

# Codul de Practici și Proceduri al certSIGN Web CA pentru certificate SSL DV

Versiunea 2.1

Data: 15 Ianuarie 2026

---

## Notă importantă

Acest document este proprietatea certSIGN SA

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

Telefon: 004-021-31.19.901

Web: [www.certsign.ro](http://www.certsign.ro)

## Istoric Document

| Versiune | Data efectivă     | Motiv                          | Persoana care a făcut modificarea |
|----------|-------------------|--------------------------------|-----------------------------------|
| 1.0      | 6 Octombrie 2022  | Publicarea primei versiuni     | Manager Politici PKI              |
| 1.1      | 31 Ianuarie 2023  | Revizuire anuală               | Manager Politici PKI              |
| 1.2      | 31 Iulie 2023     | Actualizari conform cu CABF BR | Manager Politici PKI              |
| 1.3      | 31 Ianuarie 2024  | Revizuire anuală               | Manager Politici PKI              |
| 1.4      | 31 Martie 2024    | Adăugare chei de 3k și 4k      | Manager Politici PKI              |
| 1.5      | 18 Aprilie 2024   | Adăugare certificat încrucișat | Manager Politici PKI              |
| 1.6      | 15 August 2024    | Actualizari cf. CABF BR        | Manager Politici PKI              |
| 1.7      | 26 Noiembrie 2024 | Adaugare metoda ACME           | Manager politici PKI              |
| 1.8      | 15 Ianuarie 2025  | Revizuire anuală               | Manager Politici PKI              |
| 1.9      | 30 Aprilie 2025   | Revizuire si afisare politica  | Manager Politici PKI              |
| 2.0      | 30 Noiembrie 2025 | Adaugare mass revocation       | Manager Politici PKI              |
| 2.1      | 15 Ianuarie 2026  | Revizuire anuală               | Manager Politici PKI              |

## Acest document a fost creat de către și este proprietatea:

| Proprietar | Autor                | Data creării   |
|------------|----------------------|----------------|
| certSIGN   | Manager Politici PKI | Octombrie 2022 |

## Lista de distribuție

| Destinație      | Data distribuirii |
|-----------------|-------------------|
| Public-Internet | Octombrie 2022    |
| Public-Internet | Ianuarie 2023     |
| Public-Internet | Iulie 2023        |
| Public-Internet | Ianuarie 2024     |
| Public-Internet | Martie 2024       |
| Public-Internet | Aprilie 2024      |
| Public-Internet | August 2024       |
| Public-Internet | Noiembrie 2024    |
| Public-Internet | Ianuarie 2025     |
| Public-Internet | Aprilie 2025      |
| Public-Internet | Noiembrie 2025    |
| Public-Internet | Ianuarie 2026     |

## Acest document a fost aprobat de:

| Versiune | Nume  | Data           |
|----------|---|----------------|
| 1.0      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Octombrie 2022 |
| 1.1      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Ianuarie 2023  |
| 1.2      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Iulie 2023     |
| 1.3      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Ianuarie 2024  |
| 1.4      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Martie 2024    |

### certSIGN S.A.

Cod fiscal **RO18288250**, Registrul Comerțului: **J2006000484402**, EUID: **ROONRC.J2006000484402**, Capital social: **2.130.120,00 LEI**

Sediul social: Șoseaua Olteniței Nr. 107A, Corp C1, Etaj 1, Camera 16, Sector 4, București

Telefon: +40 31 101 18 70, Fax: +40 21 311 99 05, E-mail: office@certsign.ro

ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR

ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

Pag. 2 / 103

CPP DV SSL

v2.1 -Ian.2026

Public

| Versiune | Nume  | Data           |
|----------|---|----------------|
| 1.5      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Aprilie 2024   |
| 1.6      | Comitet de Management al Politicilor și Procedurilor (PPMB) | August 2024    |
| 1.7      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Noiembrie 2024 |
| 1.8      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Ianuarie 2025  |
| 1.9      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Aprilie 2025   |
| 2.0      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Noiembrie 2025 |
| 2.1      | Comitet de Management al Politicilor și Procedurilor (PPMB) | Ianuarie 2026  |

**certSIGN S.A.**Cod fiscal **RO18288250**, Registrul Comerțului: **J40/484/2006**, Capital social: **2,095,560 LEI**

Sediul social: Șoseaua Olteniței Nr. 107A, Corp C1, Etaj 1, Camera 16, Sector 4, București

Telefon: +40 31 101 18 70, Fax: +40 21 311 99 05, E-mail: office@certsign.ro

ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR

ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806; ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

Pag. 3 / 103

CPP DV SSL

v2.1 -Ian.2026

Public

## Cuprins

|       |  |    |
|-------|--|----|
| 1     | Introducere .....  | 10 |
| 1.1   | Descriere generală .....   | 10 |
| 1.2   | Denumirea documentului și identificarea .....                        | 10 |
| 1.3   | Participanți PKI .....   | 10 |
| 1.3.1 | Autoritățile de Certificare .....                                    | 11 |
| 1.3.2 | Autoritățile de Înregistrare .....                                   | 11 |
| 1.3.3 | Beneficiarii .....   | 11 |
| 1.3.4 | Entitățile partenere .....   | 12 |
| 1.3.5 | Alți participanți .....  | 12 |
| 1.4   | Utilizarea certificatului .....                                      | 12 |
| 1.4.1 | Utilizări admise ale certificatului .....                            | 12 |
| 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 .....  | 14 |
| 1.6.1 | Definiții .....  | 14 |
| 1.6.2 | Acronime .....   | 22 |
| 2     | Publicare și responsabilități Depozitar .....                        | 24 |
| 2.1   | Depozitari .....   | 24 |
| 2.2   | Publicarea informațiilor de certificare .....                        | 24 |
| 2.3   | Timpul sau frecvența publicării .....                                | 25 |
| 2.4   | Controlul accesului la Depozitar .....                               | 25 |
| 3     | Identificarea și autentificarea .....                                | 26 |
| 3.1   | Numele .....   | 26 |
| 3.1.1 | Tipuri de nume .....   | 26 |
| 3.1.2 | Nevoia ca Numele să fie Semnificativ .....                           | 26 |
| 3.1.3 | Anonimitatea sau pseudonimitatea Beneficiarilor .....                | 27 |
| 3.1.4 | Reguli de Interpretare a Diferitelor Formate de Nume .....           | 27 |
| 3.1.5 | Unicitatea numelor .....   | 27 |
| 3.1.6 | Recunoașterea, autentificarea și rolul mărcilor Înregistrate .....   | 27 |
| 3.2   | Validarea Inițială a Identității .....                               | 27 |
| 3.2.1 | Dovada Posesiei Cheii Private .....                                  | 27 |
| 3.2.2 | Autentificarea identității organizației .....                        | 27 |
| 3.2.3 | Autentificarea identității persoanelor fizice .....                  | 32 |
| 3.2.4 | Informații neverificate ale Beneficiarului .....                     | 32 |
| 3.2.5 | Validarea autorității .....  | 32 |
| 3.2.6 | Criterii pentru interoperare .....                                   | 32 |
| 3.3   | Identificarea și autentificarea pentru cererile de re-key .....      | 32 |
| 3.3.1 | Identificarea și autentificarea pentru re-key de rutină .....        | 32 |
| 3.3.2 | Identificarea și autentificarea pentru re-key după revocare .....    | 32 |
| 3.4   | Identificarea și autentificarea pentru cererile de revocare .....    | 33 |
| 4     | Cerințe operaționale privind ciclul de viață al certificatelor ..... | 34 |

|       |  |    |
|-------|--|----|
| 4.1   | Cererile de certificat .....   | 34 |
| 4.1.1 | Cine poate trimite o cerere de certificat .....                                    | 34 |
| 4.1.2 | Procesul de înregistrare și responsabilitățile .....                               | 34 |
| 4.2   | Procesarea cererilor de certificate .....  | 35 |
| 4.2.1 | Îndeplinirea funcțiilor de identificare și autentificare .....                     | 36 |
| 4.2.2 | Aprobarea sau respingerea cererilor de certificate .....                           | 36 |
| 4.2.3 | Timpul de procesare a cererilor de certificate .....                               | 37 |
| 4.3   | Emiterea Certificatelor .....  | 37 |
| 4.3.1 | Acțiunile CA în timpul emiterii certificatului .....                               | 37 |
| 4.3.2 | Notificarea Beneficiarului de către CA cu privire la emiterea certificatului ....  | 38 |
| 4.4   | Acceptarea certificatului .....  | 38 |
| 4.4.1 | Conduita care constituie acceptarea certificatului .....                           | 38 |
| 4.4.2 | Publicarea certificatului de către CA .....  | 38 |
| 4.4.3 | Notificarea de către CA a altor entități cu privire la emiterea certificatului ... | 39 |
| 4.5   | Utilizarea perechii de chei și a certificatului .....                              | 39 |
| 4.5.1 | Utilizarea perechii de chei și a certificatului Beneficiarului .....               | 39 |
| 4.5.2 | Utilizarea cheii publice și a certificatului unei Entități Partenere .....         | 39 |
| 4.6   | Reînnoirea Certificatului .....  | 39 |
| 4.6.1 | Circumstanța reînnoirii certificatului .....                                       | 39 |
| 4.6.2 | Cine poate solicita reînnoirea .....   | 39 |
| 4.6.3 | Procesarea solicitărilor de reînnoire a certificatelor .....                       | 39 |
| 4.6.4 | Notificarea abonatului cu privire la eliberarea unui nou certificat .....          | 39 |
| 4.6.5 | Conduita care constituie acceptarea unui certificat de reînnoire .....             | 39 |
| 4.6.6 | Publicarea certificatului de reînnoire de către CA .....                           | 40 |
| 4.6.7 | Notificarea eliberării certificatului de către CA către alte entități .....        | 40 |
| 4.7   | Re-key Certificat .....  | 40 |
| 4.7.1 | Circumstanțe re-key certificat .....   | 40 |
| 4.7.2 | Cine poate solicita certificarea unei noi chei publice .....                       | 40 |
| 4.7.3 | Procesarea cererilor de re-key al certificatelor .....                             | 40 |
| 4.7.4 | Notificarea emiterii noului certificat către beneficiar .....                      | 40 |
| 4.7.5 | Conduita ce constituie acceptarea unui certificate re-key .....                    | 40 |
| 4.7.6 | Publicarea certificatului re-key de către CA .....                                 | 40 |
| 4.7.7 | Notificarea eliberării certificatului de către CA altor entități .....             | 40 |
| 4.8   | Modificarea Certificatului .....   | 40 |
| 4.8.1 | Circumstanța modificării certificatului .....                                      | 40 |
| 4.8.2 | Cine poate solicita modificarea .....  | 41 |
| 4.8.3 | Procesarea cererilor de modificare a certificatului .....                          | 41 |
| 4.8.4 | Notificarea abonatului cu privire la eliberarea unui nou certificat .....          | 41 |
| 4.8.5 | Conduita care constituie acceptarea unui certificat modificat .....                | 41 |
| 4.8.6 | Publicarea certificatului modificat de către CA .....                              | 41 |
| 4.8.7 | Notificarea eliberării certificatului de către CA către alte entități .....        | 41 |
| 4.9   | Revocarea și Suspendarea Certificatului .....                                      | 41 |
| 4.9.1 | Circumstanțele revocării .....   | 41 |
| 4.9.2 | Cine poate solicita revocarea certificatelor .....                                 | 43 |
| 4.9.3 | Procedura cererilor de revocare .....  | 43 |
| 4.9.4 | Perioada de grație a cererii de revocare .....                                     | 43 |
| 4.9.5 | Termenul în care CA trebuie să proceseze cererea de revocare .....                 | 43 |
| 4.9.6 | Verificarea cerințelor de revocare pentru Entitățile Partenere .....               | 44 |

|        |   |    |
|--------|---|----|
| 4.9.7  | Frecvența de emitere a CRL-urilor.....                                    | 44 |
| 4.9.8  | Latența maximă pentru CRL-uri .....                                       | 44 |
| 4.9.9  | Disponibilitatea verificării on-line a revocării/stării .....             | 44 |
| 4.9.10 | Verificarea on-line a cerințelor de revocare .....                        | 45 |
| 4.9.11 | Alte forme disponibile pentru anunțarea revocării .....                   | 45 |
| 4.9.12 | Cerințe speciale referitoare la compromiterea cheii .....                 | 45 |
| 4.9.13 | Circumstanțe pentru suspendare .....                                      | 45 |
| 4.9.14 | Cine poate solicita suspendarea .....                                     | 45 |
| 4.9.15 | Procedura de solicitare a suspendării.....                                | 46 |
| 4.9.16 | Limitări ale perioadei de suspendare .....                                | 46 |
| 4.10   | Servicii privind starea certificatelor .....                              | 46 |
| 4.10.1 | Caracteristici operaționale .....   | 46 |
| 4.10.2 | Disponibilitatea serviciului .....  | 46 |
| 4.10.3 | Funcții opționale .....   | 46 |
| 4.11   | Încetarea abonamentului.....  | 46 |
| 4.12   | Custodie și recuperare chei.....  | 46 |
| 4.12.1 | Principalele politici și practici de escrow și recuperare.....            | 46 |
| 4.12.2 | Politica și practicile cheie de încapsulare și recuperare a sesiunii..... | 46 |
| 5      | Facilitate, Management și Controale Operaționale .....                    | 47 |
| 5.1    | Controale fizice .....  | 48 |
| 5.1.1  | Amplasarea și construcția sediului .....                                  | 48 |
| 5.1.2  | Accesul fizic .....   | 49 |
| 5.1.3  | Alimentarea cu curent și aerul condiționat .....                          | 49 |
| 5.1.4  | Expunerea la apă.....   | 50 |
| 5.1.5  | Prevenirea și protecția împotriva incendiilor .....                       | 50 |
| 5.1.6  | Depozitarea mediilor de stocare a informațiilor .....                     | 50 |
| 5.1.7  | Eliminarea deșeurilor .....   | 50 |
| 5.1.8  | Stocarea copiilor de siguranță în afara locației .....                    | 50 |
| 5.2    | Controale procedurale.....  | 50 |
| 5.2.1  | Roluri de încredere .....   | 50 |
| 5.2.2  | Numărul de persoane necesare pentru fiecare sarcină .....                 | 52 |
| 5.2.3  | Identificarea și autentificarea pentru fiecare rol .....                  | 52 |
| 5.2.4  | Rolurile care necesită separarea sarcinilor.....                          | 52 |
| 5.3    | Controlul personalului .....  | 53 |
| 5.3.1  | Calificări, experiență și aprobări necesare.....                          | 53 |
| 5.3.2  | Proceduri de verificare a antecedentelor .....                            | 53 |
| 5.3.3  | Cerințele de pregătire a personalului .....                               | 53 |
| 5.3.4  | Frecvența și cerințele stagiilor de pregătire .....                       | 54 |
| 5.3.5  | Frecvența și secvența rotației posturilor.....                            | 54 |
| 5.3.6  | Sancțiunile pentru acțiunile neautorizate .....                           | 54 |
| 5.3.7  | Cerințele pentru contractanții independenți .....                         | 54 |
| 5.3.8  | Documentația oferită personalului.....                                    | 54 |
| 5.4    | Procedurile de înregistrare a datelor de audit.....                       | 54 |
| 5.4.1  | Evenimente Înregistrate .....   | 55 |
| 5.4.2  | Frecvența procesării jurnalelor de evenimente.....                        | 57 |
| 5.4.3  | Perioada de păstrare a log-urilor de audit .....                          | 57 |
| 5.4.4  | Protecția jurnalelor de evenimente.....                                   | 57 |
| 5.4.5  | Procedura de backup a log-urilor de Audit.....                            | 58 |

|        |  |    |
|--------|--|----|
| 5.4.6  | Sistemul de colectare a datelor pentru audit (intern vs. extern).....                              | 58 |
| 5.4.7  | Notificarea la eveniment – subiectul în cauză .....  | 58 |
| 5.4.8  | Evaluări de vulnerabilitate .....  | 58 |
| 5.5    | Arhivarea înregistrărilor .....  | 58 |
| 5.5.1  | Tipuri de date arhivate .....  | 59 |
| 5.5.2  | Perioada de retenție a arhivei.....  | 59 |
| 5.5.3  | Protecția arhivei .....  | 59 |
| 5.5.4  | Procedurile de back-up al arhivei .....  | 59 |
| 5.5.5  | Cerințe privind marcarea temporală a înregistrărilor.....  | 59 |
| 5.5.6  | Sistemul de colectare al arhivei (intern sau extern).....  | 60 |
| 5.5.7  | Procedurile de obținere și verificare a informațiilor arhivate.....                                | 60 |
| 5.6    | Schimbarea cheilor .....   | 60 |
| 5.7    | Compromiterea și recuperare în caz de dezastru .....   | 60 |
| 5.7.1  | Procedurile de administrare a incidentelor și compromiterilor.....                                 | 60 |
| 5.7.2  | Compromiterea resurselor de calcul, a aplicațiilor software și/sau datelor ...                     | 61 |
| 5.7.3  | Proceduri care se aplică la compromiterea cheii private a unei entități.....                       | 62 |
| 5.7.4  | Capacități de Continuitate a afacerii în caz de dezastru.....                                      | 63 |
| 5.8    | Încetarea activității Autorității de Certificare sau a Autorității de Înregistrare .....           | 63 |
| 5.9    | Lanțul de aprovizionare .....  | 64 |
| 6      | Controale tehnice de securitate.....   | 66 |
| 6.1    | Generarea și instalarea perechii de chei .....   | 66 |
| 6.1.1  | Generarea perechilor de chei.....  | 66 |
| 6.1.2  | Distribuirea Cheii Private către Beneficiar .....  | 68 |
| 6.1.3  | Distribuirea Cheii Publice către emitentul certificatului .....                                    | 68 |
| 6.1.4  | Distribuirea Cheii Publice a Autorității Certificare către Entitățile Partenere..                  | 68 |
| 6.1.5  | Marimea cheilor.....   | 68 |
| 6.1.6  | Parametrii de generare a Cheilor Publice și verificarea calității .....                            | 68 |
| 6.1.7  | Scopurile în care pot fi utilizate cheile (conform câmpului de utilizare a cheilor X.509 v3) ..... | 69 |
| 6.2    | Protecția cheii private și controalele modulului criptografic .....                                | 69 |
| 6.2.1  | Controalele și standardele modulelor criptografice .....   | 70 |
| 6.2.2  | Control multi-persoană (n din m) al cheilor private .....  | 70 |
| 6.2.3  | Custodia Cheii Private .....   | 71 |
| 6.2.4  | Copia de siguranță a cheii private .....   | 71 |
| 6.2.5  | Arhivarea Cheii Private .....  | 71 |
| 6.2.6  | Transferul Cheii Private într-un sau dintr-un modul criptografic .....                             | 71 |
| 6.2.7  | Stocarea cheilor private pe modul criptografic .....   | 72 |
| 6.2.8  | Metoda de activare a cheii private.....  | 72 |
| 6.2.9  | Metoda de dezactivare a cheii private.....   | 73 |
| 6.2.10 | Metoda de distrugere a cheii private .....   | 73 |
| 6.2.11 | Evaluarea Modulului Criptografic.....  | 73 |
| 6.3    | Alte aspecte legate de managementul perechilor de chei .....                                       | 73 |
| 6.3.1  | Arhivarea cheilor publice .....  | 73 |
| 6.3.2  | Perioadele operaționale ale certificatelor și perioadele de utilizare a cheilor private            | 74 |
| 6.4    | Datele de activare .....   | 74 |
| 6.4.1  | Generarea și instalarea datelor de activare .....  | 74 |
| 6.4.2  | Protejarea datelor de activare .....   | 75 |

|       |   |    |
|-------|---|----|
| 6.4.3 | Alte aspecte ale datelor de activare.....   | 75 |
| 6.5   | Controale de securitate informatică .....   | 75 |
| 6.5.1 | Cerințe tehnice specifice ale securității informatice.....                                      | 75 |
| 6.5.2 | Computer security rating .....  | 76 |
| 6.6   | Controale tehnice specifice ciclului de viață.....  | 76 |
| 6.6.1 | Controale specifice dezvoltării sistemului .....  | 76 |
| 6.6.2 | Controale specifice managementului securității.....   | 77 |
| 6.6.3 | Controale de securitate specifice ciclului de viață .....                                       | 77 |
| 6.7   | Controale de securitate a rețelei.....  | 77 |
| 6.8   | Marcare temporală .....   | 79 |
| 7     | Profilul certificatelor, CRL și OCSP .....  | 80 |
| 7.1   | Profilul certificatului .....   | 80 |
| 7.1.1 | Numerele de versiune .....  | 83 |
| 7.1.2 | Extensii de certificate .....   | 83 |
| 7.1.3 | Obiect de identificare a algoritmului .....   | 87 |
| 7.1.4 | Formate de nume .....   | 87 |
| 7.1.5 | Constrângeri privind numele .....   | 88 |
| 7.1.6 | Identificatorul obiectului politicii de certificare .....                                       | 88 |
| 7.1.7 | Utilizarea extensiei Constrângeri de politică .....   | 89 |
| 7.1.8 | Sintaxa și semantica atributelor de politică .....  | 89 |
| 7.1.9 | Semantica de procesare pentru extensia Politici critice de certificare .....                    | 89 |
| 7.2   | Profilul CRL.....   | 89 |
| 7.2.1 | Numerele de versiune .....  | 89 |
| 7.2.2 | CRL și extensiile de intrare CRL .....  | 89 |
| 7.3   | Profilul OCSP .....   | 91 |
| 7.3.1 | Numarul versiunilor .....   | 92 |
| 7.3.2 | Extensii OCSP .....   | 92 |
| 8     | Auditul de conformitate și alte evaluări .....  | 93 |
| 8.1   | Frecvența sau circumstanțele de evaluare .....  | 93 |
| 8.2   | Identitatea / calificările evaluatorului .....  | 93 |
| 8.3   | Relația evaluatorului cu entitatea evaluată .....   | 93 |
| 8.4   | Subiectele acoperite de evaluare .....  | 93 |
| 8.5   | Acțiuni întreprinse ca urmare a deficienței .....   | 94 |
| 8.6   | Comunicarea rezultatelor .....  | 94 |
| 8.7   | Audituri interne.....   | 94 |
| 9     | Alte elemente de afaceri și legale .....  | 96 |
| 9.1   | Tarife.....   | 96 |
| 9.1.1 | Tarifele serviciilor de emiterie și reînnoire a certificatelor digitale.....                    | 96 |
| 9.1.2 | Tarifele serviciilor de acces la certificate .....  | 96 |
| 9.1.3 | Tarifele serviciilor de revocare sau acces la informațiile despre starea<br>certificatelor..... | 96 |
| 9.1.4 | Alte tarife .....   | 96 |
| 9.1.5 | Politica de rambursare.....   | 96 |
| 9.2   | Răspunderea financiară .....  | 96 |
| 9.2.1 | Acoperirea prin asigurare.....  | 96 |
| 9.2.2 | Alte active .....   | 96 |
| 9.2.3 | Asigurarea sau acoperirea garanției pentru entitățile finale .....                              | 97 |
| 9.3   | Confidențialitatea informațiilor de afaceri .....   | 97 |

|        |  |     |
|--------|--|-----|
| 9.3.1  | Scopul informatiilor confidentiale .....   | 97  |
| 9.3.2  | Informații care nu sunt considerate a fi confidentiale.....  | 98  |
| 9.3.3  | Responsabilitatea de a proteja informațiile confidentiale .....  | 98  |
| 9.4    | Confidențialitatea datelor cu caracter personal .....  | 98  |
| 9.4.1  | Planul de asigurare a protecției datelor cu caracter personal .....  | 98  |
| 9.4.2  | Informații considerate ca fiind cu caracter personal.....  | 99  |
| 9.4.3  | Informații care nu sunt considerate private .....  | 99  |
| 9.4.4  | Responsabilitatea de a proteja informațiile private .....  | 99  |
| 9.4.5  | Notificarea persoanelor vizate și consimțământul acestora pentru utilizarea datelor cu caracter personal ..... | 99  |
| 9.4.6  | Divulgare ca urmare a unui proces administrativ sau juridic .....  | 99  |
| 9.4.7  | Alte circumstanțe pentru divulgare .....   | 99  |
| 9.5    | Drepturile de Proprietate Intelectuală .....   | 100 |
| 9.6    | Reprezentări și garanții .....   | 100 |
| 9.6.1  | Reprezentările și garanțiile CA.....   | 100 |
| 9.6.2  | Reprezentările și garanțiile RA.....   | 100 |
| 9.6.3  | Reprezentările și garanțiile Beneficiarului.....   | 100 |
| 9.6.4  | Reprezentările și garanțiile Entităților Partenere .....   | 101 |
| 9.6.5  | Reprezentările și garanțiile altor participanți.....   | 101 |
| 9.7    | Declinarea garanțiilor.....  | 101 |
| 9.8    | Limitarea răspunderii .....  | 101 |
| 9.9    | Despăgubiri .....  | 102 |
| 9.10   | Termenii și încetarea .....  | 102 |
| 9.10.1 | Termenii.....  | 102 |
| 9.10.2 | Încetarea.....   | 102 |
| 9.10.3 | Efectul terminării și supraviețuirii.....  | 102 |
| 9.11   | Notificări individuale și comunicarea cu participanții.....  | 102 |
| 9.12   | Amendamente .....  | 102 |
| 9.12.1 | Procedura pentru amendamente.....  | 102 |
| 9.12.2 | Mecanismul de notificare și perioada .....   | 103 |
| 9.12.3 | Circumstanțele în care OID trebuie schimbat.....   | 103 |
| 9.13   | Procedurile de soluționare a litigiilor .....  | 103 |
| 9.14   | Legea aplicabilă .....   | 103 |
| 9.15   | Conformitatea cu legea aplicabilă .....  | 103 |
| 9.16   | Prevederi diverse .....  | 103 |
| 9.16.1 | Întregul Acord .....   | 103 |
| 9.16.2 | Cesiunea .....   | 103 |
| 9.16.3 | Anulabilitatea .....   | 103 |
| 9.16.4 | Executarea (onorariile avocaților și renunțarea la drepturi) .....   | 103 |
| 9.16.5 | Forța Majoră .....   | 103 |
| 9.17   | Alte prevederi .....   | 103 |

## 1 Introducere

**Codul de Practici și Proceduri certSIGN Web CA** Calificat pentru certificate SSL DV – (denumit în continuare **CPP**) descrie politica de certificare și practicile pe care certSIGN le aplică în emiterea de **certIFICATE SSL DV** (cu **Validarea Domeniului**).

