Codul de Practici și Proceduri certSIGN ROOT CA G2

Versiunea 2.28

Data: 31 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

Istoric document

Ver.	Data efectivă	Motiv	Persoana care a făcut modificarea
1.0	28 Februarie 2017	Publicarea primei versiuni	Ofițer Securitate Informatică
2.0	15 Martie 2017	A doua versiune, după auditul intermediar	Ofițer Securitate Informatică
2.1	3 Aprilie 2017	Actualizare minoră pentru clarificare	Ofițer Securitate Informatică
2.2	5 Februarie 2018	Revizuire anuală	Ofițer Securitate Informatică
2.3	7 Mai 2018	Actualizare CPP conform GDPR	Manager politici PKI
2.4	18 Septembrie 2018	Clarificare cerinte referitoare la "Unicitatea numelui"	Manager politici PKI
2.5	25 Septembrie 2018	Semnatura la distanta cu RQSCD	Manager politici PKI
2.6	1 Noiembrie 2018	Actualizare noi profile de certificate privind semnatura la distanta	Manager politici PKI
2.7	5 Noiembrie 2018	Actualizare determinata de schimbarea sediului	Manager politici PKI
2.8	14 Ianuarie 2019	Revizuire anuala	Manager politici PKI
2.9	9 Martie 2019	Actualizare pentru adaugare profile certificate (Trusted List)	Manager politici PKI
2.10	1 Aprilie 2019	Actualizare minora pentru clarificare	Manager politici PKI
2.11	8 Aprilie 2019	Actualizare pentru adaugare profile certificate (dnQualifier)	Manager politici PKI
2.12	22 Iulie 2019	Actualizare pentru adaugare profile certificate (PSD2)	Manager politici PKI
2.13	31 Ianuarie 2020	Revizuire anuală	Manager politici PKI
2.14	3 Februarie 2020	Actualizare pentru adaugare profile certificate calificate pentru sigilii	Manager politici PKI
2.15	15 Aprilie 2020	Multiple actualizări minore pentru conformitate cu BR 1.6.9 & Mozilla	Manager Politici PKI
2.16	31 Iulie 2020	Aăugare OID cu pseudonim	Manager Politici PKI
2.17	30 Septembrie 2020	cf. CAB BR 1.7.2 CRL/OCSP 7.2/7.3	Manager Politici PKI
2.18	7 Ianuarie 2021	Actualizare Schema CA / OIDs	Manager Politici PKI
2.19	29 Ianuarie 2021	Actualizare anuală	Manager Politici PKI
2.20	31 Ianuarie 2022	Actualizare anuală	Manager Politici PKI
2.21	31 Ianuarie 2023	Actualizare anuală	Manager Politici PKI
2.22	31 Iulie 2023	Actualizări conform CABF BR v2.0.0	Manager Politici PKI
2.23	31 Ianuarie 2024	Actualizare anuală	Manager Politici PKI
2.24	15 August 2024	Actualizare profil OCSP & altele	Manager Politici PKI
2.25	15 Ianuarie 2025	Actualizare anuală	Manager Politici PKI
2.26	30 Aprilie 2025	Actualizari minore	Manager Politici PKI
2.27	15 Ianuarie 2026	Actualizare anuală	Manager Politici PKI
2.28	31 Ianuarie 2026	Adaugare Web CA G2	Manager Politici PKI

Acest document a fost creat și este proprietatea:

Proprietar	Autor	Data creării
BU Servicii de Incredere	Ofițer Securitate Informatică	Decembrie 2016

Lista de distribuție

Destinație	Data distribuirii
Public-Internet	Februarie 2017

Public-Internet	Martie 2017
Public-Internet	Aprilie 2017
Public-Internet	Februarie 2018
Public-Internet	Mai 2018
Public-Internet	Septembrie 2018
Public-Internet	Noiembrie 2018
Public-Internet	Noiembrie 2018
Public-Internet	Ianuarie 2019
Public-Internet	Martie 2019
Public-Internet	Aprilie 2019
Public-Internet	Iulie 2019
Public-Internet	Ianuarie 2020
Public-Internet	Februarie 2020
Public-Internet	Aprilie 2020
Public-Internet	Iulie 2020
Public-Internet	Septembrie 2020
Public-Internet	Ianuarie 2021
Public-Internet	Ianuarie 2022
Public-Internet	Ianuarie 2023
Public-Internet	Iulie 2023
Public-Internet	Ianuarie 2024
Public-Internet	August 2024
Public-Internet	Ianuarie 2025
Public-Internet	Aprilie 2025
Public-Internet	Ianuarie 2026

Acest document a fost aprobat de:

Versiune	Nume	Data
1	Comitet de Management al Politicilor și Procedurilor	Februarie 2017
2	Comitet de Management al Politicilor și Procedurilor	Martie 2017
2.1	Comitet de Management al Politicilor și Procedurilor	Aprilie 2017
2.2	Comitet de Management al Politicilor și Procedurilor	Februarie 2018
2.3	Comitet de Management al Politicilor și Procedurilor	Mai 2018
2.4	Comitet de Management al Politicilor și Procedurilor	Septembrie 2018
2.5	Comitet de Management al Politicilor și Procedurilor	Septembrie 2018
2.6	Comitet de Management al Politicilor și Procedurilor	Noiembrie 2018
2.7	Comitet de Management al Politicilor și Procedurilor	Noiembrie 2018
2.8	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2019
2.9	Comitet de Management al Politicilor și Procedurilor	Martie 2019
2.1	Comitet de Management al Politicilor și Procedurilor	Aprilie 2019
2.11	Comitet de Management al Politicilor și Procedurilor	Aprilie 2019
2.12	Comitet de Management al Politicilor și Procedurilor	Iulie 2019
2.13	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2020
2.14	Comitet de Management al Politicilor și Procedurilor	Februarie 2020
2.15	Comitet de Management al Politicilor și Procedurilor	Aprilie 2020
2.16	Comitet de Management al Politicilor și Procedurilor	Iulie 2020
2.17	Comitet de Management al Politicilor și Procedurilor	Septembrie 2020
2.18	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2021
2.19	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2021

Versiune	Nume	Data
2.20	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2022
2.21	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2023
2.22	Comitet de Management al Politicilor și Procedurilor	Iulie 2023
2.23	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2024
2.24	Comitet de Management al Politicilor și Procedurilor	August 2024
2.25	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2025
2.26	Comitet de Management al Politicilor și Procedurilor	Aprilie 2025
2.27	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2026
2.28	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2026

Cuprins

1 Introducere 10
1.1 Descriere Generală 10
1.2 Denumirea documentului și identificarea 10
1.3 Participanţii PKI 10
1.3.1 Autoritățile de certificare 11
1.3.2 Autoritățile de Înregistrare 11
1.3.3 Beneficiarii 12
1.3.4 Entitățile partenere 12
1.3.5 Alți participanți 12
1.4 Utilizarea certificatului 12
1.4.1 Utilizări admise ale certificatului 13
1.4.2 Utilizări interzise ale certificatului 13
1.5 Administrarea politicii 13
1.5.1 Organizația care administrează documentul 13
1.5.2 Persoana de contact 13
1.5.3 Persoana care decide conformitatea CPP cu politica 14
1.5.4 Procedurile de aprobare a CPP 14
1.6 Definiții și acronime 15
2 Publicare și Responsabilități Depozitar 17
2.1 Depozitar 17
2.2 Publicarea Informațiilor din Certificat 17
2.3 Timpul sau frecvența publicării 18
2.4 Controlul accesului la Depozitare 18
3 Identificarea și autentificarea 19
3.1 Denumirea 19
3.1.1 Tipuri de nume 19
3.1.2 Nevoia ca numele sa aibă inţeles logic 19
3.1.3 Anonimatul sau pseudonimitatea beneficiarilor 20
3.1.4 Reguli de interpretare a formatelor de nume 20
3.1.5 Unicitatea numelor 20
3.1.6 Recunoașterea, autentificarea și rolul mărcilor comerciale 20
3.2 Validarea Inițială a Identității 20
3.2.1 Dovada Posesiei Cheii Private 20
3.2.2 Autentificarea identitatii organizatiei 20
3.2.3 Autentificarea Identității Persoanelor Fizice 20
3.2.4 Informațiile neverificate ale Beneficiarului 20
3.2.5 Validarea autorității 20
3.2.6 Criterii pentru interoperare 20
3.3 Identificarea și Autentificarea pentru cererile de re-key 20
3.3.1 Identificarea și Autentificarea pentru re-key de rutină 20
3.3.2 Identificarea și Autentificarea pentru re-key după revocare 21
3.4 Identificarea și autentificarea pentru cererile de revocare 21
4 Cerinţe operaționale privind ciclul de viață al certificatului 22
4.1 Aria de aplicabilitate a certificatelor 22
4.1.1 Cine poate trimite o cerere de certificat 22
4.1.2 Procesul de înregistrare și responsabilitățile 22
4.2 Procesarea Cererilor de Certificate 22
4.2.1 Îndeplinirea funcțiilor de identificare și autentificare 22
4.2.2 Aprobarea sau respingerea cererilor de certificate 22
4.2.3 Timpul de procesare a cererilor de certificate 22
4.3 Emiterea certificatelor 22
4.3.1 Acțiunile CA în timpul emiterii certificatelor 22
4.3.2 Notificarea Subiectului de către CA cu privire la emitere certificatului 23
4.4 Acceptarea Certificatului 23

4.4.1 Conduita care constituie acceptarea certificatului 23
4.4.2 Publicarea certificatului de către CA 23
4.4.3 Notificarea de către CA a altor entități cu privire la emiterea certificatului ... 23
4.5 Utilizarea Perechii de Chei și a Certificatului 23
4.5.1 Utilizarea Cheii private a și certificatului Beneficiarului 23
4.5.2 Utilizarea cheii publice și a certificatului unei Entități Partenere 23
4.6 Reînnoirea Certificatului 24
4.7 Re-key-ul Certificatului 24
4.8 Modificarea Certificatului 24
4.9 Revocarea și Suspendarea Certificatului 24
4.9.1 Circumstanțele revocării unui certificat 24
4.9.2 Cine poate solicita revocarea certificatelor 25
4.9.3 Procedura de revocare a certificatelor 25
4.9.4 Perioada de grație a cererii de revocare 25
4.9.5 Timpul în care CA trebuie să proceseze cererea de revocare 25
4.9.6 Verificarea cerințelor de revocare pentru Entitățile Partenere 26
4.9.7 Frecvența de emitere a CRL-urilor 26
4.9.8 Latența maximă pentru CRL-uri 26
4.9.9 Disponibilitatea verificării on-line a revocării/stării 26
4.9.10 Verificarea on-line a cerințelor de revocare 26
4.9.11 Alte forme disponibile pentru anunțarea revocării 27
4.9.12 Cerințe special în cazul compromiterii re key 27
4.9.13 Circumstanțe pentru suspendare 27
4.9.14 Cine poate solicita suspendarea 27
4.9.15 Procedura de solicitare a suspendării 27
4.9.16 Limitări ale perioadei de suspendare 27
4.10 Servicii privind starea certificatelor 27
4.10.1 Caracteristici operaționale 27
4.10.2 Disponibilitatea serviciului 27
4.10.3 Elemente opționale 28
4.11 Încetarea abonamentului 28
4.12 Custodie și recuperare chei 28
5 Facilitate, Management și Controale Operaționale 29
5.1 Controale fizice 30
5.1.1 Amplasarea și construcția sediului 30
5.1.2 Accesul fizic 31
5.1.3 Alimentarea cu curent și aerul conditionat 31
5.1.4 Expunerea la apă 32
5.1.5 Prevenirea și protecția împotriva incendiilor 32
5.1.6 Depozitarea mediilor de stocare a informaţiilor 32
5.1.7 Aruncarea deșeurilor 32
5.1.8 Stocarea copiilor de siguranță în afara locației 32
5.2 Controale procedurale 32
5.2.1 Roluri de încredere 32
5.2.2 Numărul de persoane necesare pentru fiecare sarcină 33
5.2.3 Identificarea și autentificarea pentru fiecare rol 33
5.2.4 Rolurile care necesită separarea sarcinilor 34
5.3 Controlul personalului 34
5.3.1 Calificări, experință și aprobări necesare 34
5.3.2 Proceduri de verificare a antecedentelor 34
5.3.3 Cerinţele de pregătire a personalului 35
5.3.4 Frecvența și cerințele stagiilor de pregătire 35
5.3.5 Frecvența și secvența rotației posturilor 35
5.3.6 Sancțiunile pentru acțiunile neautorizate 35
5.3.7 Cerințele contractanților independenți 35

5.3.8 Documentația oferită personalului 35
5.4 Procedurile de înregistrare a datelor de audit 35
5.4.1 Tipuri de Evenimente Înregistrate 36
5.4.2 Frecvența procesării jurnalelor de evenimente 38
5.4.3 Perioada de pastrare a log-urilor de audit 38
5.4.4 Protecția jurnalelor de evenimente 38
5.4.5 Procedura de backup a log-urilor de audit 39
5.4.6 Sistemul de colectare a datelor pentru audit (intern&extern) 39
5.4.7 Notificarea sursei care a generat 39
5.4.8 Evaluări de vulnerabilitate 39
5.5 Arhivarea înregistrărilor 39
5.5.1 Tipurile de date arhivate 40
5.5.2 Perioada de retenție a arhivei 40
5.5.3 Protecția arhivei 40
5.5.4 Procedurile de back-up al arhivei 40
5.5.5 Cerințe privind marcarea temporală a înregistrărilor 40
5.5.6 Sistemul de colectare al arhivei (intern sau extern) 40
5.5.7 Procedura de obținere și verificare a informațiilor arhivate 40
5.6 Schimbarea cheilor 41
5.7 Compromiterea și recuperare în caz de dezastru 41
5.7.1 Procedurile de administrare a a incidentelor și compromiterilor 41
5.7.2 Compromiterea resurselor de calcul, a aplicațiilor software și/sau datelor ... 42
5.7.3 Proceduri care se aplică la compromiterea cheii private a unei entitati 43
5.7.4 Capacități de Continuitate a afacerii în caz de dezastru 43
5.8 Încetarea activității Autorității de Certificare sau a Autorității de Înregistrare 44
5.9 Lanțul de aprovizionare 45
6 Controale tehnice de securitate 46
6.1 Generarea și instalarea perechii de chei 46
6.1.1 Generarea perechilor de chei 46
6.1.2 Distribuirea Cheii Private către Beneficiar 48
6.1.3 Distribuirea Cheii Publice către emitentul certificatului 48
6.1.4 Distribuirea Cheii Publice a Autorității Certificare către Entitățile Partenere .. 48
6.1.5 Marimea cheilor 48
6.1.6 Parametrii de generare a Cheilor Publice și verificarea calității 48
6.1.7 Scopurile în care pot fi utilizate cheile (conform câmpului de utilizare a cheilor X.509 v3) 49
6.2 Protecția cheii private și controalele modulului criptografic 49
6.2.1 Controalele și standardele modulelor criptografice 50
6.2.2 Control multi-persoană (n din m) al cheilor private 50
6.2.3 Custodia Cheii Private 51
6.2.4 Copia de siguranță a cheii private 51
6.2.5 Arhivarea Cheii Private 52
6.2.6 Transferul Cheii Private într-un sau dintr-un modul criptografic 52
6.2.7 Stocarea cheilor private pe modul criptografic 52
6.2.8 Metoda de activare a cheii private 53
6.2.9 Metoda de dezactivare a cheii private 53
6.2.10 Metoda de distrugere a cheii private 53
6.2.11 Evaluarea Modulului Criptografic 53
6.3 Alte aspecte legate de managementul perechilor de chei 53
6.3.1 Arhivarea cheilor publice 54
6.3.2 Perioadele operaționale ale certificatelor și perioadele de utilizare a cheilor private 54
6.4 Datele de activare 55
6.4.1 Generarea și instalarea datelor de activare 55
6.4.2 Protejarea datelor de activare 55

