Codul de Practici și Proceduri
certSIGN ROOT CA

Versiunea 1.45
Data: 15 Ianuarie 2026

Notă importantă

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[1]	Motiv	Persoana care a făcut modificarea
1.0	Aprilie 2006	Publicarea primei versiuni	Manager Servicii Electronice
1.1	Iulie 2006	Termen de 1 an pt revizuirea clasificării	Manager Servicii Electronice
1.2	Octombrie 2008	S-a introdus numele persoanei responsabile cu administrarea CPS-ului ca si adresa de contact a acesteia.	Manager Servicii Electronice
		S-au introdus detalii referitoare la modul de protejare si backup al cheilor private de criptare ale abonaților.	Manager Servicii Electronice
		S-a clarificat poziția firmei certSIGN ca furnizor de servicii de certificare fata de utilizarea mărcilor înregistrate in certificatele digitale.	Manager Servicii Electronice
		S-a specificat ca, pentru moment certSIGN nu folosește serviciilor unor RA-uri externe.	Manager Servicii Electronice
		S-a specificat ca certSIGN nu oferă servicii de suspendare a certificatelor.	Manager Servicii Electronice
		S-a specificat ca mesajele de eroare ca răspuns la cererile de verificare online a stării certificatelor (prin OCSP) nu sunt semnate digital.	Manager Servicii Electronice
		S-a specificat ca certSIGN nu are implementate procese de management al ciclului de viată al tokenurilor/smartcardurilor.	Manager Servicii Electronice
		S-au dat detalii suplimentare despre site-ul de disaster recovery.	Manager Servicii Electronice
		S-a precizat ca certSIGN nu oferă servicii de key management pt abonați.	Manager Servicii Electronice
		S-a precizat ca certSIGN nu oferă servicii de schimbare a cheii unui certificate.	Manager Servicii Electronice
1.3	Februarie 2009	S-a detaliat procedura de verificare de catre RA a controlului exercitat de solicitantul certificatelor de server asupra domeniului	Manager Servicii Electronice
		S-a detaliat procedura de verificare de catre RA a controlului exercitat de Beneficiar asupra contului de mail declarat in cererea de certificat	Manager Servicii Electronice
1.4	Iulie 2009	S-a modificat adresa firmei	Manager Servicii Electronice
1.5	Octombrie 2009	S-au introdus condițiile pentru CA-urile subordinate operate de terți	Manager Servicii Electronice
1.6	Iulie 2011	S-au actualizat informațiile privind serviciile de suspendare	Manager Servicii Electronice

[1] *Data efectivă este ultima zi a lunii*

1.7	Septembrie 2011	S-au specificat condițiile trecerii la chei de 2048 de biți si alte masuri de creștere a securității algoritmilor criptografici folosiți	Manager Servicii Electronice
1.8	Martie 2014	S-a modificat antetul. S-a inclus precizarea privind verificarea domeniilor certificatelor de server utilizând noile gTLD si ccTLD aflate la ICANN. S-a inclus precizările privind certificatele wildcard SSL OV si cele Unified Communications. Înființarea unei autorități de certificare, certSIGN Enterprise CA Class 3 G2. Certificatele emise în această clasă pot fi certificate pentru securizarea obiectelor binare și protecția transmisiilor de date utilizând protocoalele IPSec, SSL și TLS	Director tehnic
1.9	August 2014	S-a exclus inițiala tatălui din formatul certificatului. S-a adoptat scrierea cu cratima a numelor si prenumelor formate din mai multe cuvinte.	Ofiter Securitate IT si conformitate
1.10	Iulie 2015	Adăugarea noilor autorități de certificare certSIGN CA Class 2 G2 certSIGN Qualified CA Class 3 G2 certSIGN Non-Repudiation CA Class 4 G2	Director Tehnic
1.11	Decembrie 2015	Durata de valabilitate a certificatelor demonstrative si a celor de clasa 2 (Tabelul 6.3.2.2) a fost modificata la nespecificat, respectiv la 1,2 sau 3 ani	Director Tehnic
1.12	10 Ianuarie 2016	Adăugarea noilor autorități de certificare cu circuit închis, certificate care sunt emise pentru Sistemul Electronic de Plăti operat de Transfond S.A	Director Tehnic
1.13	25 Ianuarie 2016	S-a adăugat 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
1.14	20 Iulie 2017	S-a indicat corespondenta dintre procedurile de validare a controlului asupra domeniilor web utilizate si procedurile cerute de Baseline Requirements	
1.15	1 Septembrie 2017	S-a creat o adresa speciala pentru raportarea de certificate cu probleme. La capitolul Revocarea si suspendarea certificatelor s-a adăugat un subcapitol dedicat raportării certificatelor cu probleme	
1.16	26 Noiembrie 2017	Clarificarea procedurii de verificare a atributelor Beneficiarului ce apar in certificat in funcție de tipul certificatelor. S-a introdus	

		si angajamentul de respectare a cerințelor BR ale CAB Forum	
1.17	Martie 2018	Actualizarea CPP cu BaseLine Requirement versiunea 1.5.6 respectiv Mozilla Root Store Policy versiunea 2.5	Manager Politici PKI
1.18	Mai 2018	Actualizare CPP conform RFC 3647, respectiv cerințe GDPR	Manager Politici PKI
1.19	Iulie 2018	Actualizare conform CAB Forum, validarea deținerii sau controlul domeniului	Manager Politici PKI
1.20	Septembrie 2018	Actualizare pentru adăugare profile certificate	Manager Politici PKI
1.21	Septembrie 2018	Actualizare pentru eliminare profile certificate	Manager Politici PKI
1.22	Noiembrie 2018	Actualizare determinata de schimbarea sediului	Manager Politici PKI
1.23	Ianuarie 2019	Revizuire anuala Actualizare determinata de precizările referitoare la eliminarea caracterului underscore „_” din numele de domeniu /dNSName -CA/B Forum/BR 1.6.2	Manager Politici PKI
1.24	Septembrie 2019	Actualizare pentru modificare valabilitate certificate certSIGN Enterprise CA Class 3 G2	Manager Politici PKI
1.25	Ianuarie 2020	Revizuire anuală. Actualizări minore cf. CA/Browser Forum BR 1.6.7 și Mozilla Policy v2.7	Manager Politici PKI
1.26	Mai 2020	Adăugare metodă validare domeniu 3.2.2.4.2	Manager Politici PKI
1.27	Mai 2020	Actualizări OCSP, limitare SSL la 1 an, și adăgare metodă identificare PF Tabel 3.2.3	Manager Politici PKI
1.28	Septembrie 2020	Actualizări CRL & OCSP ReasonCode 7.2 & 7.3	Manager Politici PKI
1.29	Ianuarie 2021	Actualizare anuală	Manager Politici PKI
1.30	Martie 2021	Actualizări DV și EV SSL CA (WebTrust NC)	Manager Politici PKI
1.31	Mai 2021	Metode dovedire compromitere chei private	Manager Politici PKI
1.32	Mai 2021	Actualizare schema autorităților PKI	Manager Politici PKI
1.33	Iulie 2021	Inlăturare referire algoritmi md5 și sha1	Manager Politici PKI
1.34	Septembrie 2021	Ballot SC42/47/48 + High Risk Cert. Requests + FQDN + OU	Manager Politici PKI
1.35	Noiembrie 2021	Actualizări metode validare domeniu	Manager Politici PKI
1.36	Ianuarie 2022	Actualizare anuală	Manager Politici PKI
1.37	Iunie 2022	Actualizări ref. Cauri (WebTrust NC), motive revocare SSL, validitate SSL	Manager Politici PKI
1.38	Octombrie 2022	Add CRL Reason	Manager Politici PKI
1.39	Ianuarie 2023	Revizuire anuală	Manager Politici PKI

1.40	Iulie 2023	Revizuire link-uri si conformitate CABF BR	Manager Politici PKI
1.41	Ianuarie 2024	Revizuire anuală	Manager Politici PKI
1.42	Aprilie 2024	Adaugare certificat incrucisat	Manager Politici PKI
1.43	15 Ianuarie 2025	Revizuire anuală	Manager Politici PKI
1.44	15 Aprilie 2025	Actualizari metode validare domeniu, ACME & MPIC	Manager Politici PKI
1.45	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	24 Martie 2014
Public-Internet	25 August 2014
Public-Internet	3 Iulie 2015
Public-Internet	27 Decembrie 2015
Public- Internet	10 ianuarie 2016
Public- Internet	25 ianuarie 2016
Public-Internet	20 Iulie 2017
Public-Internet	1 Septembrie 2017
Public-Internet	26 Noiembrie 2017
Public-Internet	31 March 2018
Public-Internet	24 May 2018
Public-Internet	31 July 2018
Public-Internet	14 September 2018
Public-Internet	27 September 2018
Public-Internet	26 November 2018
Public-Internet	31 January 2019
Public-Internet	16 September 2019
Public-Internet	31 January 2020
Public-Internet	11 Mai 2020
Public-Internet	21 Mai 2020
Public-Internet	30 Septembrie 2020
Public-Internet	29 Ianuarie 2021
Public-Internet	23 Martie 2021
Public-Internet	11 Mai 2021
Public-Internet	25 Mai 2021
Public-Internet	02 Iulie 2021
Public-Internet	31 August 2021
Public-Internet	23 Noiembrie 2021
Public-Internet	31 Ianuarie 2022
Public Internet	6 Iunie 2022
Public Internet	6 Octombrie 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 Încredere	Aprilie 2006
1.1	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Încredere	Iulie 2006
1.2	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de Încredere	August 2008
1.3	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Februarie 2009
1.4	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Iulie 2009
1.5	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Octombrie 2009
1.6	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Iulie 2011
1.7	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	August 2011
1.8	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Martie 2014
1.9	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	August 2014
1.10	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Iunie 2015
1.11	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Decembrie 2015
1.12	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Decembrie 2015
1.13	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Ianuarie 2016
1.14	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Iulie 2017
1.15	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	August 2017
1.16	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Noiembrie 2017
1.17	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Martie 2018
1.18	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Mai 2018
1.19	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Iulie 2018
1.20	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Septembrie 2018
1.21	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Septembrie 2018
1.22	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Noiembrie 2018
1.23	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Ianuarie 2019
1.24	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Septembrie 2019
1.25	Comitet de Management al Politicilor si Procedurilor pentru Serviciile de încredere	Ianuarie 2020
1.26	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Mai 2020
1.27	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Mai 2020
1.28	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Septembrie 2020
1.29	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Ianuarie 2021
1.30	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Martie 2021
1.31	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Mai 2021
1.32	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Mai 2021
1.33	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Iulie 2021
1.34	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	August 2021
1.35	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Noiembrie 2021
1.36	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Ianuarie 2022
1.37	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Iunie 2022
1.38	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Octombrie 2022
1.39	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Ianuarie 2023
1.40	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Iulie 2023
1.41	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Ianuarie 2024
1.42	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Aprilie 2024
1.43	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Ianuarie 2025
1.44	Comitet de Management al Politicilor și Procedurilor pentru Serviciile de încredere	Aprilie 2025
1.45	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.

Codul de Practici și Proceduri certSIGN ROOT CA – (denumit în continuare **Codul de Practici și Proceduri** sau **CPP**) descrie procesul de certificare a cheilor publice și aria de aplicabilitate a certificatelor care rezultă din acest proces de certificare. Codul de Practici și Proceduri prezintă importanță în mod special pentru Abonați și Entitățile Partenere. **Codul de Practici și Proceduri** descrie regulile generale ale procesului de certificare, stipulate în **Politica de certificare certSIGN** (denumită în continuare **Politica de certificare** sau **CP**). **Politica de certificare** descrie nivelul de încredere ce poate fi acordat unui anumit tip de certificat emis de **Furnizorul de Servicii de certificare certSIGN** (denumit în continuare **certSIGN**). **Codul de Practici și Proceduri** descrie modalitatea prin care certSIGN asigură nivelul de încredere garantat de politică.

Codul de Practici și Proceduri descrie patru politici de certificare aplicate de către certSIGN în vederea emiterii de certificate pentru autorități și utilizatorii finali. Aceste politici reprezintă patru nivele diferite de credibilitate (**Clasa 1, Clasa 2, Clasa 3, Clasa 4**) corespunzătoare certificatelor de chei publice. Ariile de aplicabilitate ale certificatelor emise în conformitate cu aceste politici pot fi aceleași. Cu toate acestea, responsabilităţile (inclusiv din punct de vedere legal) ale Autorităţii de certificare și utilizatorilor de certificate sunt diferite. Structura și conținutul Codului de Practici și Proceduri sunt în conformitate cu recomandările RFC 3647. Codul de Practici și Proceduri presupune faptul că cititorul este familiar cu noţiunile privind certificatele, semnătura electronica și Infrastructurile de Chei Publice (PKI).

Există mai multe documente auxiliare care au legătură cu Codul de Practici și Proceduri. Acestea sunt folosite în cadrul Autorităților de certificare certSIGN pentru a reglementa modul de funcționare al acestora. Aceste documente au însă un statut diferit și nu sunt disponibile public datorită importanței informațiilor pe care le conțin pentru securitatea sistemului.

Informații adiționale despre Codul de Practici si Proceduri se pot obține prin poștă electronica de la Managerul Serviciilor Electronice la adresa: office@certsign.ro.

Acest document este conform cu ultima versiune publicată a "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" (https://cabforum.org/baseline-requirements-documents/), respectiv ultima versiune publicată a Mozilla Root Store Policy. In eventualitatea unei neconformități intre acest document si cerințele menționate, cerințele prevalează.
certSIGN respectă Legea Română nr.214/2024 - privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea.

1.1 Descriere generală

Codul de Practici și Proceduri este specificaţia ce stă la baza funcționării **certSIGN** și a Autorităților de certificare, a Autorităţii de Înregistrare, Abonaților și a Entităților Partenere asociate acesteia. De asemenea, acest document descrie regulile de prestare a serviciilor de certificare cum ar fi înregistrarea Abonaților, certificarea cheilor publice, înnoirea cheilor și a certificatelor și revocarea certificatelor.

Arhitectura Infrastructurii de Chei Publice (PKI) a **certSIGN** este împărțită pe doua nivele (vezi Figura 1.1). Nivelul 1 conține **certSIGN ROOT CA**. Autoritățile de certificare de pe Nivelul 2 sunt direct semnate de către **certSIGN ROOT CA**. **certSIGN ROOT CA** operează numai în mod off-line. În cazul compromiterii Autorităților de nivel 2, **certSIGN ROOT CA** va fi folosită pentru a revoca certificatele acestora și pentru a emite noi certificate.

Serviciile de stare a certificatului certSIGN sunt CRL și OCSP. Accesul la aceste servicii se face prin intermediul site-ului web „www.certsign.ro" și „ocsp.certsign.ro". Serviciile de stare a certificatului furnizează informații despre starea certificatelor valide. Integritatea și autenticitatea informațiilor de stare sunt protejate printr-o semnătură digitală a CA-ului respectiv.

Intrările de revocare dintr-un răspuns CRL sau OCSP nu sunt niciodată eliminate.

Serviciile de certificare sunt disponibile 24 de ore pe zi, 7 zile pe săptămână. certSIGN menține o capacitate continuă 24x7 de a răspunde intern la un raport cu probleme de certificat cu prioritate ridicată și, după caz, transmite o astfel de reclamație autorităților de aplicare a legii și / sau revocă un certificat care face obiectul unei astfel de reclamații.

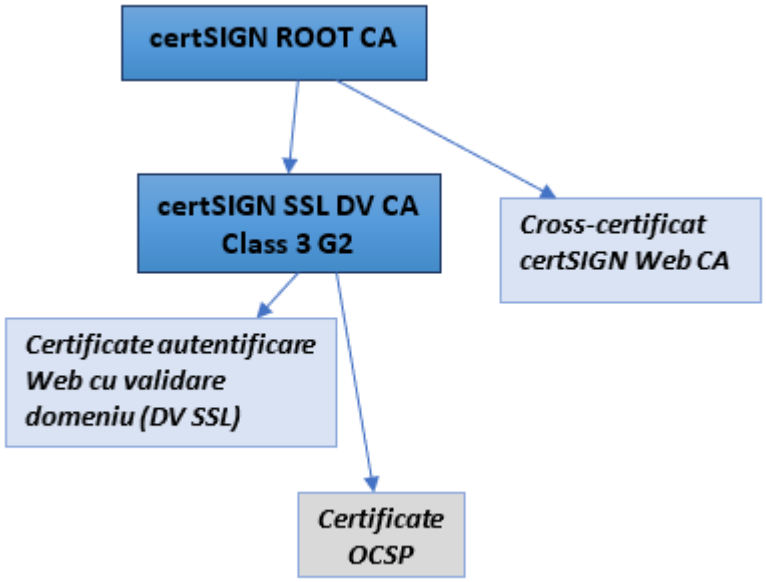

Figura 1.1. Autoritățile de emitere certificate ce operează în cadrul certSIGN ROOT CA PKI

Din punct de vedere ierarhic, există următoarele Autorități de Certificare, imediat subordonate **certSIGN ROOT CA**:

- certSIGN SSL DV CA Class 3 G2
- certSIGN Web CA - certificat cross

toate emițând certificate având nivele de credibilitate diferite.
Certificatele emise de certSIGN conţin identificatorii politicii de certificare, permiţând astfel Entităților Partenere să stabilească dacă certificatul verificat a fost folosit în conformitate cu scopul declarat al acestuia. Scopul declarat este specificat pe baza valorilor din câmpul *PolicyInformation* al extensiei *certificatesPolicies* (vezi Capitolul 7.1.2) din cadrul fiecărui certificat emis de certSIGN.

Tipurile de certificate emise de către Autoritățile de certificare sunt descrise în Tabelul 1.1.

Clasa	Tipul	Subtipul
Clasa 1 (Demo)	certificat demonstrativ simplu	
	certificat demonstrativ pentru semnarea de cod	
	certificat demonstrativ pentru servere Web	
	certificat demonstrativ pentru gateway-uri VPN	
	certificat demonstrativ pentru servere CA	
	certificat demonstrativ pentru servere TSA	
	certificat demonstrativ pentru servere de validare (OCSP)	
Clasa 2	certificat simplu	certificat simplu pentru autentificare și semnare ▪ fără DSCS şi cheie generată de Beneficiar ▪ fara DSCS si cheie generata de certSIGN ▪ cu DSCS şi cheie generată de Beneficiar ▪ cu DSCS și cheie generată de certSIGN certificat simplu pentru criptare ▪ fără DSCS şi cheie generată de Beneficiar ▪ fara DSCS si cheie generata de certSIGN ▪ cu DSCS şi cheie generată de Beneficiar ▪ cu DSCS și cheie generată de certSIGN certificat simplu de semnare si criptare ▪ fără DSCS şi cheie generată de Beneficiar ▪ fara DSCS si cheie generata de certSIGN ▪ cu DSCS şi cheie generată de Beneficiar ▪ cu DSCS şi cheie generată de certSIGN
Clasa 3 Calificate	certificat calificat	certificat calificat ▪ cu DSCS și cheie generată de Beneficiar ▪ cu DSCS și cheie generată de certSIGN
Clasa 3 Enterprise	certificat de criptare de încredere	certificat de criptare de încredere ▪ cu DSCS și cheie generată de Beneficiar ▪ cu DSCS și cheie generată de certSIGN
	certificat pentru servere Web	
	certificat pentru gateway-uri VPN	
Clasa 4	certificat pentru servere CA	
	certificat pentru servere TSA	
	certificat pentru servere de validare (OCSP)	

Tabelul 1.1. Tipuri de certificate

1.2 Denumirea documentului și identificarea

Denumirea acestui document este: **Codul de Practici și Proceduri certSIGN ROOT CA & CA-uri Intermediare**. Documentul este disponibil sub formă electronica în Depozit la adresa https://www.certsign.ro/ro/document/codul-de-practici-si-proceduri-certsign/ sau pe baza unei cereri trimisă pe adresa office@certsign.ro.

Acest document este conform cu ultima versiune publicată a cerințelor de bază pentru emiterea și gestionarea certificatelor de încredere, publicat la https://cabforum.org/baseline-requirements-documents/ și ultima versiune publicată a Mozilla Root Store Policy, a Programului Apple Root Certificate, a Programului Microsoft Trusted Root și a Politicii Chrome Root Program; structura și conținutul CPS respectă recomandările RFC 3647.

În cazul unei eventuale neconcordanțe între acest document și cerințele menționate, acele cerințe au prioritate față de acest document.

1.3 Participanții PKI

Codul de Practici și Proceduri CA Calificat reglementează cele mai importante relații dintre entitățile certSIGN, echipele de consultanți (inclusiv auditorii) și clienții (utilizatorii serviciilor furnizate) acesteia:

- Autoritățile de certificare:
  - certSIGN SSL DV CA Class 3 G2
  - certSIGN Web CA - cross
- Autoritatea de Înregistrare,
- Depozitul,
- Serverul de verificare on-line a stării certificatelor (OCSP),
- Abonaţii,
- Entităţile Partenere.

certSIGN oferă servicii de certificare pentru orice persoană fizică sau entitate juridică care este de acord cu prevederile prezentului CPP. Scopul acestor practici (ce includ procedurile de generare a cheilor, procedurile de emitere a certificatelor și securitatea sistemului informaţional) este acela de a garanta utilizatorilor serviciilor certSIGN că nivelele de credibilitate declarate ale certificatelor emise corespund practicilor Autorităţilor de Certificare.

1.3.1 Autoritățile de Certificare

Autoritatea de Certificare certSIGN ROOT CA este o Autoritate de Certificare Primară pentru domeniul certSIGN. Toate celelalte Autorități de Certificare din cadrul acestui domeniu sunt subordonate certSIGN ROOT CA (vezi Figura 1.3).

În prezent există următoarele Autorități de Certificare active subordonate direct lui certSIGN ROOT CA: **certSIGN SSL DV CA Class 3 G2, certSIGN Web CA - cross**.

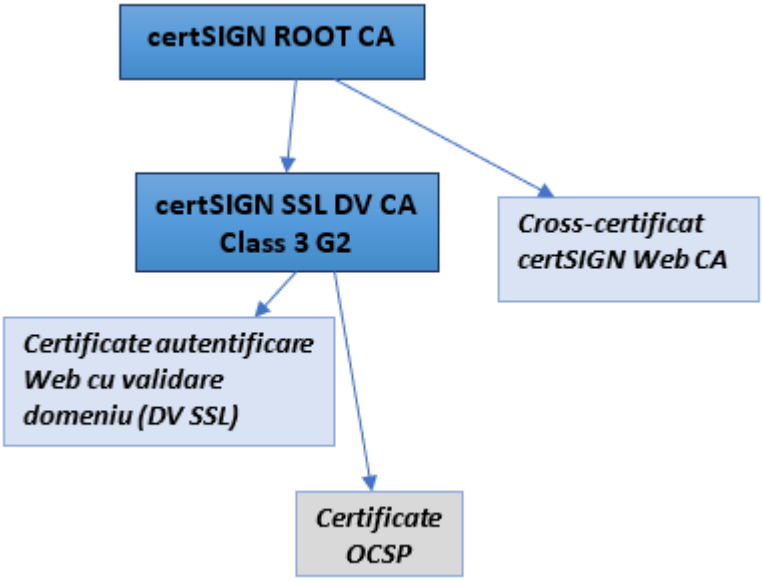

Figura 1.3. Structura domeniului de certificare certSIGN ROOT CA

Autoritatea de Certificare Primară, **certSIGN ROOT CA**, poate înregistra și emite certificate numai Autorităţilor de certificare și autorităţilor ce emit confirmări electronice de ne-repudiere ce aparţin domeniului certSIGN. Înainte de a începe activitatea, fiecare autoritate de certificare Intermediară trebuie să trimită o cerere către Autoritatea de Certificare Principală, **certSIGN ROOT CA,** pentru înregistrare și emitere de certificat de cheie publică (a se vedea și procedurile descrise în capitolul 6.1 din *prezentul cod de practici și proceduri*). Autoritatea **certSIGN ROOT CA** funcţionează pe baza unui certificat *autosemnat*, emis de ea însăşi. Într-un astfel de certificat, extensia **certificatePolicies** lipseşte (vezi Capitolul 7.1.1), ceea ce semnifică faptul că nu există limitări ale setului de **căi de certificare** la care certificatul certSIGN ROOT CA poate fi ataşat.

Autoritatea de Certificare **certSIGN ROOT CA** reprezintă **punctul de încredere** pentru clienţii certSIGN. Prin urmare, fiecare cale de certificare trebuie să înceapă cu certificatul autorităţii certSIGN ROOT CA.

Autoritatea de Certificare **certSIGN ROOT CA** furnizează servicii de certificare pentru:

- sine (emite și reînnoieşte certificate proprii),
- Autoritățile de Certificare înregistrate în domeniul de certificare certSIGN,
- entităţi ce furnizează servicii de verificare on-line a stării certificatelor și alte entităţilor ce oferă servicii de ne-repudiere (de exemplu, servicii de marcare temporala).

Autoritățile de certificare Intermediare **certSIGN SSL DV CA Class 3 G2** au emis certificate către Abonaţi, conform politicilor având identificatorii din Tabelul 1.3

Autoritatea de Certificare	Politica de Certificare
certSIGN SSL DV CA Class 3 G2	**{certSIGN} id-policy(1) id-cp(1)id-DV-CA(5) {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)**

Tabelul 1.3. Numele Autorităţilor de Certificare și politicile de certificare corespunzătoare

Autoritățile de Certificare Intermediare sunt configurate pentru a emite certificate către:

- furnizori de servicii din domeniul telecomunicaţiilor mobile,
- dispozitive de reţea care realizează conexiuni criptate peste VPN,
- dispozitive hardware (fizice și logice) deţinute de persoane particulare sau juridice, în vederea oferirii de servicii pe bază de certificate de chei publice cum ar fi serviciul de verificare on-line a stării certificatelor (OCSP),
- alte Autorități de Certificare.

Orice entitate externa care doreste incheierea unui contract pentru operarea unui CA Subordonat certSIGN ROOT CA va incheia cu certSIGN un contract prin care se obliga sa respecte versiunile curente ale CP si ale CPS si sa se supuna unui audit pentru verificarea conformitatii cu standardul WebTrust for CA.

1.3.2 Autoritățile de Înregistrare

Autoritatea de Înregistrare primeşte, verifică și aprobă sau respinge cererile de înregistrare și emitere de certificate, de reînnoire sau revocare a certificatelor. Verificarea cererilor are ca scop autentificarea (pe baza documentelor incluse în cereri) atât a solicitantului cât și a datelor menţionate în cerere. Autoritatea de Înregistrare poate trimite cereri către Autoritatea de Certificare corespunzătoare – pentru anularea cererii de înregistrare a unui Beneficiar și pentru retragerea certificatului acestuia.

Nivelul de precizie al procesului de determinare a identităţii clientului este dat de nevoile Beneficiarului și este impus de nivelul certificatului pe care îl solicită Beneficiarul (vezi Capitolul 3). În cazul celei mai simple identificări, Autoritatea de Înregistrare verifică doar corectitudinea adresei de e-mail trimisă. Cea mai precisă identificare presupune prezenţa în persoană a solicitantului la Autoritatea de Înregistrare și furnizarea de dovezi cu privire la identitatea sa. Identificarea poate fi realizată fie automat**,** fie manual de către un operator al Autorităţii de Înregistrare.

Autoritatea de Înregistrare (RA) funcţionează pe baza autorizaţiei obţinute de la Autoritatea de Certificare certSIGN.

RA desfășoară activitățile de mai sus direct sau cu contribuția autorităților de înregistrare delegate. În toate cazurile, certSIGN rămâne responsabilă.

Cu excepția cazului în care se prevede altfel, în acest document, "RA" acoperă autoritatea de înregistrare și autoritățile de înregistrare delegate.

1.3.3 Abonații

Un Abonat/Beneficiar este o entitate al cărei identificator este plasat în câmpul Subject al unui certificat și care nu emite certificate altor entităţi. O Entitate Parteneră este o entitate care foloseşte certificatul unui Beneficiar si poate verifica semnatura electronica a acestuia pentru a asigura confidenţialitatea informaţiilor transmise.

Orice persoană fizică sau juridică, precum și dispozitivele hardware pe care acestea le deţin pot fi Abonaţi ai certSIGN – CA, cu condiţia să se încadreze în termenii din definiţia Beneficiarului

În particular, operatorii Autorităţii de Înregistrare, ceilalţi angajaţi certSIGN și echipamentele indispensabile pentru asigurarea securităţii infrastructurii certSIGN (firewall-uri, routere, servere de autentificare) reprezintă beneficiari.

Organizaţiile care doresc să obţină certificate emise de certSIGN pentru angajaţii lor, pot să o facă prin intermediul reprezentanţilor lor, pe când Abonaţii individuali trebuie să ceară personal un certificat.

certSIGN emite certificate de tipuri diferite și de nivele de credibilitate diferite. Abonaţii trebuie să decidă ce tip de certificat este cel mai potrivit pentru nevoile lor (vezi Capitolul 1.3.1).

1.3.4 Entitățile Partenere

Entitate Parteneră, ce utilizează serviciile certSIGN, poate fi orice entitate care ia decizii bazându-se pe corectitudinea conexiunii dintre identitatea unui Beneficiar și cheia sa publică (conexiune confirmată de una din Autoritățile de certificare Intermediare certSIGN ROOT CA).

O Entitate Parteneră este responsabilă pentru modul în care verifică starea curentă a certificatului unui Beneficiar. O astfel de decizie trebuie luată de fiecare dată când o Entitate Parteneră doreşte să utilizeze un certificat pentru a verifica o semnatura electronica, pentru a verifica identitatea sursei sau autorul unui mesaj, sau pentru a crea un canal de comunicaţie secret cu proprietarul certificatului. O Entitate Parteneră trebuie să utilizeze informaţiile dintr-un certificat (de exemplu, identificatorii și calificatorii politicii de certificare) pentru a decide dacă un certificat a fost folosit în conformitate cu scopul declarat.

1.3.5 Alți participanți

Comitetul de Management al Politicilor și Procedurilor este un Comitet creat în cadrul certSIGN de către Consiliul de administrație pentru a supraveghea întreaga activitate a Autorităților de Certificare și a Autorităților de Înregistrare ale certSIGN. Rolurile și responsabilitățile CMMP sunt descrise în documentația internă.
Furnizorii de servicii ai certSIGN: furnizori externi care sprijină activitățile certSIGN pe baza unui acord contractual semnat.
Notarii publici: pot efectua identificarea și garanta pentru identitatea reală a Subiecților.
Furnizorii de Dispozitive de Creare a Semnăturilor Electronice Calificate: furnizorii externi care sprijină activitățile certSIGN în cadrul unui acord contractual semnat ce asigură furnizarea dispozitivelor criptografice fizice utilizate de către Subiecți.

Autoritatea de înregistrare delegată (DRA): CA se poate baza pe un DRA pentru a externaliza o parte din funcțiile RA. Un operator de DRA are puterea de a:
- solicita generarea sau reînnoirea certificatului;
- solicita revocarea certificatului;

Acesta efectuează pentru autoritate, în contextul eliberării certificatului, verificarea identității viitorului Beneficiar pentru certificat în aceleași condiții și cu același nivel de siguranță ca și cele necesare pentru operatorul RA.
Angajamentele operatorului DRA față de CA sunt specificate într-un acord întocmit și semnat cu entitatea responsabilă a operatorului. Acordul specifică faptul că operatorul trebuie să efectueze o verificare imparțială și scrupuloasă a identității și a posibilelor atribute și servicii ale Subscriberului. Operatorul DRA trebuie, de asemenea, să respecte părțile din CPS care îi revin.

1.4 Utilizarea certificatului

Aria de aplicabilitate a certificatelor stabileşte scopul în care poate fi folosit un certificat. Acest scop este definit de două elemente:

- Unul care defineşte aplicabilitatea certificatului (de exemplu, semnătura electronică, confidențialitate),
- Celalalt presupune o listă sau o descriere a aplicaţiilor permise sau interzise.

Certificatele emise de certSIGN pot fi folosite pentru a procesa și asigura securitatea informaţiilor (inclusiv autentificarea), având nivele diferite de credibilitate. Nivelul de credibilitate al informaţiei și vulnerabilitatea acesteia trebuie evaluate de către Beneficiar. În Politica de certificare și prezentul Cod de Practici și Proceduri sunt definite patru nivele de sensibilitate: Clasa 1 (nivelul de test), Clasa 2 (nivelul de bază), Clasa 3 (nivelul intermediar), Clasa 4 (nivelul ridicat). Aceste nivele corespund celor patru nivele de credibilitate ale certificatelor (vezi Tabelul 1.4).

Nivelul de sensibilitate al informaţiei	Numele politicii de certificare	Aria de aplicabilitate
Clasa 1 (de test)	certSIGN Class 1	Cel mai scăzut nivel de credibilitate al identităţii unei entităţi. Certificatele de Clasa 1 se recomandă a se folosi pentru a testa compatibilitatea serviciilor certSIGN cu cele oferite de alţi furnizori de servicii PKI și pentru a testa funcţionalitatea certificatelor în cadrul aplicaţiilor testate. De asemenea, aceste certificate pot fi folosite în alte scopuri atâta timp cât asigurarea credibilităţii mesajelor trimise sau primite nu este importantă.
Clasa 2 (de bază)	certSIGN Class 2	Acest nivel oferă o securitate de bază pentru informaţii în medii cu grad scăzut de risc (risc fără consecinţe majore). Dintre acestea, menţionăm accesul la informaţii private acolo unde probabilitatea de apariţie a unui acces neautorizat nu este foarte mare. Aceste certificate pot fi folosite pentru a autentifica și controla integritatea informaţiei care a fost semnată și pentru a asigura confidenţialitatea informaţiei, mai ales în cazul poştei electronice.
Clasa 3 (intermediar)	certSIGN Class 3	Acest nivel se recomandă pentru asigurarea securităţii informaţiei în medii unde există riscul apariţiei de breşe de securitate iar consecinţele acestor breşe sunt moderate. Certificatele pot fi folosite pentru protecția tranzacţiilor financiare sau a tranzacţiilor în

Nivelul de sensibilitate al informaţiei	Numele politicii de certificare	Aria de aplicabilitate
		care există şanse de apariţie a fraudelor. De asemenea, aceste certificate pot fi folosite și pentru crearea de semnaturi electronice extinse.
Clasa 4 (ridicat)	certSIGN Class 4	Acest nivel corespunde mediilor în care şansele compromiterii datelor sunt foarte mari și în care consecinţele unui incident de securitate sunt foarte grave. Aceste certificate pot fi folosite pentru protecția tranzacţiilor de valoare nelimitată (dacă nu se specifică altceva în certificat), a tranzacţiilor în care există mari şanse de apariţie a fraudelor.

Tabel 1.4. Nivelul de sensibilitate al informaţiei și denumirea politicii

Entitatea parteneră este responsabilă pentru stabilirea nivelului de credibilitate necesar pentru un certificat folosit într-un anume scop. Luând în considerare factorii de risc semnificativi, entitatea parteneră trebuie să stabilească ce tip de certificat emis de certSIGN se potriveşte cerinţelor formulate. Abonaţii trebuie să cunoască cerinţele entităţii partenere (de exemplu, aceste cerinţe pot fi publicate sub forma unei politici de semnatura sau politică de securitate informatică) și apoi să solicite certSIGN emiterea de certificate corespunzătoare acestor cerinţe.