Structura și conținutul **CPP** respectă recomandările [RFC 3647](#) și ultimele versiuni publicate:

- [ETSI EN 319 411-1](#) (Politica DVCP 0.4.0.2042.1.6)
- [CA/B Forum Baseline Requirements](#) (Politica DV 2.23.140.1.2.1)
- [CA/Browser Forum Network and Certificate System Security Requirements](#)
- [WebTrust Principles and Criteria for Certification Authorities](#)
- [Webtrust Principles and Criteria for Certification Authorities - TLS Baseline](#)
- [Webtrust Principles and Criteria for Certification Authorities – Network Security](#)
- [Mozilla Root Store Policy](#),
- [Apple Root Certificate Program](#),
- [Microsoft Trusted Root Program](#),
- [Chrome Root Program Policy](#).

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

certSIGN, Beneficiarii, Subiecții și funcționarea Entităților Partenere asociate depind de **CPP** pentru emiterea certificatelor SSL DV. Documentul descrie, de asemenea, regulile generale de furnizare a serviciilor de certificare, precum înregistrarea Subiecților, certificarea cheii publice, rekey certificate și revocarea certificatelor.

### 1.2 Denumirea documentului și identificarea

Titlul acestui document este **Codul de Practici și Proceduri certSIGN Web CA pentru certificate SSL DV**, denumit în continuare **CPP**.

Următorii identificatori ai politicii de certificare sunt rezervați utilizării de către certSIGN Web CA pentru a afirma conformitatea cu acest document după cum:

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) certSIGN (25017) id-policy(3) id-cp (1) certSIGN Web CA (4) domain validated website authentication certificate (5)} (1.3.6.1.4.1.25017.3.1.4.5)

Documentul este disponibil în format electronic în Depozitar, la adresa <https://www.certsign.ro/ro/document/certsign-web-ca-dv-cod-practici-si-proceduri/>.

### 1.3 Participanți PKI

CPP-ul reglementează cele mai importante relații dintre entitățile certSIGN, echipele de consultanți (inclusiv auditorii) și clienții (utilizatorii serviciilor furnizate) aceștia:

- certSIGN Web CA
- Autoritatea de Înregistrare,
- Depozitar,
- Protocolul de verificare online a stării certificatelor (Autoritatea OCSP),
- Subiecți,
- Beneficiari,
- Entitățile Partenere,

- Furnizorii relevanți ai certSIGN din punct de vedere al emiterii și managementului certificatelor digitale,
- Comitetul de Management al Politicilor și Procedurilor,
- Auditori

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

### 1.3.1 Autoritățile de Certificare

certSIGN Web CA este o Autoritate de Certificare Subordonată pentru domeniul certSIGN, subordonată certSIGN ROOT CA G2. certSIGN Web CA este identificată prin următorul OID: 1.3.6.1.4.1.25017.3.1.4.



### 1.3.2 Autoritățile de Înregistrare

Autoritatea de Înregistrare primește, verifică și aprobă sau respinge cererile de înregistrare și emiterie de certificate, de rekey certificat sau revocare a certificatelor. Verificarea cererilor are ca scop autentificarea (pe baza documentelor incluse în cereri) atât a beneficiarului, cât și a datelor incluse în cerere. Autoritatea de Înregistrare poate trimite cereri către Autoritatea de Certificare corespunzătoare pentru a anula o cerere sau pentru a retrage un certificat.

Autoritatea de înregistrare este operată de certSIGN sau de o terță parte delegată.

RA externe trebuie să respecte aceleași cerințe de securitate pe care le respectă TSP în ceea ce privește resursele umane, securitatea operațională, rețeaua și datele personale.

### 1.3.3 Beneficiarii Beneficiar

Beneficiarul este entitatea juridică căreia i se emite un certificat și care a semnat cu certSIGN un acord contractual. Beneficiarii pot solicita emiteria, revocarea sau rekey-ul certificatelor Entităților finale pentru Subiecții asociați.

Beneficiarul este responsabil de:

- Notificarea imediata a certSIGN in cazul (suspiciunii de) compromiterii cheii private;
- Trimiterea, in timp util, catre certSIGN a cererilor de reinnoire a certificatelor;
- Protejarea confidentialitatii cheii sale private in accord cu prezentul document;
- Asigurarea faptului ca accesul la cheia sa privată este controlat in conformitate cu acest document.

## Subiect

Subiectul este un dispozitiv aflat sub controlul si funcționarea Beneficiarului.

### 1.3.4 Entitățile partenere

O Entitate Parteneră care folosește serviciile certSIGN poate fi orice persoană fizică sau entitate juridică care se bazează pe un Certificat Valabil. Un Furnizor de Aplicații Software nu este considerat Entitate Parteneră atunci când software-ul distribuit de un astfel de furnizor doar afișează informații referitoare la un Certificat.

O Entitate Parteneră este responsabilă de modul cum verifică starea curentă a certificatului unui Subiect. O Entitate Parteneră va utiliza informațiile dintr-un certificat (de exemplu identificatori si calificatori ai politicii de certificare) pentru a decide dacă un certificat a fost utilizat în concordanță cu scopul definit.

### 1.3.5 Alți participanți

Comitetul de Management al Politicilor și Procedurilor este un Comitet creat în cadrul certSIGN de către Consiliul de administrație pentru a supraveghea înreaga activitate a Autorităților de Certificare și a Autorităților de Înregistrare ale certSIGN. Rolurile și responsabilitățile CMPP sunt descrise în documentația internă.

Furnizorii care prestează servicii pentru certSIGN : furnizorii externi care sprijină activitățile certSIGN în baza unui acord contractual semnat.

## 1.4 Utilizarea certificatului

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

- Unul care definește aplicabilitatea certificatului,
- Și unul care presupune o listă sau o descriere a aplicațiilor permise sau interzise.

Entitatea Parteneră este responsabilă de stabilirea nivelului de credibilitate necesar pentru un certificat utilizat într-un anumit scop. Luând în considerare factorii de risc semnificativi, Entitatea Parteneră trebuie să stabilească ce tip de certificat emis de certSIGN întrunește cerințele formulate.

### 1.4.1 Utilizări admise ale certificatului

Certificatele emise de certSIGN Web CA se folosesc pentru autentificarea serverului TLS si autentificarea clientului TLS.

Certificatele pot fi utilizate în Web servere și/sau aplicații care satisfac cel puțin următoarele condiții:

- Gestionează în mod corespunzător cheile publice și cheile private,
- Certificatele și cheile publice asociate acestora sunt folosite în concordanță 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 validității (validitatea semnăturii, data expirării etc.),
- Oferă utilizatorilor informații 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

Este responsabilitatea Entității Partenere să decidă pentru ce scop vor fi considerate certificatele ca fiind de încredere. O Entitate Parteneră trebuie să ia întotdeauna în considerare nivelul de asigurare și alte informații din CPP înainte de a decide în privința aplicabilității certificatului.

#### 1.4.2 Utilizări interzise ale certificatului

Certificatele trebuie utilizate numai în concordanță cu legislația aplicabilă și în scopurile specificate în capitolul 1.4.1.

### 1.5 Administrarea politicii

#### 1.5.1 Organizația care administrează documentul

Prezentul document este administrat de către Comitetul de Management al Politicilor și Procedurilor (PPMB) al TSP certSIGN. PPMB include membri seniori din conducere, precum și personalul responsabil pentru gestionarea operațională a mediului PKI al TSP certSIGN

|                |   |
|----------------|---|
| <b>Nume</b>    | S.C. certSIGN S.A.<br>Punct de lucru: Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, București<br>050881, România<br>Registrul comerțului: J2006000484402<br>CUI: RO 18288250<br>Sediul social: Șos. Olteniței 107A, clădirea C1, etaj 1, camera 16, Sector 4,<br>București, România, Cod postal 041303 |
| <b>Telefon</b> | (+4021)3119901  |
| <b>e-mail</b>  | office@certsign.ro  |
| <b>Web</b>     | www.certsign.ro   |

Tabel: 1.5.1 Organizația care administrează documentul

#### 1.5.2 Persoana de contact

|                |   |
|----------------|---|
| <b>Nume</b>    | Comitetul de Management al Politicilor și Procedurilor (PPMB) |
| <b>Telefon</b> | (+4021)3119901  |
| <b>e-mail</b>  | office@certsign.ro  |
| <b>Web</b>     | www.certsign.ro   |

Tabel: 1.5.2 Persoana de contact

### Procedura de raportare a certificatelor cu probleme

Din cauza unor erori, limitări tehnice sau procedurale, ori din alte motive, pot exista certificate emise greșit de certSIGN (ex. certificatul emis conține informații eronate despre subiect). Mai pot exista cazuri în care un certificat este utilizat necorespunzător (ex. pentru activități infracționale). Dacă beneficiarii,

entitățile 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 [revokecsn@certsign.ro](mailto:revokecsn@certsign.ro), informând Autoritatea de Certificare emitentă despre motive rezonabile de revocare a certificatului. certSIGN CA va începe investigarea unui raport de certificate cu probleme în 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 reclamație 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 [revokecsn@certsign.ro](mailto:revokecsn@certsign.ro).

### 1.5.3 Persoana care decide conformitatea CPP cu politica

|                |   |
|----------------|---|
| <b>Nume</b>    | Comitetul de Management al Politicilor și Procedurilor (PPMB) |
| <b>Telefon</b> | (+4021)3119901  |
| <b>e-mail</b>  | office@certsign.ro  |
| <b>Web</b>     | www.certsign.ro   |

Tabel: 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 de aprobarea CPP.

Procedura de aprobare este cuprinsă într-o instrucțiune internă.

Beneficiarii vor respecta CPP-ul implementat și publicat la: <https://www.certsign.ro/ro/document/certsign-web-ca-dv-cod-practici-si-proceduri/>

Beneficiarii care nu acceptă noii termenii și reglementările modificate ale CPP, sunt obligați să depună, în termen de 15 zile de la data la care noua versiune a CPP a fost aprobată, o declarație în acest sens. Acest lucru va duce la încetarea contractului de prestări servicii de certificare și la revocarea certificatului emis în baza acestuia.

## 1.6 Definiții și acronime

### 1.6.1 Definiții

**Afiliat:** O corporație, un parteneriat, o societate în comun sau o altă entitate care controlează, este controlată sau se află sub control comun cu o altă entitate, sau o agenție, un

departament, o subdiviziune politică sau orice entitate care funcționează sub controlul direct al unei entități guvernamentale.

**Beneficiar/solicitant:** Persoana fizică sau entitatea juridică care solicită (sau cere reînnoirea) unui certificat. Odată ce certificatul este emis, beneficiarul/solicitantul este denumit abonat. În cazul certificatelor emise pentru dispozitive, beneficiarul/solicitantul este entitatea care controlează sau operează dispozitivul menționat în certificat, chiar dacă dispozitivul trimite cererea efectivă de certificat.

**Reprezentantul beneficiarului/ solicitantului:** O persoană fizică sau un sponsor uman care este fie Beneficiarul, fie angajat al Beneficiarului, fie un agent autorizat care are autoritatea expresă de a reprezenta Beneficiarul: (i) care semnează și transmite sau aprobă o cerere de certificat în numele Beneficiarului, și/sau (ii) care semnează și transmite un Contract de abonat în numele Beneficiarului, și/sau (iii) care recunoaște Termenii de utilizare în numele Beneficiarului atunci când Beneficiarul este un afiliat al AC sau este AC.

**Furnizor de software de aplicație:** Un furnizor de software de navigare pe internet sau de alt software de aplicație al părții care se bazează pe el, care afișează sau utilizează certificate și încorporează certificate rădăcină.

**Scrisoare de atestare:** O scrisoare care atestă că informațiile vizate sunt corecte, scrisă de un contabil, avocat, funcționar guvernamental sau altă parte terță de încredere pe care se bazează în mod obișnuit pentru astfel de informații.

**Perioada de audit:** Într-un audit pe perioade de timp, perioada cuprinsă între prima zi (începutul) și ultima zi de funcționare (sfârșitul) acoperită de auditori în cadrul misiunii lor. (Aceasta nu este aceeași perioadă cu perioada în care auditorii se află la fața locului, la AC). Regulile de acoperire și durata maximă a perioadelor de audit sunt definite în secțiunea 8.1.

**Raportul de audit:** Un raport al unui auditor calificat care precizează opinia auditorului calificat cu privire la conformitatea proceselor și controalelor unei entități cu dispozițiile obligatorii ale prezentelor cerințe.

**Nume de domeniu de autorizare:** Numele de domeniu utilizat pentru a obține autorizația de emisie a certificatelor pentru un anumit FQDN. CA poate utiliza FQDN-ul returnat de o căutare DNS CNAME ca FQDN în scopul validării domeniului. În cazul în care FQDN conține un caracter wildcard, atunci CA TREBUIE să elimine toate etichetele wildcard din partea cea mai din stânga a FQDN-ului solicitat. CA poate elimina zero sau mai multe etichete de la stânga la dreapta până când întâlnește un nume de domeniu de bază și poate utiliza oricare dintre valorile intermediare în scopul validării domeniului.

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

**Numele domeniului de bază:** Porțiunea dintr-un FQDN solicitat care este primul nod al numelui de domeniu din stânga unui sufix controlat de registru sau public plus sufixul controlat de registru sau public (de exemplu, "example.co.uk" sau "example.com"). În cazul FQDN-urilor în care nodul de nume de domeniu cel mai din dreapta este un gTLD care are specificația 13 a ICANN în acordul de registru, gTLD-ul însuși poate fi utilizat ca nume de domeniu de bază.

**CAA:** Din RFC 8659 (<http://tools.ietf.org/html/rfc8659>): "Înregistrarea de resurse DNS "Certification Authority Authorization (CAA)" permite deținătorului unui nume de domeniu DNS să specifice autoritățile de certificare (CA) autorizate să emită certificate pentru domeniul respectiv. Publicarea înregistrărilor de resurse CAA permite unei autorități de certificare

publice să implementeze controale suplimentare pentru a reduce riscul de emiteri neintenționată de certificate."

**Pereche de chei CA:** O pereche de chei în care cheia publică apare ca informație privind cheia publică subiect în unul sau mai multe certificate CA rădăcină și/sau certificate CA subordonate.

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

**Date de certificat:** Cererile de certificat și datele aferente acestora (obținute de la solicitant sau în alt mod) aflate în posesia sau sub controlul AC sau la care AC are acces.

**Procesul de gestionare a certificatelor:** Procesele, practicile și procedurile asociate cu utilizarea cheilor, a software-ului și a hardware-ului, prin care AC verifică datele de certificat, emite certificate, menține un depozit și revocă certificatele.

**Politica de certificare:** Un set de reguli care indică aplicabilitatea unui certificat numit la o anumită comunitate și/sau implementare PKI cu cerințe de securitate comune și descrie limitele și utilizările acceptabile ale certificatelor dintr-o anumită PKI.

**Raport privind problemele de certificat:** Plângere privind suspiciunea de compromitere a cheilor, de utilizare abuzivă a certificatelor sau alte tipuri de fraudă, compromitere, utilizare abuzivă sau comportament necorespunzător în legătură cu certificatele.

**Profil de certificat:** Un set de documente sau fișiere care definește cerințele privind conținutul și extensiile certificatelor în conformitate cu secțiunea 7, de exemplu, o secțiune din CPP a unei CA sau un fișier șablon de certificat utilizat de software-ul CA.

**Certificate Revocation List (Lista de revocare a certificatelor):** O listă de certificate revocate, actualizată în mod regulat și marcată în timp, creată și semnată digital de către AC care a emis certificatele.

**Autoritatea de certificare (AC/CA):** O organizație care este responsabilă de crearea, emiterea, revocarea și gestionarea certificatelor. Termenul se aplică în egală măsură atât AC rădăcină, cât și AC intermediare.

**Declarația privind practicile de certificare (CPS)** este o declarație a practicilor pe care o autoritate de certificare le utilizează pentru emiterea și gestionarea certificatelor.

**Control:** "Control" (și sensurile sale corelate, "controlat de" și "sub control comun cu") înseamnă posesia, direct sau indirect, a puterii de a:

- (1) de a dirija managementul, personalul, finanțele sau planurile unei astfel de entități;
- (2) de a controla alegerea majorității directorilor; sau
- (3) de a vota acea parte din acțiunile cu drept de vot necesară pentru "control" în conformitate cu legislația din jurisdicția de constituire sau de înregistrare a entității, dar în niciun caz mai puțin de 10%.

**Țară:** Fie un membru al Organizației Națiunilor Unite, fie o regiune geografică recunoscută ca stat suveran de cel puțin două țări membre ale ONU.

**Certificat CA subordonat cu certificare încrucișată:** Un certificat care este utilizat pentru a stabili o relație de încredere între două AC.

**CSPRNG:** Un generator de numere aleatoare destinat utilizării în cadrul unui sistem criptografic.

**Parte terță delegată:** O persoană fizică sau o persoană juridică care nu este AC și ale cărei activități nu intră în sfera de aplicare a auditurilor corespunzătoare ale AC, dar care este autorizată de către AC să contribuie la procesul de gestionare a certificatelor prin îndeplinirea sau îndeplinirea uneia sau mai multor cerințe ale AC prevăzute în prezentul document.

**DNS CAA Email Contact:** Adresa de e-mail definită în CABF BR apendicele A.1.1.

**DNS CAA Contact telefonic:** Numărul de telefon definit în CABF BR apendicele A.1.2.

**DNS TXT Record Email Contact:** Adresa de e-mail definită în CABF BR apendicele A.2.1.

**DNS TXT Record Phone Contact:** Numărul de telefon definit în CABF BR apendicele A.2.2.

**Contactul de domeniu:** Titularul de registru al numelui de domeniu, contactul tehnic sau contractul administrativ (sau echivalentul în cadrul unui ccTLD), astfel cum este listat în numele de domeniu de bază sau într-o înregistrare SOA a DNS, sau astfel cum a fost obținut prin contact direct cu registratorul numelui de domeniu.

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

**Nume de domeniu:** O listă ordonată de una sau mai multe etichete de domeniu atribuite unui nod în sistemul de nume de domeniu.

**Domain Namespace (spațiu de nume de domeniu):** Ansamblul tuturor numelor de domeniu posibile care sunt subordonate unui singur nod din sistemul de nume de domeniu.

**Registrant al numelui de domeniu:** Denumit uneori „proprietarul” unui nume de domeniu, dar mai corect este persoana (persoanele sau entitățile) înregistrată (înregistrate) la un registrator de nume de domeniu ca având dreptul de a controla modul în care este utilizat un nume de domeniu, cum ar fi persoana fizică sau entitatea juridică care este listată ca „Registrant” de către WHOIS sau de către registratorul de nume de domeniu.

**Registrator de nume de domeniu:** O persoană sau o entitate care înregistrează nume de domenii sub auspiciile sau prin acord cu:

- (i) Internet Corporation for Assigned Names and Numbers (ICANN),
- (ii) o autoritate/un registru național al numelor de domenii sau
- (iii) un centru de informare în rețea (inclusiv afiliații, contractanții, delegații, succesorii sau cesionarii acestora).

**Enterprise RA:** Un angajat sau un agent al unei organizații neafiliate cu AC care autorizează emiterea de certificate pentru organizația respectivă.

**Expiry Date (Data expirării):** Data "Not After" dintr-un certificat care definește sfârșitul perioadei de valabilitate a certificatului.

**Nume de domeniu complet calificat (Fully-Qualified Domain Name):** Un nume de domeniu care include etichetele tuturor nodurilor superioare din sistemul de nume de domeniu Internet.

**Entitate guvernamentală:** O entitate juridică, agenție, departament, minister, ramură sau un element similar al guvernului unei țări sau o subdiviziune politică din cadrul unei astfel de țări (cum ar fi un stat, o provincie, un oraș, un județ etc.).

**Cerere de certificat de risc ridicat:** O cerere pe care AC o semnaleză pentru o examinare suplimentară prin referire la criteriile interne și bazele de date menținute de AC, care pot include nume cu risc ridicat de phishing sau alte utilizări frauduloase, nume conținute în cereri de certificat respinse anterior sau în certificate revocate, nume enumerate pe lista de phishing Miller Smiles sau pe lista Google Safe Browsing sau nume pe care AC le identifică folosind propriile criterii de reducere a riscurilor.

**Denumire internă:** Un șir de caractere (nu o adresă IP) într-un câmp de nume comun sau de nume alternativ al subiectului unui certificat care nu poate fi verificat ca fiind unic la nivel global în cadrul DNS public la momentul emiterii certificatului, deoarece nu se termină cu un domeniu de nivel superior înregistrat în baza de date a zonei rădăcină a IANA.

**CA intermediară:** este o CA care se situează sub CA rădăcină într-o anumită ICP și este în mod normal gestionată de aceeași entitate ca și CA rădăcină.

**CA emitentă:** în legătură cu un anumit certificat, CA care a emis certificatul. Aceasta poate fi fie o CA rădăcină, fie o CA intermediară/subordonată.

**Compromiterea cheii:** O cheie privată este considerată compromisă dacă valoarea sa a fost dezvăluită unei persoane neautorizate, dacă o persoană neautorizată a avut acces la ea.

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

**Pereche de chei:** Cheia privată și cheia publică asociată acesteia.

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

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

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

**Identificator de obiect:** Un identificator alfanumeric sau numeric unic înregistrat în conformitate cu standardul aplicabil al Organizației Internaționale de Standardizare pentru un anumit obiect sau clasă de obiecte.

**OCSF Responder:** Un server online operat sub autoritatea AC și conectat la depozitul acesteia pentru procesarea cererilor de stare a certificatelor. A se vedea, de asemenea, Protocol de stare a certificatelor online.

**Nume de domeniu Onion:** Un nume de domeniu complet calificat care se termină cu numele de domeniu cu utilizare specială RFC 7686 ".onion". De exemplu, gzyxa5ihm7nsggfnu52rck2vv4rvmdlkiu3zzui5du4xyclyen53wid.onion este un nume de domeniu Onion, în timp ce torproject.org nu este un nume de domeniu Onion.

**Protocolul de stare a certificatelor online:** Un protocol de verificare online a certificatelor (**OCSP**) care permite aplicațiilor software ale părților de încredere să determine starea unui certificat identificat. A se vedea, de asemenea, OCSP Responder.

**Companie mamă:** O societate care controlează o societate filială.

**Perspectiva primară a rețelei:** Perspectiva de rețea utilizată de AC pentru a stabili

- 1) autoritatea AC de a emite un certificat pentru domeniul (domeniile) sau adresa (adresele) IP solicitate și
- 2) autoritatea solicitantului și/sau autorizarea domeniului sau controlul asupra domeniului (domeniilor) sau adresei (adreselor) IP solicitate.

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

**Cheie publică:** Cheia unei perechi de chei care poate fi făcută publică de către deținătorul cheii private corespunzătoare și care este utilizată de către o parte fiducie pentru a verifica semnăturile digitale create cu cheia privată corespunzătoare a deținătorului și/sau pentru a cripta mesaje astfel încât acestea să poată fi decriptate numai cu cheia privată corespunzătoare a deținătorului.

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

**Certificat de încredere publică:** Un certificat de încredere în virtutea faptului că certificatul rădăcină corespunzător este distribuit ca ancoră de încredere în aplicațiile software disponibile pe scară largă.

**Etichetă P:** O etichetă XN care conține o ieșire validă a algoritmului Punycode (astfel cum este definit în RFC 3492, secțiunea 6.3) din a cincea poziție și următoarele.

**Auditor calificat:** O persoană fizică sau o entitate juridică care îndeplinește cerințele de la punctul 8.2.

**Valoare aleatorie:** O valoare specificată solicitantului de către o AC care prezintă cel puțin 112 biți de entropie.

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

**Autoritatea de înregistrare (RA):** Orice entitate juridică responsabilă de identificarea și autentificarea subiecților certificatelor, dar care nu este o AC și, prin urmare, nu semnează și nu emite certificate. O RA poate asista la procesul de solicitare a certificatelor, la procesul de revocare sau la ambele. Atunci când „RA” este folosit ca adjectiv pentru a descrie un rol sau o funcție, nu implică neapărat un organism separat, ci poate face parte din AC.

**Sursă de date fiabilă:** Un document de identificare sau o sursă de date utilizată pentru a verifica informațiile privind identitatea subiectului, care este în general recunoscută ca fiind fiabilă în rândul întreprinderilor comerciale și al guvernelor și care a fost creată de o terță parte în alt scop decât obținerea unui certificat de către solicitant.

**Metodă fiabilă de comunicare:** O metodă de comunicare, cum ar fi o adresă de livrare prin poștă/curier, un număr de telefon sau o adresă de e-mail, care a fost verificată cu ajutorul unei alte surse decât reprezentantul solicitantului.

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

**Depozitar:** O bază de date online care conține documente de guvernanță PKI făcute publice (cum ar fi politicile de certificare și declarațiile privind practicile de certificare) și informații privind starea certificatelor, fie sub forma unei CRL, fie sub forma unui răspuns OCSP.