6.4.3 Alte aspecte ale datelor de activare 55
6.5 Controale de securitate a calculatoarelor 55
6.5.1 Cerințe tehnice specifice ale securității calculatoarelor 56
6.5.2 Evaluarea securității calculatoarelor 56
6.6 Controale de securitate specifice ciclului de viață 56
6.6.1 Controale specifice dezvoltării sistemului 57
6.6.2 Controale specifice managementului securității 57
6.6.3 Controale de securitate specifice ciclului de viață 57
6.7 Controale de securitate a rețelei 57
6.8 Marcare temporală 59
7 Profilul certificatelor, CRL și OCSP 60
7.1 Profilul certificatului 60
7.1.1 Numerele de versiune 61
7.1.2 Extensii de certificate 61
7.1.3 Identificatorul algoritmului semnăturii electronice 62
7.1.4 Formate de nume 63
7.1.5 Constrangeri privind numele 63
7.1.6 Identificatorul obiectului politicii de identificare 63
7.1.7 Utilizarea extensiei Constrângeri de politică 63
7.1.8 Sintaxa și semantica calificatorilor de politică 63
7.1.9 Semantica de procesare pentru extensia Politici critice de certificare 63
7.2 Profilul CRL 63
7.2.1 Numerele de versiune 63
7.2.2 CRL și extensiile de intrare CRL 63
7.3 Profilul OCSP 64
7.3.1 Numarul versiunilor 65
7.3.2 Extensii OCSP 65
8 Auditul de conformitate și alte evaluări 66
8.1 Frecvența sau circumstanțele de evaluare 66
8.2 Identitatea / calificările evaluatorului 66
8.3 Relația evaluatorului cu entitatea evaluată 66
8.4 Subiectele acoperite de evaluare 66
8.5 Acțiuni întreprinse ca urmare a deficienței 67
8.6 Comunicarea rezultatelor 67
8.7 Audit intern 67
9 Alte elemente de afaceri și legale 68
9.1 Tarife 68
9.1.1 Tarifele serviciilor de emitere și reînnoire a certificatelor digitale 68
9.1.2 Tarifele serviciilor de acces la certificate 68
9.1.3 Tarifele serviciilor de revocare sau acces la informațiile despre starea certificatelor 68
9.1.4 Alte tarife 68
9.1.5 Rambursarea plăților 68
9.2 Răspunderea financiară 68
9.2.1 Acoperirea garantiei 68
9.2.2 Alte active 68
9.2.3 Asigurarea sau acoperirea garanției pentru entitățile finale 68
9.3 Confidențialitatea informațiilor de afaceri 68
9.3.1 Scopul informaţiilor confidenţiale 68
9.3.2 Informații care nu sunt considerate a fi confidențiale 70
9.3.3 Responsibilitatea de a proteja informațiile confidențiale 70
9.4 Confidențialitatea informațiilor personale 70
9.4.1 Planul de asigurare a protectiei datelor cu caracter personal 70
9.4.2 Informatii considerate ca fiind cu caracter personal 70
9.4.3 Informații care nu sunt considerate private 70

9.4.4 Responsabilitatea de a proteja informațiile private 71
9.4.5 Notificarea persoanelor vizate si consimtamantul acestora pentru utilizarea datelor cu caracter personal 71
9.4.6 Divulgare ca urmare a unui proces administrativ sau juridic 71
9.4.7 Alte circumstante pentru divulgare 71
9.5 Drepturile de Proprietate Intelectuală 72
9.6 Declarații și garanții 72
9.6.1 Declarațiile și garanțiile CA 72
9.6.2 Declarațiile și garanțiile RA 72
9.6.3 Declarațiile și garanțiile Subiectului 72
9.6.4 Declarațiile și garanțiile Entităților Partenere 72
9.6.5 Declarațiile și garanțiile altor participanti 73
9.7 Declinarea garanțiilor 73
9.8 Limitarea răspunderii 73
9.9 Despăgubiri 73
9.10 Termeni și încetarea 73
9.10.1 Termenii 73
9.10.2 Incetarea 73
9.10.3 Efectul terminării și supraviețuirii 73
9.11 Notificări individuale și comunicarea cu participanții 73
9.12 Amendamente 74
9.12.1 Procedura pentru amendamente 74
9.12.2 Mecanismul de notificare și perioada 74
9.12.3 Circumstanțele în care OID trebuie schimbat 74
9.13 Procedurile de soluționare a litigiilor 74
9.14 Legea aplicabilă 74
9.15 Conformitatea cu legea aplicabilă 74
9.16 Prevederi diverse 74
9.17 Alte prevederi 75

1 Introducere

Codul de practici și proceduri al certSIGN ROOT CA G2 (denumit în continuare **CPP ROOT CA G2 sau CPP**) detaliază politica de certificare și practicile pe care certSIGN le aplică pentru emiterea certificatelor digitale de către CA Root G2 pentru autoritățile de certificare subordonate.

Structura și continutul CPP ROOT CA G2 sunt în conformitate cu recomandarile RFC 3647, ETSI EN 319 411-1 și ETSI EN 319 411-2.

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

Funcţionarea certSIGN, a Autoritaţilor de certificare și a Entităţilor Partenere depinde de **CPP ROOT CA G2** pentru emiterea de certificate digitale către autoritățile de certificare subordonate. Deasemenea, acest document descrie regulile de prestare a serviciilor de certificare cum ar fi înregistrarea Beneficiarilor, certificarea cheilor publice, înnoirea cheilor şi revocarea certificatelor.

1.2 Denumirea documentului și identificarea

Titlul acestui document este **Codul de practici și proceduri certSIGN ROOT CA G2**, denumit în continuare **CPP ROOT CA G2 sau CPP**.

Versiunea electronică a acestui document este disponibilă în Depozitar la adresa: https://www.certsign.ro/ro/depozitar/.

1.3 Participanţii PKI

CPP ROOT CA G2 reglementează cele mai importante relații dintre entități aparținând certSIGN, echipele de consultanți (inclusiv auditorii) și clienții (utilizatorii serviciilor furnizate):

- Autoritățile de certificare:
  - certSIGN ROOT CA G2
  - certSIGN Public CA
  - certSIGN Qualified CA
  - certSIGN Web CA
  - certSIGN Web CA G2
- Autoritatea de Înregistrare,
- Depozitar,
- Comitetul de Management al Politicilor și Procedurilor
- Autoritati ce emit confirmari electronice de ne-repudiere,
- Subiecții,
- Beneficiarii,
- Entitățile Partenere,
- Furnizorii relevanți ai certSIGN din punct de vedere al emiterii și managementului certificatelor digitale
- Auditorii

certSIGN oferă servicii de certificare pentru orice persoană fizică sau juridică care este de accord cu prevederile prezentului CPP. Scopul acestor practici (ce includ procedurile de generare a cheilor, procedurile de emitere a certificatelor şi securitatea sistemului

informaţional) este acela de a garanta utilizatorilor serviciilor certSIGN că nivelele de credibilitate declarate ale certificatelor emise corespund practicilor Autorităţii de certificare.

1.3.1 Autoritățile de certificare

certSIGN ROOT CA G2 este Autoritatea de certificare Primară pentru domeniul certSIGN. Toate autorităţile de certificare din domeniu sunt subordonate certSIGN ROOT CA G2 (Figure 1).

În prezent, urmatoarele Autoritati de Certificare sunt subordonate certSIGN ROOT CA G2:

- certSIGN Public CA identificat cu urmatorul OID: 1.3.6.1.4.1.25017.3.1.2
- certSIGN Qualified CA identificat cu urmatorul OID: 1.3.6.1.4.1.25017.3.1.3
- certSIGN Web CA identificat cu urmatorul OID: 1.3.6.1.4.1.25017.3.1.4
- certSIGN Web CA G2 identificat cu urmatorul OID: 1.3.6.1.4.1.25017.3.1.5

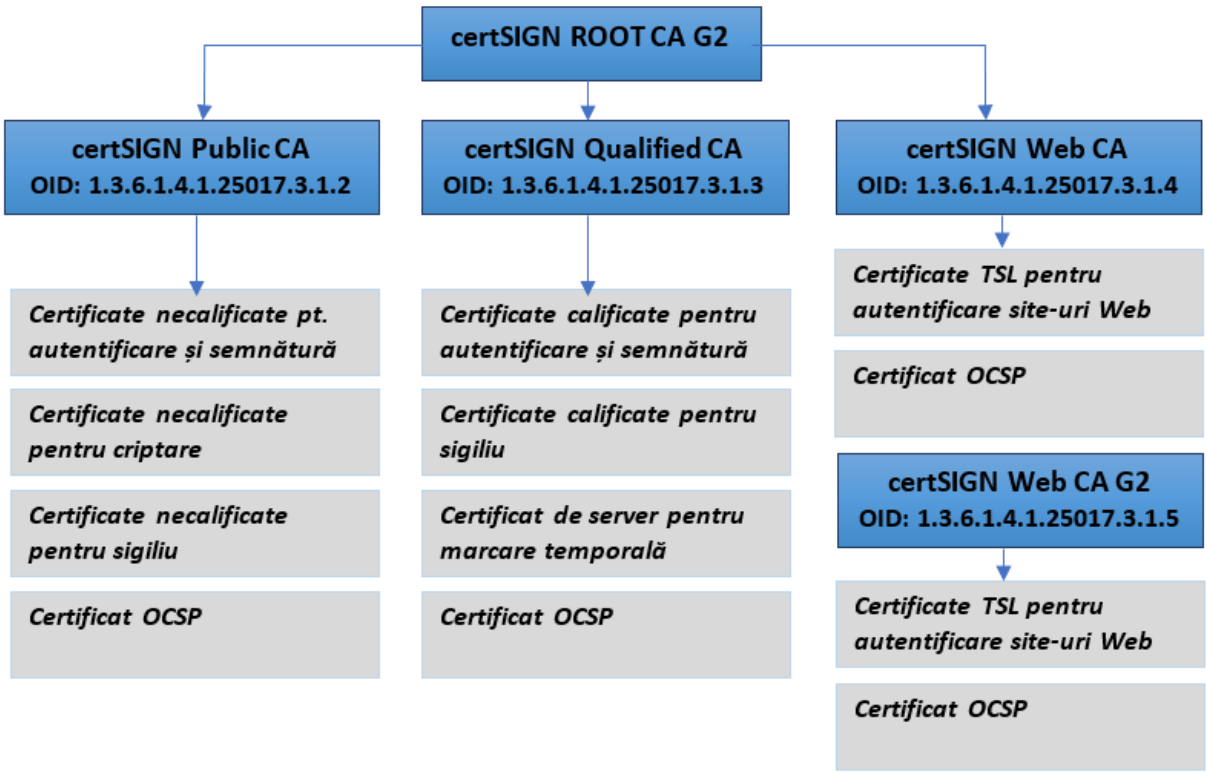

Figure 1: Structura domeniului de certificare certSIGN ROOT CA G2

Autoritatea de certificare primară, **certSIGN ROOT CA G2**, poate înregistra și emite certificate numai către Autoritățile de certificare și autoritățile care emit confirmări electronice de ne-repudiere ce aparțin domeniului certSIGN. Înainte de începerea activității, toate Autoritățile de Certificare subordonate vor trimite o solicitare către Autoritatea de certificare Primară, **certSIGN ROOT CA G2** pentru înregistrarea și emiterea cheii publice. (vezi și procedurile descrise în capitolul 6.1 al prezentului document).

1.3.2 Autoritățile de Înregistrare

Autoritatea de Înregistrare primeşte, verifică și aprobă sau respinge cererile de înregistrare şi emitere de certificate, de rekey sau revocare a certificatelor. Verificarea cererilor are ca scop autentificarea (pe baza documentelor incluse în cereri) atât a solicitantului cât și a datelor incluse în cerere. Autoritatea de Înregistrare poate trimite cereri către Autoritatea de

Certificare corespunzătoare pentru a anula cererea de înregistrare a unui Beneficiar şi pentru a retrage certificatul acestuia.

Autoritatea de Înregistrare este operată de certSIGN.

1.3.3 Beneficiarii

Beneficiarul este certSIGN, ca operator al autorităților de certificare subordonate certSIGN ROOT CA G2.

Subiecții pot fi: fie Autorități de Certificare, fie autorități care emit confirmări electronice de non-repudiere ale domeniului certSIGN.

1.3.4 Entitățile partenere

O Entitate Parteneră, care utilizează serviciile certSIGN, poate fi orice entitate care ia decizii bazându-se pe corectitudinea conexiunii dintre identitatea unui Subiect şi cheia sa publică.

