Codul de Practici și Proceduri certSIGN Web CA G2 pentru certificate de autentificare a site-urilor Web

Versiunea 1.0

Data: 22 Ian.2026

Notă importantă

Adresa: Bd. Tudor Vladimirescu, nr. 29 A,

AFI Tech Park 1, București 050881, România

Telefon: 004-021-31.19.901

Web: www.certsign.ro

Istoric document

Versiune	Data efectivă	Motiv	Persoana care a făcut modificarea
1.0	22 Ianuarie 2026	Prima versiune	Manager politici PKI

Acest document a fost creat de către și este proprietatea:

Proprietar	Autor	Data creării
BU Servicii de Incredere	Ofițer Securitate Informatică	Ianuarie 2026

Lista de distribuție

Destinație	Data distribuirii
Public-Internet	Ianuarie 2026

Acest document a fost aprobat de:

Versiune	Nume	Data
1.0	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2026

Cuprins

1 Introducere 9
1.1 Descriere generală a CPP 9
1.2 Denumirea documentului și identificarea acestuia 9
1.3 Participantii PKI 10
1.3.1 Autoritățile de certificare 10
1.3.2 Autoritatea de Înregistrare 11
1.3.3 Beneficiarii 11
1.3.4 Entitățile Partenere 12
1.3.5 Alți participanți 12
1.4 Utilizarea certificatului 12
1.4.1 Utilizări admise ale certificatului 12
1.4.2 Utilizari interzise ale certificatului 13
1.5 Administrarea politicii 13
1.5.1 Organizația care administrează documentul 13
1.5.2 Persoana de contact 14
1.5.3 Persoana care decide conformitatea CPP cu politica 14
1.5.4 Procedurile de aprobare a CPP 14
1.6 Definiții și acronime 15
1.6.1 Definiții 15
1.6.2 Acronime 26
2 Publicare și responsabilități Depozitar 29
2.1 Depozitare 29
2.2 Publicarea informațiilor de certificare 29
2.3 Timpul sau frecvența publicării 30
2.4 Controlul accesului la Depozitare 30
3 Identificarea și autentificarea 31
3.1 Nume 31
3.1.1 Tipuri de nume 31
3.1.2 Nevoia ca Numele să aibă înțeles logic 31
3.1.3 Anonimitatea sau pseudonimitatea beneficiarilor 32
3.1.4 Reguli de interpretare a diferitelor formate de nume 32
3.1.5 Unicitatea numelor 33
3.1.6 Recunoașterea, autentificarea și rolul mărcilor înregistrate 33
3.2 Validarea Inițială a Identității 33
3.2.1 Dovada Posesiei Cheii Private 33
3.2.2 Autentificarea identității organizației 33
3.2.3 Autentificarea identității persoanelor fizice 42
3.2.4 Informații neverificate ale Beneficiarului 42
3.2.5 Validarea autorității 42
3.2.6 Criterii pentru interoperare 45
3.3 Identificarea și autentificarea pentru cererile de re-key 45
3.3.1 Identificarea și autentificare pentru re-key de rutină 45
3.3.2 Identificarea și autentificarea pentru re-key după revocare 45
3.4 Identificarea și autentificarea pentru cererile de revocare 45
4 Cerințe operaționale privind ciclul de viață al certificatului 46
4.1 Cererea de certificat 46

4.1.1 Cine poate trimite o cerere de certificate 46
4.1.2 Procesul de înregistrare și responsibilitățile 46
4.2 Procesarea cererilor de certificate 48
4.2.1 Îndeplinirea funcțiilor de identificare și autentificare 50
4.2.2 Aprobarea sau respingerea cererilor de certificate 50
4.2.3 Timpul de proceare a cererilor de certificate 52
4.3 Emiterea certificatelor 52
4.3.1 Acțiunile CA în timpul emiterii certificatelor 52
4.3.2 Notificarea Beneficiarului de către CA cu privire la emiterea certificatului 53
4.4 Acceptarea certificatului 53
4.4.1 Conduita care constituie acceptarea certificatului 53
4.4.2 Publicarea certificatului de către CA 54
4.4.3 Notificarea de către CA a altor entități cu privire la emiterea certificatului 54
4.5 Utilizarea perechii de chei și a certificatului 54
4.5.1 Utilizarea cheii private și a certificatului Beneficiarului 54
4.5.2 Utilizarea cheii publice și a certificatului unei Entități Partenere 54
4.6 Reinnoirea certificatului 55
4.6.1 Circumstanța reînnoirii certificatului 55
4.6.2 Cine poate solicita reînnoirea 55
4.6.3 Procesarea solicitărilor de reînnoire a certificatelor 55
4.6.4 Notificarea abonatului cu privire la eliberarea unui nou certificat 55
4.6.5 Conduita care constituie acceptarea unui certificat de reînnoire 55
4.6.6 Publicarea certificatului de reînnoire de către CA 56
4.6.7 Notificarea eliberării certificatului de către CA către alte entități 56
4.7 Rekey-ul certificatului 56
4.7.1 Circumstante pentru rekey-ul certificatului 56
4.7.2 Cine poate solicita certificarea unei noi chei publice 56
4.7.3 Procesarea cererilor de re-key a certificatelor 56
4.7.4 Notificarea emiterii noului certificat către Beneficiar 56
4.7.5 Conduita ce constitue acceptarea unui certificate re-key 56
4.7.6 Publicarea certificatului re-key de către CA 56
4.7.7 Notificarea eliberării certificatului de către CA altor entități 56
4.8 Modificarea Certificatului 56
4.8.1 Circumstanța modificării certificatului 56
4.8.2 Cine poate solicita modificarea 57
4.8.3 Procesarea cererilor de modificare a certificatului 57
4.8.4 Notificarea abonatului cu privire la eliberarea unui nou certificat 57
4.8.5 Conduita care constituie acceptarea unui certificat modificat 57
4.8.6 Publicarea certificatului modificat de către CA 57
4.8.7 Notificarea eliberării certificatului de către CA către alte entități 57
4.9 Revocarea și Suspendarea certificatului 57
4.9.1 Circumstanțele revocării unui certificat 57
4.9.2 Cine poate solicita revocarea certificatelor 59
4.9.3 Procedura de revocare a certificatelor 59
4.9.4 Perioada de grație a cererii de revocare 60
4.9.5 Timpul în care CA trebuie să proceseze cererea de revocare 60
4.9.6 Verificarea cerințelor de revocare pentru Entitățile Partenere 60
4.9.7 Frecvența de emitere a CRL-urilor 61

4.9.8 Latența maximă pentru CRL-uri 61
4.9.9 Disponibilitatea verificării on-line a revocării/stării 61
4.9.10 Verificarea on-line a cerințelor de revocare 62
4.9.11 Alte forme disponibile pentru anunțarea revocării 62
4.9.12 Cerințe speciale în cazul compromiterii cheii 62
4.9.13 Circumstanțe pentru suspendare 62
4.9.14 Cine poate solicita suspendarea 62
4.9.15 Procedura de solicitare a suspendării 62
4.9.16 Limitări ale perioadei de suspendare 62
4.10 Servicii privind starea certificatelor 62
4.10.1 Caracteristici operaționale 62
4.10.2 Disponibilitatea serviciului 62
4.10.3 Elemente opționale 63
4.11 Încetarea abonamentului 63
4.12 Custodie și recuperare chei 63
4.12.1 Principalele politici și practici de escrow și recuperare 63
4.12.2 Politica și practicile cheie de încapsulare și recuperare a sesiunii 63
5 Facilitate, Management și Controale Operaționale 64
5.1 Controale fizice 65
5.1.1 Amplasarea și construcția sediului 65
5.1.2 Accesul fizic 66
5.1.3 Alimetarea cu curent și aerul conditionat 66
5.1.4 Expunerea la apă 67
5.1.5 Prevenirea și protecția împotriva incendiilor 67
5.1.6 Depozitarea mediilor de stocare a informaţiilor 67
5.1.7 Aruncarea deșeurilor 67
5.1.8 Stocarea copiilor de siguranță în afara locației 67
5.2 Controale procedurale 67
5.2.1 Roluri de încredere 67
5.2.2 Numărul de persoane necesare pentru fiecare sarcină 69
5.2.3 Identificarea și autentificarea pentru fiecare rol 69
5.2.4 Rolurile care necesită separarea sarcinilor 70
5.3 Controlul personalului 70
5.3.1 Calificări, experință și aprobări necesare 70
5.3.2 Proceduri de verificare a antecedentelor 70
5.3.3 Cerinţele de pregătire a personalului 70
5.3.4 Frecvența instruirilor și cerințe 71
5.3.5 Frecvența și secvența rotației posturilor 71
5.3.6 Sancțiunile pentru acțiunile neautorizate 71
5.3.7 Cerințele pentru contractanții independenți 71
5.3.8 Documentația oferită personalului 71
5.4 Procedurile de înregistrare a datelor de audit 72
5.4.1 Evenimente Înregistrate 72
5.4.2 Frecvența procesării jurnalelor de evenimente 74
5.4.3 Perioada de pastrare a log-urilor de audit 74
5.4.4 Protecția jurnalelor de evenimente 74
5.4.5 Procedura de backup a log-urilor 75
5.4.6 Audit collection system (internal vs. external) 75

5.4.7 Notification to event-causing subject 75
5.4.8 Evaluări de vulnerabilitate 75
5.5 Arhivarea înregistrărilor 76
5.5.1 Tipuri de date arhivate 76
5.5.2 Perioada de retenție a arhivei 77
5.5.3 Protecția arhivei 77
5.5.4 Procedurile de back-up al arhivei 77
5.5.5 Cerințe privind marcarea temporală a înregistrărilor 77
5.5.6 Sistemul de colectare al arhivei (intern sau extern) 78
5.5.7 Procedura de obținere și verificare a informațiilor arhivate 78
5.6 Schimbarea cheilor 78
5.7 Compromiterea și recuperare în caz de dezastru 78
5.7.1 Procedurile de administrare a a incidentelor și compromiterilor 78
5.7.2 Compromiterea resurselor de calcul, a aplicațiilor software și/sau datelor 79
5.7.3 Proceduri care se aplică la compromiterea cheii private a unei entitati 80
5.7.4 Capacități de Continuitate a afacerii în caz de dezastru 81
5.8 Încetarea activității Autorității de Certificare sau a Autorității de Înregistrare 81
5.9 Lanțul de aprovizionare 83
6 Controale tehnice de securitate 83
6.1 Generarea și instalarea perechii de chei 83
6.1.1 Generarea perechilor de chei 84
6.1.2 Distribuirea Cheii Private către Beneficiar 85
6.1.3 Distribuirea Cheii Publice către emitentul certificatului 85
6.1.4 Distribuirea Cheii Publice a Autorității Certificare către Entitățile Partenere 85
6.1.5 Marimea cheilor 86
6.1.6 Parametrii de generare a Cheilor Publice și verificarea calității 86
6.1.7 Scopurile în care pot fi utilizate cheile (cf câmpului de utilizare a cheilor X.509 v3) 86
6.2 Protecția cheii private și controalele modulului criptografic 87
6.2.1 Controalele și standardele modulelor criptografice 87
6.2.2 Control multi-persoană (n din m) al cheilor private 87
6.2.3 Custodia Cheii Private 88
6.2.4 Copia de siguranță a cheii private 89
6.2.5 Arhivarea Cheii Private 89
6.2.6 Transferul Cheii Private într-un sau dintr-un modul criptografic 89
6.2.7 Stocarea cheilor private pe modul criptografic 90
6.2.8 Metoda de activare a cheii private 90
6.2.9 Metoda de dezactivare a cheii private 90
6.2.10 Metoda de distrugere a cheii private 90
6.2.11 Evaluarea Modulului Criptografic 91
6.3 Alte aspect legate de managementul perechilor de chei 91
6.3.1 Arhivarea cheilor publice 91
6.3.2 Perioadele operaționale ale certificatelor și perioadele de utilizare a cheilor private 91
6.4 Datele de activare 92
6.4.1 Generarea și instalarea datelor de activare 92
6.4.2 Protejarea datelor de activare 92
6.4.3 Alte aspect ale datelor de activare 93

6.5 Controale de Securitate ale computerelor 93
6.5.1 Cerințe tehnice specifice ale securității calculatoarelor 93
6.5.2 Computer security rating 94
6.6 Controale tehnice specifice ciclului de viață 94
6.6.1 Controale specifice dezvoltării sistemului 94
6.6.2 Controale specifice managementului securității 94
6.6.3 Controale de securitate specifice ciclului de viață 94
6.7 Controale de securitate a rețelei 95
6.8 Marcare temporala 96
6.9 Elementele de control specifice modulelor criptografice 97
7 Profilul certificatelor, CRL și OCSP 98
7.1 Profilul certificatului 98
7.1.1 Numerele de versiune 101
7.1.2 Extensii de certificate 101
7.1.3 Obiecte de identificare a algoritmului 108
7.1.4 Formulare de nume 109
7.1.5 Constrangeri privind numele 109
7.1.6 Obiecte de identificare a politicii certificatelor 109
7.1.7 Utilizarea extensiei Constrângeri de politică 111
7.1.8 Sintaxa și semantica atributelor de politică 111
7.1.9 Semantica de procesare pentru extensia Politici critice de certificare 111
7.2 Profilul CRL 111
7.2.1 Numerele de versiune 112
7.2.2 CRL și extensiile de intrare CRL 112
7.3 Profilul OCSP 113
7.3.1 Numarul versiunilor 114
7.3.2 Extensii OCSP 114
8 Auditul de conformitate și alte evaluări 115
8.1 Frecvența sau circumstanțele de evaluare 115
8.2 Identitatea / calificările evaluatorului 115
8.3 Relația evaluatorului cu entitatea evaluată 115
8.4 Subiectele acoperite de evaluare 115
8.5 Acțiuni întreprinse ca urmare a deficienței 116
8.6 Comunicarea rezultatelor 116
8.7 Audituri interne 116
9 Alte elemente de afaceri și legale 118
9.1 Tarife 118
9.1.1 Tarifele serviciilor de emitere și reînnoire a certificatelor 118
9.1.2 Tarifele serviciilor de acces la certificate 118
9.1.3 Tarifele serviciilor de revocare sau acces la informațiile despre starea certificatelor 118
9.1.4 Taxe pentru alte servicii 118
9.1.5 Politica de rambursare 118
9.2 Răspunderea financiară 118
9.2.1 Acoperirea prin asigurare 118
9.2.2 Alte active 118
9.2.3 Asigurarea sau acoperirea garanției pentru entitățile finale 119
9.3 Confidențialitatea informațiilor de afaceri 119

9.3.1 Scopul informatiilor confidentiale 119
9.3.2 Informații care nu sunt considerate a fi confidențiale 120
9.3.3 Responsibilitatea de a proteja informațiile confidențiale 120
9.4 Confidențialitatea datelor cu caracter personal 120
9.4.1 Planul de asigurare a protectiei datelor cu caracter personal 120
9.4.2 Informatii considerate ca fiind cu caracter personal 121
9.4.3 Informații care nu sunt considerate cu caracter personal 121
9.4.4 Responsabilitatea de a proteja datele cu caracter personal 121
9.4.5 Notificarea persoanelor vizate si consimtamantul acestora pentru utilizarea datelor cu caracter personal 121
9.4.6 Divulgare ca urmare a unui process administrativ sau juridic 121
9.4.7 Alte circumstante pentru divulgare 121
9.5 Drepturile de Proprietate Intelectuală 122
9.6 Reprezentări și garanții 122
9.6.1 Reprezentările și garanțiile CA 122
9.6.2 Reprezentările și garanțiile RA 122
9.6.3 Reprezentările și garanțiile Beneficiarului 122
9.6.4 Reprezentările și garanțiile Entităților Partenere 123
9.6.5 Reprezentările și garanțiile altor participanti 123
9.7 Exonerarea de răspundere privind garanțiile 123
9.8 Limitarea răspunderii 123
9.9 Despagubiri 123
9.10 Termenii și încetarea 124
9.10.1 Termenii 124
9.10.2 Incetarea 124
9.10.3 Efectul terminării și supraviețuirii 124
9.11 Notificări individuale și comunicarea cu participanții 124
9.12 Amendamente 124
9.12.1 Procedura pentru amendamente 124
9.12.2 Mecanismul de notificare și perioada 125
9.12.3 Circumstanțele în care OID trebuie schimbat 125
9.13 Procedurile de soluționare a litigiilor 125
9.14 Legea aplicabilă 125
9.15 Conformitatea cu legea aplicabilă 125
9.16 Prevederi diverse 125
9.16.1 Întregul acord 125
9.16.2 Cesiunea 125
9.16.3 Anulabilitate 125
9.16.4 Executarea (onorariile avocaților și renunțarea la drepturi) 125
9.16.5 Forta Majora 125
9.17 Alte prevederi 125

1 Introducere

Codul de Practici și Proceduri certSIGN Web CA G2 pentru certificate de autentificare a site-urilor Web (denumit în continuare **CPP**) descrie în detaliu politica de certificare și practicile pe care certSIGN le aplică în emiterea de certificate calificate de catre Autoritățile de certificare Web CA G2 subordonate.

Structura și conținutul CPP respectă recomandările RFC 3647 și ultimele versiuni publicate:

- ETSI EN 319 411-1 (Politica DVCP - 0.4.0.2042.1.6, Politica OVCP - 0.4.0.2042.1.7, Politica EVCP - 0.4.0.2042.1.4)
- ETSI EN 319 411-2 (Politica QEVCP-w - 0.4.0.194112.1.4)
- CA/B Forum Baseline Requirements (Politica DV - 2.23.140.1.2.1, Politica OV - 2.23.140.1.2.2 și Extensia CABF - 2.23.140.3.1)
- CA/Browser Forum EV TLS Certificate Guidelines (Politica EV - 2.23.140.1.1)
- CA/Browser Forum Network and Certificate System Security Requirements
- WebTrust Principles and Criteria for Certification Authorities
- Webtrust Principles and Criteria for Certification Authorities - TLS Baseline
- Webtrust Principles and Criteria for Certification Authorities – Network Security
- Mozilla Root Store Policy,
- Apple Root Certificate Program,
- Microsoft Trusted Root Program,
- Chrome Root Program Policy.

