

Codul de Practici și Proceduri certSIGN Public CA

Versiunea 2.31

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

Istoric document

Vers.	Data efectivă	Motiv	Responsabil
1.0	28 Februarie 2017	Publicarea primei versiuni	Ofițer securitate informatică
2.0	15 Martie 2017	A doua versiune, după interim audit	Ofițer securitate informatică
2.1	3 Aprilie 2017	Actualizare minoră, pentru clarificare	Ofițer securitate informatică
2.2	14 August 2017	Actualizare minoră pentru clarificarea utilizării extensiei ECU în certificatele utilizatorilor finali	Ofițer securitate informatică
2.3	5 Februarie 2018	Revizuire anuală	Ofițer securitate informatică
2.4	7 Mai 2018	Actualizare conform Forum CA/B, Cerința 1.5.6 a BaseLine respectiv GDPR	Manager politici PKI
2.5	25 Septembrie 2018	Clarificare cerinte referitoare la „Unicitatea numelui”	Manager politici PKI
2.6	1 Noiembrie 2018	Actualizare noi profile de certificate privind semnatura la distanta	Manager politici PKI
2.7	5 Noiembrie 2018	Actualizare determinata de schimbarea sediului	Manager politici PKI
2.8	14 Ianuarie 2019	Revizuire anuală	Manager politici PKI
2.9	18 Februarie 2019	Actualizare pentru adaugarea unei noi metode de identificare a persoanelor fizice	Manager politici PKI
2.10	8 Aprilie 2019	Actualizare minoră, pentru clarificare	Manager politici PKI
2.11	31 Ianuarie 2020	Actualizare minoră pentru clarificare (identificare cetățeni din afara RO) și Revizuire anuală	Manager politici PKI
2.12	7 Februarie 2020	Actualizare profil CRL	Manager politici PKI
2.13	9 Martie 2020	Actualizare minoră pentru utilizare chei private	Manager Politici PKI
2.14	31 Iulie 2020	Adăugare OID cu pseudonim	Manager Politici PKI
2.15	4 Septembrie 2020	Corectii minore text OID pseudonim	Manager Politici PKI
2.16	29 Ianuarie 2021	Revizie anuală	Manager Politici PKI
2.17	31 Ianuarie 2022	Revizie anuală	Manager Politici PKI
2.18	15 Martie 2022	Actualizare ECU in profil certificat	Manager Politici PKI
2.19	4 Octombrie 2022	Actualizare info neverificate & FR CN	Manager Politici PKI
2.20	31 Ianuarie 2023	Revizie anuală	Manager Politici PKI
2.21	16 Martie 2023	Actualizare ECU OIDS 3.1.2.1/2/3	Manager Politici PKI
2.22	31 Iulie 2022	Reduceri de OID-uri	Manager Politici PKI
2.23	31 August 2023	S/MIME updates	Manager Politici PKI
2.24	15 Decembrie 2023	.p12 updates	Manager Politici PKI
2.25	31 Ianuarie 2024	Revizie anuală	Manager Politici PKI
2.26	15 August 2024	Actualizare profil OCSP & altele	Manager Politici PKI
2.27	9 Octombrie 2024	Stergere OID Protectie email	Manager Politici PKI
2.28	15 Ianuarie 2025	Revizie anuală	Manager Politici PKI
2.29	30 Aprilie 2025	Actualizari minore	Manager Politici PKI
2.30	30 Octombrie 2025	Adaugare revocare in masa	Manager Politici PKI
2.31	15 Ianuarie 2026	Revizie anuală	Manager Politici PKI

Acest document a fost creat de către și este proprietatea:

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

Lista de distribuție

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

Acest document a fost aprobat de:

Versiune	Nume	Data
1.0	Comitet de Management al Politicilor și Procedurilor (CMPP)	Februarie 2017
2.0	Comitet de Management al Politicilor și Procedurilor (CMPP)	Martie 2017
2.1	Comitet de Management al Politicilor și Procedurilor (CMPP)	Aprilie 2017
2.2	Comitet de Management al Politicilor și Procedurilor (CMPP)	August 2017
2.3	Comitet de Management al Politicilor și Procedurilor (CMPP)	Februarie 2018
2.4	Comitet de Management al Politicilor și Procedurilor (CMPP)	Mai 2018

2.5	Comitet de Management al Politicilor și Procedurilor (CMPP)	Septembrie 2018
2.6	Comitet de Management al Politicilor și Procedurilor (CMPP)	Noiembrie 2018
2.7	Comitet de Management al Politicilor și Procedurilor (CMPP)	Noiembrie 2018
2.8	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2019
2.9	Comitet de Management al Politicilor și Procedurilor (CMPP)	Februarie 2019
2.10	Comitet de Management al Politicilor și Procedurilor (CMPP)	Aprilie 2019
2.11	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2020
2.12	Comitet de Management al Politicilor și Procedurilor (CMPP)	Februarie 2020
2.13	Comitet de Management al Politicilor și Procedurilor (CMPP)	Martie 2020
2.14	Comitet de Management al Politicilor și Procedurilor (CMPP)	Iulie 2020
2.15	Comitet de Management al Politicilor și Procedurilor (CMPP)	Septembrie 2020
2.16	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2021
2.17	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2022
2.18	Comitet de Management al Politicilor și Procedurilor (CMPP)	Martie 2022
2.19	Comitet de Management al Politicilor și Procedurilor (CMPP)	Octombrie 2022
2.20	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2023
2.21	Comitet de Management al Politicilor și Procedurilor (CMPP)	Martie 2023
2.22	Comitet de Management al Politicilor și Procedurilor (CMPP)	Iulie 2023
2.23	Comitet de Management al Politicilor și Procedurilor (CMPP)	August 2023
2.24	Comitet de Management al Politicilor și Procedurilor (CMPP)	Decembrie 2023
2.25	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2024
2.26	Comitet de Management al Politicilor și Procedurilor (CMPP)	August 2024
2.27	Comitet de Management al Politicilor și Procedurilor (CMPP)	Octombrie 2024
2.28	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2025
2.29	Comitet de Management al Politicilor și Procedurilor (CMPP)	Aprilie 2025
2.30	Comitet de Management al Politicilor și Procedurilor (CMPP)	Octombrie 2025
2.31	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2026

Content

1	Introducere	11
1.1	Descriere Generală	11
1.2	Denumirea documentului și identificarea	11
1.3	Participanții PKI	11
1.3.1	Autoritățile de Certificare	12
1.3.2	Autoritățile de Înregistrare	12
1.3.3	Beneficiarii	12
1.3.4	Entitățile Partenere	13
1.3.5	Alți participanți	13
1.4	Utilizarea certificatului	13
1.4.1	Utilizări admise ale certificatului	14
1.4.2	Utilizări interzise ale certificatului	14
1.5	Administrarea politicii	14
1.5.1	Organizația care administrează documentul	14
1.5.2	Persoana de contact	15
1.5.3	Persoana care decide conformitatea CPP cu politica	15
1.5.4	Procedurile de aprobare a CPP	15
1.6	Definiții și acronime	16
2	Publicare și responsabilități Depozitar	18
2.1	Depozitare	18
2.2	Publicarea informațiilor de certificare	18
2.3	Timpul sau frecvența publicării	19
2.4	Controlul accesului la Depozitare	19
3	Identificarea și autentificarea	19
3.1	Denumirea	19
3.1.1	Tipuri de nume	19
3.1.2	Nevoia ca Numele să aiba înțeles logic	20
3.1.3	Anonimitatea sau pseudonimitatea Beneficiarilor	21
3.1.4	Reguli de interpretare a diferitelor formate de nume	21
3.1.5	Unicitatea numelor	21
3.1.6	Recunoașterea, autentificarea și rolul mărcilor înregistrate	21
3.2	Validarea Inițială a Identității	21
3.2.1	Dovada Posesiei Cheii Private	22
3.2.2	Autentificarea identității organizației	22
3.2.3	Autentificarea identității persoanelor fizice	22
3.2.4	Informații neverificate cu privire la Beneficiar	23
3.2.5	Validarea autorității	23
3.2.6	Criterii pentru interoperare	23
3.3	Identificarea și autentificarea pentru cererile de re-key	23
3.3.1	Identificarea și autentificare pentru re-key de rutină	23
3.3.2	Identificarea și autentificarea pentru re-key după revocare	23
3.4	Identificarea și autentificarea pentru cererile de revocare	23
4	Cerințe operaționale privind ciclul de viață al certificatului	24
4.1	Cererea de certificat	24
4.1.1	Cine poate trimite o cerere de certificat	24

4.1.2	Procesul de înregistrare și responsabilitățile	25
4.2	Procesarea cererilor de certificate	26
4.2.1	Îndeplinirea funcțiilor de identificare și autentificare	26
4.2.2	Aprobarea sau respingerea cererilor de certificate	26
4.2.3	Timpul de procesare a cererilor de certificate	27
4.3	Emiterea certificatelor	27
4.3.1	Acțiunile CA în timpul emiterii certificatelor	27
4.3.2	Notificarea Subiectului de către CA cu privire la emiterea certificatului	27
4.4	Acceptarea certificatului	28
4.4.1	Conduita care constituie acceptarea certificatului	28
4.4.2	Publicarea certificatului de către CA	28
4.4.3	Notificarea de către CA a altor entități cu privire la emiterea certificatului ...	28
4.5	Utilizarea perechii de chei și a certificatului	28
4.5.1	Utilizarea cheii private și a certificatului	28
4.5.2	Utilizarea cheii publice și a certificatului unei Entități Partenere	29
4.6	Reinnoirea certificatului	30
4.7	Rekey-ul certificatului	30
4.7.1	Circumstanțe pentru rekey-ul certificatului	30
4.7.2	Cine poate solicita certificarea unei noi chei publice	30
4.7.3	Procesarea cererilor de re-key a certificatelor	31
4.7.4	Notificarea emiterii noului certificat către beneficiar	31
4.7.5	Conduita ce constituie acceptarea unui certificate re-key	31
4.7.6	Publicarea certificatului re-key de către CA	31
4.7.7	Notificarea eliberării certificatului de către CA altor entități	31
4.8	Modificarea Certificatului	31
4.9	Revocarea și Suspendarea Certificatului	31
4.9.1	Circumstanțele revocării unui certificat	31
4.9.2	Cine poate solicita revocarea certificatelor	32
4.9.3	Procedura de revocare a certificatelor	32
4.9.4	Perioada de grație a cererii de revocare	33
4.9.5	Timpul în care CA trebuie să proceseze cererea de revocare	33
4.9.6	Verificarea cerințelor de revocare pentru Entitățile Partenere	33
4.9.7	Frecvența de emitere a CRL-urilor	33
4.9.8	Latența maximă pentru CRL-uri	33
4.9.9	Disponibilitatea verificării on-line a revocării/stării	33
4.9.10	Verificarea on-line a cerințelor de revocare	33
4.9.11	Alte forme disponibile pentru anunțarea revocării	33
4.9.12	Cerințe speciale în cazul compromiterii re key	34
4.9.13	Circumstanțe pentru suspendare	34
4.9.14	Cine poate solicita suspendarea	34
4.9.15	Procedura de solicitare a suspendării	34
4.9.16	Limitări ale perioadei de suspendare	34
4.10	Servicii privind starea certificatelor	34
4.10.1	Caracteristici operaționale	34
4.10.2	Disponibilitatea serviciului	34
4.10.3	Elemente opționale	34
4.11	Încetarea acordului contractual	34
4.12	Custodie și recuperare chei	34

4.12.1	Principalele politici și practici în materie de depozit escrow și recuperare	35
4.12.2	Politica și practicile de încapsulare și recuperare a cheii de sesiune	35
5	Locație, Management și Controale Operaționale	36
5.1	Controale fizice	36
5.1.1	Amplasarea și construcția sediului	36
5.1.2	Accesul fizic	37
5.1.3	Alimentarea cu curent și aerul condiționat	37
5.1.4	Expunerea la apă.....	38
5.1.5	Prevenirea și protecția împotriva incendiilor	38
5.1.6	Depozitarea mediilor de stocare a informațiilor	38
5.1.7	Aruncarea deșeurilor	38
5.1.8	Stocarea copiilor de siguranță în afara locației	38
5.2	Controale procedurale.....	38
5.2.1	Roluri de încredere	38
5.2.2	Numărul de persoane necesare pentru fiecare sarcină	39
5.2.3	Identificarea și autentificarea pentru fiecare rol	40
5.2.4	Rolurile care necesită separarea sarcinilor.....	40
5.3	Controlul personalului	40
5.3.1	Calificări, experiență și aprobări necesare.....	40
5.3.2	Proceduri de verificare a antecedentelor	41
5.3.3	Cerințele de pregătire a personalului	41
5.3.4	Frecvența și cerințele stagiilor de pregătire	41
5.3.5	Frecvența și secvența rotației posturilor.....	41
5.3.6	Sancțiunile pentru acțiunile neautorizate	41
5.3.7	Cerințele pentru contractanții independenți	41
5.3.8	Documentația oferită personalului.....	41
5.4	Procedurile de înregistrare a datelor de audit.....	42
5.4.1	Evenimente Înregistrate	42
5.4.2	Frecvența procesării jurnalelor de evenimente.....	44
5.4.3	Perioada de păstrare a log-urilor de audit	44
5.4.4	Protecția jurnalelor de evenimente.....	44
5.4.5	Procedura de backup a log-urilor de Audit.....	45
5.4.6	Audit collection system (intern vs. extern)	45
5.4.7	Notificarea to event-causing Subiect	45
5.4.8	Evaluări de vulnerabilitate	45
5.5	Arhivarea înregistrărilor	45
5.5.1	Tipuri de date arhivate	46
5.5.2	Perioada de retenție a arhivei.....	46
5.5.3	Protecția arhivei	46
5.5.4	Procedurile de back-up al arhivei	46
5.5.5	Cerințe privind marcarea temporală a înregistrărilor.....	46
5.5.6	Sistemul de colectare al arhivei (intern sau extern).....	46
5.5.7	Proceduri de obținere și verificare a informațiilor arhivate	47
5.6	Schimbarea cheilor	47
5.7	Compromiterea și recuperare în caz de dezastru	47
5.7.1	Procedurile de administrare a incidentelor și compromiterilor.....	47
5.7.2	Compromiterea resurselor de calcul, a aplicațiilor software și/sau datelor ...	48
5.7.3	Proceduri care se aplică la compromiterea cheii private a unei entități	49