**Token de cerere:** O valoare derivată printr-o metodă specificată de către AC care leagă această demonstrație de control de cererea de certificat.

Tokenul de cerere TREBUIE să includă cheia utilizată în cererea de certificat.

Un jeton de cerere POATE include o marcă temporală pentru a indica data la care a fost creat.

Un jeton de cerere POATE include alte informații pentru a asigura unicitatea sa.

Un jeton de cerere care include un timestamp rămâne valabil pentru cel mult 30 de zile de la momentul creării.

Un jeton de cerere care include un timestamp TREBUIE să fie tratat ca fiind invalid dacă timestamp-ul său este în viitor.

Un jeton de cerere care nu include un timestamp este valabil pentru o singură utilizare, iar AC NU îl reutilizează pentru o validare ulterioară.

Legătura TREBUIE să utilizeze un algoritm de semnătură digitală sau un algoritm de hash criptografic.

**Conținutul necesar al site-ului web:** Fie o valoare aleatorie, fie un jeton de cerere, împreună cu informații suplimentare care identifică în mod unic abonatul, după cum specifică AC.

**Cerințe:** Cerințele de bază care se găsesc în documentul CABF BR.

**Adresa IP rezervată:** O adresă IPv4 sau IPv6 pe care IANA a marcat-o ca fiind rezervată:

<http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml>

<http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml>

**Root CA:** Autoritatea de certificare de nivel superior, al cărei certificat rădăcină este distribuit de furnizorii de software de aplicație, care reprezintă "ancora de încredere" pentru lanțul de încredere și care emite certificate CA intermediare.

**Certificat rădăcină:** Certificatul autofirmat emis de către CA rădăcină pentru a se identifica și pentru a facilita verificarea certificatelor emise către CA-urile sale intermediare.

**Certificat de abonat cu durată de viață scurtă:** Pentru certificatele emise la 15 martie 2024 sau după această dată și înainte de 15 martie 2026, un certificat de abonat cu o perioadă de valabilitate mai mică sau egală cu 10 zile (864 000 secunde). Pentru certificatele emise la 15 martie 2026 sau după această dată, un certificat de abonat cu o perioadă de valabilitate mai mică sau egală cu 7 zile (604 800 secunde).

**Stat suveran:** Un stat sau o țară care își administrează propriul guvern și care nu este dependent sau supus unei alte puteri.

**Subiect:** Persoana fizică, dispozitivul, sistemul, unitatea sau entitatea juridică identificată ca subiect într-un certificat. Subiectul este fie abonatul, fie un dispozitiv aflat sub controlul și în exploatarea abonatului.

**Informații privind identitatea subiectului:** Informații care identifică subiectul certificatului. Informațiile privind identitatea subiectului nu includ un nume de domeniu menționat în extensia subjectAltName sau în câmpul Subject commonName.

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

**Subscriber (Abonat):** O persoană fizică sau o entitate juridică căreia i se eliberează un certificat și care este obligată din punct de vedere juridic de un contract de abonat sau de termenii de utilizare.

**Contract de abonat:** Un acord între AC și solicitant/abonat care specifică drepturile și responsabilitățile părților.

**Companie subsidiară:** O companie care este controlată de o companie mamă.

**Certificat de CA intermediar/subordonat cu constrângere tehnică:** Un certificat de CA intermediar care utilizează o combinație de setări privind utilizarea extinsă a cheilor și setări privind restricțiile de nume pentru a limita domeniul de aplicare în care certificatul de CA intermediar poate emite certificate de CA intermediar subscriitor sau certificate de CA intermediar suplimentare.

**Termeni de utilizare:** Dispoziții privind păstrarea și utilizările acceptabile ale unui certificat eliberat în conformitate cu prezentele cerințe atunci când solicitantul/abonatul este un afiliat al CA sau este CA.

**Sistem demn de încredere:** Hardware, software și proceduri informatice care sunt: protejate în mod rezonabil împotriva intruziunilor și a utilizării abuzive; asigură un nivel rezonabil de disponibilitate, fiabilitate și funcționare corectă; sunt adaptate în mod rezonabil pentru îndeplinirea funcțiilor prevăzute; și pun în aplicare politica de securitate aplicabilă.  
**Nume de domeniu neînregistrat:** Un nume de domeniu care nu este un nume de domeniu înregistrat.

**Certificat valabil:** Un certificat care trece procedura de validare specificată în RFC 5280.  
**Specialiști în validare:** O persoană care îndeplinește sarcinile de verificare a informațiilor specificate în aceste cerințe.

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

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

**Certificat Wildcard:** Un certificat care conține un asterisc (\*) în poziția cea mai din stânga a oricăruia dintre numele de domeniu complet calificate conținute în certificat.

**Nume de domeniu wildcard:** Un nume de domeniu format dintr-un singur caracter asterisc urmat de un singur caracter punct („\*.”) urmat de un nume de domeniu complet calificat.

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

## 1.6.2 Acronime

| Acronym | Meaning   | Traducere   |
|---------|---|---|
| ADN     | Authorization Domain Name                               | Autorizare Nume de domeniu                                      |
| AICPA   | American Institute of Certified Public Accountants      | Institutul American al Contabililor Publici Autorizați          |
| BIPM    | International Bureau of Weights and Measures            | Biroul Internațional de Măsură și Greutăți                      |
| BIS     | (US Government) Bureau of Industry and Security         | (Guvernul SUA) Biroul de Industrie și Securitate                |
| CA      | Certification Authority                                 | Autoritatea de certificare                                      |
| CAA     | Certification Authority Authorization                   | Autorizarea autorității de certificare                          |
| CARL    | Certification Authority Revocation List                 | Lista de revocare a autorității de certificare                  |
| ccTLD   | Country Code Top-Level Domain                           | Cod de țară Domeniu de nivel superior                           |
| CEO     | Chief Executive Officer                                 | Director Executiv   |
| CFO     | Chief Financial Officer                                 | Director Financiar  |
| CICA    | Canadian Institute of Chartered Accountants             | Institutul canadian al contabililor autorizați                  |
| CIO     | Chief Information Officer                               | Director Tehnologia Informațiilor (IT)                          |
| CISO    | Chief Information Security Officer                      | Director Securitatea Informațiilor                              |
| COO     | Chief Operating Officer                                 | Director Operațional  |
| CP      | Certificate Policy                                      | Politica de certificare   |
| CPA     | Chartered Professional Accountant                       | Contabil profesionist autorizat                                 |
| CPS     | Certification Practice Statement                        | Declarație privind practicile de certificare                    |
| CRL     | Certificate Revocation List                             | Lista de revocare a certificatelor                              |
| CSO     | Chief Security Officer                                  | Director Securitate   |
| DBA     | Doing Business As                                       | Făcând afaceri sub numele de                                    |
| DN      | Distinguished Name                                      | Denumire distinctă  |
| DNS     | Domain Name System                                      | Sistem de nume de domeniu                                       |
| DV      | Domain Validated  | Domeniu validat   |
| EV      | Extended Validation                                     | Validare extinsă  |
| FIPS    | (US Government) Federal Information Processing Standard | (Guvernul SUA) Standardul federal de prelucrare a informațiilor |
| FQDN    | Fully-Qualified Domain Name                             | Nume de domeniu complet calificat                               |
| gTLD    | Generic Top-Level Domain                                | Domeniul generic de vârf  |
| IANA    | Internet Assigned Numbers Authority                     | Autoritatea de atribuire a numerelor de internet                |
| ICANN   | Internet Corporation for Assigned Names and Numbers     | Corporația Internet pentru alocarea Numelor și Numerelor        |
| IFAC    | International Federation of Accountants                 | Federația Internațională a Contabililor                         |
| IM      | Instant Messaging                                       | Mesagerie instantanee   |
| IRS     | Internal Revenue Service                                | Serviciul de venituri interne                                   |
| ISO     | International Organization for Standardization          | Organizația Internațională pentru Standardizare                 |
| ISP     | Internet Service Provider                               | Furnizor de Servicii Internet                                   |

| Acronym | Meaning  | Traducere   |
|---------|--|---|
| NIST    | (US Government) National Institute of Standards and Technology                               | (Guvernul SUA) Institutul Național de Standarde și Tehnologie   |
| OCSP    | Online Certificate Status Protocol   | Protocol de stare a certificatelor online   |
| OID     | Object Identifier  | Identificator de obiect   |
| OV      | Organization Validated   | Organizație validată  |
| PKI     | Public Key Infrastructure  | Infrastructură cu cheie publică   |
| PPMB    | Policies and Procedures Management Body  | Organism de gestionare a politicilor și procedurilor  |
| QEVCP-w | Certificate Policy for EU qualified Website Authentication based on EVCP                     | Politica de certificare pentru autentificarea site-urilor web calificate de UE pe baza EVCP                         |
| QGIS    | Qualified Government Information Source  | Sursă Guvernamentală de Informații Calificate   |
| QIIS    | Qualified Independent Information Source   | Sursă Independentă de Informații Calificate   |
| QNCP-w  | Certificate policy for EU qualified website authentication certificates based on NCP and PTC | Politica de certificare pentru certificatele de autentificare a site-urilor web calificate de UE pe baza PCN și PTC |
| QSCD    | Qualified Electronic Signature Creation Device   | Dispozitiv de creare a semnăturilor electronice calificat   |
| QTIS    | Qualified Government Tax Information Source  | Sursă calificată de informații fiscale guvernamentale   |
| QWAC    | Qualified Certificate for Website Authentication   | Certificat calificat pentru autentificarea site-urilor web  |
| RA      | Registration Authority   | Autoritatea de înregistrare   |
| RSA     | Rivest, Shamir, Adleman asymmetric cryptographic algorithm                                   | Algoritm criptografic asimetric Rivest, Shamir, Adleman   |
| S/MIME  | Secure MIME (Multipurpose Internet Mail Extensions)  | MIME securizat (Extensii multifuncționale de poștă electronică pe Internet)   |
| SEC     | (US Government) Securities and Exchange Commission   | (Guvernul SUA) Comisia pentru valori mobiliare și burse   |
| SSL     | Secure Sockets Layer   | Secure Sockets Layer  |
| TLS     | Transport Layer Security   | Securitatea stratului de transport  |
| TSP     | Trust Services Provider  | Furnizor de servicii de încredere   |
| UTC     | Coordinated Universal Time   | Timp universal coordonat  |
| UTC(k)  | National realization of Coordinated Universal Time   | Realizarea națională a timpului universal coordonat   |
| VoIP    | Voice Over Internet Protocol   | Protocol de voce pe internet  |

## 2 Publicare și responsabilități Depozitar

certSIGN publică CPP-urile cel puțin anual, chiar dacă nu sunt schimbări.

### 2.1 Depozitari

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
- Șabloanele contractelor cu Beneficiarii

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

- Să deponă toate eforturile necesare pentru a se asigura că toate certificatele publicate în Depozitar aparțin Subiecților înscrși în certificate și că Beneficiarii și-au dat acordul asupra acestor certificate,
- Să se asigure că certificatele Autorităților de Certificare, Autorității de Înregistrare aparținând domeniului certSIGN, precum și certificatele Subiecților sunt publicate și arhivate la timp,
- Să asigure publicarea și arhivarea CPP, a listei aplicațiilor recomandate și a dispozitivelor recomandate,
- Să permită accesul la informațiile despre starea certificatelor prin publicarea de Liste de Certificate Revocate (CRL), prin intermediul serverelor OCSP sau prin interogări HTTP,
- Să asigure accesul permanent la informațiile din Depozitar pentru Autoritățile de Certificare, Autoritatea de Înregistrare, Beneficiarii și Entitățile Partenere,
- Să publice CRL-uri sau alte informații în timp util și în concordanță cu termenele limită menționate în CPP,
- Să asigure accesul sigur și controlat la informațiile din Depozitar.

### 2.2 Publicarea informațiilor de certificare

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

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

Toate certificatele SSL emise pot fi găsite în înregistrările CT (Certificate Transparency)

Pentru toate certificatele emise, informațiile privind starea certificatului sunt disponibile prin CRL-uri și serviciul OCSP furnizate de certSIGN 24\*7\*365.

certSIGN este conform cu ultima versiune publicată a cerințelor de bază pentru emiterea și gestionarea certificatelor de încredere publice, publicată la <http://www.cabforum.org>. În cazul unei eventuale neconcordanțe între acest document și aceste cerințe, aceste cerințe au prioritate față de acest document.

certSIGN găzduiește la <https://testssl.certsign.ro/> 3 pagini web care permit furnizorilor de aplicații software să testeze software-ul cu certificatele emise de certSIGN Web CA:

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

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

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

## Disponibilitatea

Disponibilitatea combinată a depozitarului 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 pentru 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 datorată unei catastrofe, unei defecțiuni a infrastructurii sau serviciilor 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 (Codul de Practici și Proceduri) sunt actualizate anual sau determinate de următoarele evenimente:

- Actualizări CPP;
- Certificatul autorităților de certificare - după emiterea unui nou certificat;
- Rezolvarea unor neconformități constatate de audit;
- Informații suplimentare - după fiecare actualizare;
- Ori de câte ori forumul CA / Browser emite noi cereri prin documentul BR care solicită schimbarea unei politici sau a unei practici privind certificatele.

## 2.4 Controlul accesului la Depozitar

Toate informațiile publicate de certSIGN în Depozitar la adresa <https://www.certsign.ro/ro/depozitar/> sunt accesibile publicului. Depozitarul este public și disponibil la nivel internațional 24\*7\*365.

certSIGN a implementat mecanisme logice și fizice de protecție împotriva adăugării, ștergerii și modificării neautorizate a informațiilor publicate în Depozitar.

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

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

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

## 3 Identificarea și autentificarea

### 3.1 Numele

Structura și utilizarea numelor din certificate este conform cu X.500, RFC5280, și CABF Baseline Requirements.

CERTSIGN nu permite utilizarea în certificate de nume de domenii internaționalizate (IDN). Denumirile subiectului dintr-un certificat DV respectă formularul X.500 Distinguished Name (DN). certSIGN Web CA utilizează o convenție de denumire unică, așa cum este stabilit în cerințele de bază publicate de CA / Browser Forum.

Certificatele emise în conformitate cu prezentul CPP au semnificație numai dacă numele care apar în certificate pot fi înțelese și utilizate de părțile partenere. Denumirile utilizate în certificate trebuie să identifice site-ul web căruia li se atribuie în mod semnificativ.

Atributul Numele Distinctiv este unic pentru subiectul căruia i se eliberează. Pentru fiecare certificat DV, se emite un număr de serie unic în spațiul de nume al certSIGN Web CA.

#### 3.1.1 Tipuri de nume

Certificatele emise de certSIGN sunt conforme cu standardul X.509 v3. Aceasta înseamnă că emitentul certificatului și Autoritatea de Înregistrare care acționează în numele emitentului aprobă numele Subiectului în conformitate cu prevederile standardului X.509 (cu referire la recomandările seriei X.500). Numele de bază ale Subiecților și ale emitenților de certificate plasate în certificatele certSIGN sunt conforme cu Numele Distinctive- DN – (cunoscute și ca nume directe), create utilizând recomandările X.500 și X.520.

#### 3.1.2 Nevoia ca Numele să fie Semnificativ

Certificatele SSL, cu excepția certificatelor wildcard și a celor de tip Unified Communications, sunt emise cu un Nume de Domeniu Complet Calificat (FQDN) sau cu o adresă IP.

Certificatele SSL wildcard conțin un asterisc. Înainte de emiterea unui astfel de certificat se determină dacă asteriscul apare pe prima poziție la stanga sufixului unui domeniu controlat de organizația de înregistrare a domeniilor (de exemplu \*.com.ro) sau a sufixului public (de exemplu \*.ro, \*.edu, "\*.com", "\*.co.uk"; a se vedea RFC 6454 Secțiunea 8.2 pentru detalii) și dacă acest lucru se întâmplă, CA-ul operat de certSIGN va respinge cererea, deoarece domeniul trebuie să fie detinut sau controlat de către Beneficiar.

Pentru certificatele SSL, în timp ce FQDN sau un nume de domeniu autentificat poate fi plasat în atributul Common Name (CN) al câmpului Subject, este prezent în extensia Subject Alternative Name, în DNS Name. Numele alternative ale subiectului sunt marcate ca necritice, în conformitate cu RFC5280.

CertSIGN nu emite certificate SSL care conțin „underscore character” („\_”) în numele de domeniu/dNSName, în concordanță cu recomandările CA/Browser Forum BR versiunea curentă. FQDN cuprinde doar „P-labels” și „Non-Reserved LDH-labels”.

Certificatele de tip Unified Communications SSL (multi domain) nu trebuie să includă domenii nerutabile (de exemplu .local) sau IP-uri private (conform RFC 1918) în cadrul extensiei Subject Alternative Name. Domeniul .int este tratat ca domeniu rutabil.

Numele inclus în Numele Distinctiv al Subiectului este semnificativ în limba română și în orice altă limbă care utilizează alfabetul latin. Structura Numelui Distinctiv, aprobat/desemnat și verificat de o Autoritate de Înregistrare depinde de tipul Subiectului.

certSIGN nu emite certificate SSL DV pentru persoane fizice.

Pentru Entitățile juridice, DN constă în următoarele câmpuri **obligatorii** (descrierea câmpului este urmată de abrevierea sa, care respectă recomandările X.520):

- Câmpul CN – Numele de domeniu complet calificat
- Câmpul C – Abreviere internațională pentru numele țării

### 3.1.3 Anonimitatea sau pseudonimitatea Beneficiarilor

certSIGN nu emite certificate anonime sau pseudonime.

### 3.1.4 Reguli de Interpretare a Diferitelor Formate de Nume

Interpretarea câmpurilor din certificatele emise de certSIGN se face în concordanță cu profilele de certificate descrise în Profilul certificatelor și al CRL-urilor (Capitolul 7). Crearea și interpretarea DN-ului vor fi realizate conform recomandărilor specificate în Capitolul 3.1.2.

### 3.1.5 Unicitatea numelor

Unicitatea numelui este asigurată prin utilizarea câmpului O care este obligatoriu și trebuie să fie unic pentru o anumită entitate și prin utilizarea numelui de domeniu complet calificat în numele alternativ al subiectului. Unicitatea unui nume de domeniu este garantată de Internet Corporation pentru nume și numere alocate (ICANN).

### 3.1.6 Recunoașterea, autentificarea și rolul mărcilor înregistrate

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, în care va fi inclusă cheia publică semnată de cheia privată asociată.

### 3.2.2 Autentificarea identității organizației

Este necesar să se dovedească faptul că entitatea care solicită certificatul DV SSL are control asupra domeniului la care se referă solicitarea de certificat.

Procedura de validare a dreptului de proprietate sau a controlului solicitantului asupra domeniului se bazează pe ETSI EN 319 411-1 și pe cea mai recentă versiune publicată a CA/Browser Forum - Politica de certificare a cerințelor de referință pentru eliberarea și gestionarea certificatelor de încredere publică.

#### 3.2.2.1 Identitatea

Reprezentanții organizației sunt obligați să prezinte la solicitarea Autorității de Înregistrare o cerere de cumpărare.

Procedura pe care RA o aplică pentru verificarea domeniului constă în:

- Verificarea documentelor prezentate de Beneficiar,

- Verificarea cererii, care constă în:
  - Verificarea conformității datelor specificate în cerere cu cele din documentele prezentate,
  - Verificarea dovezii de deținere a cheii private și a faptului că Distinctive Name este cel potrivit,
- Verificare dacă domeniul menționat în certificat este înregistrat de entitatea care a depus cererea de certificat sau de cea care a autorizat utilizarea domeniului de către entitatea solicitantă în conformitate cu CA/Browser Forum–#3.2.2.4.4 (Constructed Email to Domain Contact), or #3.2.2.4.7 (DNS Change) or #3.2.2.4.19 (Agreed Upon Change to Website ACME). Verificarea în registrul regional de domenii internet (baza de date RIPE pentru abonații europeni) dacă persoana care solicită certificatul SSL este proprietarul sau are dreptul de a utiliza adresa IP rutabilă pentru care se solicită certificatul.

Autoritatea de înregistrare se angajează să verifice corectitudinea și autenticitatea tuturor datelor furnizate într-o cerere.

În cazul în care verificarea este încheiată cu succes, un operator autorizat al Autorității de Înregistrare emite o confirmare care certifică conformitatea datelor din cererea de prelucrare cu datele furnizate și trimite această confirmare autorității de certificare. Autoritatea de certificare verifică dacă acest lucru a fost emis de o autoritate de înregistrare autorizată.

### **3.2.2.2 DBA (Doing Business As)/ Nume Comercial**

Nu se aplică.

### **3.2.2.3 Verificarea țării**

RA verifică țara asociată Beneficiarului utilizând una dintre următoarele:

(a) domeniul de adrese IP atribuit pe țară pentru oricare dintre:

- (i) adresa IP a site-ului Web, așa cum este indicată de înregistrarea DNS pentru site-ul web sau
- (ii) adresa IP a Beneficiarului;

(b) ccTLD (Domeniul de nivel superior al codului de țară) al numelui de domeniu solicitat;

(c) informații furnizate de Registratorul de Nume de Domeniu; sau

(d) conform celor menționate secțiunea 3.2.2.1.

CA a implementat un proces de scanare a serverelor proxy pentru a preveni dependența de adresele IP atribuite în țări diferite de cea în care este de fapt localizat solicitantul.

### **3.2.2.4 Validarea Autorizării sau Controlului Domeniului**

Această secțiune definește procesele și procedurile permise pentru validarea proprietății sau controlului asupra domeniului.

certSIGN confirmă că, înainte de emitere, a validat fiecare nume de domeniu complet calificat (FQDN) ce apare în Certificat, folosind cel puțin una din metodele de mai jos.

certSIGN nu emite certificate pentru domenii (FQDN) care conțin "onion" în partea dreaptă.

Validările complete ale autorității solicitante pot fi valabile pentru eliberarea mai multor certificate în timp. În toate cazurile, validarea trebuie să fi fost inițiată în termenul specificat în cerința relevantă (cum ar fi secțiunea 4.2.1 din acest document) înainte de eliberarea

certificatului. În scopul validării domeniului, termenul Solicitant include Compania-mamă a solicitantului, filială sau companie afiliată.

certSIGN menține evidența metodei de validare a domeniului, inclusiv a numărului de versiune BR relevant, pentru validarea fiecărui domeniu.

#### *3.2.2.4.1 Validarea solicitantului ca contact de domeniu*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.2 E-mail, fax, SMS sau poștă la contactul de domeniu*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.3 Contactul telefonic cu contactul de domeniu*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.4 E-mail construit către contactul de domeniu*

certSIGN va trimite un e-mail construit la contactul de domeniu pentru a confirma că solicitantul este conștient de proprietatea sau de controlul numelui de domeniu. E-mailul va fi trimis la una sau mai multe adrese create folosind "admin", "administrator", "webmaster", "hostmaster" sau "postmaster" ca parte locală, urmată de semnul "@", urmat de numele de domeniu de autorizare și va include o valoare aleatorie (generată prin mijloace tehnice, unică în fiecare e-mail).

Valoarea aleatorie rămâne valabilă pentru a fi utilizată într-un răspuns confirmator timp de 30 de zile de la crearea sa. E-mailul de răspuns trebuie să fie trimis utilizând contul de e-mail utilizat pentru trimiterea inițială și certSIGN verifică dacă valoarea aleatorie este aceeași. Această metodă este potrivită pentru validarea numelor de domenii Wildcard.

#### *3.2.2.4.5 Documentul de autorizare a domeniului*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.6 Schimbare la site-ul web*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.7 Modificarea DNS*

certSIGN va trimite un e-mail persoanei de contact care a trimis cererea pentru a confirma că solicitantul deține controlul asupra numelui de domeniu. Emailul va include o valoare aleatoare (generată prin mijloace tehnice, unică în fiecare e-mail) pentru a fi adăugată în intrarea DNS într-una din înregistrările DNS CNAME, TXT sau CAA a domeniului care trebuie verificat.

Valoarea aleatoare rămâne valabilă pentru utilizare timp de 30 de zile de la crearea sa. certSIGN verifică dacă valoarea din înregistrarea DNS este aceeași cu cea transmisă.

Odată ce FQDN a fost validat utilizând această metodă, CERTSIGN poate emite, de asemenea, Certificate pentru alte FQDNs care se termină cu toate etichetele de domeniu ale FQDN validat.

certSIGN a pus în aplicare coroborarea emiterii din perspective multiple (MPIC), așa cum se specifică la punctul 3.2.2.9.

Această metodă este potrivită pentru validarea numelor de domenii Wildcard.

#### *3.2.2.4.8 Această metodă este potrivită pentru validarea numelor de domenii Wildcard.Adrese IP*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.9 Certificat de testare*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.10 TLS folosind un număr aleatoriu*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.11 Orice altă metodă*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.12 Validarea solicitantului ca persoană de contact a domeniului*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.13 Email către contactul DNS CAA*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.14 Email către contactul DNS TXT*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.15 Legătură telefonică cu contactul domeniului*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.16 Legătură telefonică cu contactul DNS TXT Record*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.17 Legătură telefonică cu contactul DNS CAA Phone*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.18 Schimbare agreată la site-ul web v2*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.19 Schimbare agreată la site-ul web -ACME*

certSIGN confirmă controlul solicitantului asupra unui FQDN prin validarea controlului domeniului FQDN utilizând metoda ACME HTTP Challenge definită în secțiunea 8.3 din RFC 8555. Acest lucru se realizează prin primirea unui răspuns HTTP de succes la cerere. Tokenul nu este utilizat mai mult de 30 de zile de la crearea sa.