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

1.1 Descriere generală a CPP

CPP reprezinta documentul de baza pentru functionarea **certSIGN** și a **Autoritatii de Certificare**, **Autoritatii de Inregistrare și a Entitatilor Partenere** privind emiterea de certificate calificate pentru autentificarea site-urilor web. De asemenea, acest document descrie regulile de prestare a serviciilor de certificare cum ar fi înregistrarea Beneficiarilor, certificarea cheilor publice, înnoirea cheilor şi revocarea certificatelor.

1.2 Denumirea documentului și identificarea acestuia

Acest document este denumit **Codul de Practici și Proceduri certSIGN Web CA G2 pentru Certificate Calificate de autentificare a Site-urilor Web ,** denumit în continuare **CPP**.

Următorii identificatori ai politicii de certificare sunt rezervați utilizării de către certSIGN Web CA G2 pentru a afirma conformitatea cu acest document după cum urmează:

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) certSIGN (25017) id-cp (3) certSIGN ROOT CA G2 (1) certSIGN Web CA G2 (5) } (1.3.6.1.4.1.25017.3.1.5)

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) certSIGN (25017) id-cp (3) certSIGN ROOT CA G2 (1) certSIGN Web CA G2 (5) qualified website authentication certificate (1)} (1.3.6.1.4.1.25017.3.1.5.1)

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) certSIGN (25017) id-cp (3) certSIGN ROOT CA G2 (1) certSIGN Web CA G2 (5) organization validated website authentication certificate (2)} (1.3.6.1.4.1.25017.3.1.5.2)

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) certSIGN (25017) id-cp (3) certSIGN ROOT CA G2 (1) certSIGN Web CA G2 (5) OCSP (3)} (1.3.6.1.4.1.25017.3.1.5.3)

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) certSIGN (25017) id-cp (3) certSIGN ROOT CA G2 (1) certSIGN Web CA G2 (5) qualified website authentication certificate for PSD2 (4)} (1.3.6.1.4.1.25017.3.1.5.4)

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) certSIGN (25017) id-cp (3) certSIGN ROOT CA G2 (1) certSIGN Web CA G2 (5) domain validated website authentication certificate (5)} (1.3.6.1.4.1.25017.3.1.5.5)

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) certSIGN (25017) id-cp (3) certSIGN ROOT CA G2 (1) certSIGN Web CA G2 (5) extended validation website authentication certificate (6)} (1.3.6.1.4.1.25017.3.1.5.6)

Versiunea electronica a acestui document este disponibila În Depozitar la adresa: https://www.certsign.ro/ro/document/certsign-web-ca-G2-cod-practici-si-proceduri/.

1.3 Participantii PKI

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

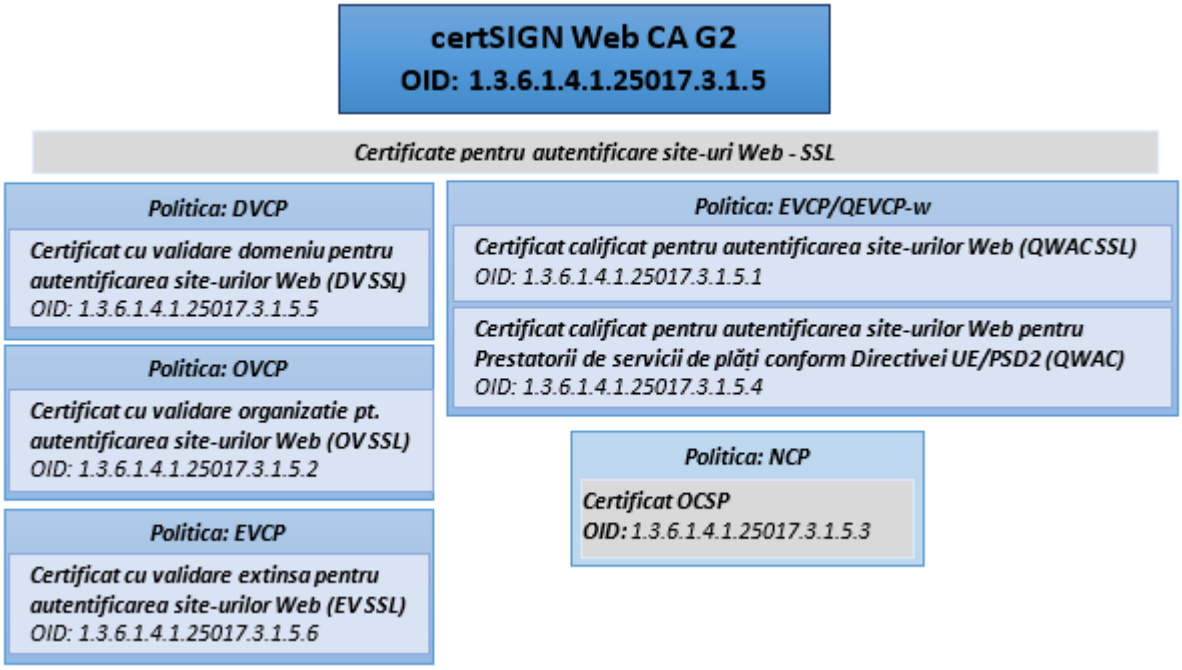
- certSIGN Web CA G2
- Autoritatea de Înregistrare,
- Depozitar,
- Online certificate status protocol (OCSP),
- Subiecții,
- Beneficiarii,
- Entitățile Partenere,
- Furnizorii relevanți ai certSIGN din punct de vedere al emiterii și managementului certificatelor digitale,
- Comitetul de Management al Politicilor și Procedurilor.
- Auditori

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

1.3.1 Autoritățile de certificare

certSIGN Web CA G2 este Autoritate de certificare pentru domeniul certSIGN, subordonata **certSIGN ROOT CA G2**.

certSIGN Web CA G2 este identificat prin urmatorul **OID: 1.3.6.1.4.1.25017.3.1.5**



1.3.2 Autoritatea de Înregistrare

Autoritatea de Înregistrare primeşte, verifică şi aprobă sau respinge cererile de înregistrare şi 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, cât şi a datelor incluse în cerere. Autoritatea de Înregistrare poate trimite cereri către Autoritatea de Certificare corespunzătoare pentru a anula o cerere sau pentru a retrage un certificat.

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

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

1.3.3 Beneficiarii

Beneficiar

Beneficiarii sunt persoane juridice cărora li se emite un certificat și care sunt obligați legal printr-un acord contractual.. Beneficiarii pot solicita eliberarea, revocarea sau re-key-ul certificatelor entității finale pentru subiecții aflați în grija lor.

Beneficiarul este responsabil de:

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

Subiect

Subiectul este un dispozitiv aflat sub controlul si funcționarea Beneficiarului.

1.3.4 Entitățile Partenere

O Entitate Parteneră care folosește serviciile certSIGN poate fi orice entitate care 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, pentru a verifica identitatea sursei sau autorul unui mesaj sau pentru a crea un canal de comunicare securizat cu Beneficiarul 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 este un Comitet creat în cadrul certSIGN de către Consiliul de administrație pentru a supraveghea înreaga activitate a Autorităților de Certificare și a Autorităților de Înregistrare ale certSIGN. Rolurile și responsabilitățile CMPP sunt descrise în documentația internă.

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

1.4 Utilizarea certificatului

Scopul principal al certificatelor DV (Domain Validated), OV (Organization Validated), EV (Extended Validation) și QWAC (Qualified Web) este autentificarea site-urilor web.

Scopul specific al Certificatelor Calificate cu Validare Extinsa pentru Autentificarea Site-urilor Web (QWAC) este descris în Regulamentul EU 1183/2024.

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

- Unul care defineşte aplicabilitatea certificatului
- Și unul care presupune o listă sau o descriere a aplicaţiilor permise sau interzise.

Entitatea parteneră este responsabilă pentru stabilirea nivelului de credibilitate necesar unui certificat utilizat pentru un anumit scop. Luând în considerare factorii de risc semnificanți, Entitatea Parteneră va decide ce tip de certificat emis de certSIGN răspunde cererilor formulate.

1.4.1 Utilizări admise ale certificatului

Certificatele emise de certSIGN Web CA G2 se folosesc pentru autentificarea serverului TLS.

Certificatele DV și OV pot fi utilizate în servere și aplicații web care îndeplinesc cel puțin următoarele condiții:

- Gestionarea corespunzătoare a cheilor publice și private,
- Certificatele și cheile publice asociate sunt utilizate în conformitate cu scopul lor declarat, confirmat de certSIGN,
- Dispun de mecanisme integrate de verificare a stării certificatelor, de creare a căilor de certificare și de control al validării (disponibilitatea semnăturii, data expirării etc.),
- Furnizează utilizatorilor informații relevante privind certificatele și statutul acestora.

Scopul principal al certificatelor EV/QWAC este să:

1. Identifice persoana juridică care controlează un site Web: Furnizează o asigurare rezonabilă pentru utilizatorul unui browser de internet că site-ul web pe care îl accesează este controlat de o entitate juridică specifică identificată în EV/QWAC după numele, adresa sediului social, Jurisdicția de înmatriculare sau Numărul de înregistrare sau alte informații disambiguante; și
2. Activeze comunicațiile criptate cu un site web: Facilitează schimbul de chei de criptare pentru a permite comunicarea criptată a informațiilor prin Internet între utilizatorul unui browser de Internet și un site web.

Scopul secundar al certificatelor EV/QWAC este de a ajuta la stabilirea legitimității unei afaceri care pretinde că operează un site web și să ofere un vehicul care poate fi utilizat pentru a ajuta la rezolvarea problemelor legate de phishing, malware și alte forme de fraudă a identității online. Prin furnizarea de informații legate de identitatea și adresa proprietarul afacerii, verificate de la terți, și mai fiabile, certificatele EV/QWAC vă pot ajuta să:

1. Facă mai dificil accesul la phishing și alte atacuri de fraudă online prin intermediul certificatelor;
2. Asiste companiile care ar putea fi ținta atacurilor de tip phishing sau a fraudei de identitate online oferindu-le un instrument pentru a se identifica mai bine către utilizatori; și
3. Asiste organizațiile de aplicare a legii în investigațiile privind phishingul și alte fraude de identitate online, inclusiv, după caz, contactarea, investigarea sau luarea de măsuri împotriva beneficiarului.

Cererile pentru care se consideră că este de încredere certificatul sunt decise de către entitatile partnere, pe baza naturii și scopului (inclusiv utilizarea cheii) a certificatului, inclusiv orice limitare aplicabilă, așa cum este scrisă în certificat.
Este responsabilitatea entității partenere să decidă în ce scop certificatele sunt considerate de încredere. O entitate parteneră trebuie să țină cont întotdeauna de nivelul de asigurare și de alte informații din CPP înainte de a decide cu privire la aplicabilitatea certificatului.

1.4.2 Utilizari interzise ale certificatului

Certificatele trebuie folosite doar in limitele admise de legislația in vigoare si doar in scopurile specificate în capitolul 1.4.1.

1.5 Administrarea politicii

1.5.1 Organizația care administrează documentul

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

Nume	CERTSIGN SA 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 Organizatia ce administreaza 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

Procedura de raportare a certificatelor cu probleme

Din cauza unor erori, limitări tehnice sau procedurale, ori din alte motive, pot exista certificate emise greșit de certSIGN (ex. certificatul emis conține informații eronate despre subiect sau organizație). Mai pot exista cazuri în care un certificat este utilizat necorespunzător (ex. pentru activități infracționale). Dacă beneficiarii, entitile sau alte terse părți se confruntă cu astfel de situații, în care suspectează compromiterea cheii private, sau un alt tip de activități frauduloase, utilizarea incorectă a certificatului sau o conduită neadecvată sau orice alte aspecte legate de certificatele emise de certSIGN, pot raporta aceste probleme la adresa **revokecsgn@certsign.ro**, informând Autoritatea de Certificare emitenta despre motive rezonabile de revocare a certificatului. certSIGN CA va începe investigarea unui raport de certificate cu probleme in maximum 24 de ore de la primire, și va decide dacă revocarea sau alte acțiuni corespunzătoare sunt justificate de cel puțin următoarele motive:

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

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

1.5.3 Persoana care decide conformitatea CPP cu politica

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

Table: 1.5.3 Persoana care decide conformitatea CPP cu politica

1.5.4 Procedurile de aprobare a CPP

Comitetul de Management al Politicilor și Procedurilor este responsabil de aprobarea CPP.

Procedura de aprobare este cuprinsă într-o instrucțiune internă.
Beneficiarii trebuie să respecte CPP-ul implementat și publicat la https://www.certsign.ro/ro/depozitar/
Beneficiarii care nu acceptă noii termenii și reglementările modificate ale CPP, sunt obligaţi să depună, în termen de 15 zile de la data la care noua versiune a CPP a fost aprobată, o declaraţie în acest sens. Acest lucru va duce la încetarea contractului de prestări servicii de certificare și la revocarea certificatului emis în baza acestuia.

1.6 Definiții și acronime

1.6.1 Definiții

Afiliat: O corporație, un parteneriat, o societate în comun sau o altă entitate care controlează, este controlată sau se află sub control comun cu o altă entitate, sau o agenție, un departament, o subdiviziune politică sau orice entitate care funcționează sub controlul direct al unei entități guvernamentale.

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

Reprezentantul beneficiarului/solicitantului: O persoană fizică sau un sponsor uman care este fie Beneficiarul, fie angajat al Beneficiarului, fie un agent autorizat care are autoritatea expresă de a reprezenta Beneficiarul:

(i) care semnează și transmite sau aprobă o cerere de certificat în numele Beneficiarului, și/sau
(ii) care semnează și transmite un Contract de abonat în numele Beneficiarului, și/sau
(iii) care recunoaște Termenii de utilizare în numele Beneficiarului atunci când Beneficiarul este un afiliat al AC sau este AC.

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

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

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

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

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

la dreapta până când întâlnește un nume de domeniu de bază și poate utiliza oricare dintre valorile intermediare în scopul validării domeniului.

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

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

CAA: Din RFC 8659 (https://www.rfc-editor.org/rfc/rfc8659.html): " Înregistrarea deresurse DNS Certification Authority Authorization (CAA) permite deținătorului unui nume de domeniu DNS să specifice una sau mai multe autorități de certificare (CA) autorizate să emită certificate pentru numele de domeniu respectiv. Înregistrările de resurse CAA permit unei AC publice să pună în aplicare controale suplimentare pentru a reduce riscul emiterii neintenționate de certificate eronate."

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

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

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

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

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

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

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

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

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

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

Control: "Control" (și sensurile sale corelative, "controlat de" și "sub control comun cu") înseamnă posesia, direct sau indirect, a puterii de a:
(1) de a dirija managementul, personalul, finanțele sau planurile unei astfel de entități;
(2) de a controla alegerea majorității directorilor; sau
(3) de a vota acea parte din acțiunile cu drept de vot necesară pentru "control" în conformitate cu legislația din jurisdicția de constituire sau de înregistrare a entității, dar în niciun caz mai puțin de 10%.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Compromiterea cheii: O cheie privată este considerată compromisă dacă valoarea sa a fost dezvăluită unei persoane neautorizate, dacă o persoană neautorizată a avut acces la ea.
Script de generare a cheilor: Un plan documentat de proceduri pentru generarea unei perechi de chei CA.

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

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

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

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

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

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

Nume de domeniu Onion: Un nume de domeniu complet calificat care se termină cu numele de domeniu cu utilizare specială RFC 7686 ".onion". De exemplu, gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion este un nume de domeniu Onion, în timp ce torproject.org nu este un nume de domeniu Onion.

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

Companie mamă: O societate care controlează o societate filială.

Perspectiva primară a rețelei: Perspectiva de rețea utilizată de AC pentru a stabili
1) autoritatea AC de a emite un certificat pentru domeniul (domeniile) sau adresa (adresele) IP solicitate și
2) autoritatea solicitantului și/sau autorizarea domeniului sau controlul asupra domeniului (domeniilor) sau adresei (adreselor) IP solicitate.

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

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

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

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

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

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

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

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

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

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

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

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

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

Token de cerere: O valoare derivată printr-o metodă specificată de către AC care leagă această demonstrație de control de cererea de certificat.
Tokenul de cerere TREBUIE să includă cheia utilizată în cererea de certificat.
Un jeton de cerere POATE include o marcă temporală pentru a indica data la care a fost creat.
Un jeton de cerere POATE include alte informații pentru a asigura unicitatea sa.
Un jeton de cerere care include un timestamp rămâne valabil pentru cel mult 30 de zile de la momentul creării.
Un jeton de cerere care include un timestamp TREBUIE să fie tratat ca fiind invalid dacă timestamp-ul său este în viitor.
Un jeton de cerere care nu include un timestamp este valabil pentru o singură utilizare, iar AC NU îl reutilizează pentru o validare ulterioară.
Legătura TREBUIE să utilizeze un algoritm de semnătură digitală sau un algoritm de hash criptografic.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Definitii din EV Guidelines:

Practician în contabilitate: Un expert contabil autorizat, un contabil autorizat sau o persoană cu o licență echivalentă în țara în care solicitantul este înregistrat sau constituit sau în orice jurisdicție în care solicitantul are un birou sau o unitate fizică; cu condiția ca un organism de standardizare contabilă din jurisdicția respectivă să mențină statutul de membru cu drepturi depline (nu "suspendat" sau "asociat") al Federației Internaționale a Contabililor.

Cerințe de bază: Cerințele de bază pentru emiterea și gestionarea certificatelor de încredere publică, astfel cum au fost publicate de CA/Browser Forum și orice modificări ale acestui document.

Entitate comercială: Orice entitate care nu este o organizație privată, o entitate guvernamentală sau o organizație de stat, entitate necomercială, astfel cum este definită în prezentul document. Exemplele includ, dar nu se limitează la parteneriate generale, asociații fără personalitate juridică, întreprinderi individuale etc.