5.7.4	Capacități de Continuitate a afacerii în caz de dezastru.....	49
5.8	Încetarea activității Autorității de Certificare sau a Autorității de Înregistrare	50
6	Controale tehnice de securitate.....	52
6.1	Generarea și instalarea perechii de chei	52
6.1.1	Generarea perechilor de chei.....	52
6.1.2	Distribuirea Cheii Private către Beneficiar	53
6.1.3	Distribuirea Cheii Publice către emitentul certificatului.....	54
6.1.4	Distribuirea Cheii Publice a Autorității Certificare către Entitățile Partenere..	54
6.1.5	Marimea cheilor.....	54
6.1.6	Parametrii de generare a Cheilor Publice și verificarea calității.....	55
6.1.7	Scopurile în care pot fi utilizate cheile (conform câmpului de utilizare a cheilor X.509 v3)	55
6.2	Protecția cheii private și controalele modulului criptografic	55
6.2.1	Controalele și standardele modulelor criptografice	56
6.2.2	Control multi-persoană (n din m) al cheilor private	56
6.2.3	Custodia Cheii Private	57
6.2.4	Copia de siguranță a cheii private	57
6.2.5	Arhivarea Cheii Private	58
6.2.6	Transferul Cheii Private într-un sau dintr-un modul criptografic	58
6.2.7	Stocarea cheilor private pe modul criptografic	58
6.2.8	Metoda de activare a cheii private.....	59
6.2.9	Metoda de dezactivare a cheii private.....	59
6.2.10	Metoda de distrugere a cheii private	59
6.2.11	Evaluarea Modulului Criptografic.....	60
6.3	Alte aspecte legate de managementul perechilor de chei	60
6.3.1	Arhivarea cheii publice	60
6.3.2	Perioadele operaționale ale certificatelor și perioadele de utilizare a cheilor private	60
6.4	Datele de activare	60
6.4.1	Generarea și instalarea datelor de activare	60
6.4.2	Protejarea datelor de activare	61
6.4.3	Alte aspect ale datelor de activare	61
6.5	Controale de Securitate a computerelor	62
6.5.1	Cerințe tehnice specifice ale securității calculatoarelor	62
6.5.2	Evaluarea securității calculatoarelor	63
6.6	Controale de securitate specifice ciclului de viață.....	63
6.6.1	Controale specifice dezvoltării sistemului	63
6.6.2	Controale specifice managementului securității.....	63
6.6.3	Controale de securitate specifice ciclului de viață	63
6.7	Controale de securitate a rețelei.....	64
6.8	Marcare temporală	65
7	Profilul certificatelor, CRL și OCSP	66
7.1	Profilul certificatului	66
7.1.1	Numerele de versiune	67
7.1.2	Extensii de certificate	67
7.1.3	Algoritmul identificatorului obiect.....	71
7.1.4	Formulare de nume.....	71
7.1.5	Constrangeri privind numele	71

7.1.6	Identificatorul de obiect pentru politica de identificare	71
7.1.7	Utilizarea extensiei Constrângerii de politică	73
7.1.8	Sintaxa și semantica calificărilor de politică	73
7.1.9	Semantica de procesare pentru extensia Politici critice de certificare	73
7.2	Profilul CRL.....	73
7.2.1	Numerele de versiune	74
7.2.2	CRL și extensiile de intrare CRL	74
7.3	Profilul OCSP	75
7.3.1	Numarul versiunilor	76
7.3.2	Extensii OCSP	76
8	Auditul de conformitate și alte evaluări	77
8.1	Frecvența sau circumstanțele de evaluare	77
8.2	Identitatea / calificările evaluatorului	77
8.3	Relația evaluatorului cu entitatea evaluată	77
8.4	Subiectele acoperite de evaluare	77
8.5	Acțiuni întreprinse ca urmare a deficienței	78
8.6	Comunicarea rezultatelor	78
9	Alte elemente de afaceri și legale	79
9.1	Tarife.....	79
9.1.1	Tarifele serviciilor de emitere și reînnoire a certificatelor digitale.....	79
9.1.2	Tarifele serviciilor de acces la certificate	79
9.1.3	Tarifele serviciilor de revocare sau acces la informațiile despre starea certificatelor.....	79
9.1.4	Tarife pentru alte servicii	79
9.1.5	Rambursarea plăților.....	79
9.2	Răspunderea financiară.....	79
9.2.1	Acoperirea prin asigurare.....	79
9.2.2	Alte active	79
9.2.3	Asigurarea sau acoperirea garanției pentru entitățile finale	80
9.3	Confidențialitatea informațiilor de afaceri	80
9.3.1	Scopul informațiilor confidențiale	80
9.3.2	Informații care nu sunt considerate a fi confidențiale.....	81
9.3.3	Responsabilitatea de a proteja informațiile confidențiale	81
9.4	Confidențialitatea informațiilor personale.....	81
9.4.1	Planul de asigurare a protecției datelor cu caracter personal	81
9.4.2	Informații considerate ca fiind cu caracter personal.....	82
9.4.3	Informații care nu sunt considerate private	82
9.4.4	Responsabilitatea de a proteja informațiile private	82
9.4.5	Notificarea persoanelor vizate și consimțământul acestora pentru utilizarea datelor cu caracter personal	82
9.4.6	Divulgare ca urmare a unui proces administrativ sau juridic	82
9.4.7	Alte circumstanțe pentru divulgare	82
9.5	Drepturile de Proprietate Intelectuală	83
9.6	Reprezentări și garanții	83
9.6.1	Reprezentările și garanțiile CA.....	83
9.6.2	Reprezentările și garanțiile RA.....	83
9.6.3	Reprezentările și garanțiile Beneficiarului.....	83
9.6.4	Reprezentările și garanțiile Entităților Partenere	83

9.6.5	Reprezentările și garanțiile altor participanți.....	84
9.7	Declinarea garanțiilor.....	84
9.8	Limitarea răspunderii	84
9.9	Despăgubiri	84
9.10	Termenii și încetarea	84
9.10.1	Termenii.....	84
9.10.2	Încetarea.....	84
9.10.3	Efectul terminării și supraviețuirii.....	84
9.11	Notificări individuale și comunicarea cu participanții.....	85
9.12	Amendamente	85
9.12.1	Procedura pentru amendamente.....	85
9.12.2	Mecanismul de notificare și perioada	85
9.12.3	Circumstanțele în care OID trebuie schimbat.....	85
9.13	Procedurile de soluționare a litigiilor	85
9.14	Legea aplicabilă	85
9.15	Conformitatea cu legea aplicabilă	86
9.16	Prevederi diverse	86
9.16.1	Acordul integral.....	86
9.16.2	Cesiunea	86
9.16.3	Separabilitate.....	86
9.16.4	Executarea (onorariile avocaților și renunțarea la drepturi)	86
9.16.5	Forța majoră.....	86
9.17	Alte prevederi	86

1 Introducere

certSIGN Public CA este la sfârșitul ciclului de viață și nu mai emite certificate end-user.

Codul de Practici și Proceduri al certSIGN CA Public (denumit în continuare CPP Public CA sau CPP) descrie politica de certificare și practicile pe care certSIGN le aplică în emiterea de certificate digitale de către Autoritatea de Certificare subordonată Public CA.

Structura și conținutul CPP Public CA respectă recomandările RFC 3647, ETSI EN 319 411-1, ETSI EN 319 411-2.

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

1.1 Descriere Generală

certSIGN, Beneficiarii, Subiecții și Entitățile Partenere asociate trebuie să respecte prezentul CPP Public CA pentru emiterea certificatelor necalificate pentru autentificare și semnătură electronică, a certificatelor necalificate pentru criptare și a certificatelor necalificate pentru sigiliile electronice. 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 CA Public, denumit în continuare CPP Public CA sau CPP.

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

1.3 Participanții PKI

CPP Public CA reglementează cele mai importante relații dintre entitățile CERTSIGN, echipele de consultanți (inclusiv auditorii) și clienții (utilizatorii serviciilor furnizate) acestea:

- certSIGN CA Public,
- Autoritatea de Înregistrare,
- Depozitar,
- Protocolul de verificare online a stării certificatelor (Autoritatea OCSP),
- Subiecții,
- Beneficiarii,
- Entitățile Partenere,
- Furnizorii relevanți ai certSIGN din punct de vedere al emiterii și managementului certificatelor digitale,
- Comitetul de Management al Politicilor și Procedurilor,
- Auditorii.

certSIGN oferă servicii de certificare pentru orice persoană fizică sau entitate juridică care este de acord cu prevederile prezentului CPP. Scopul prezentului CPP (ce include 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.

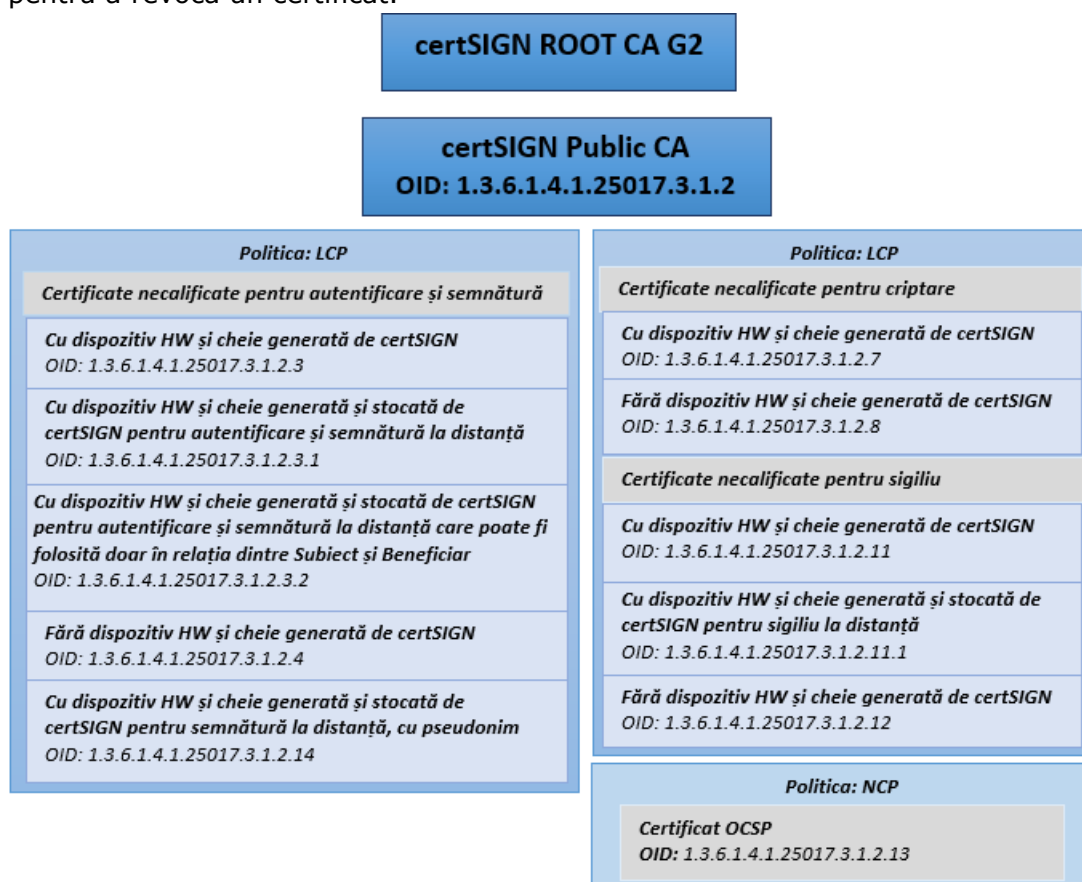
1.3.1 Autoritățile de Certificare

certSIGN CA Public este o Autoritate de Certificare Subordonată pentru domeniul CERTSIGN. Este subordonată certSIGN ROOT CA G2. certSIGN CA Public este identificată prin următorul OID: 1.3.6.1.4.1.25017.3.1.2

Înainte de începerea activității, certSIGN CA Public trimite o cerere Autorității de Certificare Primare, certSIGN ROOT CA G2 pentru înregistrare și emiterea certificatului de cheie publică.

1.3.2 Autoritățile de Înregistrare

Autoritatea de Înregistrare primește, verifică și aprobă sau respinge cererile de înregistrare și emitere de certificate, de rekey certificat sau revocare a certificatelor. Verificarea cererilor are ca scop autentificarea (pe baza documentelor incluse în cereri) atât a beneficiarului/subiectului, 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 revoca un certificat.



Autoritatea de Înregistrare este operată de certSIGN sau de către o terță parte delegată. RA-urile externe trebuie să respecte aceleași cerințe de securitate pe care le respectă TSP în ceea ce privește resursele umane, securitatea operatională a rețelei și a datelor personale așa cum este specificat în clauzele 6.4.4, 6.5.6, 6.5.7 și 6.8.4 din ETSI 319 411-1.