1.4.1 Utilizări admise ale certificatului

certSIGN emite 9 tipuri de bază de certificate având arii diferite de aplicabilitate. Aceste sunt:

1. **certificate pentru Autorităţile de Certificare** – folosirea lor nu este restricţionată la aria definită; aria de aplicabilitate poate fi dată de extensia din certificate ce stabileşte modul în care poate fi folosită cheia privată (vezi câmpul **keyUsage**, Capitolul 7), sau de rolul acesteia (de exemplu, Beneficiar, Autoritate de Certificare sau altă autoritate care furnizează servicii PKI); acest tip conține de asemenea și certificatele operaţionale ale Autorităţilor de Certificare;
2. **certificate pentru confirmarea autenticităţii serverelor** – sunt folosite de serviciile care operează pe baza protocoalelor SSL/TLS/WTLS;
3. **certificate pentru confirmarea stării unui certificat** – sunt emise pentru serverele care funcţionează conform protocolului OCSP și care furnizează informaţii despre starea certificatelor;

Certificatele emise în concordanţă cu una dintre cele patru politici de certificare pot fi folosite în aplicaţii ce satisfac cel puţin următoarele condiţii:

- gestionează **corespunzător** cheile publice și private,
- certificatele și cheile publice asociate acestora sunt folosite în concordanţă cu scopul declarat al acestora, confirmat de către certSIGN,
- dispun de mecanisme interne de verificare a stării certificatelor, de creare a căilor de certificare și controlul validităţii (validitatea semnaturii, data expirării etc.),
- oferă utilizatorului informaţii corespunzătoare despre certificate și starea acestora.

Lista aplicaţiilor recomandate (de către certSIGN) este publicata pe site la adresa: https://www.certsign.ro/ro/produse/servicii-de-incredere-eidas/aplicatii/

Aplicaţiile sunt incluse în lista aplicaţiilor recomandate pe baza unor declaraţii scrise ale producătorilor și/sau pe baza testelor făcute de certSIGN. certSIGN permite fiecărui Beneficiar să-și genereze singur cheile criptografice folosite în procesul de certificare prin intermediul dispozitivelor recomandate. Autoritatea de Certificare poate de asemenea să genereze cheile pe un dispozitiv criptografic și apoi să livreze Beneficiarului dispozitivul împreună cu cheile. În acest caz, certSIGN foloseşte dispozitive criptografice ce satisfac cel puţin cerinţele standardului FIPS PUB 140-2.

1.4.2 Utilizări interzise ale certificatului

Este interzisă folosirea certificatelor certSIGN pentru alte scopuri decât cele declarate și în aplicaţii care nu îndeplinesc condiţiile minime specificate în 1.4.1.

1.5 Administrarea politicii

1.5.1 Organizația care administrează documentul

Prezentul document este administrat de către Comitetul de Management al Politicilor și Procedurilor (CMMP) al Prestatorului de servicii de încredere certSIGN. CMMP include membri seniori din conducere, precum și personalul responsabil pentru gestionarea operațională a infrastructurii PKI a certSIGN.

Nume	S.C. certSIGN S.A. Punct de lucru: Bd. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, București, România Registrul comerțului: J2006000484402 CUI: RO 18288250 Sediul social: Șos. Olteniței 107A, clădirea C1, etaj 1, camera 16, Sector 4, București, România, Cod postal 041303
Telefon	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel 1.5.1 Organizația care administrează documentul

1.5.2 Persoana de contact

Nume	Comitetul de Management al Politicilor și Procedurilor (CMMP)
Telefon	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel 1.5.2 Persoana de contact

Procedura de raportare a certificatelor cu probleme

Din cauza unor erori, limitări tehnice sau procedurale, ori din alte motive, pot exista certificate emise greșit de certSIGN (ex. certificatul emis conține informații eronate despre subiect sau organizație). Mai pot exista cazuri în care un certificat este utilizat necorespunzător (ex. pentru activități infracționale). Dacă beneficiarii, entitile sau alte terse părți se confruntă cu astfel de situații, în care suspectează compromiterea cheii private, sau un alt tip de activități frauduloase, utilizarea incorectă a certificatului sau o conduită neadecvată sau orice alte aspecte legate de certificatele emise de certSIGN, pot raporta aceste probleme la adresa

revokecsgn@certsign.ro, informând Autoritatea de Certificare emitenta despre motive rezonabile de revocare a certificatului. certSIGN CA va începe investigarea unui raport de certificate cu probleme in maximum 24 de ore de la primire, și va decide dacă revocarea sau alte acțiuni corespunzătoare sunt justificate de cel puțin următoarele motive:

1. Natura presupusei probleme;
2. Numarul de rapoarte de certificate cu probleme primite despre un anumit Certificat sau Beneficiar.
3. Entitatea care raportează (de exemplu, o reclamatie din partea unui angajat al unei autorități de aplicare a legii potrivit căreia un site Web este implicat în activități ilegale ar trebui să aibă mai multă greutate decât o reclamație a unui consummator care susține că nu a primit bunurile comandate); și
4. Legislația relevantă.

certSIGN CA menține 24x7 capacitatea de a răspunde intern la o raportare cu probleme de certificate cu prioritate ridicată (Certificate Problem Report), și, după caz, să transmită o plângere autorităților de aplicare a legii și/sau să revoce un certificat care face obiectul unei astfel de plângeri. Raportările privind problemele de certificate se trimit la adresa **revokecsgn@certsign.ro**.

1.5.3 Persoana care decide conformitatea CPP cu politica

Nume	Comitetul de Management al Politicilor și Procedurilor (CMMP)
Telefon	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel 1.5.3 Persoana decidentă pentru conformitate

1.5.4 Procedurile de aprobare a CPP

Comitetul de Management al Politicilor și Procedurilor este responsabil de aprobarea CPP.
Procedura de aprobare este cuprinsă într-o instrucțiune internă.
Subiecții/Beneficiarii vor respecta CPP-ul publicat la:
https://www.certsign.ro/ro/document/codul-de-practici-si-proceduri-certsign/
Subiecții/Beneficiarii care nu acceptă noii termenii și reglementările modificate ale CPP, sunt obligaţi să depună, în termen de 15 zile de la data la care noua versiune a CPP a fost aprobată, o declaraţie în acest sens. Acest lucru va duce la încetarea contractului de prestări servicii de certificare și la revocarea certificatului emis în baza acestuia.

1.6 Definiții și acronime

1.6.1 Definitii

Afiliat: O corporație, parteneriat, asociere în participație sau altă entitate care controlează, este controlată de sau sub control comun cu o altă entitate sau o agenție, departament, subdiviziune politică sau orice entitate care operează sub controlul direct al unei entități guvernamentale.

Beneficiar/Solicitant: persoana fizică sau entitatea juridică care solicită (sau solicită reînnoirea) unui certificat. După emiterea certificatului, Solicitantul este denumit Beneficiar. Pentru certificatele emise dispozitivelor, Solicitantul este entitatea care controlează sau

operează dispozitivul numit în certificat, chiar dacă dispozitivul trimite cererea de certificat efectivă.

Reprezentant al Beneficiarului: o persoană fizică sau sponsor uman care este fie **Beneficiarul**, angajat de **Beneficiar**, fie un agent autorizat care are autoritate expresă pentru a-l reprezenta: (i) care semnează și depune sau aprobă o cerere de certificat în numele **Beneficiarului**și / sau (ii) care semnează și depune un acord de beneficiar în numele **Beneficiarului**și / sau (iii) care recunoaște Condițiile de utilizare în numele **Beneficiarului**atunci când **Beneficiarul**este afiliat al CA sau este CA.

Furnizor de software de aplicație: un furnizor de software de browser de Internet sau alt software de aplicație care folosește certificate care afișează sau utilizează certificate și încorporează certificate de root.

Scrisoare de atestare: o scrisoare care atestă faptul că informațiile despre subiect sunt corecte, scrise de un contabil, avocat, oficial guvernamental sau alt terț de încredere în care se bazează în mod obișnuit pentru astfel de informații.

Perioada de audit: Într-o perioadă de timp de audit, perioada cuprinsă între prima zi (începerea) și ultima zi de operațiuni (sfârșitul) acoperită de auditori în misiunea lor. (Acest lucru nu este același cu perioada de timp în care auditorii sunt la fața locului la CA.) Regulile de acoperire și durata maximă a perioadelor de audit sunt definite în secțiunea 8.1.

Raport de audit: un raport al unui auditor calificat care să precizeze opinia auditorului calificat cu privire la faptul dacă procesele și controalele unei entități sunt conforme cu prevederile obligatorii ale acestor cerințe.

Nume domeniu autorizat: Numele de domeniu utilizat pentru obținerea autorizației pentru eliberarea certificatului pentru un anumit FQDN. CA poate utiliza FQDN returnat dintr-o căutare DNS CNAME ca FQDN în scopul validării domeniului. Dacă FQDN conține un caracter wildcard, atunci CA TREBUIE să elimine toate etichetele wildcard din partea cea mai stângă a FQDN solicitat. CA poate tăia zero sau mai multe etichete de la stânga la dreapta până când întâlnește un nume de domeniu de bază și poate utiliza oricare dintre valorile intermediare în scopul validării domeniului.

Porturi autorizate: unul dintre următoarele porturi: 80 (http), 443 (http), 25 (smtp), 22 (ssh).

Nume domeniu de bază: porțiunea unui FQDN solicitat, care este primul nod de nume de domeniu rămas dintr-un sufix controlat de registru sau public, plus sufixul controlat de registru sau public (de exemplu, „exemplu.co.uk” sau „exemplu.com "). Pentru FQDN-urile în care nodul de nume de domeniu cel mai potrivit este un gTLD care are specificația ICANN 13 în acordul său de registru, gTLD în sine poate fi utilizat ca nume de domeniu de bază.

CAA: De la RFC 6844 (http: tools.ietf.org/html/rfc6844): „Înregistrarea resurselor DNS de autorizare a autorității de certificare (CAA) permite unui titular de nume de domeniu DNS să specifice autoritățile de certificare (CA) autorizate să elibereze certificate pentru acel

domeniu. Publicarea înregistrărilor de resurse CAA permite unei autorități publice de certificare să implementeze controale suplimentare pentru a reduce riscul de emisie neintenționată a certificatului. ”

Certificat: un document electronic care utilizează o semnătură digitală pentru a lega o cheie publică și o identitate.

Date de certificat: solicitări de certificat și date aferente acestora (indiferent dacă sunt obținute de la solicitant sau altfel) aflate în posesia sau controlul CA sau la care CA are acces.

Proces de gestionare a certificatelor: Procese, practici și proceduri asociate cu utilizarea cheilor, software-ului și hardware-ului, prin care CA verifică datele certificatelor, emite certificate, menține un depozit și revocă certificatele.

Politica de certificare: un set de reguli care indică aplicabilitatea unui anume certificat, la o comunitate specifică și / sau la implementarea PKI, cu cerințe comune de securitate, și care descrie limitele și utilizările acceptabile ale certificatelor din PKI.

Raport problemă certificat: reclamație privind compromisul cheie suspectat, utilizarea necorespunzătoare a certificatului sau alte tipuri de fraudă, compromis, utilizare necorespunzătoare sau comportament inadecvat legat de certificate.

Listă de revocare a certificatelor: o listă actualizată în mod regulat cu certificate revocate, care este creată și semnată digital de către CA care a emis certificatele.

Autoritatea de certificare: o organizație care este responsabilă pentru crearea, emiterea, revocarea și gestionarea certificatelor. Termenul se aplică în mod egal atât CA-urilor ROOT, cât și CA-urilor Intermediare.

Declarație de practici de certificare/Cod de Practici și Proceduri: este o declarație a practicilor pe care le folosește o Autoritate de Certificare în emiterea și managementul certificatelor.

Control: „Control” (și semnificațiile sale corelative, „controlat de” și „sub control comun cu”) înseamnă deținerea, directă sau indirectă, a puterii de a: (1) conduce conducerea, personalul, finanțele sau planurile acestor entitate; (2) controlează alegerea majorității directorilor; sau (3) votează acea parte din acțiunile cu drept de vot necesare pentru „control” conform legii jurisdicției de constituire sau înregistrare a entității, dar în niciun caz mai mică de 10%.

Țară: Fie membru al Organizației Națiunilor Unite SAU regiune geografică recunoscută ca stat suveran de cel puțin două națiuni membre ONU.

Certificat încrucișat: un certificat care este utilizat pentru a stabili o relație de încredere între două CA.

CSPRNG: Un generator de numere aleatorii destinat utilizării în sistem criptografic.

Terță parte delegată: o persoană fizică sau o entitate juridică care nu este CA și ale cărei activități nu se încadrează în auditul CA corespunzător, dar este autorizat de CA să asiste în procesul de gestionare a certificatelor prin efectuarea sau îndeplinirea unuia sau mai multor dintre cerințele CA găsite aici.

Contact de domeniu: Registrantul de nume de domeniu, contactul tehnic sau contractul administrativ (sau echivalentul unui ccTLD), așa cum este listat în numele de domeniu de bază sau într-o înregistrare DNS SOA, sau așa cum se obține prin contact direct cu Registratorul de nume de domeniu.

Eticheta domeniului: Din RFC 8499 (http://tools.ietf.org/html/rfc8499): „O listă ordonată de zero sau mai mulți octeți care alcătuiesc o parte a unui nume de domeniu. Utilizând teoria grafurilor, o etichetă identifică un nod într-o parte a grafului tuturor numelor de domenii posibile”.

Nume domeniu: O lista ordonata de una sau mai multe etichete de domeniu atribuită unui nod din sistemul de nume de domeniu (DNS).

Spațiu de nume de domeniu: ansamblul tuturor posibilelor nume de domenii care sunt subordonate unui singur nod din sistemul de nume de domenii.

Registrant de nume de domeniu: uneori denumit „proprietarul” unui nume de domeniu, dar mai corect persoana (persoanele) sau entitatea (entitățile) înregistrată la un registrator de nume de domeniu ca având dreptul de a controla modul în care este utilizat un nume de domeniu, cum ar fi persoana fizică sau Persoana Juridică care este listată ca „Registrant” de către WHOIS sau de către Registratorul de Nume de Domeniu.

Registrator de nume de domeniu: o persoană sau entitate care înregistrează nume de domenii sub auspiciile sau prin acord cu: (i) Internet Corporation for Assigned Names and Numbers (ICANN), (ii) o autoritate / registru național de nume de domeniu sau (iii)) un centru de informare a rețelei (inclusiv afiliații, contractanții, delegații, succesorii sau cesionarii lor).

Enterprise RA: un angajat sau agent al unei organizații neafiliate cu CA care autorizează eliberarea certificatelor acelei organizații.

Data expirării: data „Nu după” dintr-un certificat care definește sfârșitul perioadei de valabilitate a unui certificat.

Numele de domeniu complet calificat: un nume de domeniu care include etichetele tuturor nodurilor superioare din sistemul de nume de domenii Internet.

Entitate guvernamentală: o entitate juridică, o agenție, un departament, un minister, o filială sau un element similar al guvernului unei țări sau subdiviziuni politice din această țară (cum ar fi un stat, o provincie, un oraș, un județ etc.).

Cerere de certificat cu risc ridicat: o cerere care să fie marcată de CA pentru control suplimentar prin referire la criteriile interne și bazele de date menținute de CA, care pot

include nume cu risc mai mare de phishing sau alte utilizări frauduloase, nume conținute în cereri de certificate respinse anterior sau certificate revocate , nume enumerate în lista de phishing Miller Smiles sau în lista de navigare sigură Google sau nume pe care CA le identifică utilizând propriile criterii de reducere a riscurilor.

Nume intern: un șir de caractere (nu o adresă IP) într-un câmp Common Name sau Name Alternative Name al unui certificat care nu poate fi verificat ca unic la nivel global în cadrul DNS-ului public în momentul emiterii certificatului, deoarece nu se termină cu un Top Domeniu de nivel înregistrat în baza de date a zonei ROOT a IANA.

CA Intermediar: un CA care este sub ROOT CA intr-o structura PKI, și care este gestionat, în mod uzual, de aceeași entitate ca și cea care gestionează ROOT CA

CA emitent: în legătură cu un anumit certificat, CA care a emis certificatul. Aceasta poate fi fie o CA ROOT, fie o CA Intermediară/Subordonata.

Compromisul cheii: se spune că o cheie privată este compromisă dacă valoarea sa a fost dezvăluită unei persoane neautorizate, dacă o persoană neautorizată a avut acces la aceasta.

Script de generare a cheilor: un plan documentat de proceduri pentru generarea unei perechi de chei CA.

Pereche de chei: cheia privată și cheia publică asociată.

Eticheta LDH: Din RFC 5890 (http://tools.ietf.org/html/rfc5890): „Un șir format din litere ASCII, cifre și cratimă, cu restricția suplimentară că cratima nu poate apărea la începutul sau la sfârșitul șirului. La fel ca toate etichetele DNS, lungimea sa totală nu trebuie să depășească 63 de octeți.”

Entitate juridică: o asociație, corporație, parteneriat, proprietate, trust, entitate guvernamentală sau altă entitate cu statut juridic în sistemul juridic al unei țări.

Etichetă LDH fără rezerve: Din RFC 5890 (http://tools.ietf.org/html/rfc5890): „Setul de etichete LDH valabile care nu au «--» în a treia și a patra poziție.”

Identificator de obiect: un identificator unic alfanumeric sau numeric înregistrat conform standardului aplicabil al Organizației Internaționale pentru Standardizare pentru un anumit obiect sau clasă de obiecte.

Răspuns OCSP: un server online operat sub autoritatea CA și conectat la depozitul său pentru procesarea cererilor de stare a certificatului. A se vedea, de asemenea, Protocolul de stare a certificatului online.

Protocolul de stare a certificatului online: un protocol de verificare a certificatului online (OCSP), care permite software-ului de aplicație terță parte să determine starea unui certificat identificat. A se vedea, de asemenea, Răspuns OCSP.

Companie mamă: o companie care controlează o companie filială.

Cheie privată: cheia unei perechi de chei păstrată secretă de deținătorul perechii de chei și care este utilizată pentru a crea semnături digitale și / sau pentru a decripta înregistrări electronice sau fișiere care au fost criptate cu cheia publică corespunzătoare.

Cheie publică: cheia unei perechi de chei care poate fi dezvăluită public de deținătorul cheii private corespunzătoare și care este utilizată de o parte care se bazează pentru a verifica semnăturile digitale create cu cheia privată corespunzătoare a titularului și / sau pentru a cripta mesajele astfel încât acestea poate fi decriptat numai cu cheia privată corespunzătoare a titularului.

Infrastructură cu cheie publică: un set de hardware, software, persoane, proceduri, reguli, politici și obligații utilizate pentru a facilita crearea, emiterea, gestionarea și utilizarea de încredere a certificatelor și cheilor bazate pe criptografie cu cheie publică.

Certificat de încredere public: un certificat care este de încredere în virtutea faptului că certificatul său ROOT (rădăcină) corespunzător este distribuit ca o ancoră de încredere într-un software de aplicație disponibil pe scară largă.

P-Label: A XN-Label that contains valid output of the Punycode algorithm (as defined in RFC 3492, Section 6.3) from the fifth and subsequent positions.

Auditor calificat: O persoană fizică sau entitate juridică care îndeplinește cerințele secțiunii 8.2.

Valoare aleatorie: o valoare specificată de o CA către solicitant care prezintă cel puțin 112 biți de entropie.

Nume de domeniu înregistrat: un nume de domeniu care a fost înregistrat la un registrator de nume de domeniu.

Autoritatea de înregistrare (RA): Orice entitate juridică care este responsabilă pentru identificarea și autentificarea subiecților certificatelor, dar care nu este o CA și, prin urmare, nu semnează sau emite certificate. Un RA poate ajuta în procesul de solicitare a certificatului sau în procesul de revocare sau ambele. Când „RA” este folosit ca adjectiv pentru a descrie un rol sau o funcție, nu implică neapărat un corp separat, dar poate face parte din CA.

Sursă de date fiabile: un document de identificare sau o sursă de date utilizate pentru verificarea informațiilor de identificare a subiectului, care sunt recunoscute în general între întreprinderile comerciale și guverne ca fiind fiabile și care a fost creată de o terță parte în alt scop decât solicitantul care obține un certificat.

Metodă de comunicare fiabilă: o metodă de comunicare, cum ar fi o adresă de livrare poștală / de curierat, un număr de telefon sau o adresă de e-mail, care a fost verificată folosind o altă sursă decât reprezentantul solicitantului.

Parte terță: Orice persoană fizică sau entitate juridică care se bazează pe un certificat valabil. Un furnizor de software de aplicație nu este considerat un partener de încredere atunci când software-ul distribuit de un astfel de furnizor afișează doar informații referitoare la un certificat.

Depozit: o bază de date online care conține documente de guvernanță PKI divulgate public (cum ar fi Politicile de certificat și Declarațiile practice de certificare) și informații despre starea certificatului, fie sub forma unui CRL, fie a unui răspuns OCSP.

Jeton de solicitare: valoare derivată dintr-o metodă specificată de CA care leagă această demonstrație de control de cererea de certificat.

Jetonul de solicitare TREBUIE să încorporeze cheia utilizată în cererea de certificat.
Un jeton de cerere POATE include un timestamp pentru a indica când a fost creat.
Un jeton de cerere POATE include alte informații pentru a asigura unicitatea acestuia.
Un jeton de solicitare care include un timestamp Va rămâne valabil cel mult 30 de zile de la momentul creării.
Un jeton de solicitare care include un timestamp TREBUIE tratat ca nevalid dacă marca sa de timp este în viitor.
Un jeton de solicitare care nu include un timestamp este valid pentru o singură utilizare și CA NU îl va reutiliza pentru o validare ulterioară.
Legarea va folosi un algoritm de semnătură digitală sau un algoritm hash criptografic cel puțin la fel de puternic ca cel care va fi utilizat la semnarea cererii de certificat.

Conținut obligatoriu WebSite: fie o valoare aleatorie, fie un jeton de solicitare, împreună cu informații suplimentare care identifică în mod unic beneficiarul, așa cum este specificat de CA.

Cerințe: Cerințele de bază găsite în CABF BR.

Adresă IP rezervată: o adresă IPv4 sau IPv6 pe care IANA a marcat-o ca rezervată:
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

ROOT CA (CA rădăcină): Autoritatea de certificare de nivel superior al cărei certificat este distribuit de furnizorii de software de aplicații, care reprezintă o "ancoră de încredere" pentru lanțul de încredere, și care emite certificate CA Intermediare.

Certificat ROOT CA: certificatul auto-semnat emis de ROOT CA pentru a se identifica și pentru a facilita verificarea certificatelor eliberate către CA-urile sale Intermediare.

Certificat de abonat cu durată de viață scurtă: Pentru certificatele emise la 15 martie 2024 sau după această dată și înainte de 15 martie 2026, un certificat de abonat cu o perioadă de valabilitate mai mică sau egală cu 10 zile (864 000 de secunde). Pentru

certificatele emise la 15 martie 2026 sau după această dată, un certificat de abonat cu o perioadă de valabilitate mai mică sau egală cu 7 zile (604 800 secunde).

Stat suveran: un stat sau o țară care își administrează propriul guvern și nu este dependentă sau supusă unei alte puteri.

Subiect: persoana fizică, dispozitivul, sistemul, unitatea sau entitatea juridică identificată într-un certificat ca subiect. Subiectul este fie Beneficiarul, fie un dispozitiv aflat sub controlul și funcționarea Beneficiarului.

Informații despre identitatea subiectului: informații care identifică subiectul certificatului. Informațiile de identitate ale subiectului nu includ un nume de domeniu listat în extensia subjectAltName sau în câmpul Subject commonName.

CA Subordonată: O autoritate de certificare al cărei certificat este semnat de CA rădăcină sau de o altă CA subordonată.

Beneficiar: o persoană fizică sau o entitate juridică căreia i se eliberează un certificat și care este legată legal de un acord de beneficiar sau de Termeni de utilizare.

Acord de beneficiar: Un acord între CA și solicitant / beneficiar care specifică drepturile și responsabilitățile părților.

Companie filială: o companie care este controlată de o companie-mamă.

Certificat CA Intermediar/Subordonat constrâns tehnic: un certificat CA Intermediar care utilizează o combinație de setări de utilizare a cheii extinse și setări de constrângere nume pentru a limita domeniul de aplicare în care certificatul CA Intermediar poate emite beneficiar sau certificate CA Intermediar suplimentare.

Termeni de utilizare: dispoziții privind păstrarea în siguranță și utilizările acceptabile ale unui certificat emis în conformitate cu aceste cerințe atunci când solicitantul / beneficiarul este afiliat al CA sau este CA.

Sistem de încredere: hardware, software și proceduri de computer care sunt: în mod rezonabil sigure de intruziuni și abuzuri; să ofere un nivel rezonabil de disponibilitate, fiabilitate și funcționare corectă; sunt adecvate în mod rezonabil pentru a-și îndeplini funcțiile prevăzute; și să aplice politica de securitate aplicabilă.

Nume de domeniu neînregistrat: un nume de domeniu care nu este un nume de domeniu înregistrat.

Certificat valid: un certificat care trece procedura de validare specificată în RFC 5280.

Specialiști în validare: cineva care îndeplinește sarcinile de verificare a informațiilor specificate de aceste cerințe.

Perioada de valabilitate: Din RFC 5280, (http://tools.ietf.org/html/rfc5280) : perioada de timp de la notBefore la notAfter, inclusiv.

WHOIS: Informații preluate direct de la registratorul de nume de domeniu sau de la operatorul de registru prin intermediul protocolului definit în RFC 3912, al protocolului de acces la date de registru definit în RFC 7482 sau al unui site web HTTPS.

Certificate Wildcard: un certificat care conține un asterisc (*) în stanga-cea mai mare poziție a oricărui subiect pe deplin-Numele de domenii calificate conținute în certificat.

Nume domeniu wildcard: un nume de domeniu format dintr-un singur caracter asterisc, urmat de un singur caracter punct („*.”) Urmat de un Complet-Numele de domeniu calificat.

XN-Label: Din RFC 5890 (http://tools.ietf.org/html/rfc5890): „Clasa de etichete care încep cu prefixul «xn--» (independent de majuscule și minuscule), dar care, în rest, sunt conforme cu regulile pentru etichetele LDH”.

1.6.2 Acronime

Acronim	Original	Traducere
AICPA	American Institute of Certified Public Accountants	Institutul American al Contabililor Publici Autorizați
ADN	Authorization Domain Name	Autorizare Nume de domeniu
CA	Certification Authority	Autoritatea de certificare
CAA	Certification Authority Authorization	Autorizarea autorității de certificare
CARL	Certification Authority Revocation List	Lista de revocare a autorității de certificare
ccTLD	Country Code Top-Level Domain	Cod de țară Domeniu de nivel superior
CICA	Canadian Institute of Chartered Accountants	Institutul canadian al contabililor autorizați
CP	Certificate Policy	Politica de certificare
CPS	Certification Practice Statement	Declarație privind practicile de certificare
CRL	Certificate Revocation List	Lista de revocare a certificatelor
DBA	Doing Business As	Făcând afaceri sub numele de
DN	Distinguished Name	Denumire distinctă
DNS	Domain Name System	Sistem de nume de domeniu
DV	Domain Validated	Domeniu validat
EV	Extended Validation	Validare extinsă
FIPS	(US Government) Federal Information Processing Standard	(Guvernul SUA) Standardul federal de prelucrare a informațiilor
FQDN	Fully-Qualified Domain Name	Nume de domeniu complet calificat
IM	Instant Messaging	Mesagerie instantanee
IANA	Internet Assigned Numbers Authority	Autoritatea de atribuire a numerelor de internet
ICANN	Internet Corporation for Assigned Names and Numbers	Corporatia Internet pentru alocarea Numelor si Numerelor
ISO	International Organization for Standardization	Organizația Internațională pentru Standardizare
NIST	(US Government) National Institute of Standards and Technology	(Guvernul SUA) Institutul Național de Standarde și Tehnologie
OCSP	Online Certificate Status Protocol	Protocol de stare a certificatelor online
OID	Object Identifier	Identificator de obiect
OV	Organization Validated	Organizație validată

Acronim	Original	Traducere
PKI	Public Key Infrastructure	Infrastructură cu cheie publică
PPMB	Policies and Procedures Management Body	Organism de gestionare a politicilor și procedurilor
QSCD	Qualified Electronic Signature Creation Device	Dispozitiv de creare a semnăturilor electronice calificat
QWAC	Qualified Certificate for Website Authentication	Certificat calificat pentru autentificarea site-urilor web
RA	Registration Authority	Autoritatea de înregistrare
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm	Algoritm criptografic asimetric Rivest, Shamir, Adleman
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)	MIME securizat (Extensii multifuncționale de poștă electronică pe Internet)
SSL	Secure Sockets Layer	Secure Sockets Layer
TLS	Transport Layer Security	Securitatea stratului de transport
TSP	Trust Services Provider	Furnizor de servicii de încredere
UTC	Coordinated Universal Time	Timp universal coordonat
VoIP	Voice Over Internet Protocol	Protocol de voce pe internet

2 Publicare și responsabilități Depozitar

2.1 Depozitar

Depozitarul este disponibil on-line: http://www.certsign.ro/repository. Acesta conține:

- Politica de Certificare și Codul de Practici și Proceduri pentru CA-urile operate de certSIGN https://www.certsign.ro/ro/document/codul-de-practici-si-proceduri-certsign/
- Certificatele Root CA și ale CA-urilor Intermediare https://www.certsign.ro/ro/resurse/lantul-de-incredere/
- Certificatele Subiecților https://registru.certsign.ro/cgi-bin/pubral/pubra/get_cert
- Listele Certificatelor Revocate https://www.certsign.ro/ro/resurse/lista-certificate-revocate/
- Temenii și condițiile privind utilizarea certificatelor digitale
    - https://www.certsign.ro/ro/document/termeni-si-conditii-generale/
    - https://www.certsign.ro/ro/document/termeni-si-conditii-generale-pentru-certificate-ssl-dv-si-ov/

Depozitarul este gestionat și controlat de certSIGN; prin urmare, certSIGN se angajează:

- Să depună toate eforturile necesare pentru a se asigura că toate certificatele publicate în Depozitar aparțin Subiecților înscriși în certificate și că Subiecții și-au dat acordul asupra acestor certificate,
- Să se asigure că certificatele Autorităţilor de Certificare, Autorităţii de Înregistrare aparţinând domeniului certSIGN, precum și certificatele Subiecţilor sunt publicate și arhivate la timp,
- Să asigure publicarea și arhivarea CPP, a listei aplicaţiilor recomandate și a dispozitivelor recomandate,
- Să ofere acces la informaţiile despre starea certificatelor prin publicarea de Liste de Certificate Revocate (CRL), prin intermediul serverelor OCSP sau prin interogări HTTP,
- Să asigure accesul permanent la informaţiile din Depozitar pentru Autoritățile de Certificare, Autoritatea de Înregistrare, Subiecţi și Entităţile Partenere,
- Să publice CRL-uri sau alte informații în timp util și în concordanță cu termenele limită menționate în CPP,
- Să asigure accesul sigur și controlat la informațiile din Depozitar.

Răspunderea pentru Depozitar și consecințele serviciului său aparțin certSIGN (vezi cap.9).

2.2 Publicarea informațiilor de certificare

La emiterea unui certificat digital, certificatul complet și corect este comunicat de certSIGN Subiectului pentru care a fost emis certificatul.

Certificatele vor fi disponibile pentru publicare doar în cazurile pentru care a fost obținut acordul Subiectului, așa cum este descris în documentul Termeni și Condiții.

Pentru toate certificatele emise, informațiile privind starea certificatului sunt disponibile prin CRL-uri și serviciile de validare a certificatelor sunt furnizate de certSIGN 24x7x365.

certSIGN este conform cu ultima versiune publicată a '*Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates*' publicate la http://www.cabforum.org. În eventuale neconcordanțe între acest document și cerințele BR, respectivele *Baseline Requirements* au prioritate față de acest document.

Depozitul (repository) este o interfaţă publică către următoarele informaţii:

- versiunea curentă și cele anterioare ale Politicii de certificare și a Codului de Practici și Proceduri

- Modelele de contract cu Abonaţii și Entităţile Partenere,
- Declaraţia certSIGN cu privire la asigurarea confidenţialităţii informaţiilor recepţionate și procesate
- Registrul (în accepţiunea legii semnaturii electronice)
- certificatele certSIGN ROOT CA, certSIGN SSL DV CA Class 3 G2, precum și certificatele tuturor Autorităţilor de Certificare care aparţin sau sunt legate la domeniul certSIGN (de exemplu, certificatele Autorităţilor de Certificare noi înregistrate de RA),
- certificatele abonaţilor finali (entităţi fizice și juridice, inclusiv angajaţii certSIGN și maşinile / aplicaţiile software deţinute de aceştia și care sunt indispensabile pentru serviciile PKI) conform Legii semnaturi electronice.

În plus, în Depozit se găsesc informaţii legate de funcţionarea certificatelor, cum ar fi:

- Listele de certificate Revocate (CRL); CRL-urile sunt disponibile în aşa numitele puncte de distribuţie a CRL-urilor, a căror adresă este specificată în fiecare certificat emis de certSIGN; locaţia principala de distribuţie a CRL-urilor este în depozit la adresa: https://www.certsign.ro/ro/resurse/lista-certificate-revocate/,
- Alte informaţii ce se modifică în timp real,

Conţinutul depozitarului este disponibil prin Internet la adresa: https://www.certsign.ro/ro/depozitar/ sau prin intermediul protocolului LDAP v3, la adresa ldap.certsign.ro, port 389

2.3 Timpul sau frecvența publicării

Informațiile publicate de certSIGN sunt actualizate anual sau cu următoarea frecvență:

- Politici de Certificare și CPP – vezi Capitolul 1.5,
- Certificatele Autorităților de Certificare – după emiterea unui nou certificat;
- Certificatul Autorității de Înregistrare (RA) – după emiterea unui nou certificat;
- Certificatele Subiecților – la obținerea consimțământului, după fiecare emitere a unui nou certificat;
- Lista Certificatelor Revocate (CRL) vezi Capitolul 4.9.7;
- Rapoartele auditurilor realizate de instituții autorizate – când le primește certSIGN;
- Informațiile suplimentare – după fiecare actualizare.

2.4 Controlul accesului la Depozitar

Toate informațiile publicate de certSIGN în Depozitar la adresa https://www.certsign.ro/ro/depozitar/ sunt accesibile publicului.

certSIGN a implementat mecanisme logice și fizice de protecţie împotriva adăugării, ştergerii și modificării neautorizate a informaţiilor publicate în Depozitar.

Beneficiarii, Subiecții și Entitățile Partenere au acces doar read-only prin intermediul Internetului la toate depozitarele menționate în secțiunea 2.1.

certSIGN poate lua măsuri rezonabile de protecție împotriva și pentru prevenirea utilizării abuzive a depozitarului, a OCSP sau serviciilor de descărcare a CRL.

La descoperirea unor breșe ce afectează integritatea informaţiilor din Depozitar, certSIGN va lua măsurile corespunzătoare pentru a restabili integritatea informaţiilor, va trage la răspundere pe cei vinovaţi și va notifica imediat entităţile afectate.