Aprobator de certificate: O persoană fizică care este fie solicitantul, fie angajat al solicitantului, fie un agent autorizat care are autoritatea expresă de a reprezenta solicitantul

i. să acționeze în calitate de Solicitant de certificat și să autorizeze alți angajați sau terți să acționeze în calitate de Solicitant de certificat, și
ii. să aprobe cererile de certificat EV depuse de alți solicitanți de certificat.

Cerere de confirmare: O comunicare corespunzătoare în afara benzii care solicită verificarea sau confirmarea unui anumit fapt în cauză.

Persoană care confirmă: O poziție din cadrul organizației unui solicitant care confirmă un anumit fapt în cauză.

Semnatarul contractului: O persoană fizică care este fie Solicitantul, fie angajat al Solicitantului, fie un agent autorizat care are autoritatea expresă de a reprezenta Solicitantul și care are autoritatea de a semna, în numele Solicitantului, Contracte de abonat.

Cont de depozit la cerere: Un cont de depozit deținut la o bancă sau la o altă instituție financiară, în care fondurile depuse sunt plătibile la cerere. Scopul principal al conturilor la vedere este de a facilita plățile fără numerar prin intermediul cecurilor, cecurilor bancare, debitului direct, transferului electronic de fonduri etc. Utilizarea variază în funcție de țară, dar un cont de depozit la vedere este cunoscut în mod obișnuit sub denumirea de cont de cecuri, cont curent sau cont curent.

Autoritatea EV: O sursă, alta decât Autorul Certificatului, prin intermediul căreia se verifică faptul că Autorul Certificatului este autorizat în mod expres de către Solicitant, la data solicitării certificatului EV, să întreprindă acțiunile de solicitare descrise în prezentele orientări.

Certificat EV: Un certificat care conține informații despre subiect specificate în prezentele orientări și care a fost validat în conformitate cu prezentele orientări.

Beneficiari ai certificatului EV: Persoane cărora AC și AC rădăcină acordă garanțiile specificate pentru certificatele EV.

Reînnoirea certificatului: Procesul prin care un solicitant care are un certificat de autenticitate valabil, neexpirat și nerevocat, depune o cerere, la AC care a emis certificatul original, pentru un nou certificat emis pentru același nume de organizație și nume de domeniu înainte de expirarea certificatului existent al solicitantului, dar cu o nouă dată de "valabilitate până la" ulterioară datei de expirare a certificatului actual.

Reemiterea certificatului : Procesul prin care un solicitant care deține un certificat valabil, neexpirat și nerevocat, depune o cerere la AC care a emis certificatul original, pentru un nou certificat eliberat pentru același nume de organizație și nume de domeniu înainte de expirarea certificatului existent al solicitantului, dar cu o dată "valabil până la" care să corespundă cu cea a certificatului actual.

Cerere de certificat EV: O cerere din partea unui solicitant către AC prin care se solicită ca AC să emită un certificat EV pentru solicitant, cerere care este autorizată în mod valabil de către solicitant și semnată de către reprezentantul solicitantului.

Garanții ale certificatului EV: În legătură cu emiterea de către AC a unui certificat EV, AC și AC rădăcină a acesteia, pe perioada în care certificatul EV este valabil, promit că AC a respectat cerințele prezentelor orientări și ale politicilor EV ale AC în emiterea certificatului EV și în verificarea exactității informațiilor conținute în certificatul EV.

EV OID: Un număr de identificare, sub forma unui „identificator de obiect”, care este inclus în câmpul certificatePolicies al unui certificat care:
i. indică ce declarație de politică a AC se referă la certificatul respectiv; și
ii. este fie identificatorul de politică EV al CA/Browser Forum EV, fie un identificator de politică care, prin acord prealabil cu unul sau mai mulți furnizori de software pentru aplicații, marchează certificatul ca fiind un certificat EV.

Politici EV: Practici, politici și proceduri verificabile privind certificatele EV, cum ar fi o certificare declarație de practici de certificare și politica de certificare, care sunt elaborate, implementate și aplicate de către AC și de către AC rădăcină a acesteia.

Procesele EV: Cheile, software-ul, procesele și procedurile prin care AC verifică datele de certificat în conformitate cu prezenta orientare, emite certificate EV, menține un depozit și revocă certificatele EV.

Certificat de validare extinsă: A se vedea Certificat EV.

Agenție guvernamentală: În contextul unei organizații private, agenția guvernamentală din jurisdicția de constituire sub autoritatea căreia se stabilește existența legală a organizațiilor private (de exemplu, agenția guvernamentală care a emis certificatul de constituire). În contextul entităților comerciale, agenția guvernamentală din jurisdicția de funcționare care înregistrează entitățile comerciale. În cazul unei Entități guvernamentale, entitatea care promulgă legi, regulamente sau decrete care stabilesc existența juridică a Entităților guvernamentale.

Agenția de constituire: În contextul unei organizații private, agenția guvernamentală din jurisdicția de constituire sub a cărei autoritate este înregistrată existența juridică a entității (de exemplu, agenția guvernamentală care emite certificate de constituire sau de încorporare). În contextul unei entități guvernamentale, entitatea care promulgă legi, regulamente sau decrete care stabilesc existența juridică a entităților guvernamentale.

Confirmare independentă din partea solicitantului: Confirmare a unui anumit fapt primită de către AC în conformitate cu dispozițiile Ghidului sau care este obligatorie pentru solicitant.

Persoană fizică: O persoană fizică.

Organizație internațională: O organizație înființată printr-un document constitutiv, de exemplu, o cartă, un tratat, o convenție sau un document similar, semnat de cel puțin două guverne de state suverane sau în numele acestora.

Jurisdicția de constituire: În contextul unei organizații private, țara și (dacă este cazul) statul sau provincia sau localitatea în care a fost stabilită existența juridică a organizației prin depunerea unei cereri la (sau printr-un act al) unei agenții sau entități guvernamentale corespunzătoare (de exemplu, unde a fost constituită). În contextul unei entități guvernamentale, țara și (dacă este cazul) statul sau provincia în care existența juridică a entității a fost creată prin lege.

Jurisdicția de înregistrare: În cazul unei entități comerciale, statul, provincia sau localitatea în care organizația și-a înregistrat prezența în afaceri prin intermediul unor înregistrări efectuate de o persoană fizică principală implicată în afaceri.

Notar latin: O persoană cu pregătire juridică al cărei mandat, în conformitate cu legislația aplicabilă, nu numai că include autoritatea de a autentifica executarea unei semnături pe un document, ci și responsabilitatea pentru corectitudinea și conținutul documentului. Un notar latin este uneori denumit uneori notar de drept civil.

Entitate juridică: O organizație privată, o entitate guvernamentală, o entitate comercială sau o entitate necomercială.

Existență juridică: O organizație privată, o entitate guvernamentală sau o entitate comercială are legalitate. existență juridică dacă a fost constituită în mod valabil și nu a fost reziliată, dizolvată sau abandonată.

Practician juridic: O persoană care este fie un avocat, fie un notar latin, astfel cum este descris în aceste Ghiduri și care are competența de a emite o opinie cu privire la afirmațiile de fapt ale Solicitantului.

Perioada maximă de valabilitate:
1. Perioada maximă de timp pentru care este valabil certificatul EV eliberat.
2. Perioada maximă după validarea de către AC în care anumite informații despre solicitant pot fi invocate la eliberarea unui certificat EV în conformitate cu prezentele orientări.

Notar: O persoană al cărei mandat, în conformitate cu legislația aplicabilă, include autoritatea de a autentifica executarea unei semnături pe un document.

Sediu de afaceri: Locația oricărei instalații (cum ar fi o fabrică, un magazin de vânzare cu amănuntul, un depozit etc.) în care se desfășoară activitatea solicitantului.

Persoană fizică principală: O persoană fizică a unei organizații private, a unei entități guvernamentale sau a unei entități comerciale care este fie proprietar, partener, membru executiv, director sau funcționar, așa cum este identificat prin titlul de angajare, fie un angajat, contractant sau agent autorizat de o astfel de entitate sau organizație să desfășoare activități legate de solicitarea, eliberarea și utilizarea certificatelor EV.

Organizație privată: O entitate juridică neguvernamentală (indiferent dacă participațiile de proprietate sunt private sau publice) a cărei existență a fost creată printr-o înregistrare la (sau printr-un act al) Agenției de constituire sau un echivalent în jurisdicția de constituire a acesteia.

Auditor calificat: O firmă de contabilitate publică independentă care îndeplinește cerințele de calificare în materie de audit specificate în secțiunea 8.2.

Sursă de informații guvernamentale calificată: O bază de date întreținută de o entitate guvernamentală (de exemplu, înregistrările SEC) care îndeplinește cerințele CABF EV de la secțiunea 3.2.2.2.11.6.

Sursă de informații fiscale guvernamentale calificate: O sursă de informații guvernamentale calificate care conține în mod specific informații fiscale referitoare la organizații private, entități comerciale sau persoane fizice.

Sursă de informații independente calificate: O bază de date actualizată în mod regulat și curentă, disponibilă publicului, concepută în scopul de a furniza cu exactitate informațiile pentru care este consultată și care este în general recunoscută ca o sursă sigură de astfel de informații.

Agenția de înregistrare: O agenție guvernamentală care înregistrează informații comerciale în legătură cu înființarea unei entități sau cu autorizarea unei entități de a desfășura activități comerciale în baza unei licențe, a unei cartele sau a unei alte certificări. O agenție de înregistrare POATE include, dar nu se limitează la

i. un Departament de stat al societăților comerciale sau un secretar de stat;
ii. o agenție de acordare a licențelor, cum ar fi un Departament de asigurări de stat; sau
iii. o agenție de autorizare, cum ar fi un birou de stat sau un departament de reglementare financiară, bancară sau financiară, sau o agenție federală, cum ar fi Oficiul Controlorului Monedei sau Oficiul de Supraveghere a Economiilor (Office of the Comptroller of the Currency sau Office of Thrift Supervision).

Referință de înregistrare: Un identificator unic atribuit unei entități juridice.

Schema de înregistrare: O schemă de atribuire a unei referințe de înregistrare care îndeplinește cerințele identificate în apendicele H.

Agent înregistrat: O persoană sau o entitate care este:
i. autorizată de către Solicitant să primească notificarea sau comunicarea actelor de procedură și a comunicărilor comerciale pe în numele solicitantului; și
ii. este înscrisă în registrele oficiale ale jurisdicției de constituire a solicitantului ca acționând în calitate de rolul specificat la punctul (i) de mai sus.

Sediul social: Adresa oficială a unei societăți, înregistrată la Agenția de constituire, la care se trimit documentele oficiale și la care se primesc notificările legale.

Număr de înregistrare: Numărul unic atribuit unei organizații private de către agenția de constituire în jurisdicția de constituire a entității respective.

Instituție financiară reglementată: O instituție financiară care este reglementată, supravegheată și examinată de către autoritățile guvernamentale, naționale, de stat sau provinciale sau locale.

Script de generare a cheii de rădăcină: Un plan documentat al procedurilor care trebuie efectuate pentru generarea perechii de chei CA rădăcină.

Autoritate de semnare: Unul sau mai mulți aprobatori de certificate desemnați să acționeze în numele solicitantului.

Entitate guvernamentală superioară: Pe baza structurii guvernamentale dintr-o subdiviziune politică, entitatea sau entitățile guvernamentale care au capacitatea de a gestiona, dirija și controla activitățile solicitantului.

Codul suspectului: Cod care conține funcționalități rău intenționate sau vulnerabilități grave, inclusiv spyware, malware și alte tipuri de cod care se instalează fără consimțământul utilizatorului și/sau rezistă la propria eliminare, precum și codul care poate fi exploatat în moduri care nu au fost prevăzute de proiectanții săi pentru a compromite fiabilitatea platformelor pe care se execută.

Traducător: O persoană sau o entitate comercială care posedă cunoștințele și expertiza necesare pentru a traduce cu exactitate cuvintele unui document scris într-o limbă în limba maternă a AC.

Scrisoare a contabilului verificat: Un document care îndeplinește cerințele specificate în CABF EV secțiunea 3.2.2.2.11.2.

Aviz juridic verificat: Un document care îndeplinește cerințele specificate în CABF EV secțiunea 3.2.2.2.11.1.

Metoda de comunicare verificată: Utilizarea unui număr de telefon, a unui număr de fax, a unei adrese de e-mail sau a unei adrese de livrare poștală, confirmată de către AC în conformitate cu secțiunea 3.2.2.5 ca fiind o modalitate fiabilă de comunicare cu solicitantul.

Scrisoare profesională verificată: O scrisoare verificată a unui contabil sau un aviz juridic verificat.

Programul WebTrust EV: Procedurile de audit suplimentare specificate de AICPA/CICA pentru autoritățile de certificare care eliberează certificate EV, care trebuie utilizate împreună cu programul WebTrust pentru autoritățile de certificare.

Programul WebTrust pentru autoritățile de certificare: Versiunea curentă la momentul respectiv a programului WebTrust al AICPA/CICA pentru autoritățile de certificare.

Sigiliul de asigurare WebTrust: O confirmare de conformitate care rezultă din Programul WebTrust pentru autoritățile de certificare.

1.6.2 Acronime

Acronym	Meaning	Traducere
ADN	Authorization Domain Name	Autorizare Nume de domeniu

AICPA	American Institute of Certified Public Accountants	Institutul American al Contabililor Publici Autorizați
BIPM	International Bureau of Weights and Measures	Biroul Internațional de Măsuri și Greutăți
BIS	(US Government) Bureau of Industry and Security	(Guvernul SUA) Biroul de Industrie și Securitate
CA	Certification Authority	Autoritatea de certificare
CAA	Certification Authority Authorization	Autorizarea autorității de certificare
CARL	Certification Authority Revocation List	Lista de revocare a autorității de certificare
ccTLD	Country Code Top-Level Domain	Cod de țară Domeniu de nivel superior
CEO	Chief Executive Officer	Director Executiv
CFO	Chief Financial Officer	Director Financiar
CICA	Canadian Institute of Chartered Accountants	Institutul canadian al contabililor autorizați
CIO	Chief Information Officer	Director Tehnologia Informațiilor (IT)
CISO	Chief Information Security Officer	Director Securitatea Informațiilor
COO	Chief Operating Officer	Director Operațional
CP	Certificate Policy	Politica de certificare
CPA	Chartered Professional Accountant	Contabil profesionist autorizat
CPS	Certification Practice Statement	Declarație privind practicile de certificare
CRL	Certificate Revocation List	Lista de revocare a certificatelor
CSO	Chief Security Officer	Director Securitate
DBA	Doing Business As	Făcând afaceri sub numele de
DN	Distinguished Name	Denumire distinctă
DNS	Domain Name System	Sistem de nume de domeniu
DV	Domain Validated	Domeniu validat
EV	Extended Validation	Validare extinsă
FIPS	(US Government) Federal Information Processing Standard	(Guvernul SUA) Standardul federal de prelucrare a informațiilor
FQDN	Fully-Qualified Domain Name	Nume de domeniu complet calificat
gTLD	Generic Top-Level Domain	Domeniul generic de vârf
IANA	Internet Assigned Numbers Authority	Autoritatea de atribuire a numerelor de internet
ICANN	Internet Corporation for Assigned Names and Numbers	Corporatia Internet pentru alocarea Numelor si Numerelor
IFAC	International Federation of Accountants	Federația Internațională a Contabililor
IM	Instant Messaging	Mesagerie instantanee
IRS	Internal Revenue Service	Serviciul de venituri interne
ISO	International Organization for Standardization	Organizația Internațională pentru Standardizare
ISP	Internet Service Provider	Furnizor de Servicii Internet
NIST	(US Government) National Institute of Standards and Technology	(Guvernul SUA) Institutul Național de Standarde și Tehnologie
OCSP	Online Certificate Status Protocol	Protocol de stare a certificatelor online
OID	Object Identifier	Identificator de obiect
OV	Organization Validated	Organizație validată
PKI	Public Key Infrastructure	Infrastructură cu cheie publică
PPMB	Policies and Procedures Management Body	Organism de gestionare a politicilor și procedurilor
QEVCP-w	Certificate Policy for EU qualified Website Authentication based on EVCP	Politica de certificare pentru autentificarea site-urilor web calificate de UE pe baza EVCP

QGIS	Qualified Government Information Source	Sursă Guvernamentală de Informații Calificate
QIIS	Qualified Independent Information Source	Sursă Independentă de Informații Calificate
QNCP-w	Certificate policy for EU qualified website authentication certificates based on NCP and PTC	Politica de certificare pentru certificatele de autentificare a site-urilor web calificate de UE pe baza PCN și PTC
QSCD	Qualified Electronic Signature Creation Device	Dispozitiv de creare a semnăturilor electronice calificat
QTIS	Qualified Government Tax Information Source	Sursă calificată de informații fiscale guvernamentale
QWAC	Qualified Certificate for Website Authentication	Certificat calificat pentru autentificarea site-urilor web
RA	Registration Authority	Autoritatea de înregistrare
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm	Algoritm criptografic asimetric Rivest, Shamir, Adleman
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)	MIME securizat (Extensii multifuncționale de poștă electronică pe Internet)
SEC	(US Government) Securities and Exchange Commission	(Guvernul SUA) Comisia pentru valori mobiliare și burse
TLS	Secure Sockets Layer	Secure Sockets Layer
TLS	Transport Layer Security	Securitatea stratului de transport
TSP	Trust Services Provider	Furnizor de servicii de încredere
UTC	Coordinated Universal Time	Timp universal coordonat
UTC(k)	National realization of Coordinated Universal Time	Realizarea națională a timpului universal coordonat
VoIP	Voice Over Internet Protocol	Protocol de voce pe internet

2 Publicare și responsabilități Depozitar

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

2.1 Depozitare

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

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

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

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

2.2 Publicarea informațiilor de certificare

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

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

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

Pentru toate certificatele emise, informațiile privind starea certificatului sunt disponibile prin CRL-uri și serviciile de validare a certificatelor furnizate de certSIGN 24*7*365.

certSIGN este conform cu ultima versiune publicată a „Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates” si a „CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates”, publicată la http://www.cabforum.org. În cazul unei eventuale neconcordanțe între acest document și aceste cerințe, aceste cerințe au prioritate față de acest document.

certSIGN găzduiește pagini web care permit furnizorilor de aplicații software să testeze software-ul cu certificate end-user emise de sub certSIGN ROOT CA G2:

- testssl-valid-evcp.certsign.ro
- testssl-revoked-evcp.certsign.ro
- testssl-expired-evcp.certsign.ro

certSIGN acceptă soluții automate pentru eliberarea și reînnoirea certificatelor pentru fiecare OID al politicii de certificare a cerințelor de bază, sub forma Certificatelor de Testare Automatizate. Certificatele de Testare Automatizate valide sunt reînnoite automat o dată la 30 de zile calendaristice.