1.3.3 Beneficiarii

Beneficiar

Beneficiarii sunt persoane juridice sau fizice care solicită certSIGN emiterea unui certificat și cu care aceștia semnează un Acord contractual.

Beneficiarii pot fi:

- Persoane fizice - în acest caz, Beneficiarul este Subiectul certificatului emis de CERTSIGN,
- Persoane juridice care încheie un acord contractual cu certSIGN pentru emiterea de certificate pentru Subiecți (de exemplu: liber profesioniști, angajați),
- Persoane juridice care încheie un acord contractual cu certSIGN pentru emiterea de certificate pentru sigiliul electronic.

Beneficiarii pot solicita emiterea, revocarea sau rekey-ul certificatelor pentru Subiecții de care răspund. Un Beneficiar este responsabil, deasemenea, de notificarea certSIGN imediat după (suspiciunea de) compromitere a cheii private.

Subiect

Subiectul este entitatea căreia îi este emis un certificat și care este identificată într-un certificat ca fiind posesorul cheii private asociate cheii publice din certificat.

Subiectul poate fi:

- Beneficiarul, în cazul în care solicită certificatul pentru el însuși/ea însăși,
- Persoana fizică pentru care Beneficiarul solicită certificatul, acesta din urma având un acord contractual sau acționând ca angajator al său,
- Persoana juridică pentru care Beneficiarul solicită certificatul pentru sigiliul electronic.

Un Subiect este responsabil, deasemenea, de:

- Notificarea imediată a certSIGN în cazul (suspiciunii de) compromiterii cheii private;
- Trimiterea către certSIGN a cererilor de reînnoire a cheilor și/sau certificatelor în timp util;
- Protejarea confidențialității cheii sale private în conformitate cu acest document;
- Asigurarea faptului că accesul la cheia sa privată este controlat în conformitate cu acest document.

1.3.4 Entitățile Partenere

O Entitate Parteneră este orice entitate care folosește serviciile certSIGN și ia decizii bazate pe corectitudinea legăturii dintre identitatea Subiectului și cheia publică.

O Entitate Parteneră este responsabilă de modul cum verifică starea curentă a certificatului unui Subiect. O astfel de decizie va fi luată de fiecare dată când o Entitate Parteneră dorește să utilizeze un certificat pentru a verifica o semnătură electronică, identitatea sursei sau autorul unui mesaj sau pentru a crea un canal de comunicare securizat cu Subiectul certificatului. O Entitate Parteneră va utiliza informațiile dintr-un certificat (de exemplu identificatori și 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 ("CMPP") este un Comitet creat în cadrul certSIGN de către Consiliul de administrație pentru a supraveghea întreaga activitate a Autorităților de Certificare și a Autorităților de Înregistrare ale CERTSIGN. Rolurile și responsabilitățile CMPP sunt descrise în documentația internă CERTSIGN.

Furnizorii de servicii ai certSIGN sunt furnizori externi care sprijină activitățile certSIGN pe baza unui acord contractual semnat (de ex. Firmele de curierat).

Furnizorii de Dispozitive de Creare a Semnăturilor Electronice Calificate: furnizorii externi care sprijină activitățile certSIGN în cadrul unui acord contractual semnat ce asigură furnizarea dispozitivelor criptografice fizice utilizate de către Subiecți.

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 (de exemplu, semnătura electronică, confidențialitate),
- 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. Subiecții trebuie să cunoască cerințele Entității Parteneră (de exemplu, aceste cerințe pot fi publicate sub forma unei politici de semnătură sau a unei politici de securitate informatică) și apoi să solicite certSIGN emiterea de certificate corespunzătoare acestor cerințe.

1.4.1 Utilizări admise ale certificatului

Certificatele pot fi utilizate în 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 utilizatorului 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 Parteneră, pe baza naturii și scopului (inclusiv utilizarea cheii) Certificatului, inclusiv orice limitare aplicabilă în scris în Certificat.

Este responsabilitatea Subiectului să utilizeze certificatele în conformitate cu acest CPP. Este responsabilitatea subiectului sau a beneficiarului de a utiliza aplicații software care interpretează corect, afișează și utilizează informațiile și restricțiile codificate în certificate, cum ar fi, dar fără a se limita la: utilizarea cheilor, răspundere limitată pentru fiecare tranzacție etc.

Este responsabilitatea Beneficiarului, Subiectului și a Entității Parteneră 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.

Certificatele cu pseudonim oferă cel mai scăzut nivel de securitate în legătură cu identitatea individuală, și se recomandă a fi utilizate numai pentru a oferi integritatea datelor documentelor semnate cu aceste certificate, în condiții considerate de risc scăzut și în care autentificarea tranzacțiilor nu este necesară.

1.4.2 Utilizări interzise ale certificatului

Orice utilizare a certificatului care diferă de utilizarea permisă în mod explicit în CPP este interzisă.

1.5 Administrarea politicii

1.5.1 Organizația care administrează documentul

Prezentul document este administrat de către Prestatorul de servicii de încredere certSIGN ("TSP") prin Comitetul de Management al Politicilor și Procedurilor (CMPP). CMPP include

membri seniori din conducere, precum și personalul responsabil pentru gestionarea operațională a mediului PKI al TSP CERTSIGN.

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

Tabel: 1.5.1 Organizația ce administrează documentul

1.5.2 Persoana de contact

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

Tabel: 1.5.2 Persoana de contact

1.5.3 Persoana care decide conformitatea CPP cu politica

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

Tabel: 1.5.3 Persoana ce 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 descrisă într-un document de instrucțiuni interne.

Subiecții/Beneficiarii trebuie să respecte CPP-ul în vigoare, publicat la adresa <https://www.certsign.ro/ro/document/certsign-public-ca-cod-practici-si-proceduri/>.

Subiecții/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 publicat, 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

Auditor – persoană care evaluează conformitatea cu cerințele specificate în documentele relevante

Autentificare – proces electronic ce permite identificarea electronică a unei persoane fizice sau juridice sau originea și integritatea datelor electronice care trebuie confirmate

Certificat – cheia publică a unui Subiect, împreună cu alte informații, ce sunt protejate împotriva falsificării prin criptarea cu cheia privată emisă de o autoritate de certificare

Lista de Certificate Revocate (CRL) – o listă semnată ce indică un set de certificate ce nu mai sunt considerate valide de către TSP

Lista de revocare a Autorității de Certificare (CARL) – o lista de revocare cu certificate de CA emise către o autoritate de certificare care nu mai sunt considerate valide de către emitentul certificatului.

Certificat pe termen scurt - certificat a cărui perioadă de valabilitate, adică perioada de timp de la notBefore până la notAfter, inclusiv, este mai scurtă decât timpul maxim de procesare a unei cereri de revocare, astfel cum este specificat în acest CPP.

Codul de Practici și Proceduri (CPP) – un cod de practici pe care o Autoritate de Certificare le utilizează în emiterea, gestionarea, revocarea și reînnoire sau rekey-ul certificatelor.

Cross-certificare – un certificat care este emis pentru a stabili o relație de încredere între două autorități de certificare

Semnătură electronică – date în format electronic care sunt atașate sau asociate logic cu alte date în format electronic și care sunt utilizate de către semnatar pentru semnare

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

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

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

Infrastructura cu Cheie Publică (PKI) – arhitectura, tehnicile, practicile și procedurile care contribuie în mod colectiv la implementarea și funcționarea sistemelor criptografice cu chei publice, bazate pe certificate; PKI constă în hardware, software, baze de date, resurse de rețea, proceduri de securitate și obligații legale, legate împreună și care colaborează pentru a furniza și implementa atât serviciile de certificare, cât și alte servicii asociate infrastructurii (de ex. marcă temporală).

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

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

Autoritate de Înregistrare – entitate responsabilă în special de identificarea și autentificarea Subiecților certificatelor

Root CA – autoritate de certificare care se află la cel mai înalt nivel în cadrul domeniului TSP și care este utilizată pentru semnarea CA-ului (-urilor) subordonat(e).

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

CA subordonat - autoritate de certificare al cărei certificat este semnat de Root CA sau de un alt CA subordonat

Beneficiar – persoană juridică sau fizică legată prin contractul cu un furnizor de servicii de încredere de toate obligațiile Beneficiarului

Prestator de servicii de încredere – o persoană fizică sau juridică ce furnizează unul sau mai multe servicii de încredere, fie ca furnizor de servicii de încredere calificate, fie ca furnizor de servicii de încredere ne-calificate;

Cerintele de Baza TLS CA/Browser Forum - Cerintele de Baza pentru Emiterea și Managementul certificatelor de încredere publice (*Baseline Requirements for the Issuance and Management of Publicly - Trusted Certificates*) Versiunea 2.0.1

Cerintele de Baza S/MIME CA/Browser Forum - Cerintele de Baza pentru Emiterea și Managementul certificatelor de încredere publice de tip S/MIME (*Baseline Requirements for the Issuance and Management of Publicly - Trusted S/MIME Certificates*) Versiunea 1.0.1

BR	Cerintele de Baza TLS CA/Browser Forum
CA	Autoritate de certificare
CPP	Cod de Practici și Proceduri
CRL	Lista de Certificate Revocate
CARL	Lista de Revocare a Autorității de Certificare
DN	Nume distinctiv
HW	Hardware
NIMB	Institutul Național de Metrologie București
OCSP	Protocol de verificare online a stării certificatului
PKI	Infrastructură cu Cheie Publică
CMPP	Comitet de Management al Politicilor și Procedurilor
QSCD	Dispozitiv de Creare a Semnăturilor Electronice Calificate
RA	Autoritate de Înregistrare
RSA	Algoritmul criptografic asimetric Rivest, Shamir, Adleman
S/MIME	Extensie de email multi-scop securizată
SBR	Cerintele de Baza S/MIME CA/Browser Forum
TSP	Furnizor de Servicii de Încredere
UTC	Timpul Universal coordonat

2 Publicare și responsabilități Depozitar

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

2.1 Depozitare

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

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

Depozitarul este gestionat și controlat de CERTSIGN. certSIGN se angajează:

- Să depună toate eforturile necesare pentru a se asigura că toate certificatele publicate în Depozitar aparțin Subiecților înscriși în certificate și că Subiecții și-au dat acordul asupra acestor certificate,
- Să se asigure că certificatele 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 ofere acces 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, Subiecți 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 Subiectului pentru care a fost emis certificatul.

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

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

Disponibilitate

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

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

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

CertIFICATELE EXPIRATE CARE AU FOST REVOCATE ÎNAINTE DE EXPIRAREA LOR NU SUNT ELIMINATE DIN LISTELE DE REVOCARE A CERTIFICATELOR.

2.3 Timpul sau frecvența publicării

Informațiile publicate de certSIGN sunt actualizate cu următoarea frecvență:

- CPP – vezi Capitolul 1.5,
- Certificatele Autorităților de Certificare – după emiterea unui nou certificat;
- Certificatele Subiecților – la obținerea consimțământului, după fiecare emitere a unui nou certificat;
- Lista certificatelor revocate este creată fie o dată la 24 de ore, fie atunci când un certificat este revocat;
- Rapoartele auditurilor realizate de instituții autorizate – când le primește CERTSIGN;
- Informațiile suplimentare – după fiecare actualizare.

2.4 Controlul accesului la Depozitare

Toate informațiile publicate de certSIGN în Depozitar la adresa <http://www.certsig.ro/repository> sunt accesibile publicului.

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

Beneficiarii, Subiecții 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 Denumirea

3.1.1 Tipuri de nume

Certificatele emise de certSIGN sunt conforme cu standardul X.509 v3. Aceasta înseamnă că TSP 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). Denumirile Subiecților și ale emitentilor de certificate din certificatele certSIGN sunt în conformitate cu structura de nume Distinctive Name (DN) – (cunoscute și ca structuri de tip Directory Name), create conform recomandărilor X.500 și X.520.

Pentru a asigura o comunicare electronică ușoară cu Subiectul, în certificatele certSIGN este utilizat un nume adițional pentru Subiect. Acest nume poate conține, de asemenea, adresa de e-mail a Subiectului, conform recomandărilor RFC 822.

3.1.2 Nevoia ca Numele să aibă înțeles logic

Numele inclus în Numele Distinctiv al Subiectului trebuie să aibă înțeles logic 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.

DN constă în câmpuri obligatorii și opționale conform recomandărilor RFC 5280 și X.520

Câmpurile DN obligatorii pentru persoanele fizice, cu excepția certificatelor cu OID 1.3.6.1.4.1.25017.3.1.2.14, sunt următoarele:

- C – abrevierea internațională pentru numele țării (RO pentru România)
- SN – Numele de familie¹ al Subiectului și G – Prenumele Subiectului
- CN – Numele Subiectului²
- Serial Number – Numărul serial unic atribuit Subiectului de către CA. Semnificația SerialNumber este: Prima literă a numelui de familie + Prima literă a prenumelui + număr index

Câmpurile DN obligatorii pentru persoanele fizice, în cazul certificatelor cu OID 1.3.6.1.4.1.25017.3.1.2.14, sunt următoarele:

- C – abrevierea internațională pentru numele țării (RO pentru România)
- P – Pseudonimul Subiectului
- CN – Pseudonimul Subiectului
- Serial Number – Numărul serial unic atribuit Subiectului de către CA. Semnificația SerialNumber este: Prima literă a fiecărui cuvânt din pseudonim + număr index

Câmpurile DN opționale pentru persoanele fizice sunt următoarele:

- S – Județul / sectorul de reședință al Subiectului,
- L – Localitatea de reședință a Subiectului,
- Street – Adresa Subiectului,
- Phone – Numărul de telefon al Subiectului,

Câmpurile DN obligatorii pentru persoanele fizice asociate unei organizații sunt următoarele:

- C – abrevierea internațională pentru numele țării (RO pentru România),
- O – Numele oficial al organizației Beneficiarului, atunci când Beneficiarul este angajatorul Subiectului sau există un acord contractul încheiat între ei,
- Organization Identifier – Un identificator unic oficial al Beneficiarului ca entitate legală
- SN – Numele de familie³ al Subiectului,
- G – Prenumele Subiectului,
- CN – Numele Subiectului (prenume, nume de familie)⁴,
- SerialNumber – Numărul serial unic atribuit Subiectului de către CA. Semnificația SerialNumber este: Prima literă a numelui de familie + Prima literă a prenumelui + număr index

¹ Pentru subiecții care se identifică cu act de identitate emis de țara (C) Franța (FR), în cazul în care numele a fost schimbat prin căsătorie și atât numele inițial, cât și numele de după căsătorie apar pe documentul de identitate, numele de familie din certificat trebuie să fie cel de după căsătorie.