3 Identificarea și autentificarea

Acest capitol prezintă regulile generale pentru verificarea identităţii Beneficiarului, reguli care se aplică la emiterea de certificate de către certSIGN. Acestea au la bază anumite tipuri de informaţii care sunt incluse în certificate și specifică mijloacele indispensabile pentru a se asigura că informaţia este precisă și credibilă la momentul emiterii certificatului.

Verificarea este făcută în mod obligatoriu în etapa de înregistrare și de modificare a datelor Beneficiarului precum și la cererea certSIGN în cazul oricărui alt serviciu de certificare. Tipul verificarii depinde de tipul certificatelor. Principiul de baza care se respecta este acela ca toate informațiile oferite de Beneficiar sunt verificate folosind o sursa independenta sau un canal alternativ de comunicare, inainte de a fi incluse in certificat.

3.1 Denumirea

Structura si utilizarea numelor din certificate este conform cu X.500, RFC5280, si CABF Baseline Requirements.
certSIGN nu permite utilizarea în certificate de nume de domenii internaționalizate (IDN).

3.1.1 Tipuri de nume

Certificatele emise de certSIGN respectă standardul X.509 v3. Aceasta înseamnă că emitentul de certificate și Autoritatea de Înregistrare care acţionează în numele emitentului aprobă numele Beneficiarului, conform standardului X.509 (cu referire la recomandările seriei X.500). Numele de bază ale Abonaților și ale emitenţilor de certificate plasaţi în certificatele certSIGN sunt în concordanţă cu Numele Distinctive – ND – (cunoscute și ca nume directoare), create respectând recomandările X.500 și X.520. În cadrul ND, este posibilă definirea de atribute ale Domain Name Service (DNS). Aceasta permite Abonaților să folosească două tipuri de nume: ND și DNS simultan. Această opţiune este foarte importantă în cazul emiterii de certificate către servere sub administrarea Beneficiarului.

Pentru a asigura o comunicare electronica facilă cu Beneficiarul, în certificatele certSIGN este folosit un nume suplimentar pentru Beneficiar. Acest nume poate de asemenea să conţină adresa de e-mail a Beneficiarului, în concordanţă cu recomandările RFC 822.

Numele directoarelor unde sunt reţinute certificatele, CRL-urile și Politica de certificare, ca și numele punctelor de distribuţie ale CRL-urilor prevederile protocolului LDAP referitoare la sintaxa numelui (vezi RFC 1778).
Certificatele SSL cu exceptia celor wildcard si certificatele de tip Unified Communications sunt emise cu un nume Fully Qualified Domain Name (FQDN) sau cu o adresa IP.
certSIGN nu emite certificate SSL care conţin „caracter de subliniere” („_”) în numele domeniului / dNSName, aceasta respectând versiunea actuală a recomandărilor CA / Browser Forum BR. FQDN cuprinde doar “P-labels” și „Non-Reserved LDH-labels”.

Certificatele SSL wildcard includ un asterisc. Inainte de emiterea unui astfel de certificat se determina daca asteriscul apare pe prima pozitie la stanga sufixului unui domeniu controlat de organizatia de inregistrare a domeniilor (de exemplu *.com.ro) sau a sufixului public (de exemplu *.ro, *.edu, “*.com”, “*.co.uk”; a se vedea RFC 6454 Sectiunea 8.2 pentru detalii) si daca acest lucru se intampla, CA-ul operat de certSIGN va respinge cererea, deoarece domeniul trebuie sa fie detinut sau controlat de catre Beneficiar.

In cazul certificatelor SSL, in timp ce FQDN sau un nume de domeniu autentificat este plasat in atributul Common Name (CN) al campului Subiect, poate fi de asemenea duplicat in extensia Subject Alternative Name la DNS Name. Subject Alternative Name sunt marcate ca non critice in conformitate cu RFC5280.

Certificatele SSL pot include adrese IP publice conform RFC2460 (IP version 6) sau RFC791 (IP version 4).

Certificatele de tip Unified Communications SSL (multi domain) pot include domenii nerutabile (de exemplu .local) sau IP-uri private (conform RFC 1918) in cadrul extensiei Subject Alternative Name. Emiterea de certificate SSL pentru domenii nerutabile, adrese IP private sau adrese IP rezervate (conform http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml si http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml) este catalogata ca fiind invechita.

3.1.2 Nevoia ca numele sa aibă inteles logic

Numele incluse în Numele Distinctiv al Beneficiarului au un sens în limba română sau în altă limbă care utilizează alfabet latin. Structura Numelui Distinctiv, aprobat / atribuit și verificat de o Autoritate de Înregistrare, depinde de tipul Beneficiarului.

Pentru entităţi private (persoane fizice sau angajaţi ai companiilor), ND constă din următoarele câmpuri, obligatorii sau nu (descrierea câmpului este urmată de abrevierea sa care respectă recomandările RFC 3280 și X.520):

- câmpul C – abrevierea internaţională pentru numele ţării (RO pentru România),
- câmpul S – judeţul / sectorul în care locuieşte Beneficiarul,
- câmpul L – oraşul în care Beneficiarul are domiciliul,
- Street – adresa,
- câmpul CN – numele Beneficiarului; numele unui produs sau echipament poate de asemenea să fie specificat aici,
- câmpul O – numele instituţiei în cadrul căreia lucrează Beneficiarul, în cazul în care certificatul este profesional
- câmpul OU – numele departamentului în care este angajat Beneficiarul[2], în cazul în care certificatul este profesional
- câmpul T – funcţia
- câmpul SN – numele de familie al Beneficiarului,
- câmpul G – prenumele Beneficiarului,
- câmpul P – pseudonimul Beneficiarului pe care acesta îl foloseşte în mediul său, sau pe care doreşte să îl folosească pentru a nu-și descoperi numele sau prenumele real,
- câmpul Phone – numărul de telefon,
- câmpul Serial Number – codul personal de identificare al Beneficiarului în sensul Legii semnaturii digitale.

Pentru persoanele juridice, ND constă în următoarele câmpuri opţionale (descrierea câmpului este urmată de abrevierea sa care respectă recomandările X.520):

- câmpul C – abrevierea internaţională pentru numele ţării (RO pentru România),
- câmpul O – numele instituţiei,

[2] *Interzis pentru certificate SSL eliberate la sau după 1 septembrie 2022*

- câmpul OU – numele departamentului organizaţiei[3],
- câmpul S – judeţul / sectorul în care funcţionează organizaţia,
- câmpul L – oraşul în care Beneficiarul locuieşte sau are domiciliu,
- câmpul CN – numele instituţiei,
- câmpul Phone – numărul de telefon,

Numele Beneficiarului trebuie confirmat de un operator al Autorităţii de Înregistrare și aprobat de o Autoritate de Certificare. certSIGN asigură (în cadrul domeniului său) unicitatea ND-urilor.
CertSIGN nu emite certificate SSL care conțin „underscore character" („_") în numele de domeniu/dNSName, fiind in concordanta cu recomandarile CA/Browser Forum BR din ultima versiune publicată.

3.1.3 Anonimitatea sau pseudonimitatea Beneficiarilor
N/A

3.1.4 Reguli de interpretare a diferitelor formate de nume
Interpretarea câmpurilor din certificatele emise de certSIGN se face în concordanţă cu profilele de certificate descrise în Profilul certificatelor și al CRL-urilor (Capitolul 7). Crearea și interpretarea ND-ului vor fi realizate conform recomandărilor specificate în Capitolul 3.1.2.

3.1.5 Unicitatea numelor
Identificarea fiecărui deţinător de certificate emise de certSIGN se realizează pe baza Numelui Distinctiv(ND). *certSIGN asigură unicitatea ND-ului asignat fiecărui Beneficiar.*

ND-ul Beneficiarului este sugerat de acesta în cererea sa. Dacă numele este în concordanţă cu cerinţele generale specificate în Capitolul 3.1.1 și 3.1.2, un operator al Autorităţii de Înregistrare acceptă temporar sugestia. Dacă operatorul Autorităţii de Înregistrare are acces la baza de date cu ND-uri, acesta va verifica și unicitatea numelui în domeniul certSIGN. Dacă testul confirmă unicitatea, ND-ul este acceptat. În cazul lipsei accesului la baza de date a certSIGN, decizia cu privire la acceptarea sau refuzul ND-ului se ia de către operatorul Autorităţii de Certificare.

Dacă un ND sugerat de Beneficiar încalcă drepturile altor entităţi la acest nume, certSIGN poate adăuga alte atribute ND-ului (ex. numărul serial), care asigură unicitatea acestui nume în cadrul domeniului certSIGN. Un Beneficiar este îndreptăţit să refuze un ND sugerat în procedura specificată în Capitolul 4.4.

Formatul numelui unic global pentru un Beneficiar are următoarea formă:

certSIGN.ro / numele emitentului / numele Beneficiarului

în care **certSIGN.ro** este numele domeniului certSIGN, numele emitentului este ND-ul uneia din Autoritățile de Certificare și numele Beneficiarului este ND-ul câmpului *subject* din certificat. Valorile ultimelor două câmpuri sunt extrase din certificat.

Dacă un Beneficiar renunţă la serviciile certSIGN, eventuala cerere de atribuire a ND-ului său altui Beneficiar trebuie respinsă.

[3] *Interzis pentru certificate SSL eliberate la sau după 1 septembrie 2022*

certSIGN poate înregistra un Beneficiar cu un Nume Distinctiv folosit în trecut de alt Beneficiar numai cu acordul scris al acestuia din urmă.

Pentru certificatele SSL unicitatea numelui este asigurată prin integrarea in Common Name a numelui de domeniu, care este aprobat de ICANN ca find unic.

3.1.6 Recunoașterea, autentificarea și rolul mărcilor înregistrate

Certsign nu verifica daca Beneficiarul (utilizatorul/titularul unui certificat) este persoana în numele căreia marca este înregistrată în Registrul Naţional al Mărcilor sau daca beneficiaza de dreptul, acordat de titularul marcii, de utilizare a acesteia, Beneficiarul fiind singurul raspunzator pentru corectitudinea informaţiilor furnizate in vederea eliberarii certificatului. Oficiul de Stat pentru Invenţii și Mărci este organul de specialitate al administraţiei publice centrale, unica autoritate care asigură pe teritoriul României protecția mărcilor și indicaţiilor geografice. In conformitate cu prevederile Legii nr. 84/1998 privind mărcile și indicaţiile geografice, "Dreptul asupra mărcii este dobândit și protejat prin înregistrarea acesteia la Oficiul de Stat pentru Invenţii și Mărci." (Art. 4)."

3.2 Validarea Inițială a Identității

Înregistrarea Beneficiarului are loc atunci când un Beneficiar care cere înregistrarea nu deţine un certificat valid emis de nici o Autoritate de Certificare afiliată la certSIGN.

Înregistrarea presupune un număr de proceduri care permit unei Autorități de Certificare – înainte de a emite un certificat către un Beneficiar – să adune date valide cu privire la o anumită entitate pentru identificarea acesteia.

Fiecare Beneficiar este supus unui proces de înregistrare o singură dată. După verificarea datelor puse la dispoziţie de un Beneficiar, acesta este inclus pe lista utilizatorilor autorizaţi ai serviciilor certSIGN și i se acordă un certificat de cheie publică.

Verificarea este obligatoriu efectuată în etapa înregistrării și modificării datelor Beneficiarului, precum și la cererea certSIGN în cazul oricărui alt serviciu de certificare. Tipul de verificare depinde de tipul de certificat. Principiul de bază care este urmat este că toate informațiile furnizate de Beneficiarul certificatului TREBUIE să fie verificate folosind o sursă independentă de informații sau un canal de comunicare alternativ înainte ca acestea să fie incluse în certificat.

Fiecare Beneficiar care solicită servicii specifice infrastructurilor de chei publice și care cere emiterea unui certificat trebuie (înainte de emiterea certificatului) să:

- completeze un formular de înregistrare disponibil on-line, sau ca document ce poate fi downloadat de pe site-ul Web al certSIGN,
- genereze o pereche de chei asimetrice RSA și să furnizeze Autorităţii de Înregistrare, dovada deţinerii unei chei private; opţional, Beneficiarul poate să însărcineze o Autoritate de Certificare sau Autoritatea de Înregistrare cu generarea acestei perechi de chei,
- sugereze un nume distinctiv (ND, vezi Capitolul 3.1.1),
- completeze și să trimită un formular de înregistrare care conține o cheie publică și dovada posesiei cheii private corespunzătoare acesteia,

- să se prezinte, opţional, la Autoritatea de Înregistrare și să furnizeze documentele necesare (dacă se cere acest lucru de politica de certificare pe baza căreia se emite certificatul),
- încheie un contract cu un agent al Autorităţii de Înregistrare în legătură cu furnizarea serviciilor de către certSIGN; prezentul Cod de Practici și Proceduri este parte integrantă a acestui contract.

Procedura de înregistrare poate solicita Beneficiarului, sau unui reprezentant autorizat al acestuia, să contacteze personal Autoritatea de Înregistrare. Cu toate acestea, certSIGN permite trimiterea cererilor de înregistrare prin poştă, e-mail, site-uri Web etc.

3.2.1 Dovada Posesiei Cheii Private

Dacă o entitate deţine o cheie privată când cere emiterea unui certificat, Autoritățile de Certificare și Autoritatea de Înregistrare care funcţionează în cadrul certSIGN trebuie să se asigure că entitatea deţine o cheie privată corespunzătoare cheii publice furnizate.

Verificarea posesiei cheii private se face pe baza aşa numitei dovezi de posesie (DP) a cheii private. Această dovadă reprezintă confirmarea că o cheie publică supusă procedurilor de certificare este perechea unei chei private deţinută în mod exclusiv de Beneficiar.

Forma dovezii depinde de tipul perechii de chei ce va fi certificată (pereche de chei pentru crearea unei semnaturi electronice, pentru criptare sau pentru negocierea de cheie).

Dovada de bază se realizează prin mecanisme criptografice (semnatura electronica și / sau criptare), aplicate în procesul de înregistrare și modificare a datelor și, periodic, pe cererea de reînnoire a cheii / certificatului.

Cerinţa de prezentare a dovezii de posesie a cheii private nu se aplică dacă, la cererea Beneficiarului, perechea de chei este generată de Autoritatea de Certificare sau de către Autoritatea de Înregistrare.

Cheile private se recomandă a fi generate în interiorul unui dispozitiv criptografic (token) sau, în cazul generării lor în afara token-ului, prin intermediul unui generator software sau hardware urmând ca apoi să fie importate pe token. Orice entitate poate deţine un token la momentul generării și importului cheii, sau token-ul poate fi furnizat entităţii după procesul de generare de cheie. În ultimul caz, certSIGN garantează că token-ul și cheia vor ajunge în mod sigur, direct la entitatea respectivă.

3.2.2 Autentificarea identității organizației

certSIGN ROOT CA G4 este o Autoritate de Certificare Primară pentru domeniul certSIGN. Orice altă autoritate de certificare subordonată certSIGN ROOT CA G4 este operată de către aceaşi entitate legală.
Astfel, Autentificarea entităţii Legale nu este necesară.
Solicitările de certificate se efectuează prin roluri de încredere asociate certSIGN Root CA G4, sub supravegherea Comitetului de Management al Politicilor și Procedurilor (CMPP).

3.2.3 Autentificarea Identității Persoanelor Fizice

Nu se aplică.

3.2.4 Informațiile neverificate ale Beneficiarului

Nu se aplică.

3.2.5 Validarea autorității
Nu se aplică.

3.2.6 Criterii pentru interoperare
certSIGN va dezvălui toate certificatele încrucișate care identifică CA ca subiect, cu condiția ca certSIGN să fi agreat sau să fi acceptat stabilirea relației de încredere.
certSIGN ROOT CA a emis un certificat încrucișat pentru certSIGN Web CA, emis inițial de certSIGN ROOT CA G2, ambele sisteme PKI fiind operate de certSIGN.

3.3 Identificarea și autentificarea pentru cererile de re-key

3.3.1 Identificarea și autentificare pentru re-key de rutină
Nu se aplică.

3.3.2 Identificarea și autentificarea pentru re-key după revocare
Nu se aplică.

3.4 Identificarea și autentificarea pentru cererile de revocare
Următoarele entităţi pot trimite cereri de revocare a certificatului unui Beneficiar:

- Beneficiarul, care este proprietarul certificatului,
- un reprezentant autorizat al Autorităţii de Certificare (în cazul certSIGN acest rol este rezervat administratorului de securitate),
- un mandat al Beneficiarului, de exemplu angajatorul sau; Beneficiarul trebuie imediat informat despre acest lucru,
- Autoritatea de Înregistrare care poate cere revocarea în numele unui Beneficiar, sau în nume propriu, dacă are informaţii care justifică revocarea certificatului.

Autoritatea de Înregistrare trebuie să acţioneze cu multă precauţie când procesează cereri ce nu au fost trimise de către un Beneficiar și să accepte numai acele cereri în conformitate cu Capitolul 4.9.1.

Când partea care cere revocarea certificatului nu este proprietarul certificatului (Beneficiarul), Autoritatea de Certificare trebuie:

- să verifice faptul ca respectiva parte are dreptul să emita o astfel de cerere
- sa ceara o justificare a respectivei cereri
- să trimită o notificare Beneficiarului despre revocare, sau despre iniţierea procesului de revocare.

Fiecare cerere trebuie trimisă:

- direct Autorităţii de Certificare sub formă electronica, cu sau fără confirmarea Autorităţii de Înregistrare,
- direct sau indirect (prin intermediul Autorităţii de Înregistrare) la Autoritatea de Certificare, sub formă ne-electronica (document pe hârtie, fax, telefon etc.)

4 Cerințe operaționale privind ciclul de viață al certificatului

Acest capitol descrie procedurile de bază care sunt comune tuturor tipurilor de certificate de Subiect în cadrul procesului de certificare.

Procedurile detaliate referitoare la serviciile componentelor PKI (CA, RA, semnatarii CRL, responsabili ai OCSP, Autoritatea de marcare temporala etc.) și personalul / rolurile implicate în procesul operațional al acestor componente sunt descrise în documentația internă confidențială.

Următoarea secțiune oferă o descriere a acestor documente care pot fi dezvăluite în mod public. În linii mari, procesul de certificare începe cu Subiectul: Transmiterea indirectă a unei cereri (După confirmarea inițială a cererii de către Autoritatea de Înregistrare). Pe baza cererii, Autoritatea de Certificare ia o decizie privind furnizarea / respingerea serviciului solicitat. Cererile trimise vor conține informațiile necesare pentru identificarea corectă a subiectului și a beneficiarului.

certSIGN oferă acces la următoarele servicii:

a. Înregistrare, certificare, re-key;
b. Revocarea certificatelor;
c. Verificarea valabilității certificatelor.

Programul de lucru

Serviciile sunt oferite atât on-line, cât și la ghișeu. Serviciile online sunt oferite continuu, în timp ce cele de la ghiseu sunt oferite de luni până vineri, între orele 9 și 18. Pentru toate clasele de certificate, serviciile de revocare a certificatelor sunt oferite în maxim 24 de ore de la solicitare.

Dacă cererea trimisă conține o cheie publică, cheia trebuie să fie pregătită astfel încât să se poată conecta criptografic cheia publică cu alte date specificate în cerere, în special cu datele de identificare ale beneficiarului. O solicitare poate conține în locul cheii publice solicitarea Beneficiarului de a genera o cheie asimetrică pe numele său. Acest lucru poate fi îndeplinit de o autoritate de certificare sau de autoritatea de înregistrare. După generare, cheile sunt trimise pe o cale protejată subiectului, astfel încât acestea să nu poată fi activate de către o persoană neautorizată.

4.1 Cererea de certificat

Aria de aplicabilitate a certificatelor stabileşte scopul în care poate fi folosit un certificat. Acest scop este definit de două elemente:

- primul defineşte aplicabilitatea certificatului (de exemplu, semnatura electronica, confidenţialitate),
- celălalt este o listă sau o descriere a aplicaţiilor permise sau interzise.

Certificatele emise de certSIGN pot fi folosite pentru a procesa și asigura securitatea informaţiilor (inclusiv autentificarea), având nivele diferite de credibilitate. Nivelul de credibilitate al informaţiei și vulnerabilitatea acesteia trebuie evaluate de către Beneficiar. În Politica de certificare și prezentul Cod de Practici și Proceduri sunt definite patru nivele de sensibilitate: Clasa 1 (nivelul de test), Clasa 2 (nivelul de bază), Clasa 3 (nivelul intermediar),

Clasa 4 (nivelul ridicat). Aceste nivele corespund celor patru nivele de credibilitate ale certificatelor (vezi Tabelul 1.4).

Nivelul de sensibilitate al informaţiei	Numele politicii de certificare	Aria de aplicabilitate
Clasa 1 (de test)	certSIGN Class 1	Cel mai scăzut nivel de credibilitate al identităţii unei entităţi. Certificatele de Clasa 1 se recomandă a se folosi pentru a testa compatibilitatea serviciilor certSIGN cu cele oferite de alţi furnizori de servicii PKI și pentru a testa funcţionalitatea certificatelor în cadrul aplicaţiilor testate. De asemenea, aceste certificate pot fi folosite în alte scopuri atâta timp cât asigurarea credibilităţii mesajelor trimise sau primite nu este importantă.
Clasa 2 (de bază)	certSIGN Class 2	Acest nivel oferă o securitate de bază pentru informaţii în medii cu grad scăzut de risc (risc fără consecinţe majore). Dintre acestea, menţionăm accesul la informaţii private acolo unde probabilitatea de apariţie a unui acces neautorizat nu este foarte mare. Aceste certificate pot fi folosite pentru a autentifica și controla integritatea informaţiei care a fost semnată și pentru a asigura confidenţialitatea informaţiei, mai ales în cazul poştei electronice.
Clasa 3 (intermediar)	certSIGN Class 3	Acest nivel se recomandă pentru asigurarea securităţii informaţiei în medii unde există riscul apariţiei de breşe de securitate iar consecinţele acestor breşe sunt moderate. Certificatele pot fi folosite pentru protecția tranzacţiilor financiare sau a tranzacţiilor în care există şanse de apariţie a fraudelor. De asemenea, aceste certificate pot fi folosite și pentru crearea de semnaturi electronice extinse.
Clasa 4 (ridicat)	certSIGN Class 4	Acest nivel corespunde mediilor în care şansele compromiterii datelor sunt foarte mari și în care consecinţele unui incident de securitate sunt foarte grave. Aceste certificate pot fi folosite pentru protecția tranzacţiilor de valoare nelimitată (dacă nu se specifică altceva în certificat), a tranzacţiilor în care există mari şanse de apariţie a fraudelor.

Tabel 1.4. Nivelul de sensibilitate al informaţiei și denumirea politicii

Entitatea parteneră este responsabilă pentru stabilirea nivelului de credibilitate necesar pentru un certificat folosit într-un anume scop. Luând în considerare factorii de risc semnificativi, entitatea parteneră trebuie să stabilească ce tip de certificat emis de certSIGN se potriveşte cerinţelor formulate. Abonaţii trebuie să cunoască cerinţele entităţii partenere

(de exemplu, aceste cerinţe pot fi publicate sub forma unei politici de semnatura sau politică de securitate informatică) și apoi să solicite certSIGN emiterea de certificate corespunzătoare acestor cerinţe.

4.1.1 Cine poate trimite o cerere de certificat

Cererile pentru una dintre Autoritățile de Certificare pot fi trimise direct de către un Beneficiar sau indirect de către un operator al Autorităţii de Înregistrare. Cererile Abonaților sunt trimise direct unei Autorități de Certificare sau indirect de către Autoritatea de Înregistrare. Cererile trimise direct pot viza înregistrarea sau modificarea de certificat; alte cereri referitoare la serviciile de certificare furnizate de o Autoritate de Certificare sunt de asemenea permise.

Operatorul poate trimite către o Autoritate de Certificare cererile altor Abonaţi confirmate de operator și în cazuri bine fondate chiar și cereri de revocare de certificate aparţinând Abonaților care încalcă prezentul Cod de Practici și Proceduri.

Cererile sunt trimise prin protocoale de comunicaţie precum HTTP, S/MIME sau TCP/IP.

certSIGN emite certificate numai pe baza cererilor de înregistrare, modificare, reînnoire sau modificare de certificate trimise de un Beneficiar.

Cererile pot fi trimise de diferite entităţi și pot viza certificate a căror aplicabilitate depinde de nevoile entităţii:

- certificate pentru persoane fizice – emise ca urmare a înaintării unei cereri de către reprezentanţi sau angajaţi ai organizaţiei care deleagă acestora autorizarea respectivă.
- certificate pentru dispozitive (care se aplică, de exemplu, serverelor) sau certificate ale aplicaţiilor deţinute de persoane fizice (angajaţi ai organizaţiei sau agenţi ai lor) autorizate să folosească acest dispozitiv sau aplicaţie.

4.1.2 Procesul de înregistrare și responsabilitățile

Procesul de înregistrare este gestionat de o entitate specifică numită Autoritatea de Înregistrare sau RA, care este operată de certSIGN în mod direct sau bazându-se pe un terț, în conformitate cu legislația națională.

RA este responsabilă de verificarea următoarelor elemente:

- Identitatea solicitată a subiectului / beneficiarului,
- Atributele revendicate ale subiectului / beneficiarului,
- Dreptul Subiectului / Beneficiarului la certificatul sau certificatele solicitate.

Procesul de înregistrare este realizat în conformitate cu regulile și metodele descrise în CPP, în regulamentele interne și procedurile RA și în legislația aplicabilă.

Subiectului i se oferă următoarele informații, care fac parte din Acordul cu Beneficiarii:

- formularul de înregistrare,
- adresa online a Termenilor și Condițiilor privind utilizarea certificatului,
- adresa online a CPP,
- regulamente, notificări sau alte documente furnizate de Subiect (vor fi definite în Acordul cu Beneficiarul).

Formularul de înregistrare semnat este considerat acceptul oficial de către Subiectul specificat în Acordul cu Beneficiarul, prin care Subiectul acceptă următoarele

- responsabilitatea sa ca informațiile furnizate de Subiect către RA să fie corecte, complete, valabile și actualizate,
- că certSIGN menține o perioadă de păstrare de 10 ani de la data emiterii certificatului pentru toate informațiile referitoare la înregistrare și înscriere, la cererea de certificat și la revocarea certificatului,
- că, în cazul în care certSIGN (în calitate de CA și RA) își încetează activitatea, aceste date pot fi transferate către o terță parte, în conformitate cu aceiași termeni și condiții definiți în Acordul cu Beneficiarul,
- recunoaște drepturile, obligațiile și responsabilitățile certSIGN și ale altor participanți la PKI, astfel cum sunt definite în Acordul cu Beneficiarul și în legislațiile naționale,
- că Subiectul are obligația de a informa certSIGN cu privire la orice schimbare sau eveniment care poate afecta valabilitatea sau conținutul certificatului

Procesul de înregistrare
Procesul de înregistrare începe în cadrul RA.

Responsabilitatea entității RA este de a colecta documentele și atestatele necesare pentru validarea ulterioară a identității și atributelor Subiectului / Beneficiarului.

Operatorul RA efectuează o primă verificare a documentelor și atestărilor și verifică dacă informațiile colectate sunt complete și corecte.

După verificarea completă a formularelor Subiectului / Beneficiarului, RA îl informează și pe Subiect / Beneficiar cu privire la drepturile și obligațiile sale.

RA este responsabilă de furnizarea și / sau verificarea informațiilor referitoare la atributele Beneficiarului / Subiectului (atribute profesionale, atribute organizaționale etc.). RA verifică și completează datele de înregistrare. RA este responsabilă de corectitudinea datelor care vor fi incluse în cererea de certificat trimisă la CA. RA este responsabilă de înregistrarea / înscrierea corectă a Subiecților și de furnizarea către CA a conținutului corect pentru câmpurile variabile din certificat.

4.2 Procesarea cererilor de certificate

certSIGN acceptă cereri înaintate individual sau colectiv. Cererile pot fi trimise *on-line* și *offline*.
certSIGN la adresa: https://www.certsign.ro. Un Beneficiar care vizitează site-ul respectiv completează (conform instrucţiunilor de pe site) un formular de cerere și îl trimite unei Autorități de Certificare. Cererile pentru certificate certSIGN Class 1 sunt procesate automat, în timp ce cererile de certificate de alte nivele sunt procesate manual.

Cererile de certificate SSL în format electronic pot fi transmise printr-un canal autentificat securizat, caz în care sunt procesate automat.

Cererea trimisă off-line se poate face:

- Prin prezentarea în persoană a Beneficiarului sau a reprezentantului autorizat al companiei la Autoritatea de Înregistrare sau la Autoritatea de Certificare, caz în care se completează și se semnează de mână a cererea, se semnează contractul cu privire

la prestarea serviciilor de certificare și se generează o parola cu ajutorul căreia Beneficiarul va putea face managementul certificatului sau se generează un cod PIN pentru accesul securizat la dispozitivul criptografic ce conține cheile și certificatele.

- Prin trimiterea prin poştă a cererii și a copiilor documentelor (conform prevederilor din Tabelul 3.2.3) necesare verificării identităţii solicitantului; verificarea este urmată de generarea unei parole cu ajutorul căreia Beneficiarul va putea face managementul certificatului, sau generarea unui cod PIN pentru accesul securizat la dispozitivul criptografic ce conține cheile și certificatele; dispozitivul criptografic este trimis înapoi solicitantului (codul PIN este trimis separat).

Trimiterile off-line privesc de asemenea cererile colective. Aceste cereri sunt confirmate de către un operator al Autorităţii de Certificare sau Înregistrare și procesate în grup.

Procesarea cererilor la Autoritatea de Inregistrare:

Fiecare cerere scrisă pe hârtie este procesată (procesarea trebuie făcută în prezenţa solicitantului dacă aşa este specificat în prezentul document) după cum urmează:

- operatorul Autorităţii de Înregistrare primeşte cererea Beneficiarului
- operatorul verifică datele din cerere, cum ar fi datele personale ale Beneficiarului (vezi procedura descrisă în Capitolul 3.2.3) și verifică existenţa dovezii posesiei cheii private (vezi Capitolul 3.2.1),
- ca urmare a verificării, operatorul confirmă identitatea dintre datele declarate și cele cuprinse în cerere; dacă cererea conține date neconforme este respinsă,
- cererea confirmată este trimisă la Autoritatea de Certificare,
- Autoritatea de Înregistrarea mai verifică și alte date care nu sunt specificate în cerere dar sunt necesare pentru emiterea certificatului.

Procesarea cererilor la Autoritatea de Certificare:

Autoritatea de Certificare verifică faptul că cererile au fost confirmate de către Autoritatea de Înregistrare autorizată.

RA verifică înregistrările CAA și urmează instrucțiunile de procesare găsite, pentru fiecare dNSName în extensia subjectAltName a certificatului care urmează a fi emis, conform specificațiilor RFC 6844 modificate prin Errata 5065 (Anexa A). certSIGN nu va emite un certificat decât dacă cererea de certificat este in concordanță cu setul de înregistrări CAA aplicabil.

Dacă există înregistrare, atunci trebuie sa includă și certSIGN ca Autoritate de certificare autorizată. Înregistrarea permisă este certsign.ro și înregistrările CAA „issue" sau „issuewild" sunt permise.

4.2.1 Îndeplinirea funcțiilor de identificare și autentificare

RA realizează identificarea și autentificarea în conformitate cu procedura definite în capitolul 3.2 și în documentația internă confidențială.

RA colectează și validează informațiile despre identitatea și despre atributele Beneficiarului și ale Beneficiarului.

Cererea de certificat cu risc ridicat este o cerere pe care CA o semnalează pentru control suplimentar prin referire la criteriile interne și bazele de date menținute de CA, care pot include nume cu risc mai mare de phishing sau alte utilizări frauduloase, nume cuprinse în cereri de certificate respinse anterior sau certificate revocate, nume listate pe lista de phishing-uri Miller Smiles sau pe lista de navigare sigură Google sau nume pe care CA le identifică folosindu-și propriile criterii de atenuare a riscului.

CA utilizează documentele și datele furnizate în secțiunea 3.2 pentru a verifica informațiile despre certificat, cu condiția ca CA să obțină datele sau documentul dintr-o sursă specificată în secțiunea 3.2 cu cel mult douăsprezece (12) luni înainte de emiterea certificatului.

CA dezvoltă, întreține și implementează proceduri documentate care identifică și necesită o activitate de verificare suplimentară pentru cererile de certificat cu risc ridicat înainte de aprobarea certificatului, după cum este necesar în mod rezonabil pentru a se asigura că astfel de cereri sunt verificate în mod corespunzător.

În cazul în care un terț delegat îndeplinește oricare dintre obligațiile care îi revin CA în temeiul prezentei secțiuni, CA verifică dacă procesul utilizat de către terțul delegat pentru a identifica și verifica în continuare cererile de certificate cu risc ridicat oferă cel puțin același nivel de asigurare ca și procesele proprii ale CA.

4.2.2 Aprobarea sau respingerea cererilor de certificate

certSIGN poate refuza emiterea unui certificat oricărui solicitant fără a-și asuma vreo obligaţie sau responsabilitate pentru posibilele daune sau pierderi pe care le poate suferi Beneficiarul ca urmare a acestui refuz. Autoritatea de Certificare va restitui solicitantului taxa de certificat (dacă acesta a plătit-o), cu excepţia cazului în care solicitantul a menţionat date false în cererea sa. Refuzul emiterii de certificat poate surveni în următoarele situaţii:

- dacă identificatorul Beneficiarului (ND) coincide cu identificatorul altui Beneficiar,
- dacă există suspiciune sau certitudine cu privire la falsificarea sau folosirea unor date false de către Beneficiar,
- dacă Beneficiarul, într-o manieră neconvenabilă, angajează resurse și mijloace de procesare ale certSIGN prin trimiterea unui număr de cereri în mod clar mai mare decât nevoile pe care le are acesta,
- din alte motive decât cele de mai sus.

Informaţiile privind decizia refuzului de emitere de certificat și motivele acesteia sunt trimise solicitantului. Solicitantul poate cere din nou emiterea unui certificat numai după ce motivele care au dus la refuzul emiterii au încetat.

Din când în când, certSIGN poate modifica cerințele referitoare la informațiile solicitate, pe baza cerințelor certSIGN, a contextului de afaceri al utilizării certificatelor sau după cum este cerut de lege.

După finalizarea cu succes a tuturor validărilor necesare ale unei cereri de certificat, certSIGN va aproba o cerere.

Dacă informațiile din cererea de certificat nu pot fi confirmate, atunci certSIGN va respinge cererea de certificat. certSIGN își rezervă dreptul de a respinge o cerere de certificat dacă, în propria sa apreciere, numele bun și de încredere al certSIGN poate fi pătat sau diminuat și poate face acest lucru fără a-și asuma răspunderea sau responsabilitatea pentru orice pierdere sau cheltuieli rezultate din acest refuz . certSIGN își rezervă dreptul de a nu divulga motivele unui astfel de refuz.

Solicitanții ale căror cereri au fost respinse pot reaplica ulterior.

4.2.3 Timpul de procesare a cererilor de certificate

certSIGN nu emite certificate imediat după înregistrare. Certificatele trebuie emise de Autoritatea de certificare; prin aprobarea cererii de certificat primite de la RA, prin urmare, certificatele nu sunt disponibile imediat Beneficiarului atunci când certificatele sunt create de CA.