Disponibilitatea

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

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

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

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

2.3 Timpul sau frecvența publicării

Informațiile publicate de certSIGN (Codul de Practici si Proceduri) sunt actualizate anual sau determinate de urmatoarele evenimente specifice:

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

2.4 Controlul accesului la Depozitare

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

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

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

certSIGN poate lua măsuri rezonabile de protecție împotriva și pentru prevenirea utilizării abuzive a depozitarului, a OCSP sau serviciilor de descărcare a CRL. La descoperirea unor breşe ce afectează integritatea informaţiilor din Depozitar, certSIGN va lua măsurile corespunzătoare pentru a restabili integritatea informaţiilor, va trage la răspundere pe cei vinovaţi și va notifica imediat entităţile afectate.

3 Identificarea și autentificarea

3.1 Nume

Structura si utilizarea numelor din certificate este conform cu X.500, RFC5280, CABF Baseline Requirements si EV Guidelines.
certSIGN nu permite utilizarea în certificate de nume de domenii internaționalizate (IDN).
Numele Subiectului inclus intr-un certificat este în conformitate cu numele distinctiv X.500 (DN). certSIGN Web CA G2 utilizeaza o singură convenție de nume așa cum este stabilită în Ghidul EV și cerințele de bază (BR) publicate de Forumul CA / Browser.

Certificatele emise în baza acestui CPP sunt semnificative numai dacă numele care apar în certificate pot fi înțelese și utilizate de către entitatile partenere. Numele utilizate în certificate trebuie să identifice site-ul web la care sunt atribuite într-un mod semnificativ.

Atributul DN este unic pentru Subiectul catre care este emis. Pentru fiecare certificat se emite un număr de serie unic în spațiul de nume al certSIGN Web CA.

3.1.1 Tipuri de nume

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

3.1.2 Nevoia ca Numele să aibă înțeles logic

Certificatele TLS, cu exceptia certificatelor wildcard și a celor de tip Unified Communications, sunt emise cu un Nume de Domeniu Complet Calificat (FQDN).

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

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

CertSIGN nu emite certificate TLS care conțin „underscore character" („_") în numele de domeniu/dNSName, in concordanta cu recomandarile CA/Browser Forum BR ultima versiune publicată. FQDN cuprinde doar "P-labels" și „Non-Reserved LDH-labels".

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

certSIGN nu emite certificate TLS pentru persoane fizice.

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

- **countryName** – (C) – Codul de țară ISO 3166-1 din două litere pentru țara asociată cu Subiectul
- **commonName** (CN) – Nume de domeniu complet calificat, valoare derivată din subjectAltName

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

- **countryName** – (C) – Codul de țară ISO 3166-1 din două litere pentru țara asociată cu Subiectul
- **commonName** (CN) – Nume de domeniu complet calificat, valoare derivată din subjectAltName
- **organizationName** (O) – Numele organizatiei,
- **localityName** (L) – Localitatea de resedinta a Beneficiarului

Pentru certificate de tip OV, DN poate conține următoarele câmpuri **opționale** (descrierea câmpului este urmată de abrevierea corespunzătoare recomandărilor X.520:

- **stateOrProvinceName** (S) - Județul / sectorul în care este funcționează organizația,
- **streetAddress** – informații privind adresa Beneficiarului

Pentru certificate de tip EV certSIGN utilizeaza nume distinctive pentru identificarea subiectului certificatului (organizatie sau dispozitiv). Conținutul câmpurilor din certificatele EV trebuie să îndeplinească cerințele din secțiunea 7.1..4.2 din Ghidul EV:

- subject:**organizationName** (OID 2.5.4.10)
- subject:**commonName** (OID: 2.5.4.3)
- subject:**businessCategory** (OID: 2.5.4.15)
- subject:**serialNumber** (OID: 2.5.4.5)
- subject:**organizationIdentifier** (OID: 2.5.4.97)
- **Adresa Legală a Afacerii:**
  - subject:**jurisdictionCountryName** (OID: 1.3.6.1.4.1.311.60.2.1.3)
  - subject:**jurisdictionLocalityName** (OID: 1.3.6.1.4.1.311.60.2.1.1)
  - subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)-(optional)
- **Adresa Fizică a Locului Afacerii:**
  - subject:**countryName** (OID: 2.5.4.6)
  - subject:**localityName** (OID: 2.5.4.7)
  - subject:stateOrProvinceName (OID: 2.5.4.8) - (unde este cazul)
  - subject:streetAddress (OID: 2.5.4.9) - (optional)
  - subject:postalCode (OID: 2.5.4.17) - (optional)

Pentru certificate QWAC componentele DN sunt identice cu cele pentru certificate EV.

3.1.3 Anonimitatea sau pseudonimitatea beneficiarilor

certSIGN nu emite certificate TLS anonime sau cu pseudonime.

3.1.4 Reguli de interpretare a diferitelor formate de nume

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

3.1.5 Unicitatea numelor

Unicitatea numelui este asigurată, pentru OV si EV/QWAC, folosind câmpul O care este obligatoriu și trebuie să fie unic pentru o anumită entitate și, pentru toate TLS, prin utilizarea numelui de domeniu complet calificat în CommonName. Unicitatea unui nume de domeniu este garantată de Internet Corporation pentru nume și numere atribuite (ICANN).

3.1.6 Recunoașterea, autentificarea și rolul mărcilor înregistrate

Nu este stipulat.

3.2 Validarea Inițială a Identității

Înainte de a emite un certificat **EV/QWAC**, CA se asigură că toate informațiile despre organizația Beneficiarului din certificat sunt conforme cu cerințele și au fost verificate în conformitate cu procedurile descrise în acest CPP, Instrucțiunile EV publicate de Forumul CA / Browser și ETSI EN 319-411-2 pentru QEVCP-w și se potrivește cu informațiile confirmate și documentate de RA în conformitate cu procesele sale de verificare. Astfel de procese de verificare sunt destinate să realizeze următoarele:

1. Verifica existența și identitatea solicitantului, inclusiv:
   a. Verificața existența legală și identitatea solicitantului (așa cum se prevede în Ghidul EV),
   b. Verifica existența fizică a solicitantului (Prezența afacerii la o adresă fizică) , și
   c. Verificați existența operațională a solicitantului (activitatea de afaceri).
2. Verifica că solicitantul este titularul înregistrării sau deține controlul exclusiv asupra numelui de domeniu care urmează să fie inclus în EV/QWAC.
3. Verificarea unui mijloc fiabil de comunicare cu entitatea care urmează să fie desemnată ca subiect în certificat
4. Verifica autorizarea solicitantului pentru EV/QWAC, inclusiv:
   a. Verifica numele, titlul și autoritatea semnatarului contractului, a aprobatorului de certificat și a solicitantului de certificat;
   b. Verifica dacă semnatarul contractului a semnat Acordul contractual sau dacă un reprezentant al solicitantului autorizat în mod corespunzător a recunoscut și a fost de acord cu Termenii de utilizare;
   c. Verifica dacă un aprobator de certificat a semnat sau a aprobat în alt mod solicitarea EV/QWAC.

3.2.1 Dovada Posesiei Cheii Private

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

3.2.2 Autentificarea identității organizației

Pentru DV, OV, EV, QWAC

Este necesar să se demonstreze că entitatea care solicită certificatul TLS deține controlul asupra domeniului la care se referă cererea de certificat.

Procedura de validare a proprietății sau a controlului solicitantului asupra domeniului se bazează pe ETSI EN 319 411-1 și pe ultima versiune publicată a CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates.

Pentru OV, EV, QWAC

Autentificarea identității persoanei juridice se realizează pentru a dovedi că, la procesarea unei cereri, persoana juridică menționată în cerere există cu adevărat; de asemenea, este necesar să se dovedească faptul că o persoană fizică care solicită un certificat din partea unei societăți sau care îl primește este autorizată de această persoană juridică să o reprezinte.
Organizațiile românești sunt autentificate pe baza documentelor și atestatelor recente, valabile în România, organizațiile din alte țări, sunt autentificate pe baza documentelor și atestatelor echivalente, după cum este aplicabil pentru țara în cauză.
În România, autoritatea cu drept de înregistrare a organizațiilor comerciale pe întreg teritoriul României este Oficiul Național al Registrului Comerțului, https://www.onrc.ro/index.php/ro/.
CA inspectează orice document invocat în temeiul prezentei secțiuni pentru a depista alterarea sau falsificarea acestuia.

Pentru EV, QWAC

RA care operează sub certSIGN Web CA G2 efectuează o verificare a identităților organizaționale care sunt trimise de un solicitant sau de un beneficiar. Acesta determină dacă identitatea organizațională, existența legală, existența fizică, existența operațională și numele de domeniu furnizate cu o cerere EV/QWAC sunt compatibile cu cerințele stabilite în Ghidul EV publicat de Forumul CA / browser. Informațiile și sursele utilizate pentru verificarea cererilor EV/QWAC pot varia în funcție de competența solicitantului sau a beneficiarului.

CA-ul verifică orice document eliberat în cadrul acestei secțiuni pentru alterare sau falsificare.

certSIGN va lua măsuri rezonabile pentru a stabili că o cerere de certificat făcută în numele unei organizații este legitimă și autorizată corespunzător:

- beneficiarul sau administratorul organizației trebuie să furnizeze dovezi (documente semnate de persoane autorizate) iar identificarea trebuie sa fie realizata de catre reprezentantii certSIGN sau terte parti față în față.
- documentele solicitate de catre certSIGN referitoare la organizatie (status, adresa, nume, etc.) sunt eliberate de autoritati de incredere locale, statale sau naționale.

In acest sens certSIGN va lua toate masurile pentru stabilirea autenticitatii documentelor:

- prin verificarea valabilitatea înregistrării, prin autoritatea care a eliberat documentul
- intr-o bază de date reputată a unui terț sau alta resursă
- verificarea validitatii organizației printr-o terță parte de încredere

CMPP al certSIGN poate, la discreția sa, să actualizeze practicile de verificare pentru a îmbunătăți procesul de verificare a identității organizației. Orice modificare a practicilor de verificare se publică în conformitate cu procedurile standard de actualizare a CPP.

3.2.2.1 Identitatea

3.2.2.1.1 Identitatea pentru TLS - DV, OV, EV, QWAC

Aplicantul este obligat să prezinte la solicitarea Autorității de înregistrare o cerere de cumpărare.
Procedura pe care RA o aplică pentru verificarea domeniului constă în:

- Verificarea documentelor prezentate de Beneficiar,
- Verificarea cererii, care constă în:

- Verificarea conformității datelor specificate în cerere cu cele din documentele prezentate,
- Verificarea dovezii de deținere a cheii private și a faptului că Distinctive Name este cel potrivit,

- Verificare dacă domeniul menționat în certificat este înregistrat de entitatea care a depus cererea de certificat sau de cea care a autorizat utilizarea domeniului de către entitatea solicitantă în conformitate cu CA/Browser Forum – #3.2.2.4.7 (DNS Change) sau #3.2.2.4.19 (Agreed Upon Change to Website ACME, sau #3.2.2.4.4 (Constructed Email to Domain Contact).
- Verificarea în registrul regional de domenii internet (baza de date RIPE pentru abonații europeni) dacă persoana care solicită certificatul TLS este proprietarul sau are dreptul de a utiliza adresa IP rutabilă pentru care se solicită certificatul.

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

3.2.2.1.2 Identitatea pentru OV, EV, QWAC

Reprezentanții autorizați ai organizației sunt obligați să prezinte la solicitarea Autorității de înregistrare următoarele documente:

- Copie certificată „conform cu originalul" a certificatului de inregistrare a companiei;
- Documente care atestă identitatea solicitantului (act de identitate sau pașaport) și împuternicirea care să confirme că este reprezentantul companiei;
- Cererea de cumpărare;

Procedura pe care RA o aplică pentru verificarea identității persoanei juridice și a reprezentanților autorizați ai acesteia constă în:

- Verificarea documentelor prezentate de Beneficiar,
- Verificarea cererii, care constă în:
  - Verificarea conformității datelor specificate în cerere cu cele din documentele prezentate,
  - Verificarea dovezii de deținere a cheii private și a faptului că Distinctive Name este cel potrivit,
  - Verificarea autorizării și a identității reprezentantului persoanei juridice care depune cererea în numele entității.

Autoritatea de înregistrare se angajează să verifice corectitudinea și autenticitatea tuturor datelor furnizate în cadrul unei cereri.

3.2.2.1.3 Identitatea pentru EV, QWAC

certSIGN verifică faptul că beneficiarul este o organizație existentă și legitimă.
Ca dovadă că este o organizație existentă și legitimă, certSIGN cere și verifică cel puțin următoarele documente:

- Pentru instituții publice/guvernamentale, un extras recent (nu mai vechi de 1 luna) de la Camera de Comerț sau conform legii aplicabile, act sau decret guvernamental care atestă reprezentantul legal (sau reprezentanții);

- Pentru organizațiile private un extras certificat recent (nu mai vechi de 1 lună) de la Registrul Național al Comerțului sau organisme nationale similare de incredere in cazul beneficiarilor din afara Romaniei.

Ca dovadă că este o organizație legală, TSP verifică dacă organizația este în ultima listă a UE privind persoanele interzise de teroriști și previne organizațiile, publicată de Consiliul European și nu va emite certificat dacă organizația este în acea listă.

Numele organizației

certSIGN verifică dacă numele organizației care este inclus în certificat este corect și complet și corespunde numelui organizației înregistrate de beneficiar
Ca dovadă a corectitudinii denumirii organizației oficiale declarate, certSIGN va obține cel puțin și va verifica următoarele documente:
Organizații private: un extras certificat recent (până la 1 lună) din registrul comerțului Camerei de Comerț sau organisme nationale similare de incredere in cazul beneficiarilor din afara Romaniei.
În plus, în dovezile furnizate, entitatea organizațională ar trebui să se distingă de orice alte organizații cu același nume. Un extras din Registrul Național al Comerțului, sau, pentru beneficiari externi României, de la organisme naționale de încredere similare, conține aceste informații.
Entități guvernamentale: Informațiile de mai sus cu privire la existența și identitatea unei entități guvernamentale pot fi de asemenea furnizate de o entitate guvernamentală superioară guvernamentală în aceeași subdiviziune politică ca și solicitantul (de exemplu, un secretar de stat poate verifica existența legală a unui anumit departament de stat) .
Entitățile Organizației Internaționale: Existența legală și identitatea pot fi confirmate:
(a) cu referire la actul constitutiv în care sa format Organizația Internațională; sau
(b) direct la guvernul unei țări semnatare (adică de la o agenție guvernamentală competentă sau de la legile țării respective sau prin verificarea faptului că guvernul țării are misiunea de ao reprezenta la Organizația Internațională); sau
(c) Direct contra oricărei liste actuale de entități calificate pe care Forumul CAB le poate menține la www.cabforum.org. În cazul în care organizația internațională care solicită EV/QWAC este un organ sau o agenție - inclusiv o organizație neguvernamentală (ONG) a unei organizații internaționale verificate, atunci certSIGN poate verifica solicitantul Organizației Internaționale direct de la organizația internațională verificată, la care solicitantul este un organ sau o agenție.

Adresa organizatiei

certSIGN verifică dacă datele furnizate de beneficiar cu privire la adresa organizației sunt corecte și complete și că este adresa la care organizația isi desfășoară activitatea.

Adresa va conține cel puțin țara, localitatea, numele străzii, numărul clădirii și codul poștal.

Ca dovadă a corectitudinii și existenței operațiunilor organizației la adresa specificată, certSIGN solicită și verifică cel puțin următoarele documente:

- Pentru organizatii publice / guvernamentale verificarea este efectuată pe baza serviciului public de verificare online: mfinante.ro (Ministerul Finanțelor);
- Pentru organizațiile private și neîncorporate un extras certificat recent (nu mai vechi de 1 lună) de la Registrul Național al Comerțului sau de la organisme nationale similare de incredere in cazul beneficiarilor din afara Romaniei.

Dacă adresa din documentele justificative corespunde adresei de pe cerere, certSIGN va considera că este suficientă dovada că aceasta este adresa la care organizația își desfășoară activitatea.

Dacă adresa nu se potrivește cu dovezile, atunci certSIGN trebuie să efectueze o vizită la fața locului la locația specificată a beneficiarului și să-și noteze constatările într-un raport. Raportul trebuie să includă cel puțin următoarele informații:

- Verifica că afacerea solicitantului este localizată la adresa exactă menționată în cererea EV/QWAC (de exemplu prin intermediul semnelor permanente, confirmării angajaților etc.);
- Identifica tipului cladirii (de exemplu, un birou într-o clădire comercială, o reședință privată, un magazin etc.) și dacă aceasta pare să fie o locație permanentă a unei companii;
- Indica dacă există un semn permanent (care nu poate fi mutat) care identifică solicitantul;
- Indica dacă există dovezi că solicitantul desfășoară activități de afaceri la locul respectiv (de exemplu, nu este doar o adresa de corespondenta, o casuta postala), și
- Include una sau mai multe fotografii cu (i) exteriorul locatiei (indicând semnele care indică numele solicitantului dacă este prezent și afișând adresa strazii, dacă este posibil) și (ii) zona de recepție sau spațiul de lucru.

În mod alternativ, certSIGN va accepta declarația unui notar că adresa specificată este adresa la care organizația își desfășoară activitatea.

Verificarea telefonului organizatiei

certSIGN verifică dacă numărul de telefon al organizației specificat de beneficiar este corect și complet.