Atunci când certSIGN Web CA urmează redirectionări, acestea sunt inițiate la nivelul protocolului HTTP și sunt rezultatul unui răspuns cu cod de stare HTTP 301, 302 sau 307, astfel cum este definit în RFC 7231, secțiunea 6.4, sau al unui răspuns cu cod de stare HTTP 308, astfel cum este definit în RFC 7538, secțiunea 3. Redirectionările sunt valoarea finală a antetului de răspuns HTTP Location, astfel cum este definit în RFC 7231, secțiunea 7.1.2. certSIGN a pus în aplicare coroborarea emiterii multiperspective (MPIC), așa cum se specifică la punctul 3.2.2.9.

Această metodă NU este adecvată pentru validarea numelor de domenii wildcard.

#### *3.2.2.4.20 TLS folosind ALPN*

Nu este folosită această metodă de validare a domeniului.

#### *3.2.2.4.21 DNS Marcat cu Account ID – ACME*

Nu este folosită această metodă de validare a domeniului.

### 3.2.2.4.22 DNS TXT Record with Persistent Value

Nu este folosită această metodă de validare a domeniului.

### 3.2.2.5 Autentificarea pentru o Adresă IP

Nu se emite niciun certificat de adresă IP în baza acestui CPP.

### 3.2.2.6 Validarea unui Domeniu Wildcard

Înainte de emiterea unui certificat cu caracter wildcard (\*) într-un CN sau subjectAltName de tipul DNS-ID, RA-ul stabilește și urmează o procedură documentată ce determină dacă caracterul wildcard apare în poziția primei etichete, la stânga unei etichete "controlate prin registru" sau a unui "sufix public" (de exemplu, "\*.com", "\*.co.uk", conform RFC 6454, Secțiunea 8.2.)

Dacă wildcard-ul se află în interiorul etichetei, la stânga unui sufix controlat prin registru sau public, CA-urile refuză emiterea, dacă solicitantul nu dovedește dreptul de a controla întregul

### 3.2.2.7 Acuratețea Sursei Datelor

Înainte de utilizarea oricărei surse de date ca fiind o Sursă de Date de Încredere, RA evaluează nivelul de încredere, acuratețe și rezistența la alterare sau falsificare a sursei. În timpul evaluării, RA are în vedere următoarele lucruri:

1. Vechimea informațiilor furnizate,
2. Frecvența actualizării sursei informațiilor
3. Datele furnizate și scopul colectării datelor,
4. Accesibilitatea publică și disponibilitatea datelor și
5. Dificultatea relativă cu care datele pot fi falsificate sau alterate.

### 3.2.2.8 Înregistrările Autorității de Autentificare și Certificare (CAA)

Autoritatea de Înregistrare verifică înregistrările CAA și urmează instrucțiunile de procesare găsite, pentru fiecare dNSName din extensia subjectAltName a certificatului care urmează a fi emis, așa cum se specifică în RFC 8659.

La procesarea înregistrărilor CAA, certSIGN procesează etichetele de proprietate issuewild și iodef, așa cum este specificat în RFC 8659. certSIGN respectă nivelul critic și nu emite un certificat dacă întâmpină o etichetă de proprietate cu acest flag set. certSIGN tratează un set de înregistrări de resurse CAA care nu este gol și care nu conține nicio etichetă de proprietate (și care nu conține o etichetă de proprietate issuewild atunci când efectuează procesarea CAA pentru un domeniu Wild Card) ca permisiune de a emite, cu condiția să nu existe înregistrări în registrul de resurse CAA care de altfel să interzică emiterea.

certSIGN NU va emite un certificat, cu excepția cazului în care cererea de certificat este compatibilă cu setul de înregistrare a resurselor din CAA aplicabil.

Dacă există o înregistrare CAA, atunci trebuie să fie listată certSIGN ca CA autorizat. Înregistrarea permisă este certsign.ro. În cazul în care CA-ul emite, aceasta o face în termenul TTL al înregistrării CAA sau în termen de 8 ore, oricare dintre acestea este mai mare.

certSIGN va documenta orice problemă potențială care a fost prevenită datorită înregistrării CAA, suficient de detaliat, va oferi feedback în toate situațiile către CAB Forum, și va depune rapoarte referitoare la aceste cereri de emitere către contactele stipulate în înregistrările CAA iodef, dacă acestea există.

certSIGN a pus în aplicare coroborarea emiterii din perspective multiple (MPIC), așa cum se specifică la punctul 3.2.2.9.

### **3.2.2.9 Coroborarea Emiterii prin Perspective Multiple (MPIC)**

Coroborarea emiterii prin perspective multiple (Multi-Perspective Issuance Corroboration) încearcă să coroboreze determinările (de exemplu, validarea domeniului admisă/respinsă, permisiunea/prohibiția CAA) făcute din perspectiva principală a rețelei, cu determinările din mai multe perspective de rețea, la distanță, înainte de eliberarea certificatului.

Setul de răspunsuri de la perspectivele de rețea invocate furnizează CA informațiile necesare pentru a-i permite să evalueze în mod afirmativ

- a. prezența valorii aleatorii, a tokenului de cerere sau a adresei de contact preconizate, în conformitate cu metoda de validare de încredere specificată în secțiunea 3.2.2.4 și
- b. autoritatea CA de a emite pentru domeniul (domeniile) solicitat(e), astfel cum se specifică în secțiunea 3.2.2.8.

Detalii privind cerințele MPIC se regăsesc în CA/B Forum Baseline Requirements #3.2.2.9. certSIGN a implementat MPIC utilizând cel puțin două (2) perspective de rețea la distanță.

### **3.2.3 Autentificarea identității persoanelor fizice**

certSIGN nu eliberează certificate SSL persoanelor fizice.

### **3.2.4 Informații neverificate ale Beneficiarului**

Nu este stipulat.

### **3.2.5 Validarea autorității**

Autentificarea autorizațiilor face parte din procedura îndeplinită de autoritatea de înregistrare sau de autoritățile de certificare pentru a procesa cererea de certificat pentru un dispozitiv ce aparține unei persoane juridice.

certSIGN va folosi o metodă de comunicare fiabilă pentru a verifica autenticitatea cererii de certificare a reprezentantului solicitant, conform secțiunii 3.2.2.

Eliberarea certificatului este o confirmare a faptului că o persoană juridică sau un dispozitiv are dreptul de a utiliza cheia privată în numele persoanei juridice.

### **3.2.6 Criterii pentru interoperare**

certSIGN va dezvălui toate certificatele încrucișate care identifică CA drept subiect, cu condiția ca certSIGN să fi aranjat sau acceptat stabilirea relației de încredere.

certSIGN ROOT CA a emis un certificat încrucișat pentru certSIGN Web CA, emis inițial de certSIGN ROOT CA G2, ambele sisteme PKI fiind operate de certSIGN.

## **3.3 Identificarea și autentificarea pentru cererile de re-key**

### **3.3.1 Identificarea și autentificarea pentru re-key de rutină**

Este folosit același proces ca la validarea inițială a identității (Cap.3.2).

### **3.3.2 Identificarea și autentificarea pentru re-key după revocare**

Este folosit procesul utilizat în cazul validării inițiale a identității (Cap.3.2).

### 3.4 Identificarea și autentificarea pentru cererile de revocare

Cererile de revocare pot fi trimise prin e-mail direct emitentului certificatului sau indirect, Autorității de Înregistrare. Se pot trimite cereri și în alt format decât cel electronic.

- În primul caz, Beneficiarul trebuie să trimită o cerere autentificată pentru revocarea certificatului. Beneficiarul autentifică cererea aplicându-i o semnătură electronică.
- În al doilea caz, Beneficiarul nu poate trimite o cerere electronică de revocare. Cererea de revocare trebuie să fie certificată de Autoritatea de Înregistrare.

În ambele cazuri, trebuie să existe o identificare fără echivoc a identității Beneficiarului. Cererea de revocare poate să vizeze mai multe certificate. Autentificarea și identificarea Beneficiarului la Autoritatea de Înregistrare se realizează ca și la înregistrarea inițială (vezi Capitolul 3.2). Autentificarea Beneficiarului la Autoritatea de Certificare constă în verificarea autenticității cererii. Procedura detaliată de revocare este descrisă în Capitolul 4.9.

Următoarele entități pot trimite cereri de revocare a certificatelor:

- Beneficiarul care încheie un acord contractual cu certSIGN pentru emiterea de certificate.
- Autoritatea de Înregistrare care poate cere revocarea fie în numele unui Beneficiar, sau dacă deține informații care justifică revocarea certificatului, prin crearea unei cereri autentificate utilizând mecanismele de securitate ale software-ului Autorității de Înregistrare
- Rolurile de încredere asociate certSIGN Web CA, sub supravegherea Comitetului de Management al Politicilor și Procedurilor (PPMB), prin crearea unei cereri autentificate utilizând mecanismele de securitate ale software-ului Autorității de Certificare.

## 4 Cerințe operaționale privind ciclul de viață al certificatelor

Acest capitol descrie procedurile de bază care se aplică tuturor certificatelor DV emise de certSIGN Web CA.

### 4.1 Cererile de certificat

#### 4.1.1 Cine poate trimite o cerere de certificat

certSIGN menține o bază de date internă a tuturor Certificatelor revocate anterior și a solicitărilor de certificare respinse anterior din cauza presupusului phishing sau a altor utilizări sau preocupări frauduloase. certSIGN utilizează aceste informații pentru a identifica solicitările ulterioare de certificate suspecte.

#### Cererile de certificat ale Persoanelor Fizice

certSIGN nu emite certificate SSL pentru persoane fizice.

#### Cererile de certificat ale Persoanelor Juridice (Organizații)

Beneficiarul va respecta prevederile și obligațiile stabilite în formularul de înregistrare, în Acordul cu contractual cu Beneficiarul aplicabil și în Termenii și Condițiile serviciilor de certificare ce încorporează acest CPP și Declarația de Transparența PKI.

Autoritatea de Certificare emite certificate doar ca răspuns la o cerere autentificată primită de la Autoritatea de Înregistrare operată de certSIGN.

certSIGN arhivează informațiile referitoare la înregistrare. Arhiva este menținută în conformitate cu cerințele definite în CPP și în legislația aplicabilă.

#### 4.1.2 Procesul de înregistrare și responsabilitățile

Procesul de înregistrare este gestionat de o entitate specifică numită Autoritatea de Înregistrare sau RA, care este operată de certSIGN sau de o parte terta, conform cu legislația. certSIGN asigură supravegherea, suportul pentru și auditarea tuturor proceselor și serviciilor RA. RA este responsabilă de verificarea următoarelor elemente:

- Dreptul Beneficiarului asupra certificatului solicitat

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

Înainte de emiterea unui certificat, certSIGN obține următoarele documente de la un Beneficiar:

1. O cerere de certificat, care poate fi electronică; și
2. Un contract sau Termenii și Condiții în execuție, care pot fi în format electronic.

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

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

Formularul de înregistrare semnat este considerat acceptul oficial de către Beneficiar a contractului, prin care Beneficiarul acceptă următoarele:

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

### Procesul de înregistrare

Procesul de înregistrare începe în cadrul RA.

Operatorul RA efectuează verificarea solicitării CSR.

RA este responsabilă pentru acuratețea datelor care vor fi încorporate în cererea de certificat depusă la CA. RA este responsabilă pentru înregistrarea / înscrierea corectă a beneficiarilor și pentru furnizarea de către CA a conținutului corect pentru câmpurile variabile din certificat.

## 4.2 Procesarea cererilor de certificate

certSIGN acceptă cereri depuse individual sau colectiv.

Cererile pot fi trimise on-line sau off-line.

Cererea de certificat se completează în format electronic:

- Cererea de certificat se completează prin intermediul paginilor de pe site-ul certSIGN la următoarea adresă: <https://www.certsign.ro>. Un abonat care vizitează site-ul respectiv completează (în conformitate cu instrucțiunile de pe site-ul web) un formular de cerere și o procedează la plata, identificarea și înregistrarea online, urmând instrucțiunile de pe site, sau o îl înmânează personal unei AR sau direct autorității de certificare, sau o îl transmite prin servicii de curierat/poștă către AC, împreună cu scrisoarea care trebuie să conțină copii ale tuturor documentelor originale
- Formularul de cerere completat (primit prin e-mail sau de pe site-ul web [www.certsign.ro](http://www.certsign.ro)) este semnat electronic cu un certificat digital calificat valabil (nu revocat sau expirat) emis de CERTSIGN și trimis autorității de certificare prin e-mail sau pe un canal autentificat
- Cererea de certificat poate fi completată și postată pe site-ul: <https://shop.certsign.ro/>

Cererea de certificat este completată off-line:

- Prin prezența în persoană a Beneficiarului la Autoritatea de Înregistrare sau la Autoritatea de Certificare, caz în care cererea este completată și semnată de mână. Beneficiarul semnează acordul privind serviciile de certificare furnizate sau
- Beneficiarul transmite cererea completată și semnată manual, prin intermediul serviciilor poștale / poștale către CA, împreună cu o scrisoare care conține copii ale tuturor documentelor originale.

RA verifică înregistrările CAA și urmează instrucțiunile de procesare găsite, pentru fiecare dNSName în extensia subjectAltName a certificatului care urmează a fi emis, conform

specificațiilor RFC8659. certSIGN nu va emite un certificat decât dacă cererea de certificat este în concordanță cu setul de înregistrări CAA aplicabil.

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

#### 4.2.1 Îndeplinirea funcțiilor de identificare și autentificare

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

Cererea de Certificat cu Risc Înalt este o Cerere pe care CA-ul o marchează pentru o examinare suplimentară în raport cu criteriile interne și bazele de date întreținute de CA, care pot include nume cu un risc mai mare de phishing sau alte utilizări frauduloase, nume incluse în cererile de certificate respinse anterior sau certificate revocate, nume incluse în lista de phishing de la Miller Smiles sau în lista de Navigare sigură de la Google sau nume pe care CA le identifică utilizând propriile criterii de diminuare a riscurilor.

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

CA dezvoltă, întreține și implementează proceduri documentate care identifică și necesită activitate suplimentară de verificare pentru Cererile de Certificat cu Risc Înalt înainte de aprobarea Certificatului, în măsura în care acest lucru este în mod rezonabil necesar pentru a se asigura că astfel de solicitări sunt verificate corect.

Pentru a preveni emiterea de Certificate cu Risc Înalt, înainte de aprobarea certificatului, procedura internă de verificare va solicita încă una din următoarele acțiuni:

- Examinarea atentă a FQDN pentru a confirma dacă intenția Solicitantului este de a imita sau induce în eroare clienții;
- Verificarea încrucișată manuală și revizuirea tuturor informațiilor furnizate de Beneficiar
- Documentație suplimentară care confirmă controlul domeniului de la solicitant și / sau alte dovezi verificabile, considerate necesare de către PPMB.

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

#### 4.2.2 Aprobarea sau respingerea cererilor de certificate

Aprobarea sau respingerea cererilor de certificate sunt realizate de RA. RA validează fiecare cerere și poate respinge o cerere de certificat dacă cererea nu poate fi autentificată sau dacă Cererea nu respectă regulile și standardele care guvernează certSIGN Web CA sau din alte motive, la discreția și sub răspunderea RA.

Cererile de certificate sunt prelucrate în cele din urmă de sistemul certSIGN CA care validează fiecare cerere și poate respinge o cerere de certificat în cazul în care cererea nu poate fi

autentificată sau dacă cerea nu respectă regulile și standardele definite pentru tipul de certificat, la discreția și sub răspunderea certSIGN.

certSIGN nu eliberează certificate cu extensia `subjectAlternativeName` sau un câmp `Subject commonName` care să conțină Adresa IP rezervată sau `Internal Name`.

Intrările în `the dNSName` sunt în "sintaxa de nume preferată", conform RFC 5280, și nu trebuie să conțină caractere de tip `underscore` ("\_").

#### 4.2.3 Timpul de procesare a cererilor de certificate

certSIGN nu emite un certificat imediat după înregistrare. Certificatele trebuie să fie emise de Autoritatea de Certificare prin aprobarea cererii de certificat după ce ea a fost validată de RA. Prin urmare, certificatele nu sunt disponibile imediat Beneficiarului, atunci când certificatele sunt emise de CA.

### 4.3 Emiterea Certificatelor

După primirea și prelucrarea unei solicitări (a se vedea capitolele 4.1 și 4.2), Autoritatea de Certificare emite un certificat. După emiterea certificatului, certSIGN îl publică în depozitarele corespunzătoare. Perioada de valabilitate a certificatelor eliberate depinde de tipul certificatului și de categoria Subiectului și se conformează perioadelor prezentate în Tabelul 6.3.2.2.

certSIGN informează Beneficiarul cu privire la emiterea certificatului prin trimiterea unui e-mail (la adresa furnizată de către Beneficiar) care permite Beneficiarului să obțină certificatul. Fiecare certificat emis este publicat în depozitarul certSIGN. Publicarea certificatului este echivalentă cu notificarea de către alte entități partenere a faptului că a fost emis un certificat pentru un subiect.

#### 4.3.1 Acțiunile CA în timpul emiterii certificatului

Certificatul este eliberat ca parte a procesului de înscriere a certificatului. CA va primi doar cereri de certificate de la RA. CA, RA și procesul de personalizare sunt sisteme integrate și comunică prin conexiuni de rețea închise. CA procesează numai cereri care provin de la un RA/DRA al certSIGN.

Pentru fiecare solicitare de certificat, CA va efectua următoarele verificări și acțiuni:

- Cererea provine de la RA?,
- CA verifică autorizația solicitantului pentru tipul de solicitare și refuză cererile care se referă la profilurile certificatelor pentru care solicitantul nu este autorizat.
- CA, de asemenea, compară cererea de certificat cu un profil de certificat predefinit. Informațiile variabile din cerere trebuie să se potrivească cu șablonul și setul de reguli al profilului certificatului.
- CA adaugă la certificat informații non-variabile și variabile, așa cum sunt definite în profilul de certificat specificat.
- CA-ul asigură unicitatea fiecărui certificat pe care îl emite pe baza câmpului `SerialNumber` din fiecare certificat.

certSIGN Web CA G4 a implementat un proces de Linting pentru a testa conformitatea tehnică a fiecărui artefact care urmează să fie semnat înainte de a-l semna. Metoda utilizată pentru a produce un certificat care conține conținutul certificatului care urmează să fie semnat constă în semnarea certificatului `tbsCertificate` cu o cheie privată "fictivă" a cărei componentă cheie publică nu este certificată de un certificat care se leagă de un certificat CA de încredere publică.

certSIGN Web CA G4 utilizează un proces Linting pentru a testa fiecare certificat emis.

#### 4.3.2 Notificarea Beneficiarului de către CA cu privire la emiterea certificatului

Certificatul este emis ca parte a procesului de înregistrare a certificatului. Beneficiarul primește o notificare cu privire la emiterea certificatului.

Cu o lună înainte de expirarea certificatului, Beneficiarul este informat cu privire la faptul că certificatul este pe cale să expire.

#### 4.4 Acceptarea certificatului

##### 4.4.1 Conduita care constituie acceptarea certificatului

Atunci când primește un certificat, Beneficiarul se obligă să verifice conținutul său, în special corectitudinea datelor și complementaritatea cheii publice cu cheia privată pe care o deține. Dacă certificatul are defecte sau greșeli care nu pot fi acceptate de către Beneficiar, Beneficiarul va informa imediat Autoritatea de Certificare cu privire la revocarea certificării.

Certificatul este considerat acceptat în cazul apariției următoarelor evenimente în termen de maximum 3 zile calendaristice de la data primirii certificatului de către Beneficiar:

- Acceptarea explicită a certificatului emis în momentul obținerii certificatului de pe site-ul certSIGN.

În cazul în care un certificat nu este respins în termen de 3 zile calendaristice de la primirea sa, certificatul este considerat acceptat.

Acceptarea certificatelor se face numai de către Beneficiar, înainte de utilizarea sa și de utilizarea sa la orice operație criptografică prin care se consideră că a acceptat termenii și condițiile specificate în prezentul CPP, Politica de certificare și acordul de furnizare a serviciilor. În cazul depunerii cererii în format electronic, solicitantul acceptă în mod automat certificatul în momentul solicitării acestui certificat.

Prin acceptarea certificatului, Beneficiarul acceptă regulile CPP și ale Politicii de Certificare și este de acord să urmeze prevederile acordului încheiat cu certSIGN.

RA și Beneficiarul au dreptul de a respinge certificatul, cu condiția ca cel puțin una dintre următoarele obiecții să se aplice:

- Informația din certificat nu este corectă,
- Informația din certificat a devenit invalida de la data înregistrării,
- Pierderea dreptului Beneficiarului

Obligațiile Beneficiarului și ale RA în cazul respingerii:

- RA solicită revocarea certificatelor,
- RA execută revocarea certificatelor

##### 4.4.2 Publicarea certificatului de către CA

Vezi capitolul 2 (Publicare și Responsabilități Depozitar).

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

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

#### 4.5 Utilizarea perechii de chei și a certificatului

##### 4.5.1 Utilizarea perechii de chei și a certificatului Beneficiarului

certSIGN emite certificate pentru chei furnizate de Beneficiari în cererile de certificat.

Beneficiarii își protejează accesul la cheile private de personalul neautorizat sau de alte terțe părți. Beneficiarii utilizează cheile private numai în conformitate cu uzanțele specificate în extensia de utilizare a cheii.

Vezi secțiunile 1.4.1, 6.1.7 și 7.1.

##### 4.5.2 Utilizarea cheii publice și a certificatului unei Entități Partenerere

certSIGN presupune că toate aplicațiile software ale utilizatorului sunt conforme cu standardul X.509, protocolul SSL/TLS și alte standarde aplicabile ce impun cerințele din acest CPP. certSIGN nu garantează că software-ul oricărei terțe părți va suporta sau impune asemenea controale și cerințe, iar toate Entitățile Partenerere sunt sfătuite să solicite suport tehnic și legal adecvat.

Entitățile Partenerere vor folosi 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 acordului dintre Beneficiar și certSIGN,
- Numai după verificarea stării lor și verificarea semnăturii Autorității de Certificare care a emis respectivul certificat.

Încrederea într-o sesiune SSL/TLS ce nu poate fi verificată poate avea ca rezultat riscuri pe care Entitatea Parteneră și le va asuma în totalitate și pe care certSIGN nu și le asumă în niciun fel.

#### 4.6 Reînnoirea Certificatului

certSIGN permite reînnoirea certificatelor de CA doar în condiții speciale, cu aprobarea CMPP. certSIGN nu reînnoiește certificate end-user SSL.

##### 4.6.1 Circumstanța reînnoirii certificatului

Nu este stipulat.

##### 4.6.2 Cine poate solicita reînnoirea

Nu este stipulat.

##### 4.6.3 Procesarea solicitărilor de reînnoire a certificatelor

Nu este stipulat.

##### 4.6.4 Notificarea abonatului cu privire la eliberarea unui nou certificat

Nu este stipulat.

##### 4.6.5 Conduita care constituie acceptarea unui certificat de reînnoire

Nu este stipulat.

#### 4.6.6 Publicarea certificatului de reînnoire de către CA

Nu este stipulat.

#### 4.6.7 Notificarea eliberării certificatului de către CA către alte entități

Nu este stipulat.

### 4.7 Re-key Certificat

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

#### 4.7.1 Circumstanțe re-key certificat

certSIGN efectuează re-key-ul certificatelor digitale valide (neexpire și nerevocate) emise de certSIGN, care nu necesită modificări ale datelor din certificat sau ale extensiilor. Procesul de re-key constă în re-emiterea unui certificat cu o pereche nouă de chei pentru a prelungi data de expirare fără a schimba identitatea sau alte extensii ale certificatului.

#### 4.7.2 Cine poate solicita certificarea unei noi chei publice

certSIGN informează întotdeauna Beneficiarii (cu cel puțin 30 de zile înainte) despre apropierea perioadei de expirare.

Re-key-ul se efectuează atunci când un Beneficiar care deține un certificat digital valabil (nerevocat și neexpirat) generează o nouă pereche de chei și solicită emiterea unui nou certificat pentru a confirma deținerea unei chei publice nou create.

Re-key-ul certificatului se efectuează numai la solicitarea Beneficiarului și este precedat de depunerea unei cereri pe un formular corespunzător completat de către Beneficiar.

#### 4.7.3 Procesarea cererilor de re-key al certificatelor

RA folosește aceleași procese ca pentru un certificate nou solicitat.

#### 4.7.4 Notificarea emiterii noului certificat către beneficiar

RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

#### 4.7.5 Conduita ce constituie acceptarea unui certificate re-key

RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

#### 4.7.6 Publicarea certificatului re-key de către CA

RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

#### 4.7.7 Notificarea eliberării certificatului de către CA altor entități

RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

### 4.8 Modificarea Certificatului

certSIGN permite modificarea certificatelor de CA doar în condiții speciale, cu aprobarea CMPP. certSIGN nu permite modificarea detaliilor certificatelor SSL end-user pe durata de viață a certificatului. Dacă se schimbă informații referitoare la certificat, Beneficiarul trebuie să solicite revocarea certificatului original și să solicite eliberarea unui nou certificat.

#### 4.8.1 Circumstanța modificării certificatului

Nu este stipulat.

#### 4.8.2 Cine poate solicita modificarea

Nu este stipulat.

#### 4.8.3 Procesarea cererilor de modificare a certificatului

Nu este stipulat.

#### 4.8.4 Notificarea abonatului cu privire la eliberarea unui nou certificat

Nu este stipulat.

#### 4.8.5 Conduita care constituie acceptarea unui certificat modificat

Nu este stipulat.

#### 4.8.6 Publicarea certificatului modificat de către CA

Nu este stipulat.

#### 4.8.7 Notificarea eliberării certificatului de către CA către alte entități

Nu este stipulat.