O Entitate Pateneră este responsabilă pentru modul în care verifică starea curentă a certificatului unui Subiect. 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 Subiectul certificatului. O Entitate Parteneră va utiliza informaţiile dintr-un certificat pentru a decide dacă un certificat a fost folosit în conformitate cu scopul declarat.

1.3.5 Alți participanți

Comitetùl de Management al Politicilor și Procedurilor este un comitet creat în certSIGN de către Consiliul de Administrație pentru a superviza întreaga activitate a Autorităților de certificare și de înregistrare certSIGN. Rolurile și responsabilitățile CMPP sunt descrise în documentația internă.

Furnizorii de servicii certSIGN: furnizori externi care susțin activitățile certSIGN pe baza unui acord contractual semnat.

Furnizorii de Dispozitive pentru Creare Semnăturii Calificate (QSCD): furnizarea QSCD-urilor fizice utilizate de Subiecți este asigurată de furnizorii externi care susțin activitățile certSIGN pe baza unui acord contractual semnat.

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:

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

Entitatea Parteneră este responsabilă pentru stabilirea nivelului de credibilitate necesar pentru un certificat utilizat 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. Subiecţii trebuie să cunoască cerinţele Entităţii Partenere (de exemplu, aceste cerinţe pot fi publicate sub forma unei politici de semnătură sau a unei politici de securitate informatică) şi apoi să solicite certSIGN emiterea de certificate corespunzătoare acestor cerinţe.

1.4.1 Utilizări admise ale certificatului

certSIGN ROOT CA G2 poate înregistra și emite certificate numai către Autoritățile de certificare și Autoritățile ce emit confirmări electronice de repudiere aparținând domeniului certSIGN.

Certificatele pot fi folosite în aplicații care întrunesc cel puțin următoarele condiții:

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

Aplicațiile pentru care se consideră că Certificatul este de încredere vor fi decise chiar de către Entitățile Partenere, pe baza naturii și scopului (inclusiv utilizarea cheii) Certificatului, inclusiv orice limitare aplicabilă în scris în Certificat.

1.4.2 Utilizări interzise ale certificatului

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

1.5 Administrarea politicii

1.5.1 Organizația care administrează documentul

Nume	certSIGN S.A. Sediu: Bd. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, București, România Nr. înregistrare Registrul Comerțului: J2006000484402 Cod de înregistrare fiscală: RO 18288250 Sediu social: Str. Olteniței, nr. 107A, clădirea C1, etaj 1, camera 16, Sector 4, București, România, CP 041303
Telefon	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table 1.5.1 Organizația care administrează documentul

1.5.2 Persoana de contact

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

Table 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 consumator 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
Telefon	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Table 1.5.3 Persoana care decide conformitatea CPP cu politica

1.5.4 Procedurile de aprobare a CPP

Comitetul de Management al Politicilor și Procedurilor este responsabil pentru aprobarea CPP. Procedura de aprobare este descrisă într-un document de instrucțiuni interne.

Beneficiarii vor respecta CPP-ul implementat și publicat la: https://www.certsign.ro/ro/document/certsign-root-ca-g2-cod-practici-si-proceduri/
Beneficiarii care nu acceptă noul CPP, conţinând termenii și reglementările modificate, 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 duce la încetarea contractului de prestări servicii de certificare și la revocarea certificatului emis în baza acestuia.

1.6 Definiții și acronime

Definitii

Auditor – persoana ce atesta conformitatea cu cerintele specificate În documentele relevante

Autentificare – procese electronice ce permit identificarea electronica a unei persoane fizice sau juridice, sau originea și integritatea datelor În forma electronica.

Autoritate de Certificare – autoritate considerate de incredere de unul sau mai multi utilizatori, utilizata pentru crearea și asignarea certificatelor.

Beneficiar – persoana fizica sau juridical, legata prin contract cu un prestator de servicii de incredere

CA subordonat – autoritate de certificare al carei certificate este semnat de Root CA, sau alta autoritate suboedonata.

Certificat – cheia publica a unui utilizator, impreuna cu alte informatii, ce sunt protejate la falsificare prin criptare cu cheia privata a autoritatii de certificare ce l-a emis.

Cheie privată – una dintre cheile asimetrice aparţinând unui Subiect şi care este folosită numai de acel Subiect. În cazul sistemelor cu chei asimetrice, o cheie privată descrie transformarea unei semnături. În cazul sistemului asimetric de criptare, o cheie privată descrie transformarea care are loc la decriptare. Cheia privată este (1) cheia al cărei scop este decriptarea sau crearea de semnătură pentru uzul exclusiv al proprietarului; (2) acea cheie dintr-o pereche de chei care este cunoscută numai proprietarului.

Cheie publică – una dintre cheile perechii de chei asimetrice ale unui Subiect, care poate fi disponibilă publicului. În cazul sistemelor de criptare asimetrică, cheia publică defineşte transformarea de verificare a semnăturii. În cazul criptării asimetrice, cheia publică defineşte transformarea mesajelor la criptare.

Codul de Practici și proceduri (CPP) - Declarație privind practicile pe care o autoritate de certificare le utilizează în emiterea, gestionarea, revocarea și reînnoire sau re-key-ul certificatelor.

Cross-certificare – certificate ce este emis pentru stabilirea unei relatii de incredere intre doua autoritati de certificare.

Dispozitiv de Creare a Semnăturilor Electronice Calificate un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele prevăzute în Anexa II a Regulamentului (UE) 910/2014.

Furnizor de servicii de incredere – o persoana fizica sau juridical ce furnizeaza unul sau mai multe servicii de incredere fie ca un furnizor de servicii de incredere calificate fie ca un furnizor de servicii de incredere ne-calificate.

Identificator de obiect (OID) – identificator alfanumeric / numeric înregistrat în concordanţă cu standardul ISO/IEC 9834 şi care descrie în mod unic un obiect sau clasa sa.

Infrastructura de cheie publică (PKI) – arhitectura, tehnicile, practicile și procedurile care contribuie în mod colectiv la implementarea și funcţionarea sistemelor criptografice cu chei publice, bazate pe certificate; PKI constă în hardware, software, baze de date, resurse de reţea, proceduri de securitate și obligaţii legale, legate împreună și care colaborează pentru

a furniza și implementa atât serviciile de certificare, cât şi alte servicii asociate infrastructurii (de ex. marcă temporală).

Lista de Certificate Revocate (CRL) – lista semnata ce indica un set de certificate ce nu mai sunt considerate valide de catre emitentul certificatului.

Lista de Revocare a Autoritatii de Certificare (CARL) – lista de revocare ce contine o lista de certificate de CA emise catre autoritati de certificare ce nu mai sunt considerate valide de catre emitentul certificatului.

Regulamentul (UE) nr. 910/2014 – REGULAMENTUL (UE) NR. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

Root CA – autoriitate de certificare ce are cel mai inalt nivel în cadrul domeniului TSP și care este utilizata pentru semnarea CA-urilor subordonate.

Semnatura electronica – date În format electronic ce sunt atasate sau associate logic cu alte date În format electronic ce sunt utilizate de catre semnatar pentru semnare.

Subiect (Entitate finală): entitate identificată într-un certificat ca fiind deținătorul cheii private asociate cheii publice din certificat

Acronime

CA Autoritate de Certificare
CPP Codul de Practici și Proceduri
CRL Lista Certificatelor Revocate
CARL Lista de Revocare a Autoritatilor de Certificare
DN Nume Distinctiv
NIMB Institutul National de Metrologie Bucuresti
OCSP Protocol de verificare online a stării certificatului
PKI Infrastructură cu Cheie Publică
CMPP Comitet de Management al Politicilor și Procedurilor
QSCD Dispozitiv de Creare a Semnăturilor Electronice Calificate
RSA Algoritmul criptografic Asimetric Rivest, Shamir, Adleman
TSP Funizor de Servicii de Încredere
UTC Timpul Universal coordonat

2 Publicare și Responsabilități Depozitar

certSIGN publică CPP-urile in Depozitar cel puțin anual, chiar dacă nu există schimbări.

2.1 Depozitar

Depozitarul este disponibil on-line: https://www.certsign.ro/ro/depozitar. Acesta conține:

- Codul de Practici și Proceduri pentru CA-urile operate de certSIGN
- Certificatele Root CA și ale CA-urilor Subordonate
- Certificatele Subiecților
- Listele Certificatelor Revocate
- Temenii și condițiile privind utilizarea certificatelor digitale

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

- Să facă 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 şi arhivarea Politicii de certificare, a CPP, a listei aplicaţiilor şi a dispozitivelor recomandate,
- Să permită accesul 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 Autorităţile 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 Politica de Certificare,
- Să asigure accesul sigur și controlat la informațiile din Depozitar.

2.2 Publicarea Informațiilor din Certificat

La emitere, un certificat digital este publicat în Depozitar.

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

certSIGN se conformează ultimii versiuni publicate din 'Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates' precum si din „CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates" publicată pe http://www.cabforum.org. În eventualitatea oricărei inconsistențe între acest document și BR, cerințele din BR/EV au prioritate în raport cu cele din acest document.

certSIGN găzduiește 3 pagini web, cu reînnoire automată lunară, care permit Aplicațiilor Software ale Beneficiarilor/Furnizorilor să testeze software cu certificate emise de CA-urile certSIGN pe https://testssl.certsign.ro:

https://testssl-valid-evcp.certsign.ro

https://testssl-revoked-evcp.certsign.ro

https://testssl-expired-evcp.certsign.ro

Disponibilitate

Disponibilitatea combinata a depozitarului de documente și a depozitarului CRL este proiectată să depășească 99,8% din programul de lucru - definit ca 24 de ore pe zi, șapte zile pe săptămână, cu excepția perioadelor planificate de întreținere.

Perioadele planificate de întreținere vor fi anunțate pe https://www.certsign.ro cu cel puțin 24 de ore în avans.

În caz de indisponibilitate datorata unei catastrofe, unei defectiuni a infrastructurii aflate În afara controlului certSIGN sau din orice alt motiv, certSIGN va depune toate eforturile pentru restabilirea serviciului în termen de 24 ore.

Certificatele expirate care au fost revocate înainte de expirarea lor nu sunt eliminate din listele de revocare a certificatelor.

2.3 Timpul sau frecvența publicării

Informațiile publicate de certSIGN sunt actualizate anual sau după evenimente precum:

- Actualizări CPP ;
- Certificatele Autorităților de Certificare – după emiterea unui nou certificat;
- Lista certificatelor revocate este creată fie odată la 12 luni sau când un certificate este revocat;
- Soluționarea neconformităților găsite în urma unui audit;
- Informațiile suplimentare – după fiecare actualizare
- Ori de câte ori CA/Browser Forum publică noi cerințe prin documentele BR care solicită o schimbare a politicii unui certificat sau a practicilor.

2.4 Controlul accesului la Depozitare

Toate informațiile publicate de certSIGN în Depozitar la adresa https://www.certsign.ro/ro/depozitar sunt accesibile public. Depozitarul este disponibil public, și internațional, 24x7x365.

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

Beneficiarii, Subiectii și Entitatile Partenere au acces doar read-only prin intermediul Internetului la toate depozitarele mentionate În sectiunea 2.1.

certSIGN poate lua masuri rezonabile de protecţie impotriva și pentru prevenirea utilizarii abusive a depozitarelor, a OCSP sau serviciilor de descarcare a CRL.

La descoperirea unor breşe 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 entităţile afectate.

3 Identificarea și autentificarea

3.1 Denumirea

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

3.1.1 Tipuri de nume

Certificatele emise de catre certSIGN sunt conforme cu standardul X.509 v3. Aceasta inseamna ca emitentul certificatului și Autoritatea de Inregistrare ce lucreaza in numele emitentului, aproba numele Subiectului in conformitate cu prevederile standardului X.509 (cu referire la recomandarile X.500). Denumirile Subiectilor și ale emitentilor de certificate din certificatele certSIGN sunt in conformitate cu structura de nume Distinctive Name (DN) – (cunoscute și ca structuri de tip Directory Name), create conform recomandarilor X.500 și X.520. În cadrul structurii de tip DN, se pot defini atribute specific Domain Name Service (DNS). Aceasta permite subiectilor sa utilizeze doua tipuri de nume simultan: de tip DN și de tip DNS. Aceasta este o optiune foarte importanta in cazul emiterii de certificate pentru servere administrate de catre Subiect.

3.1.2 Nevoia ca numele sa aibă inţeles logic

Numele utilizate în certificate sunt astfel alese incat să:

- Fie clar că este vorba de un certificat de CA,
- Fie clar scopul CA-ului,
- Includă o identificare precisa a Beneficiarului în calitate de entitate legală.

Numele certificatelor de CA emise vor conţine următoarele informaţii:

OrganizationIdentifier = VATRO-18288250

O= certSIGN SA

C= RO

Multe aplicaţii software utilizează câmpul commonName pentru a prezenta o selecţie de certificate catre utilizatorul final. Pentru a ajuta utilizatorul final să aleaga certificatul potrivit, câmpul commonName poate să mai conţină și cuvinte clare ce descriu scopul certificatului (de exemplu "CA calificat").

commonName	Nume intuitiv al unei CA subordonate
organizationName	Nume oficial înregistrat al CA Beneficiar, ca și corporaţie sau organizaţie
countryName	Codul țării din două litere, conform ISO 3166-1, pentru țara în care este afacerea CA
OrganizationIdentifier	Un identificator unic oficial al beneficiarului ca și corporaţie sau organizaţie (asa cum este formatat în ETSI EN 319 412-1)

Numele Subiectului va fi confirmat de catre CMPP și aprobat de catre Root CA. certSIGN asigură (în cadrul domeniului său) unicitatea tuturor DN-urilor.

3.1.3 Anonimatul sau pseudonimitatea beneficiarilor
certSIGN nu emite certificate anonime dar poate emite certificate cu pseudonime pentru utilizatori finali cu OID-uri specifice.

3.1.4 Reguli de interpretare a formatelor de nume
Interpretarea câmpurilor din cadrul certificatului emis de certSIGN se face în conformitate cu profilul certificatului descris în Certificate și în profilele CRL prezentate în Capitolul 7 al prezentului document. Crearea și interpretarea DN va fi realizată în conformitate cu recomandarile din capitolul 3.1.2 al prezentului document.

3.1.5 Unicitatea numelor
Unicitatea numelui este asigurată prin utilizarea numelui SerialNumber al subiectului atribuit de către CA. Semantica lui SerialNumber este: prima literă din nume + prima literă din primul prenume +Numarul indexului. Numărul indexului este numărul secvențial al prefixului (ca code + inițiale) în baza de date.