² Pentru Subiecții care se identifică cu act de identitate emis de țara (C) Franța (FR) CN este format din primul prenume (G) urmat de numele complet (SN); pentru restul (C diferit de FR) CN este format din prenumele complet (G) urmat de numele complet (SN).

³ Idem Nota 1

⁴ Idem Nota 2

Câmpurile DN opționale pentru persoanele fizice asociate unei organizații sunt:

- OU – numele departamentului organizației,
- S – județul / sectorul în care este înregistrat Beneficiarul,
- L – localitatea în care este înregistrat Beneficiarul,
- Street – Adresa Beneficiarului,
- T – Funcția,
- Field Phone – Numărul de telefon

Câmpurile DN obligatorii pentru persoanele juridice sunt:

- C – abrevierea internațională pentru numele țării (RO pentru România),
- O – Numele oficial al organizației
- Organization Identifier – Un identificator unic oficial al Beneficiarului ca entitate legală,
- CN – Numele organizației

Câmpurile DN opționale pentru persoanele juridice sunt:

- OU – numele departamentului organizației,
- S – județul / sectorul în care este înregistrată organizația,
- L – localitatea în care este înregistrată organizația,
- Phone – numărul de telefon

Numele Subiectului va fi confirmat de către un operator al Autorității de Înregistrare și va fi aprobat de Autoritatea de Certificare. certSIGN asigură (în cadrul domeniului său) unicitatea DN-urilor.

3.1.3 Anonimitatea sau pseudonimitatea Beneficiarilor

Se acceptă utilizarea de pseudonime exclusiv pentru certificate cu OID 1.3.6.1.4.1.25017.3.1.2.14.

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). Caracterele speciale din nume se preiau din documentul de identitate: fie din MRZ, fie din câmpurile de nume, în conformitate cu standardele precizate în procedurile interne ale certSIGN. 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 numărului serial al Subiectului atribuit de CA. Semantica lui SerialNumber este: Prima literă de familie + Prima literă de prim nume + număr index. Numărul indexului este numărul secvențial al prefixului (precum codul + inițialele) în baza de date.

3.1.6 Recunoașterea, autentificarea și rolul mărcilor înregistrate

Nu se aplică.

3.2 Validarea Inițială a Identității

În cazul emiterii de certificate cu OID 1.3.6.1.4.1.25017.3.1.2.14 se verifica doar telefonul.

3.2.1 Dovada Posesiei Cheii Private

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

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

3.2.2 Autentificarea identității organizației

Autentificarea identității organizației se realizează pentru a dovedi că persoana juridică există cu adevărat.

Când persoana juridică intră într-un acord contractual cu certSIGN pentru emiterea certificatelor necalificate, următoarele documente sunt necesare pentru identificarea Beneficiarului (entitate juridică):

- Extrasul valid de la Registrul Comerțului (sau echivalentul, pentru societățile străine înregistrate conform legislației străine);
- Extras din Registrul asociațiilor și fundațiilor (sau echivalent pentru asociațiile și fundațiile străine)
- Mandatul oficial, atunci când persoana fizică care reprezintă persoana juridică nu este reprezentantul legal al entității.
- În cazul entităților fără personalitate juridică, identificarea Subiectului se va face în baza actului normativ de înființare sau, în lipsa acestuia, se pot utiliza documente emise și semnate de reprezentantul legal al instituției publice în subordonarea căreia se află, care să ateste identitatea respectivei entități.

Procedura descrisă în acest capitol va fi aplicată la fiecare 6 ani pentru a verifica identitatea organizației, începând cu data emiterii primului certificat în baza prezentului CPP.

3.2.3 Autentificarea identității persoanelor fizice

Documentele de identitate necesare verificării identității persoanelor fizice trebuie să fie valide și să întrunească standardele minime de securitate. Acestea sunt:

- act de identitate sau pașaport, în cazul cetățenilor români
- act de identitate, pașaport sau act de identitate emis de Autoritățile Române, în cazul cetățenilor străini

Verificarea identității persoanelor fizice trebuie realizată:

- Atunci când persoana fizică este Subiectul unui certificat digital emis de CERTSIGN.
- Atunci când persoana fizică reprezintă o entitate legală care încheie un acord contractual cu certSIGN

Autoritatea de Certificare Emitentă	Autoritatea de Înregistrare realizează identificarea persoanelor fizice printr-una dintre următoarele metode:
certSIGN Public CA	• prin prezența personală la Autoritatea de Înregistrare
	• prin transmiterea copiei actului de identitate fizic (prin posta, curier, mandatar etc.)
	• prin transmiterea în format electronic a actului de identitate

Tabel 1: Cerințe pentru verificarea identității persoanelor fizice

3.2.4 Informații neverificate cu privire la Beneficiar

Subiectul sau Beneficiarul, după caz, este responsabil de furnizarea unor informații actualizate, exacte și corecte în cadrul procesului de înregistrare.

În cazul OID: 1.3.6.1.4.1.25017.3.1.2.3.1 (cu dispozitiv HW și cheie generată și stocată de certSIGN pentru semnatura la distanță și autentificare), OID: 1.3.6.1.4.1.25017.3.1.2.3.2 (cu dispozitiv HW și cheie generată și stocată de certSIGN pentru semnătura la distanță și autentificare care poate fi folosită doar în relația dintre Subiect și Beneficiar) și OID 1.3.6.1.4.1.25017.3.1.2.14 numărul de telefon al subiectului (posesia acestuia) este verificat de către certSIGN sau de către terțe părți.

În toate celelalte cazuri adresa de e-mail și numărul de telefon reprezintă informații neverificate ale Subiectului.

3.2.5 Validarea autorității

Nu este stipulat.

3.2.6 Criterii pentru interoperare

Nu este stipulat.

3.3 Identificarea și autentificarea pentru cererile de re-key

3.3.1 Identificarea și autentificare pentru re-key de rutină

Capitolul 4.7 al acestui document descrie acest proces.

3.3.2 Identificarea și autentificarea pentru re-key după revocare

Este folosit același proces, ca în cazul validării inițiale a identității.

3.4 Identificarea și autentificarea pentru cererile de revocare

Următoarele entități pot trimite cereri de revocare a certificatelor:

- Subiectul care este deținătorul cheii private asociate cheii publice din certificat va trimite cererea de revocare utilizând oricare dintre următoarele metode:
 - online, prin utilizarea codului de revocare primit de la CERTSIGN. În această situație, certificatul este revocat după ce certSIGN primește cererea.
 - În format electronic, prin trimiterea la office@certsign.ro a unei cereri semnate cu o semnătură electronică calificată creată utilizând un certificat digital calificat emis Subiectului (cu același Common Name). În această situație, certificatul este revocat după ce certSIGN verifică și validează cererea.
 - Prin completarea și depunerea cererii în fața unui angajat al Autorității de Înregistrare. În această situație, certificatul este revocat după ce certSIGN verifică și validează cererea.
- Beneficiarul care încheie un acord contractual cu certSIGN pentru emiterea de certificate Subiecților va trimite cererea de revocare utilizând oricare dintre următoarele metode:
 - online, prin trimiterea unei cereri utilizând codul de revocare primit de la CERTSIGN. În această situație, certificatul este revocat după ce certSIGN primește cererea.
 - În format electronic, prin trimiterea la office@certsign.ro a unei cereri semnate cu o semnătură electronică calificată sau cu un sigiliu electronic calificat. În

această situație, certificatul este revocat după ce certSIGN verifică și validează cererea.

- Prin completarea și depunerea cererii în fața unui angajat al Autorității de Înregistrare. În această situație, certificatul este revocat după ce certSIGN verifică și validează cererea.
- Autoritatea de Înregistrare care poate cere revocarea fie în numele unui Subiect, fie fiindcă deține informații care justifică revocarea certificatului utilizând mecanismele de securitate ale software-ului Autorității de Înregistrare.
- Rolurile de încredere asociate certSIGN CA Public, sub supravegherea Comitetului de Management al Politicilor și Procedurilor (CMPP) utilizând mecanismele de securitate ale software-ului Autorității de Certificare

4 Cerințe operaționale privind ciclul de viață al certificatului

Acest capitol descrie procedurile de bază care se aplică tuturor tipurilor de certificate emise de certSIGN CA Public.

O descriere detaliată a procedurilor referitoare la serviciile componente PKI (CA-uri, RA-uri, CRL Signers, Responder OCSP etc.) și persoanele/rolurile implicate în procesul operațional al acestor componente este inclusă în documentația internă confidențială.

certSIGN oferă acces la următoarele servicii:

- a. Înregistrare, emitere, rekey;
- b. Revocarea certificatelor;
- c. Verificarea valabilității certificatelor.

4.1 Cererea de certificat

4.1.1 Cine poate trimite o cerere de certificat

Persoanele Fizice

Pot solicita certificate:

- Persoanele fizice, în cazul solicitării certificatului în nume personal,
- Persoana/persoanele fizice (Subiecți) pentru care Beneficiarul a solicitat certificatul, având un acord contractual sau acționând ca angajator al acestora.

Beneficiarul și Subiectul vor respecta prevederile și obligațiile stabilite în Acordul contractual cu Beneficiarul și în Termenii și Condițiile serviciilor de certificare ce încorporează acest CPP și Declarația de Transparență PKI.

Autoritatea de Certificare emite certificate doar ca răspuns la o cerere primită de la Autoritatea de Înregistrare operată de certSIGN sau de la o terță parte delegată.

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

Entitățile Juridice (Organizații)

certSIGN emite certificate pentru sigiliile electronice entităților juridice. Subiectul va respecta prevederile și obligațiile stabilite în Acordul contractual cu Beneficiarul și în Termenii și Condițiile serviciilor de certificare ce încorporează acest CPP și Declarațiile de Transparență PKI.

Autoritatea de Certificare emite certificate doar ca răspuns la o cerere primită de la Autoritatea de Înregistrare operată de certSIGN sau de la o terță parte delegată.

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 în mod direct sau bazându-se pe un terț.

certSIGN poate delega atribuțiile de identificare a subiecților către terțe părți care pot asigura metode/proceduri de identificare ce oferă un nivel de asigurare echivalent Autorității de Înregistrare (vezi. Cap.3.2.3.).

În orice situație, CERTSIGN, în calitate de furnizor de servicii de încredere, raspunde, în limitele prevăzute în prezentul CPP, pentru actele sau omisiunile tuturor agenților, angajaților și colaboratorilor săi implicați în procesul de înregistrare.

RA este responsabilă de verificarea următoarelor elemente:

- Identitatea asumată de Subiect/Beneficiar,
- Atributele asumate de către Subiect/Beneficiar,
- Cererea Subiectului/Beneficiarului pentru certificatul solicitat

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

Subiectului/Beneficiarului i se pun la dispoziție următoarele informații și documente:

- Acord contractual
- Termeni și Condiții
- adresa online a Termenilor și Condițiilor privind utilizarea certificatului
- adresa online a CPP, notificări sau alte documente necesar a fi furnizate de Subiect (vor fi definite în Acordul contractual cu Beneficiarul)

Prin semnarea Acordului contractual și a Termenilor și Condițiilor, Subiectul/Beneficiarul înțelege și acceptă următoarele:

- responsabilitatea sa ca informațiile furnizate către RA sunt corecte, complete, valabile și actualizate,
- că certSIGN păstrează o perioadă de 10 ani de la data expirării/revocării certificatului 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,
- recunoaște drepturile, obligațiile și responsabilitățile certSIGN și ale altor participanți la PKI, astfel cum sunt definite în Acordul cu Beneficiarul și în legislațiile naționale,
- că Subiectul/Beneficiarul are obligația de a informa certSIGN cu privire la orice schimbare sau eveniment care poate afecta valabilitatea sau conținutul certificatului.

Procesul de înregistrare

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

Procesul de înregistrare începe în cadrul RA.

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

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

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

RA verifică și completează datele de înregistrare. RA este responsabilă de corectitudinea datelor care vor fi incluse în cererea de certificat trimisă la CA. RA este responsabilă de înregistrarea/înscierea corectă a Subiecților/Beneficiarilor și de furnizarea către CA a conținutului corect pentru câmpurile variabile din certificat.

4.2 Procesarea cererilor de certificate

certSIGN acceptă cereri pentru un subiect sau mai mulți. Cererile pot fi trimise fizic și electronic.

Cererea de certificat este completată în format electronic:

- Acordul contractual, Termeni și Condiții și copie după actul de identitate⁵ sunt trimise electronic prin email și semnate electronic cu un certificat digital calificat valid (nerevocat sau expirat) emis de certSIGN și trimise Autorității de Certificare.