Ca dovadă a corectitudinii și existenței numărului de telefon specificat al organizației certSIGN:

- Apeleaza numărul de telefon și obține un răspuns afirmativ suficient pentru a permite unei persoane să concluzioneze că solicitantul este accesibil prin telefon la numerele formate; și
- Confirmă numărul de telefon al organizației, așa cum apare în versiunea cea mai recentă a site-ului (online) "Pagini Aurii" " - https://www.paginiaurii.ro/;

În mod alternativ, în timpul unei vizite la fața locului, persoana care efectuează vizita la fața locului poate să sune la numărul de telefon furnizat și să concluzioneze, vorbind cu persoana care se află la locatia solicitantului în timpul vizitei - care este de asemenea la telefon cu persoana care a sunat - este accesibil prin telefon la numărul format; Cu condiția ca numărul confirmat să nu fie un telefon mobil.

Existenta operationala

Beneficiarii EV/QWAC trebuie să îndeplinească cerința de "existență operațională", care presupune că solicitantul a fost în funcțiune timp de trei (3) ani sau mai mult. Dacă acestea există de mai puțin de trei ani, după cum indică înregistrările agenției guvernamentale, atunci ei trebuie inclusi în informațiile actuale furnizate de o sursă independentă de informații calificate sau trebuie să aibă un cont curent actual de depozit la o instituție financiară reglementată care poate fi stabilită cu documentație autentificată primită direct de la o instituție financiară reglementată, care să verifice că solicitantul are un cont curent activ de depozit la cerere cu instituția.

3.2.2.2 DBA (Doing Business)/Denumire comercială

Nu se aplică – certSIGN nu emite certificate cu denumirea comercială sau DBA.

3.2.2.3 Verificarea tarii

Pentru TLS - DV, OV, EV, QWAC
Dacă este prezent obiectul: fieldName, RA verifică țara asociată subiectului utilizând una din următoarele opțiuni:

a) Cesiunea de adrese IP pentru fiecare țară
   (i) adresa IP a site-ului web, după cum indică înregistrarea DNS pentru site-ul web sau
   (ii) adresa IP a subiectului / beneficiarului;
b) ccTLD (Domeniul de nivel superior al codului de țară) al numelui de domeniu solicitat;
c) informații furnizate de către registrul de nume de domeniu; sau
d) conform cu secțiunea 3.2.2.1.

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

3.2.2.4 Validarea autorizării sau a controlului domeniului

Pentru TLS - DV, OV, EV, QWAC
Această secțiune definește procesele și procedurile permise pentru validarea proprietății sau controlului asupra domeniului.

certSIGN confirmă că, înainte de emitere, a validat fiecare nume de domeniu complet calificat (FQDN) ce apare in Certificat, folosindcel putin una din metodele de mai jos.

certSIGN va efectua verificarea domeniului pentru toate SAN-urile incluse în cerere. Prin urmare, pot fi accesate mai multe contacte administrative sau pot fi necesare mai multe acțiuni pentru a demonstra verificarea domeniului pentru toate SAN-urile solicitate.

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

Validările complete ale autorității solicitante pot fi valabile pentru eliberarea mai multor certificate în timp. În toate cazurile, validarea trebuie să fi fost inițiată în termenul specificat în cerința relevantă (cum ar fi secțiunea 4.2.1 din acest document) înainte de eliberarea certificatului. În scopul validării domeniului, termenul Solicitant include Compania-mamă a solicitantului, filială sau companie afiliată.

certSIGN păstrează înregistrări cu metodele de validare a domeniului, inclusiv numărul relevant de versiune BR folosit pentru a valida fiecare domeniu.

3.2.2.4.1 Validarea solicitantului ca contact de domeniu
Nu este folosită această metodă de validare a domeniului.

3.2.2.4.2 E-mail, fax, SMS sau poștă la contactul de domeniu
Nu este folosită această metodă de validare a domeniului.

3.2.2.4.3 Contactul telefonic cu contactul de domeniu
Nu este folosită această metodă de validare a domeniului.

3.2.2.4.4 E-mail construit pentru a contacta domenii

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

Valoarea aleatorie rămâne valabilă pentru a fi utilizată într-un răspuns confirmator timp de 30 de zile de la crearea sa.

E-mailul de răspuns trebuie să fie trimis utilizând contul de e-mail utilizat pentru trimiterea inițială și certSIGN verifică dacă valoarea aleatorie este aceeași.

Această metodă este potrivită pentru validarea numelor de domeniu Wilcard (pentru DV și OV).

3.2.2.4.5 Documentul de autorizare a domeniului

Nu este folosită această metodă de validare a domeniului

3.2.2.4.6 Schimbare la site-ul web

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.7 Modificarea DNS

certSIGN va trimite un e-mail persoanei de contact care a trimis cererea pentru a confirma că solicitantul deține controlul asupra numelui de domeniu. Emailul va include o valoare aleatoare (generată prin mijloace tehnice, unică în fiecare e-mail) pentru a fi adăugată în intrarea DNS într-una din înregistrările DNS CNAME, TXT sau CAA a domeniului care trebuie verificat.
Valoarea aleatoare rămâne valabilă pentru utilizare timp de 30 de zile de la crearea sa.
certSIGN verifică dacă valoarea din înregistrarea DNS este aceeași cu cea transmisă.
Odată ce FQDN a fost validat utilizând această metodă, CERTSIGN poate emite, de asemenea, Certificate pentru alte FQDNs care se termină cu toate etichetele de domeniu ale FQDN validat.
certSIGN a pus în aplicare coroborarea emiterii din perspective multiple (MPIC), asa cum se specifică la punctul 3.2.2.9.
Această metodă este potrivită pentru validarea numelor de domeniu Wilcard (pentru DV și OV).

3.2.2.4.8 Adrese IP

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.9 Certificat de testare

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.10 TLS folosind un număr aleatoriu

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.11 Orice altă metodă

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.12 Validarea solicitantului ca persoană de contact a domeniului

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.13 Email către contactul DNS CAA

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.14 Email către contactul DNS TXT record

Nu este folosită această metodă devalidare a domeniului.

3.2.2.4.15 Legătură telefonică cu contactul domeniului

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.16 Legătură telefonică cu contactul DNS TXT record

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.17 Legătură telefonică cu contactul DNS CAA

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.18 Schimbare agreată la site-ul web v2

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.19 Schimbare agreată la site-ul web -ACME

certSIGN confirmă controlul solicitantului asupra unui FQDN prin validarea controlului domeniului FQDN utilizând metoda ACME HTTP Challenge definită în secțiunea 8.3 din RFC 8555. Acest lucru se realizează prin primirea unui răspuns HTTP de succes la cerere. Tokenul nu este utilizat mai mult de 30 de zile de la crearea sa.
Atunci când certSIGN Web CA G2 urmează redirecționări, acestea sunt inițiate la nivelul protocolului HTTP și sunt rezultatul unui răspuns cu cod de stare HTTP 301, 302 sau 307, astfel cum este definit în RFC 7231, secțiunea 6.4, sau al unui răspuns cu cod de stare HTTP 308, astfel cum este definit în RFC 7538, secțiunea 3. Redirecționările sunt valoarea finală a antetului de răspuns HTTP Location, astfel cum este definit în RFC 7231, secțiunea 7.1.2.
certSIGN a pus în aplicare coroborarea emiterii din perspective multiple (MPIC), asa cum se specifică la punctul 3.2.2.9.

3.2.2.4.20 TLS folosind ALPN

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.21 DNS marcat cu Account ID – ACME

Nu este folosită această metodă de validare a domeniului.

3.2.2.4.22 DNS TXT Record with Persistent Value

Nu este folosită această metodă de validare a domeniului.

3.2.2.5 Autentificare pentru o adresa IP

Nu sunt emise certificate de adresa IP conform acestui CPP.

3.2.2.6 Validarea domeniului Wildcard

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

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

3.2.2.7 Precizia sursei de date

Înainte de a utiliza orice sursă de date ca sursă de date fiabile, certSIGN evaluează sursa pentru fiabilitatea, precizia și rezistența la alterare sau falsificare. certSIGN consideră în timpul evaluării următoarele:

1. Vechimea informațiilor furnizate,
2. Frecvența actualizărilor la sursa de informații,
3. Furnizorul de date și scopul colectării datelor,
4. Accesibilitatea publică și disponibilitatea datelor,
5. Dificultatea relativă în falsificarea sau modificarea datelor,
6. Alte industrii, în afară de cea a certificatelor, se bazează pe sursa de date pentru localizare precisă, contact, sau alte informații,
7. Furnizorul sursei de informații își actualizează datele cel puțin anual.

3.2.2.8 Inregistrarile Autorității de Autentificare si Certificare (CAA)

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

La procesarea înregistrărilor CAA, certSIGN procesează etichetele de proprietate issuewild și iodef, asa cum este specificat în RFC 8659. certSIGN respectă nivelul critic și nu emite un certificate daca întâmpină o etichetă de proprietate cu acest flag set. certSIGN tratează un set de înregistrări de resurse CAA care nu este gol și care nu conține nici o etichetă de proprietate ca permisiune de a emite, cu condiția să nu existe înregistrări în registrul de resurse CAA care de altfel să interzică emiterea.

CertSIGN NU va emite un certificat, cu excepția cazului în care cererea de certificat este compatibilă cu setul de înregistrare a resurselor din CAA aplicabil. Dacă există o înregistrare CAA, atunci trebuie să fie listată certSIGN ca CA autorizat. Înregistrarea permisă este certsign.ro. În cazul în care CA-ul emite, aceasta o face în termenul TTL al înregistrării CAA sau în termen de 8 ore, oricare dintre acestea este mai mare.

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

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

3.2.2.9 Coroborarea Emiterii prin Perspective Multiple (MPIC)

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

Setul de răspunsuri de la perspectivele de rețea invocate furnizează CA informațiile necesare pentru a-i permite să evalueze în mod afirmativ
- a. prezența valorii aleatorii, a tokenului de cerere sau a adresei de contact preconizate, în conformitate cu metoda de validare de încredere specificată în secțiunea 3.2.2.4 și
- b. autoritatea CA de a emite pentru domeniul (domeniile) solicitat(e), astfel cum se specifică în secțiunea 3.2.2.8.
Detalii privind cerințele MPIC se regăsesc în CA/B Forum Baseline Requirements #3.2.2.9. certSIGN a implementat MPIC utilizând cel puțin două (2) perspective de rețea la distanță.

3.2.3 Autentificarea identității persoanelor fizice

certSIGN nu eliberează certificate TLS persoanelor fizice.

Procesul de înregistrare conține dispoziții pentru determinarea identității persoanelor care acționează în calitate de **Solicitanți**. Identificarea se realizează după cum urmează:

- Abonatul este prezent în persoană sau printr-o procedură la distanță echivalentă în conformitate cu ETSI EN 319 411-1 #6.2.2. Această etapă poate fi efectuată de către:
  - operatorul RA care procesează cererea de certificat,
  - un notar acreditat,
  - un partener instruit și contractat, delegat pentru serviciul de identificare.
- Solicitantul persoană fizică prezintă un original valabil al unui document de identificare recunoscut de legislația națională. Agentul de identificare trebuie să facă o copie, o scanare sau o fotografie de înaltă calitate a documentului de identificare, să inspecteze copia pentru a depista orice indiciu de alterare sau falsificare și să confirme executarea corectă a identificării în scris sau electronic, astfel cum s-a convenit cu FST.
- Fotografia din documentul de identificare este comparată și trebuie să corespundă (trăsături faciale, vârstă, sex și mărime) persoanei prezente, astfel cum este descris mai sus.

Pentru certificate EV/QWAC, RA care operează sub certSIGN Web CA G2 efectuează o verificare a identității și autorității semnatarului contractului, a aprobatorului certificatului și a solicitantului certificatului asociat cu cererile EV/QWAC care sunt prezentate de un solicitant sau un beneficiar. Pentru a stabili acuratețea unei identități individuale, RA trebuie să efectueze verificarea identității și a autorității în conformitate cu cerințele stabilite în Ghidul EV publicat de Forumul CA / Browser.

CMPP al certSIGN Poate, la discreția sa, să actualizeze practicile de verificare pentru a îmbunătăți procesul de verificare a identității organizației. Orice modificare a practicilor de verificare se publică în conformitate cu procedurile standard de actualizare a CPP.

3.2.4 Informații neverificate ale Beneficiarului

certSIGN nu include informații neconfirmate despre beneficiari în Certificate. certSIGN nu este răspunzător pentru informațiile neconfirmate ale Beneficiarului transmise certSIGN sau prezentate în alt mod cu intenția de a fi incluse într-un certificat, cu excepția cazului în care ar fi fost altfel specificat în legătură cu certificatele TLS emise în conformitate cu cerințele Regulamentului European 1183 / 2024.

3.2.5 Validarea autorității

Toate TLS:

Autentificarea autorizațiilor face parte din procedura efectuată de Autoritatea de Înregistrare sau de Autoritățile de Certificare pentru a procesa cererea de certificat pentru un dispozitiv

care aparține unei persoane juridice. certSIGN utilizează o Metodă de Comunicare Fiabilă pentru a verifica autenticitatea cererii de certificat a Reprezentantului Solicitantului, așa cum este enumerat în secțiunea 3.2.2.

certSIGN stabilește autenticitatea cererii de certificat direct cu Reprezentantul Solicitantului sau cu o sursă autorizată din cadrul organizației Solicitantului, cum ar fi birourile principale de afaceri ale Solicitantului, birourile corporative, birourile de resurse umane, birourile de tehnologia informației sau alt departament pe care certSIGN îl consideră adecvat.

În plus, certSIGN a stabilit un proces care permite unui solicitant să specifice persoanele care pot solicita certificate. În cazul în care un Solicitant specifică, în scris, persoanele care pot solicita un certificat, certSIGN nu va accepta nicio solicitare de certificat care nu se încadrează în această specificație. certSIGN furnizează Solicitantului o listă a solicitanților autorizați de certificate la solicitarea scrisă verificată a Solicitantului.

EV/QWAC:
Pentru certificatele emise la solicitarea agentului beneficiarului, atât agentul, cât și Beneficiarul vor da despăgubiri în totalitate și în deplină siguranță companiei certSIGN, companiilor sale mamă, filialelor, directorilor, ofițerilor, angajaților, agenților și contractanților.

Beneficiarul controlează și răspunde de datele pe care un agent al beneficiarului le furnizează certSIGN. Beneficiarul trebuie să notifice cu promptitudine certSIGN despre orice declarații false și omisiuni făcute de un agent al Beneficiarului. Datoria acestui articol este continuă.

Autoritatea persoanelor fizice - semnatarii contractelor, aprobatorii de certificate și solicitanții de certificate - care acționează ca agenți ai beneficiarului, este confirmată prin primirea unui inscris de autoritate EV/QWAC de la beneficiar semnat de o persoană cu autoritate (adică o "persoană care confirmă").

(1) Solicitare de confirmare. Persoanele care au această autoritate sunt contactate de certSIGN printr-o comunicare adecvată offline care solicită verificarea sau confirmarea faptului particular în cauză, adică autorizația persoanei în calitate de semnatar al contractului, de aprobator al certificatului sau de reclamant al certificatului.

(A) Destinatar. Cererea pentru Scrisoarea de autoritate EV/QWAC / Contractul Master este îndreptată către:

a. O poziție în cadrul organizației solicitantului care se califică drept Persoană de confirmare (de exemplu secretar, președinte, CEO, CFO, COO, CIO, CSO, director etc.) și care este identificată prin nume și titlu într-un extras curent de la Registrul național al comerțului , Un aviz juridic verificat, o scrisoare de verificare verificată sau prin contactarea departamentului de resurse umane al solicitantului prin telefon sau prin poștă (la numărul de telefon sau adresa pentru sediul solicitantului, verificată în conformitate cu Ghidul); sau
b. Agentul înregistrat al solicitantului, persoana fizică înregistrată sau sediul social aflat în jurisdicția de înființare sau de înregistrare, astfel cum figurează în fișele oficiale ale Agenției, cu instrucțiuni de transmitere către o persoană de confirmare; sau
c. O persoană denumită individual, verificată și care se afla pe linie manageriala deasupra semnatarului contractului sau a aprobatorului de certificat prin contactarea

departamentului de resurse umane al solicitantului prin telefon sau prin poștă (la numărul de telefon sau adresa pentru sediul solicitantului, verificată în conformitate cu ghidurile EV).

(B) Mijloace de comuniare. Bazat pe (A) cele de mai sus, cererea de confirmare este directionata catre Persoana de confirmare intr-o maniera rezonabila astfel incat sa ajunga la persoana respective. Urmatoarele optiuni sunt acceptate:

(i) În cazul în care cererea pentru scrisoarea de autorizare EV / contractul master este trimisă prin corespondență pe suport de hârtie, aceasta este adresată:

(a) Adresa verificată a locului de afaceri al solicitantului;

(b) Adresa comerciala a Persoanei de Confirmare specificată într-un extras curent din Registrul Național al Comerțului, un aviz legal verificat sau o scrisoare contabila verificată; sau

(c) Adresa inregistrata a Agentului solicitantului înscrisă în înregistrările oficiale ale jurisdicției de înființare sau înregistrare.

(ii) Dacă cererea pentru scrisoarea de autorizare EV/QWAC / contract Master este trimisă prin e-mail, aceasta este adresată adresei de e-mail a Persoanei de Confirmare furnizată de Departamentul de Resurse Umane al solicitantului în conformitate cu punctul (A) de mai sus sau așa cum sunt enumerate în extrasul Registrul Național al Comerțului, un aviz legal verificat sau o scrisoare contabilă verificată.

(iii) În cazul în care cererea pentru autorizare EV/QWAC / Contract Master se face prin apel telefonic, persoana de confirmare este contactată prin apelarea numărului principal de telefon confirmat al locului de afaceri al solicitantului, solicitând să vorbească cu o astfel de persoană, iar persoana care efectuează apelul identifică insași sau ca atare persoană.

(iv) În cazul în care cererea pentru autorizare EV/QWAC / Acordul general este trimisă prin fax, atunci aceasta este trimisă la numărul de fax menționat într-o sursă actuală de informații guvernamentale calificate, o sursă independentă de informații calificate, un aviz legal verificat sau o scrisoare de verificare, verificată cu Pagina de titlu a faxului adresată în mod clar Persoanei de Confirmare.