3.1.6 Recunoașterea, autentificarea și rolul mărcilor comerciale
Nu este stipulat.

3.2 Validarea Inițială a Identității

3.2.1 Dovada Posesiei Cheii Private
Deținerea cheii private, corespunzătoare cheii publice pentru care se solicită generarea unui certificat, va fi dovedită prin trimiterea cererii de semnare a certificatului (CSR), conform standardului RSA PKCS # 10, care va include cheia publică semnată de catre cheia privată asociată.

3.2.2 Autentificarea identitatii organizatiei
certSIGN ROOT CA G2 este o Autoritate de Certificare Primară pentru domeniul certSIGN. Orice altă autoritate de certificare subordonată certSIGN ROOT CA G2 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 G2, 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
Nu se aplică.

3.3 Identificarea și Autentificarea pentru cererile de re-key

3.3.1 Identificarea și Autentificarea 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

Cererile de Revocare sunt realizate prin roluri de încredere asociate certSIGN Root CA G2, cu aprobarea Comitetului de Management al Politicilor și Procedurilor (CMPP).

4 Cerinţe operaționale privind ciclul de viață al certificatului

Acest capitol descrie procedurile de bază care sunt comune tuturor tipurilor de certificate emise direct de certSIGN Root CA G2.

4.1 Aria de aplicabilitate a certificatelor

4.1.1 Cine poate trimite o cerere de certificat

Cererile de Emitere sunt realizate prin roluri de încredere asociate certSIGN Root CA G2, cu aprobarea Comitetului de Management al Politicilor și Procedurilor (CMPP).

4.1.2 Procesul de înregistrare și responsabilitățile

Procesul de inregistrare este realizat prin roluri de încredere asociate certSIGN Root CA G2, cu aprobarea Comitetului de Management al Politicilor și Procedurilor (CMPP).
certSIGN pune la dispoziţie infrastructura și resursele pentru operarea certSIGN Root CA G2. De asemenea, certSIGN asigura supervizarea, suportul și auditarea pentru toate procesele și serviciile certSIGN Root CA G2.
certSIGN asigura segregarea proceselor de livrare pentru un QSCD și a datelor de activare associate.

4.2 Procesarea Cererilor de Certificate

4.2.1 Îndeplinirea funcțiilor de identificare și autentificare

certSIGN ROOT CA G2 este Autoritate de Certificare Prrimara pentru domeniul certSIGN. Orice altă autoritate de certificare subordonată certSIGN ROOT CA G2 este operată de catre aceaşi entitate legală.

Astfel, funcţiile de autentificare și identificare sunt realizate prin roluri de încredere asociate certSIGN Root CA G2, sub supravegherea Comitetului de Management al Politicilor și Procedurilor (CMPP).

4.2.2 Aprobarea sau respingerea cererilor de certificate

Aprobarea sau respingerea cererilor de certificate se face prin roluri de încredere asociate certSIGN Root CA G2, sub supravegherea Comitetului de Management al Politicilor și Procedurilor (CMPP).

4.2.3 Timpul de procesare a cererilor de certificate

Timpul de procesare al cererilor de certificate poate lua mai multe ore, depinzând de aprobarea Comitetului de Management al Politicilor și Procedurilor (CMPP) si de implementarea procedurilor aferente Ceremoniei Cheilor.

4.3 Emiterea certificatelor

4.3.1 Acțiunile CA în timpul emiterii certificatelor

Dupa primirea, procesarea și aprobarea unei cereri, Autoritatea de Certificare emite un certificat. Dupa ce certificatul este emis, certSIGN il va publica in depozitarele corespunzatoare. Perioada de disonibilitate a certificatului emis depinde de tipul certificatului și de categoria Subiectului, și este în conformitate cu timpii descriși în tabelul 6.3.2.1.
Emiterea de certificate de către ROOT CA G2 necesită ca o persoană autorizată de CA (de ex. Operator de sistem CA, Ofițer de sistem sau Administrator PKI) să transmită în mod deliberat o dispoziție astfel încât Root CA-ul să execute operațiunea de semnare a certificatului.

certSIGN a implementat propriul instrument 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.

4.3.2 Notificarea Subiectului de către CA cu privire la emitere certificatului

Notificarea emiterii unui certificat de către certSIGN Root CA G2 este implicită și este specificată în documentația internă.

4.4 Acceptarea Certificatului

4.4.1 Conduita care constituie acceptarea certificatului

Acceptarea unui certificat se face prin roluri de încredere asociate certSIGN Root CA G2, sub supravegherea Comitetului de Management al Politicilor și Procedurilor (CMPP).

4.4.2 Publicarea certificatului de către CA

Vezi capitolul 2 al prezentului document.

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

Fiecare certificat emis este publicat în Depozitarul certSIGN. Publicarea certificatului este echivalentă cu notificarea către alte entităţi (de exemplu Entităţi Partenere) referitor la emiterea unui certificat pentru o CA subordonată.

4.5 Utilizarea Perechii de Chei și a Certificatului

4.5.1 Utilizarea Cheii private a și certificatului Beneficiarului

certSIGN protejeaza cheia privată de accesul neautorizat al personalului și al partilor terte.
certSIGN utilizeaza cheia privată numai în accord cu utilizarile specificate în extensia de utilizare a cheii.
Vezi sectiunile 1.4.1, 6.1.7 și 7.1.

4.5.2 Utilizarea cheii publice și a certificatului unei Entități Partenere

certSIGN presupune ca toate aplicatiile software sunt conforme cu standardul X.509, protocolul SSL/TLS, și alte standarde aplicabile ce impun cerinţele și seturile de cerinţe menţionate în acest CPP. certSIGN nu garanteaza ca soft-ul oricarei entitati partenere va suporta sau impune asemenea controale și cerinte, și toate entitatile partenere sunt sfătuite sa identifice suport tehnic și legal adecvat.

Entitatile partenere vor utiliza cheile private și certificatele:

- În conformitate cu scopul declarat în prezentul CPP și în conformitate cu conținutul certificatului (câmpurile *keyUsage* și *extendedKeyUsage*),
- În conformitate cu prevederile Contractului încheiat între Beneficiar/Subiect și certSIGN,
- Numai dupa ce statusul și semnatura Autoritatii de Certificare emitente au fost verificate.

Încrederea intr-o semnătură digitală neverificabilă sau o sesiune SSL / TLS, poate genera riscuri pe care entitatea parteneră și le asuma și pe care certSIGN nu și le asumă în nici un fel.

4.6 Reînnoirea Certificatului

certSIGN permite reînnoirea certificatelor de CA doar în condiții speciale, cu aprobarea CMPP.

4.7 Re-key-ul Certificatului

certSIGN permite re-key-ul certificatelor de CA doar în condiții speciale, cu aprobarea CMPP.

4.8 Modificarea Certificatului

certSIGN permite rmodificarea certificatelor de CA doar în condiții speciale, cu aprobarea CMPP.

4.9 Revocarea și Suspendarea Certificatului

Certificatele emise de certSIGN Root CA G2 pot fi revocate dar niciodata suspendate. Revocarea certificatelor este un process ireversibil.
Revocarea certificatului de CA include și revocarea tuturor certificatelor emise de CA.
Revocarea nu afecteaza nici tranzactiile efectuate inainte de revocare nici obligatiile ce rezulta din aderarea la prezentul CPP.
Aceste capitol prezinta conditiile necesare pentru ca o autoritate de certificare sa revoce un certificat.

4.9.1 Circumstanțele revocării unui certificat

Motive pentru revocarea unui certificat de CA Subordonat
CA-ul emitent, certSIGN ROOT CA G2, 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 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 de a suspecta acest lucru,
(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 se face prin roluri de incredere associate certSIGN Root CA G2, sub supravegherea CMPP.

4.9.2 Cine poate solicita revocarea certificatelor

Comitetul de Management al Politicilor și Procedurilor (CMPP) este singura entitate ce poate solicita revocarea unui certificat emis de certSIGN Root CA G2.
Îm plus, beneficiarii, entitățile partenere, furnizorii de aplicații software și alte părți implicate, pot depune rapoarte de probleme la certificate, informând CA-ul emitent despre cauze rezonabile de a revoca certificatul.

4.9.3 Procedura de revocare a certificatelor

Revocarea certificatelor se face prin roluri de incredere associate certSIGN Root CA G2, sub supravegherea CMPP.
Înainte de revocarea certificatului unei CA subordonate, toate certificatele valide semnate de această autoritate vor fi revocate.
Informaţiile despre certificatele revocate sunt plasate în Lista de certificate Revocate emisă de Autoritatea de Certificare corespunzatoare.
CA-ul menține continuu, 24x7, capabilitatea de a accepta și răspunde la cereri de revocare și rapoarte de probleme la certificate.
CA-ul oferă beneficiarilor, entităților partenere, furnizorilor de aplicații software și altor părți implicate instrucțiuni clare pentru raportarea suspiciunilor privind compromiterea de chei private, utilizarea greșită a certificatelor, precum și alte tipuri de fraudă, compromisuri, utilizări greșite, ținută necorespunzătoare, sau orice altă problemă legată de certificate. CA-ul prezintă instrucțiunile pe site online precum și în secțiunea 1.5.2 a acestui document.

4.9.4 Perioada de grație a cererii de revocare

certSIGN efectuează revocarea în maxim 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

În termen de 24 de ore de la primirea unui raport cu probleme de certificat, certSIGN va cerceta faptele și circumstanțele legate de un raport cu probleme de certificat și va furniza un raport preliminar asupra constatărilor sale atât beneficiarului, cât și entității care a depus Raportul cu problema certificatului.

După analizarea faptelor și circumstanțelor, certSIGN lucrează cu Beneficiarul și cu orice entitate care raportează Problema Certificatului sau un alt aviz legat de revocare pentru a stabili dacă certificatul va fi revocat sau nu și, dacă este cazul, o dată în care CA va revoca certificatul. Perioada de la primirea raportului cu probleme de certificat sau avizul aferent revocării până la revocarea publicată nu va depăși termenul prevăzut în secțiunea 4.9.1.1. certSIGN va avea în vedere următoarele:

1. Natura presupusei probleme (sfera de aplicare, contextul, gravitatea, amploarea, riscul de vătămare);

2. Consecințele revocării (impacturi directe și colaterale pentru beneficiary și părți afiliate);
3. Numărul de rapoarte cu probleme de certificate primite despre un anumit certificat sau beneficiar;
4. Entitatea care face reclamația (de exemplu, o reclamație de la un oficial de aplicare a legii potrivit căreia un site web este angajat în activități ilegale ar trebui să aibă mai multă greutate decât o reclamație a unui consumator care susține că nu a primit bunurile comandate);
5. Legislație relevantă

Cu titlu de excepție, în cazul în care cererea de revocare nu poate fi confirmată în termenul specificat la punctul 4.9.1, certSIGN nu va revoca certificatul și justificarea va fi înregistrată.

4.9.6 Verificarea cerințelor de revocare pentru Entitățile Partenere

Entitățile Partenere vor utiliza toate resursele pe care le pune la dispoziție certSIGN prin depozitarul său pentru verificarea stării unui Certificat în orice moment, înainte de a se baza pe ea.

4.9.7 Frecvența de emitere a CRL-urilor

Lista Certificatelor Revocate (CRL) a Autorității certSIGN Root CA G2 este emisă cel puțin o dată pe an, cu condiția să nu fie revocate certificate ale uneia dintre autoritățile subordonate autorității certSIGN Root CA G2.
În cazul revocării certificatului unei autorități afiliate la certSIGN, acest certificat este publicat imediat în Lista de Certificate Revocate (in maxim 24 de ore).
certSIGN ROOT CA G2 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

Disponibilitatea verificării on-line a revocării/stării este specificată mai jos, în 4.10.2.

Raspunsurile OCSP responses sunt semnate de catre un OCSP Responder al carui certificat este semnat de catre CA-ul care a emis certificatul al carui status de revocare se verifică.
Certificatul de semnare al OCSP contine o extensie de tipul id-pkix-ocsp-nocheck, asa cum este definit de catre RFC6960.

4.9.10 Verificarea on-line a cerințelor de revocare

CA-ul suportă o capabilitate OCSP utilizând metoda GET pentru certificatele emise în concordanță cu versiunea curentă a CA/B Forum Baseline Requirements.
Pentru starea certificatelor emise de certSIGN ROOT CA, CA actualizează informaţiile furnizate prin protocolul OCSP cel puţin:

- La fiecare 12 luni sau
- În 24 de ore dupa revocarea certificatului unei CA subordonate.

Daca un responder OCSP primeste o cerere de status a unui certificate ce nu a fost emis, atunci responderul nu raspunde cu status "good" pentru astfel de certificate.
certSIGN monitorizează responderul OCSP pentru cereri de numere seriale "neutilizate", ca parte a procedurilor sale de răspuns de securitate.
Responderul OCSP oferă răspunsuri definitive pentru certificate cu numere seriale "rezervate", ca și cum ar exista un certificat corespunzător care se potrivește cu Precertificatul [RFC6962].
În cadrul unei cereri OCSp pentru un număr serial de certificat, există următoarele variante:

1. "alocat" (assigned) dacă un certificat cu acel număr serial a fost emis de către CA-ul emitent, utilizând orice cheie curentă sau anterioară, asociată cu acel subiect;
2. "rezervat" (reserved) dacă un Precertificat [RFC6962] cu acel număr serial a fost emis de către:
    a. CA-ul emitent;
    b. un Precertificat al unui Certificat de semnare [RFC6962] a fost associat cu CA-ul emitent;
3. "neutilizat" (unused) dacă nici una dintre condițiile anterioare nu se aplică.

Vezi și capitolul 4.9.6 al prezentului document.

4.9.11 Alte forme disponibile pentru anunțarea revocării

Nu se aplică.

4.9.12 Cerințe special în cazul compromiterii re key

Nu se aplică.

4.9.13 Circumstanțe pentru suspendare

Nu se aplică

4.9.14 Cine poate solicita suspendarea

Nu se aplică

4.9.15 Procedura de solicitare a suspendării

Nu se aplică

4.9.16 Limitări ale perioadei de suspendare

Nu se aplică

4.10 Servicii privind starea certificatelor

4.10.1 Caracteristici operaționale

Serviciile certSIGN de verificare a stării certificatelor sunt CRL și OCSP. Accesul la aceste servicii se realizează prin intermediul site-ului web "certsign.ro" și prin directorul on-line LDAP "ldap.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 pentru un răspuns CRL sau OCSP nu sunt șterse decât după data de expirare a certificatului revocat.