Cererea de certificat se mai poate face:

- Prin prezența în persoană a Subiectului la Autoritatea de Înregistrare sau la Autoritatea de Certificare, caz în care Acordul contractual, Termeni și Condiții sunt completate și semnate olograf și se depune o copie după actul de identitate¹.
- Subiectul transmite către RA - Acordul contractual și Termeni și Condiții, completate și semnate olograf precum și o copie după actul de identitate¹.

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.

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

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 respectă regulile și standardele care guvernează certSIGN CA Public sau din alte motive, la discreția și sub răspunderea RA.

⁵ Copia după actul de identitate NU este necesară în cazul emiterii de certificate cu OID 1.3.6.1.4.1.25017.3.1.2.14

4.2.3 Timpul de procesare a cererilor de certificate

certSIGN nu emite un certificat imediat după înregistrarea cererii. Certificatele trebuie să fie emise de Autoritatea de Certificare prin aprobarea cererii de certificat după ce ea a fost validată de RA.

Certificatele sunt stocate pe un dispozitiv hardware sau în format software conform cu standardele PKCS#12 și Java Keystore. Dispozitivul hardware poate fi pus la dispoziția entității de către certSIGN după procesul de generare a cheilor sau entitatea poate avea propriul dispozitiv când generează cheile.

Procesul de livrare a certificatelor poate dura mai multe ore sau mai multe zile, dar nu mai mult de 5 zile lucratoare și depinde de disponibilitatea Subiectului de a primi sau colecta dispozitivul hardware care stochează certificatul digital sau să primească PKCS#12 în format electronic.

4.3 Emiterea certificatelor

4.3.1 Acțiunile CA în timpul emiterii certificatelor

Certificatul este emis de CA numai după primirea unei solicitări de certificat de la RA. CA și RA sunt sisteme integrate și comunică prin conexiuni de rețea închise. CA procesează numai cererile care provin de la RA-ul de încredere al CERTSIGN.

CA asigură unicitatea fiecărui certificat pe care îl emite utilizând câmpul SerialNumber din fiecare certificat.

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

4.3.2 Notificarea Subiectului de către CA cu privire la emiterea certificatului

CA utilizează următoarele metode pentru a informa Subiectul cu privire la emiterea certificatului:

- Când cheile sunt generate pe dispozitiv hardware de către Subiect, CA trimite un e-mail Subiectului utilizând adresa de e-mail furnizată la înregistrare. E-mail-ul informează Subiectul despre eliberarea certificatului și oferă informații care permit Subiectului să obțină certificatul și să-l încarce pe dispozitivul hardware.
- Când cheile sunt generate de certSIGN pe dispozitiv hardware, certificatul este livrat fie personal Subiectului, fie este trimis prin intermediul serviciilor poștale sau de curierat către Subiect. Datele de activare secretă (codul PIN) necesare pentru a accesa dispozitivul hardware sunt trimise utilizând un plic securizat.
- Când cheile sunt generate în format PKCS#12 de către CERTSIGN, RA trimite un email Subiectului utilizând adresa de email primită în procesul de aplicare. Email-ul care informează Subiectul de emiterea certificatului are atașat certificatul PKCS#12. Datele secrete de activare (de exemplu parola pentru certificatul PKCS#12) sunt transmise către Subiect utilizând un canal off-line.

Datele secrete de activare (codul PIN) sunt necesare pentru a putea utiliza cheile private stocate pe un dispozitiv hardware. Când certSIGN furnizează dispozitivul hardware, datele secrete de activare (codul PIN) sunt generate și livrate de un sistem care permite păstrarea confidențialității necesare.

Fiecare certificat emis este publicat în Depozitarul CERTSIGN. Publicarea certificatului este echivalentă cu notificarea Entităților Partenerere cu privire la faptul că un certificat a fost emis pentru un Subiect.

certSIGN poate utiliza „certIFICATE de testare”, care sunt certificate cu o utilizare limitată doar la testare, cu o valabilitate de maximum 30 de zile și care sunt identificate prin atributul Nume comun (CN) care începe cu textul „TEST”. „Certificatul de testare” va fi emis de un operator de înregistrare certSIGN, utilizând procedura standard. „Certificatul de testare” poate fi revocat după perioada de testare, la cerere.

4.4 Acceptarea certificatului

4.4.1 Conduita care constituie acceptarea certificatului

Certificatul va fi considerat acceptat de către Subiect după prima utilizare sau după perioada definită în Termeni și condiții, în funcție de evenimentul care survine primul.

RA și Subiectul au dreptul să respingă certificatul cu condiția ca cel puțin una dintre următoarele obiecții să se aplice:

- Informația din certificat nu este corectă,
- Informațiile din certificat au devenit nevalide de la data înregistrării,
- Dispozitivul hardware prezintă semne de deteriorare sau de manipulare neautorizată,
- Dispozitivul hardware funcționează defectuos sau nu poate fi activat,
- Plicul care conține datele de activare secretă (codul PIN) necesare pentru accesarea dispozitivului hardware prezintă semne de acces neautorizat

Obligațiile Subiectului și ale RA în caz de respingere:

- Dispozitivul hardware este returnat către RA
- RA cere revocarea certificatelor,
- RA execută revocarea certificatelor.

4.4.2 Publicarea certificatului de către CA

Vezi capitolul 2.

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

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

4.5 Utilizarea perechii de chei și a certificatului

4.5.1 Utilizarea cheii private și a certificatului

Subiectul este responsabil personal pentru:

- utilizarea cheilor numai pentru uzul prevăzut, așa cum este definit în acest CPP și codat în certificate;
- Cheile private care corespund certificatelor calificate emise în baza acestui CPP vor fi utilizate numai pentru a crea semnături electronice sau sigilii electronice.
- Utilizarea de instrumente care pot interpreta în mod corect utilizarea cheii așa cum este ea codificată în certificat și care respectă condițiile cheie de utilizare
- Utilizarea corectă a dispozitivului hardware
- Nedistribuirea dispozitivului hardware către o altă persoană

- Ștergerea datelor secrete de activare (de exemplu codul PIN) care sunt unice și respectă directivele din CPP
- Păstrând confidențialitatea acestor informații secrete
- Stocarea în siguranță a oricărui document sau a unui mediu care conține transcrierile unei părți sau a tuturor datelor de activare secretă asociate (de exemplu cod PIN)
- Separarea spațiului de stocare pentru dispozitivul hardware și a datelor de activare secretă asociate (de exemplu codul PIN)
- Nedezvăluirea datele de activare secretă (de exemplu codul PIN) unei alte persoane.

Cheia privată generată de CERTSIGN

Atunci când generează cheia privată pentru Subiect, certSIGN este responsabil pentru:

- Inițializarea dispozitivului hardware și a datelor sale de activare secretă asociate inițial (de exemplu cod PIN)
- Distribuirea sigură a dispozitivului hardware către subiect;
- Distribuirea sigură a datelor inițiale asociate secrete necesare activării (de exemplu codul PIN) către subiect.

Subiectul este legat de condițiile și obligațiile menționate în Acordul contractual care referă acest CPP. Subiectul va proteja dispozitivul hardware și orice date de activare secretă asociate (de exemplu cod PIN) sau alte informații împotriva pierderii, furtului, dezvăluirii, compromisului sau modificării.

certSIGN emite certificate pentru cheile stocate pe dispozitiv hardware:

- Cheia privată nu poate fi extrasă din dispozitivul criptografic
- Cheia privată se află sub controlul (exclusiv) al subiectului prin intermediul datelor de activare secretă (de exemplu codul PIN).

Aceste date de activare secrete (de exemplu codul PIN) sunt transmise Beneficiarului folosind un canal aflat în afara benzii și sunt modificate de către Subiect.

Cheia privată generată de Beneficiar

Atunci când cheia privată este generată de Beneficiar, Subiectul este obligat să respecte condițiile și obligațiile menționate în Acordul contractual care includ și acest CPP. Subiectul va proteja dispozitivul hardware sau containerul p12 și certificatele cu orice date de activare secrete asociate (de exemplu cod PIN) sau alte informații, împotriva pierderii, furtului, dezvăluirii, compromisului sau modificării.

Cheia privată generată și stocată de CERTSIGN

Când cheia privată este generată și găzduită de CERTSIGN, există un control tehnic pentru a se asigura că certificatul este valabil în momentul utilizării cheii private.

4.5.2 Utilizarea cheii publice și a certificatului unei Entități Partenere

certSIGN presupune că toate aplicațiile software sunt conforme cu standardul X.509 și alte standarde aplicabile ce impun cerințele și seturile de cerințe menționate în acest CPP. certSIGN nu garantează că software-ul oricărei entități partenere va suporta sau impune

asemenea controale și cerințe, și toate entitățile partenere sunt sfătuite să identifice suport tehnic și legal adecvat.

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

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

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

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

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

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

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

4.6 Reinnoirea certificatului

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

4.7 Rekey-ul certificatului

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

4.7.1 Circumstanțe pentru rekey-ul certificatului

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

4.7.2 Cine poate solicita certificarea unei noi chei publice

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

Rekey-ul se efectuează atunci când un subiect care deține un certificat digital valabil (nu este revocat și nu este expirat) generează o nouă pereche de chei (sau solicită certSIGN să genereze o astfel de pereche de chei) și solicită emiterea unui nou certificat pentru a confirma deținerea unei chei publice nou create.

Rekey-ul certificatului se efectuează numai la solicitarea Subiectului și este precedat de depunerea unei cereri pe un formular corespunzător completat de către Beneficiar/Subiect.

4.7.3 Procesarea cererilor de re-key a certificatelor

RA utilizează aceleași procese ca și pentru un certificat 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 modifică certificatele end-user emise.

Subiectul sau Beneficiarul, după caz, solicită certSIGN să revoce certificatul de îndată ce informațiile incluse în certificat nu mai sunt conforme cu realitatea.

4.9 Revocarea și Suspendarea Certificatului

Certificatele emise de certSIGN Public CA pot fi revocate dar niciodată suspendate.

Revocarea certificatelor este un process 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 Subiectului, după revocare ar trebui să fie stocată în siguranță până când este distrusă.

4.9.1 Circumstanțele revocării unui certificat

Certificatul se revocă atunci când:

- Informația din certificat s-a schimbat,
- O cheie privată asociată unei chei publice din certificat a fost compromisă sau există un motiv serios de a bănuși că a fost compromisă,
- Sunt încheiate relațiile de muncă sau acordurile juridice între Beneficiar și Subiect,
- Subiectul, deținătorul cheii private asociate cheii publice din certificat, solicită revocarea,
- Subiecții / Beneficiarii nu acceptă noii termeni și reglementările modificate ale CPP,
- Autoritatea de Certificare își încetează activitatea, în acest caz toate certificatele emise de această Autoritate de Certificare, înainte de expirarea perioadei declarate pentru încetarea furnizării serviciilor, trebuie revocate împreună cu certificatul Autorității de Certificare,
- Beneficiarul întârzie sau nu plătește valoarea serviciilor furnizate de Certsign Public CA,

- Cheia privată sau securitatea certificatului certSIGN au fost compromise într-un mod care amenință credibilitatea certificatelor,
- CA primește o notificare sau este informat despre orice împrejurare care indica utilizarea ilegală a adresei de email din certificat,
- În alte cazuri în care Subiectul nu respectă regulile prezentului CPP, acordul contractual, Termenii și condițiile sau alte acorduri încheiate între părți în legătură cu serviciile furnizate de Certsign Public CA.

Cheie privată compromisă înseamnă:

- (1) accesul neautorizat la cheia privată sau un motiv întemeiat de a suspecta acest lucru,
- (2) pierderea cheii private sau 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.

CertIFICATELE PE TERMEN SCURT NU SE REVOCĂ.

4.9.2 Cine poate solicita revocarea certificatelor

Următoarele entități pot trimite cereri de revocare a certificatelor:

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

Cererea de revocare poate viza mai multe certificate.

4.9.3 Procedura de revocare a certificatelor

Procedura de trimitere a cererii de revocare este descrisă în capitolul 3.4.

Cererea de revocare a certificatului trebuie să identifice cu precizie fiecare certificat, să conțină motivul (motivele) pentru care se solicită revocarea.

Informațiile despre certificatele revocate sunt înscrise pe Lista Certificatelor Revocare emise de certSIGN Public CA.

Procesarea cererii de revocare a certificatului are loc după cum urmează:

- certSIGN verifică cererea de revocare, inclusiv că este prezentată de o entitate legitimă. Dacă cererea este verificată cu succes, certSIGN Public CA înscrie informațiile referitoare la revocarea certificatului în Lista Certificatelor Revocare (CRL);
- certSIGN notifică subiectul despre revocare sau despre decizia de respingerea cererii, împreună cu motivele acestei respingeri.

Ori de câte ori un certificat sau o cheie privată corespunzătoare unui certificat care urmează să fie revocat stocate pe un dispozitiv hardware, în urma revocării certificatului, dispozitivul este șters în condiții de siguranță. Această acțiune este efectuată de proprietarul dispozitivului hardware - o persoană fizică sau juridică (un reprezentant al unei astfel de entități). Proprietarul dispozitivului hardware trebuie să îl păstreze în siguranță, pentru a preveni furtul sau utilizarea neautorizată până la ștergerea cheii private.

Daca certificatul a fost emis in format PKCS#12 si este revocat, Subiectul îl va păstra în condiții de siguranță sau îl va șterge securizat împreună cu toate copiile sale pentru a preveni utilizarea neautorizată a cheilor.

4.9.4 Perioada de grație a cererii de revocare

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

4.9.5 Timpul în care CA trebuie să proceseze cererea de revocare

certSIGN garantează o perioadă maximă de 24 de ore pentru procesarea unei cereri de revocare a certificatului. În această situație, certificatul este revocat după ce certSIGN primește solicitarea. Atunci când se trimite o cerere autentificată utilizând codul de revocare primit de la certSIGN certificatul este revocat automat.