(2) Răspunsul la confirmare. Primirea de către certSIGN a scrisorii de autorizare EV/QWAC de la Persoana de Confirmare este verificată prin telefon, e-mail sau prin orice altă comunicare scrisă între certSIGN și Persoana de Confirmare.

(3) Verificarea numelui, titlului și autorității semnatarului contractului și a aprobării certificatului. Liniile directoare impun ca certSIGN să verifice numele, titlul și autoritatea semnatarilor contractului și a aprobatorilor de certificate. scrisoarea de autorizare EV/QWAC / acordul general încheiat îndeplinește aceste obiective prin furnizarea de către solicitant a unei confirmări independente cu privire la acest nume, titlu și autoritate, așa cum este prezentat mai sus. Atestările din scrisoarea de autorizare EV/QWAC / acordul general includ autoritatea de angajare și semnare a semnatarului contractului și a autorității de aprobare a autorității de certificare a certificatelor.

(4) În conformitate cu Sectiunea 22(d)(3) a Ghidului, certSIGN se pot baza pe o Persoană de confirmare pentru a confirma propriile informații de contact: Adresa de e-mail, numărul de telefon și numărul de fax. certSIGN se poate baza, de asemenea, pe aceste informații de contact verificate pentru corespondența ulterioară cu Persoana de Confirmare dacă:

(i) Domeniul adresei de e-mail este deținut de Solicitant și este adresa de e-mail a Persoanei de Confirmare și nu un alias al unui grup de e-mail-uri.

(ii) Numărul de telefon / fax al Persoanei de Confirmare este verificat de CA pentru a fi un număr de telefon care face parte din sistemul telefonic al organizației și nu este numărul personal de telefon al persoanei.

3.2.6 Criterii pentru interoperare

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

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

Vezi sectiunea 4.9.1 pentru informatii despre procedurile de revocare ale certSIGN.

3.4 Identificarea și autentificarea pentru cererile de revocare

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

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

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

Următoarele entități pot trimite cereri de revocare a certificatelor:

- Beneficiarul care încheie un acord contractual cu certSIGN pentru emiterea de certificate.
- Autoritatea de Înregistrare care poate cere revocarea fie în numele unui Beneficiar, sau dacă deține informații care justifică revocarea certificatului, prin crearea unei cereri autentificate utilizând mecanismele de securitate ale software-ului Autorității de Înregistrare
- Rolurile de încredere asociate certSIGN Web CA G2, sub supravegherea Comitetului de Management al Politicilor și Procedurilor (PPMB), prin crearea unei cereri autentificate utilizând mecanismele de securitate ale software-ului Autorității de Certificare.

4 Cerințe operaționale privind ciclul de viață al certificatului

Acest capitol descrie procedurile de bază care sunt comune certificatelor TLS emise de certSIGN Web CA G2.

4.1 Cererea de certificat

4.1.1 Cine poate trimite o cerere de certificate

certSIGN Web CA G2 păstrează o bază de date internă a tuturor certificatelor revocate anterior și a cereri lor de certificate respinse anterior din cauza presupusului phishing sau a altor utilizări frauduloase. Aceste informații sunt utilizate pentru a identifica ulterior cererile de certificate suspecte.

certSIGN eliberează certificate EV/QWAC numai solicitanților care îndeplinesc condițiile de Organizație Privată, Entitate guvernamentală, Entitate comercială sau Entitate necomercială specificate la punctul 4.1.1 din versiunea actuală a " CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates".

Cererile de certificat ale Persoanelor Fizice

certSIGN nu emite certificate TLS pentru persoane fizice.

Cererile de certificat ale Persoanelor Juridice (Organizații)

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

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

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

4.1.2 Procesul de înregistrare și responsibilitățile

Procesul de înregistrare este gestionat de o entitate specifică numită Autoritatea de Înregistrare sau RA, care este operată direct de certSIGN sau se bazeaza pe terta parte in acord cu legile nationale si cerintele ETSI/CABF.

certSIGN furnizează infrastructura și resursele operaționale pentru funcționarea RA. certSIGN oferă de asemenea supraveghere, suport și audit pentru toate procesele și serviciile RA. RA este responsabil pentru verificarea următoarelor elemente:

- Identitatea declarată a Beneficiarului,
- Atributele revendicate ale Beneficiarului,
- Dreptul Beneficiarului la certificatul solicitat.

Procesul de inregistrare este realizat în conformitate cu regulile și metodele descrise în prezentul CPP și în ghidurile și procedurile interne ale RA și în legislația aplicabilă.

Pentru EV/QWAC:

Următoarele roluri sunt necesare pentru emiterea unui EV/QWAC:

- Solicitantul certificatului –Cererea EV/QWAC trebuie sa fie semnata și transmisa de catre un solicitant de certificate autorizat.
- Aprobator de certificat – Cererea EV/QWAC trebuie verificata și aprobata de catre un Aprobator de Certificat autorizat.
- Semnatar al contractului – Un contract asociat EV/QWAC-ului solicitat trebuie semnat de un semnatar de contract autorizat.

Pentru toate TLS-urile:

Înainte de eliberarea unui certificat, CA va OBȚINE următoarea documentație de la solicitant:

1. O solicitare de certificat, care poate fi electronică; și
2. Un Contract sau Condiții de utilizare, care pot fi electronice.

Beneficiarului i se oferă următoarele informații care constituie Contractul:

- Formularul de inregistrare
- Termenii și Conditiile certificatului
- Adresa online a CPP
- Notele, notificările sau alte documente furnizate de Beneficiar (care vor fi definite în contract)

Formularul de înscriere semnat este considerat acceptarea formală de către Beneficiar a Contractului prin care Beneficiarul acceptă următoarele:

- Raspunderea sa ca informatiile furnizate catre RA sunt corecte, complete, valabile și actualizate,
- Ca certSIGN are o perioada de retentie de 10 ani, începând cu data emiterii certificatului, cu privire la toate informațiile referitoare la înregistrare și înscriere, cererea de certificat, revocarea certificatului,
- În cazul în care certSIGN (CA și RA) își încetează activitățile, aceste date pot fi transferate către o terță parte, respectând aceasi termeni și condiții definite în Contract,
- Recunoaște drepturile, obligațiile și responsabilitățile certSIGN și ale celorlalți participanți PKI, așa cum sunt definiți în contract și în legislația națională,
- Beneficiarul are obligația de a informa certSIGN despre orice schimbări sau evenimente care pot afecta valabilitatea sau conținutul certificatului.

Pentru OV, EV, QWAC:

Informatiile extrase din CSR-ul PKCS#10, de exenplu: numele companiei din campul Organizational name (e.g., O= CERTSIGN SA) și numele domeniului din domeniul Common Name (CN=www.certsign.ro) incluse în CSR-ul PKCS#10 sunt verificate cu numele legal al organizatiei din cerere. Dacă numele comun nu este acelasi, solicitantul de certificate trebuie să facă corecțiile necesare și să genereze și să retrimită noul PKCS # 10 pentru a putea continua. (Dacă alte informații nu se potrivesc, este posibil ca un nou PKCS # 10 să nu fie necesar, în funcție de platforma serverului.). Personalul de înregistrare certSIGN compară informațiile transmise de solicitant pentru a se asigura că sunt în concordanță cu informațiile primite conform cap. 3.2.2.4, CA/Browser Forum BR înainte de a permite continuarea procesului de aplicare.

Procesul de înregistrare

Procesul de înregistrare începe în cadrul RA.

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

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

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

RA este responsabilă pentru furnizarea și / sau verificarea informațiilor cu privire la atributele Beneficiarului (atribute profesionale, atribute organizaționale etc.). RA verifică și completează datele de înscriere. RA este responsabilă pentru acuratețea datelor care vor fi încorporate în

cererea de certificat depusă la CA. RA este responsabilă pentru înregistrarea / înscrierea corectă a beneficiarilor și pentru furnizarea de către CA a conținutului corect pentru câmpurile variabile din certificat.

4.2 Procesarea cererilor de certificate

Pentru DV:

certSIGN acceptă cereri depuse individual sau colectiv.
Cererile pot fi trimise on-line sau off-line.
Cererea de certificat se completează în format electronic:

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

Pentru DV si OV:

Cererea de certificat este completată off-line:

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

Pentru EV & QWAC:

În timpul procesului de aprobare a certificatului, personalul de înregistrare al certSIGN utilizează controale pentru a valida identitatea Beneficiarului și alte informații prezentate în cererea de certificat. Personalul de înregistrare al certSIGN revizuiește informațiile furnizate de catre solicitant pentru a asigura conformitatea cu Ghidul CABF EV.

Procesarea cererii în Autoritatea de Inregistrare

Orice cerere este procesată în modul următor:

- Operatorul Autorității de Înregistrare primește solicitarea Beneficiarului,
- Operatorul verifică datele din solicitare referitoare la subiect și beneficiar,
- În urma verificării, operatorul confirmă identitatea dintre datele declarate și cele incluse în cerere; Dacă cererea conține date neconforme, aceasta este respinsă,
- Solicitarea confirmată este trimisă Autorității de Certificare,
- Autoritatea de înregistrare verifică și alte date care nu sunt specificate în cerere, dar sunt, de asemenea, necesare pentru emiterea certificatului.

Procesarea cererii în Autoritatea de Certificare

Autoritatea de Certificare verifică dacă Autoritatea de Înregistrare a confirmat cererile. Următorii pași descriu etapele privind procesarea cererilor de certificate:

Pasul 1: Solicitantul certificatului completează formularul de solicitare a certificatului, PKCS # 10 CSR, numele comun, informațiile despre organizatie, adresa și informațiile de facturare, împreună cu semnătura sa electronică sau în formatul fizic, cu semnătură scrisă de mână. Solicitantul transmite certSIGN alte informații necesare, inclusiv numele de contact ale personalului din cadrul organizației care au autoritatea de a aproba cererea și de a semna contractul. Solicitantul furnizează o comandă de cumpărare pentru a verifica plata pentru procesarea solicitării și pentru emiterea certificatului EV/QWAC.

Pasul 2: certSIGN verifică toate informațiile din Ghiduri care trebuie verificate, utilizând o varietate de surse, inclusiv Registrul Național al Comerțului sau organisme nationale similare de incredere in cazul beneficiarilor din afara Romaniei, ICANN, Ministerul Finanțelor, Scrisorile Contabile, Avizele juridice și Departamentul de Resurse Umane al Solicitantului.

Pasul 3: certSIGN solicită și primește de la Solicitant o scrisoare de autorizare EV/QWAC / acord general semnat (cu excepția cazului în care deja este în posesia unei scrisoari de autorizare EV/QWAC / acord general).

Pasul 4: Semnatarul contractului acceptă și semnează contractul în format electronic sau fizic pe suport de hârtie și semnătură scrisă de mână. După aceasta, procesarea cererii.

Pasul 5: Aprobatorul certificatului este fie contactat prin telefon, fie direcționat către o pagină web prin care se obține aprobarea emiterii certificatului.

Pasul 6: Toate semnăturile solicitanților de certificare, a aprobatorilor de certificate și a semnatarilor contractului sunt verificați prin proceduri de urmărire sau prin apeluri telefonice. În mod alternativ, în cazul în care semnăturile sunt efectuate utilizând certificate calificate conforme cu normele UE 1183/2024, nu se efectuează alte verificări.

Pasul 7: Doi (2) operatori certSIGN (Un ofiter de Inregistrare și un specialist validare) sunt necesari pentru aprobarea emiterii certificatului (vezi Final Cross-Correlation și Due Diligence de mai jos).

Pasul 8: Un sistem securizat este utilizat pentru a trimite solicitarea de generare a certificatelor către certSIGN Web CA, iar certificatul Web calificat este creat.

Pasul 9: Solictantul certificatului este notificat că certificatul a fost creat și este gata pentru descărcare (sau este trimis către solicitant arhivat printr-un e-mail).

Pentru toate TLS-urile:

RA verifică înregistrările CAA și urmează instrucțiunile de procesare găsite, pentru fiecare dNSName în extensia subjectAltName a certificatului care urmează a fi emis, conform specificațiilor RFC 8659 (Anexa A). certSIGN nu va emite un certificat decât dacă cererea de certificat este in concordanță cu setul de înregistrări CAA aplicabil.
Dacă există înregistrare CAA, atunci trebuie sa includă și certSIGN ca Autoritate de certificare autorizată. Înregistrarea permisă este certsign.ro și înregistrările CAA „issue" sau „issuewild" sunt permise.

4.2.1 Îndeplinirea funcțiilor de identificare și autentificare

RA realizează identificarea și autentificarea în conformitate cu procedura definite în capitolul 3.2.
RA colectează și validează informațiile despre identitatea și despre atributele Subiectului și ale Beneficiarului.
Cererea de Certificat cu Risc Înalt este o Cerere pe care CA-ul o marchează pentru o examinare suplimentară în raport cu criteriile interne și bazele de date întreținute de CA, care pot include nume cu un risc mai mare de phishing sau alte utilizări frauduloase, nume incluse în cererile de certificate respinse anterior sau certificate revocate, nume incluse în lista de phishing de la Miller Smiles sau în lista de Navigare sigură de la Google sau nume pe care CA le identifică utilizând propriile criterii de diminuare a riscurilor.

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

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

Pentru a preveni Cererile de Certificat cu Risc Inalt înainte de aprobarea certificatului, procedura internă de verificare va solicita incă una din următoarele dovezi:

- Examinarea atentă a FQDN pentru a confirma dacă intenția Solicitantului este de a imita sau induce în eroare clienții;
- Verificarea încrucișată manuală și revizuirea tuturor informațiilor furnizate de Beneficiar
- Verificare cel puțin a listei actualizate de persoane, grupuri și entități, care sunt subiectul Articolelor 2,3 și 4 din Common Position 2001/931/CFSP în aplicarea măsurilor specifice de combatere a terorismului. Documentație suplimentară care confirmă controlul domeniului de la solicitant și / sau alte dovezi verificabile, considerate necesare de către CMPP.

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

4.2.2 Aprobarea sau respingerea cererilor de certificate

Pentru DV si OV:

Aprobarea sau respingerea cererilor de certificate sunt realizate de RA. RA validează fiecare cerere și poate respinge o cerere de certificat dacă cererea nu poate fi autentificată sau dacă Cererea nu respectă regulile și standardele care guvernează certSIGN Web CA G2 sau din alte motive, la discreția și sub răspunderea RA.

Cererile de certificate sunt prelucrate în cele din urmă de sistemul certSIGN CA care validează fiecare cerere și poate respinge o cerere de certificat în cazul în care cererea nu poate fi autentificată sau dacă cerea nu respectă regulile și standardele definite pentru tipul de certificat, la discreția și sub răspunderea certSIGN.

Pentru EV si QWAC:

Înainte de a determina dacă să aprobe sau să respingă o cerere de EV/QWAC, certSIGN efectuează alte verificări cerute de Ghiduri, inclusiv următoarele:

1. Cererile pentru EV/QWAC sunt testate pentru ținte cu risc ridicat de phishing și alte scheme frauduloase. certSIGN verifică liste interne și externe ale denumirilor organizațiilor care sunt cel mai frecvent vizate în phishing și alte scheme frauduloase și marcheaza automat astfel de cereri de EV/QWAC pentru examinare suplimentara înainte de emitere.
2. Numele persoanelor fizice, numele solicitanților, locațiile fizice și juridice ale solicitanților de EV/QWAC sunt revizuite pentru a determina dacă sunt identificate pe o listă a persoanelor interzise, sau pe o altă listă care interzice desfășurarea afacerilor cu o astfel de organizație, conform 3.2.2.1.

Final Cross-Correlation și Due Diligence

Aprobarea emiterii de certificate de catre certSIGN necesita doi Operatori (Operator Inregistrare și Specialist Validare. (Vezi sectiunea 5.2.2, Numărul de persoane necesare pentru fiecare sarcină și secțiunea 5.2.4, Roluri care necesită separarea sarcinilor).

(a) Procedurile certSIGN garantează că un operator de înregistrare care nu este responsabil pentru colectarea și revizuirea informațiilor examinează toate informațiile și documentația asamblate în sprijinul EV/QWAC și caută discrepanțe sau alte detalii care necesită explicații suplimentare.
(b) certSIGN solicită, obține și documentează explicații sau clarificări suplimentare din partea solicitantului, a aprobatorului de certificat, a solicitantului de certificate, a surselor de informații independente calificate și / sau a altor surse de informații necesare pentru a rezolva discrepanțele sau detaliile care necesită explicații suplimentare.
(c) certSIGN nu eliberează un EV/QWAC până când întregul corp de informații și documentație asamblat în sprijinul EV/QWAC este de așa natură încât emiterea certificatului nu va comunica informații factuale inexacte pe care certSIGN le cunoaște sau dacă exercițiul de diligență ar trebui să le descopere. Dacă nu se primește o explicație satisfăcătoare și / sau o documentație suplimentară într-un termen rezonabil, certSIGN va refuza cererea EV/QWAC și va notifica Solicitantul.
(d) certSIGN îndeplinește cerințele legate de corectitudinea finală și diligența datorată prin intermediul angajaților aflați sub controlul său și care au pregătirea, experiența și judecata corespunzătoare pentru a confirma identificarea și autorizarea organizațională.
(e) În cazul în care o parte sau toată documentația utilizată pentru a susține cererea este într-o altă limbă decât cea engleză sau română, un angajat al certSIGN cu calificare, experiență și judecată corespunzătoare în confirmarea identificării și autorizării organizaționale îndeplinește cerințele acestei corelații finale și a diligenței datorate. Atunci când angajații certSIGN nu dispun de competențele lingvistice necesare, certSIGN se bazează pe traducerile părților relevante ale documentației furnizate de un traducător calificat.

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

După finalizarea cu succes a tuturor validărilor cerute pentru o cerere de certificate, certSIGN va aproba cererea de EV/QWAC.