### 4.9 Revocarea și Suspendarea Certificatului

CertIFICATELE emise de certSIGN Web CA pot fi revocate, dar niciodată suspendate. Revocarea certificatelor este un proces ireversibil.

Revocarea nu afectează nici tranzacțiile efectuate înainte de revocare, nici obligațiile ce rezultă din aderarea la prezentul CPP.

Aceste capitole prezintă condițiile necesare pentru ca o autoritate de certificare să revoce un certificat.

*Dacă o cheie privată care corespunde unei chei publice conținute într-un certificat revocat rămâne sub controlul Beneficiarului, după revocare ar trebui să fie stocată în siguranță până când este distrusă.*

CertIFICATELE pe termen scurt nu sunt revocate. În cazul certificatelor pe termen scurt, mecanismul de notificare a problemelor este același mecanism descris la punctul 1.5 în „Procedura de raportare a problemelor legate de certificate”.

#### 4.9.1 Circumstanțele revocării

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

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

5. CA obține dovezi că validarea autorizării sau controlului domeniului pentru orice nume de domeniu complet calificat sau adresă IP din certificat nu ar trebui să se bazeze pe aceasta (CRLReason #4, superseded).

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

6. Certificatul nu mai respectă cerințele din secțiunea 6.1.5 și secțiunea 6.1.6 din CABF BR (CRLReason #4, înlocuit);

7. CA obține dovezi că certificatul a fost utilizat în mod abuziv (CRLReason #9, privilegeWithdrawn);

8. CA este informată că un abonat a încălcat una sau mai multe obligații materiale ale acestuia

în temeiul acordului de abonat sau al condițiilor de utilizare (CRLReason #9, privilegeWithdrawn);

9. CA este informată de orice circumstanță care indică faptul că utilizarea unui nume de domeniu sau a unei adrese IP complet calificate în certificat nu mai este permisă din punct de vedere legal (de exemplu, o instanță sau un arbitru a revocat dreptul unui solicitant de înregistrare a numelui de domeniu de a utiliza numele de domeniu, un acord de licență sau de servicii relevant între solicitantul și solicitantul de înregistrare a numelui de domeniu a încetat sau solicitantul de înregistrare a numelui de domeniu nu a reînnoit numele de domeniu) (CRLReason #5, cessationOfOperation);

10. CA este informată că un certificat Wildcard a fost utilizat pentru a autentifica un nume de domeniu complet calificat subordonat care induce în eroare în mod fraudulos (CRLReason #9, privilegeWithdrawn);

11. CA este informată despre o modificare semnificativă a informațiilor conținute în certificat (CRLReason #9, privilegeWithdrawn);

12. CA este informată că certificatul nu a fost eliberat în conformitate cu aceste cerințe sau cu CA/Browser Forum Baseline Requirements (CRLReasonReason, #4, superseded);

13. CA stabilește sau ia cunoștință de faptul că oricare dintre informațiile care apar în certificat este inexactă (CRLReason #9, privilegeWithdrawn);

14. Dreptul CA de a elibera certificate în temeiul prezentelor cerințe expiră sau este revocat sau încetat, cu excepția cazului în care CA a luat măsuri pentru a continua să mențină depozitul CRL/OCSP [CRLReason "unspecified (0)", ceea ce are ca rezultat faptul că în CRL nu este furnizată o extensie a codului de motiv (reasonCode)];

15. Revocarea este impusă de practicile de certificare ale certSIGN (CPP) pentru un motiv care nu este altfel necesar să fie specificat în prezenta secțiune [CRLReason "unspecified (0)", ceea ce are ca rezultat faptul că în CRL nu este furnizată o extensie reasonCode; sau

16. CA are cunoștință de o metodă demonstrată sau dovedită care expune cheia privată a Beneficiarului la compromitere sau dacă există dovezi clare că metoda specifică utilizată pentru a genera cheia privată a fost defectuoasă (CRLReason #1, keyCompromise).

Compromiterea cheii private înseamnă:

- (1) accesul neautorizat la cheia privată sau un motiv întemeiat de a crede acest lucru,
- (2) pierderea cheii private sau apariția unui motiv de a suspecta o astfel de pierdere,
- (3) furtul cheii private sau apariția unui motiv de a suspecta un astfel de furt,
- (4) ștergerea accidentală a cheii private.

#### 4.9.2 Cine poate solicita revocarea certificatelor

Următoarele entități pot trimite cereri de revocare a certificatelor:

- Beneficiarul care este titularul cheii private asociate cheii publice din certificat,
- Beneficiarul care încheie un acord contractual cu certSIGN pentru emiterea de certificate,
- Autoritatea de înregistrare care poate solicita revocarea fie în numele unui beneficiar, fie în cazul în care dispune de informații care justifică revocarea certificatului,
- Roluri de încredere asociate certSIGN Qualified CA, sub supravegherea PPMB.

Beneficiarii, Entitățile partenere, Furnizorii de Aplicații Software și alte terțe părți pot trimite Rapoarte privind Problemele Certificatelor care să informeze certSIGN în legătură cu un motiv rezonabil pentru revocarea certificatului.

Cererea de revocare poate viza mai multe certificate.

#### 4.9.3 Procedura cererilor de revocare

CA menține o capacitate continuă, 24x7, de a accepta și de a răspunde la cererile de revocare și solicitările conexe.

Procedura de revocare este descrisă în secțiunea 3.4 a prezentului CPP. Cererea de revocare de certificate trebuie să identifice precis fiecare certificat, trebuie să cuprindă motivul pentru care este cerută revocarea, și trebuie să fie autenticată. Informațiile despre certificatele revocate sunt plasate în Lista de Certificate Revocate (CRL) emisă de certSIGN Web CA. O cerere de revocare certificat se desfășoară astfel:

- certSIGN verifică cererea de revocare, incluzând transmiterea acesteia de către o entitate legitimă. Dacă verificarea este confirmată, certSIGN Web CA pune informația despre certificatul revocat în lista CRL;
- certSIGN notifică Beneficiarul despre revocare sau despre decizia de anulare a cererii de revocare, împreună cu motivația acestei anulări.
- Dacă certSIGN stabilește că revocarea este adecvată, personalul certSIGN revocă certificatul și actualizează CRL.

#### 4.9.4 Perioada de grație a cererii de revocare

certSIGN efectuează revocarea în maximum 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 Termenul 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

Ca o excepție, dacă cererea de revocare nu poate fi confirmată sau validată în termen de 24 de ore, certSIGN nu va revoca certificatul și justificarea va fi înregistrată..

#### 4.9.6 Verificarea cerințelor de revocare pentru Entitățile Partenere

Entitățile partenere vor folosi toate resursele pe care certSIGN le pune la dispoziție prin depozitarul său pentru a verifica starea unui certificat în orice moment înainte de a se baza pe acesta. certSIGN actualizează OCSP, CRL-uri în consecință.

#### 4.9.7 Frecvența de emiterie a CRL-urilor

Fiecare autoritate de certificare parte a certSIGN emite liste de revocare a certificatelor diferite. Un nou CRL este publicat în Depozitar imediat după fiecare revocare a certificatului sau în maxim o zi. Perioada de disponibilitate a CRL este de 48 de ore și se actualizează zilnic. 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 CA.

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

#### 4.9.8 Latența maximă pentru CRL-uri

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

#### 4.9.9 Disponibilitatea verificării on-line a revocării/stării

Răspunsurile OCSP sunt semnate de către un OCSP Responder al cărui certificat este semnat de CA-ul care a emis certificatul al carui status de revocare se verifica.

Răspunsurile OCSP operate de certSIGN acceptă metoda HTTP GET, astfel cum este descrisă în RFC 6960, procesează extensia Nonce (1.3.6.1.5.5.7.48.1.2) în conformitate cu RFC 8954 și furnizează un răspuns autorizat în termen de cel mult 15 minute de la prima publicare a certificatului sau precertificatului.

Certificatul de semnare al OCSP contine o extensie de tipul id-pkix-ocsp-nocheck, așa cum este definit de către RFC6960.

Pentru starea Certificatelor de Beneficiar, CA actualizează informațiile furnizate prin intermediul unui Protocol de Verificare Online a Stării Certificatelor (OCSP) cel puțin o dată la fiecare oră. Răspunsurile OCSP din partea acestui serviciu au un termen maxim de expirare implicit de 24 h.

Pentru starea Certificatelor CA-urilor subordonate:

CA actualizează informațiile furnizate prin intermediul unui Protocol de Verificare Online a Stării Certificatelor cel puțin

- O data la 12 luni și
- în termen de 24 de ore după revocarea Certificatului unui CA Subordonat.

Dacă responder-ul OCSP primește o solicitare cu privire la starea unui certificat care nu a fost emis, atunci responder-ul nu răspunde cu o stare "good" pentru aceste certificate.

certSIGN monitorizează respondentul OCSP pentru cererile de numere de serie „neutilizate” ca parte a procedurilor sale de răspuns de securitate.

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

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

1. „atribuit” dacă un certificat cu acea serie a fost emis de CA emitent, folosind orice cheie curentă sau anterioară asociată subiectului CA; sau
2. „rezervat” dacă un pre-certificat [RFC6962] cu acea serie a fost emis de (a) CA emitent; sau (b) un pre-certificat de semnare [RFC6962] asociat cu CA emitent;
3. „neutilizat” dacă niciuna din condițiile de mai sus nu sunt îndeplinite.

#### **4.9.10 Verificarea on-line a cerințelor de revocare**

Nu este stipulat.

#### **4.9.11 Alte forme disponibile pentru anunțarea revocării**

Nu este stipulat.

#### **4.9.12 Cerințe speciale referitoare la compromiterea cheii**

Dacă un beneficiar cunoaște sau suspectează că integritatea cheii private a certificatului său a fost compromisă, subiectul trebuie să:

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

Compromiterea cheii private poate avea implicații asupra informațiilor protejate cu această cheie. Subiectul decide cum să se ocupe de informațiile afectate înainte de a șterge cheia compromisă.

Metode acceptabile pe care terții le pot utiliza pentru a demonstra compromisul cheii private:

1. Utilizează procedura descrisă în secțiunea 7.6 din RFC 8555 și semnează cererea de revocare cu cheia privată compromisă.
2. Semnează un text oferit de certSIGN folosind cheia privată compromisă.
3. Trimiterea cheii private.

#### **4.9.13 Circumstanțe pentru suspendare**

Nu este stipulat.

#### **4.9.14 Cine poate solicita suspendarea**

Nu este stipulat.

#### 4.9.15 Procedura de solicitare a suspendării

Nu este stipulat

#### 4.9.16 Limitări ale perioadei de suspendare

Nu este stipulat

### 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-urilor web "www.certsign.ro" și "ocsp.certsign.ro". Serviciile de verificare a stării certificatelor oferă informații despre starea certificatelor valide. Integritatea și autenticitatea informațiilor despre starea lor este protejată prin semnătura electronică a CA-ului respectiv. Intrările de revocare din CRL sau răspunsurile OCSP nu sunt șterse înainte de data expirării certificatului revocat.

#### 4.10.2 Disponibilitatea serviciului

certSIGN operează și menține capabilitățile CRL și OCSP cu resurse suficiente pentru a asigura un timp de răspuns de două secunde sau mai puțin, în condiții normale de operare.

certSIGN menține 24x7 un Depozitar online, astfel încât aplicațiile software să poată verifica automat starea curentă a tuturor certificatelor ne-expirate emise de CA.

CA are capacitatea de a răspunde intern 24 de ore din 24, 7 zile din 7, la o informare de prioritate ridicată privind probleme la certificate și, după caz, să trimită o plângere la autoritățile de aplicare a legii, și/sau să revoce certificatul care face obiectul unei astfel de plângeri.

#### 4.10.3 Funcții opționale

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

### 4.11 Încetarea abonamentului

Sfârșitul abonamentului apare după:

- Revocarea cu succes a ultimului certificat al unui beneficiar/ subiect,
- Expirarea ultimului certificat al unui beneficiar/ subiect.

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

### 4.12 Custodie și recuperare chei

certSIGN nu permite custodia cheii pentru certificate SSL.

#### 4.12.1 Principalele politici și practici de escrow și recuperare

Nu este stipulat.

#### 4.12.2 Politica și practicile cheie de încapsulare și recuperare a sesiunii

Nu este stipulat.

## 5 Facilitate, Management și Controale Operaționale

Acest capitol descrie cerințele generale referitoare la controalele de securitate, securitatea fizică și operațională, precum și activitatea personalului, utilizate în certSIGN, de exemplu în perioada generării de chei, a verificărilor de autentificare, a emiterii și publicării de certificate, a revocării de certificate, a auditării sau a creării de copii backup.

În calitate de furnizor de servicii de 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,
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted 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, terminalele operatorilor și resursele informaționale ale certSIGN se află într-o zonă dedicată, protejată fizic împotriva accesului neautorizat, distrugerilor sau perturbării activității. Aceste locații sunt monitorizate. Fiecare intrare și ieșire este înregistrată în jurnalul de evenimente (log-urile sistemului); stabilitatea sursei de electricitate precum și temperatura și umiditatea sunt de asemenea monitorizate și controlate.

### 5.1.1 Amplasarea și construcția sediului

certSIGN CA se află în București, România, la următoarea adresă: b-dul.Tudor Vladimirescu nr.29, AFI Tech Park 1, București, Romania.

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;
- A 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 intrușilor și sisteme de alimentare cu energie electrică în caz de urgență.

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

Vizitatorii locațiilor aparținând certSIGN trebuie să fie însoțiți 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 mișcare, efracție și incendiu. Accesul în această zonă este permis numai personalului autorizat. Monitorizarea drepturilor de acces se face folosind carduri de identitate și cititoare, montate lângă punctul de acces. Fiecare intrare și ieșire 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 informațiile sensibile sunt protejate prin folosirea unor seifuri, iar accesul la terminalele operatorilor și administratorilor necesită autorizarea prealabilă a acestora, securitatea fizică în această zonă este considerată ca fiind adecvată. Cheile de acces pot fi ridicate numai de personalul autorizat. Zona este accesibilă exclusiv personalului certSIGN și persoanelor autorizate; prezența în zonă a celor din urmă le este permisă doar dacă sunt însoțiți de un angajat certSIGN.

Zonele de dezvoltare și testare sunt protejate într-un mod similar cu protejarea zonelor de operare și administrare. În această zonă nu este permisă prezența persoanelor neînsoțite. Programatorii și dezvoltatorii nu au acces la informații sensibile. Dacă este necesar accesul la astfel de informații, el este permis doar în prezența administratorului de securitate. Proiectele în curs de implementare și software-ul aferent sunt testate în mediul de dezvoltare al certSIGN.

### 5.1.3 Alimentarea cu curent și aerul condiționat

Toate zonele sunt prevăzute cu aer condiționat. În zona serverelor, echipamentele de aer condiționat sunt redundante, iar temperatura este monitorizată atât automat (cu o alertă când un anumit nivel este atins) cât și manual. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgență (UPS) permit continuarea neperturbată a activității până la intervenția automată a grupului electrogen al clădirii. Infrastructura de curent electric este concepută astfel încât la o întrerupere a curentului în clădire toate activitățile să fie disponibile pentru cel puțin 24 de ore cu ajutorul generatorului diesel. Fiecare server, echipament de

rețea și toate calculatoarele angajaților care desfășoară activități importante pentru activitățile CA și RA sunt conectate la UPS-uri. Principalele componente ale securității fizice sunt de asemenea conectate la UPS-uri și la generatorul diesel.

#### **5.1.4 Expunerea la apă**

Riscul de inundație în zona serverelor este controlat prin rack-uri. Toate echipamentele sunt plasate în rack-uri la o distanță 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**

Locația certSIGN dispune de sistem de prevenire și protecție 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 informațiilor**

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 Eliminarea deșeurilor**

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

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

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

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

#### **5.1.8 Stocarea copiilor de siguranță în afara locației**

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

Stocarea în afara locației cuprinde, de asemenea, arhive, copii curente ale informațiilor procesate de sistem și kit-urile de instalare al aplicațiilor certSIGN. Aceasta permite recuperarea de urgență a fiecărei activități certSIGN în termen de 48 de ore în sediul certSIGN sau într-un sediu auxiliar.

## **5.2 Controale procedurale**

### **5.2.1 Roluri de încredere**

Toate rolurile implicate în furnizarea serviciilor de certificare ale certSIGN sunt completate cu angajați ai 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 aplicate suficiente controale de securitate a calculatoarelor pentru separarea rolurilor de încredere identificate, inclusiv separarea rolurilor de administrare de securitate de restul rolurilor operationale. În special, utilizarea de programe utilitare de sistem este limitată și controlată.

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

- **Ofițer de securitate** – Responsabilitate globală pentru implementarea politicilor și procedurilor de securitate.
- **Administratorul de sistem** – Autorizat să instaleze, configureze și să întrețină sistemele de încredere ale Autorității de Certificare pentru înregistrarea, generarea de certificate, furnizarea dispozitivelor subiecților și gestiunea revocărilor de certificate. Instalează dispozitivele hardware și sistemele de operare; instalează și configurează echipamentele de rețea.
- **System operator** – Responsabil de operarea zilnică a sistemelor de încredere ale Autorității de Certificare. Autorizat să execute operațiile de backup și restaurare a sistemului. Are acces la certificatele Subiecților; revocă certificatele Subiecților; asigură continuitatea copiilor de siguranță și a arhivelor bazelor de date și crearea log-urilor de sistem; manages databases; administrează bazele de date; are acces la informații confidențiale despre Subiecți/Beneficiari, dar nu are dreptul de a accesa fizic nici o altă resursă a sistemului; transferă copiile de siguranță ale arhivei și ale datelor curente către locațiile desemnate.
- **Ofițer înregistrare:** Responsabil de verificarea informațiilor care sunt necesare pentru emiterea de certificate și pentru aprobarea cererilor de certificare;
- **Ofițeri de revocare:** Responsabil de operarea modificării stărilor certificatelor;
- **Auditor de system** – autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale Autorității de Certificare. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici și Proceduri de către Autoritatea de Certificare; această responsabilitate se extinde și asupra Autorității de Înregistrare care operează în cadrul certSIGN.

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

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

### 5.2.2 Numărul de persoane necesare pentru fiecare sarcină

Acolo unde controlul dual sau controlul multiplu este necesar, cel puțin două persoane distincte, cu roluri de încredere relevante sunt prezente pentru a putea îndeplini operațiunea.

Circumstanțele ce necesită control dual sau multiplu sunt descrise în documentația internă confidențială.

### 5.2.3 Identificarea și autentificarea pentru fiecare rol

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

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

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

Fiecare cont alocat:

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

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

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

Toate acțiunile angajaților care au roluri de încredere sunt urmărite și este asigurată răspunderea deplină.

### 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 solicitări de abilități și experiență specifice, definite din punctul de vedere al rolurilor îndeplinite. Segregarea sarcinilor și principiul celui mai mic privilegiu sunt aplicate. Sensibilitatea poziției stabilită în funcție de sarcini determină nivelul de acces, screening-ul înainte de angajare și trainingul angajaților.

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 îndeplinește responsabilitățile funcției, conform cu rolul atribuit în cadrul unei Autorități de Certificare sau Înregistrare:

- a absolvit cel puțin liceul,
- A inteles și a semnat un contract ce descrie rolul și responsabilitățile sale în cadrul sistemului,
- a beneficiat de un stagiu de pregătire avansată în conformitate cu obligațiile și sarcinile asociate funcției sale,
- a fost instruit cu privire la protecția datelor personale și informațiilor confidențiale sau private,
- a semnat un contract ce conține clauze referitoare la protejarea informațiilor sensibile ale certSIGN și a datelor confidențiale și private ale Beneficiarilor,
- nu îndeplinește sarcini care pot genera conflicte de interese între Autoritatea de Certificare și Autoritatea de Înregistrare care acționează 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, experiență 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 asigură efectuarea controalelor relevante personalului potențial prin intermediul rapoartelor de stare emise de o autoritate competentă, al declarațiilor de la terți sau al declarațiilor auto-semnate.

#### 5.3.3 Cerințele de pregătire a personalului

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

- Cerințele CPP,
- Procedurile și controalele de securitate folosite de Autoritatea de Certificare și Autoritatea de Înregistrare;
- Cunoștințe de bază PKI, politici și proceduri de autentificare și verificare;
- Amenințările comune ale procesului de verificare a informațiilor (inclusiv phishing și alte tactici de inginerie socială) și cerințele CA/B Forum Baseline Requirements
- Responsabilitățile ce decurg din rolurile și sarcinile executate în sistem,

După încheierea pregătirii, participanții semnează un document prin care confirmă familiarizarea lor cu Codul de Practici și Proceduri, Politica de certificare și acceptă restricțiile și obligațiile impuse.

CA garantează că personalul încredințat cu îndatoririle Specialistului în Validare trebuie să mențină un nivel de calificare care să le permită îndeplinirea acestor sarcini în mod

satisfăcător. CA documentează faptul că fiecare Specialist în Validare posedă competențele necesare unei sarcini înainte de a permite Specialistului în Validare să îndeplinească acea sarcină. CA solicită tuturor Specialiștilor în Validare să treacă un examen furnizat de CA cu privire la cerințele de verificare a informațiilor prezentate în CPP și cerințele CA/B Forum Baseline Requirements.

#### **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 rol de încredere își menține un nivel al competențelor corespunzător cu programele de instruire și performanță ale certSIGN.

#### **5.3.5 Frecvența și secvența rotației posturilor**

Nu este stipulat.

#### **5.3.6 Sancțiunile pentru acțiunile neautorizate**

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

#### **5.3.7 Cerințele pentru contractanții independenți**

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) face obiectul unor verificări similare celor efectuate în cazul angajaților 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 își desfășoară activitatea în locația certSIGN, trebuie să fie însoțit permanent de un angajat al certSIGN, cu excepția celor care au primit avizare din partea administratorului de securitate și care pot accesa informații clasificate intern sau în conformitate cu normele legale în vigoare.

#### **5.3.8 Documentația oferită personalului**

certSIGN oferă personalului său accesul la următoarele documente:

- CPP,
- Lista Responsabilităților și obligațiilor asociate rolului deținut în sistem
- Politicile și procedurile de securitate

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

### **5.4 Procedurile de înregistrare a datelor de audit**

Pentru gestionarea eficientă a sistemelor și aplicațiilor folosite de certSIGN în activitatea sa în calitate de furnizor de servicii de certificare, dar și pentru a permite auditarea acțiunilor angajaților și clienților, toate informațiile cu privire la evenimente importante, generate de sisteme și aplicații sunt înregistrate. Aceste informații, cunoscute în mod colectiv sub numele de log-uri trebuie să fie păstrate în așa fel încât să poată fi accesate de către Entitățile

Partenere, auditori și autoritățile de stat oricând au nevoie de ea, pentru a furniza dovezi ale funcționării corecte a serviciilor în scopul procedurilor legale sau pentru a detecta încercările de a compromite securitatea certSIGN. Evenimentele înregistrate sunt arhivate și păstrate într-o locație secundară.

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

#### 5.4.1 Evenimente Înregistrate

Fiecare activitate critică din punctul de vedere al securității certSIGN este înregistrată în log-urile de evenimente și arhivată. Arhivele sunt depozitate pe medii de stocare ce nu pot fi suprascrise sau distruse cu ușurință (cu excepția cazului în 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 conțin înregistrări ale tuturor activităților generate de componentele software din cadrul sistemului. Aceste înregistrări sunt împărțite în trei categorii separate:

- **Intrări de sistem** – conțin informații despre cererile clienților și răspunsurile serverului (sau invers) la nivelul protocolului de rețea (de exemplu http, https); datele concrete care se înregistrează sunt: adresa IP a stației sau a server-ului, operațiunile executate (de exemplu: căutare, editare, scriere etc.) și rezultatele lor (de exemplu introducerea cu succes a unei înregistrări în baza de date),
- **Erori** – conțin informații despre erori la nivelul protoalelor de rețea și la nivelul modulelor aplicațiilor;
- **Audit logs** – conțin informații specifice serviciilor de certificare, de exemplu: cererea de înregistrare 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 stație de lucru și au o capacitate prestabilită. Atunci când se depășește această capacitate, este creată automat o nouă versiune de jurnal. Jurnalul anterior este arhivat și șters 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.
- Rezultate ale verficarilor cu coroborarea emiterii prin perspective multiple (MPIC)

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, conține următoarele informații:

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

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

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

Toate informațiile de înregistrare, inclusiv următoarele sunt înregistrate:

- tipul de document(e) prezentat de către solicitant la înregistrare;
- înregistrarea datelor de identificare unice, numere, sau o combinație a acestora (de exemplu, cartea de identitate a solicitantului sau pașaport) a documentelor de identificare, dacă este cazul;
- locul de depozitare al copiilor cererilor și a documentelor de identificare, inclusiv contractul semnat de Beneficiar
- orice opțiuni specifice din contract (de exemplu, acceptarea publicării certificatului)
- Identitatea entității care acceptă cererea;

- Metoda utilizată pentru validarea documentelor de identificare, Accesul la log-uri este permis exclusiv pentru ofițerul de securitate, personal special desemnat, și auditori, prin cerere adresată pe email sau în format hartie către 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 siguranță sunt făcute în mod continuu.

#### 5.4.3 Perioada de păstrare a log-urilor de audit

Înregistrările evenimentelor sunt stocate în fișiere 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 depășirea spațiului alocat, jurnalele sunt păstrate în arhive și pot fi accesate numai off-line, de la o anumită stație de lucru.

Jurnalele arhivate sunt păstrate cel puțin 10 ani.