4.10.2 Disponibilitatea serviciului

CA-ul operează și menține capabilitățile OCSP și CRL, cu resurse suficiente pentru a oferi un timp de răspuns de două secunde sau mai puțin, în condiții normale de operare.
CA-ul menține un depozitar online 24x7, pe care aplicațiile software îl pot folosi pentru verificarea automată a stării certificatelor neexpirate emise de CA.
CA-ul menține o capabilitate continuă, 24x7, de a răspunde intern la rapoartele de înaltă prioritate despre certificate, iar unde este cazul, înaintează acest raport către autoritățile de impunere a legii, și/sau revocă certificatul care este subiectul unei astfel de cereri.

4.10.3 Elemente opționale

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

4.11 Încetarea abonamentului

Nu se aplică.

4.12 Custodie și recuperare chei

Nu se aplică.

5 Facilitate, Management și Controale Operaționale

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 următoarele 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, Politica și cerințele de securitate pentru Furnizorii de Servicii de Încredere care emit mărci temporale.
    - CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates
    - CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates
    - CA/Browser Forum Network and Certificate System Security Requirements

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 şi 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 şi temperatura și umiditatea sunt de asemenea monitorizate și controlate.

5.1.1 Amplasarea și construcția sediului

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 intruşilor 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 şi 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 şi 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 şi 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 permisă prezenţa persoanelor neînsoţite. Programatorii și dezvoltatorii nu au acces la informaţii sensibile. Dacă este necesar accesul la astfel de informații, el este permis doar în prezenţa administratorului de securitate. Proiectele în curs de implementare şi software-ul aferent sunt testate în mediul de dezvoltare al certSIGN.

5.1.3 Alimentarea cu curent și aerul conditionat

Toate zonele sunt prevăzute cu aer conditionat. 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 curect electric este concepută astfel încât la o întrerupere a curentului în cladire 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 securitatii 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 controlat prin rack-uri. Toate echipamentele sunt plasate în rack-uri la o distanta de minim 15 cm de la sol. În plus, toate camerele serverelor sunt monitorizate cu senzori de umiditate.

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. Când nu mai sunt necesara, HSM-urile vor fi resetate pentru a preveni orice posibilitate de reutilizare a cheilor private CA și returnate la inventarul criptografic. După încetarea operațiunilor, tokenurile și cardurile rolurilor de încredere vor fi distruse. Stergerea securizata 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

Toate rolurile implicate în furnizarea serviciilor de certificare ale certSIGN atribuite catre angajați certSIGN.

Toți angajații certSIGN se angajează, sub semnătură, să nu aibă conflicte de interese cu certSIGN, să păstreze confidențialitatea informațiilor și să protejeze datele cu caracter personal.

certSIGN asigură o separare a sarcinilor pentru funcțiile critice pentru a împiedica o persoană rău intenționată, să folosească sistemele CA fără a fi detectată.

Securitatea informațiilor prelucrate de certSIGN și a serviciilor sale este pusă în aplicare prin controale procedurale legate de controlul accesului. Astfel, accesul la informații și la funcțiile de sistem ale aplicațiilor este restricționat în conformitate cu Politica de Control al Accesului. certSIGN administrează drepturile de acces ale operatorilor, administratorilor și auditorilor de sistem, iar administrarea include managementul conturilor utilizatorilor și modificarea la timp sau eliminarea accesului. Sunt furnizate suficiente controale de securitate a calculatoarelor

pentru separarea rolurilor de încredere identificate, inclusiv separarea funcțiilor de administrare de securitate și de funcționare. În special, utilizarea de programe utilitare de sistem este limitată și controlată.

certSIGN poate aloca următoarele roluri de încredere la una sau mai multe persoane:

- **Ofițer de securitate** – Responsabilitate globală pentru implementarea politicilor şi procedurilor de securitate .
- **Administrator de sistem** – Autorizat să instaleze, configureze și să întreţină sistemele de încredere ale Autorităţii de Certificare pentru înregistrarea, generarea de certificate, furnizarea dispozitivelor subiecților şi gestiunea revocărilor de certificate. Instalează dispozitivele hardware şi sistemele de operare; instalează şi configurează echipamentele de reţea.
- **Operator 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 Subiecţilor; revocă certificatele Subiecţilor; asigură continuitatea copiilor de siguranţă şi a arhivelor bazelor de date şi crearea log-urilor de sistem; manages databases; administrează bazele de date; are acces la informaţii confidenţiale despre Subiecți/Beneficiari, dar nu are dreptul de a accesa fizic nici o altă resursă a sistemului; transferă copiile de siguranţă ale arhivei și ale datelor curente catre locaţiile desemnate.
- **Ofițer de înregistrare**: Responsabil de introducerea informațiilor necesare pentru emiterea de certificate și pentru aprobarea cererilor de certificare;
- **Ofițer de revocare:** Responsabil de operarea modificării stărilor certificatelor;
- **Specialist validare:** Responsabil de verificarea informațiilor introduse pentru emiterea de certificate și pentru aprobarea cererilor de certificare;
- **Auditor 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 şi asupra Autorităţii de Înregistrare care operează în cadrul certSIGN.

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

Angajaților li se alocă în mod oficial roluri de încredere de către CMPP. Principiul "cel mai mic privilegiu" "este aplicat atunci când se configurează privilegiile de acces catre rolurile de incredere.

5.2.2 Numărul de persoane necesare pentru fiecare sarcină

Acolo unde controlul dual sau controlul multiplu este necesar, cel putin doua persoane distincte, cu roluri de incredere relevante sunt prezente pentru a putea indeplini operatiunea.

Circumstantele ce necesita control dual sau multiplu sunt descrise în documentatia interna confidentiala.

5.2.3 Identificarea și autentificarea pentru fiecare rol

Fiecare angajat certSIGN ce are un rol de incredere este identificat și autentificat la accesarea infrastructurii pentru indeplinirea rolului sau prin mijloace de autentificare cu cel putin doi factori.

Fiecare cont alocat:

- este unic şi 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 şi a controalelor de aplicaţii.

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.

Procedurile sunt stabilite și implementate 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 Autorităţi de Certificare sau Înregistrare:

- a absolvit cel puţin liceul,
- A inteles și a semnat un contract ce descrie rolul şi 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 protecţia datelor personale şi informaţiilor confidenţiale sau private,
- a semnat un contract ce conţine clauze referitoare la protejarea informaţiilor senzitive ale certSIGN și a datelor confidenţiale şi 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 identitatea, încrederea, calificările, cunoștințele de specialitate, experiențe și autorizarea 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 realizează sau se asigură că sunt efectuate verificările relevante pentru potențialii angajați, prin intermediul rapoartelor emise de o autoritate competentă, declarațiile unor terțe părți sau auto-declarații.

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:

- cunoștințe de bază privind Infrastructura de Chei Publice (PKI),
- cerințele CPP,
- procedurile și controalele de securitate folosite de Autoritatea de Certificare și Autoritatea de Înregistrare
- responsabilităţile ce decurg din rolurile și sarcinile executate în sistem,

După încheierea pregătirii, participanţii semnează un document prin care confirmă familiarizarea lor cu Codul de Practici și Proceduri, Politica de certificare și acceptă restricţiile și obligaţiile impuse.

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.

Tot personalul cu roluri de încredere își menține abilitățile consistent cu programele de instruire și performanță ale CA-ului.

5.3.5 Frecvența și secvența rotației posturilor

Nu este stipulat.

5.3.6 Sancțiunile pentru acțiunile neautorizate

certSIGN va lua masuri impotriva celor ce incalca politicile sau procedurile, realizeaza 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 contractanților 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.

5.3.8 Documentația oferită personalului

certSIGN ofera personalului său accesul la următoarele documente:

- CPP,
- Lista Responsabilităţilor şi 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 şi dezvăluită atunci când se desfăşoară un audit, dacă este necesar. Acuratețea temporală a log-urilor este asigurată de un server de timp care este sincronizat cu cel putin doua surse de timp care pot fi sateliţi GPS sau UTC (NIMB). Ora utilizată pentru înregistrarea evenimentelor necesare în jurnalul de audit este sincronizată cu UTC cel puțin o dată pe zi.

5.4.1 Tipuri de Evenimente Înregistrate

Fiecare activitate critică din punctul de vedere al securităţii certSIGN este înregistrată în log-urile de evenimente şi arhivată. Arhivele sunt depozitate pe medii de stocare ce nu pot fi suprascrise sau distruse cu ușurință (cu excepția cazului 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:

- **Inregistrări de sistem** – conţin informaţii despre cererile clienţilor şi 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.) şi 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;
- **Inregistrări de audit** – 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 intrării,
- 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 Subiect / 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, personal special desemnat, și auditori, prin cerere adresata pe email sau in format hartie catre CISO.

Confidențialitatea informațiilor Subiectului 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 siguranta sunt facute în mod continuu.

5.4.3 Perioada de pastrare 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 10 ani.

CA și fiecare terț delegat păstrează:
1. înregistrări ale evenimentelor de gestionare a ciclului de viață al certificatelor și cheilor CA după apariția ulterioară a:
   - distrugerea cheii private a AC; sau
   - revocarea sau expirarea ultimului certificat CA din acel set de certificate care au o extensie X.509v3 basicConstraints cu câmpul cA setat la true și care au o cheie publică comună corespunzătoare cheii private a CA;
2. înregistrări ale evenimentelor de gestionare a ciclului de viață al certificatului de abonat (astfel cum se prevede în secțiunea 5.4.1) după expirarea certificatului de abonat;
3. Orice înregistrări ale evenimentelor de securitate (astfel cum se prevede la secțiunea 5.4.1) după producerea evenimentului.

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 ofițerul 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 centrala de jurnale arhiveaza sau sterge automat fisierele (dupa arhivarea lor) care contin evenimentele inregistrate,
- 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 conţinutul 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&extern)

Toate log-urile generate de servere, dispozitive de retea, echipamente de Securitate, aplicatii sunt trimise periodit la o platforma centrala, al carei scop este sa:

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

5.4.7 Notificarea sursei care a generat

Nu este stipulat.

5.4.8 Evaluări de vulnerabilitate

Întreaga infrastructură face obiectul evaluării vulnerabilității ca parte a procedurilor de evaluare internă a riscurilor și de gestionare a riscurilor de către certSIGN.

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 data pe an și:

1. Identifică amenințările interne și externe previzibile care ar putea avea ca rezultat accesul neautorizat, dezvăluire, utilizare incorectă, modificare sau distrugere a oricăror Date de Certificat sau Procese de Gestionare a Certificatelor;
2. Evaluează probabilitatea și potențialul daunelor cauzate de aceste amenințări, ținând cont de sensibilitatea Datelor de Certificat și a Proceselor de Gestionare a Certificatelor; și
3. Verifică dacă politicile, procedurile, sistemele informatice, tehnologia și alte aranjamente ale CA sunt suficiente pentru a contracara 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 Autoritățile 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 Tipurile de date arhivate

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 mentinerea integrității în timpul perioadei sale de reținere.

Arhivele sunt accesibile exclusive 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

certSIGN garantează că ora exactă de arhivare a tuturor evenimentelor, înregistrările și documentelor menționate mai sus este înregistrată. Acest lucru este realizat prin sincronizarea tuturor sistemelor cu serverele de timp. Acurateţea timpului este asigurată de un server de timp care este sincronizat cu cel puţin doua surse de timp care pot fi sateliţi GPS sau UTC (NIMB).

5.5.6 Sistemul de colectare al arhivei (intern sau extern)

Sistemele de colectare ale arhivei certSIGN sunt interne.

5.5.7 Procedura 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 Key changeover 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 trei ani 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. Noul certificat de CA este furnizat catre clienti si Entitati Partenere prin metodele de transmitere specificate la punctul 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 are un proces pentru Managementul Crizelor, pus în aplicare printr-o procedură de gestionare a incidentelor de securitate, în scopul de a răspunde rapid și coordonat la incidente și pentru a limita impactul breșelor de securitate. Angajaților le sunt atribuite roluri de încredere pentru a urmări alertele evenimentelor de securitate potențial 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 caz de incidente de Securitate, se utilizeaza procedurile interne. Aceste proceduri includ și notificarea Organismului National de Supraveghere, CSIRT sau alte autorități competente.

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.

certSIGN are un Plan de răspuns la incidente și un Plan de recuperare în caz de dezastru, care includ Planul de Management în situații de Criză, precum și proceduri documentate de continuitatea afacerii și recuperare în caz de dezastre, proiectate astfel încât să notifice și să protejeze în mod rezonabil furnizorii de aplicații software, beneficiarii și entitățile partenere, în eventualitatea unui dezastru, compromitere a securității sau eșec al afacerii. certSIGN pune

la dispoziția auditorilor, la cerere, planurile de continuitate a afacerii și de securitate. Toate procedurile sunt anual testate, revizuite și actualizate.

Planul de continuitate a afacerii include elementele specificate în 5.7.1 din CAB Forum BR.

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 şi 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 şi distrugerea legăturilor de reţea.
- Distrugerea unei părţi din Intranetul folosit de certSIGN pentru a furniza servicii – acest lucru poate duce la obstrucţionarea clienţilor şi 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 locatia 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 reactioneze în timp util la orice tentativă neautorizată și/sau neobișnuită 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 TIC 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 baza factuală în sprijinul deciziei certSIGN că vulnerabilitatea nu necesită remediere.

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

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

5.7.4 Capacități de Continuitate a afacerii în caz de dezastru

certSIGN a stabilit într-un Plan de Continuitate a afacerii și de Recuperare în caz de dezastru 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 TIC 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 unui eșec al 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 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 Subiecților/Beneficiarilor şi Entităţilor Partenere ce pot apărea ca urmare a deciziei unei Autorităţi de Certificare de a-şi înceta activitatea. Planul include obligativitatea notificarii Subiecților/Beneficiarilor (daca exista) in legatura cu autoritatea de certificare ce urmeaza sa isi inceteze activitatea și translatarea responsabilitatilor (servicii furnizate catre Subiecți/Beneficiari, baze de date, etc) În conformitate cu reglementarile aplicabile catre alta Autoritate de Certificare.