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

Solicitanții ale căror cereri au fost respinși pot reaplica ulterior.
Pentru toate TLS:
certSIGN nu emite certificate cu extensia subjectAlternativeName sau câmpul Subject commonName care conține o adresă IP rezervată sau un nume intern.

Intrările din dNSName TREBUIE să fie în "sintaxa preferată a numelui", astfel cum se specifică în RFC 5280, și, prin urmare, NU TREBUIE să conțină caractere de subliniere ("_").

4.2.3 Timpul de proceare a cererilor de certificate
certSIGN nu emite un certificat imediat după înregistrare. Certificatele trebuie să fie emise de Autoritatea de Certificare prin aprobarea cererii de certificat după ce ea a fost validată de RA; de aceea certificatele nu sunt disponibile Beneficiarului imediat dupa ce sunt create de catre CA.

4.3 Emiterea certificatelor
După primirea și prelucrarea unei solicitări (a se vedea capitolele 4.1 și 4.2), Autoritatea de Certificare emite un certificat. După emiterea certificatului, certSIGN îl publică în depozitarele corespunzătoare. Perioada de valabilitate a certificatelor eliberate depinde de tipul certificatului și de categoria Subiectului și se conformează perioadelor prezentate în Tabelul 6.3.2.2.
certSIGN informează Beneficiarul cu privire la emiterea certificatului prin trimiterea unui e-mail (la adresa furnizată de către Beneficiar) care permite Beneficiarului să obțină certificatul. Fiecare certificat emis este publicat în depozitarul certSIGN. Publicarea certificatului este echivalentă cu notificarea de către alte entitati partenere a faptului că a fost emis un certificat pentru un subiect.

4.3.1 Acțiunile CA în timpul emiterii certificatelor
Certificatul este emis ca parte a procesului de înscriere a certificatului. CA va primi doar cereri de certificate de la RA. CA, RA și procesul de personalizare sunt sisteme integrate și comunică prin conexiuni de rețea închise. CA proceseaza numai cereri care provin de la RA-ul de incredere al certSIGN.
Pentru fiecare solicitare de certificat, CA va efectua următoarele verificări și acțiuni:

- Cererea provine de la RA?,
- CA verifică autorizația solicitantului pentru tipul de solicitare și refuză cererile care se referă la profilurile certificatelor pentru care solicitantul nu este autorizat.
- CA, de asemenea, compara cererea de certificat cu un profil de certificat predefinit. Informațiile variabile din cerere trebuie sa se potrivesc cu șablonul și setul de reguli al profilului certificatului.
- CA adaugă la certificat informații non-variabile și variabile, așa cum sunt definite în profilul de certificat specificat.

- CA-ul asigură unicitatea fiecărui certificat pe care îl emite pe baza câmpului SerialNumber din fiecare certificat.

certSIGN Web CA G2 a implementat un proces de Linting pentru a testa conformitatea tehnică a fiecărui artefact care urmează să fie semnat înainte de a-l semna. Metoda utilizată pentru a produce un certificat care conține conținutul certificatului care urmează să fie semnat constă în semnarea certificatului tbsCertificate cu o cheie privată "fictivă" a cărei componentă cheie publică nu este certificată de un certificat care se leagă de un certificat CA de încredere publică.
certSIGN Web CA G2 utilizează un proces Linting pentru a testa fiecare certificat emis.

4.3.2 Notificarea Beneficiarului de către CA cu privire la emiterea certificatului

Certificatul este emis ca parte a procesului de înscriere a certificatului. Beneficiarul primește o notificare privind eliberarea certificatului.
Cu o lună înainte de expirarea certificatului, Beneficiarul este informat că certificatul este pe cale să expire.

4.4 Acceptarea certificatului

4.4.1 Conduita care constituie acceptarea certificatului

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

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

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

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

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

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

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

- Informațiile din certificat sunt incorecte,
- Informațiile din certificat au devenit nevalide de la data înregistrării,
- Pierderea dreptului Beneficiarului.

Obligațiile Beneficiaruluișsi RA în cazul respingerii:

- RA solicită revocarea certificatelor,
- RA execută revocarea certificatului.

4.4.2 Publicarea certificatului de către CA

Vezi capitolul " PUBLICARE ȘI RESPONSABILITĂȚI DEPOZITAR "

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

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

4.5 Utilizarea perechii de chei și a certificatului

4.5.1 Utilizarea cheii private și a certificatului Beneficiarului

certSIGN emite certificate pentru cheile furnizate de abonați în cererile de certificate.

Beneficiarii își protejează accesul la cheile private de personalul neautorizat sau de alte terțe părți.

Beneficiarii utilizează cheile private numai în conformitate cu uzanțele specificate în extensia de utilizare a cheii.

Vezi sectiunile 1.4.1, 6.1.7 și 7.1.

4.5.2 Utilizarea cheii publice și a certificatului unei Entități Partenere

certSIGN presupune ca toate aplicatiile software sunt conforme cu standardul X.509, protocolul TLS, și alte standard aplicabile ce impun cerintele și seturile de cerinte mentionate În acest CPP. certSIGN nu garanteaza ca soft-ul oricarei entitati partenere va suporta sau impune asemenea controale și cerinte, și tpoate entitatile partenere sunt sfatuite sa identifice suport tehnic și legal adecvat.

Părțile terte utilizează cheile publice și certificatele:

- În conformitate cu scopul lor declarat în prezenta SPC și în conformitate cu conținutul certificatului (câmpurile keyUsage și extendedKeyUsage),
- în conformitate cu dispozițiile acordului încheiat între abonat și certSIGN,
- numai după verificarea statutului acestora și verificarea semnăturii autorității de certificare care a emis certificatul respectiv.

Bazarea pe o sesiune TLS neverificabilă poate duce la riscuri pe care partea care se bazează și le asumă în totalitate și pe care certSIGN nu și le asumă în niciun fel.

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. În cadrul condițiilor pentru ca un certificat QWAC să fie validat ca certificat calificat UE, ancora de încredere pentru validarea certificatului va fi cea specificată în identificatorul digital al serviciului (SDI) corespunzător, din lista sigură a UE (Trusted List) pentru certSIGN.

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

Decizia finală privind posibilitatea de a avea incredere sau nu intr-o semnătură digitală sau la securitatea unei sesiuni TLS este exclusiv cea a părții de incredere. Increderea intr-o semnătură digitală sau,

TLS handshake ar trebui sa aiba loc numai daca:

- Semnatura digitala sau sesiunea TLS a fost creată în perioada operationala a unui certificat valid și poate fi verificată prin trimiterea la un certificat validat.
- Entitatea Partenera a verificat starea de revocare a certificatului prin trimiterea la CRL relevante și certificatul nu a fost revocat.
- Entitatea Partenera 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.

Increderea este acceptată ca fiind rezonabilă în conformitate cu prevederile CPP și în cadrul contractului incheiat cu Entitatea partenere. În cazul în care circumstanțele de încredere depășesc asigurările furnizate de certSIGN în conformitate cu prevederile prezentului CPP, entitatea partenera trebuie să obțină asigurări suplimentare.

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

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

Prin intermediul acestui CPP, certSIGN a informat în mod corespunzător părțile implicate cu privire la utilizarea și validarea semnăturilor digitale și a sesiunilor TLS prin intermediul acestui CPP și a altor documente publicate în depozitarul public disponibil la https://www.certsign.ro/ro/depozitar/și datorită disponibilității certSIGN prin adresele de contact specificate în secțiunile 2.2 și 9.11 ale acestui CPP.

4.6 Reinnoirea certificatului

Reînnoirea certificatului reprezintă reemiterea unui certificat pe baza datelor conținute în certificatul original.

4.6.1 Circumstanța reînnoirii certificatului

certSIGN depune eforturi rezonabile pentru a notifica abonații cu privire la datele de expirare ale certificatelor, utilizând datele de contact furnizate de abonat.

4.6.2 Cine poate solicita reînnoirea

Vezi sectiunea 4.1.1.

4.6.3 Procesarea solicitărilor de reînnoire a certificatelor

Reînnoirile sunt procesate în același mod ca și certificatele noi, astfel cum este descris în secțiunile 4.1.2 și 4.2.

4.6.4 Notificarea abonatului cu privire la eliberarea unui nou certificat

Vezi sectiunea 4.3.2.

4.6.5 Conduita care constituie acceptarea unui certificat de reînnoire

Vezi sectiunea 4.4.1.

4.6.6 Publicarea certificatului de reînnoire de către CA
Vezi sectiunea 4.4.2.

4.6.7 Notificarea eliberării certificatului de către CA către alte entități
Vezi sectiunea 4.4.3.

4.7 Rekey-ul certificatului

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

4.7.2 Cine poate solicita certificarea unei noi chei publice
certSIGN permite inițierea procesului de re-key de către Beneficiarul certificatului sau de către CA / RA care gestionează certificatul respectiv.

4.7.3 Procesarea cererilor de re-key a certificatelor
Procesul solicitarii inițiale a certificatului va fi modificat după cum urmează:

Identificarea solicitantului și rezultatele validării din cererile anterioare sunt considerate valide atata timp cat informațiile validate nu s-au modificat și acele informații sunt obținute dintr-o sursă specificată în secțiunea 3.2 cu nu mai mult de douasprezece (12) de luni înainte de eliberarea certificatului.

Dacă certSIGN și-a schimbat termenii și condițiile, Subiectul trebuie să semneze din nou noua versiune și trebuie să fie identificat față în față. Orice date care s-au schimbat trebuie să fie validate ca și cum aceasta ar fi o nouă cerere.

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 constitue 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 nu permite modificarea detaliilor certificatului pe durata de viață a certificatului. Dacă se schimbă informații referitoare la certificat, Beneficiarul trebuie să solicite revocarea certificatului original și să solicite eliberarea unui nou certificat.

4.8.1 Circumstanța modificării certificatului
Nu este stipulat.

4.8.2 Cine poate solicita modificarea
Nu este stipulat.

4.8.3 Procesarea cererilor de modificare a certificatului
Nu este stipulat.

4.8.4 Notificarea abonatului cu privire la eliberarea unui nou certificat
Nu este stipulat.

4.8.5 Conduita care constituie acceptarea unui certificat modificat
Nu este stipulat.

4.8.6 Publicarea certificatului modificat de către CA
Nu este stipulat.

4.8.7 Notificarea eliberării certificatului de către CA către alte entități
Nu este stipulat.

4.9 Revocarea și Suspendarea certificatului
Certificatele emise de certSIGN Web CA G2 pot fi revocate, dar niciodată suspendate. Revocarea certificatelor este un proces ireversibil.
Revocarea nu afectează nici tranzacțiile efectuate înainte de revocare, nici obligațiile care decurg din următoarele din prezentul CPP.
Acest capitol precizează condițiile necesare pentru ca o autoritate de certificare să aibă motive să revoce certificatul.
Dacă o cheie privată care corespunde unei chei publice conținută într-un certificat revocat rămâne sub controlul Beneficiarului*, după revocare, ar trebui să fie stocată în siguranță până când este distrusă.*
Certificatele pe termen scurt nu sunt revocate. În cazul certificatelor pe termen scurt, mecanismul de notificare a problemelor este același mecanism descris la punctul 1.5 in „Procedura de raportare a problemelor legate de certificate”.

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

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

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

1.

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

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

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

8. CA este informată că un abonat a încălcat una sau mai multe obligații materiale ale acestuia în temeiul acordului de abonat sau al condițiilor de utilizare (CRLReason #9, privilegeWithdrawn);

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

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

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

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

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

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

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

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

Cheie privată compromisă înseamnă:

(1) accesul neautorizat la cheia privată sau un motiv întemeiat de a suspecta acest lucru,

(2) pierderea cheii private sau apariţia unui motiv de a suspecta o astfel de pierdere,

(3) furtul cheii private sau apariţia unui motiv de a suspecta un astfel de furt,

(4) ştergerea accidentală a cheii private.

Cererea de revocare poate fi trimisă prin intermediul Autorității de Înregistrare (aceasta implică ca Beneficiarul trebuie să contacteze autoritatea) sau direct către o Autoritate de Certificare (cererea poate fi autentificată prin semnătură). Cererea de revocare trebuie să

conține informații care să permită autentificarea sigură a Beneficiarului de către Autoritatea de Înregistrare, în conformitate cu prevederile Capitolului 3.1.4. Dacă autentificarea identității Beneficiarului nu este de succes, Autoritatea de Certificare respinge cererea de revocare.

4.9.2 Cine poate solicita revocarea certificatelor

Beneficiarul și părțile sale autorizate pot solicita revocarea unui TLS. De asemenea certSIGN poate solicita, dacă este necesar, ca cererea de revocare să fie făcută fie de către un contact organizațional, de un contact de facturare sau de solicitantul înregistrării domeniului.
Pentru o parte care nu este Beneficiarul, depunerea unui "Raport de probleme privind certificatul" este primul pas în inițierea unei cereri de revocare a certificatului. Aceste persoane includ părți contractante, furnizori de aplicații software și alte părți terțe care pot face rapoarte către certSIGN despre plângeri sau presupuse compromisuri privind cheia privată, utilizarea abuzivă a TLS sau alte tipuri de fraudă, compromitere, utilizare incorectă sau comportament inadecvat legat de TLS.
Autoritatea de Înregistrare acționează cu mare atenție atunci când procesează cererile de revocare care nu au fost trimise de către Beneficiar *și acceptă numai acele solicitări în conformitate cu Capitolul 4.9.1.* [1]
Atunci când partea care solicită revocarea certificatului nu este proprietarul certificatului (Beneficiar), autoritatea de certificare efectuează următoarele:

- Verifică dacă partea respectivă are dreptul să emită o astfel de solicitare,
- Solicită o justificare a cererii respective,
- Trimite o notificare privind revocarea sau începerea procesului de revocare de la Beneficiar.

Fiecare cerere trebuie trimisă:

- Direct la Autoritatea de Certificare în format electronic cu sau fără confirmarea Autorității de Înregistrare,
- Direct sau indirect (prin intermediul Autorității de Înregistrare) către Autoritatea de Certificare dar nu în format electronic (document pe suport de hârtie, fax, telefon etc.)

Furnizorii de aplicații software și alte părți terțe pot prezenta rapoarte privind problemele de certificare informand certSIGN în legătură cu un motiv rezonabil pentru revocarea certificatului. Cererea de revocare poate viza mai multe certificate.

4.9.3 Procedura de revocare a certificatelor

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

Procedura de revocare este descrisă în secțiunea 3.4 a prezentului CPP. Cererea de revocare de certificate trebuie să identifice precis fiecare certificat, trebuie să cuprindă motivul pentru care este cerută revocarea, și trebuie să fie autentificată. Informațiile despre certificatele revocate sunt plasate în Lista de Certificate Revocate (CRL) emisă de certSIGN Web CA G2. O cerere de revocare certificat se desfășoară astfel:

[1] *Pentru certificatele cu OID 1.3.6.1.4.1.25017.3.1.4.4, Autoritatea Națională Competentă care a autorizat sau înregistrat prestatorul de servicii de plată (BNR în România) poate solicita, de asemenea, revocarea*

- certSIGN verifică cererea de revocare, incluzând transmiterea acesteia de către o entitate legitimă. Dacă verificarea este confirmată, certSIGN Web CA G2 pune informația despre certificatul revocat în lista CRL;
- certSIGN notifică Beneficiarul despre revocare sau despre decizia de anulare a cererii de revocare, împreună cu motivația acestei anulări.
- Dacă certSIGN stabilește că revocarea este adecvată, personalul certSIGN revocă certificatul și actualizează CRL.

4.9.4 Perioada de grație a cererii de revocare

certSIGN efectuează revocarea în 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

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

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

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

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

4.9.6 Verificarea cerințelor de revocare pentru Entitățile Partenere

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

4.9.7 Frecvența de 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 subordinate este emis în conformitate cu capitolul 4.9.7 și publicate fără întârziere.

4.9.9 Disponibilitatea verificării on-line a revocării/stării

Raspunsurile OCSP responses sunt semnate de catre un OCSP Responder al carui certificate este semnat de catre CA-ul care a emis certificatul al carui status de revocare se verifica.
Răspunsurile OCSP operate de certSIGN acceptă metoda HTTP GET, astfel cum este descrisă în RFC 6960, procesează extensia Nonce (1.3.6.1.5.5.7.48.1.2) în conformitate cu RFC 8954 și furnizează un răspuns autorizat în termen de cel mult 15 minute de la prima publicare a certificatului sau precertificatului.
Certificatul de semnare al OCSP contine o extensie de tipul id-pkix-ocsp-nocheck, asa cum este definit de catre RFC6960.

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

Pentru starea certificatelor de CA subordonate:

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

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

Dacă răspunsul OCSP primește o cerere de status a unui certificat care nu a fost emis, atunci respondentul nu răspunde cu o stare "bună" pentru aceste certificate.

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

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

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

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

2. „rezervat” dacă un pre-certificat [RFC6962] cu acea serie a fost emis de (a) CA emitent; sau (b) un pre-certificat de semnare [RFC6962] asociat cu CA emitent;

3. „neutilizat” dacă niciuna din contițiile de mai sus nu sunt îndeplinite.

4.9.10 Verificarea on-line a cerințelor de revocare
Nu se stipuleaza.

4.9.11 Alte forme disponibile pentru anunțarea revocării
În prezent, nu există alte forme de comunicare a revocarii.

4.9.12 Cerințe speciale în cazul compromiterii cheii
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.
Metode acceptabile pe care terții le pot utiliza pentru a demonstra compromisul cheii private:
1. Utilizează procedura descrisă în secțiunea 7.6 din RFC 8555 și semnează cererea de revocare cu cheia privată compromisă.
2. Semnează un text oferit de certSIGN folosind cheia privată compromisă.
3. Trimiterea cheii private.