Cererea de înregistrare și certificare sau de reînnoire (de chei sau certificate) va fi examinata, iar Autoritatea de Certificare va emite un certificat în intervalul de timp specificat în Tabelul 4.2.3. Aceste perioade depind în primul rând de acurateţea datelor trimise în cerere și de modul de cooperare dintre certSIGN și solicitant.

Nivelul de credibilitate al certificatului	Perioada de aşteptare
certSIGN Clasa 1	1 zi
certSIGN Clasa 2	5 zile
certSIGN Clasa 3	5 zile
certSIGN Clasa 4	5 zile

Tabelul 4.2.3. Perioada de aşteptare maximă pentru emiterea de certificate

În cazul în care datele necesare nu sunt puse la dispoziţia Autorităţii de Certificare în termen, sau este necesară o completare a documentaţiei, termenul de emitere a documentaţiei va fi prelungit.

4.3 Emiterea certificatelor

4.3.1 Acțiunile CA în timpul emiterii certificatelor

După primirea și procesarea unei cereri (vezi Capitolele 4.1 și 4.2), Autoritatea de Certificare emite un certificat.

Emiterea de certificate de către ROOT CA necesită ca o persoană autorizată de CA (de exemplu, operatorul sistemului CA, ofițerul de sistem sau administratorul ICP) să emită în mod deliberat o comandă directă pentru ca ROOT CA să efectueze o operațiune de semnare a certificatului.

Un certificat este considerat valid (în stare activă sau pregătit) în momentul acceptării lui de către Beneficiar (vezi Capitolul 4.4). Perioada de valabilitate a certificatelor emise depinde de tipul de certificat și de categoria Beneficiarului și sunt în conformitate cu perioadele prezentate în Tabelul 6.3.2.1

certSIGN a implementat propriul instrument de Linting pentru certificate, care utilizează și instrumente Linting externe, pentru a testa conformitatea tehnică a fiecărui artefact care urmează să fie semnat, înainte de a-l semna.

Fiecare certificat este emis on-line. Procedura de emitere este următoarea:

- cererea procesată este trimisă serverului de emitere de certificate,
- dacă cererea conține solicitarea generării unei perechi de chei, serverul cere generatorului hardware de chei acest lucru,
- se testează calitatea cheilor publice generate sau emise de Autoritatea de Certificare,
- dacă procedurile sunt încheiate cu succes, serverul emite un certificat și însărcinează modulul hardware de securitate cu semnarea certificatului; certificatul este stocat în baza de date a Autorităţii de Certificare,
- Autoritatea de Certificare pregăteşte răspunsul conţinând certificatul emis (dacă a fost emis) și îl trimite Beneficiarului; certificatul nu este publicat în Depozit până la primirea confirmării Beneficiarului cu privire la acceptarea certificatului (vezi Capitolul 4.4).

4.3.2 Notificarea Beneficiarului de către CA cu privire la emiterea certificatului

Autoritatea de Certificare certSIGN foloseşte o metodă de bază pentru anunţarea unui Beneficiar despre emiterea unui certificat:

- Când cheile sunt generate de certSIGN pe QSCD, QSCD-ul unde este stocat certificatul digital este livrat fie personal Subiectului, fie este trimis prin intermediul serviciilor poștale sau de curierat către Subiect. Datele de activare secretă (codul PIN) necesare pentru a accesa QSCD sunt trimise utilizând un plic securizat, ce permite identificarea încercarilor de acces neautorizat la conținutul său.

Fiecare certificat emis este publicat în Depozitul certSIGN. Publicarea certificatului este echivalenta cu notificarea altor Entităţi Partenere despre faptul că un certificat a fost emis pentru un Beneficiar. certSIGN publică un certificat în Depozitar după acceptarea certificatului de către Beneficiar.

4.4 Acceptarea certificatului

4.4.1 Conduita care constituie acceptarea certificatului

La primirea unui certificat, Beneficiarul se angajează să verifice conținutul acestuia, în special corectitudinea datelor și complementaritatea cheii publice cu cea privată pe care o deţine. Dacă certificatul are nereguli sau greşeli ce nu pot fi acceptate de Beneficiar, acesta din urmă va sesiza imediat Autoritatea de Certificare în vederea revocării certificatului.

Certificatul este considerat acceptat în ipoteza apariţiei unuia dintre următoarele evenimente în termen de maxim 7 zile calendaristice de la data primirii certificatului de către Beneficiar:

- acceptarea explicită a certificatului emis, la momentul ridicării certificatului de pe site-ul certSIGN
- primirea unui pachet înregistrat (trimis de certSIGN) conţinând certificatul

Dacă un certificat nu este respins în 7 zile calendaristice de la data primirii sale, certificatul este considerat acceptat.

Fiecare certificat acceptat este publicat în Depozitul certSIGN și este accesibil publicului. Acceptarea certificatului este o decizie unilaterală a Beneficiarului, anterior utilizării lui în

efectuarea oricărei operaţii criptografice, prin care se consideră că a acceptat termenii și condiţiile stipulate în prezentul Cod de Practici și Proceduri, Politica de Certificare și Contractul de prestări servicii de certificare. În cazul trimiterii electronice a cererii, solicitantul acceptă în mod automat certificatul la momentul cererii acestui certificat.

Prin acceptarea certificatului, Beneficiarul acceptă regulile Codului de Practici și Proceduri și a Politicii de Certificare și subscrie să respecte prevederile contractului încheiat cu certSIGN.

4.4.2 Publicarea certificatului de către CA

Vezi capitolul 2 - Publicare și responsabilități Depozitar.

4.4.3 Notificarea de către CA a altor entități cu privire la emiterea certificatului

certSIGN notifică alte entități cu privire la emiterea certificatului prin publicarea certificatului în Depozitar, așa cum este descris în capitolul 2.

4.5 Utilizarea perechii de chei și a certificatului

4.5.1 Utilizarea cheii publice și a certificatului Beneficiarului

Abonaţii trebuie să folosească cheia privată și certificatele:

- în concordanţă cu scopul lor declarat în prezentul Cod de Practici și Proceduri și în concordanţă cu conținutul certificatului (câmpurile *keyUsage* și *extendedKeyUsage*, vezi Capitolul 4.3),
- în concordanţă cu prevederile contractului dintre Beneficiar și certSIGN,
- numai în perioada de valabilitate (nu se aplică certificatelor pentru verificarea semnaturii digitale),

Când certificatul este suspendat, până la eventuala sa revocare, Beneficiarul nu poate folosi cheia privată pentru crearea unei semnaturi.

Entităţile Partenere, trebuie să folosească cheile publice și certificatele:

- în concordanţă cu scopul lor declarat în prezentul Cod de Practici și Proceduri și în concordanţă cu conținutul certificatului (câmpurile *keyUsage* și *extendedKeyUsage,* vezi Capitolul 4.3),
- în concordanţă cu prevederile contractului dintre Beneficiar și certSIGN,
- numai după verificarea stării acestora (vezi Capitolul 4.8) și verificarea semnaturii Autorităţii de Certificare care a emis acel certificat.

4.5.2 Utilizarea cheii publice și a certificatului de Entități Partenere

certSIGN presupune că toate aplicațiile software sunt conforme cu standardul X.509, protocolul SSL/TLS, și alte standarde aplicabile ce impun cerințele și seturile de cerințe menționate în acest CPP. certSIGN nu garantează că soft-ul oricărei entități partenere va suporta sau impune asemenea controale și cerințe, și toate entitățile partenere sunt sfătuite să identifice suport tehnic și legal adecvat.

Părțile care se bazează pe un certificat verifică în orice moment o semnătură digitală prin verificarea valabilității unui certificat digital cu ajutorul serviciului OCSP la adresa http://ocsp.certsign.ro sau a CRL relevante publicate de certSIGN.

Entitățile partenere sunt avertizate că o semnătură digitală neverificată nu poate fi atribuită ca semnătură valabilă a Beneficiarului.

Decizia finală privind posibilitatea de a avea încredere sau nu într-o semnătură digitală verificată este exclusiv a părții de încredere. Acordarea încrederii unei semnături digitale ar trebui să aibă loc numai dacă:

- Semnătura digitală a fost creată în perioada de funcționare a unui certificat valid și poate fi verificată prin trimiterea la un certificat validat.
- Entitatea Parteneră a verificat statutul de revocare al certificatului prin trimiterea la CRL relevante și certificatul nu a fost revocat.
- Entitatea Parteneră înțelege că un certificat digital este emis unui beneficiar pentru un anumit scop și că cheia privată asociată cu certificatul digital poate fi utilizată numai în conformitate cu uzanțele specificate în acest CPP și conținute în certificat.

Încrederea în certificat este acceptată ca fiind rezonabilă daca sunt îndeplinite condițiile prevăzute în CPP și în cadrul contractului încheiat cu Entitatea parteneră. În cazul în care nu sunt îndeplinite asigurările furnizate de certSIGN în conformitate cu prevederile prezentului CPP, entitatea parteneră trebuie să obțină asigurări suplimentare.

Garanțiile sunt valabile numai dacă s-au efectuat pașii detaliați mai sus.

Încrederea într-o semnătură digitală care nu poate fi verificată, poate să ducă la riscuri pe care entitatea parteneră și le asumă în întregime și pe care certSIGN nu și le asumă în niciun fel.

4.6 Reînnoirea certificatului

Un Beneficiar sau o Autoritate de Certificare foloseşte reînnoirea dacă deţine deja un certificat și o cheie privată asociată acestuia și doreşte să continue să folosească aceeaşi pereche de chei. Noul certificat, creat ca rezultat al înnoirii, constă în aceeaşi cheie publică, acelaşi nume și restul informaţiilor care se preiau din certificatul anterior, dar perioada de valabilitate, numărul serial și semnatura emitentului sunt diferite faţă de datele din certificatul anterior.

Reînnoirea se aplică numai certificatelor emise de certSIGN a căror perioadă de validitate nu a expirat, nu au fost revocate și informaţiile conţinute de acestea sunt intacte.

Fiecare cerere semnată de reînnoire este procesată în mod off-line, adică necesită acceptarea manuală a operatorului Autorităţii de Certificare.

4.6.1 Circumstanțe pentru reînnoirea certificatului

Fără stipulare.

4.6.2 Cine poate solicita reînnoirea

Fără stipulare.

4.6.3 Procesarea cererilor de reînnoire a certificatului

Fără stipulare.

4.6.4 Notificarea emiterii de certificate noi către beneficiar

Fără stipulare.

4.6.5 Conduita care constituie acceptarea unui certificat de reînnoire

Fără stipulare.

4.6.6 Publicarea certificatului de reînnoire de către CA
Fără stipulare.

4.6.7 Notificarea emiterii certificatului de către CA către alte entități
Fără stipulare.

4.7 Procesul de Re-key pentru certificat

4.7.1 Situațiile în care se poate face re-key
Pentru a păstra continuitatea certificatului, înainte de expirarea sa, utilizatorul trebuie să solicite un nou certificat. Noul certificat poate conține aceeaşi cheie (reînnoire – vezi capitolul anterior) daca se respecta conditia ca durata de viaţă a cheilor să nu depăşească o durată de două ori mai mare decât durata maximă de viaţă a unui certificat. In caz contrar se va emite un nou certificat

4.7.2 Cine poate solicita certificarea unei noi chei publice
certSIGN informează întotdeauna Subiecții (cu cel puțin 30 de zile înainte) despre apropierea perioadei de expirare.
Re-Key-ul este realizat numai la cererea Beneficiarului și trebuie precedat de înaintarea unei cereri pe formular corespunzător, completată de Beneficiar.

Cererile trebuie să fie confirmate în situaţia în care operatorul Autorităţii de Înregistrare solicită acest lucru.

4.7.3 Procesarea cererilor de re-key a certificatelor
Procedura pentru procesarea cererii de re-key este echivalenta procedurilor de procesare a cererilor de certificate descrise în Capitolul 4.2 și procedurilor de emitere de certificate descrise în Capitolul 4.3.

4.7.4 Notificarea emiterii noului certificat către Beneficiar
RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.7.5 Conduita care constituie acceptarea certificatului
RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.7.6 Publicarea certificatului rezultat dupa re-key de către CA
RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.7.7 Notificarea eliberării certificatului de către CA altor entități
RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.8 Modificarea Certificatului
Modificarea certificatului se referă la crearea unui nou certificat pe baza certificatului deţinut în prezent de Beneficiar. Un nou certificat are o cheie publică diferită, un nou număr serial, dar diferă prin cel puţin un câmp (prin conţinut sau prin apariţia unui câmp complet nou) faţă de certificatul pe baza căruia este emis. Modificarea poate fi necesară, de exemplu, în cazul schimbării poziţiei în cadrul companiei sau al schimbării numelui, cu condiţia ca aceste date să fi fost menţionate iniţial în certificat, sau dacă trebuie adăugate. Dacă datele, verificate pe baza unor documente în concordanţă cu procedurile de autentificare ale Beneficiarului au fost modificate, fiecare cerere trebuie confirmată de Autoritatea de Înregistrare (vezi Capitolul

4.8). Pot fi modificate numai certificatele valide care nu au fost revocate și al căror nume al Beneficiarului și alte caracteristici nu au fost schimbate.

4.8.1 Circumstanța pentru modificarea certificatului
Fără stipulare.
4.8.2 Cine poate solicita modificarea certificatului
Fără stipulare.
4.8.3 Procesarea cererilor de modificare a certificatului
Fără stipulare.
4.8.4 Notificarea emiterii de certificate modificate către beneficiar
Fără stipulare.
4.8.5 Conduită care constituie acceptarea certificatului modificat
Fără stipulare.
4.8.6 Publicarea certificatului modificat de către CA
Fără stipulare.
4.8.7 Notificarea eliberării certificatului modificat de către CA către alte entități
Fără stipulare.

4.9 Revocarea și Suspendarea Certificatului
Revocarea unui certificat are o influenţă semnificativă asupra utilizării acestuia și asupra obligaţiilor unui Beneficiar care deţine un astfel de certificat. Imediat după după revocarea certificatului unui Beneficiar, certificatul trebuie considerat invalid (în stare de revocare). Similar, în cazul certificatului Autorităţii de Certificare – anularea validităţii unui certificat de acest tip semnifică retragerea drepturilor de emitere de certificate pentru proprietarul său și revocarea tuturor certificatelor emise de aceasta.

Revocarea nu afectează tranzacţiile făcute înainte de revocare și nici obligaţiile care rezultă din respectarea prezentului Cod de Practici și Proceduri.

Acest capitol specifică condiţiile necesare pentru ca o Autoritate de Certificare să aibă motive de revocare a certificatului.

Supendarea unui certificat reprezinta o revocare reversibila, deci poate fi considerata o revocare temporara.

Dacă o cheie privată, care corespunde unei chei publice, conţinută într-un certificat revocat, rămâne sub controlul Beneficiarului, după revocare ar trebui stocata în siguranţă, până este distrusă fizic.

4.9.1 Circumstanțele revocării unui certificat
Un exemplu de caz în care se revoca certificatul unui Beneficiar este pierderea controlului (sau existenţa suspiciunii acestui lucru) asupra cheii private deţinută de Beneficiar sau încălcarea de către Beneficiar a obligaţiilor/cerinţelor cuprinse în Politica de Certificare, contractului încheiat cu Autoritatea de Certificare sau Codului de Practici și Proceduri.

4.9.1.1 Motive pentru revocarea unui certificat de Entitate finală

certSIGN va revoca un certificat în termen de 24 de ore și va completa motivul corespunzător de revocare în CRLReason (vezi cap.7.2.2) dacă apare una sau mai multe din următoarele situații:

1. Beneficiarul solicită în scris, fără a preciza un motiv, ca CA să revoce un certificat (CRLReason "nespecificat (0)", ceea ce înseamnă că nu se adaugă niciun reasonCode în CRL);
2. Beneficiarul notifică CA că cererea inițială de certificat nu a fost autorizată și nu acordă retroactiv autorizația (CRLReason #9, privilegeWithdrawn);
3. CA obține dovezi că cheia privată a Beneficiarului care corespunde cheii publice din certificat a suferit o compromitere a cheii (CRLReason #1, keyCompromise);
4. CA are cunoștință de o metodă demonstrată sau dovedită care poate calcula cu ușurință cheia de securitate privată a abonaților pe baza cheii publice din certificat (cum ar fi o metodă de calcul a cheii private Debian slabă, a se vedea https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompropromise);
5. CA obține dovezi că validarea autorizării sau controlului domeniului pentru orice nume de domeniu complet calificat sau adresă IP din certificat nu ar trebui să se bazeze pe aceasta (CRLReason #4, supersededed).

certSIGN va revoca un certificate in maximum 5 zile și va completa motivul corespunzător de revocare în CRLReason (vezi cap.7.2.2) în următoarele situații:

6. Certificatul nu mai respectă cerințele din secțiunea 6.1.5 și secțiunea 6.1.6 din CABF BR (CRLReason #4, înlocuit);
7. CA obține dovezi că certificatul a fost utilizat în mod abuziv (CRLReason #9, privilegeWithdrawn);
8. CA este informată că un abonat a încălcat una sau mai multe obligații materiale ale acestuia în temeiul acordului de abonat sau al condițiilor de utilizare (CRLReason #9, privilegeWithdrawn);
9. CA este informată de orice circumstanță care indică faptul că utilizarea unui nume de domeniu sau a unei adrese IP complet calificate în certificat nu mai este permisă din punct de vedere legal (de exemplu, o instanță sau un arbitru a revocat dreptul unui solicitant de înregistrare a numelui de domeniu de a utiliza numele de domeniu, un acord de licență sau de servicii relevant între solicitantul și solicitantul de înregistrare a numelui de domeniu a încetat sau solicitantul de înregistrare a numelui de domeniu nu a reînnoit numele de domeniu) (CRLReason #5, cessationOfOperation);
10. CA este informată că un certificat Wildcard a fost utilizat pentru a autentifica un nume de domeniu complet calificat subordonat care induce în eroare în mod fraudulos (CRLReason #9, privilegeWithdrawn);
11. CA este informată despre o modificare semnificativă a informațiilor conținute în certificat (CRLReason #9, privilegeWithdrawn);
12. CA este informată că certificatul nu a fost eliberat în conformitate cu aceste cerințe sau cu CA/Browser Forum Baseline Requirements (CRLReasonReason, #4, supersededed);
13. CA stabilește sau ia cunoștință de faptul că oricare dintre informațiile care apar în certificat este inexactă (CRLReason #9, privilegeWithdrawn);
14. Dreptul CA de a elibera certificate în temeiul prezentelor cerințe expiră sau este revocat sau încetat, cu excepția cazului în care CA a luat măsuri pentru a continua să mențină depozitul CRL/OCSP [CRLReason "unspecified (0)", ceea ce are ca rezultat faptul că în CRL nu este furnizată o extensie a codului de motiv (reasonCode)];

15. Revocarea este impusă de practicile de certificare ale certSIGN (CPP) pentru un motiv care nu este altfel necesar să fie specificat în prezenta secțiune [CRLReason "unspecified (0)", ceea ce are ca rezultat faptul că în CRL nu este furnizată o extensie reasonCode; sau
16. CA are cunoștință de o metodă demonstrată sau dovedită care expune cheia privată a Beneficiarului la compromitere sau dacă există dovezi clare că metoda specifică utilizată pentru a genera cheia privată a fost defectuoasă (CRLReason #1, keyCompromise).

4.9.1.2 Motive pentru revocarea unui certificat de CA Subordonat

CA-ul emitent, certSIGN ROOT CA, va revoca certificatul unui CA Subordonat în maxim șapte (7) zile dacă unul sau mai multe dintre următoarele motive apar:

1. CA-ul Subordonat solicită revocarea în scris;
2. CA-ul Subordonat notifică CA-ul emitent că cererea originală pentru emitere de certificat nu a fost autorizată, și nu se asigură o autorizare retroactivă;
3. CA-ul emitent obține dovezi că Cheia Privată a CA-ului Subordonat care corespunde cheii publice din certificat a fost compromisă și/sau nu mai este conformă cu cerințele CABF BR din secțiunile 6.1.5 și 6.1.6;
4. CA-ul emitent obține dovezi că certificatul a fost folosit greșit;
5. CA-ul emitent a descoperit că Certificatul nu a fost emis, sau CA-ul Subordonat nu s-a conformat cu cerințele din acest document sau din documentele de politici sau proceduri aplicabile;
6. CA-ul emitent descoperă că informații care apar în certificat sunt incorecte sau inadecvate;
7. CA-ul emitent sau CA-ul subordonat își încetează operațiile din orice motiv, și nu au arajamente cu alte CA-uri pentru a oferi suport de revocare a certificatelor;
8. Dreptul de a emite certificate conform cu cerințele din BR, de către CA-ul emitent sau CA-urile subordonate, expiră, sunt revocate sau terminate, cu excepția situației în care CA-ul emitent are aranjamente de continuare a depozitarului pentru OCSP/CRL;
9. Revocarea este cerută de politica sau CPP-ul CA-ului emitent.

În orice alte situații în care Beneficiarul nu respectă prezentul CPP, Acordul contractual, Termenii și conditiile, sau alte acorduri încheiate între părți cu privire la serviciile furnizate de certSIGN CA.

Cheie privată compromisă înseamnă:
(1) accesul neautorizat la cheia privată sau un motiv întemeiat pe baza căruia să se suspecteze acest acces,
(2) pierderea cheii private sau apariţia unui motiv de a suspecta o astfel de pierdere,
(3) furtul cheii private sau apariţia unui motiv de a suspecta un astfel de furt,
(4) ştergerea accidentală a cheii private.
Cererea de revocare poate fi trimisă prin intermediul Autorităţii de Înregistrare (aceasta implică contactarea autorităţii de către Beneficiar), sau direct unei Autorități de Certificare (cererea poate fi autentificată prin semnatura) Cererea de revocare trebuie să conţină informaţii care să permită autentificarea sigură a Beneficiarului de către Autoritatea de Înregistrare. Dacă autentificarea identităţii Beneficiarului nu se realizează cu succes, Autoritatea de Certificare respinge cererea de revocare și suspendă certificatul până când cererea de revocare va fi examinată în detaliu.

Certificatele pe termen scurt nu se revocă.

4.9.2 Cine poate solicita revocarea certificatelor

Următoarele entităţi pot trimite cereri de revocare a certificatului unui Beneficiar:

- Beneficiarul, care este proprietarul certificatului,
- un reprezentant autorizat al Autorităţii de Certificare (în cazul certSIGN acest rol este rezervat administratorului de securitate),
- un repezentant al Beneficiarului, de exemplu angajatorul sau; Beneficiarul trebuie imediat informat despre acest lucru,
- Autoritatea de Înregistrare care poate cere revocarea în numele unui Beneficiar, sau în nume propriu, dacă are informaţii care justifică revocarea certificatului.

Autoritatea de Înregistrare trebuie să acţioneze cu multă precauţie când procesează cereri ce nu au fost trimise de către un Beneficiar și să accepte numai acele cereri în conformitate cu acest document.

Când partea care cere revocarea certificatului nu este proprietarul certificatului (Beneficiarul), Autoritatea de Certificare trebuie:

- să verifice faptul ca respectiva parte are dreptul să emita o astfel de cerere
- sa ceara o justificare a respectivei cereri
- să trimită o notificare Beneficiarului despre revocare, sau despre iniţierea procesului de revocare.

Fiecare cerere trebuie trimisă:

- direct Autorităţii de Certificare sub formă electronica, cu sau fără confirmarea Autorităţii de Înregistrare,
- direct sau indirect (prin intermediul Autorităţii de Înregistrare) la Autoritatea de Certificare, sub formă ne-electronica (document pe hârtie, fax, telefon etc.)

Cererea de revocare poate viza mai multe certificate.

4.9.3 Procedura de revocare a certificatelor

Cererea de revocare a certificatului se poate transmite în următoarele moduri:

- prima metodă se bazează pe trimiterea unei cereri de revocare în format electronic, autorizată printr-o parolă, către o Autoritate de Certificare; o astfel de revocare poate fi iniţiată numai la cererea Beneficiarului
- a doua metodă necesită trimiterea unei cereri electronice de revocare către certSIGN, confirmată (prin semnatura electronica) de Autoritatea de Înregistrare; această metodă se aplică în situaţiile în care (a) Beneficiarul a pierdut cheia sa privată sau parola ei, sau cheia privată a fost furată sau (b) cererea de revocare a fost trimisă de reprezentantul Beneficiarului, un reprezentant autorizat al unei Autorități de Certificare sau al Autorităţii de Înregistrare, cu condiţia de a exista suficiente motive pentru a cere o astfel de revocare;

- a treia metodă implică trimiterea unei cereri ne-electronice autentificate (document pe hârtie, fax, telefon etc.) către certSIGN; autentificarea unui document pe hârtie (inclusiv faxul) poate fi efectuată la Autoritatea de Înregistrare, de exemplu cu o ştampilă şi o semnatura de mână a unei persoane recunoscute de certSIGN, sau prin plasarea unei parole în cadrul documentului, parola cunoscută doar de persoana care cere revocarea; o cerere făcută prin telefon este îndeplinită numai după ce se trimite şi parola; după verificarea cu succes a cererii, Autoritatea de Înregistrare pregăteşte confirmarea electronica a cererii de revocare şi o înaintează Autorităţii de Certificare.

Informaţiile despre certificatele revocate sau suspendate sunt plasate în Lista de certificate Revocate (vezi Capitolul 7.2), emisă de Autoritatea de Certificare. Autoritatea de Certificare notifică entitatea care cere revocarea certificatului despre această revocare, sau despre decizia de a anula cererea, împreună cu motivele anulării.

Fiecare cerere de revocare de certificat trebuie să ofere mijloace de identificare indubitabilă a certificatului de revocat, să conţină motivele pentru care se cere revocarea, conform cap. 7.2, şi trebuie să fie autentificată, conform cap. 3.4.

Procedura de revocare a unui certificat se desfăşoară astfel:

- Autoritatea de Certificare, ca urmare a primirii unei cereri de revocare certificat, o verifica; dacă cererea este făcută electronic, Autoritatea de Certificare verifică corectitudinea certificatului de revocat şi (opţional) corectitudinea certificatului ataşat cererii; cererea făcută pe hârtie necesită autorizarea solicitantului; o astfel de confirmare poate fi obţinută prin telefon, fax, sau în timp ce Beneficiarului vizitează personal un reprezentant autorizat al Autorităţii de Certificare (sau invers);
- dacă cererea este verificată cu succes, Autoritatea de Certificare plasează informaţiile despre revocarea certificatului în Lista certificatelor Revocate (CRL), împreună cu informaţii privind motivele de revocare (vezi Capitolul 7.2);
- Autoritatea de Certificare notifică, electronic sau prin poşta, entitatea care cere revocarea despre revocare sau decizia de anulare a cererii împreună cu motivele anulării.
- în plus, dacă partea care cere revocarea nu este Beneficiarul, Autoritatea de Certificare trebuie să notifice Beneficiarul în privinţa revocării certificatului, sau iniţierii procesului de revocare.

Dacă un certificat, sau o cheie privată corespunzătoare unui certificat de revocat au fost stocate pe un dispozitiv criptografic, ca urmare a revocării certificatului, dispozitivul criptografic trebuie distrus fizic sau şters în codiţii de maximă securitate. Această operaţie se îndeplineşte de către posesorul dispozitivului criptografic – o persoană fizică sau juridică (un reprezentant al unei astfel de entităţi). Deţinătorul dispozitivului criptografic trebuie să-l păstreze astfel încât să prevină furtul sau utilizarea neautorizată a sa până la distrugerea fizică sau la ştergerea cheii private.

4.9.3.1 Procedura de raportare a problemelor certificatelor

Din cauza unor erori, limitari tehnice, procedurale sau din alte motive, pot exista certificate emise de catre certSIGN intr-un mod necorespunzator (de exemplu, certificatul emis contine infomatii eronate despre despre titular sau organizatie). De asemenea, pot aparea situatii in

care un certificat nu este folosit in mod corespunzator (de exemplu, in activitati infractionale). Daca Beneficiarii sau entitatile care isi bazeaza comportamentul pe serviciile de certificare oferite de catre certSIGN sau alte terte parti intalnesc astfel de situatii, daca suspecteaza compromiterea unei chei sau alte tipuri de fraude, folosirea necorespunzatoare a unui certificat sau un comportament necorespunzator legat de certificate emise de catre certSIGN, pot sesiza aceste cazuri la adresa **revokecsgn@certsign.ro**, informand Autoritatea de Certificare despre motive rezonabile de revocarea a acestor certificate. Autoritatea de Certificarea trebuie sa inceapa investigarea unui raport de certificat cu probleme in maximum 24 de ore de la primirea sa si sa decida daca revocarea sau alte actiuni corespunzatoare sunt necesare, bazat cel putin pe următoarele motive:

1. Natura presupusei probleme;
2. Numarul de rapoarte de certificate cu probleme primite referitor la un anumit certificat sau un anumit Beneficiar;
3. Entitatea care raporteaza (de exemplu, o plangere de la un angajat al unei autorități de aplicare a legii referitoare la faptul ca un site web este implicat in activitati ilegale ar trebui sa cantareasca mai mult decat o plangere de la un client care sustine ca nu a primit produsele comandate)
4. Legislatia relevanta.

Autoritatea de Certificare certSIGN poate raspunde 24x7 la un raport al unui certificat cu probleme de mare prioritate si, acolo unde este cazul, poate trimite mai departe plangerea catre autoritatile de aplicare a legii si revoca certificatul care este referit in plangere.
Sesizarile referitoare la certificate cu probleme se pot face la adresa **revokecsgn@certsign.ro**

4.9.4 Perioada de grație a cererii de revocare

certSIGN efectuează revocarea in mai putin de 24 de ore, pentru a se asigura că timpul necesar pentru procesarea cererii de revocare și pentru publicarea notificării de revocare (CRL actualizat) este cât mai mic posibil.

4.9.5 Timpul în care CA trebuie să proceseze cererea de revocare

certSIGN garantează următoarea perioadă maximă pentru procesarea unei cereri de revocare certificat,

- trimisă electronic (în formatul corect) sau prin telefon,
- trimisă sub formă de document din hârtie,

după cum este descris în Tabelul 4.9.4.

Politica de certificare	Perioada de graţie admisibilă
certSIGN Clasa 1	Fără obligaţie de revocare
certSIGN Clasa 2	în 24 de ore
certSIGN Clasa 3	în 24 de ore
certSIGN Clasa 4	în 24 de ore

Tabel 4.9.6. Perioada maximă de procesare a cererii de revocare de certificat

CA decide dacă revocarea sau altă acțiune corespunzătoare este justificată pe baza a cel puțin următoarelor criterii:

1. Natura presupusei probleme;
2. Consecințele revocării (impact direct și colateral asupra abonaților și părților);
3. Numărul de rapoarte privind problemele de certificat primite în legătură cu un anumit certificat sau cu un Beneficiar;
4. Entitatea care face plângerea (de exemplu, o plângere din partea unui ofițer de aplicare a legii că un site Web este implicat în activități ilegale va avea mai multă pondere decât o plângere din partea unui consumator care susține că nu a primit bunurile pe care le-a comandat); și
5. Legislația relevantă.

Informaţiile despre revocarea de certificat sunt stocate în baza de date a certSIGN. Certificatele revocate sunt plasate în Lista Certificatelor Revocate (CRL) în concordanţă cu perioadele de publicare a CRL.

În momentul revocării certificatului, operatorii Autorității de Înregistrare și Beneficiarul implicați sunt informați automat despre această revocare. Informații despre starea actuală a certificatului sunt disponibile prin intermediul serviciului de verificare a stării certificatului imediat după perioada de grație declarată. Acest serviciu poate fi solicitat, de exemplu, de o parte invocată care verifică disponibilitatea unei semnături electronice aplicată unui document primit de la Beneficiar.

4.9.6 Verificarea cerințelor de revocare de către Entitățile Partenere

certSIGN oferă în timp real serviciul de verificare a stării certificatelor. Acest serviciu este realizat pe baza protocolului OCSP descris în RFC 6960. Utilizând OCSP este posibil să obținem date mai exacte (în raport cu folosirea exclusiv a CRL-ului) privind starea unui certificat.

Funcțiile OCSP se bazează pe modelul cerere-răspuns. Ca răspuns la o cerere, serverul OCSP furnizează următoarele informații despre starea unui certificat:

- *Bun* (good) – este un răspuns pozitiv la o cerere care trebuie interpretat ca o confirmare a validității certificatului;
- *Revocat (revoked)* – înseamnă că certificatul a fost revocat;
- *Necunoscut (unknown)* – înseamnă că certificatul nu a fost emis de o Autoritate de Certificare afiliată.

Serviciul OCSP este disponibil pentru orice Beneficiar sau Entitate Parteneră care a semnat un contract cu certSIGN referitor la oferirea acestor servicii.

Starea certificatului este furnizată în timp real (imediat după revocarea certificatului) bazat pe informațiile din bazele de date certSIGN și conține informații mai noi decât cele publicate în CRL.

O entitate parteneră nu este obligată să verifice on-line starea certificatului bazată pe serviciul menționat anterior. Totuși, este recomandată utilizarea serviciului OCSP când riscul de falsificare a documentelor electronice folosind semnătură electronicaă este mai mare, sau dacă aceasta este solicitată de alte regulamente pentru aceste situații.

4.9.7 Frecvența de emitere a CRL-urilor

Fiecare Autoritate de Certificare care face parte din certSIGN emite diferite Liste de Revocare de certificat. Un nou CRL complet este publicat în Depozitar imediat după fiecare revocare de

certificat, sau într-un interval de maxim o zi. Perioada de valabilitate a CRL-ului este de 48 de ore si se actualizeaza zilnic.

Lista de certificate Revocate (CRL) pentru autoritatea certSIGN ROOT CA este emisă cel puţin în fiecare an cu condiţia să nu existe nici o revocare de certificat a uneia dintre autorităţile afiliate la certSIGN CA.

În cazul revocării certificatului unei autorități afiliate la certSIGN acest certificat este imediat publicat în Lista de certificate Revocate.

certSIGN ROOT CA continuă să emită CRL-uri până când una dintre următoarele situații este adevărată:
- toate certificatele CA subordonate care conțin aceeași cheie publică a subiectului sunt expirate sau revocate; SAU
- cheia privată a CA subordonate corespunzătoare este distrusă.

4.9.8 Latența maximă pentru CRL-uri

CRL-ul acestei CA și ale tuturor CA-urilor emitente subordonate este emis în conformitate cu capitolul 4.9.7 și publicate fără întârziere.

4.9.9 Disponibilitatea verificării on-line a revocării/stării

Răspunsurile OCSP sunt semnate de un Responsabil OCSP al cărui certificat este semnat de CA care a emis certificatul a cărui stare de revocare este verificată.
Certificatul de semnătură OCSP conține o extensie de tipul id-pkix-ocsp-nocheck, așa cum este definită de RFC6960.
CA administreaza o capacitate OCSP utilizând metoda GET pentru certificatele emise în conformitate cu cerințele curente ale Forumului CA / Basline Requirements.

Pentru statutul certificatelor de Beneficiar, CA actualizează informațiile furnizate printr-un protocol de stare online a certificatelor cel puțin o dată pe ora. Răspunsurile OCSP din partea acestui serviciu au un termen maxim de expirare de 24 ore.

Pentru starea certificatelor de CA Intermediare:

CA actualizează informațiile furnizate printr-un protocol de certificat online cel puțin:

(i) La fiecare 12 luni și
(ii) În termen de 24 de ore dupa revocarea certificatului de CA Intermediar.