Informațiile despre revocarea de certificat sunt stocate în baza de date a CERTSIGN. Certificatele revocate sunt plasate în Lista Certificatelor Revocate (CRL) în concordanță cu perioadele de publicare a CRL.

4.9.6 Verificarea cerințelor de revocare pentru Entitățile Partenere

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

4.9.7 Frecvența de emitere 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 către CA-ul care a emis certificatul al cărui status de revocare se verifica.

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

4.9.10 Verificarea on-line a cerințelor de revocare

Vezi capitolul 4.9.6 al prezentului document.

4.9.11 Alte forme disponibile pentru anunțarea revocării

Nu se aplică.

4.9.12 Cerințe speciale în cazul compromiterii re key

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

- Înceteze imediat utilizarea certificatului,
- Inițieze imediat revocarea certificatului,
- Șterga certificatul de pe toate dispozitivele și sistemele,
- Informeze toate părțile terte 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.

4.9.13 Circumstanțe pentru suspendare

Nu se aplică.

4.9.14 Cine poate solicita suspendarea

Nu se aplică.

4.9.15 Procedura de solicitare a suspendării

Nu se aplică.

4.9.16 Limitări ale perioadei de suspendare

Nu se aplică.

4.10 Servicii privind starea certificatelor

4.10.1 Caracteristici operaționale

Serviciile certSIGN de verificare a stării certificatelor sunt CRL și OCSP. Accesul la aceste servicii se realizează prin intermediul site-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.

4.10.2 Disponibilitatea serviciului

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

4.10.3 Elemente opționale

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

4.11 Încetarea acordului contractual

Incetarea acordului contractual se produce după:

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

certSIGN și toate Autoritățile de Înregistrare păstrează toate datele și documentația pentru o perioadă de 10 ani de la expirarea/revocarea certificatului.

4.12 Custodie și recuperare chei

certSIGN nu ofera custodia cheilor pentru certificatele emise de certSIGN Public CA.

4.12.1 Principalele politici și practici în materie de depozit escrow și recuperare

Nu este stipulat.

4.12.2 Politica și practicile de încapsulare și recuperare a cheii de sesiune

Nu este stipulat.

5 Locație, Management și Controale Operaționale

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

Toate acele controale aferente activelor și activităților CA și RA sunt conforme cu cerințele aplicabile din următoarele standarde:

- ETSI EN 319 401, Cerințele generale privind politicile Furnizorilor de Servicii de Încredere,
- ETSI EN 319 411-1, Politica și cerințele de securitate pentru Furnizorii de Servicii de Încredere care emit certificate; Partea 1: Cerințe generale.

5.1 Controale fizice

Rețeaua de sisteme de calcul, 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

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

- un perimetru clar definit și protejat, prin care sunt controlate toate intrările și ieșirile;
- Componentele critice sunt protejate cu mai multe perimetre;
- un sistem de control de intrare, care admite numai acele persoane autorizate în mod corespunzător să intre în zonă;
- Monitorizare cu echipaj uman și electronic a intruziunilor neautorizate, în orice moment;
- Personalul care nu se regăsește pe lista de acces este însoțit și supravegheat în mod corespunzător;
- Un jurnal de acces este întreținut și controlat periodic;
- Echipamentul este întreținut în mod corect pentru a-i asigura disponibilitatea continuă și integritatea.

5.1.2 Accesul fizic

Accesul fizic în cadrul certSIGN este controlat și monitorizat de un sistem de alarmă integrat. certSIGN dispune de sisteme de prevenire a incendiilor, sisteme de detectare a 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 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.

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 cladire toate activitățile să fie disponibile pentru cel puțin 24 de ore cu ajutorul generatorului diesel. Fiecare server, echipament de rețea și toate calculatoarele angajaților care desfășoară activități importante pentru activitățile CA și RA sunt conectate la UPS-uri. Principalele componente ale 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 Aruncarea deșeurilor

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

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

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

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

5.1.8 Stocarea copiilor de siguranță în afara locației

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

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

5.2 Controale procedurale

5.2.1 Roluri de încredere

Toate rolurile implicate în furnizarea serviciilor de certificare ale certSIGN sunt completate cu angajații CERTSIGN.

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

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

Securitatea informațiilor prelucrate de certSIGN și a serviciilor sale este pusă în aplicare prin controale procedurale legate de controlul accesului. Astfel, accesul la informații și la funcțiile de sistem ale aplicațiilor este restricționat în conformitate cu Politica de Control al Accesului. certSIGN administrează drepturile de acces ale operatorilor, administratorilor și auditorilor de sistem, iar administrarea include managementul conturilor utilizatorilor și modificarea la timp sau eliminarea accesului. Sunt furnizate suficiente controale de securitate a calculatoarelor pentru separarea rolurilor de încredere identificate, inclusiv separarea funcțiilor de administrare de securitate și de funcționare. În special, utilizarea de programe utilitare de sistem este limitată și controlată.

certSIGN poate 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/Abonați, 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 sistem** – 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. Nicio entitate care are un rol diferit de cel de auditor nu poate prelua responsabilitățile auditorului.

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

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.

Toate acțiunile angajaților care au roluri de încredere sunt monitorizate.

5.2.4 Rolurile care necesită separarea sarcinilor

certSIGN implementează și impune o separare a rolurilor și a sarcinilor pentru rolurile de Administrator, Operator și Auditor pentru a se asigura că aceeași persoană nu poate deține mai multe roluri. Toate aceste roluri au fișe de post, cu solicitări de abilități și experiența specifice, definite din punctul de vedere al rolurilor îndeplinite. Segregarea sarcinilor și principiul celui mai mic privilegiu sunt aplicabile. Sensibilitatea poziției bazată pe sarcini determină nivelul de acces, screening-ul de fond 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 înțeles și a semnat un contract ce descrie rolul și responsabilitățile sale în cadrul sistemului,
- a beneficiat de un stagiul 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 sensitive 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
- 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.

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.

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 încalcă politicile sau procedurile, realizează acțiuni neautorizate, folosirea neautorizată a autorității și utilizarea neautorizată a sistemelor. Acestea pot include, printre altele, revocarea de privilegii, disciplinare administrativă, sancțiuni reglementate de legislația muncii din România și/sau urmărirea penală.

5.3.7 Cerințele pentru contractanții independenți

Personalul angajat pe baza de contract (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) face obiectul unor verificări similare celor efectuate în cazul angajaților certSIGN (vezi Capitolul 5.3.1, 5.3.2 și 5.3.3). 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 Partener, 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 un server de timp care este sincronizat cu cel puțin două surse de timp care pot fi sateliți GPS sau UTC (NIMB). Ora utilizată pentru înregistrarea evenimentelor necesare în jurnalul de audit este sincronizată cu UTC cel puțin o dată pe zi.

5.4.1 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.

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,
- 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 Subiect / Beneficiar
- orice opțiuni specifice din contract (de exemplu, acceptarea publicării certificatului)
- Identitatea entității care acceptă cererea;
- Metoda utilizată pentru validarea documentelor de identificare,

Accesul la log-uri este permis exclusiv pentru ofițerul de securitate, personal special desemnat, și auditori, prin cerere 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 și fiecare terț delegat păstrează:

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

5.4.4 Protecția jurnalelor de evenimente

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

- Doar 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 Audit collection system (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 to event-causing Subject

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.

5.5 Arhivarea înregistrărilor

Este necesar ca toate datele și fișierele referitoare la înregistrarea informațiilor asociate securității sistemului, cererile trimise de Subiecți/Abonați, informațiile despre Subiecți/Abonați, certificatele emise și CRL-urile, cheile folosite de Autoritățile de Certificare și Înregistrare, și toată corespondența dintre certSIGN și Subiecți/Abonați 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 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 Subiect.

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

5.6 Schimbarea cheilor

Procedurile de Key changeover 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. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed În chapter 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.

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.

5.7.1 Procedurile de administrare a incidentelor și compromiterilor

certSIGN a pus în aplicare o procedură de gestionare a incidentelor de securitate, în scopul de a răspunde rapid și coordonat la incidente și pentru a limita impactul breșelor de securitate. Angajaților le sunt atribuite roluri de încredere pentru a urmări alertele evenimentelor de securitate potențial critice și pentru a se asigura că incidentele relevante sunt raportate în conformitate cu procedura. În cazul defecțiunilor critice se acționează pe baza aceleiași proceduri.

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

În caz de incidente de Securitate, se utilizează procedurile interne. Aceste proceduri includ și notificarea Forului de Supraveghere.

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

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

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

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

Politica de Securitate certSIGN ia în 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 acestuia. 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 rentabil, având în vedere impactul, va fi creat și pus în aplicare un plan pentru a reduce vulnerabilitatea sau va fi documentată baza factuală în sprijinul deciziei certSIGN că vulnerabilitatea nu necesită remediere.

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

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

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

- Notificarea - asupra compromiterii - a tuturor Subiecților / Beneficiarilor și a celorlalte entități cu care certSIGN are acorduri sau alte forme de relații stabilite, între care Entitățile Partenerere și alți Furnizori de Servicii de Încredere. În plus, aceste informații vor fi puse la dispoziția altor Entități Partenerere 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 compromisului cheie CA, certSIGN Root CA G2 va emite un CRL nou în termen de 24 de ore de la primirea notificării privind compromisul și va publica CRL-urile online imediat.

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

Atunci când o cheie privată asociată unei chei publice din certificat a fost compromisă sau există motive serioase pentru a suspecta că aceasta a fost compromisă, Subiectul sau Beneficiarul, după caz, va solicita certSIGN să revocare a certificatului.

5.7.4 Capacități de Continuitate a afacerii în caz de dezastru

certSIGN a stabilit într-un Plan de Continuitate a afacerii (BCP) și un Plan de recuperare în caz de dezastru (DRP) toate măsurile necesare pentru a asigura recuperarea integrală a serviciilor noastre de certificare și marcare temporală în caz de dezastru, sau în cazul unei discontinuități a oricărei componente 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 unui eșec al mediilor de stocare. Activitățile de back-up sunt testate în mod regulat pentru a se asigura că acestea îndeplinesc cerințele planurilor de continuitate a afacerii.

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

Planurile BCP și DRP abordează de asemenea compromiterea, pierderea sau suspiciunea de compromitere a cheii private 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 Subiecților/Beneficiarilor și Entităților Partenere ce pot apărea ca urmare a deciziei unei Autorități de Certificare de a-și înceta activitatea. Planul include obligativitatea notificării Subiecților/Beneficiarilor asupra autorității ce a certificat autoritatea de certificare ce urmează să își înceteze activitatea (daca exista) și translatarea responsabilităților (servicii furnizate către Subiecți/Abonați, 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/Abonații 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 organisme de supraveghere. În plus, această informație va fi făcută disponibilă și altor Entități Partenere;
- Revoca 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 marcarea 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 Subiecților / Beneficiarilor și Entității Partenere;

- Distruge sau retrage din uz cheile private ale CA, inclusiv copiile de rezervă, într-o manieră care să facă imposibilă recuperarea cheilor private;
- Dacă este posibil, se vor realiza anumite înțelegeri pentru a transfera furnizarea de servicii de certificare pentru clienții existenți către un alt furnizor de servicii de certificare.

certSIGN va păstra sau va 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 / sau Subiecților 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 Public CA.

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, depozitările, cheile private și datele de activare pentru cheile private ale Subiecților CA-urilor, și ai altor Participanți PKI, și 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 Public 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 SHA-2 criptografică digest.

certSIGN emite certificate pentru chei stocate pe dispozitive hardware sau în format software.

6.1.1 Generarea perechilor de chei

certSIGN are o procedură documentată pentru efectuarea generării cheilor de CA. 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 dovedeste că a fost efectuată în conformitate cu procedura declarată și că integritatea și confidențialitatea perechii de chei au fost asigurate de către rolul de încredere responsabil pentru securitatea ceremoniei de gestionare a cheilor certSIGN (de exemplu, ofițer de securitate), ca martor că raportul înregistrează corect ceremonia de gestionare a cheilor în timp ce a fost efectuată.

În toate cazurile, CERTSIGN:

- 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 Public CA** precum și cheile altor autorități subordonate și certificarea ulterioară a cheilor publice sunt efectuate într-un mediu fizic securizat de către personal în roluri de încredere, sub cel puțin, control dual:

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

Perechile de chei ale **certSIGN Public CA** 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.

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

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

Generarea 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, abonați, 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 Subiectului sunt generate de către Subiect sau de către CERTSIGN, ambele utilizând un dispozitiv hardware (de exemplu QSCD) sau în format software (container p12 în conformitate cu standardul PKCS12).

certSIGN oferă proceduri tehnice și non-tehnice pentru a șterge în siguranță cheile private subiecților după ce au fost generate de CA și au fost livrate subiectului.

6.1.2 Distribuirea Cheii Private către Beneficiar

Cheia privată generată de CERTSIGN

Atunci cand cheia este generata pe un dispozitiv hardware de catre CERTSIGN, dispozitivul hardware unde este stocat certificatul digital este fie livrat personal Subiectului, fie utilizand serviciile postale sau de curierat. Datele secrete de activare (de exemplu codul PIN) necesare pentru activarea dispozitivului hardware sunt transmise utilizand un plic securizat.