CA-ul și fiecare terț delegat păstrează:

1. Înregistrările de evenimente de gestionare a certificatului și a cheilor de la CA în timpul ciclului de viață după apariția ulterioară a:
  - distrugerea cheii private a CA; 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 în comun o cheie publică corespunzătoare cheii private a CA;
2. Înregistrările de evenimente 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 sunt prevăzute în 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 entitățile de mai sus au dreptul să citească înregistrările jurnalului,
- Platforma centrală de jurnale arhivează sau șterge automat fișierele (după arhivarea lor) care conțin evenimentele înregistrate,
- Este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conțin lacune sau falsuri,
- Nici o entitate nu are dreptul să modifice conținutul unui jurnal.

În plus, procedurile de protecție a jurnalului sunt implementate în așa fel încât, chiar și după arhivarea jurnalului, este imposibil să ștergi înregistrări, sau să ștergi jurnalul înaintea expirării perioadei de retenție a jurnalului.

#### 5.4.5 Procedura de backup a log-urilor de Audit

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

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

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

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

#### 5.4.7 Notificarea la eveniment – subiectul în cauză

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 dată 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 înregistrarea informațiilor asociate securității sistemului, cererile trimise de Beneficiari, informațiile despre Subiecți/Beneficiari, certificatele emise și CRL-urile, cheile folosite de Autoritățile de Certificare și Înregistrare, și toată corespondența dintre certSIGN și Beneficiari să fie arhivate.

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

Arhiva offline conține certificate expirate, inclusiv certificatele revocate. Arhiva certificatelor revocate conține informații despre certificat, motivul revocării, dacă când a fost certificatul plasat în CRL. Arhiva este folosită pentru rezolvarea eventualelor dispute, referitoare la documente vechi, semnate electronic de un Beneficiar.

Copiile de siguranță sunt ținute în afara locației certSIGN.

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

### 5.5.2 Perioada de retenție a arhivei

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

### 5.5.3 Protecția arhivei

certSIGN asigură:

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

Arhivele sunt accesibile exclusiv personalului autorizat.

### 5.5.4 Procedurile de back-up al arhivei

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

### 5.5.5 Cerințe privind marcarea temporală a înregistrărilor

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. Acuratetea timpului este asigurată de un server de timp care este sincronizat cu cel puțin două surse de timp care pot fi sateliti 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 Proceduri de obținere și verificare a informațiilor arhivate

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

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

## 5.6 Schimbarea cheilor

Procedurile de schimbare a cheilor permit tranziția ușoară de la certificate de CA expirate către certificate noi. Spre sfârșitul vieții Chei Private a CA, certSIGN încetează să utilizeze cheia privată a CA care expiră pentru a semna Certificate (cu cel puțin un an înaintea expirării) și utilizează vechea cheie privată doar pentru a semna CRL-uri. O nouă pereche de chei de semnare CA este comandată și toate certificatele emise ulterior și CRL-urile, sunt semnate cu noua cheie privată de semnare. Atât vechile, cât și cele noi perechi de chei pot fi active simultan. Acest proces de schimbare a cheilor ajută la minimizarea oricăror efecte negative ale expirării certificatului CA. Noul certificat de CA este furnizat către clienți și Entități Parteneri 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 situații anormale (inclusiv dezastrele naturale) pentru restaurarea serviciilor la nivelul garantat. Aceste proceduri sunt executate în concordanță cu Planul de continuitate a afacerii și de recuperare în caz de dezastru.

### 5.7.1 Procedurile de administrare 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/sau 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 utilizează procedurile interne. Aceste proceduri includ și notificarea Furnizorilor de Aplicații Software, auditorilor certSIGN, Autorității 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 din Dezastre, care includ Planul de Management în situații de Criză, și a documentat proceduri de continuitatea afacerii și de recuperare la dezastre, concepute să notifice și să protejeze în mod rezonabil Furnizorii de Aplicații Software, Beneficiarii și Entitățile Parteneri în eventualitatea unui dezastru, a unei compromiteri de securitate, sau al unui eșec al afacerii. certSIGN pune la dispoziție, la cerere, către auditorii CA-ului, planul de continuitate al afacerii și planurile de securitate disponibile. CA-ul revizuieste, testează și actualizează anual aceste proceduri.

Planul de continuitate al afacerii include elementele din CAB Forum BR secțiunea 5.7.1

certSIGN CA menține un plan cuprinzător și aplicabil pentru evenimente de revocare în masă, efectuează teste anuale ale procedurilor sale și încorporează lecțiile învățate pentru a îmbunătăți pregătirea în timp.

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

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

- distrugerea fizică a sistemului de calcul al certSIGN, inclusiv alterarea resurselor de rețea – această amenințare se referă la distrugerile provocate de situațiile de urgență,
- funcționarea defectuoasă a aplicațiilor, având ca efect imposibilitatea accesării datelor - aceste deteriorări se referă la sistemul de operare, aplicațiile utilizatorilor și executarea de aplicații periculoase, cum ar fi virusii, viermii, caii troieni,
- pierderea unor servicii de rețea importante pentru activitatea certSIGN. Acestea se referă în primul rând la căderile de tensiune și distrugerea legăturilor de rețea.
- distrugerea unei părți din Intranetul folosit de certSIGN pentru a furniza servicii – acest lucru poate duce la obstrucționarea clienților și refuzul (neintenționat) 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 apariției unui eveniment ce blochează funcționarea certSIGN, în maxim 48 de ore, va fi activată locația auxiliară ce poate substitui toate funcțiile importante ale unei Autorității de Certificare până la restaurarea locației principale. Distanța dintre locația primară și cea secundară este suficient de mare pentru ca potențialul dezastru care afectează locația primară să nu afecteze și locația secundară.
- Instalarea de versiuni noi ale aplicațiilor software în producție 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 aplicații pentru crearea copiilor de rezervă a datelor pe baza cărora se poate face în orice moment restaurarea sistemului și auditarea

acestui. Copiile de siguranță includ toate datele relevante din punct de vedere al securității.

- Toate sistemele din care este compusă infrastructura IT pentru furnizarea de servicii de certificare și timestamp sunt monitorizate în mod continuu și toate evenimentele de securitate sunt înregistrate și analizate. Activitățile de sistem anormale care indică o potențială încălcare a securității, inclusiv intruziune în sistemele de rețea sunt detectate și raportate ca alarme pentru a permite certSIGN să detecteze, înregistreze și reacționeze în timp util la orice tentative neautorizate și/sau neobișnuite de a accesa resursele sale.
- Sensibilitatea oricăror informații colectate sau analizate este luată în considerare, protejându-le împotriva accesului neautorizat.
- Pentru a detecta orice discontinuitate în operațiunile de monitorizare, pornirea și oprirea funcțiilor de logare este, de asemenea, monitorizată
- Disponibilitatea tuturor componentelor importante ale infrastructurii 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 fezabil financiar, 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 entități

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

În cazul compromiterii cheii private a CA sau în cazul în care există suspiciunea că ea a fost compromisă, trebuie luate și următoarele măsuri:

- Notificarea - asupra compromiterii - a tuturor 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 Subiecți
- Noile certificate sunt trimise Subiecților în mod gratuit
- Dacă un certificat este revocat din cauza compromiterii cheii CA, certSIGN Root CA G2 va emite un CRL nou în termen de 24 de ore de la primirea notificării privind compromisul și va publica CRL-urile online imediat.

Când o cheie privată asociată cu o cheie publică din certificat a fost compromisă, sau există un motiv serios de a suspecta că a fost compromisă, Beneficiarul trebuie să solicite certSIGN revocarea certificatului.

Paragraful anterior este de asemenea aplicabil în cazul în care algoritmi PKI sau parametri asociați sunt compromise sau dacă aceștia devin insuficienți pentru utilizarea dorită rămasă.

#### 5.7.4 Capacități de Continuitate a afacerii în caz de dezastru

certSIGN a stabilit într-un Plan de Continuitate a afacerii (BCP) și un Plan de recuperare în caz de dezastru (DRP) toate măsurile necesare pentru a asigura recuperarea integrală a serviciilor noastre de certificare și marcarea 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 marcarea 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 a unei defecțiuni a mediilor de stocare. Activitățile de back-up sunt testate în mod regulat pentru a se asigura că acestea îndeplinesc cerințele planurilor de continuitate a afacerii.

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

Planurile BCP și DRP abordează de asemenea compromiterea, pierderea sau suspiciunea de compromitere a cheii private sau compromiterea algoritmilor PKI a CA ca pe un dezastru, iar procesele planificate sunt puse în aplicare.

În urma unui dezastru, acolo unde este posibil, vor fi luate măsuri pentru a evita repetarea unui dezastru.

### 5.8 Încetarea activității Autorității de Certificare sau a Autorității de Înregistrare

certSIGN are un plan la zi de încetare a activității pentru a minimiza efectele negative asupra Beneficiarilor și Entităților Partenere ce pot apărea ca urmare a deciziei unei Autorități de Certificare de a-și înceta activitatea. Planul include obligativitatea notificării în avans a tuturor Beneficiarilor asupra autorității ce a certificat autoritatea de certificare ce urmează să își înceteze activitatea (dacă există) și tranziția responsabilităților (servicii furnizate către Subiecți/Beneficiari, baze de date, etc), în conformitate cu reglementările aplicabile, către 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 (neexpire și nerevocate) emise de această autoritate și alte entități cu care certSIGN are înțelegeri sau alte forme de colaborare, printre care Entități Partenere, alți furnizori de servicii de încredere și autorități relevante, cum ar fi organismele de supraveghere. În plus, această informație va fi făcută disponibilă și altor Entități Partenere;
- Revocă certificatele neexpire 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 neexpire care au fost emise și la arhivele jurnalului de evenimente pentru perioada respectivă de timp, astfel cum a fost menționată Beneficiarului și Entității Partenerie;
- Distrugă 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 transfera 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 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 Autorității de Certificare care își încetează activitatea preia drepturile și obligațiile acestei autorități în ceea ce privește managementul certificatelor care rămân în uz.

Arhiva Autorității de Certificare care-și încetează activitatea trebuie predată Autorității de Certificare primare – certSIGN ROOT CA G2 (în cazul încetării activității autorității certSIGN Web CA) sau instituției cu care a fost semnat contractul (în cazul în care certSIGN ROOT CA G2 își încetează activitatea).

## **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 revizuieste politica privind lanțul de aprovizionare și monitorizează, revizuieste, 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 Autorități 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, depozitățile, cheile private și datele de activare pentru cheile private ale CA-urilor, și ale altor Participanți PKI și alți parametri critici de securitate.

Procedurile de management al cheii se referă la păstrarea și folosirea în siguranță de către proprietar a cheilor sale. O atenție deosebită se acordă generării și protecției cheii private a certSIGN, care influențează funcționarea în siguranță a întregului sistem de certificare a cheilor publice.

**certSIGN Web CA** detine cel puțin un certificat semnat de **certSIGN ROOT CA G2**. Cheia privată corespunzătoare cheii publice conținute în certificat este utilizată exclusiv pentru a semna cheile publice ale subiecților și lista de revocare a certificatelor necesare pentru funcționarea CA.

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 pentru efectuarea generării cheilor. 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 elaborează un raport al ceremoniei cheilor care dovedește că ea a fost efectuată în conformitate cu procedura declarată și că integritatea și confidențialitatea perechii de chei au fost asigurate. Acest raport este semnat de toți participanții, în special de către rolul de încredere responsabil pentru securitatea ceremoniei de management al cheilor certSIGN (de exemplu, ofițer de securitate), ca martor că raportul înregistrează corect ceremonia de management al cheilor în timpul execuției sale.

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 cadrul Scriptului Ceremoniei cheilor.

Cheile certSIGN Web CA sunt angajate într-un mediu fizic securizat de către personal cu roluri de încredere sub, cel puțin, control dual 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 (PPMB),
- Administrator ceremonie chei,
- Cel puțin un Auditor Calificat, independent sau extern

Perechile de chei ale CA-ului sunt generate pe stații de lucru desemnate, autentificate și conectate la module hardware de securitate, conforme cu cerințele FIPS 140-2 Nivel 3 sau ISO/IEC 15408 EAL 4. Ele sunt păstrate în permanență criptate pe aceste dispozitive.

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 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 aplica 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 operații 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.

Cheile Beneficiarului sunt generate de către Subiect, prin aplicații software sau dispozitive criptografice.

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

- perechea de chei nu îndeplinește cerințele stabilite în secțiunea 6.1.5 și / sau în secțiunea 6.1.6
- Există dovezi clare că metoda specifică utilizată pentru a genera cheia privată a fost compromisă;
- CA are la cunoștință despre o metodă demonstrată sau dovedită care expune cheia privată a solicitantului la compromisuri;
- CA a fost informată anterior că cheia privată a solicitantului a suferit un compromis, cum ar fi cele menționate în secțiunea 4.9.1.1 don BR;
- CA are la cunoștință despre o metodă demonstrată sau dovedită pentru a calcula cu ușurință cheia privată a solicitantului pe baza cheii publice (cum ar fi o cheie slabă Debian, consultați <https://wiki.debian.org/SSLkeys>).

În cazul în care certificatul SSL abonat conține o extensie extKeyUsage care conține valorile id-kp-serverAuth sau anyExtendedKeyUsage, CA-ul NU va genera o pereche de chei în numele abonatului și NU va accepta o cerere de certificat SSL utilizând o pereche de chei generată anterior de CA.

#### **6.1.2 Distribuirea Cheii Private către Beneficiar**

Nu livram cheia private Beneficiarului din cauza ca aceasta este generate doar de Subscriber.

#### **6.1.3 Distribuirea Cheii Publice către emitentul certificatului**

Beneficiarii trimit cheile publice generate ca o solicitare electronică al cărei format trebuie să respecte protocoalele din PKCS#10 (CSR).

#### **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 Autorități de Certificare care emite certificate Subiecților sunt distribuite exclusiv sub formă de certificate conforme recomandărilor ITU-T X.509 v.3.

CA-ul își publică certificatele prin plasarea lor în depozitarul public disponibil la adresa: <https://www.certsign.ro/resurse/lantul-de-incredere-g2>

Certificatele CA-urilor pot fi livrate Entităților 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**

certSIGN Web CA utilizează o cheie de 4096 biți pentru semnarea certificatelor și semnarea CRL-urilor.

Certificatele digitale emise de certSIGN Web CA utilizează chei RSA de 2048, 3072 sau 4096 biți. Certificatele digitale sunt semnate folosind algoritmul RSA în combinație cu algoritmul SHA-2.

Acești algoritmi și aceste dimensiuni de chei sunt permise acum, dar certSIGN își rezervă dreptul de a introduce în viitor alți algoritmi și protocoale decât RSA cu SHA-2 sau lungimi de chei mai lungi. Aceasta poate include algoritmi de Curbă Eliptică în loc de RSA și alți algoritmi de hash.

#### **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 certSIGN Web CA. 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 Capitolul 7.1.1.2) din cadrul extensiilor standard ale certificatelor X.509 v3. Acest câmp trebuie verificat în mod obligatoriu de aplicația Beneficiarului care face managementul certificatelor.

Folosirea biților din câmpul KeyUsage trebuie să respecte următoarele reguli:

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

Cheia private a certSIGN Web CA este folosită doar în următoarele cazuri:

1. Certificate pentru utilizatori finali;
2. Certificate pentru scopuri de infrastructură (certificate de verificarea a Răspunsului OCSP);

### 6.2 Protecția cheii private și controalele modului 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.

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
- 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

Generarea perechilor de chei de CA este efectuată pe 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 CA folosite la semnarea certificatelor și a CRL-urilor.

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

Procedura comună de transfer a secretului trebuie să includă: procesul de generare și distribuire a cheilor, acceptarea secretului livrat și responsabilitățile care rezultă pentru protejarea acestuia.

### Acceptarea secretului partajat de către deținătorii săi

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

oferirii părții sale din secret), numai după autorizarea transmiterii secretului. Această situație trebuie înregistrată în mod corespunzător în log-urile de securitate.

În cazul dezastrelor naturale, deținătorul secretului trebuie să se prezinte la locul de recuperare în caz de urgență al certSIGN, conform instrucțiunilor primite de la emitentul secretului partajat. Secretul partajat trebuie livrat personal de către deținător la locul recuperării în caz de urgență, într-un mod care să permită folosirea lui pentru restaurarea activității certSIGN la starea sa normală.

### **Responsabilitățile deținătorului secretului partajat**

Deținătorul secretului partajat trebuie să-și îndeplinească îndatoririle și obligațiile conform cerințelor acestui Cod de Practici și Proceduri, în mod deliberat și responsabil în orice situație posibilă. Un deținător de secret partajat trebuie să anunțe emitentul secretului în cazul furtului, pierderii, dezvăluirii neautorizate sau compromiterii securității secretului, imediat după incident. Un deținător de secret partajat nu este responsabil pentru neîndeplinirea îndatoririlor/obligațiilor sale din cauza unor motive ce sunt imposibil de controlat de către acesta, dar este responsabil pentru dezvăluirea inoportună a secretului sau pentru neglijarea obligațiilor de a notifica emitentul secretului despre dezvăluirea inoportună sau violarea securității secretului ca urmare a greșelilor, neglijenței sau iresponsabilității deținătorului.

Controlul multiplu nu se aplică cheii private a Beneficiarului.

### **6.2.3 Custodia Cheii Private**

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

Cheile private ale beneficiarului nu sunt supuse custodiei.

### **6.2.4 Copia de siguranță a cheii private**

CA creează o copie de siguranță a cheii lor private. Copiile sunt folosite în cazul punerii în aplicare a procedurilor standard, sau de urgență (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 Autorității de Certificare.

Cheia privată de semnare a CA este salvată, stocată și recuperată 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 Autorității de Certificare folosite pentru crearea de semnături electronice nu sunt arhivate – sunt distruse imediat după încheierea operației 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 realizează în următoarele cazuri:

- În cazul creării copiilor de siguranță pentru cheile private socate 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 operațiune critică și de aceea în timpul executării operației trebuie implementate măsuri și proceduri care să prevină dezvoltarea, modificarea sau falsificarea cheii private.

Introducerea unei chei private într-un modul hardware de securitate al CA necesită restaurarea cheii de pe carduri în prezența unui număr corespunzător de deținători ai secretului partajat care protejează modulul ce conține cheile private. Deoarece fiecare CA poate deține o copie criptată a cheii sale private, cheile pot fi de asemenea transferate între module.

În cazul în care Cheia Privată a CA a fost comunicată unei persoane neautorizate sau unei organizații neafiliate la CA, certSIGN ROOT CA G2 revocă toate certificatele care includ Cheia Publică ce corespunde Cheii Private comunicate.

### 6.2.7 Stocarea cheilor private pe modul criptografic

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

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

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

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) care respectă cel puțin standardul FIPS 140-2 nivel 3 sau Common Criteria EAL 4. 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.

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.

### 6.2.8 Metoda de activare a cheii private

Toate cheile private ale CA sunt introduse în modul după generarea lor, se importă în formă criptată de pe un alt modul sau după restaurarea cu ajutorul secretelor partajate. Activarea cheilor private este precedată întotdeauna de autentificarea operatorului. Autentificarea se

realizează pe baza unui card criptografic deținut de operator. După introducerea cardului în modulul criptografic și introducerea codului PIN, cheia privată rămâne activă până când cardul este scos din modul.

### 6.2.9 Metoda de dezactivare a cheii private

Metoda de dezactivare a cheii private este aplicată pentru dezactivarea cheii după utilizare, sau după încheierea fiecărei sesiuni de utilizare în timpul căreia cheia a fost folosită.

### 6.2.10 Metoda de distrugere a cheii private

La sfârșitul duratei lor 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 (PPMB), 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-urile permit resetarea dispozitivului prin acces fizic și setări pe dispozitiv. Aceasta reinitializează dispozitivul și suprascrive 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. PPMB autorizează distrugerea cheii private a CA și desemnează personalul pentru această activitate.

Fiecare distrugere a unei chei private este înregistrată în jurnalul de evenimente.

Beneficiarul este responsabil de distrugerea cheii private.

### 6.2.11 Evaluarea Modulului Criptografic

Vezi mai sus.

## 6.3 Alte aspecte legate de managementul perechilor de chei

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

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

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

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

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

### 6.3.1 Arhivarea cheilor publice

certSIGN își arhivează propriile chei publice de CA și toate cheile publice certificate de certSIGN Web CA sub forma de certificate X509 care conțin cheia.

Vezi capitolul 5.5 pentru condițiile de arhivare.

### 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. Aceasta este de asemenea, perioada de valabilitate aplicată cheii private. Perioada maximă de utilizare a cheilor Beneficiarului nu poate depăși perioada de valabilitate a unui certificat.

Perioada de valabilitate a certificatului certSIGN Qualified CA este de 10 ani.

Perioada de valabilitate a unui certificat de Beneficiar este de până la 3 ani.

Perioadele de utilizare a certificatelor și cheilor private aferente pot fi reduse în cazul revocării unui certificat.

În general, data de începere a valabilității unui certificat corespunde datei emiterii acestuia. Nu este permisă setarea acestei date în viitor sau în trecut.

| Detinatorul cheii      | Scopul principal al utilizarii cheii         |
|------------------------|--|
|                        | <b>RSA pentru certificate și semnare CRL</b> |
| <b>certSIGN Web CA</b> | 10 ani                                       |

Tabel 6.3.2.1 Perioada maxima de utilizare

| Detinatorul cheii        | Politica de Certificare | Scopul principal al utilizarii cheii |
|--------------------------|-------------------------|--------------------------------------|
| <b>Entități juridice</b> | certSIGN Web            | 397 zile <sup>1</sup>                |

Tabel 6.3.2.2. Perioadele maxime de utilizare ale certificatelor Beneficiarilor

Reutilizarea informațiilor de validare este limitată la durata de viață a certificatului emis.

## 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 Autorității de Înregistrare și ai Autorităților de Certificare, precum și alte persoane care îndeplinesc rolurile descrise în Capitolul 5.2, trebuie să folosească parole rezistente (token-uri/carduri) ca să se autentifice la rolurile lor. Cheile lor private care sunt generate pe dispozitive de semnătură electronică calificate sau smartcard-HSM de către 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.

<sup>1</sup> Din 15 Martie 2026 durata maxima este de 200 zile; Din 15 Martie 2027 se reduce la 100 zile.

Secretele partajate folosite pentru protejarea cheii private a Autorității de Certificare sunt generate în concordanță cu cerințele prezentate în Capitolul 6.2 și 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.

Atunci când Beneficiarii își generează cheile private, este responsabilitatea lor să genereze și datele de activare (codul PIN).

#### **6.4.2 Protejarea datelor de activare**

Protejarea datelor de activare include metode de control al datelor de activare prin care se previne dezvăluirea lor. Metodele de control al datelor de activare depind de natura acestora: dacă sunt fraze de autentificare sau dacă acest control se bazează pe cheia privată sau pe distribuirea informațiilor 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.

Beneficiarii sunt responsabili pentru gestionarea și protejarea sigură a datelor de activare (codul PIN).

#### **6.4.3 Alte aspecte ale datelor de activare**

Nu este stipulat.

### **6.5 Controale de securitate informatică**

Acest capitol descrie controalele de securitate informatică ale certSIGN.

Beneficiarul este responsabil de propriile controale de securitate informatică. Aceste aspecte nu sunt acoperite în subcapitolele de mai jos.

#### **6.5.1 Cerințe tehnice specifice ale securității informatice**

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

Computerele sunt configurate cu următoarele mecanisme de securitate:

- autentificarea obligatorie la nivelul sistemului de operare și al aplicațiilor,
- control discreționar 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 și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- prevenirea refolosirii unui obiect de către un alt proces după eliberarea acestuia de către un proces autorizat,
- protecția criptografică a schimburilor de informații și protecția bazelor de date,
- arhivarea istoricului operațiunilor executate pe un calculator și a datelor necesare auditării,
- o cale sigură ce permite identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- metode de restaurare a cheilor (numai în cazul modulelor hardware de securitate), a aplicațiilor și a sistemului de operare,
- mijloace de monitorizare și alertare în cazul accesului neautorizat la resursele de calcul.

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

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

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

Datele sensibile sunt protejate împotriva relevării prin obiecte de stocare re-utilizate (de exemplu, fișiere șterse), fiind accesibile utilizatorilor neautorizați. În acest scop, trebuie utilizat un software special, cu algoritmi de ștergere siguri pentru mediile de stocare, HSM-urile se resetează, dispozitivele criptografice securizate (token-uri / carduri) trebuie formate 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 Computer security rating

Sistemul informatic certSIGN îndeplinește cerințele descrise în standard: ETSI EN 319 411-1

## 6.6 Controale tehnice 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 de definire a cerințelor a oricărui proiect de dezvoltare a sistemelor întreprins de certSIGN sau în numele certSIGN, pentru a se asigura că securitatea este inclusă în sistemele informatice.

Înainte de a fi folosită în producție în cadrul certSIGN, fiecare aplicație 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 așa fel încât să poată fi urmărită și evaluată ruta fiecăruia, până la locul său de instalare,
- livrarea unui dispozitiv fizic pentru înlocuire se realizează într-un mod similar celui de livrare al dispozitivului original; înlocuirea se realizează de către personal calificat și de încredere.

### 6.6.2 Controale specifice managementului securității

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

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

### 6.6.3 Controale de securitate specifice ciclului de viață

Politicile și procedurile de control al modificărilor sunt aplicate lansărilor, modificărilor și remediilor de urgență ale oricărui software operațional, precum și modificărilor de configurație care aplică 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.

Configurațiile Sistemelor de Emitere, a Sistemelor de Management al Certificatelor, a Sistemelor Suport de Securitate și a Sistemelor Front-End/ Sistemelor de Suport Intern sunt verificate cel puțin săptămânal pentru a determina orice schimbări 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 dedicată serviciilor de certificare, cererile de capacitate sunt monitorizate și proiecțiile cerințelor de capacitate viitoare sunt făcute pentru a se asigura că puterea de procesare și de stocare adecvate sunt disponibile.