Dacă răspunsul OCSP primește o cerere de status a unui certificat care nu a fost emis, atunci atunci Responderul nu răspunde cu starea „bună” pentru astfel de certificate. certSIGN monitorizează responderul OCSP pentru cererile de numere de serie „neutilizate” ca parte a procedurilor sale de răspuns de securitate.

Responderul OCSP furnizează răspunsuri definitive despre numerele de serie ale certificatului „rezervat”, ca și cum ar exista un certificat corespunzător care se potrivește cu pre-certificatul [RFC6962].

Seria de certificat în cadrul unei cereri OCSP poate fi una din următoarele trei opțiuni:

1. „atribuit” dacă un certificat cu acea serie a fost emis de CA emitent, folosind orice cheie curentă sau anterioară asociată subiectului CA; sau

2. „rezervat” dacă un pre-certificat [RFC6962] cu acea serie a fost emis de (a) CA emitent; sau (b) un pre-certificat de semnare [RFC6962] asociat cu CA emitent;
3. „neutilizat” dacă niciuna din contițiile de mai sus nu sunt îndeplinite.espondentul nu răspunde cu o stare "bună" pentru aceste certificate.

4.9.10 Cerințe pentru verificarea revocării on-line
Fara cerinte.

4.9.11Alte forme disponibile pentru anunțarea revocării
Alte forme pentru anuntarea revocarii sunt descrise in cap. 4.9.3

4.9.12 Cerințe speciale în cazul compromiterii re key
Dacă un Beneficiar cunoaște sau suspectează că integritatea cheii private a certificatului său a fost compromisă, Beneficiarul trebuie să:

- Înceteze imediat utilizarea certificatului,
- Inițieze imediat revocarea certificatului,
- Șteargă certificatul de pe toate dispozitivele și sistemele,
- Informeze toate părțile terțe care pot depinde de acest certificat.

Compromiterea cheii private poate avea implicații asupra informațiilor protejate cu această cheie. Beneficiarul decide cum să se ocupe de informațiile afectate înainte de a șterge cheia compromisă.
Metode acceptabile pe care terții le pot utiliza pentru a demonstra compromisul cheii private:
1. Utilizează procedura descrisă în secțiunea 7.6 din RFC 8555 și semnează cererea de revocare cu cheia privată compromisă.
2. Semnează un text oferit de certSIGN folosind cheia privată compromisă.
3. Trimiterea cheii private.

4.9.13Circumstanțe pentru suspendare
N/A

4.9.14Cine poate solicita suspendarea
N/A

4.9.15Procedura de solicitare a suspendării
N/A

4.9.16Limitări ale perioadei de suspendare
N/A

4.10 Servicii privind starea certificatelor

4.10.1Caracteristici operaționale
Serviciile certSIGN de verificare a stării certificatelor sunt CRL și OCSP. Accesul la aceste servicii se realizează prin intermediul site-urilor web “www.certsign.ro” și “ocsp.certsign.ro”. Serviciile de verificare a stării certificatelor oferă informații despre starea certificatelor valide.

Integritatea și autenticitatea informațiilor despre starea lor este protejată prin semnătura electronică a CA-ului respectiv.

Intrările de revocare la un răspuns CRL sau OCSP nu vor fi eliminate decât după data de expirare a Certificatului revocat.

4.10.2 Disponibilitatea serviciului

Serviciile de stare a certificatului sunt disponibile 24 de ore pe zi, 7 zile pe săptămână.

CA menține o capacitate continuă de 24x7 de a răspunde intern la un raport privind problemele de certificare cu prioritate ridicată și, după caz, transmite o astfel de plângere autorităților de aplicare a legii și / sau revocă un certificat care face obiectul unei astfel de plângeri.

4.10.3 Elemente opționale

Serviciile certSIGN de verificare a stării certificatelor nu includ sau nu necesită elemente suplimentare.

4.11 Încetarea abonamentului

Sfârșitul abonamentului apare după:

- Revocarea cu succes a ultimului certificat al unui Beneficiar,
- Expirarea ultimului certificat al unui Beneficiar

Din motive de respectare a legii, certSIGN și toate autoritățile de înregistrare păstrează toate datele și documentația pentru o perioadă de 10 ani de la încheierea abonamentului.

4.12 Custodie și recuperare chei

Autoritățile de Certificare care operează în cadrul certSIGN creează o copie de siguranţă a propriilor chei private. Copiile sunt folosite în cazul punerii în aplicare a procedurilor standard, sau de urgenţă (de exemplu, după dezastru) de recuperare a cheii. Copiile cheilor private sunt protejate prin secrete partajate.

certSIGN nu păstrează copii ale cheilor private ale operatorilor Autorităţii de Certificare. Copiile cheilor private ale Abonaților sunt create numai la cererea Beneficiarului și în conformitate cu metodele prezentate în 6.2.3.

"Copiile cheilor private de criptare ale utilizatorilor sunt pastrate criptat in baza de date a Autoritatilor de Certificare.

Astfel, fiecare cheie privata a utilizatorului este criptata simetric cu o cheie de sesiune. Cheile de sesiune sunt criptate cu o cheie master de decriptare. Accesul la aceasta cheie de decriptare se face prin secrete partajate, pe principiul K din N. Cheile private de semnare ale utilizatorilor nu sunt salvate."

4.12.1 Politica și practicile esențiale pentru custodie și recuperare

Fără stipulare.

4.12.2 Politica și practicile privind încapsularea și recuperarea cheilor de sesiune

Fără stipulare.

5 Facilități, Management și Controale Operaționale

Acest capitol descrie cerințele generale privind controlul, securitatea fizică și organizațională, precum și activitatea personalului, utilizate în certSIGN de exemplu în timpul generării cheii, verificării autenticității entității, emiterea și publicarea certificatelor, revocarea certificatului, audit și crearea copiilor de rezervă.

În calitate de furnizor de servicii certificare, certSIGN pune securitatea în centrul activităților sale. Pentru ca toate activele, activitățile și serviciile sale să fie sigure, certSIGN a implementat, menține și îmbunătățește continuu un sistem informatic de management al securității certificat ISO 27001:2013. În acord cu cerințele acestui cadru de securitate, toate activitățile de securitate încep cu o evaluare a riscului, pentru a identifica și clasifica toate activele informaționale, pentru a evalua riscurile la care sunt expuse și pentru a determina controalele tehnice, manageriale, organizatorice și procedurale necesare. certSIGN menține un inventar al tuturor activelor informaționale și le atribuie o clasificare în concordanță cu evaluarea riscurilor.

Toate acele controale aferente activelor și activităților CA și RA sunt conforme cu cerințele aplicabile din ultima versiune a următoarelor standarde:

- ETSI EN 319 401, Cerințele generale privind politicile Furnizorilor de Servicii de Încredere,
- ETSI EN 319 411-1, Politica și cerințele de securitate pentru Furnizorii de Servicii de Încredere care emit certificate; Partea 1: Cerințe generale,
- ETSI EN 319 411-2, Politica și cerințele de securitate pentru Furnizorii de Servicii de Încredere care emit certificate; Partea 2: Cerințe pentru Furnizorii de Servicii de Încredere care eliberează certificate calificate UE,
- ETSI EN 319 421, Politicile și cerintele de securitate pentru furnizorii de servicii de încredere care emite marci temporale.
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates

certSIGN a dezvoltat, implementat și menținut un program de securitate cuprinzător conceput pentru ca:
- să protejeze confidențialitatea, integritatea și disponibilitatea datelor de certificare și a proceselor de gestionare a certificatelor;
- să protejeze împotriva amenințărilor sau pericolelor anticipate la adresa confidențialității, integrității și disponibilității datelor de certificare și a proceselor de gestionare a certificatelor;
- să protejeze împotriva accesului neautorizat sau ilegal, a utilizării, a divulgării, a modificării sau a distrugerii neautorizate sau ilegale a oricăror date de certificat sau procese de gestionare a certificatelor;
- să protejeze împotriva pierderii sau distrugerii accidentale sau a deteriorării oricăror date de certificat sau procese de gestionare a certificatelor;
- să respecte toate celelalte cerințe de securitate aplicabile CA în temeiul legii.

Procesul de gestionare a certificatelor include:
- controale de securitate fizică și de mediu;

- controale de integritate a sistemului, inclusiv gestionarea configurației, menținerea integrității codului de încredere și detectarea/prevenirea programelor malware;
- securitatea rețelei și gestionarea firewall-ului, inclusiv restricțiile de porturi;
- gestionarea utilizatorilor, alocarea separată a rolurilor de încredere, educația, sensibilizarea și formarea;
- controlul accesului logic, înregistrarea activităților.

Programul de securitate al certSIGN include o evaluare anuală a riscurilor care:
- Identifică amenințările interne și externe previzibile care ar putea avea ca rezultat accesul neautorizat, divulgarea, utilizarea necorespunzătoare, modificarea sau distrugerea oricăror date de certificare sau procese de gestionare a certificatelor;
- evaluează probabilitatea și daunele potențiale ale acestor amenințări, luând în considerare caracterul sensibil al datelor de certificare și al proceselor de gestionare a certificatelor;
- evaluează caracterul suficient al politicilor, procedurilor, sistemelor de informații, tehnologiei și al altor măsuri pe care CA le are în vigoare pentru a contracara astfel de amenințări.

Pe baza evaluării riscurilor, certSIGN a elaborat, implementat și menține un plan de securitate constând în proceduri, măsuri și produse de securitate concepute pentru a atinge obiectivele stabilite mai sus și pentru a gestiona și controla riscurile identificate în timpul evaluării riscurilor, proporțional cu gradul de sensibilitate al datelor de certificare și al proceselor de gestionare a certificatelor.

Planul de securitate include măsuri de protecție administrative, organizaționale, tehnice și fizice, corespunzătoare gradului de sensibilitate a datelor de certificat și a proceselor de gestionare a certificatelor. Planul de securitate ține seama de tehnologia disponibilă la momentul respectiv și de costurile de punere în aplicare a măsurilor specifice și pune în aplicare un nivel de securitate rezonabil, adecvat pentru prejudiciul care ar putea rezulta dintr-o încălcare a securității și natura datelor care trebuie protejate.

5.1 Controale fizice

Rețeaua de sisteme de calcul, terminalele operatorilor și resursele informaţionale ale certSIGN se află într-o zonă dedicată, protejată fizic împotriva accesului neautorizat, distrugerilor sau perturbării activităţii. Aceste locaţii sunt monitorizate. Fiecare intrare și ieşire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum și temperatura și umiditatea sunt de asemenea monitorizate și controlate.

5.1.1 Amplasarea și construcția sediului

certSIGN CA este amplasat în București, la următoarea adresă: B-dul Tudor Vladimirescu nr.29A, AFI Tech Park 1, București, România.

Toate operațiunile CA-ului și RA-ului certSIGN sunt realizate într-un mediu fizic protejat cu controale bazate pe evaluarea riscurilor care anticipează, previn, detectează și contracarează materializarea riscurilor pentru activele sale. De asemenea, menținem facilități de recuperare în caz de dezastru pentru operațiunile noastre CA și RA, facilități care sunt protejate prin măsuri de securitate fizică similare celor implementate la facilitatea noastră primară. Toate controalele de securitate fizică puse în aplicare de certSIGN sunt în conformitate cu standardele ISO 27001 și 27002 și sunt descrise în detaliu în politicile și procedurile de securitate. Printre cele mai importante controale de securitate sunt:

- Un perimetru clar definit și protejat, prin care sunt controlate toate intrările și ieșirile;
- Componentele critice sunt protejate cu mai multe perimetre;

- Un sistem de control de intrare, care admite numai acele persoane autorizate în mod corespunzător să intre în zonă;
- Monitorizare cu echipaj uman și electronic a intruziunilor neautorizate, în orice moment;
- Personalul care nu se regăsește pe lista de acces este însoțit și supravegheat în mod corespunzător;
- Un jurnal de acces este întreținut și controlat periodic;
- Echipamentul este întreținut în mod corect pentru a-i asigura disponibilitatea continuă și integritatea.

5.1.2 Accesul fizic

Accesul fizic în cadrul certSIGN este controlat și monitorizat de un sistem de alarmă integrat. certSIGN dispune de sisteme de prevenire a incendiilor, sisteme de detectare a persoanelor neautorizate şi sisteme de alimentare cu energie electrică în caz de urgenţă.

Sediul certSIGN este accesibil publicului în fiecare zi lucrătoare între 09:00 şi 18:00. În restul timpului (inclusiv în zilele nelucrătoare), accesul este permis numai persoanelor autorizate de către conducerea certSIGN.

Vizitatorii locaţiilor aparţinând certSIGN trebuie să fie însoţiţi permanent de personal autorizat.

Zonele ocupate de certSIGN se împart în:

- Zona de birouri,
- Zonele IT,
- Zona operatorilor CA
- Zona operatorilor RA și administratorilor,
- Zona de dezvoltare și testare.

Zonele IT sunt echipate cu un sistem de securitate monitorizat, compus din senzori de mişcare, efracţie și incendiu. Accesul în această zonă este permis numai personalului autorizat. Monitorizarea drepturilor de acces se face folosind carduri de identitate și cititoare, montate lângă punctul de acces. Fiecare intrare și ieşire în și din zonă este înregistrată automat în jurnalul de evenimente.

Accesul în **zona operatorilor** se face pe baza unui card electronic și a unui cititor de card. Deoarece toate informaţiile sensibile sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor și administratorilor necesită autorizarea prealabilă a acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. Cheile de acces pot fi ridicate numai de personalul autorizat. Zona este accesibilă exclusiv personalului certSIGN și persoanelor autorizate; prezenţa în zonă a celor din urmă le este permisă doar dacă sunt însoțiți de un angajat certSIGN.

În această zonă nu este permis accesul persoanelor neînsoţite.

Zona de dezvoltare și testare este protejată într-o manieră similară cu zona operatorilor și administratorilor. În această zonă este permisă și prezenţa persoanelor neînsoţite.

Programatorii și dezvoltatorii nu au acces la informaţii senzitive. Dacă este necesar un astfel de acces, atunci el se poate face numai în prezenţa administratorul de securitate. Proiectele în curs de implementare și software-ul aferent este testat în mediul de dezvoltare al certSIGN.

5.1.3 Alimetarea cu curent și aerul condiționat

Toate zonele sunt prevăzute cu aer condiționat. În zona serverelor, echipamentele de aer condiționat sunt redundante, iar temperatura este monitorizată atât automat (cu o alertă când un anumit nivel este atins) cât și manual. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a grupului electrogen al clădirii. Infrastructura de curent electric este concepută astfel încât la o întrerupere a curentului în clădire toate activitățile să fie disponibile pentru cel puțin 24 de ore cu ajutorul generatorului diesel. Fiecare server, echipament de rețea și toate calculatoarele angajaților care desfășoară activități importante pentru activitățile CA și RA sunt conectate la UPS-uri. Principalele componente ale securității fizice sunt de asemenea conectate la UPS-uri și la generatorul diesel.

5.1.4 Expunerea la apă

Riscul de inundație în zona serverelor este minim. In acest sens, toate echipamentele sunt plasate în rack-uri la o distanță de minim 15 cm de la sol, suplimentar fiind instalati senzori de inundatie cu alerte in timp real catre echipele de interventie.

5.1.5 Prevenirea și protecția împotriva incendiilor

Locaţia certSIGN dispune de sistem de prevenire și protecţie împotriva incendiilor în conformitate cu standardele și reglementările în domeniu. Ușile camerelor serverelor sunt certificate ca ignifuge și toate culoarele de acces sunt protejate cu substanțe rezistente la foc.

5.1.6 Depozitarea mediilor de stocare a informaţiilor

În conformitate cu cerințele politicii de clasificare a informațiilor, mediile care conțin date sau informații de rezervă sunt manipulate și stocate în siguranță în interiorul facilității primare. Mediile de backup sunt stocate în siguranță, într-o locație separată de locația principală, cu același nivel de securitate ca locația principală. Mediile care conțin date sensibile sunt distruse securizat atunci când nu mai sunt necesare.

5.1.7 Aruncarea deșeurilor

După expirarea perioadei de păstrare, hârtia și suporturile electronice care conțin informații semnificative pentru securitatea certSIGN sunt distruse. Modulele hardware de securitate sunt distruse în conformitate cu recomandările producătorului.

Atunci când nu mai este necesar, HSM-urile vor fi resetate pentru a preveni orice posibilitate de reutilizare a cheilor private ale CA și vor fi returnate inventarului criptografic.

După încetarea operațiunii, token-urile și cardurile rolurilor de încredere vor fi distruse.

Ștergerea securizată se face în conformitate cu politica de securitate a informațiilor a certSIGN.

5.1.8 Stocarea copiilor de siguranță în afara locației

Copiile cardurilor criptografice sunt stocate într-un seif aflat în afara locației principale a certSIGN.

Stocarea în afara locației cuprinde, de asemenea, arhive, copii curente ale informațiilor procesate de sistem și kit-urile de instalare al aplicațiilor certSIGN. Aceasta permite

recuperarea de urgență a fiecărei activități certSIGN în termen de 48 de ore în sediul certSIGN sau într-un sediu auxiliar.

5.2 Controale procedurale

5.2.1 Roluri de încredere

Roluri de încredere în certSIGN

În certSIGN sunt definite următoarele roluri de încredere, care pot fi atribuite uneia sau mai multor persoane:

- **Administrator de securitate** – Responsabilitate globală pentru implementarea politicilor și procedurilor de securitate. În plus poate aproba/revoca/suspenda certificate.
    - Iniţiază instalarea, configurarea și managementul aplicaţiilor software și hardware (inclusiv resursele de reţea) ale certSIGN; iniţiază și suspendă serviciile oferite de certSIGN; coordonează administratorii, iniţiază și supraveghează generarea de chei și secrete partajate; atribuie drepturi din punct de vedere al securităţii și privilegiilor de acces ale utilizatorilor; atribuie parole pentru conturile utilizatorilor noi; verifică jurnalele de evenimente; supervizează auditurile interne și externe; primeşte și răspunde la rapoartele de audit; supervizează eliminarea deficienţelor constatate în urma auditului.
    - Supraveghează operatorii Autorităţii de Certificare; configurează sistemele și reţeaua, activează și configurează mecanismele de protecţie a reţelei; creează conturile pentru utilizatorii certSIGN; verifică log-urile de sistem; verifică respectarea Politicii de certificare și a Codului de Practici și Proceduri; generează secrete partajate și chei; administrează Lista de certificate Revocate; creează copiile de siguranţă de urgenţă; modifică numele și adresele serverelor.
- **Administratorul de sistem** – Autorizat să instaleze, configureze și să întreţină sistemele de încredere ale Autorităţii de Certificare pentru înregistrarea, generarea de certificate, iniţializarea dispozitivelor și gestiunea revocărilor de certificate. Instalează dispozitivele hardware și sistemele de operare; instalează și configurează echipamentele de reţea.
- **Operatorul de sistem** – Responsabil de operarea zilnică a sistemelor de încredere ale Autorităţii de Certificare. Autorizat să execute operaţiile de backup și restaurare a sistemului. Are acces la certificatele Abonaților; revocă certificatele Abonaților; asigură continuitatea copiilor de siguranţă și arhivelor bazelor de date și a creării log-urilor de sistem; administrează bazele de date; are acces la informaţii confidenţiale despre Abonaţi, dar nu poate accesa fizic nici o altă resursă a sistemului; transferă copiile de siguranţă ale arhivei și ale datelor curente în afara locaţiei certSIGN.
- **Auditorul de sistem** – autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale Autorităţii de Certificare. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici și Proceduri de către Autoritatea

de Certificare; această responsabilitate se extinde și asupra Autorităţii de Înregistrare care operează în cadrul certSIGN.

- **Administratorul depozitarului** – administrează directoarele certSIGN disponibile publicului, creează și actualizează conținutul directoarelor din depozit, creează paginile Web și administrează legăturile (link-urile).

*În cadrul certSIGN, rolul de **auditor** nu poate fi combinat cu nici un alt rol. O entitate care are un rol diferit de cel de auditor nu poate prelua responsabilităţile auditorului.*

Roluri de încredere în Autoritatea de Înregistrare

certSIGN trebuie să se asigure că personalul Autorităţii de Înregistrare este conştient de responsabilităţile pe care le are cu privire la verificarea informaţiilor despre Abonaţi. Prin urmare, în cadrul unei Autorități de Înregistrare trebuie definite cel puţin următoarele 3 roluri de încredere:

- **Administratorul de sistem** – instalează dispozitivele hardware și sistemele de operare; instalează programe; configurează sistemul și aplicaţiile; activează și configurează resursele de securitate; creează conturi și parole pentru operatori; creează copii de siguranţă și arhivează datele; verifică jurnalele de evenimente (log-uri) și (împreună cu operatorul Autorităţii de Înregistrare), la ordinul administratorului de secrete, şterge datele în exces.
- **Administratorul de secrete** – supervizează și transferă secretele (cheile criptografice și alte date protejate) către operatorii Autorităţii de Înregistrare; ia parte la activarea modulului criptografic și la încărcarea cheilor operatorilor (în prezenţa acestora); transferă și activează cardurile de identitate ale operatorilor (dacă aceste carduri sunt blocate); mediază contactele dintre Autoritatea de Înregistrare și Autoritatea de Certificare;
- **Operatorii** – verifică identitatea Abonaților și corectitudinea cererilor primite; emit confirmări ale cererilor pe care le trimit Autorităţii de Certificare; generează cheile și iau parte la generarea certificatelor, trimiţând informaţiile din cerere la o Autoritate de Certificare; arhivează (sub formă de documente pe hârtie) cererile și confirmările emise, care fac obiectul ştergerii, la ordinul administratorului de secrete și în prezenţa acestuia,

Funcţiile de încredere ale Abonaților

Beneficiarul poate nominaliza o persoană (operator) care să exploateze aplicaţiile pentru schimbul electronic de date. Persoana respectivă este răspunzătoare de semnarea, criptarea și transmiterea mesajelor.

5.2.2 Numărul de persoane necesare pentru fiecare sarcină

Procesul de generare a cheilor - pentru necesitățile certificării și a semnarii CRL - este una dintre operațiunile care necesită o atenție deosebită. Generarea necesită prezența a cel puțin trei roluri de încredere, prezența ofițerului de securitate, a administratorului Autorității de Certificare și a unui număr corespunzător de persoane care dețin un secret partajat sunt necesare atunci când se încarcă cheia criptografică a Autorității de Certificare în modulul de securitate hardware.

Pentru sarcinile legate de funcțiile critice ale CA, cum ar fi, dar nu se limitează la, gestionarea cheilor și, în special, generarea de chei de CA, sunt necesare mai mult de două persoane pentru motive de securitate și control. Emiterea certificatului de către ROOT CA G2 are cel puțin un control dual efectuat de către personal autorizat și de încredere, astfel încât o persoană să nu poată semna singură certificate Intermediare.

5.2.3 Identificarea și autentificarea pentru fiecare rol

Personalul certSIGN este supus procedurii de identificare și autentificare în următoarea situație:

- Plasarea pe lista persoanelor autorizate să acceseze locațiile certSIGN,
- Plasarea pe lista persoanelor autorizate să acceseze fizic resursele de sistem și de rețea ale certSIGN,
- Emiterea unei confirmări care să autorizeze îndeplinirea rolului atribuit,
- Alocarea unui cont și a unei parole în sistemul informațional certSIGN.

Every assigned account:

- este unic și alocat direct unei anumite persoane,
- nu este folosit în comun cu nici o altă persoană,
- este restricţionat conform funcţiei (ce reiese din rolul îndeplinit de persoana respectivă) pe baza software-ului de sistem al certSIGN, a sistemului de operare și a controalelor de aplicaţii.

Operațiile efectuate în certSIGN care necesită acces prin resursele de rețea partajate sunt protejate cu mecanisme de autentificare puternică și criptare a informațiilor transmise.

Toți membrii personalului certSIGN implicați în furnizarea serviciilor de certificare sunt identificați și autentificați înainte de a utiliza aplicații critice legate de aceste servicii. În special, administratorii și operatorii HSM și operatorii CA și RA primesc o acreditare (certificate digitale pe tokenuri sau carduri inteligente HSM) pentru a asigura identificarea și autentificarea puternică (doi factori) înainte de a li se permite să efectueze orice acțiune de încredere. Toate acreditările criptografice sunt stocate în siguranță în cutii individuale.

Toate acțiunile in legatura cu certificatele, ale angajaților care au roluri de încredere sunt monitorizate

5.2.4 Rolurile care necesită separarea sarcinilor

certSIGN implementează și impune o separare a rolurilor și a sarcinilor pentru rolurile de Administrator, Operator și Auditor pentru a se asigura că aceeași persoană nu poate deține mai multe roluri. Toate aceste roluri au fișe de post, cu solicitari de abilitati și experienta specifice, definite din punctul de vedere al rolurilor indeplinite. Segregarea sarcinilor și principiul celui mai mic privilegiu sunt aplicabile. Sensibilitatea pozitiei bazata pe sarcini determina nivelul de acces, screening-ul de fond și trainingul angajatilor.

Sunt stabilite și implementate proceduri pentru toate rolurile de încredere și administrative care au impact asupra furnizării de servicii.

5.3 Controlul personalului

certSIGN se asigură că persoana care îndeplineşte responsabilităţile funcţiei, conform cu rolul atribuit în cadrul unei Autorități de Certificare sau Înregistrare:

- A absolvit cel puţin liceul,
- Are cetățenie română,
- A inteles și a semnat un contract ce descrie rolul și responsabilităţile sale în cadrul sistemului,
- A beneficiat de un stagiu de pregătire avansată în conformitate cu obligaţiile și sarcinile asociate funcţiei sale,
- A fost instruit cu privire la protecția datelor personale și informaţiilor confidenţiale sau private,
- A semnat un contract ce conține clauze referitoare la protejarea informaţiilor senzitive ale certSIGN și a datelor confidenţiale și private ale Beneficiarilor,
- Nu îndeplineşte sarcini care pot genera conflicte de interese între Autoritatea de Certificare și Autoritatea de Înregistrare care acţionează în numele acesteia.

Rolurile și responsabilitățile de securitate, așa cum sunt specificate în politica certSIGN privind securitatea informațiilor, sunt documentate în fișa postului sau în documentele aflate la dispoziția personalului în cauză.

5.3.1 Calificări, experință și aprobări necesare

certSIGN se asigură că toți angajații care acționează pentru furnizarea de servicii de certificare sunt verificați înainte de angajare în ceea ce privește calificările, cunoștințele de specialitate, experiențe și autorizare necesare și, după caz, pentru a îndeplini roluri de încredere și pentru a îndeplini funcția specifică postului ocupat. Personalul de conducere posedă expertiză și experiență în domeniul tehnologiei PKI și suficientă experiență de management al securității informațiilor și de gestionare a riscurilor pentru a-și îndeplini funcțiile de conducere.

5.3.2 Proceduri de verificare a antecedentelor

certSIGN asigură efectuarea controalelor relevante personalului potențial prin intermediul rapoartelor de stare emise de o autoritate competentă, al declarațiilor de la terți sau al declarațiilor auto-semnate.

5.3.3 Cerinţele de pregătire a personalului

Personalul care îndeplinește roluri și sarcini ca urmare a angajării în cadrul certSIGN trebuie să fie instruit cu privire la:

- Cerințele CPP,
- Cerințele politicii de certificare,
- procedurile și controalele de securitate folosite de Autoritatea de Certificare și Autoritatea de Înregistrare,
- Amenințările comune la adresa procesului de verificare a informațiilor (inclusiv phishing și alte tactici de inginerie socială) și cerințele de bază pentru Forumul CA/B,
- Responsabilitățile care decurg din rolurile și sarcinile efectuate în sistem.

După terminarea cursului, participanții semnează un document care confirmă familiarizarea lor cu CPP, politica de certificare și acceptarea restricțiilor și obligațiilor asociate.

certSIGN se asigură că personalul însărcinat cu operatiunile de validare își menține un nivel de calificare care îi permite să îndeplinească aceste sarcini în mod satisfăcător. CA documentează faptul că fiecare specialist în validare posedă competențele necesare unei sarcini înainte de a permite specialiștilor de validare să îndeplinească acea sarcină. CA solicită

tuturor specialiștilor de validare să treaca un examen furnizat de CA cu privire la cerințele de verificare a informațiilor prezentate în CPP și cerințele de bază ale forumului CA / B.

5.3.4 Frecvența și cerințele stagiilor de pregătire

Pregătirea descrisă în Capitolul 5.3.3 trebuie repetată sau suplimentată de fiecare dată când apar modificări semnificative în modul de funcționare al certSIGN sau al Autorității de Înregistrare.

5.3.5 Frecvența și secvența rotației posturilor

Acest Cod de Practici și Proceduri nu specifică nici un fel de cerinţe în această privinţă.

5.3.6 Sancțiunile pentru acțiunile neautorizate

certSIGN va lua masuri împotriva celor ce incalcă politicile sau procedurile, realizează acțiuni neautorizate, folosirea neautorizată a autorității și utilizarea neautorizată a sistemelor. Acestea pot include, printre altele, revocarea de privilegii, disciplinare administrativă, sancțiuni reglementate de legislația muncii din România și / sau urmărirea penală.

5.3.7 Cerințele pentru contractanții independenți

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicaţii etc.) face obiectul unor verificări similare celor efectuate în cazul angajaţilor certSIGN (vezi Capitolul 5.3.1, 5.3.2, 5.3.3 și 5.4.1). În plus, personalul angajat pe bază de contract, pe timpul cât îşi desfăşoară activitatea în locaţia certSIGN, trebuie să fie însoţit permanent de un angajat al certSIGN, cu excepţia celor care au primit avizare din partea administratorului de securitate și care pot accesa informaţii clasificate intern sau în conformitate cu normele legale în vigoare.

Controalele asupra personalului care sunt contractori independenți, mai degrabă decât angajații entității, includ auditarea și monitorizarea personalului contractorului; și alte controale asupra personalului contractant.

5.3.8 Documentația oferită personalului

certSIGN oferă personalului său accesul la următoarele documente:

- Politica de certificare,
- CPP,
- Lista Responsabilităţilor și obligaţiilor asociate rolului deţinut în sistem
- Politicile și procedurile de securitate

Alte documente relevante (proceduri operaționale, instrucțiuni de lucru, manuale) necesare personalului pentru a-și îndeplini funcțiile specifice legate de furnizarea de servicii de certificare certSIGN, sunt distribuite în timpul formării inițiale, training-urilor anuale și ori de câte ori este cazul.

5.4 Procedurile de înregistrare a datelor de audit

Pentru gestionarea eficientă a sistemelor și aplicațiilor folosite de certSIGN în activitatea sa în calitate de furnizor de servicii de certificare, dar și pentru a permite auditarea acțiunilor angajaților și clienților, toate informațiile cu privire la evenimente importante, generate de sisteme și aplicații sunt înregistrate. Aceste informații, cunoscute în mod colectiv sub numele

de log-uri trebuie să fie păstrate în așa fel încât să poată fi accesate de către Entitățile Partenere, auditori și autoritățile de stat oricând au nevoie de ea, pentru a furniza dovezi ale funcționării corecte a serviciilor în scopul procedurilor legale sau pentru a detecta încercările de a compromite securitatea certSIGN. Evenimentele înregistrate sunt arhivate și păstrate într-o locație secundară.

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. Fiecare înregistrarea în log, electronic sau de mână, este păstrată și dezvăluită atunci când se desfăşoară un audit, dacă este necesar. Acuratețea temporală a log-urilor este asigurată de trei servere de timp. Două dintre ele folosesc ca referință de timp sateliți GPS, iar unul este sincronizat cu sistemulcare furnizează ora ofocială din România (NIMB). Ora utilizată pentru înregistrarea evenimentelor necesare în jurnalul de audit este sincronizată cu UTC cel puțin o dată pe zi.

5.4.1 Evenimente Înregistrate

Fiecare activitate critică din punctul de vedere al securităţii certSIGN este înregistrată în log-urile de evenimente și arhivată. Arhivele sunt depozitate pe medii de stocare ce nu pot fi suprascrise sau distruse cu ușurință (cu excepția cazului în cazul în care sunt transferate pe un suport de păstrare pe termen lung) în perioada de timp în care acestea sunt obligate să fie păstrate. Log-urile de evenimente certSIGN conţin înregistrări ale tuturor activităţilor generate de componentele software din cadrul sistemului. Aceste înregistrări sunt împărţite în trei categorii separate:

- **Intrări de sistem** – conţin informaţii despre cererile clienţilor și răspunsurile server-ului (sau invers) la nivelul protocolului de reţea (de exemplu http, https); datele concrete care se înregistrează sunt: adresa IP a staţiei sau a server-ului, operaţiunile executate (de exemplu: căutare, editare, scriere etc.) și rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- **Erori** – conţin informaţii despre erori la nivelul protocoalelor de reţea și la nivelul modulelor aplicaţiilor;
- **Audit logs**– conţin informaţii specifice serviciilor de certificare, de exemplu: cererea de înregistrarea și de certificare, cererea de rekey, acceptarea certificatului, emiterea certificatului și CRL etc.

Jurnalele de evenimente de mai sus sunt comune fiecărei componente instalate pe un server sau staţie de lucru și au o capacitate prestabilită. Atunci când se depăşeşte această capacitate, este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat şi şters de pe disc.

CA certSIGN și fiecare parte terță delegată înregistrează evenimentele legate de securitatea sistemelor lor de certificate, a sistemelor de gestionare a certificatelor, a sistemelor CA rădăcină și a sistemelor părților terțe delegate. CA și fiecare parte terță delegată înregistrează evenimentele legate de acțiunile întreprinse pentru a procesa o cerere de certificat și pentru a emite un certificat, inclusiv toate informațiile generate și documentația primită în legătură cu cererea de certificat; ora și data; și personalul implicat. certSIGN CA pune aceste înregistrări la dispoziția auditorului său calificat ca dovadă a conformității CA cu aceste cerințe.

CA înregistrează cel puțin următoarele evenimente:

1. Evenimentele legate de ciclul de viață al certificatelor și cheilor CA, inclusiv:

- generarea, salvarea, stocarea, recuperarea, arhivarea și distrugerea cheilor;
- cereri de certificate, reînnoire și cereri de recheie și revocare;
- aprobarea și respingerea cererilor de certificate;
- evenimente de gestionare a ciclului de viață al dispozitivelor criptografice;
- generarea listelor de revocare a certificatelor;
- Semnarea răspunsurilor OCSP

Introducerea de noi profiluri de certificat și retragerea profilurilor de certificat existente.2. Evenimentele de gestionare a ciclului de viață al certificatului de abonat, inclusiv:

- Cereri de certificate, reînnoire și cereri de rechemare și revocare;
- toate activitățile de verificare prevăzute în prezentele cerințe și în Declarația privind practicile de certificare ale CA;
- aprobarea și respingerea cererilor de certificate;
- emiterea de certificate;
- generarea listelor de revocare a certificatelor;
- semnarea răspunsurilor OCSP.

3. Evenimente de securitate, inclusiv:

- încercări reușite și nereușite de acces la sistemul PKI;
- acțiunile efectuate de sistemul PKI și de securitate;
- modificări ale profilului de securitate;
- instalarea, actualizarea și eliminarea de software pe un sistem de certificare;
- pornirea și oprirea sistemului, blocări, defecțiuni hardware și alte anomalii;
- activități relevante ale routerului și ale firewall-ului (astfel cum sunt descrise mai jos);
- intrările și ieșirile din incaperile CA.