Cand cheile sunt generate in format PKCS#12 de catre CERTSIGN, RA trimite un e-mail Subiectului utilizand adresa de e-mail pusa la dispozitie in procesul de aplicare. E-mail-ul care informeaza Subiectul despre emiterea certificatului contine atasat si certificatul PKCS#12. Datele secrete de activare (de exemplu parola pentru certificatul PKCS#12) sunt transmise catre Beneficiar utilizand un canal off-line.

certSIGN are proceduri tehnice și non-tehnice pentru a șterge în siguranță cheile private ale subiectului după ce au fost generate de către AC și livrate subiectului.

Cheia privată generată de Subiect

Cand cheile sunt generate de catre Subiect, este responsabilitatea acestuia sa utilizeze un dispozitiv hardware adecvat sau instrumente software conforme pentru generarea cheilor in format software, in conformitate cu prevederile prezentului CPP. certSIGN respinge o cerere de certificate ce nu este conforma cu cerintele prezentului CPP.

6.1.3 Distribuirea Cheii Publice către emitentul certificatului

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

Distribuirea unei chei publice nu se aplică în cazul în care o pereche de chei este generată la cererea Subiectului / Beneficiarului de către CERTSIGN, care emite un certificat pentru perechea de chei generate.

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. În cazul autorității de certificare certSIGN Public CA certificatele sunt semnate.

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

Certificatele Autoritatilor de certificare certSIGN pot fi livrate entitatilor partenera 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

Certificatul CA certSIGN utilizează o cheie de 4096 biți pentru certificate și semnarea CRL.

Certificatele digitale emise de certSIGN Public CA utilizează chei RSA de 2048 biți.

Certificatele digitale sunt semnate folosind algoritmul RSA în combinație cu recomandările criptografice SHA-2.

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 curba 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 CA pentru toate CA-urile, inclusiv certSIGN Public CA.

Pentru cheile publice ale Subiectului nu exista o politica specifica implementata privind parametrii de generare a cheilor si parametrii de verificare a calitatii.

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-repudiere de către persoane fizice, cât și pentru alte scopuri decât cele descrise la punctele f) și g). Bitul de ne-repudiere poate fi setat numai într-un certificat de cheie publică cu care se 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.

6.2 Protecția cheii private și controalele modulului criptografic

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

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

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

- ETSI EN 319 401
- ETSI EN 319 411-1

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

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

Cheile Subiectului sunt generate de către Subiect sau de către CERTSIGN, utilizând fie un dispozitiv hardware (de exemplu QSCD) sau în format software.

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

Controlul multi-persoană al unei chei private se aplică cheilor private ale **certSIGN Public 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 eliberat și responsabilitățile care rezultă din păstrarea acestuia în siguranță.

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 Subiectului.

6.2.3 Custodia Cheii Private

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

Cheile private ale subiectului nu sunt supuse custodiei.

6.2.4 Copia de siguranță a cheii private

Autoritățile de Certificare care operează în cadrul certSIGN 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.

Existența unei copii de siguranță a cheii private nu se aplică cheii private a Subiectului.

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 sau după revocarea sa.

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 Autorității de Certificare **certSIGN Public 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 Autoritate de Certificare poate deține o copie criptată a cheii sale private, cheile pot fi de asemenea transferate între module.

6.2.7 Stocarea cheilor private pe modul criptografic

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

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

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

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

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

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

Cheile private ale subiecților sunt stocate pe dispozitive criptografice hardware cryptographic (de exemplu QSCD).

Microcipul încorporat protejează cheile private și alte informații legate de securitate împotriva atacurilor.

6.2.8 Metoda de activare a cheii private

Toate cheile private ale **certSIGN Public CA** sunt introduse în modul după generare, importate sub formă criptată dintr-un alt modul sau restaurate dintr-un secret partajat. Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea este realizată pe baza unui card criptografic deținut de operator.

Cheia privată este stocată pe QSCD, sub controlul Subiectului. Cheia poate fi accesată numai prin utilizarea de date de activare secrete (de exemplu cod PIN).

6.2.9 Metoda de dezactivare a cheii private

Metodele de dezactivare a cheii private **certSIGN Public CA** se referă la dezactivarea cheii după folosirea acesteia sau ca urmare a terminării unei sesiuni în timpul căreia a fost folosită cheia (de exemplu iesirea din aplicație).

Cand este stocată pe un dispozitiv criptografic hardware cheia privată a Subiectului poate fi dezactivată prin deconectarea dispozitivului de la computer sau de la orice alt dispozitiv.

Cand este stocată în format software, deactivarea cheii private a Subiectului depinde de configurația software ce o stochează.

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, pentru a se asigura că aceste chei private nu mai pot fi recuperate sau utilizate niciodată.

Cheia privată CA poate fi distrusă prin ștergerea tuturor cardurilor HSM (Operator și Administrator). În plus, HSM permit resetarea dispozitivului prin acces fizic și setări pe dispozitiv. Aceasta reinitializează dispozitivul și 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. CMPP autorizează distrugerea cheii private a CA și personalul alocat pentru aceasta activitate.

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

Subiectul este responsabil pentru distrugerea cheii private. Pentru cheile stocate pe dispozitive criptografice hardware (de exemplu QSCD) aceasta poate fi efectuată fie utilizând

utilitarul dispozitivului fie prin distrugerea fizică a dispozitivului. Pentru chei stocate în format software Subiectul va șterge (shred) toate copiile pentru a preveni utilizarea neautorizată a cheilor.

6.2.11 Evaluarea Modulului Criptografic

Vezi mai sus.

6.3 Alte aspecte legate de managementul perechilor de chei

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

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

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

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

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

Atributele certificatului **certSIGN Public CA** vor fi compatibile cu utilizarea definită a cheilor, așa cum se prevede în Recomandarea ITU-T X.

6.3.1 Arhivarea cheii publice

certSIGN își arhivează propriile chei publice de CA și toate cheile publice certificate de certSIGN Public CA sub forma de certificate X509 ce 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 Subiectului nu poate depăși perioada de valabilitate a unui certificat.

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

Perioada de valabilitate a unui certificat de Subiect 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.

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.

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 subiecții generează cheile private este responsabilitatea lor să genereze și datele de activare (de exemplu codul PIN).

Atunci când cheile sunt generate de către CERTSIGN, pentru transmiterea datelor de activare (de exemplu codul PIN) către Subiect, sunt utilizate măsuri de securitate adecvate (vezi #6.1.2).

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.

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

6.4.3 Alte aspecte ale datelor de activare

Nu este stipulat.

6.5 Controale de Securitate a computerelor

Sarcinile de lucru ale Autoritatii de Inregistrare si ale Autoritatilor de Certificare ce opereaza in cadrul certSIGN sunt executate prin intermediul mijloacelor hardware si software de incredere.

6.5.1 Cerințe tehnice specifice ale securității calculatoarelor

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 Evaluarea securității calculatoarelor

Sistemul informatic certSIGN îndeplinește cerințele descrise în standardele ETSI: ETSI EN 319 411-2 (Cerințe de politică și de securitate pentru furnizorii de servicii de încredere care eliberează certificate, Partea 2: Cerințe pentru furnizorii de servicii de încredere care eliberează certificate calificate UE) și CEN CWA 14167 (Cerințe de securitate pentru sisteme de încredere care gestionează certificate pentru semnături electronice).

6.6 Controale de securitate specifice ciclului de viață

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

6.6.1 Controale specifice dezvoltării sistemului

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

Înainte de a fi folosită în 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 managementului securității este de a superviza funcționalitatea sistemelor certsign oferind siguranța ca toate sistemele funcționează corect și în conformitate cu configurațiile acceptate și implementate.

Controalele aplicate sistemelor certSIGN permit verificarea continuă a integrității aplicațiilor, a versiunilor acestora precum și autentificarea și verificarea originii hardware-ului.

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 se aplică la politica de securitate CERTSIGN.

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

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 standard a vulnerabilității adreselor IP publice și private identificate de certSIGN și se înregistrează dovezi că fiecare scanare a vulnerabilității a fost realizată de către o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.
- h) Serviciile de certificare ale certSIGN sunt supuse unui test de 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/Abonați și 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 Public CA** se află într-o zonă de înaltă securitate.

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

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

Numele câmpului	Valoarea sau restricțiile valorii	
Version	3	
Serial Number	1001660345dd0680e322	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Department (OU)=	certSIGN ROOT CA G2
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before (validity period beginning date)	Feb 6 09:52:49 2017 GMT	
Not after (validity period end date)	Feb 6 09:52:49 2027 GMT	
Subiect (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	certSIGN Public CA
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Subiect Public Key Info	4096 bits RSA key	
Signature	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	

Table 7.1. Profilul câmpurilor de bază al certSIGN Public CA

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

Numele câmpului	Valoarea sau restricțiile valorii
Version	Version 3

Numele campului	Valoarea sau restricțiile valorii	
Serial Number	Valoare unică mai mare decât zero (0) pentru toate certificatele emise de autoritățile de certificare din cadrul CERTSIGN. Acesta conține o valoare aleatorie de 8 octeți. Pentru generarea acestei valori se utilizează un modul criptografic hardware.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	certSIGN Public CA
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Not before (validity period beginning date)	Universal Time Coordinated based.	
Not after (validity period end date)	Universal Time Coordinated based.	
Subiect (Distinguished Name)	Codificate în conformitate cu RFC 5280, pot conține câmpurile prezentate în capitolul 3.1.2.	
Subiect Public Key Info	Codificate în conformitate cu RFC 5280, pot conține informații despre cheile publice RSA, DSA sau ECDSA (identificatorul cheii, dimensiunea cheii în biți și valoarea cheii publice); Dimensiunea cheii RSA este prezentată în capitolul 6.1.5.	
Signature	Semnătura certificatului, generată și codificată în conformitate cu cerințele descrise în RFC 5280.	

Table 7.2. Profilul câmpurilor de bază ale certificatelor emise de certSIGN Public CA

7.1.1 Numerele de versiune

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

7.1.2 Extensii de certificate

Extensiile certificatelor pentru certSIGN Public CA sunt descrise în Tabelul 7.3.

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/certsign-rootg2.crt	Ne-Critic
Basic Constraints	Subiect type=CA, Path length constraint=0	Critic
Key Usage	keycertSIGN (bit 5), cRLSign (bit 6)	Critic
Authority Key Identifier	82 21 2d 66 c6 d7 a0 e0 15 eb ce 4c 09 77 c4 60 9e 54 6e 03	Ne-Critic
Subiect Key Identifier	b3 85 9c b0 8d f4 d0 6f 54 c0 81 08 ba fc fd 7e 53 5f a9 88	Ne-Critic
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Ne-Critic
CRL Distribution Points	http://crl.certsign.ro/certsign-rootg2.crl	Ne-Critic

Tabel 7.3. Extensiile certificatului certSIGN Public CA

Extensiile certificatelor pentru utilizatorii finali sunt descrise in Tabelul 7.4.1, 7.4.2 si 7.4.3

Extension	Value or Value constraint	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ocsp.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/CERTSIGN-publicca.crt	Ne-Critic
Key Usage	digitalSignature (bit 0) și nonRepudiation (bit 1)	Critic
Authority Key Identifier	b3 85 9c b0 8d f4 d0 6f 54 c0 81 08 ba fc fd 7e 53 5f a9 88	Ne-Critic
Subiect Key Identifier	KeyIdentifier este compus din hash-ul SHA-1 de 160 biți al valorii lui BIT STRING SubiectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizati).	Ne-Critic
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=0.4.0.2042.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.2.{3, 3.1, 3.2, 4, 11, 11.1, 12, 14} [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2,2]* Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=The certificate can be used only in the relationships between the subject and the subscriber. * Această extensie este prezentă numai în certificate cu OID 1.3.6.1.4.1.25017.3.1.2.3.2	Ne-Critic
CRL Distribution Points	http://crl.certsign.ro/certsign-publicca.crl	Ne-Critic
Subiect Alternative Name	Other Name: RFC822 Name and Principal Name (UPN) <i>This extension is optional</i>	Ne-Critic
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) și Document Signing (1.3.6.1.4.1.311.10.3.12)	Ne-Critic

Tabel 7.4.1 Extensiile certificatelor de semnare pentru utilizatori finali

Extension	Value or Value constraint	Extension status
Authority Info Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ocsp.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.certsign.ro/certcrl/CERTSIGN-publicca.crt	Ne-Critic
Key Usage	keyEncipherment (bit 2) și dataEncipherment (bit 3)	Critic
Authority Key Identifier	b3 85 9c b0 8d f4 d0 6f 54 c0 81 08 ba fc fd 7e 53 5f a9 88	Ne-Critic
Subiect Key Identifier	KeyIdentifier este compus din hash-ul SHA-1 de 160 biți al valorii lui BIT STRING SubiectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizati).	Ne-Critic
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=0.4.0.2042.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.2.{7, 8} [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Ne-Critic
CRL Distribution Points	http://crl.certsign.ro/certsign-publicca.crl	Ne-Critic
Subiect Alternative Name	Other Name: RFC822 Name and Principal Name (UPN) <i>This extension is optional</i>	Ne-Critic

Tabel 7.4.2 Extensiile certificatelor de criptare pentru utilizatori finali

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

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Key Usage	digitalSignature (bit 0)	Critic
Authority Key Identifier	b3 85 9c b0 8d f4 d0 6f 54 c0 81 08 ba fc fd 7e 53 5f a9 88	Ne-Critic
Subiect Key Identifier	3c 76 7c 4a 3c 2d 6c 5a 82 c0 2d 62 f9 2e 17 89 e5 55 f0 b6	Ne-Critic
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Ne-Critic
OCSPNoCheck	-	Ne-Critic

Tabel 7.5. Extensiile certificatelor pentru certificatele OCSP

7.1.3 Algoritmul identificatorului obiect

SubjectPublicKeyInfo

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 cu cod hexazecimal: 300d06092a864886f70d0101010500.