## 6.7 Controale de securitate a rețelei

certSIGN își protejează rețeaua și sistemele de atacuri. În acest scop și pe baza evaluărilor de risc și a celor mai bune practici, implementăm un set integrat de controale de securitate:

- a) Sistemele sunt segmentate în rețele sau zone luând în considerare relația funcțională, logică și fizică (inclusiv de locație) dintre sistemele și servicii de încredere. certSIGN aplică aceleași controale de securitate pentru toate sistemele co-localizate în aceeași zonă.
- b) Accesul și comunicarea între zone sunt permise doar persoanelor necesare funcționării serviciilor de certificare. Conexiunile și serviciile care nu sunt necesare sunt interzise în mod explicit sau dezactivate. Setul de reguli stabilite sunt revizuite 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 canale de încredere care sunt distincte logic de alte canale de comunicații și oferă identificarea sigură a punctelor terminale și protecția datelor canalului de modificare sau divulgare.
- f) Dacă este necesar un nivel înalt de disponibilitate a accesului extern la un anumit serviciu de certificare, conexiunea externă la rețea este redundantă, pentru a asigura disponibilitatea serviciilor, în cazul unui singur eșec.
- g) Se realizează o scanare periodică a vulnerabilității adreselor IP publice și private identificate de certSIGN și se înregistrează dovezi că fiecare scanare a vulnerabilității a fost realizată de către o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.
- h) Serviciile de certificare ale certSIGN sunt supuse unui test de penetrare pe sistemele aferente la inițiere și după upgrade-uri de infrastructură 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/ Beneficiariși terți. Firewall-urile sunt configurate pentru împiedica toate protocoalele și intrările 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, și este fie în 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 remediarea vulnerabilităților sunt următoarele:

- 48 de ore – pentru vulnerabilități cu severitate „critică”
- 96 de ore – pentru vulnerabilități cu severitate „ridicăată”
- 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 și al Listei de certificate Revocate (CRL) respectă formatul descris în standardul ITU-T X.509 v.3, în timp ce profilul OCSP respectă cerințele RFC 6960. Informațiile de mai jos descriu semnificația câmpurilor din certificat, CRL și OCSP, standardul aplicat și extensiile folosite de certSIGN.

### 7.1 Profilul certificatului

certSIGN Web CA îndeplinește cerințele tehnice stabilite în CABF BR secțiunea 2.2 - Publicarea informațiilor, secțiunea 6.1.5 - Dimensiunile cheilor și secțiunea 6.1.6 - Generarea parametrilor cheii publice și verificarea calității.

Câmpul SerialNumber este un număr nesecvențial mai mare decât zero (0) și mai mic de  $2^{159}$ , care conține cel puțin 64 de biți de la un CSPRNG.

Toate obiectele semnate de o cheie privată certSIGN CA sunt conforme cu cerințele CABF BR #7.1.3.2, RSA sau ECDSA privind utilizarea AlgorithmIdentifier sau a tipului AlgorithmIdentifier-derivat în contextul semnăturilor.

Câmpul SubjectPublicKeyInfo indică o cheie RSA utilizând identificatorul de algoritm rsaEncryption (OID: 1.2.840.113549.1.1.1), cu un parametru NULL explicit.

AlgorithmIdentifier pentru cheile RSA este identic, octet cu octet, cu următorii octeți codificați hexagonal: 300d06092a864886f70d0101010500.

Pentru ECDSA, se vor utiliza identificatorii și codificările specificate în #7.1.3.2 din CABF BR.

### Profilul certificatului CA subordonat

Toate denumirile subiecților sunt codificate conform specificațiilor din secțiunea 7.1.4 și conțin AttributeTypes conform #7.1.2.10.2 "CA Certificate Naming" din CABF BR.

Profilul câmpurilor de bază pentru certificatele certSIGN Web CA este descris în Tabelul 7.1.

| Numele câmpului                                      | Valoarea sau restricțiile valorii                    |                     |
|--|--|---------------------|
| <b>Versiune</b>                                      | 3  |                     |
| <b>Serie</b>   | 10034b8e66f50920f6c5                                 |                     |
| <b>Algoritm de semnare</b>                           | sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) |                     |
| <b>Emitent (Nume distinctiv)</b>                     | Department (OU) =                                    | certSIGN ROOT CA G2 |
|  | Organization (O) =                                   | certSIGN SA         |
|  | Country (C) =  | RO                  |
| <b>Nu înainte de (data de început a validității)</b> | Feb 6 10:18:16 2017 GMT                              |                     |
| <b>Nu după (data de sfârșit a validității)</b>       | Feb 6 10:18:16 2027 GMT                              |                     |
| <b>Subiect (Nume distinctiv)</b>                     | OrganizationIdentifier (OID: 2.5.4.97) =             | VATRO-18288250      |
|  | Common Name (CN) =                                   | certSIGN Web CA     |
|  | Organization (O) =                                   | certSIGN SA         |
|  | Country (C) =  | RO                  |

|  |  |
|--|--|
| <b>Informații despre cheia publică a subiectului</b> | 4096 bits RSA key                                    |
| <b>Semnătura</b>                                     | sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) |

Tabelul 7.1. Profilul câmpurilor de bază al certSIGN Web CA

### Profilul certificatului de end-user (server)

Câmpul notBefore are o valoare în termen de max 48 de ore de la operațiunea de semnare a certificatului.

Toate denumirile subiecților sunt codificate în conformitate cu CABF BR secțiunea 7.1.4 și conțin AttributeTypes conform #7.1.2.7.2 "Domain Validated".

Atributul "Subscriber Certificate Common Name" conține exact o intrare care este una dintre valorile conținute în extensia subjectAltName a certificatului, codificată ca o copie caracter cu caracter a valorii intrării dNSName din extensia subjectAltName. În mod specific, toate etichetele de domeniu ale porțiunii Fully-Qualified Domain Name sau FQDN din Wildcard Domain Name vor fi codificate ca etichete LDH, iar etichetele P NU vor fi convertite în reprezentarea lor Unicode.

Profilul câmpurilor de bază pentru certificatele end-user DV emise de certSIGN Web CA este descris în Tabelul 7.2.

| Numele câmpului                                      | Valoarea sau restricțiile valorii   |                 |
|--|---|-----------------|
| <b>Versiune</b>                                      | Version 3   |                 |
| <b>Serie</b>   | Valoare unică mai mare decât zero (0) pentru toate certificatele emise de autoritățile de certificare din cadrul certSIGN. Seriele sunt construite folosind un prefix incremental unic constrâns în baza de date care este concatenat cu o secvență aleatorie de 8 octeți. Un modul criptografic hardware este utilizat pentru generarea valorii aleatorii. |                 |
| <b>Algoritm de semnare</b>                           | sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)  |                 |
| <b>Emitent (Nume distinctiv)</b>                     | OrganizationIdentifier (OID: 2.5.4.97) =  | VATRO-18288250  |
|  | Common Name (CN) =  | certSIGN Web CA |
|  | Organization (O) =  | certSIGN SA     |
|  | Country (C) =   | RO              |
| <b>Nu înainte de (data de început a validității)</b> | Timpul Universal Coordonat  |                 |
| <b>Nu după (data de sfârșit a validității)</b>       | Timpul Universal Coordonat  |                 |
| <b>Subiect (Nume distinctiv)</b>                     | Codificate în conformitate cu RFC 5280, pot conține câmpurile countryName & commonName prezentate în capitolul 7.1.4.   |                 |
| <b>Informații despre cheia publică a subiectului</b> | 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).   |                 |
| <b>Semnătură</b>                                     | Semnătura certificatului, generată și codificată în conformitate cu   |                 |

| Numele câmpului | Valoarea sau restricțiile valorii |
|-----------------|-----------------------------------|
|                 | cerințele descrise în RFC 5280.   |

Tabelul 7.2. Profilul câmpurilor de bază ale certificatelor DV emise de certSIGN Web CA

### Profilul de precertificat

Un precertificat este identic din punct de vedere structural cu un certificat de server pentru utilizatorul final, cu excepția unei extensii speciale de „otrăvire” critică în câmpul extensions, cu OID-ul 1.3.6.1.4.1.11129.2.4.3, și este creat după ce CA-ul a decis să emită un certificat, dar înainte de semnarea efectivă a certificatului.

Câmpurile de bază ale precertificatului:

- **version** codificată este identică, octet cu octet, cu câmpul "versiune" din certificat.
- **serialNumber** codificată este identică, octet cu octet, cu câmpul serialNumber din certificat (ca o excepție de la RFC 5280, secțiunea 4.1.2.2).
- **signature** codificată este identică, octet cu octet, cu câmpul de semnătură din certificat.
- **issuer** codificată este identică, octet cu octet, cu câmpul issuer din certificat.
- **validity** codificată este identică, octet cu octet, cu câmpul validity al certificatului.
- **subject** codificată este identică, octet cu octet, cu câmpul "subject" al certificatului.
- **subjectPublicKeyInfo** codificată este identică, octet cu octet, cu câmpul subjectPublicKeyInfo din certificat.
- **issuerUniqueID** Encoded value este identic octet cu octet cu câmpul issuerUniqueID din certificat sau este omis dacă este omis în certificat.
- **subjectUniqueID** codificată este identică octet cu octet la octet cu câmpul subjectUniqueID din certificat sau este omisă dacă este omisă în certificat.

| Field name                          | Value or value's constraint for Precertificates   |
|-------------------------------------|---|
| <b>Version</b>                      | Version 3   |
| <b>Serial Number</b>                | Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value. |
| <b>Signature Algorithm</b>          | sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)  |
| <b>Issuer (Distinguished Name)</b>  | Common Name (CN) = certSIGN Web CA  |
|                                     | OrganisationIdentifier = VATRO-18288250   |
|                                     | Organization (O) = certSIGN SA  |
|                                     | Country (C) = RO  |
| <b>Not before</b>                   | Universal Time Coordinated based.   |
| <b>Not after</b>                    | Universal Time Coordinated based.   |
| <b>Subject (Distinguished Name)</b> | Encoded in accordance with RFC 5280, contains countryName and commonName fields.  |
| <b>Subject Public Key Info</b>      | Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).  |
| <b>Signature</b>                    | Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.   |

### Profilul de certificat OCSP Responder

certSIGN S.A.

Cod fiscal **RO18288250**, Registrul Comerțului: **J2006000484402**, EUID: **ROONRC.J2006000484402**, Capital social: **2.130.120,00 LEI**

Sediul social: Șoseaua Olteniței Nr. 107A, Corp C1, Etaj 1, Camera 16, Sector 4, București

Telefon: +40 31 101 18 70, Fax: +40 21 311 99 05, E-mail: office@certsign.ro

ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10: RINA SIMTEX-RENAR

ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-850322: IQNET ISO 20000-1-ITSMS-31/13: ACCREDIA

CA emitentă a respondentului este aceeași cu CA emitentă pentru certificatele pentru care furnizează răspunsuri.

| Field name                          | Value or value's constraint for OCSP Responder  |
|-------------------------------------|---|
| <b>Version</b>                      | Version 3   |
| <b>Serial Number</b>                | Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value. |
| <b>Signature Algorithm</b>          | sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)  |
| <b>Issuer (Distinguished Name)</b>  | Common Name (CN) = certSIGN Web CA  |
|                                     | OrganizationIdentifier = VATRO-18288250   |
|                                     | Organization (O) = certSIGN SA  |
|                                     | Country (C) = RO  |
| <b>Not before</b>                   | Universal Time Coordinated based.   |
| <b>Not after</b>                    | Universal Time Coordinated based.   |
| <b>Subject (Distinguished Name)</b> | Encoded in accordance with RFC 5280, contains countryName and commonName fields.  |
| <b>Subject Public Key Info</b>      | Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).  |
| <b>Signature</b>                    | Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.   |

### 7.1.1 Numerele de versiune

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

### 7.1.2 Extensii de certificate

Extensiile profilelor de certificat sunt în conformitate cu CABF BR nr. 7.1.2 "Certificate Content and Extensions".

#### Extensii ale profilului de certificat de CA subordonat

**AuthorityInfoAccess** conține una sau mai multe AccessDescriptions. Fiecare AccessDescription conține doar o AccessMethod permisă, iar fiecare AccessLocation este codificată ca tip GeneralName specificat.

Extensia **Authority Key Identifier** conține doar câmpul keyIdentifier, identic cu câmpul subjectKeyIdentifier al autorității de certificare emitente.

CA Certificate **Basic Constraints**: cA set TRUE; pathLenConstraint setat la 0 sau NULL.

Extensia **Certificate Policies** conține cel puțin o "PolicyInformation", care conține exact un identificator rezervat al politicii de certificat - pentru certificatele CA emise după 2023.

Extensia **CRL Distribution Points** conține cel puțin un DistributionPoint, de tip uniformResourceIdentifier, iar schema fiecăruia este "http". Primul GeneralName conține URL-ul HTTP al serviciului CRL al CA emitente pentru certificatul CA.

certSIGN CA generează un **subjectKeyIdentifier** care este unic în cadrul tuturor certificatelor pe care le-a emis pentru fiecare cheie publică unică.

Pentru certificatele CA emise după 2023 - CA Certificate **Extended Key Usage** conține id-kp-serverAuth key și, opțional, id-kp-clientAuth.

Extensiile certificatelor pentru certSIGN Web CA sunt descrise în Tabelul 7.3

| Extensie                                 | Valoarea sau restricțiile valorii  | Stare extensie |
|--|--|----------------|
| <b>Date de acces ale Autorității</b>     | [1]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.certsign.ro<br>[2]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://www.certsign.ro/certcrl/certsign-rootg2.crt | Non-critică    |
| <b>Constrângeri de bază</b>              | Subject type=CA, Path length constraint=0  | Critică        |
| <b>Utilizarea cheii</b>                  | keyCertSign (bit 5), cRLSign (bit 6)   | Critică        |
| <b>Identificatorul cheii autorității</b> | 82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03  | Non-critică    |
| <b>Identificatorul cheii subiectului</b> | 65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41  | Non-critică    |
| <b>Politici de certificare</b>           | Certificate Policies<br>[1]Certificate Policy:<br>Policy Identifier=All issuance policies <sup>2</sup><br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br><a href="http://www.certsign.ro/repository">http://www.certsign.ro/repository</a>  | Non-critică    |
| <b>Puncte de distribuție CLR</b>         | <a href="http://crl.certsign.ro/certsign-rootg2.crl">http://crl.certsign.ro/certsign-rootg2.crl</a>  | Non-critică    |
| <b>Extended Key Usage<sup>3</sup></b>    | Server Authentication (1.3.6.1.5.5.7.3.1)  | Non-critică    |

Tabelul 7.3. Extensii ale certSIGN Web CA certificate

### Extensii ale profilului de certificat de end-user (server)

**AuthorityInfoAccess** conține una sau mai multe AccessDescriptions. Fiecare AccessDescription conține doar o AccessMethod permisă, iar fiecare AccessLocation este codificată ca fiind de tipul GeneralName specificat.

Extinderea **Authority Key Identifier** conține doar câmpul keyIdentifier, identic cu câmpul subjectKeyIdentifier al CA emitente.

Extensia **Certificate Policies** conține cel puțin un "PolicyInformation" și conține exact un singur identificator de politică de certificat rezervat:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)}**(2.23.140.1.2.1)**

<sup>2</sup> certSIGN va înlocui certificatul actual de Web CA cu unul nou care poate avea Policy Identifier: 2.23.140.1.2.1

<sup>3</sup> Pentru CA-urile Intermediare noi, dedicate emiterii de certificate TLS aceasta extensie va fi adaugata

The permitted **policyQualifiers**, id-qt-cps (OID: 1.3.6.1.5.5.7.2.1), URL HTTP sau HTTPS pentru declarația privind practicile de certificare a autorității de certificare emitente.

End-user DV Certificate **Extended Key Usage** conține cheia id-kp-serverAuth și, opțional, id-kp-clientAuth.

**Subject Alternative Name** este prezent și conține cel puțin un dNSName. dNSName conține fie un nume de domeniu complet calificat, fie un nume de domeniu cu caractere wildcard pe care CA l-a validat în conformitate cu secțiunea 3.2.2.4 din CABF BR. Numele de domeniu wildcard sunt validate în conformitate cu secțiunea 3.2.2.2.6 din CABF BR. Intrarea dNSName nu conține un nume intern. Numele de domeniu complet calificat sau porțiunea FQDN a numelui de domeniu wildcard conținută în intrare este compusă în întregime din etichete P sau etichete LDH nerezervate, unite între ele printr-un caracter U+002E FULL STOP ("."). Eticheta de domeniu de lungime zero care reprezintă zona rădăcină a sistemului de nume de domeniu Internet NU este inclusă.

Valori de utilizare a cheilor (**Key Usage**): digitalSignature și keyEncipherment.

Extensia **CRL Distribution Points** conține cel puțin un DistributionPoint, de tip uniformResourceIdentifier, iar schema fiecăruia este "http". Primul GeneralName conține URL-ul HTTP al serviciului CRL al CA emitente pentru certificatul CA.

Certificatul end-user SSL DV conține extensiile descrise în Tabelul 7.4.

| Extensie                                 | Valoarea sau restricțiile valorii   | Stare extensie |
|--|---|----------------|
| <b>Date de acces ale Autorității</b>     | [1]Authority Info Access<br>Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)<br>Alternative Name:<br>URL=http://ocsp.certsign.ro<br>[2]Authority Info Access<br>Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)<br>Alternative Name:<br>URL=http://www.certsign.ro/certcrl/certsign-webca.crt | Non-critică    |
| <b>Constrângeri de bază</b>              | digitalSignature (bit 0), Key Encipherment (bit 2)  | Critică        |
| <b>Identificatorul cheii autorității</b> | 65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41   | Non-critică    |
| <b>Identificatorul cheii subiectului</b> | 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 neutilizati).  | Non-critică    |
| <b>Politici de certificare</b>           | Certificate Policies<br>[1]Certificate Policy:<br>Policy Identifier=2.23.140.1.2.1<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br><a href="http://www.certsign.ro/repository">http://www.certsign.ro/repository</a><br>[2]Certificate Policy:   | Non-critică    |

| Extensie                                | Valoarea sau restricțiile valorii   | Stare extensie |
|---|---|----------------|
|   | Policy Identifier=0.4.0.2042.1.6<br>[2,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br><a href="http://www.certsign.ro/repository">http://www.certsign.ro/repository</a><br>[3]Certificate Policy:<br>Policy Identifier=1.3.6.1.4.1.25017.3.1.4.5<br>[3,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br><a href="http://www.certsign.ro/repository">http://www.certsign.ro/repository</a> |                |
| <b>Puncte de distribuție CLR</b>        | <a href="http://crl.certsign.ro/certsign-webca.crl">http://crl.certsign.ro/certsign-webca.crl</a>   | Non-critică    |
| <b>Nume alternative ale Subiectului</b> | Această extensie conține cel puțin o intrare. Fiecare intrare este un Nume DNS conținând Numele de Domeniu Fully-Qualified<br>FQDN-uri Wildcard sunt permise.   | Non-critică    |
| <b>Utilizare sporită a cheii</b>        | Server Authentication (1.3.6.1.5.5.7.3.1)<br>Client Authentication (1.3.6.1.5.5.7.3.2)  | Non-critică    |

Tabelul 7.4. Extensii certificat SSL DV

### Extensiile profilului de precertificat

Precertificatul conține extensia "Precertificate Poison" (OID:1.3.6.1.4.1.11129.2.4.3). Această extensie are o valoare OCTET STRING care este exact octetul 0500, reprezentarea codificată a valorii ASN.1 NULL, astfel cum este specificată în RFC 6962, secțiunea 3.1.

### Extensii ale profilului de certificat OCSP Responder

Extensia Authority Key Identifier are doar câmpul keyIdentifier, identic cu câmpul subjectKeyIdentifier al autorității de certificare emitente.

OCSP Responder Extended Key Usage este doar OCSP Signing (1.3.6.1.5.5.5.7.3.9).

certSIGN include extensia id-pkix-ocsp-nocheck (OID: 1.3.6.1.5.5.5.7.7.48.1.5).

Această extensie are un extnValue OCTET STRING care este exact octetul 0500 codificat hexagonal, reprezentarea codificată a valorii NULL ASN.1, astfel cum este specificat în RFC 6960, secțiunea 4.2.2.2.2.1.

OCSP Responder Key Usage este doar digitalSignature.

subjectAltName, authorityInformationAccess, certificatePolicies, crlDistributionPoints nu sunt stabilite ca extensii pentru certificatele OCSP emise după 2023.

Certificatul OCSP conține extensiile descrise în Tabelul 7.5.

| Extensie                     | Valoarea sau restricțiile valorii                           | Stare extensie |
|------------------------------|---|----------------|
| <b>Utilizarea cheii</b>      | digitalSignature (bit 0)                                    | Critică        |
| <b>Identificatorul cheii</b> | 65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41 | Non-critică    |

| Extensie                                 | Valoarea sau restricțiile valorii                           | Stare extensie |
|--|---|----------------|
| <b>Autorității</b>                       |   |                |
| <b>Identificatorul cheii Subiectului</b> | 3c 76 7c 4a 3c 2d 6c 5a 82 c0 2d 62 f9 2e 17 89 e5 55 f0 b6 | Non-critică    |
| <b>Utilizare extinsă a cheii</b>         | OCSP Signing (1.3.6.1.5.5.7.3.9)                            | Non-critică    |
| <b>OCSPNoCheck</b>                       | -   | Non-critică    |

Tabelul 7.5. Extensii certificat OCSP

### 7.1.3 Obiect de identificare a algoritmului

#### SubjectPublicKeyInfo

Câmpul SubjectPublicKeyInfo indică o cheie RSA folosind identificatorul de algoritm rsaEncryption (OID: 1.2.840.113549.1.1.1.1), cu un parametru NULL explicit.

AlgorithmIdentifier pentru cheile RSA este identic, octet cu octet, cu următorii octeți codificați hexagonal: 300d06092a864886f70d0101010500.

Pentru ECDSA, se vor utiliza identificatorii și codificările specificate în #7.1.3.1.1.2 din CABF BR.

#### Identificatorul algoritmului de semnătură

Toate obiectele TLS semnate de o cheie privată certSIGN CA sunt conforme cu cerințele din CABF BR #7.1.3.2, RSA sau ECDSA privind utilizarea AlgorithmIdentifier sau a tipului AlgorithmIdentifier-derivat în contextul semnăturilor. În cazul certSIGN, algoritmul utilizat este sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.1.11).

### 7.1.4 Formate de nume

#### Codificarea numelui

Conținutul câmpurilor din certificatele DV respectă cerințele din secțiunea 3.1 și ale actualei Politici de Certificare 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 metadata precum ‘.’, ‘-’, și ‘ ’ (adică spațiu) pentru a indica faptul că valoarea nu există, este incompletă, sau nu este aplicabilă.

Pentru fiecare cale de certificare validă (conform definiției din RFC 5280, secțiunea 6):

- Pentru fiecare certificat din calea de certificare, conținutul codificat al câmpului Issuer Distinguished Name al unui certificat este identic, octet cu octet, cu forma codificată a câmpului Subject Distinguished Name al certificatului CA emitent.
- Pentru fiecare certificat TLS CA din calea de certificare, conținutul codificat al câmpului Subject Distinguished Name al unui certificat este identic octet cu octet între toate certificatele ale căror Subject Distinguished Names pot fi comparate ca fiind egale în conformitate cu RFC 5280, secțiunea 7.1, inclusiv certificatele expirate și revocate.

#### Codificarea TLS Subject

Atributele din câmpul subiect al certificatului vor fi codificate și poziționate în conformitate cu tabelul 77: "Cerințe de codificare și ordine pentru atributele selectate" din secțiunea 7.1.4.2 Codificarea atributelor subiectului din CABF BR.

### Atributul "Subscriber TLS Certificate Common Name"

Acest atribut conține exact o intrare care reprezintă una dintre valorile conținute în extensia subjectAltName a certificatului.

În cazul în care valoarea este un nume de domeniu complet calificat sau un nume de domeniu wildcard, atunci valoarea este codificată ca o copie, caracter cu caracter, a valorii intrării dNSName din extensia subjectAltName. Mai exact, toate etichetele de domeniu ale unui domeniu complet calificat (Fully-Qualified Domain Labels) Name sau FQDN din partea Wildcard Domain Name trebuie să fie codificate ca etichete LDH, iar etichetele P NU vor fi convertite în reprezentarea lor Unicode.

#### 7.1.5 Constrângeri privind numele

Nu este stipulat.

#### 7.1.6 Identificatorul obiectului politicii de certificare

Identificatorii de obiect ai politicii de certificare utilizați la nivelul de certSIGN Web CA sunt descriși în Tabelul 7.6 și Tabelul 7.7.

| Numele Politicii de Certificare | Identificatorul politicii  |
|---------------------------------|--|
| <b>certSIGN Web CA</b>          | <p><b><i>{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) domain-validated(1)} (2.23.140.1.2.1)</i></b></p> <p><b><i>{certSIGN} .{id-policy}(3). {id-cp}(1).{id-Web-CA}(4) . subpolicy ID=1.3.6.1.4.1.25017.3.1.4. subpolicy ID</i></b><br/>See below table for <i>subpolicyID</i> values.</p> <p><b><i>itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6)(0.4.0.2042.1.6)</i></b></p> |

Tabelul 7.6. Identificatori ai politicilor și numele lor pentru certificatele SSL DV

| Nivel CA   | OID   |
|--|---|
| <b>certSIGN Web CA</b><br><b>1.3.6.1.4.1.25017.3.1.4</b> | <i>DV certificate for website authentication - .5</i><br><i>OCSP certificate - .3</i> |

Tabelul 7.7 Identificatorii obiectului politicii de certificare

### 7.1.7 Utilizarea extensiei Constrângerii de politică

Nu este stipulat.