Fiecare înregistrare, automată sau manuală, conţine următoarele informaţii:

- Tipul evenimentului,
- Identificatorul evenimentului,
- Descrierea evenimentului
- Data și ora apariţiei evenimentului,
- Identificatorul persoanei responsabile de eveniment.

Înregistrarea activităților routerului și a firewall-ului include cel puțin:

- încercări de conectare reușite și nereușite la routere și firewall-uri;
- înregistrarea tuturor acțiunilor administrative efectuate asupra routerelor și firewall-urilor, inclusiv a modificărilor de configurare, a actualizărilor de firmware și a modificărilor de control al accesului;
- înregistrarea tuturor modificărilor aduse regulilor de firewall, inclusiv adăugări, modificări și ștergeri;
- înregistrarea tuturor evenimentelor și erorilor de sistem, inclusiv a defecțiunilor hardware, a blocărilor de software și a repornirilor de sistem.

Toate informațiile de înregistrare, inclusiv următoarele sunt înregistrate:

- tipul de document(e) prezentat de către solicitant la înregistrare;
- înregistrarea datelor de identificare unice, numere, sau o combinație a acestora (de exemplu, cartea de identitate a solicitantului sau pașaport) a documentelor de identificare, dacă este cazul;

- locul de depozitare al copiilor cererilor și a documentelor de identificare, inclusiv contractul semnat de Beneficiar;
- orice opțiuni specifice din contract (de exemplu, acceptarea publicării certificatului)
- Identitatea entității care acceptă cererea;
- Metoda utilizată pentru validarea documentelor de identificare,

Accesul la log-uri este permis exclusiv pentru ofițerul de securitate, personalul desemnat special și auditori, prin cerere adresata pe email sau in format hartie catre CISO.

Confidențialitatea informațiilor Beneficiarului este menținută.

5.4.2 Frecvența procesării jurnalelor de evenimente

Jurnalele de audit sunt prelucrate în mod continuu și/sau ca urmare a unei alarme sau eveniment anormal. Jurnalele de audit sunt arhivate și copii de siguranță sunt făcute în mod continuu.

5.4.3 Perioada de păstrare a log-urilor de audit

Înregistrările evenimentelor sunt stocate în fişiere pe discul sistem până când ajung la capacitatea maximă permisă. În tot acest timp sunt disponibile on-line, la cererea fiecărei persoane sau proces autorizat. După depăşirea spaţiului alocat, jurnalele sunt păstrate în arhive și pot fi accesate numai off-line, de la o anumită stație de lucru.

Jurnalele arhivate sunt păstrate cel puțin 10 ani.

5.4.4 Protecția jurnalelor de evenimente

Fișierele jurnalelor sunt protejate în mod corespunzător printr-un mecanism de control al accesului. Un sistem de protecție adecvată împotriva modificărilor și ștergerii jurnalelor de audit este pus în aplicare astfel încât nimeni nu poate modifica sau șterge înregistrări de audit, cu excepția transferului pe un mediu de păstrare pe termen lung, în scopuri de arhivare. Doar administratorul de securitate, administratorii sau un auditor poate revizui un jurnal de evenimente. Accesul la jurnalul de evenimente este configurat în așa fel încât:

- Doar entităţile de mai sus au dreptul să citească înregistrările jurnalului,
- Platforma centrală de jurnale arhivează sau șterge automat fișierele (după arhivarea lor) care conțin evenimentele înregistrate,
- Este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conţin lacune sau falsuri,
- Nici o entitate nu are dreptul să modifice conținutul unui jurnal.

În plus, procedurile de protecţie a jurnalului sunt implementate în aşa fel încât, chiar și după arhivarea jurnalului, este imposibil să ştergi înregistrări, sau să ştergi jurnalul înaintea expirării perioadei de retenţie a jurnalului.

5.4.5 Procedura de backup a log-urilor de Audit

Politicile de securitate ale certSIGN cer ca jurnalul de evenimente să fie salvat periodic într-o copie de rezervă. Aceste copii de rezervă sunt păstrate în locațiile auxiliare ale certSIGN. Copiile de rezervă ale fișierelor-jurnal și ale pistelor de audit sunt salvate în conformitate cu procedurile interne.

5.4.6 Sistemul de colectare a datelor pentru audit (intern vs extern)

Toate log-urile generate de servere, dispozitive de rețea, echipamente de Securitate, aplicații sunt trimise periodic la o platforma centrală, al cărei scop este să:

- Colecteze
- Depoziteze
- Analizeze
- Coreleze
- Arhiveze
- Genereze copii de siguranță pe termen lung ok

5.4.7 Notificarea sursei care a generat

Modulul de analiză a jurnalului de evenimente implementat în sistem examinează evenimentele curente și sesizează automat activităţile suspecte sau pe cele care au ca scop compromiterea securităţii. În cazul activităţilor care au influenţă asupra securităţii sistemului, sunt notificaţi automat administratorul de securitate și administratorul Autorităţii de Certificare. În celelalte cazuri, notificarea este direcţionată numai către administratorul de sistem. Transmiterea informaţiilor către persoanele autorizate despre situaţiile critice – din punctul de vedere al securităţii sistemului – se face prin alte mijloace de comunicare, protejate corespunzător, de exemplu, pager, telefon mobil, poştă electronica. Entităţile notificate iau măsurile corespunzătoare pentru a proteja sistemul faţă de ameninţarea detectată.

5.4.8 Evaluări de vulnerabilitate

Întreaga infrastructură face obiectul evaluării amenintarilor si a vulnerabilităților specifice, de către specialistii certSIGN, ca parte a procedurilor de evaluare internă a riscurilor precum si diminuarea acestuia conform nivelului acceptat.

Pentru a se asigura că toate activele, activitățile și serviciile sale sunt sigure, certSIGN a implementat, menține și îmbunătățește continuu sistemul de management al securității informațiilor certificat ISO 27001: 2013. În conformitate cu cerințele prezentului cadru de securitate, toate activitățile de securitate încep cu o evaluare a riscurilor pentru a identifica și a clasifica toate activele informaționale, pentru a evalua riscurile la care sunt expuse și pentru a determina controalele tehnice, manageriale, organizaționale și procedurale necesare. certSIGN menține un inventar al tuturor activelor informaționale și le atribuie o clasificare compatibilă cu evaluarea riscurilor.
Evaluarea riscurilor este actualizată cel puțin o dată pe an și:
1. Identifică amenințările interne și externe previzibile care ar putea duce la acces neautorizat, dezvăluire, utilizare incorectă, modificare sau distrugere a oricărui proces de procesare a datelor de certificat sau a procesului de administrare a certificatelor;
2. Evaluează probabilitatea și posibilele pagube ale acestor amenințări, ținând cont de sensibilitatea proceselor de certificare a datelor și a certificatelor; și
3. Evaluează suficiența politicilor, a procedurilor, a sistemelor informatice, a tehnologiei și a altor aranjamente pe care CA dispune de astfel de amenințări.

5.5 Arhivarea înregistrărilor

Este necesar ca toate datele și fișierele referitoare la înregistarea informaţiior asociate securității sistemului, cererile trimise de Subiecți/ Beneficiari, informaţiile despre Subiecți/ Beneficiari, certificatele emise şi CRL-urile, cheile folosite de Autorităţile de Certificare și Înregistrare, și toată corespondenţa dintre certSIGN și Subiecți/ Beneficiari să fie arhivate.

Depozitarul on-line conţine certificatele active și poate fi folosit pentru efectuarea unor servicii externe ale Autorităţii de Certificare, cum ar fi verificarea validităţii unui certificat, publicarea certificatelor pentru proprietarii acestora (restaurarea certificatelor) și entităţile autorizate.

Arhiva conţine certificate expirate, inclusiv certificatele revocate. Arhiva certificatelor revocate conţine informaţii despre certificat, motivul revocării, dacă cand a fost certificatul plasat în CRL. Arhiva este folosită pentru rezolvarea eventualelor dispute, referitoare la documente vechi, semnate electronic de un Subiect.

Copiile de siguranţă sunt ţinute în afara locaţiei certSIGN.

5.5.1 Tipuri de date arhivate

certSIGN și fiecare DRA arhivează toate jurnalele de audit (astfel cum se prevede în secțiunea 5.4.1).
În plus, certSIGN și fiecare DRA arhivează:
1. Documentația referitoare la securitatea sistemelor lor de certificate, a sistemelor de gestionare a certificatelor, a sistemelor AC rădăcină și a sistemelor terților delegați;
2. Documentația referitoare la verificarea, emiterea și revocarea cererilor de certificate și a certificatelor.
Următoarele date sunt incluse într-o arhivă de încredere:

- Toate certificatele pentru o perioadă de 10 ani după expirarea acestora
- Jurnalele de log-uri arhivate sunt păstrate timp de 10 ani
- Log-urile de emitere și revocare a certificatelor pentru o perioadă de 10 ani de la data emiterii / revocării
- CRL-urile sunt păstrate 10 ani de la publicare
- Următoarele, timp de 10 ani de la expirarea valabilității tuturor certificatelor care se bazează pe aceste înregistrări:
    - log-ul tuturor evenimentelor legate de ciclul de viață al cheilor gestionate de CA, inclusiv orice perechi de chei Subiect generate de CA
    - termeni și condiții (semnați) privind utilizarea certificatului

5.5.2 Perioada de retenție a arhivei

Vezi secțiunea 5.5.1 de mai sus. După expirarea perioadei de păstrare declarate, datele arhivate sunt distruse.

5.5.3 Protecția arhivei

certSIGN asigură:

- implementarea controalelor pentru prevenirea pierderilor de date din arhivă
- confidențialitatea datelor arhivate și menținerea integrității în timpul perioadei sale de reținere,

Arhivele sunt accesibile exclusiv personalului autorizat.

5.5.4 Procedurile de back-up al arhivei

Backup-ul datelor arhivate se face în conformitate cu politicile și procedurile interne privind back-up-ul.

5.5.5 Cerințe privind marcarea temporală a înregistrărilor

Timpul de sistem pentru calculatoarele certSIGN este actualizat utilizând Network Time Protocol (NTP) pentru a sincroniza ceasurile sistemului cel puțin o dată la fiecare opt ore

(Windows default). Următoarele articole arhivate din lista de verificare a aprobării certificatului sunt marcate cu data, cu data, ora și numele angajatului certSIGN care verifică informațiile și fac înregistrarea:

- Instantaneu al starii organizationale;
- Instantaneu al site-ului web.

Următoarele înregistrări sunt marcate temporal de sistemul de administrare a certificatului atunci când un element este fie primit automat, fie este verificat de către angajatul certSIGN:

- Confirmare a cererii de certificate și CSR PKCS#10;
- Scrisoare de autorizare;
- Numele, adresa de e-mail și adresa IP a persoanei care recunoaște autoritatea organizatorică; alte informații despre aplicație, după caz.

Emiterea certificatului este marcată temporal în funcție de câmpul "Valid From", în conformitate cu profilul de certificat X.509.

Revocarea certificatului este marcată temporal, în funcție de câmpul "Data revocării", în conformitate cu profilul CRL al certificatului X.509.

5.5.6 Sistemul de colectare al arhivei (intern sau extern)

Sistemele de colectare ale arhivei certSIGN sunt interne.

5.5.7 Proceduri de obținere și verificare a informațiilor arhivate

Arhivele sunt accesibile angajaților autorizați ai certSIGN și auditorilor desemnați. Înregistrările sunt păstrate în format electronic, sau în format pe suport de hârtie.

Beneficiarul / Subiectul poate primi acces la înregistrări și alte informații referitoare la Subiectul Certificatului.

5.6 Schimbarea cheilor

Procedurile de schimbare a cheilor permit tranzitia usoara de la certificate de CA expirate catre certificate noi. Spre sfârșitul vieții Chei Private a CA, certSIGN încetează să utilizeze cheia privată a CA care expiră pentru a semna Certificate (cu cel puțin un an înaintea expirării) și utilizează vechea cheie privată doar pentru a semna CRL-uri. O nouă pereche de chei de semnare CA este comandată și toate certificatele emise ulterior și CRL-urile, sunt semnate cu noua cheie privată de semnare. Atât vechile, cât și cele noi perechi de chei pot fi active simultan. Acest proces de schimbare a cheilor ajută la minimizarea oricăror efecte negative ale expirării certificatului CA. Certificatul corespunzator noului CA este furnizat Beneficiarilor si tertilor prin metodele de livrare detaliate in sectiunea 6.1.4.

5.7 Compromiterea și recuperare în caz de dezastru

Acest capitol descrie procedurile folosite de certSIGN în situaţii anormale (inclusiv dezastrele naturale) pentru restaurarea serviciilor la nivelul garantat. Aceste proceduri sunt executate în concordanţă cu Planul de continuitate a afacerii și de recuperare în caz de dezastru.

5.7.1 Procedurile de administrare a a incidentelor și compromiterilor

certSIGN a pus în aplicare o procedură de gestionare a incidentelor de securitate, în scopul de a răspunde rapid și coordonat la incidente și pentru a limita impactul evenimentelor de

securitate. Angajaților le sunt atribuite roluri de încredere pentru a urmări alertele evenimentelor de securitate potențiale critice și pentru a se asigura că incidentele relevante sunt raportate în conformitate cu procedura. În cazul defecțiunilor critice se acționează pe baza aceleiași proceduri.

Procedura de administrare a incidentelor de securitate specifică de asemenea modul în care se face notificarea părților corespunzătoare în conformitate cu normele de reglementare aplicabile oricărei breșe de securitate sau pierderii integrității care are un impact semnificativ asupra serviciului de încredere furnizat și asupra datelor cu caracter personal păstrate de acesta în termen de 24 de ore de la identificarea breșei.

În cazul producerii unor incidente de Securitate, se utilizează procedurile interne. Aceste proceduri includ și notificarea Organismului de Supraveghere.

În cazul în care breșa de securitate sau pierderea integrității poate afecta în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de certificare, vom notifica de asemenea, persoana fizică sau juridică imediat.

Toate jurnalele evenimentelor de securitate sunt analizate în mod continuu prin mecanisme automate, pentru a identifica dovezi de activitate rău intenționată și pentru a alerta personalul asupra posibilelor evenimente critice de securitate.

Toate incidentele și/sau compromiterile sunt documentate și toate înregistrările asociate sunt arhivate așa cum este descris în secțiunea 5.5 a CPP.

5.7.2 Compromiterea resurselor de calcul, a aplicațiilor software și/sau datelor

Politica de Securitate certSIGN ia în considerate următoarele amenințări care pot influența disponibilitatea și continuitatea serviciilor furnizate:

- distrugerea fizică a sistemului de calcul al certSIGN, inclusiv alterarea resurselor de reţea – această amenințare se referă la distrugerile provocate de situaţiile de urgenţă,
- funcţionarea defectuoasă a aplicaţiilor, având ca efect imposibilitatea accesării datelor - aceste deteriorări se referă la sistemul de operare, aplicaţiile utilizatorilor și executarea de aplicaţii periculoase, cum ar fi viruşii, viermii, caii troieni,
- pierderea unor servicii de reţea importante pentru activitatea certSIGN. Acestea se referă în primul rând la căderile de tensiune și distrugerea legăturilor de reţea.
- distrugerea unei părţi din Intranetul folosit de certSIGN pentru a furniza servicii – acest lucru poate duce la obstrucţionarea clienţilor și refuzul (neintenţionat) serviciilor.

Pentru a preveni sau limita rezultatele amenințărilor de mai sus:

- Politica de securitate a certSIGN include un Plan de continuitate a afacerii și recuperare în caz de dezastru,
- În cazul apariţiei unui eveniment ce blochează funcţionarea certSIGN, în maxim 48 de ore, va fi activată locaţia auxiliară ce poate substitui toate funcţiile importante ale unei Autorităţii de Certificare până la restaurarea locaţiei principale. Distanța dintre locația primară și cea secundară este suficient de mare pentru ca potențialul dezastru care afectează locația primară să nu afecteze și locația secundară.

- Instalarea de versiuni noi ale aplicaţiilor software în producţie se poate face numai după testarea intensivă a acestora într-un mediu de test, în conformitate cu procedurile descrise. Orice modificare a sistemului necesită aprobarea administratorului de securitate al certSIGN.
- Sistemele certSIGN utilizează aplicaţii pentru crearea copiilor de rezervă a datelor pe baza cărora se poate face în orice moment restaurarea sistemului și auditarea acestuia. Copiile de siguranţă includ toate datele relevante din punct de vedere al securităţii.
- Toate sistemele din care este compusă infrastructura IT pentru furnizarea de servicii de certificare și timestamp sunt monitorizate în mod continuu și toate evenimentele de securitate sunt înregistrate și analizate. Activitățile de sistem anormale care indică o potențială încălcare a securității, inclusiv intruziune în sistemele de rețea sunt detectate și raportate ca alarme pentru a permite certSIGN să detecteze, înregistreze și reacționeze în timp util la orice tentativă neautorizată și/sau neobișnuite de a accesa resursele sale.
- Sensibilitatea oricăror informații colectate sau analizate este luată în considerare, protejându-le împotriva accesului neautorizat.
- Pentru a detecta orice discontinuitate în operațiunile de monitorizare, pornirea și oprirea funcțiilor de logare este, de asemenea, monitorizată.
- Disponibilitatea tuturor componentelor importante ale infrastructurii ICT utilizate pentru furnizarea serviciilor de certificare, precum și disponibilitatea serviciilor critice sunt, de asemenea, monitorizate.
- certSIGN va aborda orice vulnerabilitate critică care anterior nu a fost adresată, într-o perioadă de 48 de ore de la descoperirea sa. Dacă acest lucru este rentabil, având în vedere impactul, va fi creat și pus în aplicare un plan pentru a reduce vulnerabilitatea sau va fi documentată decizia că vulnerabilitatea nu necesită remediere.

5.7.3 Proceduri care se aplică la compromiterea cheii private a unei entități

Compromiterea cheii(lor) private ale CA sau a datelor de activare asociate implică revocarea imediată a certificatului cheii(lor) compromise.

În cazul compromiterii cheilor private a unei Autorități de Certificare (afiliate la certSIGN) sau în cazul în care există suspiciunea că ele au fost compromise, trebuie luate și următoarele măsuri:

- Notificarea - asupra compromiterii - a tuturor Subiecților / Beneficiarilor și a celorlalte entități cu care certSIGN are acorduri sau alte forme de relații stabilite, între care Entitățile Partenere și alți Furnizori de Servicii de Încredere. În plus, aceste informații vor fi puse la dispoziția altor Entități Partenere prin intermediul sistemului mass-media și prin poșta electronică.
- Notificarea publicului prin mai multe canale, inclusiv un mesaj în depozitarul certSIGN CA și pe web site, un comunicat de presă în mass-media.
- Un certificat corespunzător cheii compromise este plasat pe Lista Certificatelor Revocate

- Toate certificatele semnate de CA-ul compromis sunt revocate, specificându-se motivul revocării
- Autoritatea de Certificare generează o nouă pereche de chei și un nou certificat
- Se generează noi certificate pentru Subiecţi
- Noile certificate sunt trimise Subiecților în mod gratuit.
- Dacă un certificat este revocat din cauza compromisului cheie CA, certSIGN Root CA G2 va emite un CRL nou în termen de 24 de ore de la primirea notificării privind compromisul și va publica CRL-urile online imediat.

Paragraful anterior este de asemenea aplicabil în cazul în care algoritmii PKI sau parametrii asociați sunt compromise sau dacă acestea devin insuficiente pentru utilizarea dorită rămasă.

5.7.4 Capacități de Continuitate a afacerii în caz de dezastru

certSIGN a stabilit într-un Plan de Continuitate a afacerii (BCP) și un Plan de recuperare în caz de dezastru (DRP) toate măsurile necesare pentru a asigura recuperarea integrală a serviciilor noastre de certificare și marcare temporală în caz de dezastru, sau în cazul unei discontinuități a oricărei componente ICT ori a unui serviciu important, mai mare decât Downtime-ul Maxim Tolerabil. Orice astfel de măsuri sunt conforme cu standardele ISO/IEC 27001 și 27002. Funcționarea fiecărei componente sau serviciu va fi restaurată în timpul Maxim Tolerabil de Downtime stabilit în planul de continuitate.

Toate datele sistemelor necesare pentru reluarea operațiunilor CA sunt salvate și stocate într-un loc la distanță și în condiții de siguranță, pentru a permite serviciilor de certificare și marcare temporală să își reia activitatea în timp util în cazul unui incident / dezastru.

Copiile de siguranță ale informațiilor și software-ului esențial sunt realizate în mod regulat. Se oferă facilități de back-up adecvate pentru a se asigura că toate informațiile și software-urile esențiale pot fi recuperate în urma unui dezastru sau unei defectiuni a mediilor de stocare. Activitățile de back-up sunt testate în mod regulat pentru a se asigura că acestea îndeplinesc cerințele planurilor de continuitate a afacerii.

Funcțiile de backup și restaurare sunt efectuate de rolurile de încredere relevante.

Planurile BCP și DRP abordează de asemenea compromiterea, pierderea sau suspiciunea de compromitere a cheii private sau compromiterea algoritmilor PKI a CA ca pe un dezastru, iar procesele planificate sunt puse în aplicare.
În urma unui dezastru, acolo unde este posibil, vor fi luate măsuri pentru a evita repetarea unui dezastru.

5.8 Încetarea activității Autorității de Certificare sau a Autorității de Înregistrare

certSIGN are un plan la zi de încetare a activității pentru a minimiza efectele negative asupra Beneficiarilor şi Entităților Partenere ce pot apărea ca urmare a deciziei unei Autorități de Certificare de a-și înceta activitatea. Planul include obligativitatea notificării Beneficiarilor (dacă există) în legatură cu autoritatea de certificare ce urmează să își înceteze activitatea și transferarea responsabilităților (servicii furnizate către Beneficiari, baze de date, etc) în conformitate cu reglementarile aplicabile către altă Autoritate de Certificare.

5.8.1 Cerințe asociate transferului responsabilității

Înainte ca o Autoritate de Certificare să își înceteze activitatea, aceasta va:

- Informa (cu cel puțin 30 de zile înainte) despre decizia de încetare a serviciilor pe următorii: toți Beneficiarii care dețin certificate active (neexpirate și nerevocate) emise de această autoritate și alte entități cu care certSIGN are înțelegeri sau alte forme de colaborare, printre care Entități Partenere, alți furnizori de servicii de încredere și autorități relevante, cum ar fi organismele de supraveghere. În plus, această informație va fi facută disponibilă și altor Entități Partenere;
- Revocă certificatele neexpirate care au fost emise.
- Transferă obligațiile sale unei părți de încredere pentru a menține toate informațiile necesare pentru furnizarea dovezilor privind funcționarea certificării și a serviciilor de marcare temporală pentru o perioadă rezonabilă, cu excepția cazului în care se poate demonstra că certSIGN nu deține nicio astfel de informație; informațiile se referă la informații de înregistrare, la starea de revocare a certificatelor neexpirate care au fost emise și la arhivele jurnalului de evenimente pentru perioada respectivă de timp, astfel cum a fost menționată Beneficiarilor și Entității Partenere;
- Distruge sau retrage din uz cheile private ale CA, inclusiv copiile de rezervă, într-o manieră care să facă imposibilă recuperarea cheilor private;
- Dacă este posibil, se vor realiza anumite înțelegeri pentru a transfera furnizarea de servicii de certificare pentru clienții existenți către un alt furnizor de servicii de certificare.

certSIGN va păstra sau va trasfera unei părți de încredere obligațiile sale, astfel încât să asigure disponibilitatea cheii sale publice pentru o perioadă rezonabilă de timp.

În cazul în care certSIGN își încetează activitatea, fără a transfera o parte sau toate activitățile sale, va revoca certificatele afectate după o lună de la notificarea Beneficiarilor

certSIGN are un aranjament care să acopere costurile îndeplinirii acestor cerințe minime, în cazul în care intră în faliment sau dacă din orice alt motiv nu poate acoperi aceste costuri de una singură, în măsura în care este posibil, în limitele legislației aplicabile privind falimentul.

5.8.2 Emiterea certificatelor de către succesorul Autorității de Certificare care își încetează activitatea

Pentru a asigura continuitatea serviciilor de emitere certificate pentru Abonaţi, Autoritatea de Certificare care îşi încetează activitatea poate semna un contract cu o altă Autoritate de Certificare ce oferă servicii similare, pentru a emite certificate care să înlocuiască certificatele rămase în uz, emise de Autoritatea de Certificare care îşi încheie activitatea.

Prin emiterea unui certificat care să-l înlocuiască pe cel vechi, succesorul Autorităţii de Certificare care îşi încetează activitatea preia drepturile și obligaţiile acestei autorități în ceea ce priveşte managementul certificatelor care rămân în uz.

Arhiva Autorităţii de Certificare care-și încetează activitatea trebuie predată Autorităţii de Certificare primară, certSIGN ROOT CA (în cazul încetării activităţii autorități certSIGN SSL DV CA Class 3 G2), sau instituţiei cu care s-a semnat contractul (în cazul sistării activităţii autorități certSIGN ROOT CA).

6 Controale tehnice de securitate

6.1 Generarea și instalarea perechii de chei

Procedurile de management a cheii se referă la păstrarea și folosirea în siguranţă de către proprietar a cheilor sale. O atenţie deosebită se acordă generării și protecţiei cheii private a certSIGN, care influenţează funcţionarea în siguranţă a întregului sistem de certificare a cheilor publice.

Autoritatea de Certificare **certSIGN ROOT CA** deţine cel puţin un certificat autosemnat. Cheia privată corespunzătoare cheii publice conţinută de certificatul autosemnat este folosită exclusiv în scopul semnării cheilor publice ale Autorităţilor de Certificare **certSIGN SSL DV CA Class 3 G2** prin semnarea certificatelor operaţionale și a Listei de certificate Revocate, necesare pentru funcţionarea autorităţilor respective. Un rol similar îl au cheile private deţinute de fiecare autoritate: **certSIGN SSL DV CA Class 3 G2** corespunzătoare cheilor publice incluse în certificatele emise de **certSIGN ROOT CA** pentru fiecare autoritate.

Perechile de chei deţinute de fiecare Autoritate de Certificare trebuie să permită semnarea de certificate și CRL - o cheie publică asociată cu o cheie privată autentificată cu un certificat autosemnat (în cazul **certSIGN ROOT CA**) sau certificat (în cazul **certSIGN SSL DV CA Class 3 G2**).

O semnătură electronică este creată prin intermediul algoritmului RSA în combinație cu algoritmul de hash SHA-2.

6.1.1 Generarea perechilor de chei

Cheile **certSIGN SSL DV CA Class 3 G2** precum și ale altor autorități Intermediare sunt generate în cadrul locaţiei certSIGN, în prezenţa unui grup de persoane de încredere (administratorul de securitate și administratorul Autorităţii de Certificare sunt membri ai acestui grup).

Perechile de chei pentru Autoritățile de Certificare care funcţionează în cadrul certSIGN sunt generate la anumite staţii de lucru autentificate și conectate la module hardware de securitate, conforme cu cerinţele FIPS 140-2 Nivel 3. Ele sunt menţinute în permanenţă criptate pe aceste dispozitive.

Procesul de generare de perechi de chei pentru Autoritățile de Certificare este similar cu procedura acceptată de generare a cheilor în cadrul certSIGN, descrisa mai sus. Acţiunile întreprinse în momentul generării perechii de chei sunt înregistrate, datate și semnate de fiecare persoană prezentă în timpul generării. Înregistrările sunt păstrate din motive de audit sau pentru verificările obișnuite ale sistemului.

Operatorii Autorităţii de Înregistrare deţin numai chei pentru autentificarea tuturor acţiunilor lor. Aceste chei sunt generate de operator (în prezenţa administratorilor de secrete) prin intermediul unei aplicaţii software autentificată, furnizată de Autoritatea de Certificare și conectată la un modulul hardware de securitate conform cu cerinţele FIPS 140-2 Nivel 2.

În general, fiecare Beneficiar își generează singur perechea de chei. Pentru aceasta se va folosi de aplicaţia disponibila pe site-ul web al certSIGN, în momentul creării cererii. Aplicaţia permite crearea cheilor atât pe dispozitive securizate (tokenuri, smart carduri), cat și în

format p12 criptat. Generarea poate fi, de asemenea, făcută de către o Autoritate de Certificare.

CA respinge o cerere de certificat SSL dacă sunt îndeplinite una sau mai multe dintre următoarele condiții:

- perechea de chei nu îndeplinește cerințele stabilite în secțiunea 6.1.5 și / sau în secțiunea 6.1.6
- Există dovezi clare că metoda specifică utilizată pentru a genera cheia privată a fost compromisă;
- CA are la cunoștință despre o metodă demonstrată sau dovedită care expune cheia privată a solicitantului la compromisuri;
- CA a fost informată anterior că cheia privată a solicitantului a suferit un compromis, cum ar fi cele menționate în secțiunea 4.9.1;
- CA are la cunoștință despre o metodă demonstrată sau dovedită pentru a calcula cu ușurință cheia privată a solicitantului pe baza cheii publice (cum ar fi o cheie slabă Debian, consultați https://wiki.debian.org/SSLkeys).

În cazul în care certificatul SSL Beneficiar conține o extensie extKeyUsage care conține valorile id-kp-serverAuth sau anyExtendedKeyUsage, CA-ul NU va genera o pereche de chei în numele Beneficiarului și NU va accepta o cerere de certificat SSL utilizând o pereche de chei generată anterior de CA.
certSIGN poate, la cererea Beneficiarului sau la cererea operatorului Autorităţii de Certificare, să genereze o pereche de chei și să o trimită în siguranţă Beneficiarului. În astfel de cazuri sunt folosite aplicaţii și dispozitive criptografice conforme cu FIPS 140-2 Nivel 2 (vezi Capitolul 6.1.2).

În toate cazurile, certSIGN CA:
- va pregăti și va urma un script de generare a cheilor,
- va avea un auditor calificat care să asiste la procesul de generare a perechilor de chei ale CA
- va genera perechile de chei ale CA într-un mediu fizic securizat, astfel cum este descris în prezentul CPP;
- va genera perechea de chei CA folosind personal cu roluri de încredere în conformitate cu principiile controlului de către mai multe persoane și al cunoașterii separate;
- va genera perechea de chei CA în cadrul unor module criptografice care îndeplinesc cerințele tehnice și comerciale aplicabile, astfel cum sunt prezentate în prezentul CPP;
- va înregistra activitățile de generare a perechii de chei CA; și
- va menține controale eficiente pentru a oferi o asigurare rezonabilă că cheia privată a fost generată și protejată în conformitate cu procedurile descrise în prezentul CPP și în scenariul de generare a cheilor.

6.1.1.1 Procedurile de generare a cheilor initiale ale certSIGN ROOT CA

Procedurile de generare a cheii iniţiale a certSIGN ROOT CA sunt folosite numai la iniţierea sistemului certSIGN sau în cazul suspectării faptului că cheia privată a Autorităţii de Certificare a fost compromisă. Procedura include:

- generarea în siguranţă a perechii principale de chei pentru semnarea de certificate și CRL-uri și distribuirea cheii private,
- emiterea unui certificat de cheie publică autosemnat.

- emiterea, de către auditorul calificat, a unui raport în care să se aprecieze că certSIGN CA a respectat scriptul de generare chei în timpul procesului de generare a cheilor și a certificatelor, precum și controalele utilizate pentru a asigura integritatea și confidențialitatea perechii de chei.

După generarea perechii de chei pentru semnarea de certificate și CRL-uri, activarea cheii private în modulul hardware de securitate, cheile pot fi folosite în operaţiile criptografice până la expirarea perioadei de validitate sau până când au fost compromise.

6.1.1.2 Procedurile de generare a cheilor initiale ale certSIGN CA

Procedurile de generare a cheilor iniţiale pentru certSIGN CA includ:

- generarea în siguranţă a perechii principale de chei pentru semnarea de certificate și CRL-uri și distribuirea cheii private,
- emiterea unui certificat de cheie publică semnat de certSIGN ROOT CA.

După generarea perechii de chei pentru semnarea de certificate și CRL-uri și activarea cheii private în modulul hardware de securitate, cheile pot fi folosite în operaţiile criptografice până la expirarea perioadei de validitate sau până la o eventuala compromitere.

6.1.1.3 Procedurile de schimbare a cheii certificatului pentru certSIGN ROOT CA

Cheile criptografice ale certSIGN ROOT CA au o perioadă de viaţă limitată; dacă această perioadă a expirat, cheile trebuie actualizate.

Actualizarea perechii de chei folosite pentru semnarea de certificate și CRL-uri se face folosind o procedură specifică. Aceasta se bazează pe emiterea de certificate speciale de către certSIGN ROOT CA. certificatele dau posibilitatea Abonaților care au instalat deja un certificat expirat al certSIGN ROOT CA să treacă în siguranţă la utilizarea noului certificat; noii Abonaţi care posedă deja noul certificat pot să obţină în siguranţă certificatul expirat, care poate fi necesar la verificarea datelor semnate în trecut.

Pentru a obţine efectul descris mai sus, certSIGN ROOT CA aplică o procedură prin intermediul căreia generarea unei noi perechi de chei va permite autentificarea noii chei publice prin folosirea cheii private vechi și invers (o cheie publică veche este autentificată cu o cheie privată nouă). Aceasta înseamnă că, drept rezultat al actualizării certificatului Autorităţii de Certificare, certSIGN ROOT CA, în afară de certificatul nou, mai sunt create încă două certificate. După actualizarea cheii, sunt create patru certificate pentru semnarea de certificate și CRL-uri: certificatul vechi **OldWithOld** (cheia publică veche este semnată cu cheia privată veche), certificatul nou **NewWithNew** (cheia publică nouă este semnată cu cheia privată nouă), certificatul **OldWithNew** (cheia publică veche este semnată cu cheia privată noua) și certificatul **NewWithOld** (cheia publică nouă este semnată cu cheia privată veche).

Procedura de actualizare a perechii de chei pentru certSIGN ROOT CA, folosită pentru semnarea de certificate și CRL-uri, se desfăşoară astfel:

- generarea unei perechi de chei noi,
- crearea unui certificat conţinând cheia publică nouă a certSIGN ROOT CA, semnat cu cheia privată vechea (certificatul **NewWithOld**),

- dezactivarea cheii private vechi și activarea celei noi în modulul hardware de securitate – este încărcată cheia privată nouă pentru semnarea de certificate și CRL-uri,
- crearea unui certificat conţinând cheia publică veche a certSIGN ROOT CA, semnat cu cheia privată nouă (certificatul **OldWithNew**),
- crearea unui certificat conţinând cheia publică nouă a certSIGN ROOT CA, semnat cu cheia privată nouă (certificatul **NewWithNew**),
- publicarea în depozit a noilor certificate, difuzarea de informaţii despre noile certificate disponibile și, opţional, publicarea rezumatului criptografic al noii chei publice în ziare.

După generarea și activarea cheii private noi (acest lucru se poate face în orice moment, în timpul perioadei de validitate a vechiului certificat), autoritatea certSIGN ROOT CA semnează noile certificate folosind exclusiv noua cheie privată.

Vechea cheie publică (vechiul certificat) este disponibilă publicului până când toţi Abonaţii obţin noul certificat (noua cheie publică) a certSIGN ROOT CA (acesta trebuie obţinută înaintea datei de expirare a vechiului certificat).

