introducere
5.3.6 Sanctions for unauthorized actions	1.	Introducere
5.3.7 Independent contractor requirements	1.	Introducere
5.3.8 Documentation supplied to personnel	1.	Introducere
5.4 Audit logging procedures	1.	Introducere
5.4.1 Types of events recorded	1.	Introducere
5.4.2 Frequency of processing log	1.	Introducere
5.4.3 Retention period for audit log	1.	Introducere
5.4.4 Protection of audit log	1.	Introducere
5.4.5 Audit log backup procedures	1.	Introducere
5.4.6 Audit collection system (internal vs. external)	1.	Introducere
5.4.7 Notification to event-causing subject	1.	Introducere
5.4.8 Vulnerability assessments	1.	Introducere
5.5 Records archival	1.	Introducere
5.5.1 Types of records archived	1.	Introducere
5.5.2 Retention period for archive	1.	Introducere
5.5.3 Protection of archive	1.	Introducere
5.5.4 Archive backup procedures	1.	Introducere
5.5.5 Requirements for time-stamping of records	1.	Introducere
5.5.6 Archive collection system (internal or external)	1.	Introducere
5.5.7 Procedures to obtain and verify archive information	1.	Introducere
5.6 Key changeover	1.	Introducere
5.7 Compromise and disaster recovery	1.	Introducere
5.7.1 Incident and compromise handling procedures	1.	Introducere
5.7.2 Computing resources, software, and/or data are corrupted	1.	Introducere
5.7.3 Entity private key compromise procedures	1.	Introducere
5.7.4 Business continuity capabilities after a disaster	1.	Introducere
5.8 CA or RA termination	1.	Introducere
6. TECHNICAL SECURITY CONTROLS (11)	1.	Introducere
6.1 Key pair generation and installation	1.	Introducere
6.1.1 Key pair generation	1.	Introducere
6.1.2 Private key delivery to subscriber	1.	Introducere
6.1.3 Public key delivery to certificate issuer	1.	Introducere
6.1.4 CA public key delivery to relying parties	1.	Introducere
6.1.5 Key sizes	1.	Introducere
6.1.6 Public key parameters generation and quality checking	1.	Introducere
6.1.7 Key usage purposes (as per X.509 v3 key usage field)	1.	Introducere
6.2 Private Key Protection and Cryptographic Module Engineering Controls	1.	Introducere
6.2.1 Cryptographic module standards and controls	1.	Introducere
6.2.2 Private key (n out of m) multi-person control	1.	Introducere
6.2.3 Private key escrow	1.	Introducere
6.2.4 Private key backup	1.	Introducere
6.2.5 Private key archival	1.	Introducere

Cuprins RFC 3647	No	Cuprins Politica Certificare
6.2.6 Private key transfer into or from a cryptographic module	1.	Introducere
6.2.7 Private key storage on cryptographic module	1.	Introducere
6.2.8 Method of activating private key	1.	Introducere
6.2.9 Method of deactivating private key	1.	Introducere
6.2.10 Method of destroying private key	1.	Introducere
6.2.11 Cryptographic Module Rating	1.	Introducere
6.3 Other aspects of key pair management	1.	Introducere
6.3.1 Public key archival	1.	Introducere
6.3.2 Certificate operational periods and key pair usage periods	1.	Introducere
6.4 Activation data	1.	Introducere
6.4.1 Activation data generation and installation	1.	Introducere
6.4.2 Activation data protection	1.	Introducere
6.4.3 Other aspects of activation data	1.	Introducere
6.5 Computer security controls	1.	Introducere
6.5.1 Specific computer security technical requirements	1.	Introducere
6.5.2 Computer security rating	1.	Introducere
6.6 Life cycle technical controls	1.	Introducere
6.6.1 System development controls	1.	Introducere
6.6.2 Security management controls	1.	Introducere
6.6.3 Life cycle security controls	1.	Introducere
6.7 Network security controls	1.	Introducere
6.8 Time-stamping	3.1	Marcile Temporare
7. CERTIFICATE, CRL, AND OCSP PROFILES	2.	Certificatele
7.1 Certificate profile	2.	Certificatele
7.1.1 Version number(s)	2.	Certificatele
7.1.2 Certificate extensions	2.	Certificatele
7.1.3 Algorithm object identifiers	2.	Certificatele
7.1.4 Name forms	2.	Certificatele
7.1.5 Name constraints	2.	Certificatele
7.1.6 Certificate policy object identifier	2.	Certificatele
7.1.7 Usage of Policy Constraints extension	2.	Certificatele
7.1.8 Policy qualifiers syntax and semantics	2.	Certificatele
7.1.9 Processing semantics for the critical Certificate Policies extension	2.	Certificatele
7.2 CRL profile	1.	Introducere
7.2.1 Version number(s)	1.	Introducere
7.2.2 CRL and CRL entry extensions	1.	Introducere
7.3 OCSP profile	1.	Introducere
7.3.1 Version number(s)	1.	Introducere
7.3.2 OCSP extensions	1.	Introducere
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	1.	Introducere
8.1 Frequency or circumstances of assessment	1.	Introducere
8.2 Identity/qualifications of assessor	1.	Introducere
8.3 Assessor’s relationship to assessed entity	1.	Introducere
8.4 Topics covered by assessment	1.	Introducere
8.5 Actions taken as a result of deficiency	1.	Introducere