### 7.1.8 Sintaxa și semantica atributelor de politică

certSIGN emite certificate care conțin un atribut de politică în cadrul extensiei politicii de certificate. Această extensie conține un atribut pointer care indică către CPP.

### 7.1.9 Semantica de procesare pentru extensia Politici critice de certificare

Nu este stipulat.

## 7.2 Profilul CRL

certSIGN CA utilizează o CRL completă și integrală, adică o CRL a cărei sferă de aplicare include toate certificatele emise de CA.

Câmpul **nextUpdate** indică data până la care va fi emisă următoarea CRL. Pentru CRL-urile care acoperă certificatele de abonat, cel mult 10 zile după **thisUpdate**. Pentru celelalte CRL, la cel mult 12 luni de la thisUpdate.

Câmpul **revokedCertificates** este prezent dacă CA a emis un certificat care a fost revocat și dacă intrarea corespunzătoare nu a apărut încă în cel puțin o CRL programată în mod regulat după perioada de valabilitate a certificatului revocat. CA va elimina o intrare pentru un certificat corespunzător după ce acesta a apărut în cel puțin o CRL programată periodic după perioada de valabilitate a certificatului revocat.

Profilul CRL este descris în Tabelul 7.8.

| Numele câmpului             | Valoarea sau restricțiile valorii                    |                 |
|-----------------------------|--|-----------------|
| <b>Version</b>              | V2   |                 |
| <b>Signature Algorithm</b>  | sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) |                 |
| <b>Issuer</b>               | OrganizationIdentifier (OID: 2.5.4.97) =             | VATRO-18288250  |
|                             | Common Name (CN) =                                   | certSIGN Web CA |
|                             | Organization (O) =                                   | certSIGN SA     |
|                             | Country (C) =  | RO              |
| <b>ThisUpdate</b>           | Date of CRL issuance                                 |                 |
| <b>NextUpdate</b>           | Date of next expected CRL update                     |                 |
| <b>Revoked Certificates</b> | List of revoked certificates                         |                 |

Tabel 7.8 Profilul CRL pentru certSIGN Web CA

### 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

Extensia **CRLNumber** conține un număr INTEGER mai mare sau egal cu zero (0) și mai mic de  $2^{159}$  și transmite o secvență strict crescătoare.

Extensiile CRL pentru certSIGN Web CA sunt descrise în Tabelul 7.9.

| Extensie                               | Valoarea sau restricțiile valorii                           | Stare extensie |
|--|---|----------------|
| <b>Authority Identifier</b> <b>Key</b> | 65 29 2b 19 2b 5a 41 d3 01 62 9b 7b 47 00 e2 18 08 71 c3 41 | Non-critică    |
| <b>CRL Number</b>                      | monotonically increasing sequence number                    | Non-critică    |
| <b>ExpiredCertsOnCRL</b>               | Generalized Time  | Non-critică    |

Tabel 7.9. Extensii CRL pentru certSIGN Web CA

**serialNumber** este identic, octet cu octet, cu serialNumber conținut în certificatul revocat.

**revocationDate** este data și ora la care a avut loc revocarea.

CA actualizează data revocării într-o intrare CRL atunci când se stabilește că cheia privată a certificatului a fost compromisă înainte de data revocării care este indicată în intrarea CRL pentru certificatul respectiv. Data inversă a câmpului revocationDate reprezintă o excepție de la cele mai bune practici descrise în RFC 5280 (secțiunea 5.3.2); câmpul revocationDate sprijină implementările TLS care procesează câmpul revocationDate ca fiind data la care certificatul este considerat pentru prima dată ca fiind compromis.

| Extension                 | Value or Value constraint                        | Extension status |
|---------------------------|--|------------------|
| <b>serialNumber</b>       | serialNumber of the revoked certificate          | Non-critical     |
| <b>revocationDate</b>     | date of the certificate compromission/revocation | Non-critical     |
| <b>crlEntryExtensions</b> | reason for revocation                            | Non-critical     |
| <b>CRL Reason</b>         | Revocation reason code                           | Non-critical     |

Extensiile de intrare CRL (crlEntryExtensions) acceptate de certSIGN conțin următoarele câmpuri: **ReasonCode**: codul motivului revocării. Acest câmp nu este critic, permițând determinarea motivului revocării certificatului. Sunt permise următoarele motive pentru revocarea certificatului:

1. Nici un motiv furnizat sau nespecificat (RFC 5280 CRLReason # 0)
  - În cazul în care codurile de motiv nu se aplică cererii de revocare, solicitantul NU TREBUIE să furnizeze un alt cod de motiv decât "nespecificat".
2. KeyCompromise (RFC 5280 CRLReason # 1)
  - Beneficiarul certificatului TREBUIE să aleagă motivul revocării "keyCompromise" atunci când are motive să creadă că cheia privată a certificatului său a fost compromisă, de exemplu, o persoană neautorizată a avut acces la cheia privată a certificatului său.
3. AffiliationChanged (RFC 5280 CRLReason # 3)
  - Beneficiarul certificatului ar trebui să aleagă motivul revocării "affiliationChanged" atunci când numele subiectului sau alte informații privind identitatea subiectului din certificat s-au schimbat, dar nu există niciun motiv pentru a suspecta că cheia privată a certificatului a fost compromisă.
4. Superseded (RFC 5280 CRLReason # 4)
  - Beneficiarul certificatului ar trebui să aleagă motivul revocării "superseded" atunci când certificatul este înlocuit deoarece: abonatul a solicitat un nou certificat, CA are dovezi rezonabile că nu ar trebui să se bazeze pe validarea autorizării sau controlului domeniului pentru orice nume de domeniu complet calificat sau adresă IP din certificat, sau CA a revocat certificatul din motive de conformitate, cum ar fi faptul că certificatul nu este conform cu cerințele de bază sau cu CPS ale CA. ).
5. CessationOfOperation (RFC 5280 CRLReason # 5)

- Beneficiarul certificatului ar trebui să aleagă motivul revocării "cessationOfOperation" atunci când site-ul web certificat este închis înainte de expirarea certificatului sau dacă Beneficiarul nu mai deține sau nu mai controlează numele de domeniu din certificat înainte de expirarea certificatului..
6. `privilegeWithdrawn` (RFC 5280 CRLReason #9)<sup>4</sup>
- `PrivilegeWithdrawn` este destinat să fie utilizat atunci când a existat o infracțiune de partea abonatului care nu a dus la `keyCompromise`, cum ar fi abonatul certificatului a furnizat informații înșelătoare în cererea lor de certificat sau nu și-a respectat obligațiile materiale în temeiul acordului de abonat sau al termenilor de utilizare.

Contractul de abonat informează abonații cu privire la opțiunile privind motivele de revocare enumerate mai sus și oferă explicații cu privire la momentul în care trebuie aleasă fiecare opțiune. Modelele de cereri de revocare, pe care AC le pune la dispoziția abonatului, permit ca aceste opțiuni să fie ușor de specificat în momentul în care abonatul solicită revocarea certificatului său, valoarea implicită fiind aceea că nu este furnizat niciun motiv de revocare [adică valoarea implicită corespunde la CRLReason "unspecified (0)", ceea ce are ca rezultat faptul că nu este furnizată nicio extensie `reasonCode` în CRL].

### 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 Autorităților de Certificare afiliate. Serverul OCSP, care emite confirmări ale stării certificatelor, folosește o pereche specială de chei pentru fiecare CA Subordonat și Root CA, generată exclusiv pentru acest scop.

Certificatul serverului OCSP conține extensia `extKeyUsage`, descrisă în RFC 5280.

Această extensie este 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 (aparținând Beneficiarilor acestei autorități).

De asemenea, certificatul serverului OCSP conține extensia `OCSPNoCheck`, descrisă de RFC 6960. Această extensie este declarată ca fiind ne-critică și semnifică faptul că un client de OCSP care primește 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 primește o confirmare emisă de serverul OCSP trebuie să suporte formatul standard de răspuns având identificatorul **id-pkix-ocsp-basic**.

Informațiile 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 informații pentru determinarea stării certificatului respectiv

---

<sup>4</sup> *privilegeWithdrawn nu trebuie să fie pus la dispoziția abonatului ca o opțiune motiv de revocare, deoarece utilizarea acestui motiv este determinată de operatorul CA și nu de abonat*

Când răspunsul OCSP conține un cod de eroare (mesaj), răspunsul nu este semnat digital (RFC 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** – Legătura unei cereri și a unui răspuns pentru a preveni atacurile replay. **Nonce** este inclus în **requestExtension** al **OCSPRequest** și repetat în câmpul **responseExtension** al **OCSPResponse**.

## 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 CA ca furnizor de servicii de certificare și conformitatea serviciilor CA cu criteriile din Regulamentul 910/2014, al actelor de punere în aplicare și ale CA/B Forum Baseline Requirements, urmărind cerințele din standardul ETSI EN 319 401 și ESTI EN 319 411-1 și ne conformăm 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 prezentul CPP și cu standardele tehnice ETSI 319 401, ETSI 319 411 și CA/B Forum Baseline Requirements.

Auditurile la cerere pot fi realizate la discreția certSIGN, la cererea organismului de supraveghere, astfel cum este definit în Regulamentul UE 910/2014 și în CA/B Forum Baseline Requirements, 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 în specificațiile CA/B Forum Baseline Requirements.

### 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 includ referințe normative la ETSI EN 319 401.

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

- managementul configurației 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 identității Abonaților,
- serviciile de certificare și procedurile de furnizare a serviciilor,
- securitatea aplicațiilor software și a accesului la rețea,
- 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 aplicațiile 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 PPMP. certSIGN și organismul de evaluare a conformității analizează concomitent rezultatele raportului și aprobă un plan de corecție și un interval de timp pentru punerea în aplicare a acestuia.

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

### 8.6 Comunicarea rezultatelor

Organismul de Evaluare a Conformității comunică raportul de audit conducerii certSIGN și către PPMB.

Raportul de Audit va specifica în mod explicit faptul că acoperă sistemele și procesele relevante utilizate în emiterea tuturor certificatelor care impugnat identificatorii de politică declarati. CA pune Raportul de Audit la dispoziția publicului în cel mult trei luni de la încheierea perioadei de audit. 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 amprență digitală SHA-256 din raportul de audit va fi scrisă cu majuscule și nu va conține două puncte, spații sau linii.

### 8.7 Auditudini interne

certSIGN CA monitorizează respectarea cerințelor CPP și ale CA/B Forum Baseline Requirements și controlează strict calitatea serviciului prin efectuarea de auditudini interne trimestrial pe un eșantion selectat aleatoriu, un certificat sau cel puțin trei la sută din certificatele emise din perioada începând imediat după ce eșantionul auditului intern anterior a fost selectat.

certSIGN CA controlează strict calitatea serviciului de calitate a certificatelor emise sau care conțin informații verificate de o terță parte delegată, prin faptul că un specialist în validare sau un auditor intern angajat de certSIGN efectuează auditudini trimestriale continue în raport cu un eșantion selectat aleatoriu de cel puțin cel mai mare dintre un certificat sau trei procente din certificatele verificate de către terță parte delegată în perioada care începe imediat după

prelevarea ultimului eșantion. certSIGN utilizează un proces de lintage pentru a verifica acuratețea tehnică a certificatelor din setul de eșantioane selectate, independent de lintage anterior efectuat pe aceleași certificate.

certSIGN CA examinează practicile și procedurile fiecărei părți delegate pentru a se asigura că partea terță delegată respectă aceste cerințe și politica de certificare și/sau declarația privind practicile de certificare relevante.

certSIGN CA efectuează anual un audit intern cu fiecare parte terță delegată pentru verificarea conformității cu aceste cerințe.

## 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 prețuri disponibilă la adresa <http://www.certsign.ro>. Prețurile sunt formate conform politici interne de preț.

Serviciile oferite de certSIGN sunt stabilite după cum urmează:

- **Servicii de certificare individuale** – prețul 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** – prețul este stabilit pentru pachete de servicii prestate unei singure entități,
- **Servicii prestate pe baza de abonament** – prețul este stabilit pentru servicii prestate periodic; valoarea sumelor plătite depinde de tipul și numărul serviciilor accesate și este utilizat în special pentru serviciile de marcare temporală și de verificare a stării certificatelor prin intermediul protocoalelor OCSP,
- **Servicii indirecte** – prețul este stabilit pentru fiecare serviciu oferit clienților săi de un partener certSIGN, care își bazează activitatea pe infrastructura certSIGN.

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

#### 9.1.1 Tarifele serviciilor de emiterie 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 formate conform politicii interne de preț.

#### 9.1.4 Alte tarife

Prețurile sunt formate conform politicii interne de preț.

#### 9.1.5 Politica de rambursare

Plățile pot fi rambursate conform condițiilor contractuale aplicabile..

## 9.2 Răspunderea financiară

### 9.2.1 Acoperirea prin asigurare

certSIGN are încheiate polițe de asigurare profesionale și va acoperi daunele pe care le-ar putea provoca din cauza serviciilor de certificare pentru persoanele care își construiesc etica pe baza efectelor juridice ale certificatelor emise de certSIGN Web CA în limitele stabilite de prezentul CPP, acordurile contractuale încheiate, după caz.

### 9.2.2 Alte active

Nu este stipulat.

### 9.2.3 Asigurarea sau acoperirea garanției pentru entitățile finale

certSIGN beneficiază de asigurare care acoperă responsabilitățile profesionale.

## 9.3 Confidențialitatea informațiilor de afaceri

### 9.3.1 Scopul informațiilor confidențiale

Toate informațiile referitoare la Beneficiar/Entități Partener pe care le prelucrează certSIGN sunt obținute, păstrate și procesate în concordanță cu prevederile Regulamentului (UE) nr. 910/2014. Relațiile dintre un Beneficiar, o Entitate Parteneră și certSIGN se bazează pe încredere.

O terță parte poate avea acces doar la informațiile disponibile public în certificate. Celelalte date furnizate certSIGN nu vor fi dezvăluite în nicio circumstanță vreunei terțe părți, în mod voluntar (cu excepția situațiilor prevăzute de lege).

O parte va fi exonerată de răspunderea pentru dezvăluirea de informații confidențiale, dacă:

- a) informația era cunoscută părții contractante înainte ca ea să fi fost primită de la cealaltă parte contractantă; sau
- b) informația a fost dezvăluită după ce a fost obținut acordul scris al celeilalte părți; sau
- c) partea a fost obligată în mod legal să dezvăluie informația.

Dezvăluirea oricărei informații entităților implicate în îndeplinirea obligațiilor se va face confidențial și se va extinde doar asupra informațiilor necesare pentru îndeplinirea obligațiilor.

### Tipuri de informații considerate a fi confidențiale și private

certSIGN, angajații săi precum și entitățile care desfășoară activități de certificare sunt obligate să păstreze secretul informațiilor, atât pe durata, cât și după încetarea contractului de muncă, în cazul angajaților. Sunt catalogate drept informații private sau confidențiale:

- informațiile furnizate de Beneficiari, în plus față de informațiile care apar în certificate și în Depozitar; dezvăluirea acestor informații se face doar cu aprobare scrisă, în prealabil, din partea proprietarului informației sau în alte condiții prevăzute de lege;
- conținutul contractelor încheiate cu Beneficiarii sau Entitățile Partener, conturi bancare, aplicațiile de înregistrare, emitere, reînnoire, revocare certificate; aceste informații pot fi dezvăluite doar cu aprobarea și în scopul menționat de proprietarul informațiilor (de exemplu, Beneficiarul), cu excepția informațiilor incluse în certificate sau în Depozitar, conform prezentului CPP;
- înregistrările corespunzătoare tranzacțiilor din sistem (toate tipurile de tranzacții, precum și datele pentru controlul tranzacțiilor, așa numitele loguri ale tranzacțiilor din sistem);
- înregistrările corespunzătoare evenimentelor (log-uri) ce țin de serviciile de certificare, păstrate de certSIGN;
- rezultatele auditurilor externe vor fi făcute publice;
- planurile în caz de urgență;

- informațiile referitoare la măsurile luate pentru protecția dispozitivelor hardware și aplicațiilor software, informațiile 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 informațiilor confidențiale și răspund conform legislației în vigoare.*

### **Dezvăluirea motivului pentru care un certificat a fost revocat**

Dacă un certificat a fost revocat la cererea unei părți autorizate alta decât Beneficiarul, informațiile cu privire la revocare și motivele acestei revocări sunt comunicate ambelor părți.

### **Dezvăluirea Informațiilor Confidențiale Reprezentanților Autorităților Legale**

Informațiile confidențiale pot fi dezvăluite reprezentanților autorităților legale numai după îndeplinirea tuturor formalităților cerute de legislația în vigoare în România.

#### **9.3.2 Informații care nu sunt considerate a fi confidențiale**

Informațiile incluse într-un certificat de către Autoritățile de Certificare emitente, în conformitate cu specificațiile din Capitolul 7 nu sunt confidențiale. Un Beneficiar care aplică pentru obținerea unui certificat cunoaște ce fel de informații vor fi incluse în certificat și este de acord cu publicarea acestora.

Cu excepția informațiilor prevăzute la alineatul anterior, informațiile furnizate de către Beneficiar pot fi puse la dispoziția altor entități, doar cu acordul scris al Beneficiarului și în scopul menționat în contractul încheiat cu Beneficiarului.

#### **9.3.3 Responsibilitatea de a proteja informațiile confidențiale**

certSIGN și angajații săi, păstrează confidențialitatea informațiilor atât în timpul prestării serviciilor de certificare, cât și după încetarea valabilității certificatelor.

### **9.4 Confidențialitatea datelor cu caracter personal**

În prestarea serviciilor de încredere certSIGN prelucrează date cu caracter personal ale Beneficiarului în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea dispozițiilor de drept intern, a Regulamentului nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație 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 protecției 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, atunci când sunt schimbate între componentele sistemului certSIGN, precum și atunci când sunt depozitate.

#### **9.4.2 Informatii considerate ca fiind cu caracter personal**

certSIGN tratează toate informațiile despre Beneficiar care nu sunt disponibile public în conținutul certificatului sau în CRL, ca date private, cu caracter personal. .

#### **9.4.3 Informații care nu sunt considerate private**

Conținutul certificatelor digitale și informațiile accesibile prin Depozitar sunt informații publice.

#### **9.4.4 Responsabilitatea de a proteja informațiile private**

certSIGN se angajează să păstreze confidențialitatea datelor cu caracter personal atât în timpul prestării serviciilor de certificare, cât și după încetarea valabilității certificatelor. certSIGN nu va divulga informații cu caracter personal niciunui tert, pentru niciun motiv, cu excepția situațiilor în care va fi obligată să o facă prin lege sau standarde aplicabile sau de către autoritățile competente.

#### **9.4.5 Notificarea persoanelor vizate și consimțământul acestora pentru utilizarea datelor cu caracter personal**

În procesul de emitere a unui certificat digital persoanele desemnate de sau reprezentanții Beneficiarului sunt informați despre necesitatea utilizării datelor cu caracter personal care le aparțin, în vederea prestării serviciului. Dacă persoanele vizate nu sunt de acord ca certSIGN să le prelucreze date, certSIGN nu poate emite certificatele digitale.

De asemenea, 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 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 circumstanțe 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 Beneficiarului, în cazul în care acesta a optat pentru transmiterea certificatului la adresa de domiciliu sau la o altă adresă comunicată, cu respectarea aceluiași 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 Beneficiarului;
- ✓ în orice alte situații justificate cu înștiințarea în prealabil a Beneficiarului.

## 9.5 Drepturile de Proprietate Intelectuală

Toate mărcile, patentele, siglele, licențele, imaginile grafice etc. folosite de certSIGN sunt și vor rămâne proprietatea intelectuală a deținătorilor legali ai acestora. certSIGN se obligă să specifice acest lucru conform cerințelor impuse de deținători.

Toate mărcile, patentele, siglele, licențele, imaginile grafice etc., aparținând certSIGN sunt și rămân proprietatea acesteia, indiferent dacă sunt însoțite sau nu de patente, modele de utilitate, copyright sau altele asemenea și nu pot fi reproduse sau furnizate unei terțe părți fără acordul prealabil în scris al certSIGN.

## 9.6 Reprezentări și garanții

### 9.6.1 Reprezentările și garanțiile CA

Prin emiterea unui certificat, certSIGN oferă următoarele garanții de certificare către:

1. Beneficiar, care este parte a unui acord contractual și a unor Termeni și condiții pentru Certificat;
1. Toți Furnizorii de aplicații software cu care CERTSGIN a intrat într-un contract de includere a certificatului CA în aplicațiile distribuite de astfel de furnizori; și
2. Toate entitățile partenere care se bazează pe un certificate valid.

certSIGN reprezintă și garantează Beneficiarilor și entităților partenere că, pe toate perioade de valabilitate a certificatului, certSIGN a respectat cerințele acestui CPP în emiterea și administrarea certificatului.

Garanțiile Certificatului le includ în mod specific pe cele menționate în ultima versiune publicată a CA/B Forum Baseline Requirements, paragraful 9.6.1.

### 9.6.2 Reprezentările și garanțiile RA

RA are obligația de a respecta cu strictețe CPP, secțiunea relevantă din CP aplicabil, precum și procedurile interne relevante ale certSIGN.

### 9.6.3 Reprezentările și garanțiile Beneficiarului

Beneficiarul acceptă acordul contractual și Termenii și Condițiile relevante pentru serviciul furnizat de certSIGN.

Beneficiarul este de acord cu CPP-ul și cu responsabilitățile, îndatoririle și obligațiile sale relevante, așa cum sunt prevăzute în secțiunile relevante ale CPP și ale CP-ului aplicabil.

Acordul Contractul conține prevederi ce impun Beneficiarului obligațiile și garanțiile din CA/B Forum Baseline Requirements, paragraful 9.6.3

#### 9.6.4 Reprezentările și garanțiile Entităților Partenere

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

- Realizarea cu succes a operațiunilor de chei publice, înainte de a se baza pe un Certificat certSIGN,
- Validarea unui Certificat certSIGN utilizând CRL-urile sau serviciile de validare a certificatelor furnizate de certSIGN,
- Încetarea imediată a oricărei utilizări a unui certificat certSIGN în cazul în care a fost revocat sau atunci când a expirat.
- Luarea la cunoștință a prevederilor prezentului CPP, a garanțiilor și limitelor răspunderii Certsign SA

#### 9.6.5 Reprezentările și garanțiile altor participanți

Nu este stipulat.

#### 9.7 Declinarea garanțiilor

Cu excepția celor prevăzute în mod expres în CPP, și în legislația aplicabilă, certSIGN nu își asuma nici o garanție și obligație 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 celor provenite dintr-o sursă autorizată) și nu își asumă nicio răspundere pentru neglijența și neatenția Subiecților, Beneficiarilor și Entităților Partenere.

#### 9.8 Limitarea răspunderii

În măsura permisă 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, de venit sau afaceri;
- Orice pierderi de date;
- Orice daune indirecte, subsecvente sau punitive ce decurg din sau în legătură cu utilizarea, livrarea, licența, și performanța sau non-performanța certificatelor sau a semnăturilor electronice;
- Orice alte daune.

[certSIGN nu răspunde față de nicio o persoană \(beneficiar, subiect, tert, entitate parteneră etc.\) în cazul în care datele prezentate la emiterea certificatelor sunt false, inexacte, incomplete sau expirate. certSIGN nu răspunde pentru daunele suportate de Beneficiar sau terți provocate de utilizarea de către Beneficiar a certificatelor emise de CERTSIGN.](#)

Fără a aduce atingere celor de mai sus, dacă certSIGN nu a emis sau gestionat certificatul în conformitate cu cerințele CAB Forum Baseline Requirements și cu politica de certificare, certSIGN acoperă orice daune directe aduse Beneficiarilor sau partilor care se bazează pe certificate pentru o creanță recunoscută și probată, limitată la o sumă egală cu valoarea certificatului, per Beneficiar sau Entitate Parteneră per certificat DV SSL.

## 9.9 Despăgubiri

certSIGN nu își asumă nicio responsabilitate financiară pentru Certificatele, CRL-urile și serviciile asociate specificate în acest CPP utilizate în mod necorespunzător.

certSIGN acționează conform prevederilor paragrafului "9.9 Indemnification by CAs" din CA/B Forum Baseline Requirements.

certSIGN raspunde si despagubeste doar in limitele aratate mai sus.

## 9.10 Termenii și încetarea

### 9.10.1 Termenii

Prezentul CPP și orice modificări ale acestuia vor intra în vigoare după publicare în Depozitar și în conformitate cu secțiunea 9.12.2 și vor rămâne în vigoare perpetuu până la încetarea lor în conformitate cu prezenta secțiune 9.10.

### 9.10.2 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 internațional, (iii) livrarea în mână sau (iv) 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 (PPMB) și Procedurilor, de aprobarea și modificarea prezentului CPP. CPP-se revizuieste cel puțin odata pe an.

Singurele modificări pe care le poate face PPMB 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.

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

Orice modificări la CPP sunt aprobate de PPMB și sunt anunțate clienților certSIGN. 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 PPMB vor fi diseminate părților interesate înainte 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**

certSIGN asigură accesul nerestricționat la serviciile furnizate pentru persoanele cu dizabilități în conformitate cu legislația și standardele în vigoare.

##### **9.16.1 Întregul Acord**

Nu este stipulat.

##### **9.16.2 Cesiunea**

Nu este stipulat.

##### **9.16.3 Anulabilitatea**

CA acționează conform prevederilor din paragraful "9.16.3 Severability" din CA/B Forum Baseline Requirements.

##### **9.16.4 Executarea (onorariile avocaților și renunțarea la drepturi)**

Nu este stipulat.

##### **9.16.5 Forța Majoră**

CA acționează conform legilor române cu privire la Forța Majoră.

#### **9.17 Alte prevederi**

Nu este stipulat.