Începutul și expirarea perioadei de validitate a certificatului **OldWithNew** ar trebui să fie aceeaşi cu data de început și de expirare a certificatului vechi.

Perioada de validitate a certificatului **NewWithOld** începe din momentul generării noii perechi de chei și expiră în momentul în care toţi Abonaţii vor obţine noile certificate (certificatul noii chei publice) ale certSIGN ROOT CA. Momentul expirării nu ar trebui să fie mai mare decât cel al expirării vechiului certificat.

Perioada de validitate a certificatului **NewWithNew** începe din momentul generării noii perechi de chei și expiră la cel puţin 180 de zile după data următoarei generări de perechi de chei. Acest lucru înseamnă că Autoritatea de Certificare certSIGN ROOT CA încetează a mai folosi cheia privată pentru semnarea de certificate și CRL-uri cu cel puţin 180 de zile înainte de data expirării certificatului corespunzător acestei chei private.

6.1.1.4 Procedura de schimbare a cheii certificatelor autoritatilor Intermediare

Procedura de schimbare (actualizare) a cheii Autorităţii de Certificare pentru certSIGN SSL DV CA Class 3 G2 se desfăşoară în mod similar cu cea pentru certSIGN ROOT CA (a se vedea capitolul 6.1.1.3) cu excepţia unui singur pas: certificatul **NewWithNew** este emis de o autoritate superioară.

6.1.2 Distribuirea Cheii Private către Beneficiar

Dacă perechea de chei a Beneficiarului este generată de către o Autoritate de Certificare, cheile se distribuie Beneficiarului astfel:

- cheile sunt stocate pe un dispozitiv criptografic (de exemplu, token), sau în format PKCS#12 pentru anumite cazuri și sunt livrate personal Beneficiarului, sau printr-o scrisoare poştală recomandată; datele pentru activarea cardului (codul PIN) sau pentru decriptarea cheii (parola) sunt trimise separat de mediul de stocare care conține perechile de chei; cardurile emise sunt personalizate și înregistrate de Autoritatea de Certificare.

certSIGN garantează că după generarea perechii de chei la cererea unui Beneficiar, cheile nu vor fi folosite pentru crearea de semnaturi electronice și că Autoritatea de Certificare nu va

crea condiţii pentru crearea de semnaturi de către nici o entitate neautorizată, cu excepţia proprietarului cheii private.

6.1.3 Distribuirea Cheii Publice către emitentul certificatului

Abonaţii trimit cheia lor publică generată sub formă de cerere electronica, al cărui format trebuie să respecte standardul PKCS#10 (CRS).

Cererile trimise unei Autorități de Certificare pot necesita, în anumite cazuri, o confirmare emisă de Autoritatea de Înregistrare (vezi Capitolele 3 și 4).

Trimiterea cheii publice nu este necesară atunci când perechea de chei este generată, la cererea Beneficiarului sau la cererea operatorului Autorităţii de Înregistrare, de către Autoritatea de Certificare, care emite simultan un certificat pentru perechea de chei generată.

6.1.4 Distribuirea Cheii Publice a Autorității Certificare către Entitățile Partenere

Cheile publice ale unei Autorități de Certificare care emite certificate către Abonaţi sunt distribuite în exclusivitate sub formă de certificate conform recomandărilor ITU-T X.509 v.3. În cazul Autorităţii de Certificare certSIGN ROOT CA, certificatele sunt autosemnate.

Autoritățile de Certificare certSIGN distribuie certificatele proprii în două moduri diferite:

- prin plasarea în depozitul public al certSIGN; obţinerea certificatelor necesită vizitarea paginii Web disponibilă la https://registru.certsign.ro/cgi-bin/pubral/pubra/get_cert,
- distribuirea împreună cu aplicaţiile software (browsere Web, clienţi de email etc.), care permit folosirea serviciilor oferite de certSIGN.

In cazul schimbării (actualizării) cheii Autorităţii de Certificare certSIGN-ROOT CA, depozitul trebuie să conţină toate certificatele autosemnate sau certificatele emise ca urmare a execuţiei procedurii descrise în Capitolul 6.1.1.3

6.1.5 Mărimea cheilor

Dimensiunea cheilor folosite de Autoritățile de Certificare, operatorii Autorităţii de Înregistrare și Abonaţi sunt prezentate în Tabelul 6.1. Numai acești algoritmi și aceste dimensiuni de chei sunt permise pentru CA-urile enumerate în tabel.

Proprietarul cheii	Principala utilizare a cheii		
	RSA pentru semnarea de certificat și CRL	RSA pentru semnarea de mesaje	RSA pentru schimbul de chei
certSIGN ROOT CA	2048 biţi	-	-
certSIGN SSL DV CA Class 3 G2	2048 biți		

Tabel 6.1. Dimensiunea cheilor folosite

6.1.6 Parametrii de generare a Cheilor Publice și verificarea calității

Cel care generează o cheie este responsabil de verificarea calităţii parametrilor cheii generate. Acesta trebuie să verifice:

- posibilitatea de a efectua operaţii de criptare și decriptare, inclusiv creare de semnaturi electronice și verificare a acestora,

- procesul de generare a cheii trebuie să se bazeze pe generatoare puternice de numere aleatoare – surse fizice de zgomot alb, dacă este posibil,
- imunitatea la atacuri cunoscute (în cazul algoritmilor RSA și DSA).

certSIGN are o procedură pentru efectuarea generării perechilor de chei CA pentru certSIGN Web CA. Procedurile de verificare includ etape de verificare a faptului că valoarea exponentului public este un număr impar egal cu 3 sau mai mare. Modulul trebuie să aibă următoarele caracteristici: să fie un număr impar, să nu fie puterea unui număr prim și să nu aibă factori mai mici decât 752. În plus, exponentul public trebuie să se situeze în intervalul recomandat, între $2^{16}+1$ și $2^{256}-1$.

6.1.7 Scopurile în care pot fi utilizate cheile (conform câmpului de utilizare a cheilor X.509 v3)

Scopurile în care pot fi folosite cheile sunt descrise în câmpul KeyUsage (vezi Capitolul 7.1) din cadrul extensiilor standard ale certificatelor X.509 v3. Acest câmp trebuie verificat în mod obligatoriu de aplicaţia Beneficiarului care face managementul certificatelor.

Folosirea biţilor din câmpul KeyUsage trebuie să respecte următoarele reguli:

a) digitalSignature: certificate pentru verificarea semnăturii electronice,
b) nonRepudiation: certificate pentru furnizarea serviciului de ne-repudiere de către persoane fizice, cât și pentru alte scopuri decât cele descrise la punctele f) și g). Bitul de ne-repudiere poate fi setat numai într-un certificat de cheie publică cu care se intenţionează verificarea semnăturilor electronice și nu trebuie combinat cu cele descrise la punctele c) - e) și legate de asigurarea confidenţialităţii,
c) keyEncipherment: folosite pentru criptarea cheilor algoritmilor simetrici, oferind confidenţialitatea datelor,
d) dataEncipherment: folosite pentru criptarea datelor Beneficiarului, altele decât cele descrise la punctele c) și e),
e) keyAgreement: folosite pentru protocoale de schimbare a cheilor,
f) keyCertSign: cheia publică este folosită pentru verificarea semnăturii electronice în certificatele emise de entităţi care oferă servicii de certificare,
g) cRLSign: cheia publică este folosită pentru verificarea semnăturilor electronice de pe listele de certificate revocate și suspendate emise de entităţile care oferă servicii de certificare,
h) encipherOnly: poate fi folosit exclusiv cu bitul de keyAgreement pentru a indica scopul de criptare a datelor în cadrul protocoalelor de schimbare a cheilor,
i) decipherOnly: poate fi folosit exclusiv cu bitul de keyAgreement pentru a indica scopul de decriptare a datelor în cadrul protocoalelor de schimbare a cheilor.

Cheile private care corespund certificatelor de bază sunt folosite numai pentru a semna certificatele în următoarele cazuri:

- Certificate cu auto-semnare ale CA Root;
- Certificate pentru CA Intermediare și certificate încrucișate.

6.2 Protecția cheii private și controalele modulului criptografic

Fiecare Beneficiar, operator al Autorităţii de Certificare și Autoritate de Certificare generează și stochează cheia sa privată folosind un sistem sigur care previne pierderea, dezvăluirea, modificarea sau accesul neautorizat la această cheie. Dacă o Autoritate de Certificare generează o pereche de chei la cererea Beneficiarului, trebuie să o livreze acestuia în siguranţă și să impună Beneficiarului protejarea cheii sale private.

HSM-urile nu părăsesc mediul securizat din incinta securizată a CA. În cazul în care HSM-urile necesită întreținere sau reparații care nu pot fi efectuate în incinta securizată a CA (în condiții de dublă control dublu al mai multor angajați cu rol de încredere), acestea sunt scoase din uz în condiții de siguranță.

6.2.1 Controalele și standardele modulelor criptografice

Modulele hardware de securitate folosite de Autoritățile de Certificare respectă cerinţele standardului FIPS 140-2. În cazul Abonaților care folosesc mecanisme hardware de protecţie a cheii, se recomandă de asemenea respectarea cerinţelor FIPS 140-2 sau Common Criteria.

Crearea de semnatura electronica și criptarea datelor se face conform standardului PKCS#7. Cheile private (ca și cheile publice) pot fi în una dintre următoarele stări (în conformitate cu standardul ISO/IEC 11770-1):

- **în aşteptare pentru activare** (**pregătită**) – cheia a fost deja generată, dar nu este utilizabilă (data curentă nu este încă aceeaşi cu data începerii perioadei de validitate a certificatului),
- **activă** – cheia poate fi folosită în operaţiile criptografice (de exemplu pentru crearea de semnaturii electronice), data curentă este în cadrul perioadei de validitate a certificatului, cheia nu a fost revocată,
- **inactivă** – cheia aflată în această stare poate fi folosită numai pentru verificarea de semnaturii electronice sau pentru operaţii de decriptare (Beneficiarului nu-i este permisă folosirea cheii private pentru crearea de semnaturi electronice – validitatea cheii a expirat; în cazul unei chei publice, Beneficiarului nu îi este permisă criptarea informaţiei); data curentă este în afara perioadei de validitate a certificatului.

6.2.2 Control multi-persoană (n din m) al cheilor private

Controlul dual a unei chei private se aplică doar cheilor private ale Autorităţilor de Certificare certSIGN SSL DV CA Class 3 G2 folosite pentru semnarea de certificate și CRL-uri.

Controlul dual al accesului se realizează prin distribuirea de secrete operatorilor autorizaţi. Secretele sunt stocate pe carduri criptografice sau token-uri, protejate printr-un cod PIN și transferate în mod autentificat deţinătorilor acestora.

Pentru operaţiuni de tipul: iniţierea modulului criptografic hardware, transferul cheilor private ale Autorităţilor de Certificare, se implementează scheme prag de acces (de tip k din n) prin distribuire **de secrete partajate**. Numărul acceptat de secrete partajate și numărul necesar de secrete care permit restaurarea cheii private sunt expuse în Tabelul 6.2.2.

Autoritatea de emitere certificate	Numărul de secrete partajate	Numărul total de secrete distribuite
certSIGN ROOT CA	2	3
certSIGN SSL DV CA Class 3 G2	2	3

Tabelul 6.2.2. Distribuirea secretelor partajate pentru inițierea și transferul cheilor private

Procedura de transfer a secretului partajat implică prezenţa deţinătorului de secret pe timpul procesului de generare a cheii și a distribuirii sale, acceptarea secretului dat și a responsabilităţilor care reies din păstrarea sa.

6.2.2.1 Acceptarea secretului partajat de către deținătorii săi

Fiecare deţinător de secrete partajate, înainte de a primi partea sa de secret, trebuie să asiste personal la împărţirea secretului, să verifice corectitudinea secretului creat și distribuirea sa. Fiecare parte a secretului partajat trebuie transferată deţinătorului său pe un card criptografic protejat de un cod PIN, ales de deţinător și ştiut numai de el. Primirea secretului partajat și crearea sa sunt confirmate printr-o semnătură de mână pe un formular, a cărui copie este păstrată în arhivele Autorităţii de Certificare și de către deţinătorul de secret.

6.2.2.2 Protejarea secretului partajat

Deținătorii secretului partajat trebuie să protejeze partea lor împotriva divulgării. Deținătorul declară că:

- Nu va dezvălui, copia sau partaja secretul cu nimeni și că nu va folosi partea sa din secret în mod neautorizat,
- Că nu va dezvălui (direct sau indirect) că este deținătorul secretului

6.2.2.3 Disponibilitatea și ștergerea (transferul) secretului partajat

Deținătorul secretului partajat trebuie să permită accesul la partea sa din secret persoanelor juridice autorizate (printr-un formular corespunzător semnat de către deţinător înaintea oferirii părţii sale din secret), numai după autorizarea transmiterii secretului. Această situaţie trebuie înregistrată în mod corespunzător în log-urile de securitate.

În cazul dezastrelor naturale, deţinătorul secretului trebuie să se prezinte la locul de recuperare în caz de urgenţă al certSIGN, conform instrucţiunilor primite de la emitenul secretului partajat. Secretul partajat trebuie livrat personal de către deţinător la locul recuperării în caz de urgenţă, într-un mod care să permită folosirea lui pentru restaurarea activităţii certSIGN la starea sa normală.

6.2.2.4 Responsibilitățile deținătorului secretului partajat

Deţinătorul secretului partajat trebuie să-și îndeplinească îndatoririle și obligaţiile conform cerinţelor acestui Cod de Practici și Proceduri, în mod deliberat și responsabil în orice situaţie posibilă. Un deţinător de secret partajat trebuie să anunţe emitentul secretului în cazul furtului, pierderii, dezvăluirii neautorizate sau compromiterii securităţii secretului, imediat după incident. Un deţinător de secret partajat nu este responsabil pentru neîndeplinirea îndatoririlor/obligaţiilor sale din cauza unor motive ce sunt imposibil de controlat de către acesta, dar este responsabil pentru dezvăluirea inoportună a secretului sau pentru neglijarea obligaţiilor de a notifica emitentul secretului despre dezvăluirea inoportună sau violarea securităţii secretului ca urmare a greşelilor, neglijenţei sau iresponsabilităţii deţinătorului.

Controlul multiplu nu se aplică cheii private a Beneficiarului.

6.2.3 Custodia Cheii Private

Cheile private de semnare ale Beneficiarului nu sunt supuse custodiei.

Copiile cheilor private de criptare ale abonaţilor sunt create numai la cererea Beneficiarului şi sunt supuse custodiei.

6.2.4 Copia de siguranță a cheii private

Autoritățile de Certificare care operează în cadrul certSIGN creează o copie de siguranţă a cheii lor private. Copiile sunt folosite în cazul punerii în aplicare a procedurilor standard, sau de urgenţă (de exemplu, după dezastru) de recuperare a cheii. Atunci când se regăsesc în exteriorul dispozitivului criptografic securizat, cheile private ale CA sunt protejate într-un mod care să asigure același nivel de protecție asigurat de dispozitivul criptografic securizat. Copiile cheilor private sunt protejate prin secrete partajate.

certSIGN nu păstrează copii ale cheilor private ale operatorilor Autorităţii de Certificare.

Copiile cheilor private ale Abonaților sunt create numai la cererea Beneficiarului și în conformitate cu metodele prezentate în 6.2.3.

"Copiile cheilor private de criptare ale utilizatorilor sunt pastrate criptat in baza de date a Autoritatilor de Certificare.

Astfel, fiecare cheie privata a utilizatorului este criptata simetric cu o cheie de sesiune. Cheile de sesiune sunt criptate cu o cheie master de decriptare. Accesul la aceasta cheie de decriptare se face prin secrete partajate, pe principiul K din N. Cheile private de semnare ale utilizatorilor nu sunt salvate."

6.2.5 Arhivarea Cheii Private

Cheile private ale Autorităţii de Certificare folosite pentru crearea de semnături electronice nu sunt arhivate – sunt distruse imediat după încheierea operaţiei criptografice ce necesită aceste chei sau la expirarea/revocarea certificatului cheii publice asociate.

6.2.6 Transferul Cheii Private într-un sau dintr-un modul criptografic

Operaţiunea de introducere a unei chei private într-un modul criptografic se aplică în următoarele cazuri:

- când cheile sunt generate în afara modulului criptografic; această situaţie apare, de exemplu, în cazul generării cheii de către o Autoritate de Certificare la cererea Beneficiarului, la introducerea lor într-un dispozitiv criptografic, înainte de trimiterea suportului de stocare către Beneficiar. O operaţie similară de introducere a cheii într-un modul criptografic poate fi îndeplinită de un Beneficiar când cheile sunt livrate sub formă criptată și necesită stocare locală pe un dispozitiv criptografic,
- în cazul creării copiilor de siguranţă ale cheilor private stocate într-un modul criptografic, poate fi necesară, ocazional, (ex. în cazul compromiterii sau defectării modulului) introducerea unei perechi de chei într-un modul de securitate diferit,
- când este necesară transferarea unei chei private din modulul operaţional folosit pentru operaţii standard ale entităţii, pe un alt modul; situaţia poate apărea în cazul defectării modulului sau în cazul necesităţii distrugerii acestuia.

Introducerea unei chei private într-un modul de securitate este o operaţiune critică și de aceea trebuie implementate măsuri și proceduri care să prevină dezvăluirea, modificarea sau falsificarea cheii private.

Introducerea unei chei private într-un modul hardware de securitate al Autorităţilor de Certificare **certSIGN ROOT CA** sau **certSIGN SSL DV CA Class 3 G2** necesită restaurarea cheii de pe carduri în prezenţa unui număr corespunzător de deţinători de secret partajat care protejează modulul ce conține cheile private (vezi Capitolul 6.2.2). Deoarece fiecare Autoritate de Certificare poate deţine o copie criptată a cheii sale private (vezi Capitolul 6.2.4), cheile pot fi de asemenea transferate între module.

6.2.7 Stocarea cheilor private pe modul criptografic

certSIGN folosește module de securitate hardware (HSM) pentru a îndeplini sarcinile de management al cheilor CA. Sunt luate măsuri pentru ca dispozitivele criptografice sigure să nu fie alterate în timpul transportului și în timp ce acestea sunt depozitate la sediul certSIGN.

Controlul accesului este activat pentru a se asigura că cheile nu sunt accesibile în afara dispozitivelor criptografice securizate dedicate pe care sunt stocate cheile de semnare CA și orice copii ale acestora.

HSM-urile nu părăsesc mediul sigur al sediului securizat al CA.

Cheile private ale CA rămân sub controlul multiplu al n din m angajați. Custozii CA sunt însărcinați cu activarea și dezactivarea cheilor private ale CA-urilor. Cheile CA-urilor sunt apoi active pentru perioade definite de timp.

Operatorii utilizează dispozitive de generare a semnăturii electronice calificate (token-uri/carduri). Cheile sunt întotdeauna generate pe dispozitive și nu le părăsesc niciodată. Dispozitivele securizate sunt protejate în timpul transportului de la furnizor la certSIGN, în timpul depozitării și la distribuție.

6.2.8 Metoda de activare a cheii private

Metodele de activare a cheii private, deţinute de diverşi utilizatori sau Abonaţi ai sistemului certSIGN, se referă la activarea cheii înainte de orice folosire a sa, sau de începerea unei sesiunii de lucru ce necesită folosirea cheii respective (de exemplu, conectarea la Internet). O cheie odată activată poate fi folosită până la dezactivare.

Executarea procedurilor de activare (și dezactivare) a unei chei private depinde de tipul entităţii care deţine cheia respectivă (Beneficiar, Autoritate de Înregistrare, Autoritate de Certificare, dispozitiv hardware etc.), de senzitivitatea datelor protejate de cheie și de intervalul de timp în care cheia trebuie să rămână activă (pe timpul unei singure operaţiuni, sesiuni sau pentru o perioadă nelimitată).

Toate cheile private ale **certSIGN ROOT CA** sau **certSIGN SSL DV CA Class 3 G2** introduse în modul după generare, importate sub formă criptată dintr-un alt modul sau restaurate dintr-un secret partajat, rămân în stare activă până la ştergerea lor fizică de pe modul sau până la scoaterea lor din serviciile certSIGN. Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea este realizată pe baza unui card criptografic deţinut de operator. După introducerea cardului în modulul criptografic și folosirea codului PIN, cheia privată rămâne în stare activă până la scoaterea cardului din modul.

Cheile private ale operatorilor Autorităţii de Înregistrare sunt activate după autentificarea operatorului (folosirea codului PIN) și numai pentru durata unei singure operaţii criptografice care necesită folosirea cheii respective. Ca urmare a încheierii acestei operaţii, cheia privată este dezactivată automat și trebuie reactivată înaintea executării altei operaţii criptografice.

Activarea cheii private a unui Beneficiar se face în mod similar cu procedura de activare a cheii private a operatorilor Autorităţii de Certificare, indiferent dacă sunt stocate pe un card criptografic sau sub formă criptată, ca fişier pe o dischetă sau orice alt mediu de stocare. În cazul Abonaților persoane juridice (organizaţii, instituţii etc.) activarea trebuie să se facă de către o persoană autorizată a Beneficiarului.

6.2.9 Metoda de dezactivare a cheii private

Metodele de dezactivare a cheii private se referă la dezactivarea cheii după folosirea acesteia sau ca urmare a terminării unei sesiuni în timpul căreia a fost folosită cheia.

În cazul unui Beneficiar sau al unui operator al Autorităţii de Înregistrare, dezactivarea cheii private de semnatura se face imediat după încheierea sesiunii (la ieşire din aplicaţie). Dacă în timpul executării operaţiei criptografice, cheia privată a fost stocată în memoria aplicaţiei, aplicaţia trebuie să prevină refacerea neautorizată a cheii private. Dacă o cheie privată este deţinută de un Beneficiar persoană juridică, cheia poate fi dezactivată numai de reprezentantul autorizat al acestui Beneficiar.

În cazul certSIGN, dezactivarea unei chei private se face de către ofiţerul de securitate numai în cazul în care o sesiune de lucru a fost încheiată, perioada de validitate a cheii a expirat, cheia a fost revocată sau este necesar să se suspende imediat activităţile sistemului. Dezactivarea unei chei private se face prin scoaterea cardului din modul.

6.2.10 Metoda de distrugere a cheii private

La sfârșitul duratei de viață, cheile private ale CA sunt distruse de roluri de încredere ale CA în prezența a mai mult de un reprezentant al Corpului de gestionare a politicilor și procedurilor (PPMB), pentru a se asigura că aceste chei private nu pot fi recuperate sau folosite din nou .

Cheia privată CA poate fi distrusă prin ștergerea tuturor cardurilor HSM (Operator și Administrator). În plus, HSM permit zeroirea dispozitivului prin acces fizic și setări pe dispozitiv. Aceasta reinitializează dispozitivul și suprascrie toate datele de pe acesta cu zerouri binare. În cazurile în care această procedură de zeroiziere sau de reinitializare nu reușește, certSIGN va zdrobi, arunca și / sau arde aparatul într-o manieră care distruge capacitatea de a extrage orice secret.

Aceste module hardware sunt tratate într-o manieră sigură, așa cum este descris în procedurile interne distruse de documente documentate. Dosarele asociate sunt arhivate în siguranță. Organismul de gestionare a politicilor și procedurilor (PPMB) autorizează distrugerea cheii private a CA și atribuie personalului sarcina.

Fiecare distrugere a cheii private este înregistrată în jurnalul evenimentului.

Subiectul este responsabil să distrugă cheia privată.

6.2.11 Evaluarea Modulului Criptografic

Vezi mai sus.

6.3 Alte aspecte legate de managementul perechilor de chei

certSIGN va utiliza în mod corespunzător cheile private de semnare ale CA și nu le va utiliza după sfârșitul ciclului lor de viață.

Cheile de semnare ale CA utilizate pentru generarea certificatelor și a listelor de certificate revocate nu vor fi utilizate pentru niciun alt scop.

Cheile de semnare a certificatelor se utilizează numai în incinte securizate fizic.

Utilizarea cheii private a CA trebuie să fie compatibilă cu algoritmul de hash, algoritmul semnăturii și lungimea cheii semnăturii utilizate pentru generarea de certificate, în conformitate cu practica curentă (lungimea cheii selectate și algoritmul pentru cheia de semnare a CA sunt RSA 4096 biți în acord cu Cerințele în ETSI TS 119 312 în scopul de semnare a CA).

Toate copiile cheilor private de semnare CA sunt distruse la sfârșitul ciclului lor de viață.

6.3.1 Arhivarea cheilor publice

Scopul arhivării cheilor publice este acela de a crea posibilitatea verificării semnaturii electronice după eliminarea unui certificat din depozit (vezi Capitolul 2). Acest lucru este foarte important în cazul serviciilor de ne-repudiere, cum ar fi serviciul de marcă temporala sau serviciul de verificare a stării unui certificat.

Arhivarea cheilor publice presupune arhivarea certificatelor care conţin aceste chei.

Fiecare autoritate care emite certificate arhivează cheile publice ale Abonaților către care au fost emise certificatele. Cheile publice ale Autorităţii de Certificare sunt arhivate împreună cu cheile private, în modul descris în Capitolul 6.2.5. Certificatele pot fi, de asemenea, arhivate local de către Abonaţi, în special când acest lucru este cerut de aplicaţiile folosite (de exemplu, sistemele de poştă electronica).

Arhivele cheilor publice trebuie protejate în aşa fel încât să se prevină adăugarea, inserarea, modificarea și ştergerea neautorizată de chei din arhivă. Protecţia este realizată prin autentificarea entităţii care face arhivarea și autorizarea cererilor.

În cadrul certSIGN, numai cheile folosite pentru verificarea semnaturii electronice fac obiectul arhivării. Orice alt tip de chei publice (ex. chei folosite la criptarea mesajelor) sunt distruse imediat după scoaterea lor din depozit.

Administratorul de securitate verifică lunar integritatea arhivelor de chei publice. Scopul acestei verificări este de a asigura faptul că nu sunt goluri în arhive și că certificatele din arhive nu au fost modificate. Mecanismul de verificare a integrităţii arhivelor ţine cont de faptul că perioada de păstrare poate fi mai lungă decât cea a mecanismelor de securitate folosite la crearea arhivelor.

Cheile publice sunt păstrate în arhivele cu certificate digitale 15 ani după momentul expirării.

6.3.2 Perioadele operaționale ale certificatelor și perioadele de utilizare a cheilor private

Perioada de folosire a cheilor publice este definită de valoarea câmpului validitate a fiecărui certificat de cheie publică. Există, de asemenea, și o perioadă de validitate a cheii private. Perioada maxima de utilizare a cheilor Abonaților nu poate depăși de 2 ori durata de viata a unui certificat, care este specificata mai jos.

Valorile standard ale perioadei maxime de folosire a certificatelor Autorităţii de Certificare sunt descrise în Tabelul 6.3.2.1, iar a certificatelor Abonaților sunt descrise în Tabelul 6.3.2.2

Perioada de folosire a certificatelor și a cheilor private corespunzătoare poate fi mai scurtă în cazul suspendării sau revocării unui certificat.

În general, data de început a validităţii certificatului corespunde cu data emiterii sale. Nu este permisă stabilirea acestei date în trecut sau în viitor.

Deţinătorul cheii	**Scopul principal al folosirii cheii**
	RSA pentru semnarea de certificate și CRL
certSIGN ROOT CA	25 ani
certSIGN SSL DV CA Class 3 G2	10 ani

Tabelul 6.3.2.1 Perioada maximă de folosire a certificatelor CA

6.4 Datele de activare

Datele de activare sunt folosite pentru activarea unei chei private cu care operează o Autoritate de Înregistrare, o Autoritate de Certificare, sau un Beneficiar. De obicei sunt folosite pentru autorizarea entităţilor și pentru a controla accesul la cheia privată.

6.4.1 Generarea și instalarea datelor de activare

Datele de activare sunt folosite în două situaţii principale:

- ca element al unei proceduri de autentificare bazată pe unul sau mai mulţi factori (aşa-numitele fraze de autentificare, parolă, cod PIN etc.),
- ca parte a unui secret partajat.

Operatorii Autorităţii de Înregistrare și ai Autorităţilor de Certificare, administratorul, precum și alte persoane care îndeplinesc rolurile descrise în Capitolul 5.2, trebuie să folosească credențiale sigure (token-uri/card-uri) pentru a se identifica și autoriza înșiși pentru rolurile lor. Cheile lor private, care sunt generate în dispozitive calificate pentru semnătură electronică sau in smart-card-uri HSM de către certSIGN, sunt asociate cu datele de activare utilizator (Cod PIN) fiind personalizate și distribuite în mod securizat. certSIGN se asigură că datele de activare ale operatorilor și administratorilor RA și CA sunt menținute și protejate în siguranță de către utilizatori prin proceduri interne care sunt puse la dispoziția acestora.

Secretele partajate folosite pentru protejarea cheii private a Autorităţii de Certificare sunt generate în concordanţă cu cerinţele prezentate în Capitolul 6.2 și păstrate pe carduri criptografice. Cardurile sunt protejate printr-un cod PIN, creat în concordanţă cu cerinţele FIPS-112. Secretele partajate devin date de activare după activarea acestora, de exemplu,

prin introducerea corectă a codului PIN care protejează cardul. certSIGN se asigură că datele de activare asociate cu cheile private CA și cu operațiunile acestora sunt generate, organizate, stocate și arhivate în conformitate cu procedurile descrise în secțiunile 6.1 și 6.2. Instalarea și restaurarea perechilor de chei criptografice într-un dispozitiv criptografic securizat necesită controlul simultan a cel puțin doi angajați cu roluri de încredere.

Când Subiecții își generează cheile private este responsabilitatea lor să genereze și datele de activare (de ex. codul PIN).

6.4.2 Protectia datelor de activare

Protecţia datelor de activare include metodele de control a acestor date prin care se previne dezvăluirea lor. Metodele de control a datelor de activare depind de natura acestora: dacă sunt fraze de autentificare sau dacă acest control este bazat pe distribuirea informaţiilor de activare în secrete partajate. În cazul frazei de autentificare, trebuie impuse recomandările descrise în FIPS 112, pe când protejarea secretelor partajate necesită implementarea standardului FIPS 140.

Se recomandă ca datele de activare folosite pentru activarea cheii private să fie protejate prin controale criptografice și de acces fizic. Datele de activare pot fi datele biometrice sau memorate (nu scrise) de către entitatea de autentificat. Dacă datele de autentificare sunt scrise, nivelul de protecţie trebuie să fie acelaşi cu cel al datelor pe care le protejează prin folosirea cardului criptografic. Mai multe încercări nereuşite de a accesa modulul criptografic trebuie să ducă la blocarea acestuia. Datele de activare stocate nu trebuie să fie păstrate niciodată împreună cu cardul criptografic.

6.4.3 Alte aspecte ale datelor de activare

Datele de activare sunt stocate într-un singur exemplar. Datele de activare care protejează accesul la cheia privată stocată pe carduri criptografice pot fi schimbate periodic. Datele de activare fac obiectul arhivării.

6.5 Controale de Securitate ale computerelor

Acest capitol descrie controalele de securitate informatică ale certSIGN.
Beneficiarul este responsabil de propriile controale de securitate informatică. Aceste aspecte nu sunt acoperite în subcapitolele de mai jos.

6.5.1 Cerințe tehnice specifice ale securității calculatoarelor

Cerinţele tehnice prezentate în acest capitol se referă la controalele de securitate specifice calculatoarelor și aplicaţiilor, folosite în cadrul certSIGN. Măsurile de securitate care protejează sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicaţiilor precum și din punct de vedere fizic.

Calculatoarele aparţinând Autorităţilor de Certificare și componentelor asociate acestora (de exemplu Autoritatea de Înregistrare) dispun de următoarele mijloace de securitate:

- autentificarea obligatorie la nivelul sistemului de operare și al aplicaţiilor,
- control discreţionar al accesului,
- posibilitatea de a fi auditate din punct de vedere al securităţii,

- calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în certSIGN ,
- separarea sarcinilor, conform rolului în cadrul sistemului,
- identificarea și autentificarea rolurilor și a personalului care îndeplineşte aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către procesul autorizat,
- protecția criptografică a schimburilor de informaţii și protecția bazelor de date,
- arhivarea istoricului operaţiunilor executate pe un calculator și a datelor necesare auditării,
- o cale sigură ce permite identificarea și autentificarea rolurilor și a personalului care îndeplineşte aceste roluri,
- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicaţilor și a sistemului de operare,
- mijloace de monitorizare și alertare în cazul accesului neautorizat la resursele de calcul.

Integritatea sistemelor și informațiilor certSIGN este protejată împotriva virușilor, software-urilor rău intenționate și neautorizate.

Mediile utilizate în cadrul sistemelor certSIGN sunt manipulate în siguranță, pentru a proteja mediile împotriva deteriorării, furtului, accesul neautorizat și uzurii morale.

Procedurile de gestionare a mediilor sunt puse în aplicare pentru a proteja împotriva uzurii morale și deteriorării mediilor în perioada de timp în care este obligatorie păstrarea înregistrărilor.

Datele sensibile sunt protejate împotriva relevării prin obiecte de stocare re-utilizate (de exemplu, fișiere șterse), fiind accesibile utilizatorilor neautorizați. În acest scop, trebuie utilizat un software special, cu algoritmi de ștergere siguri pentru mediile de stocare, HSM-urile se resetează, dispozitivele criptografice securizate (token-uri / carduri) trebuie formatate înainte de reutilizare / sau distruse fizic la sfârșitul ciclului lor de viață.

Pentru toate conturile capabile să producă în mod direct emiterea de certificate, este pusă în aplicare autentificarea multi-factor.

6.5.2 Evaluarea securității calculatoarelor

Sistemele de calcul certSIGN respectă cerinţele descrise în standardele ETSI: EN 319 411-1 și CEN CWA 14167 (Cerinţele de Securitate pentru Sistemele de Încredere care asigură Managementul certificatelor pentru Semnatura Electronica).

6.6 Controale de securitate specifice ciclului de viață

certSIGN utilizează sisteme și produse de încredere care sunt protejate împotriva modificărilor și asigură securitatea tehnică și fiabilitatea proceselor susținute de acestea.

6.6.1 Controale specifice dezvoltării sistemului

O analiză a cerințelor de securitate se realizează în etapa de proiectare precum și o definire a cerințelor a oricărui proiect de dezvoltare a sistemelor întreprinse de certSIGN sau în numele certSIGN, pentru a se asigura că securitatea este construită în sistemele informatice.

Înainte de a fi folosită în producţie in cadrul certSIGN, fiecare aplicaţie este instalată astfel încât să se permită controlul versiunii curente și să se prevină instalarea neautorizată de programe sau falsificarea celor existente.

Reguli similare se aplică în cazul înlocuirii componentelor hardware, cum ar fi:

- dispozitivele fizice sunt furnizate în aşa fel încât să poată fi urmărită și evaluată ruta fiecăruia, până la locul său de instalare,
- livrarea unui dispozitiv fizic pentru înlocuire se realizează într-un mod similar celui de livrare al dispozitivului original; înlocuirea se realizează de către personal calificat și de încredere.

6.6.2 Controale specifice managementului securității

Scopul controalelor specifice managementului securităţii este de a superviza funcţionalitatea sistemelor certSIGN, garantând astfel că acestea operează corect și în concordanţă cu configurarea acceptată și implementată.