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 Subiecții/Beneficiarii care dețin certificate active (neexpirate și nerevocate) emise de această autoritate și alte entități cu care certSIGN are întelegeri sau alte forme de colaborare, printre care Entitati 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;
- Revoca certificatele neexpirate care au fost emise.
- Transfera 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 Subiecților / Beneficiarului 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 și / sau Subiectilor și va iniția procedura de terminare a contractelor încheiate cu partenerii și/sau furnizorii implicați.

certSIGN are un aranjament care să acopere costurile îndeplinirii acestor cerințe minime, în cazul în care intră 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.

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

Pentru a asigura continuitatea serviciilor de emitere a certificatelor pentru Subiecți, Autoritatea de Certificare care își 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 își încheie activitatea.

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

Arhiva Autorităţii de Certificare care-și încetează activitatea trebuie predată Autorităţii de Certificare primare - certSIGN ROOT CA G2 (în cazul încetării activităţii autorităţii certSIGN ROOT CA).

5.9 Lanțul de aprovizionare

certSIGN a documentat și implementat procese și proceduri pentru gestionarea riscurilor de securitate a informațiilor asociate cu utilizarea produselor sau serviciilor furnizorilor. Acestea sunt detaliate în politica internă certSIGN de gestionare a furnizorilor terți („ Politica de Management al Serviciilor Furnizate de Terți”).

Procesul și procedurile implementate gestionează riscurile de securitate a informațiilor asociate lanțului de aprovizionare cu produse și servicii din domeniul tehnologiilor informației și comunicațiilor, astfel cum se solicită în ETSI EN 319 401 #7.14.

Atunci când certSIGN apelează la alte părți, inclusiv la furnizorii de componente ale serviciilor de încredere, pentru a furniza părți ale serviciului său prin subcontractare, externalizare sau alte acorduri cu terți, acesta păstrează responsabilitatea generală pentru conformitatea cu politica privind lanțul de aprovizionare, cu politica sa privind securitatea informațiilor și cu cerințele definite în politica privind serviciile de încredere.

certSIGN revizuiește politica privind lanțul de aprovizionare și monitorizează, revizuiește, evaluează și gestionează schimbările în practicile de securitate cibernetică ale furnizorilor direcți sau ale prestatorilor de servicii la intervale planificate sau după un incident legat de furnizarea de servicii de către furnizorii direcți sau prestatorii de servicii.

6 Controale tehnice de securitate

6.1 Generarea și instalarea perechii de chei

Acest capitol descrie procedurile de generare și management a perechii de chei criptografice a unei Autorităţi de Certificare, inclusiv cerințele tehnice asociate. Controalele de securitate corespunzătoare sunt puse în aplicare pentru gestionarea oricăror chei criptografice și a oricărui dispozitiv criptografic pe parcursul ciclului lor de viață. Aceste măsuri de securitate protejează, de asemenea, datele de activare a cheilor criptografice, depozitarele, cheile private și datele de activare pentru cheile private ale CA-urilor, și ai altor Participanți PKI, precum si alti parametrii critici de securitate.

Procedurile de management al 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 G2** 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 Qualified CA, certSIGN Public CA, certSIGN Web CA** si **certSIGN Web CA G2**, prin semnarea certificatelor operaţionale şi a Listei de certificate Revocate, necesare pentru funcţionarea autorităţilor respective. Un rol similar îl au cheile private deţinute de fiecare autoritate: **certSIGN Qualified CA, certSIGN Public CA, certSIGN Web CA** si **certSIGN Web CA G2** ce corespund cheilor publice incluse in certificatele emise de catre **certSIGN ROOT CA G2** pentru fiecare autoritate.

Perechile de chei deținute 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 (in cazul **certSIGN ROOT CA G2**) sau un certificat (în cazul **certSIGN Qualified CA, certSIGN Public CA, certSIGN Web CA** si **certSIGN Web CA 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

certSIGN are o procedură documentată (ceremonia cheilor) pentru generarea cheilor de CA pentru toate autoritatile de certificare, fie ca este vorba de CA-uri root sau CA-uri subordonate, incluzand CA-uri care emit certificate catre utilizatori. Această procedură indică următoarele:

- Rolurile care participă la ceremonie (interne și externe organizației);
- Ce funcții trebuie îndeplinite de fiecare rol și în ce fază;
- Responsabilități în timpul și după ceremonie; și
- Cerințe cu privire la dovezile care trebuie colectate În timpul ceremoniei.

După ceremonia cheilor, certSIGN va elabora un raport al ceremoniei cheilor care va dovedi că a fost efectuată în conformitate cu procedura declarată și că integritatea și confidențialitatea perechii de chei au fost asigurate. Acest raport va fi semnat de toti participantii, in special:

- Pentru ROOT CA G2: de rolul de incredere responsabil pentru securitatea ceremoniei de management a cheilor certSIGN (ofiter de securitate) și o persoana de incredere independenta de managementul certSIGN (Auditor Calificat) ca martor ce atesta ca

raportul include date corecte referitoare la ceremonia de management al cheilor, urmând scenariul ceremoniei cheii și utilizând controalele implementate pentru a asigura integritatea și confidențialitatea perechii de chei..

- Pentru CA-uri subordonate: De către rolul de încredere responsabil pentru securitatea ceremoniei de gestionare a cheilor certSIGN (ofițer de securitate), ca martor că raportul înregistrează corect ceremonia de gestionare a cheilor în timp ce a fost efectuată.

În toate cazurile, CA-ul:

- Generează cheile CA în cadrul modulelor criptografice care îndeplinesc cerințele tehnice și de afaceri aplicabile, conform descrierii din CPP;
- Înregistrează activitățile sale de generare a cheilor CA; și
- Menține controale eficiente pentru a oferi o asigurare rezonabilă că cheia privată a fost generată și protejată în conformitate cu procedurile descrise în CPP și, dacă este cazul, în conformitate cu scriptul ceremoniei cheilor.

Cheile **certSIGN Qualified CA, certSIGN Public CA** și **certSIGN Web CA**, precum și cheile altor autorități subordonate și certificarea ulterioară a cheilor publice sunt efectuate într-un mediu fizic securizat de către personal în roluri de încredere, sub cel puțin, control dublu și cu distribuirea cunoștințelor:

- Cel puțin trei angajați cu roluri de încredere,
- Ofițerul de securitate,
- Cel puțin un reprezentant al Comitetului de Management al Politicilor și Procedurilor (CMPP),
- Un Coordonator al Ceremonialului Cheilor,
- Cel puțin un Auditor Calificat, independent sau extern,

Perechile de chei ale autoritatilor de certificare ce opereaza În cadrul certSIGN sunt generate pe stații de lucru desemnate, autentificate și conectate la module hardware de securitate, conforme cu cerinţele FIPS 140-2 Nivel 3 sau ISO/IEC 15408 EAL 4. Ele sunt păstrate în permanenţă criptate pe aceste dispozitive.

Procesul de generare a perechilor de chei ale CA este similar cu procedura acceptata privind generarea cheilor in certSIGN, asa cum este descrisa mai sus. Acțiunile executate în timpul generării perechii de chei sunt înregistrate, datate și semnate de fiecare persoană prezentă în timpul generării. Înregistrările sunt păstrate pentru necesitățile auditurilor și revizuirilor comune ale sistemului.

Operatorii Autorității de Înregistrare dețin numai chei pentru autentificarea tuturor acțiunilor lor. Aceste chei sunt generate de către operator (în prezența ofițerului de securitate) prin intermediul software-ului de autentificat furnizat de o autoritate de certificare și pe un dispozitiv QSCD.

Generarea perechilor de chei se face pe un dispozitiv criptografic securizat ce este conform EAL 4 sau superior În conformitate cu ISO/IEC 15408 sau FIPS PUB 140-2 nivel 3.

Generarea perechii de chei CA este realizată folosind algoritmul RSA cu lungimea cheii de 4096 biți.

Înainte de expirarea certificatului său de CA, care este utilizat pentru semnarea cheilor Subiecților, CA va genera un nou certificat pentru semnarea perechilor de chei ale Subiecților

și va aplică toate măsurile necesare pentru a evita perturbarea operațiunilor oricărei entități care se bazează pe certificatul CA. Noul certificat CA va fi, de asemenea, generat și distribuit în conformitate cu prezentul CPP. Aceste operațiuni trebuie efectuate la un interval de timp adecvat între data expirării certificatului și ultimul certificat semnat pentru a permite tuturor părților care au relații cu certSIGN (subiecți, beneficiari, entități partenere, CA-uri mai mari în ierarhia CA etc.) să fie conștienți de această modificare de cheie și să pună în aplicare operațiunile necesare pentru a evita crearea unor inconveniențe și defecțiuni. Acest lucru nu se aplică în cazul în care am înceta operațiunile noastre înainte de data de expirare a propriului nostru certificat de semnare.

6.1.2 Distribuirea Cheii Private către Beneficiar

Nu se aplică.

6.1.3 Distribuirea Cheii Publice către emitentul certificatului

Nu se aplică.

6.1.4 Distribuirea Cheii Publice a Autorității Certificare către Entitățile Partenere

Cheile (publice) CA de verificare a semnăturii sunt puse la dispoziția Entităților Partenere într-un mod care să asigure integritatea cheii publice a CA și care să îi autentifice originea.

Cheile publice ale unei Autorităţi de Certificare care emite certificate Subiecţilor sunt distribuite exclusiv sub formă de certificate conforme recomandărilor ITU-T X.509 v.3. În cazul autoritatii de certificare certSIGN ROOT CA G2, certificatele sunt auto-semnate.

Autoritatile de certificare certSIGN isi publica certificatele prin plasarea acestora În depozitarul public disponibil la adresa: https://www.certsign.ro/ro/resurse/lantul-de-incredere-g2/

Certificatele Autoritatilor de certificare certSIGN pot fi livrate entitatilor partenere împreună cu software-ul (sisteme de operare, browsere web, clienți de e-mail etc.), ce permite utilizarea serviciilor oferite de certSIGN.

Depozitarul certificatelor impune controlul accesării după adăugarea, ștergerea certificatelor sau modificarea informațiilor aferente.

6.1.5 Marimea cheilor

Marimea cheilor folosite de Web CA, operatorii Autorității de Înregistrare și Subiecți sunt prezentate în Tabelul 6.1. Numai acești algoritmi și aceste dimensiuni de chei sunt permise pentru CA-urile enumerate în tabel, conform cu ultima versiune a ETSI TS 119 312:

Proprietarul cheii	Uzul principal a cheii		
	RSA pentru semnarea certificatelor și CRL	**RSA pentru semnarea mesajelor**	**RSA pentru schimbul de chei**
certSIGN ROOT CA G2	4096 bit	-	-
certSIGN Qualified CA	4096 bit	-	-
certSIGN Public CA	4096 bit	-	-
certSIGN Web CA	4096 bit	-	-
certSIGN Web CA G2	4096 bit	-	-

Table 6.1. Marimea cheilor utilizate

6.1.6 Parametrii de generare a Cheilor Publice și verificarea calității

certSIGN are o procedură documentată pentru efectuarea generării de perechi de chei pentru CA-uri. Procedurile de verificare includ pași de verificare a faptului că valoarea exponentului

public este un număr impar egal cu 3 sau mai mult. Modulul trebuie să aibă următoarele caracteristici: un număr impar, nu puterea unui nr. prim și să nu aibă factori mai mici de 752.

În plus, exponentul public este 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 Chapter 7.1.1.2) din cadrul extensiilor standard ale certificatelor X.509 v3. Acest câmp trebuie verificat în mod obligatoriu de aplicaţia Beneficiarului care face managementul certificatelor.

Cheile private corespunzând certificatelor ROOT CA G2 pot fi folosite pentru a semna:

1. Certificate auto-semnate reprezentând însuși Root CA-ul;
2. Certificate pentru CA-urile subordonate;
3. Certificate pentru verificarea răspunsurilor OCSP.

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 şi 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) şi legate de asigurarea confidenţialităţii,

c) **keyEncipherment**: folosite pentru criptarea cheilor algoritmilor simetrici, oferind confidenţialitatea datelor,

d) **dataEncipherment**: folosite pentru criptarea datelor Subiectului, altele decât cele descrise la punctele c) și e),

e) **keyAgreement**: folosite pentru protocoale de schimare 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 şi suspendate emise de entităţile care oferă servicii de certificare,

h) **encipherOnly**: poate fi folosit exclusiv cu bitul keyAgreement pentru a indica scopul de criptare a datelor în cadrul protocoalelor de schimbare a cheilor,

i) **decipherOnly**: poate fi folosit exclusiv cu bitul keyAgreement pentru a indica scopul de decriptare a datelor în cadrul protocoalelor de schimbare a cheilor.

6.2 Protecția cheii private și controalele modulului criptografic

Fiecare Subiect, operator al Autorității de Certificare și Autoritate de Certificare generează și stochează cheia sa private folosind un sistem de încredere care previne pierderea, dezvăluirea, modificarea sau accesul neautorizat la cheia privată. Dacă o Autoritate de Certificare generează o pereche de chei la cererea autorizată a Subiectului/Beneficiarului, trebuie să o livreze în siguranță Subiectului și să impună Subiectului să își protejeze cheia privată.

certSIGN utilizează dispozitive criptografice securizate corespunzătoare pentru a îndeplini sarcinile de management al cheilor CA. Aceste dispozitive criptografice sunt cunoscute și ca Module de Securitate Hardware (HSM-uri).

Mecanismele hardware și software care protejează cheile private ale CA sunt documentate în mod adecvat. HSM-urile sunt pregătite, distribuite și gestionate în conformitate cu următoarele standarde tehnice:

- ETSI EN 319 401
- ETSI EN 319 411-1
- ETSI EN 319 411-2
- CA/B Forum Baseline Requirements

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.

HSM-urile nu părăsesc mediul sigur al sediului securizat al CA. În cazul în care HSM-urile necesită lucrări de întreținere sau reparații care nu pot fi efectuate în incinta securizată a CA (sub controlul dual a mai mult de un angajat cu rol de încredere), acestea sunt transportate în siguranță către fabricantul lor.

Între sesiunile de utilizare, HSM-urile sunt păstrate în siguranță în incinta securizată a CA.