Pentru ECDSA, se vor utiliza identificatorii și codificările specificate în #7.1.3.1.2 din CABF BR.

AlgorithmIdentifier al semnăturii

Toate obiectele semnate de o cheie privată CA certSIGN sunt conforme cu cerințele CABF BR #7.1.3.2, RSA sau ECDSA privind utilizarea AlgorithmIdentifier sau a tipului derivat din AlgorithmIdentifier în contextul semnăturilor. În cazul certSIGN, algoritmul utilizat este sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

7.1.4 Formulare de nume

Vezi secțiunea 3.1.

7.1.5 Constrangeri privind numele

Nu se aplica.

7.1.6 Identificatorul de obiect pentru politica de identificare

Certificatele de identificare a obiectului de politică utilizate la nivel de certSIGN Public CA sunt descrise în Tabelele 7.6 și Table 7.7.

Numele politicii de certificare	Identificatorul politicii
certSIGN Public CA	{CERTSIGN} .{id-policy}(3). {id-cp}(1).{id-Public-CA}(2) . <i>subpolicy ID=1.3.6.1.4.1.25017.3.1.2. subpolicy ID</i> See below <i>subpolicyID</i> values.

Tabel 7.6. Identificatorii politicii și numele lor

CA Level	Type	OID
certSIGN Public CA 1.3.6.1.4.1.25017.3.1.2	Certificate ne-calificat	<p><i>Certificate ne-calificat pentru autentificare si semnare</i></p> <ul style="list-style-type: none"> ▪ cu Dispozitiv HW si cheie generata de certSIGN - .3 <ul style="list-style-type: none"> ○ cu Dispozitiv HW si cheie generata si stocata de certSIGN pentru semnatura la distanta si autentificare - 3.1 ○ cu Dispozitiv HW si cheie generata si stocata de certSIGN pentru semnatura la distanta si autentificare care poate fi folosita doar in relatia dintre Subiect si Beneficiar-3.2 ▪ fara Dispozitiv HW si cheie generata de certSIGN -.4 ▪ cu Dispozitiv HW și cheie generată și stocată de certSIGN pentru semnătură la distanță si autentificare, cu pseudonim -.14 <p><i>Certificat ne-calificat pentru criptare</i></p> <ul style="list-style-type: none"> ▪ cu Dispozitiv HW si cheie generata de certSIGN -.7 ▪ fara Dispozitiv HW si cheie generata de certSIGN - .8 <p><i>Certificat ne-calificat pentru sigiliu</i></p> <ul style="list-style-type: none"> ▪ cu Dispozitiv HW si cheie generata de certSIGN - .11 <ul style="list-style-type: none"> ○ cu dispozitiv Dispozitiv HW si cheie generata si stocata de certSIGN pentru sigiliu la distanta- .11.1

CA Level	Type	OID
		<ul style="list-style-type: none"> ▪ fara Dispozitiv HW si cheie generata de certSIGN -.12 OCSP certificate - .13

Tabel 7.7 Identificatori de obiect pentru politica de certificare

7.1.7 Utilizarea extensiei Constrângerii de politică

Nu se aplica.

7.1.8 Sintaxa și semantica calificărilor de politică

certSIGN emite certificate care conțin un calificativ de politică în cadrul extensiei Politicile certificatului. Această extensie conține un calificativ CPP pointer care directează către CPP.

7.1.9 Semantica de procesare pentru extensia Politici critice de certificare

Nu se aplica.

7.2 Profilul CRL

certSIGN Public CA utilizează CRL complete, adică un CRL al cărei domeniu 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, la cel mult 10 zile după **thisUpdate**. Pentru alte CRL-uri, la cel mult 12 luni după **thisUpdate**.

câmpul **revokedCertificates** este prezent în cazul în care CA a emis un certificat care a fost revocat, iar mențiunea corespunzătoare nu a apărut încă în cel puțin un CRL programat periodic după perioada de valabilitate a certificatului revocat. CA va elimina o mențiune pentru un certificat corespunzător după ce acesta a apărut pe cel puțin un CRL programat în mod regulat după perioada de valabilitate a certificatului revocat.

Profilul CRL este descris în Tabelul 7.8.

Nume camp	Valoarea sau restricțiile valorii	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	OrganizationIdentifier (OID: 2.5.4.97) =	VATRO-18288250
	Common Name (CN) =	certSIGN Public CA
	Organization (O) =	certSIGN SA
	Country (C) =	RO
ThisUpdate	Date of CRL issuance	

Nume camp	Valoarea sau restricțiile valorii
NextUpdate	Date of next expected CRL update
Revoked Certificates	List of revoked certificates

Table 7.8 Profilul CRL pentru certSIGN Public 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

ensiile CRL pentru certSIGN Public CA sunt descrise în Tabelul 7.9.

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Authority Key Identifier	b3 85 9c b0 8d f4 d0 6f 54 c0 81 08 ba fc fd 7e 53 5f a9 88	Ne-critic
CRL Number	monotonically increasing sequence number	Ne-critic
ExpiredCertsOnCRL	Generalized Time	Ne-critic

Table 7.9. Extensii CRL ale certSIGN Public CA

serialNumber este identic byte cu byte cu **serialNumber** din certificatul revocat.

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

CA actualizează data revocării dintr-o intrare CRL atunci când se stabilește că cheia privată a certificatului a fost compromisă înainte de data revocării care este indicată în CRL pentru certificatul respectiv. Antedatarea câmpului **revocationDate** este o excepție de la cele mai bune practici descrise în RFC 5280 (secțiunea 5.3.2); câmpul **revocationDate** acceptă implementări care procesează câmpul **revocationDate** ca data la care certificatul este considerat pentru prima dată compromis.

Extensia	Valoarea sau limitarea valorii	Status
serialNumber	serialNumber al certificatului revocat	Non-critical
revocationDate	data certificatului compromis/revocat	Non-critical
crfEntryExtensions	Motivul revocării	Non-critical
CRL Reason	Codul motivului revocării	Non-critical

Tabelul 7.10. Componenta revokedCertificates pentru CA public certSIGN

Extensiile de intrare CRL (crfEntryExtensions) acceptate de certSIGN conțin următoarele câmpuri: **ReasonCode**: codul motivului revocării. Acest câmp este necritic, permițând determinarea motivului revocării certificatului. Sunt permise următoarele motive de revocare a certificatului:

- 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".
- 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)⁶
 - 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 trebuie să conțină extensia extKeyUsage, descrisă în RFC 5280.

⁶ *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*

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

De asemenea, certificatul serverului OCSP conține extensia OCSPNoCheck, descrisă de RFC 6960. Această extensie trebuie 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

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

8 Auditul de conformitate și alte evaluări

8.1 Frecvența sau circumstanțele de evaluare

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

Auditul verifică conformitatea cu standardele tehnice CPP și ETSI 319 401 și ETSI 319 411.

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

8.2 Identitatea / calificările evaluatorului

Evaluarea va fi efectuată de un organism de evaluare a conformității, astfel cum este definit în Regulamentul UE 910/2014.

Legat de conformitatea / calificările evaluatorului, operarea consistentă și imparțialitatea atestării efectuate de corpurile de conformitate ce evaluează și certifică conformitatea noastră ca și furnizori de servicii de certificare și conformitatea serviciilor noastre de certificare conform Regulamentului 910/2014 și a actelor de implementare, noi urmărim cerințele din standardul ETSI EN 319 401.

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 CPP Public CA.

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 și de securitate (evaluări, rapoarte etc)
- securitate procedurală (actualizare fișe post personal cu atribuții 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 CMPP.

9 Alte elemente de afaceri și legale

9.1 Tarife

Tarifele serviciilor de certificare și ale altor categorii de servicii 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 stabilite conform politicii interne de preț.

9.1.4 Tarife pentru alte servicii

Prețurile sunt stabilite conform politicii interne de preț.

9.1.5 Rambursarea plăților

Plățile pot fi rambursate conform condițiilor contractuale aplicabile..

9.2 Răspunderea financiară

9.2.1 Acoperirea prin asigurare

certSIGN 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 calificate emise de certSIGN Public 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

Nu este stipulat.

9.3 Confidențialitatea informațiilor de afaceri

9.3.1 Scopul informațiilor confidențiale

Toate informațiile referitoare la Subiect/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 Subiect, 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 Subiecți / 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 Subiecții / 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, Subiectul), cu excepția informațiilor incluse în certificate sau din 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 interne și externe, dacă acestea reprezintă o amenințare pentru securitatea CERTSIGN;
- 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 Subiectul, 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 Subiect /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 Subiect / Beneficiar pot fi puse la dispoziția altor entități, doar cu acordul scris al Subiectului / Beneficiarului și în scopul menționat în contractul încheiat cu Subiectul / 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 informațiilor personale

În prestarea serviciilor de încredere certSIGN prelucrează date cu caracter personal ale Subiectului/Beneficiarului în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea 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 / subiectul, atunci când sunt schimbate între componentele sistemului CERTSIGN, precum și atunci când sunt depozitate.

9.4.2 Informații considerate ca fiind cu caracter personal

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

9.4.3 Informații care nu sunt considerate private

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

9.4.4 Responsabilitatea de a proteja informațiile private

certSIGN și angajații săi, se angajează să păstreze confidențialitatea informațiilor 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 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 Subiectii/Beneficiarii sunt informați despre necesitatea utilizării datelor cu caracter personal care le aparțin, în vederea prestării serviciului și necesitatea acordării consimțământului. Dacă persoanele vizate nu sunt de acord ca certSIGN să le prelucreze date, nu pot beneficia de serviciile de certificare.

De asemenea, Subiectii/Beneficiarii au posibilitatea de a opta explicit pentru utilizarea datelor cu caracter personal pentru alte scopuri comunicate în mod expres de certSIGN prin contract sau în alt mod.

9.4.6 Divulgare ca urmare a unui proces administrativ sau juridic

certSIGN este exonerat de răspundere pentru dezvăluirea datelor cu caracter personal ale Subiectilor/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 Subiectului/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 Subiectului/Beneficiarului;
- ✓ în orice alte situații justificate cu înștiințarea în prealabil a Subiectului/Beneficiarului.

9.5 Drepturile de Proprietate Intelectuală

Toate mărcile, patentele, siglele, licențele, aplicațiile, 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, aplicațiile, 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

certSIGN emite certificate compatibile X509 v3.

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

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

9.6.2 Reprezentările și garanțiile RA

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

9.6.3 Reprezentările și garanțiile Beneficiarului

Subiectul acceptă Termenii și Condițiile relevante pentru serviciul furnizat de CERTSIGN.

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

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

9.6.4 Reprezentările și garanțiile Entităților Partenerere

Exemplele de obligații și responsabilități ale Entităților Partenerere 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 altă parte decât în CPP, în CP-ul aplicabil și în legislația aplicabilă, certSIGN neagă toate garanțiile și obligațiile de orice tip, inclusiv orice garanție de comercializare, orice garanție de adecvare pentru un anumit scop, precum și orice garanție a exactității informațiilor oferite (cu excepția faptului că a venit dintr-o sursă autorizată) și nu își asumă nicio răspundere pentru neglijența și neatenția Subiecților, Beneficiarilor și Entităților Partenerere.

9.8 Limitarea răspunderii

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

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

CertSIGN nu răspunde față de nicio o persoană (beneficiar, subiect, terț, entitate parteneră etc.) în cazul în care datele prezentate la emiterea certificatelor sunt false, inexacte, incomplete sau expirate sau sunt prezentate acte de identitate false. certSIGN nu răspunde pentru daunele suportate de Beneficiar sau terți provocate de utilizarea certificatelor emise de certSIGN de către Subiect.

În orice caz răspunderea certSIGN în cazul unei cereri de despăgubire va fi limitată la valoarea certificatelor implicate în producerea unui prejudiciu.

9.9 Despăgubiri

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

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 Încetarea

Prezentul 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 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 a fi transmise într-o anumită formă, 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 (CMPP) și Procedurilor, de aprobarea și modificarea prezentului CPP. CPP-se revizuieste cel puțin odata pe an.

Singurele modificări pe care le poate face CMPP acestor specificații CPP fără notificare sunt modificări minore care nu afectează nivelul de încredere al acestui CPP, de exemplu, corecturi editoriale sau tipografice sau modificări ale detaliilor de contact.

Erorile, actualizările sau sugestiile de modifica a acestui document vor fi comunicate așa cum este menționat în prezentul CPP, secțiunea 1.5.4. O astfel de comunicare va include o descriere a schimbării, o justificare a schimbării, precum și informațiile de contact ale persoanei care solicită modificarea.

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

Orice modificări la CPP sunt aprobate de CMPP și sunt anunțate clienților CERTSIGN. Subiectii/Beneficiarii trebuie să respecte numai cerințele CPP aplicabile în prezent.

9.12.2 Mecanismul de notificare și perioada

Toate modificările aduse prezentului CPP aflate în analiza CMPP vor fi distribuite 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 (cu excluderea oricui conflict de legi care ar determina aplicarea altor legi naționale sau internaționale).

9.15 Conformitatea cu legea aplicabilă

Prezentul CPP și furnizarea serviciilor certSIGN sunt conforme cu legile române relevante și aplicabile și Regulamentul UE 910/2014.

9.16 Prevederi diverse

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

9.16.1 Acordul integral

Nu este stipulat.

9.16.2 Cesiunea

Nu este stipulat.

9.16.3 Separabilitate

Nu este stipulat.

9.16.4 Executarea (onorariile avocaților și renunțarea la drepturi)

Nu este stipulat.

9.16.5 Forța majoră

CA acționează în conformitate cu legile României privind forța majoră.

9.17 Alte prevederi

Nu este stipulat.