Controalele aplicate sistemelor certSIGN permit verificarea continuă a integrităţii aplicaţiilor, versiunii și autentificarea și verificarea originii dispozitivelor hardware.

6.6.3 Controale de securitate specifice ciclului de viață

Politicile și procedurile de control al modificărilor sunt aplicate lansărilor, modificărilor și remedierilor de urgență ale oricărui software operațional, precum și modificărilor de configurație care se aplică prin politica de securitate certSIGN.

Configurarea actuală a sistemului certSIGN, orice modificare a lor, precum și a oricărei lansări, modificări și remedieri de urgență ale oricărui software operațional sunt documentate.

certSIGN pune în aplicare procedurile de securitate internă pentru a asigura că:

- patch-urile de securitate sunt aplicate într-un termen rezonabil după ce au venit disponibile;
- patch-urile de securitate nu se aplică dacă ele aduc vulnerabilități sau instabilități suplimentare care depășesc beneficiile aplicării acestora;

Motivele pentru care nu se aplică nici un patch de securitate sunt documentate.

certSIGN implementează o procedură de gestionare a capacității interne care să garanteze că pentru infrastructura TIC dedicată serviciilor de certificare, cererile de capacitate sunt monitorizate și proiecțiile cerințelor de capacitate viitoare sunt făcute pentru a se asigura că puterea de procesare și de stocare adecvate sunt disponibile.

6.7 Controale de securitate a rețelei

certSIGN are implementate mecanisme si proceduri de securitate impotriva tuturor atacurilor specifice resurselor sistemelor informatice si de comunicatii, conforme cu CA/Browser Forum Network and Certificate System Security Requirements. În acest scop și pe baza evaluărilor de risc și a celor mai bune practici, implementăm un set integrat de controale de securitate:

a) Sistemele sunt segmentate în rețele sau zone luând în considerare relația funcțională, logică și fizică (inclusiv de locație) dintre sistemele și servicii de încredere. certSIGN aplică aceleași controale de securitate pentru toate sistemele co-localizate în aceeași zonă.
b) Accesul și comunicarea între zone sunt permise doar persoanelor necesare funcționării serviciilor de certificare. Conexiunile și serviciile care nu sunt necesare sunt interzise în mod explicit sau dezactivate. Setul de reguli stabilite sunt reviziuite periodic.
c) Toate sistemele critice pentru funcționarea serviciilor de certificare sunt păstrate într-una sau mai multe zone securizate)
d) Rețeaua dedicată administrării sistemelor IT și rețeaua operațională sunt separate. Sistemele utilizate pentru administrarea implementării politicii de securitate nu sunt utilizate în alte scopuri. Sistemele de producție ale serviciilor de certificare sunt separate de sistemele utilizate în dezvoltare și testare (de exemplu, sistemele de dezvoltare, testare și planificare).
e) Comunicarea între sisteme de încredere distincte se realizează doar prin intermediul unor canaluri de încredere care sunt distincte logic de alte canale de comunicații și oferă identificarea sigură a punctelor terminale și protecția datelor canalului de modificare sau divulgare.
f) Dacă este necesar un nivel înalt de disponibilitate a accesului extern la un anumit serviciu de certificare, conexiunea externă la rețea este redundantă, pentru a asigura disponibilitatea serviciilor, în cazul unui singur eșec.
g) Se realizează o scanare periodică a vulnerabilității adreselor IP publice și private identificate de certSIGN și se înregistrează dovezi că fiecare scanare a vulnerabilității a fost realizată de către o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.
h) Serviciile de certificare ale certSIGN sunt supuse unui test de penentrare pe sistemele aferente la inițiere și după upgrade-uri de infastructură sau de aplicații sau după modificări pe care certSIGN le consideră importante. Se înregistrează dovezi că fiecare test de penetrare a fost realizat de către o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.

Serverele și stațiile de lucru de încredere ale sistemului certSIGN sunt conectate printr-o rețea locală (LAN) și împărțite în mai multe sub-rețele, cu control al accesului. Accesul din Internet la oricare dintre segmente este protejat printr-un firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului și a filtrelor de trafic aplicate la nivelul routerelor și serviciilor Proxy care protejează domeniile rețelei interne ale certSIGN împotriva accesului neautorizat, inclusiv împotriva accesării de către Subiecți/Beneficiari și terți. Firewall-urile sunt configurate pentru a împiedica toate protocoalele și porturile care nu sunt necesare operării certSIGN CA.

Mijloacele de protecție a securității rețelei acceptă doar mesajele transmise utilizând protocoalele http, https, NTP, POP3 și SMTP. Evenimentele (log-uri) sunt înregistrate în jurnalele de system și permit supervizarea corectitudinii utilizării serviciilor furnizate de certSIGN. Componentele rețelei locale (de exemplu routere) trebuie să fie păstrate într-un

mediu sigur fizic și logic, iar configurațiile acestora se verifică periodic pentru asigurarea conformității cu cerințele specificate de certSIGN.

certSIGN menține și protejează toate sistemele CA cel puțin într-o zonă sigură și are implementată o procedură de securitate care protejează sistemele și comunicațiile dintre sistemele din zonele sigure și cele din zonele de înaltă securitate.

certSIGN configurează toate sistemele CA prin eliminarea sau dezactivarea tuturor conturilor, aplicațiilor, serviciilor, protocoalelor și a porturilor care nu sunt utilizate în operațiunile CA-ului.

certSIGN oferă acces la zonele sigure și la cele de înaltă securitate exclusiv rolurilor de încredere.

6.8 Marcare temporală

Marcarea temporala a jurnalelor de audit este asigurată de un server de timp (NTP) sincronizat cu cel puțin două surse de timp care pot fi sateliți GPS sau UTC (NIMB).

7 Profilul certificatelor, CRL și OCSP

Profilul certificatelor și al Listei de certificate Revocate (CRL) respectă formatul descris în standardul ITU-T X.509 v.3, în timp ce profilul OCSP respectă cerinţele RFC 6960. Informaţiile de mai jos descriu semnificaţia câmpurilor din certificat, CRL și OCSP, standardul aplicat și extensiile folosite de certSIGN.

7.1 Profilul certificatelor

Profilele certificatelor sunt descrise in documentul extern „certSIGN ROOT CA - Anexa Profile.docx”.

7.1.1 Numarul versiunii

Conform cu documentul extern „certSIGN ROOT CA - Anexa Profile.docx”.

7.1.2 Extensia certificatelor

Extensiile sunt descrise in #7.1.2 din documentul extern „certSIGN ROOT CA - Anexa Profile.docx”.

7.1.3 Identificatorul algoritmului semnăturii electronice

Identificatorul de algoritm criptografic este descris in #7.1.3 din documentul extern „certSIGN ROOT CA - Anexa Profile.docx”..

7.1.4 Formate de nume

Conținuul câmpurilor de nume trebuie să fie conforme cu cerințele din secțiunea 3.1 precum și cu cerințele ultimei versiuni publicate a CAB Forum BR.
Numele Emitentului, pentru toate căile de certificare posibile, trebuie să fie identic octet-cu-octet cu Numele Subiectului din certificatul emitentului. Atributele Subiectului nu pot conține doar metadate precum ‘.’ , ‘ - ’ , și ’ ’ (adică spațiu) pentru a indica faptul că valoarea nu există, este incompletă, sau nu este aplicabilă.

7.1.5 Constrângeri privind numele

Nu se aplică.

7.1.6 Identificatorul de obiect pentru politica de identificare

Table 7.1.2 Identificatori de obiect pentru politica de certificare din documentul extern „certSIGN ROOT CA - Anexa Profile.docx”.

7.1.7 Utilizarea extensiei „Policy Constraints”

Nu se aplică.

7.1.8 Sintaxa și semantica calificatorilor de politică

certSIGN emite certificate care conțin un calificator de politică în cadrul extensiei Politicile certificatului. Această extensie conține un calificator CPS care trimite către CPP.

7.1.9 Semantica de procesare pentru extensia critică „Certificate Policies”

Nu se aplică.

7.2 Profilul CRL

Conform cu #7.2 din documentul extern „certSIGN ROOT CA - Anexa Profile.docx”..

7.2.1 Numerele de versiune

Toate CRL-urile emise de certSIGN sunt X.509 versiunea 2.

7.2.2 CRL și extensiile de intrare CRL

Rolul și semnificaţia extensiilor sunt aceleași ca în cazul extensiilor de certificat (vezi Capitolul 7.1.2). Extensiile dintr-o intrare CRL (**crlEntryExtensions**) acceptate de certSIGN- conţin câmpurile descrise in #7.2.2 din documentul extern „certSIGN ROOT CA - Anexa Profile.docx”.

7.3 Profilul OCSP

Protocolul de verificare on-line a stării certificatelor (OCSP) este descris in #7.3 din documentul extern „certSIGN ROOT CA - Anexa Profile.docx”.

7.3.1 Numărul versiunilor

Serverul OCSP care operează în cadrul certSIGN emite confirmări de stare a certificatului în conformitate cu RFC 6960. Singura valoare admisibilă a numărului de versiune este 0 (este echivalentul versiunii v1).

7.3.2 Extensii OCSP

În conformitate cu RFC 6960, serverul OCSP certSIGN acceptă extensiile descrise in #7.3.2 din documentul extern „certSIGN ROOT CA - Anexa Profile.docx”.

8 Auditul de conformitate și alte evaluări

În ceea ce privește auditurile de conformitate și competența, funcționarea consecventă și imparțialitatea conformității organismelor de evaluare care evaluează și certifică conformitatea noastră ca furnizor de servicii de certificare și conformitatea serviciilor noastre de certificare pentru criteriile din Regulamentul 910/2014 și al actelor de punere în aplicare, urmărim cerințele din standardul ETSI EN 319 401. și să se conformeze cu:
- cerințele din cea mai recentă versiune a „Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates".
- cerințele de audit de la cap. 8 din cea mai recentă versiune a „Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates".
- cerințele din partea organismului de supraveghere din România (ADR), deoarece suntem licențiați ca CA în România.

8.1 Frecvența sau circumstanțele de evaluare

Activitățile certSIGN care sprijină furnizarea serviciilor prezentate de acest CPP sunt auditate cel puțin o dată la 12 de luni, care formează o secvență continuă, neîntreruptă, de perioade auditate.

Auditul verifică conformitatea cu standardele tehnice CPP și ETSI 319401, ETSI 319411, CA/B Forum Baseline Requirements.

Auditurile la cerere pot fi realizate la discreția certSIGN, la cererea organismului de supraveghere, astfel cum este definit în Regulamentul UE 910/2014, sau pentru a demonstra conformitatea cu cerințele specifice industriei, juridice sau de afaceri.

8.2 Identitatea / calificările evaluatorului

Evaluarea va fi efectuată de un organism independent de evaluare a conformității, astfel cum este definit în Regulamentul UE 910/2014, conform cu criteriile WebTrust Program pentru CA.

8.3 Relația evaluatorului cu entitatea evaluată

Organismul de evaluare a conformității este un auditor independent, care nu este afiliat direct sau indirect cu certSIGN.

8.4 Subiectele acoperite de evaluare

Auditurile planificate acoperă, dar nu se limitează la, toate aspectele operațiunilor și serviciilor certSIGN specificate în prezentul CPP, în conformitate cu următoarea schemă:.
„WebTrust for CAs" v2.2.2 sau o versiune mai nouă și „WebTrust for CAs SSL Baseline" v2.8 sau o versiune mai nouă.

Auditurile interne și externe se desfăşoară conform regulilor și procedurilor acceptate pe plan internaţional pentru Autoritățile de Certificare și vizează:

- managementul configuratiei sistemelor
- managementul riscurilor operationale si de securitate (evaluari, rapoarte etc)
- securitate procedurala (actualizare fise post personal cu atributii specifice) ....
- securitatea fizică a certSIGN,
- procedurile de verificare a identităţii Abonaților,
- serviciile de certificare și procedurile de furnizare a serviciilor,
- securitatea aplicaţiilor software și a accesului la reţea,
- securitatea personalului certSIGN,

- jurnalele de evenimente și procedurile de monitorizare a sistemului,
- arhivarea și restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru certSIGN,
- înregistrările referitoare la analizele și verificările efectuate pentru aplicaţiile software și dispozitivele hardware.

În cazul terților delegați (DRA) care nu sunt RA de întreprindere, CA obține un raport de audit, care oferă o opinie dacă performanța terțului delegat este conformă cu Declarația privind practicile de certificare a CA. În cazul în care opinia este că terțul delegat (DRA) nu respectă această practică, atunci CA nu va permite terțului delegat să continue să îndeplinească funcțiile delegate.

8.5 Acțiuni întreprinse ca urmare a deficiențelor

Organismul de evaluare a conformității raportează deficiențele și neconformitățile detectate către PPMP. certSIGN și organismul de evaluare a conformității analizează concomitent rezultatele raportului și aprobă un plan de corecție și un interval de timp pentru punerea în aplicare a acestuia.

Este posibil să se efectueze un audit ulterior, pentru a verifica acțiunile de remediere.

8.6 Comunicarea rezultatelor

Organismul de evaluare a conformității comunică raportul de audit conducerii certSIGN și catre PPMB.

Raportul de audit va prevedea în mod explicit că acoperă sistemele și procesele relevante utilizate pentru emiterea tuturor certificatelor care confirma identificatorii de politica declarati. CA pune la dispoziția publicului raportul de audit în cel mult trei luni de la încheierea perioadei de audit. Raportul de audit va fi conform cu cap.8.6 din CABF Baseline Requirements.

Auditorul calificat va furniza o versiune autorizată în limba engleză a informațiilor de audit disponibile publicului, iar AC se va asigura că aceasta este disponibilă publicului.

Raportul de audit va fi disponibil în format PDF și va putea fi căutat în text pentru toate informațiile solicitate. Fiecare amprentă digitală SHA-256 din raportul de audit va fi scrisă cu majuscule și nu va conține două puncte, spații sau linii.

8.7 Audituri interne

În timpul perioadei în care CA eliberează certificate, CA monitorizează respectarea cerințelor sale de bază privind CPP și a Ghidurilor CA / B Forum și controlează strict calitatea serviciilor sale prin efectuarea de audituri interne cel puțin trimestrial pe un eșantion selectat aleatoriu de un certificat sau cel puțin trei la sută din certificatele emise din perioada începând imediat după ce eșantionul auditului intern anterior a fost selectat.

9 Alte elemente de afaceri și legale

9.1 Tarife

Tarifele serviciilor de certificare și ale categoriilor de servicii pentru care sunt percepute taxe sunt publicate în lista de preţuri disponibilă la adresa http://www.certsign.ro. Prețurile sunt formate conform politici interne de preț.

Serviciile oferite de certSIGN sunt stabilite după cum urmează:

- **Servicii de certificare individuale** – preţul este stabilit pentru fiecare serviciu în parte, de exemplu, pentru fiecare certificat vândut sau pentru un număr mic de certificate,
- **Pachete de servicii de certificare** – preţul este stabilit pentru pachete de servicii prestate unei singure entităţi,
- **Servicii prestate pe baza de abonament** – preţul este stabilit pentru servicii prestate periodic; valoarea sumelor plătite depinde de tipul și numărul serviciilor accesate și este utilizat în special pentru serviciile de marcare temporală și de verificare a stării certificatelor prin intermediul protocoalelor OCSP,
- **Servicii indirecte –** preţul este stabilit pentru fiecare serviciu oferit clienţilor săi de un partener certSIGN, care își bazează activitatea pe infrastructura certSIGN.

Plăţile se vor face în numerar, prin ordin de plată, și prin carduri bancare, conform reglementărilor legale în vigoare.

9.1.1 Tarifele serviciilor de emitere și reînnoire a certificatelor digitale

Prețurile sunt stabilite conform politicii interne de preț.

9.1.2 Tarifele serviciilor de acces la certificate

Serviciu gratuit.

9.1.3 Tarifele serviciilor de revocare sau acces la informațiile despre starea certificatelor

Prețurile sunt stabilite conform politicii interne de preț.

9.1.4 Alte tarife

Prețurile sunt stabilite conform politicii interne de preț.

9.1.5 Rambursarea plăților

Plățile pot fi rambursate conform condițiilor contractuale aplicabile..

9.2 Răspunderea financiară

9.2.1 Acoperirea prin asigurare

certSIGN asigură cerințele ultimei versiuni a "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" publicată la: https://cabforum.org/baseline-requirements-documents/ și ale ultimii versiuni publicate ale Mozilla Root Store Policy.

9.2.2 Alte active

Nu se aplică.

9.2.3 Asigurarea sau acoperirea garanției pentru entitățile finale

certSIGN beneficiază de asigurare care acoperă răspunderile profesionale și asigură cerințele ultimii versiuni a "Baseline Requirements for the Issuance and Management of Publicly-

Trusted Certificates" publicată la: https://cabforum.org/baseline-requirements-documents/ și ale ultimii versiuni publicate ale Mozilla Root Store Policy.

9.3 Confidențialitatea informațiilor de afaceri

9.3.1 Scopul informațiilor confidențiale

Toate informaţiile referitoare la Subiect/Beneficiar/Entități Partenere pe care le prelucrează certSIGN sunt obţinute, păstrate și procesate în concordanţă cu prevederile Regulamentului (UE) nr. 910/2014. Relaţiile dintre un Subiect, Beneficiar, o Entitate Parteneră și certSIGN se bazează pe încredere.

O terţă parte poate avea acces doar la informaţiile disponibile public în certificate. Celelalte date furnizate certSIGN nu vor fi dezvăluite în nicio circumstanţă vreunei terţe părţi, în mod voluntar (cu excepţia situaţiilor prevăzute de lege).

O parte va fi exonerată de răspunderea pentru dezvăluirea de informaţii confidenţiale, dacă:

a) informaţia era cunoscută părţii contractante înainte ca ea să fi fost primită de la cealaltă parte contractantă; sau

b) informaţia a fost dezvăluită după ce a fost obţinut acordul scris al celeilalte părţi; sau

c) partea a fost obligată în mod legal să dezvăluie informaţia.

Dezvăluirea oricărei informaţii entităților implicate în îndeplinirea obligaţiilor se va face confidenţial și se va extinde doar asupra informaţiilor necesare pentru îndeplinirea obligaţiilor.

Tipuri de informații considerate a fi confidențiale și private

certSIGN, angajații săi precum și entitățile care desfăşoară activităţi de certificare sunt obligate să păstreze secretul informaţiilor, atât pe durata, cât și după încetarea contractului de muncă, în cazul angajaţilor. Sunt catalogate drept informaţii private sau confidenţiale:

- informaţiile furnizate de Subiecți / Beneficiari, în plus faţă de informaţiile care apar in certificate si in Depozitar; dezvăluirea acestor informaţii se face doar cu aprobare scrisă, în prealabil, din partea proprietarului informaţiei sau în alte condiţii prevăzute de lege;
- conținutul contractelor încheiate cu Subiecții / Beneficiarii sau Entităţile Partenere, conturi bancare, aplicaţiile de înregistrare, emitere, reînnoire, revocare certificate; aceste informații pot fi dezvăluite doar cu aprobarea și în scopul menţionat de proprietarul informaţiilor (de exemplu, Subiectul), cu excepţia informaţiilor incluse în certificate sau din Depozitar, conform prezentului CPP;
- înregistrările corespunzătoare tranzacţiilor din sistem (toate tipurile de tranzacţii, precum și datele pentru controlul tranzacţiilor, aşa numitele loguri ale tranzacţiilor din sistem);
- înregistrările corespunzătoare evenimentelor (log-uri) ce ţin de serviciile de certificare, păstrate de certSIGN;
- rezultatele auditurilor interne și externe, dacă acestea reprezintă o ameninţare pentru securitatea certSIGN;
- planurile în caz de urgenţă;
- informaţiile referitoare la măsurile luate pentru protecția dispozitivelor hardware și aplicaţiilor software, informaţiile referitoare la administrarea serviciilor de certificare și la regulile de înregistrare planificate.

Persoanele care au acces la informaţii confidențiale se supun regulilor referitoare la modul de gestiune a informaţiilor confidențiale și răspund conform legislaţiei în vigoare.

Dezvăluirea motivului pentru care un certificat a fost revocat
Dacă un certificat a fost revocat la cererea unei părţi autorizate alta decat Subiectul, informaţiile cu privire la revocare și motivele acestei revocări sunt comunicate ambelor părţi.
Dezvăluirea Informațiilor Confidențiale Reprezentanților Autorităților Legale
Informaţiile confidenţiale pot fi dezvăluite reprezentanţilor autorităţilor legale numai după îndeplinirea tuturor formalităţilor cerute de legislaţia în vigoare în România.

9.3.2 Informații care nu sunt considerate a fi confidențiale
Informaţiile incluse într-un certificat de către Autoritățile de Certificare emitente, în conformitate cu specificaţiile din Capitolul 7 nu sunt confidențiale. Un Subiect /Beneficiar care aplică pentru obţinerea unui certificat cunoaşte ce fel de informaţii vor fi incluse în certificat și este de acord cu publicarea acestora.
Cu excepția informațiilor prevăzute la alineatul anterior, informaţiile furnizate de / către Subiect / Beneficiar pot fi puse la dispoziţia altor entităţi, doar cu acordul scris al Subiectului / Beneficiarului și în scopul menţionat în contractul încheiat cu Subiectul / Beneficiarului.

9.3.3 Responsibilitatea de a proteja informațiile confidențiale
certSIGN si angajații săi, păstrează confidențialitatea informațiilor atât în timpul prestării serviciilor de certificare, cât și după încetarea valabilității certificatelor.

9.4 Confidențialitatea informațiilor personale
În prestarea serviciilor de încredere certSIGN prelucrează date cu caracter personal ale Subiectului/Beneficiarului în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea dispozițiile de drept intern, a Regulamentului nr. 679/2016 privind protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal și privind libera circulaţie a acestor date și al altor dispoziții de drept al Uniunii referitoare la protecția datelor. Scopul prelucrării datelor cu caracter personal este acela de a presta servicii de certificare.

9.4.1 Planul de asigurare a protectiei datelor cu caracter personal
În prestarea serviciilor de certificare, certSIGN acționează ca operator de date cu caracter personal conform alin.7 al art.4 din Regulamentul nr. 679/2016.
Măsurile de securitate cerute de Regulamentului (UE) nr. 910/2014, Regulamentul nr. 679/2016 și de autoritatea de supraveghere în domeniul prelucrării datelor cu caracter personal sunt puse în aplicare de certSIGN pentru a garanta că:

- sunt luate măsuri tehnice și organizatorice adecvate împotriva prelucrării neautorizate sau ilegale a datelor cu caracter personal și împotriva pierderii accidentale sau distrugerii sau deteriorării datelor cu caracter personal .
- accesul la serviciile certSIGN se referă la prelucrarea doar a acelor date de identificare, care sunt adecvate, pertinente și care nu sunt excesive pentru a acorda acces la serviciul respectiv
- este asigurată confidențialitatea și integritatea datelor de înregistrare: atunci când sunt schimbate cu beneficiarul / subiectul, atunci când sunt schimbate între componentele sistemului certSIGN, precum și atunci când sunt depozitate.

9.4.2 Informatii considerate ca fiind cu caracter personal
Toate informațiile despre Subiect care conduc la identificarea sa sunt considerate ca fiind cu caracter personal.

9.4.3 Informații care nu sunt considerate private

Continutul certificatelor digitale si informațiile accesibile prin Depozitar sunt informații publice.

9.4.4 Responsabilitatea de a proteja informațiile private

certSIGN si angajații săi, se angajează să păstreze confidențialitatea informațiilor cu caracter personal atât în timpul prestării serviciilor de certificare, cat și după încetarea valabilității certificatelor. certSIGN nu va divulga informatii cu carcater personal niciunui tert, pentru niciun motiv, cu exceptia situatiilor in care va fi obligata sa o faca prin lege sau de catre autoritatile competente.

9.4.5 Notificarea persoanelor vizate si consimtamantul acestora pentru utilizarea datelor cu caracter personal

In procesul de emitere a unui certificate digital Subiectii/Beneficiarii sunt informati despre necesitatea utilizarii datelor cu caracter personal care le apartin, in vederea prestarii serviciului si necesitatea acordării consimtamântului. Dacă persoanele vizate nu sunt de acord ca certSIGN sa le prelucreze date, nu pot beneficia de serviciile de certificare.
De asemenea, Subiectii/Beneficiarii au posibilitatea de a opta explicit pentru utilizarea datelor cu caracter personal pentru alte scopuri comunicate în mod expres de certSIGN prin contract sau în alt mod.

9.4.6 Divulgare ca urmare a unui process administrativ sau juridic

certSIGN este exonerat de răspundere pentru dezvăluirea datelor cu caracter personal ale Subiecților/Beneficiarilor în următoarele situații:

- dezvăluirea informațiilor personale față de Organismul de supraveghere conform legislației aplicabile;
- față de instituțiile și organismele abilitate, în baza obligațiilor de drept public pe care certSIGN le are, în conformitate cu prevederile legale;

9.4.7 Alte circumstante pentru divulgare

De asemenea, constituie excepții de la obligația de păstrare a confidențialității datelor cu caracter personal care exonerează certSIGN de răspundere, următoarele situații:

- ✓ dezvăluirea informațiilor personale față de:
  - auditori în cadrul auditurilor la care certSIGN este supus conform prevederilor Regulamentului (UE) nr. 910/2014 în condiții de confidențialitate;
  - firmele de curierat cu care certSIGN are contract, cu acordul Subiectului/Beneficiarului, în cazul în care acesta a optat pentru transmiterea certificatului la adresa de domiciliu sau la o altă adresă comunicată, cu respectarea acelorași obligații privind securitatea datelor cu caracter personal pe care le are și certSIGN;
  - împuterniciți către care am externalizat anumite servicii;
  - firmele afiliate certSIGN
- ✓ informațiile personale care apar în certificate sau în Directoarele publice (Depozitar), cu acordul Subiectului/Beneficiarului;
- ✓ în orice alte situații justificate cu înștiințarea în prealabil a Subiectului/Beneficiarului.

9.5 Drepturile de Proprietate Intelectuală

Toate mărcile, patentele, siglele, licenţele, imaginile grafice etc. folosite de certSIGN sunt și vor rămâne proprietatea intelectuală a deţinătorilor legali ai acestora. certSIGN se obligă să specifice acest lucru conform cerinţelor impuse de deţinători.

Toate mărcile, patentele, siglele, licenţele, imaginile grafice etc., aparţinând certSIGN sunt și rămân proprietatea acesteia, indiferent dacă sunt însoţite sau nu de patente, modele de utilitate, copyright sau altele asemenea și nu pot fi reproduse sau furnizate unei terţe părţi fără acordul prealabil în scris al certSIGN.

9.6 Reprezentări și garanții

9.6.1 Reprezentările și garanțiile CA

certSIGN emite certificate compatibile X509 v3 conforme fie cu cerințele ETSI TS 102 042 sau cu ETSI TS 101 456.

certSIGN garantează că toate cerințele prevăzute în CP-ul aplicabil (și indicate în certificat, în conformitate cu capitolul 7) sunt respectate. De asemenea, își asumă responsabilitatea de a asigura o astfel de conformitate și furnizarea acestor servicii în conformitate cu CPP.

Singura garanție oferită de certSIGN este că procedurile sale sunt puse în aplicare în conformitate cu CPP și cu procedurile de verificare care erau în vigoare, și că toate Certificatele emise cu un identificator de obiect CP (OID) au fost emise în conformitate cu dispozițiile relevante ale CP–ului aplicabil, procedurile de verificare, precum și CPP, după caz, la momentul emiterii.

Garanțiile certificatelor include în mod specific pe cele menționate în cerințele din VAB Forum BR, paragraful 9.6.1.

9.6.2 Reprezentările și garanțiile RA

RA are obligația de a respecta cu strictețe CPP, secțiunea relevantă din CP aplicabil, precum și procedurile interne relevante ale certSIGN.

9.6.3 Reprezentările și garanțiile Beneficiarului

Subiectul acceptă Termenii și Condițiile relevante pentru serviciul furnizat de certSIGN.

Subiectul este de acord cu CPP-ul și cu responsabilitățile, îndatoririle și obligațiile sale relevante, așa cum sunt prevăzute în secțiunile relevante ale CPP și ale CP-ului aplicabil.

Acordul Contractual conține prevederi ce impun Beneficiarului obligațiile și garanțiile din CA/B Forum Baseline Requirements, paragraful 9.6.3

9.6.4 Reprezentările și garanțiile Entităților Partenere

Exemplele de obligații și responsabilități ale Entităților Partenere includ (fără a se limita la):

- Realizarea cu succes a operațiunilor de chei publice, înainte de a se baza pe un Certificat certSIGN,
- Validarea unui Certificat certSIGN utilizând CRL-urile sau serviciile de validare a certificatelor furnizate de certSIGN,
- Încetarea imediată a oricărei utilizări a unui Certificat certSIGN în cazul în care a fost revocat sau atunci când a expirat.
- Luarea la cunoștință a prevederilor prezentului CPP, a garanțiilor și limitelor răspunderii Certsign SA

9.6.5 Reprezentările și garanțiile altor participanți
Nu se aplică.

9.7 Declinarea garanțiilor
Cu excepția celor prevăzute în mod expres în altă parte decât în CPP, în CP-ul aplicabil și în legislația aplicabilă, certSIGN neagă toate garanțiile și obligațiile de orice tip, inclusiv orice garanție de comercializare, orice garanție de adecvare pentru un anumit scop, precum și orice garanție a exactității informațiilor oferite (cu excepția faptului că a venit dintr-o sursă autorizată) și nu își asumă nicio răspundere pentru neglijența și neatenția Subiecților, Beneficiarilor și Entităților Partenere.

9.8 Limitarea răspunderii
In măsura permisă de legea română, în nici un caz (cu excepția fraudelor sau a faptelor ilicite săvârșite cu intenție de certSIGN) certSIGN nu va fi răspunzătoare pentru:

- Orice pierderi de profit, de venit sau afaceri;
- Orice pierderi de date;
- Orice daune indirecte, subsecvente sau punitive ce decurg din sau în legătură cu utilizarea, livrarea, licența, și performanța sau non-performanța certificatelor sau a semnăturilor electronice;
- Orice alte daune.

certSIGN nu răspunde față de nicio o persoană (beneficiar, subiect, terț, entitate parteneră etc.) in cazul în care datele prezentate la emiterea certificatelor sunt false, inexacte, incomplete sau expirate sau sunt prezentate acte de identitate false. certSIGN nu răspunde pentru daunele suportate de Beneficiar sau terți provocate de utilizarea certificatelor emise de certSIGN de către Subiect.

În orice caz răspunderea certSIGN în cazul unei cereri de despăgubire va fi limitată la valoarea certificatelor implicate în producerea unui prejudiciu

9.9 Despăgubiri
certSIGN nu își asumă nicio responsabilitate financiară pentru Certificatele, CRL-urile și serviciile asociate menționate în CPP, utilizate în mod necorespunzător.

certSIGN acționează conform prevederilor paragrafelor 9.9 "Indemnification by CAs"și 18 "Liability and Indemnification" din CA/B Forum Baseline Requirements.

9.10 Termeni și încetarea

9.10.1 Termenii
Prezentul CPP și orice modificări ale acestuia vor intra în vigoare după publicare în Depozitar și în conformitate cu secțiunea 9.12.2 și vor rămâne în vigoare perpetuu până la încetarea lor în conformitate cu prezenta secțiune 9.10.

9.10.2 Încetarea
CPP rămâne în vigoare până la înlocuirea cu o nouă versiune.

9.10.3 Efectul terminării și supraviețuirii
Condițiile și efectul care rezultă din terminarea acestui CPP vor fi comunicate prin intermediul site-ului web certSIGN. Această comunicare va evidenția dispozițiile care pot supraviețui

rezilierii acestui CPP și vor rămâne în vigoare. Responsabilitățile de protejare a informațiilor confidențiale și a informațiilor personale trebuie să supraviețuiască încetării, iar termenii și condițiile pentru toate certificatele existente vor rămâne valabile pentru restul perioadelor de valabilitate ale acestor certificate.

9.11 Notificări individuale și comunicarea cu participanții

Toate notificările și alte comunicări care pot sau trebuie date, servite sau trimise în mod obligatoriu în temeiul CPP se vor face în scris și se vor transmite, cu excepția celor prevăzute în mod expres în CPP, fie prin (i) adresa de e-mail înregistrată, confirmare de primire, poșta preplătită, (ii) un serviciu de curierat "în 24 de ore" sau expres recunoscut international, (iii) livrarea în mână (iv) transmiterea prin fax, considerată a fi primită la livrarea efectivă sau la finalizarea fax-ului, sau (v) în format electronic, semnat cu o semnătură electronică calificată și să fie adresată certSIGN, folosind datele de contact furnizate în capitolul 1.5.1 din prezentul document.

9.12 Amendamente

9.12.1 Procedura pentru amendamente

certSIGN este responsabilă, prin Comitetul de Management al Politicilor (CMMP) și Procedurilor, de aprobarea și modificarea prezentului CPP. CPP-se revizuiește cel puțin odată pe an.

Singurele modificări pe care le poate face CMMP acestor specificații CPP fără notificare sunt modificări minore care nu afectează nivelul de încredere al acestui CPP, de exemplu, corecturi editoriale sau tipografice sau modificări ale detaliilor de contact.

Erorile, actualizările sau sugestiile de modificare a acestui document vor fi comunicate așa cum este menționat în prezentul CPP, secțiunea 1.5.4. O astfel de comunicare va include o descriere a schimbării, o justificare a schimbării, precum și informațiile de contact ale persoanei care solicită modificarea.

CMMP va accepta, modifică sau respinge modificarea propusă după finalizarea unei faze de revizuire.

Orice modificări la CPS sunt aprobate de CMMP și sunt anunțate clienților certSIGN. Subiecții /Beneficiarii trebuie să respecte numai cerințele CPP aplicabile în prezent.

9.12.2 Mecanismul de notificare și perioada

Toate modificările aduse prezentului CPP aflate în analiza CMMP vor fi distribuite părților interesate înainte de publicare. Data intrării în vigoare este indicată pe pagina titlului prezentului CPP.

9.12.3 Circumstanțele în care OID trebuie schimbat

Nu se aplică.

9.13 Procedurile de soluționare a litigiilor

Toate disputele asociate prezentului CPP vor fi rezolvate în conformitate cu legile din România.

9.14 Legea aplicabilă

Legea română guvernează aplicabilitatea, construirea, interpretarea, și validitatea prezentului CPP (fără a avea ca efect orice conflict de prevedere a legii care ar determina aplicarea altor legi).

9.15 Conformitatea cu legea aplicabilă

Prezentul CPP și furnizarea serviciilor certSIGN sunt conforme cu legile române relevante și aplicabile și regulamentul EU 910/2014.

9.16 Prevederi diverse

certSIGN asigura accesul nerestrictionat la serviciile furnizate pentru persoanele cu disabilitati in conformitate cu legislatia si standardele in vigoare.

9.16.1 Întregul Acord

Nu se stipulează.

9.16.2 Cesiunea

Nu se stipulează.

9.16.3 Anulabilitatea

CA acționează conform prevederilor din paragraful "9.16.3 Severability" din CA/B Forum Baseline Requirements.

9.16.4 Executarea

Nu se stipulează.

9.16.5 Forța Majoră

CA acționează conformi legilor române cu privire la Forța Majoră.

9.17 Alte prevederi

Nu se aplică.