Cheile private ale CA rămân sub controlul multiplu al n din m angajați. Custozii CA au funcția de a activa și dezactiva cheile private ale CA-urilor. Cheile CA-urilor sunt apoi active pentru perioade definite de timp.

Cheile de semnare private ale CA stocate pe dispozitiv criptografic securizat sunt distruse după retragerea dispozitivului.

6.2.1 Controalele și standardele modulelor criptografice

Subiectul utilizează o protecție hardware a cheilor care respectă cel puțin standardele FIPS 140-2 nivel 3 sau Common Criteria EAL 4. Generarea perechilor de chei de CA va fi efectuată într-un dispozitiv criptografic securizat, care este un sistem de încredere care respectă cel puțin standardele FIPS 140-2 nivel 3 sau Common Criteria EAL 4.

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

Controlul multi-persoană al unei chei private se aplică cheilor private ale **certSIGN Root CA G2** folosite la semnarea certificatelor și a CRL-urilor.

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 şi transferate în mod autentificat deţinătorilor acestora.

Procedura comună de transfer a secretului trebuie să includă: procesul de generare și distribuire a cheilor, acceptarea secretului eliberat și responsabilitățile care rezultă din păstrarea acestuia.

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 şi ştiut numai de el. Primirea secretului partajat şi 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.

Protejarea secretului partajat

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

- Nu va dezvălui, copia sau partaja secretul partajat 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.

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.

Responsibilitățile deținătorului secretului partajat

Deţinătorul secretului partajat trebuie să-şi îndeplinească îndatoririle şi 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.

6.2.3 Custodia Cheii Private

Cheile private de semnare ale Autorității de Certificare nu fac obiectul predării în custodie.

6.2.4 Copia de siguranță a cheii private

Autorităţile 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 regasesc 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.

Cheia private de semnare a CA este salvată, stocată și recuperate doar de personal cu roluri de încredere utilizând, cel puțin, control dual într-un mediu securizat fizic. Numărul personalului autorizat să îndeplinească această funcție este menținut la un nivel minim și în concordanță cu practicile CA-ului.

Copiile cheilor private de semnare ale CA sunt supuse aceluiași nivel (sau mai mare) de controale de securitate ca și cheile aflate în prezent în uz.

6.2.5 Arhivarea Cheii Private

Cheile private ale Autorităţii de Certificare folosite pentru crearea de semnaturi 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

Operația de introducere a cheii private într-un modul criptografic se realizeaza în următoarele cazuri:

- În cazul creării copiilor de siguranță pentru cheile private stocate într-un modul criptografic, poate fi necesară, ocazional, (de ex. în cazul compromiterii sau defectării modulului) introducerea unei perechi de chei într-un modul de securitate diferit,
- Este necesar transferul de către entitate a unei chei private din modulul operațional utilizat pentru operațiuni standard către un alt modul; situația poate apărea în cazul defectării modulului sau atunci când este necesară distrugerea sa.

Introducerea unei chei private într-un modul de securitate este o operaţiune critică și de aceea în timpul executării operației 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 Autorităţii de Certificare **certSIGN ROOT CA G2** necesită restaurarea cheii de pe carduri în prezenţa unui număr corespunzător de deţinători ai secretului partajat care protejează modulul ce conţine cheile private. Deoarece fiecare Autoritate de Certificare poate deţine o copie criptată a cheii sale private, 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.

certSIGN își protejează cheile private în module de securitate hardware (HSM) care au fost validate conform cel puțin FIPS 140-2 nivel 3, sau FIPS 140-3 nivel 3, sau un profil de protecție Common Criteria Protection Profile sau Security Target, EAL 4 (sau mai mare), care include cerințe de protecție a cheii private și a altor active împotriva amenințărilor cunoscute.

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.

Între sesiunile de utilizare, HSM-urile sunt păstrate în siguranță în incinta securizată a 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

Toate cheile private ale **certSIGN ROOT CA G2** sunt introduse în modul după generare, importate sub formă criptată dintr-un alt modul sau restaurate dintr-un secret partajat. 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 şi folosirea codului PIN, cheia privată rămâne în stare activă până la scoaterea cardului din modul.

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.

Dezactivarea unei chei private se efectuează atunci când cardul este scos din modul.

6.2.10 Metoda de distrugere a cheii private

La sfârșitul duratelor de viață, cheile private ale CA sunt distruse de roluri de încredere din cadrul CA, în prezența a mai mult de un reprezentant al Comitetului de Management al Politicilor și Procedurilor, pentru a se asigura că aceste chei private nu mai pot fi recuperate sau utilizate niciodată.
Cheia privată CA poate fi distrusă prin ștergerea tuturor cardurilor HSM (Operator și Administrator). În plus, HSM permit resetarea dispozitivului prin acces fizic și setări pe dispozitiv. Aceasta reinitializează dispozitivul și suprascrie toate datele din acesta cu zerouri binare. În cazurile în care această procedură de resetare sau de reinitializare nu reușește, certSIGN va zdrobi, arunca și / sau incinera dispozitivul într-o manieră care distruge capacitatea de a extrage orice secret.
Aceste module hardware sunt tratate într-un mod securizat așa cum s-a descris în cadrul procedurilor interne documentate de distrugere a cheilor. Înregistrările asociate sunt arhivate în siguranță. CMPP autorizează în scris distrugerea cheii private a CA și personalul alocat pentru aceasta activitate.
Fiecare distrugere a unei chei private este înregistrată în jurnalul de evenimente.

6.2.11 Evaluarea Modulului Criptografic

Vezi mai sus (6.2.2).

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.

Cheia / cheile de semnare a / ale CA utilizate pentru generarea de certificate și / sau emiterea informațiilor despre starea de revocare, 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.

Atributele certificatului ROOT CA G2 (certificat auto-semnat) vor fi compatibile cu utilizarea definită a cheilor, așa cum se prevede în Recomandarea ITU-T X..

6.3.1 Arhivarea cheilor publice

certSIGN își arhivează propriile chei publice de CA. A se vedea secțiunea 5.5 a CPP, pentru condițiile de arhivare.

Scopul arhivării cheilor publice este acela de a crea posibilitatea verificării semnăturii electronice după eliminarea unui certificat din depozitar. Acest lucru este foarte important în cazul furnizării 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 Subiecţilor cărora le-au fost emise certificate. Cheile publice ale Autorităţii de Certificare sunt arhivate împreună cu cheile private, în modul descris în Capitolul 6.2.5. Certificatele pot fi arhivate, de asemenea, local de către Subiecți, în special atunci când acest lucru este cerut de aplicaţia folosită (de exemplu, sistemele de poştă electronică).

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

Administratorul de securitate verifică integritatea arhivelor de chei publice de două ori pe an. Scopul acestei verificări este de a asigura faptul că nu sunt goluri în arhive și că certificatele din arhive nu au fost modificate. Mecanismele de verificare a integrităţii arhivelor ţin 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 timp de cel puțin 10 ani.

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, şi o perioadă de validitate a cheii private. Perioada maxima de utilizare a cheilor Subiecţilor nu poate depăşi 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 Subiecţilor sunt descrise în Tabelul 6.3.2.2

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

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

Deținătorul cheii	Scopul principal al folosirii cheii
	RSA pentru semnarea de certificate și CRL
certSIGN ROOT CA G2	25 ani
certSIGN Public CA	10 ani
certSIGN Qualified CA	10 ani
certSIGN Web CA	10 ani
certSIGN Web CA G2	7 ani

Table 6.3.2.1 Perioada maximă de utilizare a certificatelor CA

6.4 Datele de activare

6.4.1 Generarea și instalarea datelor de activare

Datele de activare sunt folosite în două situații principale:

- Ca element al unei proceduri de autentificare bazate pe unul sau mai mulți factori (așa-numitele fraza de autentificare, de ex. parolă, cod PIN etc),
- Ca parte a secretului partajat.

Operatorii și administratorul Autorităţii de Înregistrare şi ai Autorităţilor de Certificare, precum și alte persoane care îndeplinesc rolurile descrise în Capitolul 5.2, trebuie să folosească parole rezistente (token-uri/carduri) ca sa se autentifice la rolurile lor. Cheile lor private care sunt generate pe dispozitive de semnătură electronică calificate sau smartcard-HSM de catre certSIGN sunt asociate cu datele de activare ale utilizatorului (cod PIN) fiind personalizate și distribuite în siguranță. certSIGN garantează că datele de activare ale operatorilor și administratorilor RA și CA și sunt gestionate și protejate de astfel de participanți, prin proceduri interne aplicabile puse la dispoziția acestor participanți.

Secretele partajate folosite pentru protejarea cheii private a Autorităţii de Certificare sunt generate în concordanţă cu cerinţele prezentate în Capitolul 6.2 şi păstrate pe carduri criptografice. Cardurile sunt protejate printr-un cod PIN. Secretele partajate devin date de activare după activarea acestora, de exemplu, prin introducerea corectă a codului PIN care protejează cardul. certSIGN asigură faptul că datele de activare a cheilor și a operațiunilor de activare a cheilor private ale CA, sunt generate, gestionate, stocate și arhivate așa cum s-a descris în subsecțiunea relevantă a secțiunilor 6.1 și 6.2. Instalarea și recuperarea perechilor de chei ale CA într-un dispozitiv criptografic securizat necesită controlul simultan al cel puțin doi angajați cu roluri de încredere.

6.4.2 Protejarea datelor de activare

Protejarea datelor de activare include metode de control a datelor de activare 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 se bazează pe cheia privată sau pe distribuirea informaţiilor de activare în secrete partajate.

Datele de activare folosite pentru activarea cheii private trebuie să fie protejate prin intermediul unor controale criptografice și printr-un control al accesului fizic. Datele de activare trebuie să fie memorate (nu scrise) de către entitatea autentificată. În cazul în care datele de activare sunt scrise, nivelul lor de protecție ar trebui să fie aceleași ca al datelor protejate prin utilizarea unui card criptografic. Mai multe încercări nereușite de a accesa modulul criptografic trebuie să ducă la blocarea acestuia. Datele de activare stocate nu trebuie să fie păstrate împreună cu cardul criptografic.

6.4.3 Alte aspecte ale datelor de activare

Nu este stipulat.

6.5 Controale de securitate a calculatoarelor

Sarcinile Autorităților de Înregistrare și ale Autorităților de Certificare care funcționează în cadrul certSIGN sunt realizate prin intermediul unor dispozitive hardware și al unor aplicații software de încredere.

6.5.1 Cerințe tehnice specifice ale securității calculatoarelor

Măsurile de securitate care protejează sistemele de calcul sunt aplicate la nivelul sistemului de operare, al aplicaţiilor precum și din punct de vedere fizic.

Computerele sunt configurate cu următoarele mecanisme de securitate:

- Autentificarea obligatorie la nivelul sistemului de operare şi al aplicaţiilor,
- Control discreţionar al accesului,
- Posibilitatea de a efectua un audit de securitate,
- Calculatorul este accesibil doar personalului autorizat, cu roluri de încredere în certSIGN,
- Separarea sarcinilor, conform rolului în cadrul sistemului,
- Identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- Prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către un proces autorizat,
- Protecţia criptografică a schimburilor de informaţii și protecţia bazelor de date,
- Arhivarea istoricului operaţiunilor executate pe un calculator și a datelor necesare auditării,
- Cale sigură ce permite identificarea şi autentificarea rolurilor şi a personalului care îndeplineşte aceste roluri,
- Metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicaţiilor şi a sistemului de operare,
- Mijloace de monitorizare și alertare în cazul accesului neautorizat la resursele de calcul.

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

Sistemul informatic certSIGN îndeplinește cerințele descrise în standardele ETSI: ETSI EN 319 411-2 (Cerințe de politică și de securitate pentru furnizorii de servicii de incredere care eliberează certificate, Partea 2: Cerințe pentru furnizorii de servicii de încredere care eliberează certificate calificate UE).

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 și 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 de 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 şi 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 şi în concordanţă cu configurarea acceptată şi implementată.

Controalele aplicate sistemelor certSIGN permit verificarea continuă a integrităţii aplicaţiilor, versiunii și autentificarea şi 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 la 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.

Configuratiile Sistemelor de Emitere, a Sistemelor de Management al Certificatelor, a Sistemelor Suport de Securitate si a Sistemelor Front-End/ Sistemelor de Suport Intern sunt verificate cel putin saptamanal pentru a determina orice schimbari care ar viola politicile de securitate ale CA-ului.

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 dedicata 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 protejeaza reteaua si sistemele impotriva atacurilor. In acest scop si in baza unei evaluari a riscurilor si al bunelor practice, implementăm controale de securitate integrate:

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 celor 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 disponibilitaea serviciilor, în cazul unui singur eșec.
g) Se realizează o scanare standard 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 sistemle 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 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.

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.

Sistemul **certSIGN ROOT CA** se află într-o zonă de înaltă securitate cu separare fizică, si este fie in starea offline, fie, când este online, este separat fizic, fără contact direct cu exteriorul.

Conform procedurii interne certSIGN pentru gestionarea vulnerabilităților tehnice, termenele stabilite pentru remedierea vulnerabilităților sunt următoarele:

- 48 de ore – pentru vulnerabilități cu severitate „critică”
- 96 de ore – pentru vulnerabilități cu severitate „ridicată”
- 30 de zile – pentru vulnerabilități cu severitate „medie”
- 180 de zile – pentru vulnerabilități cu severitate „scăzută”.

6.8 Marcare temporală

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

7 Profilul certificatelor, CRL și OCSP

Profilul certificatelor şi 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 şi extensiile folosite de certSIGN.

7.1 Profilul certificatului

Profilul câmpurilor de bază pentru certificatul certSIGN ROOT CA G2 este descris în Tabelul 7.1.

Numele câmpului	Valoarea sau restricțiile valorii	
Versiune	3	
Serie	110034b64ec6362d36	
Altoritm de semnare	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Emitent (Nume distinctiv)	Department (OU)=	certSIGN ROOT CA G2
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Nu înainte de (data de început a validității)	Feb 6 09:27:35 2017 GMT	
Nu înainte de (data de început a validității)	Feb 6 09:27:35 2042 GMT	
Subiect (Nume distinctiv)	Department (OU)=	certSIGN ROOT CA G2
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Informații despre cheia publica a subiectului	4096 bits RSA key	
Semnătură	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	

Table 7.1. Profilul câmpurilor de bază al certificatelor certSIGN ROOT CA G2

Profilul câmpurilor de bază pentru certificatele emise de certSIGN ROOT CA G2 este descris în Tabelul 7.2.