Cuprins RFC 3647	No	Cuprins Politica Certificare
8.6 Communication of results	1.	Introducere
9. OTHER BUSINESS AND LEGAL MATTERS	1.	Introducere
9.1 Fees	10.	Taxe
9.1.1 Certificate issuance or renewal fees	10.	Taxe
9.1.2 Certificate access fees	10.	Taxe
9.1.3 Revocation or status information access fees	10.	Taxe
9.1.4 Fees for other services	10.	Taxe
9.1.5 Refund policy	10.	Taxe
9.2 Financial responsibility	1.	Introducere
9.2.1 Insurance coverage	1.	Introducere
9.2.2 Other assets	1.	Introducere
9.2.3 Insurance or warranty coverage for end-entities	1.	Introducere
9.3 Confidentiality of business information	1.	Introducere
9.3.1 Scope of confidential information	1.	Introducere
9.3.2 Information not within the scope of confidential information	1.	Introducere
9.3.3 Responsibility to protect confidential information	1.	Introducere
9.4 Privacy of personal information	1.	Introducere
9.4.1 Privacy plan	1.	Introducere
9.4.2 Information treated as private	1.	Introducere
9.4.3 Information not deemed private	1.	Introducere
9.4.4 Responsibility to protect private information	1.	Introducere
9.4.5 Notice and consent to use private information	1.	Introducere
9.4.6 Disclosure pursuant to judicial or administrative process	1.	Introducere
9.4.7 Other information disclosure circumstances	1.	Introducere
9.5 Intellectual property rights	1.	Introducere
9.6 Representations and warranties	4.	Garantiile oferite de certSIGN
9.6.1 CA representations and warranties	4.	Garantiile oferite de certSIGN
9.6.2 RA representations and warranties	4.	Garantiile oferite de certSIGN
9.6.3 Subscriber representations and warranties	4.	Garantiile oferite de certSIGN
9.6.4 Relying party representations and warranties	4.	Garantiile oferite de certSIGN
9.6.5 Representations and warranties of other participants	4.	Garantiile oferite de certSIGN
9.7 Disclaimers of warranties	4.	Garantiile oferite de certSIGN
9.8 Limitations of liability	1.	Introducere
9.9 Indemnities	1.	Introducere
9.10 Term and termination	1.	Introducere
9.10.1 Term	1.	Introducere
9.10.2 Termination	1.	Introducere
9.10.3 Effect of termination and survival	1.	Introducere
9.11 Individual notices and communications with participants	1.	Introducere
9.12 Amendments	1.	Introducere
9.12.1 Procedure for amendment	1.	Introducere
9.12.2 Notification mechanism and period	1.	Introducere
9.12.3 Circumstances under which OID must be changed	1.	Introducere
9.13 Dispute resolution provisions	1.	Introducere
9.14 Governing law	1.	Introducere

Cuprins RFC 3647	No	Cuprins Politica Certificare
9.15 Compliance with applicable law	1.	Introducere
9.16 Miscellaneous provisions	1.	Introducere
9.16.1 Entire agreement	1.	Introducere
9.16.2 Assignment	1.	Introducere
9.16.3 Severability	1.	Introducere
9.16.4 Enforcement (attorneys' fees and waiver of rights)	1.	Introducere
9.16.5 Force Majeure	1.	Introducere
9.17 Other provisions	1.	Introducere