Numele câmpului	Valoarea sau restricțiile valorii	
Versiune	Version 3	
Serie	Valoare unică mai mare decât zero (0) pentru toate certificatele emise de autoritățile de certificare din cadrul certSIGN. Seriile sunt construite folosind un prefix incremental unic constrâns in baza de date care este concatenat cu o secvență aleatorie de 8 octeți Un modul criptografic hardware este utilizat pentru generarea valorii aleatorii.	
Altoritm de semnare	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Emitent (Nume distinctiv)	Department (OU)=	certSIGN ROOT CA G2
	Organization (O) =	certSIGN SA

Numele câmpului	Valoarea sau restricțiile valorii	
	Country (C) =	RO
Nu înainte de (data de început a validității)	Universal Time Coordinated based.	
Nu înainte de (data de început a validității)	Universal Time Coordinated based.	
Subiect (Nume distinctiv) **Informații despre cheia publica a subiectului**	Name (CN) =	Common Name of the CA
	Organization (O) =	Organization name
	Country (C) =	CA country
	OrganizationIdentifier (OID: 2.5.4.97)	Organization Identifier
Semnătură	Codificate în conformitate cu RFC 5280, pot conține informații despre cheile publice RSA, DSA sau ECDSA (identificatorul cheii, dimensiunea cheii în biți și valoarea cheii publice); Dimensiunea cheii RSA este prezentată în capitolul 6.1.5.	
Altoritm de semnare	Semnătura certificatului, generată și codificată în conformitate cu cerințele descrise în RFC 5280.	

Table 7.2. Profilul câmpurilor de bază ale certificatelor emise la nivelul ROOT CA

7.1.1 Numerele de versiune

Toate certificate emise de certSIGN sunt X.509 versiunea 3.

7.1.2 Extensii de certificate

Extensiile de certificate pentru certSIGN ROOT CA G2 sunt descrise în Tabelul 7.3.

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Constrângeri de bază	Subject type=CA, Path length constraint=none	Critic
Utilizare cheie	keyCertSign (bit 5), cRLSign (bit 6)	Critic
Identificatorul cheii Beneficiarului	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Ne-Critic

Table 7.3. Extensiile certificatului certSIGN ROOT CA G2

Extensiile de certificate pentru CA subordonate sunt descrise în Tabelul 7.4

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Identificatorul cheii autorității	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Ne-Critic
Identificatorul cheii Beneficiarului	KeyIdentifier este compus din hash-ul SHA-1 de 160 biți al valorii lui BIT STRING subjectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizate).	Ne-Critic
Constrângeri de bază	Subject type=CA, Path length constraint=0	Critic
Utilizarea cheii	keyCertSign (bit 5), cRLSign (bit 6)	Critic
Puncte de distribuție CRL	http://crl.certsign.ro/certsign-rootg2.crl	Ne-Critic

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Politici de certificare	Certificate Policies [1]Certificate Policy: Policy Identifier=All issuance policies[1] [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Ne-Critic
Date de access ale Autorității	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/certsign-rootg2.crt	Ne-Critic
Extended Key Usage[2]	Server Authentication (1.3.6.1.5.5.7.3.1)	Non-critical

Table 7.4. Extensiile certificatelor pentru certificatele autorităților subordonate

Extensiile de certificate pentru certificatele OCSP sunt descrise în Tabelul 7.5.

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Identificatorul cheii Autorității	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Ne-Critic
Identificatorul cheii Beneficiarului	KeyIdentifier este compus din hash-ul SHA-1 de 160 biți al valorii lui BIT STRING subjectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizate).	Ne-Critic
Utilizarea cheii	digitalSignature (bit 0)	Critic
Utilizarea sporită a cheii	OCSP Signing (1.3.6.1.5.5.7.3.9)	Ne-Critic
OCSPNoCheck	-	Ne-Critic

Table 7.5. Extensiile certificatelor pentru certificatele OCSP

7.1.3 Identificatorul algoritmului semnăturii electronice

Câmpul algoritmului de semnătură conține un identificator algoritm criptografic utilizat pentru semnătură electronică creat de o autoritate de certificare pe certificat. În cazul certSIGN, algoritmul utilizat este sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

[1] Pentru CA-urile Intermediare noi, "all issuance policies" va fi inlocuita cu o singura politica specifica.
[2] Pentru CA-urile Intermediare noi, dedicate emiterii de certificate TLS aceasta extensie va fi adaugata

7.1.4 Formate de nume

Conținutul câmpurilor de nume din certificate este conform cu cerințele din sectiunea 3.1 a acestui document, și cu cerințele politicilor de certificate din versiunea curentă a CAB Forum Baseline Requirements.

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 Constrangeri privind numele

Nu se aplică.

7.1.6 Identificatorul obiectului politicii de identificare

Certificatele de identificare a obiectului de politică utilizate la nivel de CA Root sunt descrise în Tabelul 7.6.

Nivel Root CA	Tip	OID
certSIGN ROOT CA G2	**CA certificates**	**2.5.29.32.0**
	OCSP certificate	**1.3.6.1.4.1.25017.3.1.1.1**

Table 7.6 Identificatori de obiect pentru politica de certificare

7.1.7 Utilizarea extensiei Constrângeri de politică

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 CPP care trimite catre CPP.

7.1.9 Semantica de procesare pentru extensia Politici critice de certificare

Nu se aplică.

7.2 Profilul CRL

Profilul CRL este descris în Tabelul 7.7.

Nume camp	Valoarea sau restricțiile valorii	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	Department (OU)=	certSIGN ROOT CA G2
	Organization (O) =	certSIGN SA
	Country (C) =	RO
ThisUpdate	Date emiterii CRL	
NextUpdate	Data urmatorului update CRL	
Revoked Certificates	Lista certificatelor revocate	

Table 7.7 profilul CRL pentru certSIGN ROOT CA G2

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

Extensiile CRL pentru certSIGN ROOT CA G2 sunt descrise în Tabelul 7.8.

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Authority Key Identifier	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Ne-critic
CRL Number	monotonically increasing sequence number	Ne-critic
crlEntryExtensions	ReasonCode for revocation	Ne-critic

Table 7.8. Extensions of certSIGN ROOT CA G2 CRL

Extensiile dintr-o intrare CRL (**crlEntryExtensions**) acceptate de certSIGN - conţin următoarele câmpuri:

- **ReasonCode**: codul motivului revocării certificatului. Acest câmp nu este critic și permite determinarea motivului revocării unui certificat. Sunt permise următoarele motive de revocare:
  - **keyCompromise** – compromiterea cheii;
  - **cACompromise** – compromiterea cheii Autorităţii de Certificare;
  - **affiliationChanged** – modificarea datelor Abonatului;
  - **superseded** – înnoirea certificatului;
  - **cessationOfOperation** – sistarea folosirii certificatului;
  - **removeFromCRL** – eliminarea certificatului din CRL.

Motivul ReasonCode **unspecified** – nespecificat, NU este permis.

7.3 Profilul OCSP

Protocolul de verificare on-line a stării certificatelor (OCSP) permite evaluarea stării unui certificat.

Serviciul OCSP este oferit de certSIGN în numele tuturor Autorităţilor de Certificare afiliate. Serverul OCSP, care emite confirmări ale stării certificatelor, foloseşte o pereche specială de chei pentru fiecare CA Subordonat și Root CA, generată exclusiv pentru acest scop.

Certificatul serverului OCSP trebuie să conţină extensia extKeyUsage, descrisă în RFC 5280.

Această extensie trebuie setată ca fiind ne-critică și semnifică faptul că o Autoritate de Certificare care emite certificatul pentru serverul OCSP confirmă prin semnătura sa delegarea autorizării de a emite confirmări ale stării certificatelor (aparţinând Beneficiarilor acestei autorităţi).

De asemenea, certificatul serverului OCSP conţine extensia OCSPNoCheck, descrisă de RFC 6960. Această extensie trebuie declarată ca fiind ne-critică și semnifică faptul că un client de OCSP care primeşte un răspuns semnat cu cheia privată asociată acestui certificat poate avea încredere în starea certificatului serverului OCSP, nefiind necesară verificarea stării de revocare a acestuia.

Entitatea care primeşte o confirmare emisă de serverul OCSP trebuie să suporte formatul standard de răspuns având identificatorul **id-pkix-ocsp-basic**.

Informaţiile despre starea certificatului sunt incluse în câmpul **certStatus** al structurii **SingleResponse**. Acesta poate avea una dintre următoarele trei valori principale:

- GOOD – indică faptul că certificatul este în stare validă
- REVOKED – indică faptul că certificatul a fost emis și a fost revocat sau certificatul nu a fost emis conform RFC 6960

- UNKNOWN – indică faptul că nu există suficiente informaţii pentru determinarea stării certificatului respectiv

Când răspunsul OCSP conține un cod de eroare (mesaj), răspunsul nu este semnat digital (RCF 6960).

7.3.1 Numarul 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 următoarea extensie:

Nonce – Obligarea unei solicitări și a unui răspuns pentru a preveni atacurile de replay. **Nonce** este inclus În **requestExtension** al **OCSPRequest** și repetat În campul **responseExtension** al **OCSPResponse**.

Câmpul **revocationReason** din cadrul **RevokedInfo** al **CertStatus** este prezent, și are o valoare permisă pentru CRLuri, conform cu secțiunea 7.2.2 de mai sus.

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, al CAB Forum BR, urmărim cerințele din standardul ETSI EN 319 401 și ESTI EN 319 411-1 și ne conformam 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 CPP ROOT CA 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, cu standardele tehnice ETSI 319 401, ETSI 319 411 și cerințele CA/B Forum Baseline și EV.

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 de evaluare a conformității, astfel cum este definit în Regulamentul UE 910/2014 și specificațiile CA/B Forum Baseline/EV.

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 cuprind, dar nu se limitează la, toate aspectele operațiunilor și serviciilor certSIGN specificate în acest CPP și în conformitate cu ETSI EN 319 411-1, ce include referințe normative la ETSI EN 319 401.

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 deficienței

Organismul de evaluare a conformității raportează deficiențele și neconformitățile detectate către CMPP. 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 CMPP. Raportul de audit va fi în conformitate cu ETSI EN 319 403, capitolul 7.4.4, și cu CABF Baseline Requirements, capitolul 8.6.

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 Audit intern

certSIGN 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. Preturile sunt formate conform politici interne de preț.

Serviciile oferite de certSIGN sunt soluționate 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 şi numărul serviciilor accesate şi este utilizat în special pentru serviciile de marcare temporală şi 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 îşi 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

Plăți pot fi rambursate conform condițiilor contractuale aplicabile.

9.2 Răspunderea financiară

9.2.1 Acoperirea garantiei

Nu este stipulat.

9.2.2 Alte active

Nu este stipulat.

9.2.3 Asigurarea sau acoperirea garanției pentru entitățile finale

Nu este stipulat.

9.3 Confidențialitatea informațiilor de afaceri

9.3.1 Scopul informaţiilor confidenţiale

Toate informaţiile referitoare la Subiect/Beneficiar/Entități Partenere pe care le prelucrează certSIGN sunt obţinute, păstrate şi 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;
- conţinutul 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 protecţia dispozitivelor hardware și aplicaţiilor software, informaţiile referitoare la administrarea serviciilor de certificare și la regulile de înregistrare planificate.

Persoanele care au acces la informații 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 Autorităţile 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 şi 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 protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi 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 pentru asigurarea securității datelor prelucrate, pentru protejarea drepturilor Subiecților și respectarea principiilor prevăzute de Regulamentul nr. 679/2016 și a prevederilor Regulamentului (UE) nr. 910/2014.
- 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 informatiile despre Subiect care conduc la identificarea sunt considerate ca fiind cu caracter personal.

9.4.3 Informații care nu sunt considerate private

Continutul certificatelor digitale si informatiile 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 caracter 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 certificat 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 proces 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 şi 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 şi 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 Declaraţii și garanții

9.6.1 Declaraţiile și garanțiile CA

certSIGN emite certificate compatibile X509 v3.

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.

Root CA G2 este responsabil de performanța și garanțiile CA-urilor subordonate, de conformitatea cu cerințele CAB Forum BR, și de toate răspunderile și obligațiile de despăgubiri ale CA-urilor subordonate, in limitele stabilite prin prezentul CPP, acționând conform cerințelor CAB Forum BR, ca și cum ROOT CA G2 ar fi CA-ul subordonat care a emis certificatele.

9.6.2 Declaraţiile 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 Declaraţiile și garanțiile Subiectului

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.

Subiectul este răspunzător, în special, față de Entitățile Partenere pentru orice utilizare a QSCD-ul său, inclusiv a cheilor sau a certificatului/certificatelor.

9.6.4 Declaraţiile și garanțiile Entităților Partenere

Exemplele de obligații și responsabilități ale Entităților Partenere includ (fără a se limita la):

- Realizarea cu success 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 Declaraţiile și garanțiile altor participanti

Nu este stipulat.

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 limitele stabilite de legea română, în nici un caz (cu excepția fraudelor sau a faptelor ilicite săvârșite cu intenție de către certSIGN) certSIGN nu va fi răspunzător pentru:

- Orice pierderi de profit;
- 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 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.

9.9 Despăgubiri

certSIGN nu își asumă nicio responsabilitate financiară pentru Certificatele, CRL-urile etc. utilizate în mod necorespunzător sau in scopuri ilicite.

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 incetarea lor în conformitate cu prezenta secțiune 9.10.

9.10.2 Incetarea

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 a fax-ului complet, 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 (CMPP) și Procedurilor, de aprobarea și modificarea prezentului CPP. CPP se revizuieste cel putin odata pe an.

Singurele modificări pe care le poate face CMPP 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 modifica 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.

CMPP va accepta, modifica sau respinge modificarea propusă după finalizarea unei faze de revizuire.

Orice modificări la CPP sunt aprobate de CMPP și sunt anunțate clienților certSIGN. Subiectii / 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 CMPP vor fi diseminate părților interesate inainte de sau la publicare. Data intrării în vigoare este indicată pe pagina titlului prezentului CPP.

9.12.3 Circumstanțele în care OID trebuie schimbat

Nu este stipulat.

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

Nu este stipulat.

9.17 Alte prevederi

Nu este stipulat.