4.9.13 Circumstanțe pentru suspendare
Nu este stipulat.

4.9.14 Cine poate solicita suspendarea
Nu este stipulat.

4.9.15 Procedura de solicitare a suspendării
Nu este stipulat.

4.9.16 Limitări ale perioadei de suspendare
Nu este stipulat.

4.10 Servicii privind starea certificatelor

4.10.1 Caracteristici operaționale
Serviciile certSIGN de verificare a stării certificatelor sunt CRL și OCSP. Accesul la aceste servicii se realizează prin intermediul site-urilor web “www.certsign.ro” și “ocsp.certsign.ro”. Serviciile de verificare a stării certificatelor oferă informații despre starea certificatelor valide. Integritatea și autenticitatea informațiilor despre starea lor este protejată prin semnătura electronică a CA-ului respectiv. Intrările de revocare din CRL sau răspunsurile OCSP nu sunt șterse înainte de data expirării certificatului revocat.

4.10.2 Disponibilitatea serviciului
certSIGN operează și menține capabilitățile CRL și OCSP cu resurse suficiente pentru a asigura un timp de răspuns de două secunde sau mai puțin, în condiții normale de operare.
certSIGN menține 24x7 un Depozitar online, astfel încât aplicațiile software să poată verifica automat starea curentă a tuturor certificatelor ne-expirate emise de CA.

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

4.10.3 Elemente opționale

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

4.11 Încetarea abonamentului

Sfârșitul abonamentului apare după:

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

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

4.12 Custodie și recuperare chei

certSIGN nu permite custodia cheilor pentru certificate calificate.

4.12.1 Principalele politici și practici de escrow și recuperare

Nu este stipulat.

4.12.2 Politica și practicile cheie de încapsulare și recuperare a sesiunii

Nu este stipulat.

5 Facilitate, Management și Controale Operaționale

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

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

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

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

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

Programul de securitate al certSIGN include o evaluare anuală a riscurilor care:

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

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

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

5.1 Controale fizice

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

5.1.1 Amplasarea și construcția sediului

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

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

- un perimetru clar definit și protejat, prin care sunt controlate toate intrările și ieșirile;
- Componentele critice sunt protejate cu mai multe perimetre;
- un sistem de control de intrare, care admite numai acele persoane autorizate în mod corespunzător să intre în zonă;
- Monitorizare cu echipaj uman și electronic a intruziunilor neautorizate, în orice moment;

- Personalul care nu se regăsește pe lista de acces este însoțit și supravegheat în mod corespunzător;
- A Un jurnal de acces este întreținut și controlat periodic;
- Echipamentul este întreținut în mod corect pentru a-i asigura disponibilitatea continuă și integritatea.

5.1.2 Accesul fizic

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

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

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

Zonele ocupate de certSIGN se împart în:

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

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

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

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

5.1.3 Alimetarea cu curent și aerul conditionat

Toate zonele sunt prevăzute cu aer conditionat. În zona serverelor, echipamentele de aer condiționat sunt redundante, iar temperatura este monitorizată atât automat (cu o alertă când un anumit nivel este atins) cât și manual. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a grupului electrogen al clădirii. Infrastructura de curect electric este concepută astfel încât la o întrerupere a curentului în cladire toate activitățile să fie disponibile

pentru cel puțin 24 de ore cu ajutorul generatorului diesel. Fiecare server, echipament de rețea și toate calculatoarele angajaților care desfășoară activități importante pentru activitățile CA și RA sunt conectate la UPS-uri. Principalele componente ale securitatii fizice sunt de asemenea conectate la UPS-uri și la generatorul diesel.

5.1.4 Expunerea la apă

Riscul de inundație în zona serverelor este controlat prin rack-uri. Toate echipamentele sunt plasate în rack-uri la o distanta de minim 15 cm de la sol. În plus, toate camerele serverelor sunt monitorizate cu senzori de umiditate.

5.1.5 Prevenirea și protecția împotriva incendiilor

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

5.1.6 Depozitarea mediilor de stocare a informaţiilor

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

5.1.7 Aruncarea deșeurilor

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

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 24 de ore în sediul certSIGN sau în sediul pentru recuperarea din dezastre.

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 şi procedurilor de securitate .
- **Administratorul de sistem** – Autorizat să instaleze, configureze și să întreţină sistemele de încredere ale Autorităţii de Certificare pentru înregistrarea, generarea de certificate, furnizarea dispozitivelor subiecților şi gestiunea revocărilor de certificate. Instalează dispozitivele hardware şi sistemele de operare; instalează şi configurează echipamentele de reţea.
- **System operator** – Responsabil de operarea zilnică a sistemelor de încredere ale Autorităţii de Certificare. Autorizat să execute operaţiile de backup și restaurare a sistemului. Are acces la certificatele Subiecţilor; revocă certificatele Subiecţilor; asigură continuitatea copiilor de siguranţă şi a arhivelor bazelor de date şi crearea log-urilor de sistem; manages databases; administrează bazele de date; are acces la informaţii confidenţiale despre Subiecți/Beneficiari, dar nu are dreptul de a accesa fizic nici o altă resursă a sistemului; transferă copiile de siguranţă ale arhivei și ale datelor curente catre locaţiile desemnate.
- **Ofițer 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;
- **Specialist în validare**: aplicarea unor proceduri riguroase de control pentru separarea sarcinilor de validare, astfel încât nicio persoană să nu poată valida și autoriza singură emiterea unui certificat EV/QWAC . Un specialist în validare poate examina și verifica toate informațiile solicitantului, iar un al doilea specialist în validare poate aproba emiterea unui certificat EV/QWAC.
- **Auditor de system** – autorizat să acceseze arhivele și log-urile de audit ale sistemelor de încredere ale Autorităţii de Certificare. Responsabil de efectuarea de audituri interne pentru respectarea Codului de Practici și Proceduri de către Autoritatea de Certificare; această responsabilitate se extinde şi asupra Autorităţii de Înregistrare care operează în cadrul certSIGN.

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

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 catre rolurile de incredere.

5.2.2 Numărul de persoane necesare pentru fiecare sarcină

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

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

5.2.3 Identificarea și autentificarea pentru fiecare rol

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

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

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

Fiecare cont alocat:

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

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

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

Toate acțiunile angajaților în roluri de încredere sunt trasabile și se asigură o responsabilitate deplină.

5.2.4 Rolurile care necesită separarea sarcinilor

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

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

5.3 Controlul personalului

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

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

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

5.3.1 Calificări, experință și aprobări necesare

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

5.3.2 Proceduri de verificare a antecedentelor

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

5.3.3 Cerinţele de pregătire a personalului

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

- Cerințele CPP,

- procedurile și controalele de securitate folosite de Autoritatea de Certificare și Autoritatea de Înregistrare,
- Cunoștințe de bază PKI, politici și proceduri de autentificare și verificare;
- Amenințările comune la adresa procesului de verificare a informațiilor (inclusiv phishing și alte tactici de inginerie socială) și cerințele de bază pentru Forumul CA/B,
- Responsabilitățile care decurg din rolurile și sarcinile efectuate în sistem,

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

CA garantează că personalul însărcinat cu operatiunile de validare își menține un nivel de calificare care îi permite să îndeplinească aceste sarcini în mod satisfăcător. CA documentează faptul că fiecare Specialist în Validare posedă competențele necesare unei sarcini înainte de a permite Specialiștilor de Validare să îndeplinească acea sarcină. CA solicită tuturor Specialiștilor de Validare să treaca o examinare furnizata de CA cu privire la cerințele de verificare a informațiilor prezentate în CPP și cerințele de bază ale CA / B Forum.

5.3.4 Frecvența instruirilor și cerințe

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

Tot personalul cu rol de încredere își menține un nivel al competențelor corespunzător cu progamele de instruire și performanță ale certSIGN.

5.3.5 Frecvența și secvența rotației posturilor

Nu este stipulat.

5.3.6 Sancțiunile pentru acțiunile neautorizate

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

5.3.7 Cerințele pentru contractanții independenți

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

Toate contractele includ referiri la acest CPP precum și implicit la cerințele CABF BR și/sau EV.

5.3.8 Documentația oferită personalului

certSIGN ofera personalului său accesul la următoarele documente:

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

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

5.4 Procedurile de înregistrare a datelor de audit

Pentru gestionarea eficientă a sistemelor și aplicațiilor folosite de certSIGN în activitatea sa în calitate de furnizor de servicii de certificare, dar și pentru a permite auditarea acțiunilor angajaților și clienților, toate informațiile cu privire la evenimente importante, generate de sisteme și aplicații sunt înregistrate. Aceste informații, cunoscute în mod colectiv sub numele de log-uri trebuie să fie păstrate în așa fel încât să poată fi accesate de către Entitățile Partenere, auditori și autoritățile de stat oricând au nevoie de ea, pentru a furniza dovezi ale funcționării corecte a serviciilor în scopul procedurilor legale sau pentru a detecta încercările de a compromite securitatea certSIGN. Evenimentele înregistrate sunt arhivate și păstrate într-o locație secundară.

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

5.4.1 Evenimente Înregistrate

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

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

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

CA certSIGN și fiecare parte terță delegată înregistrează evenimentele legate de securitatea sistemelor lor de certificate, a sistemelor de gestionare a certificatelor, a sistemelor CA

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

CA înregistrează cel puțin următoarele evenimente:

1. **Evenimentele legate de ciclul de viață al certificatelor și cheilor CA**, inclusiv:
   - generarea, salvarea, stocarea, recuperarea, arhivarea și distrugerea cheilor;
   - cereri de certificate, reînnoire și cereri de recheie și revocare;
   - aprobarea și respingerea cererilor de certificate;
   - evenimente de gestionare a ciclului de viață al dispozitivelor criptografice;
   - generarea listelor de revocare a certificatelor;
   - Semnarea răspunsurilor OCSP
   - Introducerea de noi profiluri de certificat și retragerea profilurilor de certificat existente.
2. **Evenimentele de gestionare a ciclului de viață al certificatului de abonat**, inclusiv:
   - Cereri de certificate, reînnoire și cereri de rechemare și revocare;
   - toate activitățile de verificare prevăzute în prezentele cerințe și în Declarația privind practicile de certificare ale CA;
   - aprobarea și respingerea cererilor de certificate;
   - emiterea de certificate;
   - generarea listelor de revocare a certificatelor;
   - semnarea răspunsurilor OCSP.
   - Rezultate ale verificarilor cu coroborarea emiterii prin perspective multiple (MPIC)
3. **Evenimente de securitate**, inclusiv:
   - încercări reușite și nereușite de acces la sistemul PKI;
   - acțiunile efectuate de sistemul PKI și de securitate;
   - modificări ale profilului de securitate;
   - instalarea, actualizarea și eliminarea de software pe un sistem de certificare;
   - pornirea și oprirea sistemului, blocări, defecțiuni hardware și alte anomalii;
   - activități relevante ale routerului și ale firewall-ului (astfel cum sunt descrise mai jos);
   - intrările și ieșirile din incaperile CA.

Fiecare înregistrare, automată sau manuală, conţine următoarele informaţii:

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

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

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

Toate informațiile de înregistrare, inclusiv următoarele sunt înregistrate:

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

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

Confidențialitatea informațiilor Subiectului este menținută.

5.4.2 Frecvența procesării jurnalelor de evenimente

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

5.4.3 Perioada de pastrare a log-urilor de audit

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

Jurnalele arhivate sunt păstrate cel puțin 10 ani.

CA-ul și fiecare terț delegat păstrează:

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

5.4.4 Protecția jurnalelor de evenimente

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

- Doar entităţile de mai sus au dreptul să citească înregistrările jurnalului,

- Platforma centrala de jurnale arhiveaza sau sterge automat fisierele (dupa arhivarea lor) care contin evenimentele inregistrate,
- Este posibilă detectarea oricărei violări de integritate; acest lucru asigură faptul că înregistrările nu conţin lacune sau falsuri,
- Nici o entitate nu are dreptul să modifice conţinutul unui jurnal.

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

5.4.5 Procedura de backup a log-urilor

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 (internal vs. external)

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

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

5.4.7 Notification 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.

Evaluarea riscurilor este actualizată cel puțin o dată pe an și:

1. Identifică amenințările interne și externe previzibile care ar putea duce la acces neautorizat, dezvăluire, utilizare incorectă, modificare sau distrugere a oricărui proces de procesare a datelor de certificat sau a procesului de administrare a certificatelor;
2. Evaluează probabilitatea și posibilele pagube ale acestor amenințări, ținând cont de sensibilitatea proceselor de certificare a datelor și a certificatelor; și
3. Evaluează suficiența politicilor, a procedurilor, a sistemelor informatice, a tehnologiei și a altor aranjamente pe care CA dispune de astfel de amenințări.

5.5 Arhivarea înregistrărilor

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

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

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

Copiile de siguranţă sunt ţinute în afara locaţiei certSIGN.

5.5.1 Tipuri de date arhivate

Următoarele date sunt incluse într-o arhivă de încredere:

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

Emiterea certificatului

Toate înregistrările de emitere a certificatelor (copiile certificatelor sunt mentinute, indiferent de statutul lor: expirat sau revocat) sunt păstrate ca înregistrări în arhive electronice și / sau pe hârtie pe perioada descrisă mai sus. certSIGN poate cere solicitanților să prezinte documentația corespunzătoare în sprijinul unei cereri de certificate. În astfel de circumstanțe, certSIGN păstrează astfel de înregistrări, după cum se menționează în acest CPP.

certSIGN înregistrează următoarele informații referitoare la emiterea certificatului ca parte a procesului de verificare a aprobării certificatului său:

- CSR-ul PKCS#10 al Beneficiarului;
- Documentația privind existența organizațională pentru solicitanții companii menționați în secțiunea 3.2.2;
- Documentația privind identitatea individuală pentru solicitanții indivizi menționati în secțiunea 3.2.3;
- Verificarea existenței și statutului organizațional primite de la o baza de date terță și entități guvernamentale (inclusiv instantanee ale site-urilor web care raportează astfel de informații);

- Validarea adresei de corespondenta (dacă este diferită de cea identificată prin resursele enumerate mai sus);
- Scrisoare de autorizare pentru site-urile web gestionate de agenți terți ai solicitanților (dacă este cazul);
- Prezentarea cererii de certificat, inclusiv acceptarea contractului;
- Numele, adresa de e-mail și adresa IP a persoanei care recunoaște autoritatea solicitantului / Beneficiarului, colectată în conformitate cu secțiunea 3.2.5;
- Instantaneu al site-ului web;
- Alte informații de contact relevante pentru solicitant / Beneficiar; și
- Copie a certificatelor digitale emise.

Revocarea certificatelor

Cererile de revocare a certificatelor sunt înregistrate și arhivate, inclusiv numele persoanei care solicită revocarea, motivul cererii și personalul certSIGN implicat în autorizarea revocării. Aceste informații și toate CRL-urile rezultate sunt păstrate ca înregistrări în arhive electronice pentru perioada descrisă în secțiunea 5.5.2 de mai sus.

Alte informatii

certSIGN arhivează, de asemenea, următoarele informații privind operațiunile CA:

- Versiuni ale acestui CPP,
- Obligatiile contractuale,
- Înregistrările privind configurarea echipamentului CA și accesul și utilizarea cheilor private ale CA,
- Datele de audit privind securitatea și conformitatea (vezi Sectiunea 5.4); și
- Orice alte date sau aplicații necesare pentru a verifica conținutul arhivei.

5.5.2 Perioada de retenție a arhivei

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

5.5.3 Protecția arhivei

certSIGN asigură:

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

Arhivele sunt accesibile exclusiv personalului autorizat.

5.5.4 Procedurile de back-up al arhivei

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

5.5.5 Cerințe privind marcarea temporală a înregistrărilor

Timpul de sistem pentru calculatoarele certSIGN este actualizat utilizând Network Time Protocol (NTP) pentru a sincroniza ceasurile sistemului cel puțin o dată la fiecare opt ore (Windows default). Următoarele articole arhivate din lista de verificare a aprobării certificatului sunt marcate cu data, cu data, ora și numele angajatului certSIGN care verifică informațiile și fac înregistrarea:

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

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

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

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

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

5.5.6 Sistemul de colectare al arhivei (intern sau extern)

Sistemele de colectare ale arhivei certSIGN sunt interne.

5.5.7 Procedura de obținere și verificare a informațiilor arhivate

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

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

5.6 Schimbarea cheilor

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

5.7 Compromiterea și recuperare în caz de dezastru

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

5.7.1 Procedurile de administrare a a incidentelor și compromiterilor

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

Procedura de administrare a incidentelor de securitate specifică de asemenea modul în care se face notificarea părților corespunzătoare în conformitate cu normele de reglementare

aplicabile oricărei breșe de securitate sau pierderii integrității care are un impact semnificativ asupra serviciului de încredere furnizat și asupra datelor cu caracter personal păstrate de acesta în termen de 24 de ore de la identificarea breșei.

În caz de incidente de Securitate, se utilizeaza procedurile interne. Aceste proceduri includ și notificarea Furnizorilor de Aplicații Software, auditorilor certSIGN, Organismului National de Supraveghere, CSIRT sau alte autorități competente.

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

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

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

certSIGN are un Plan de Răspuns la Incidente și un Plan de Recuperare din Dezastre, care includ Planul de Management în situații de Criză, și a documentat proceduri de continuitatea afacerii si de recuperare la dezastre, concepute să notifice și să protejeze în mod rezonabil Furnizorii de Aplicații Software, Beneficiarii și Entitățile Partenere în eventualitatea unui dezastru, a unei compromiteri de securitate, sau al unui eșec al afacerii. certSIGB pune la dispoziție, la cerere, către auditorii CA-ului, planul de continuitate al afacerii și planurile de securitate disponibile. CA-ul revizuiește, testează și actualizează anual aceste proceduri.

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

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

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

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

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

Pentru a preveni sau limita rezultatele amenințărilor de mai sus:

- Politica de securitate a certSIGN include un Plan de continuitate a afacerii și recuperare în caz de dezastru,
- În cazul apariţiei unui eveniment ce blochează funcţionarea certSIGN, în maxim 48 de ore, va fi activată locaţia auxiliară ce poate substitui toate funcţiile importante ale unei

Autorităţii de Certificare până la restaurarea locaţiei principale. Distanța dintre locația primară și cea secundară este suficient de mare pentru ca potențialul dezastru care afectează locația primară să nu afecteze și locatia secundară.

- Instalarea de versiuni noi ale aplicaţiilor software în producţie se poate face numai după testarea intensivă a acestora într-un mediu de test, în conformitate cu procedurile descrise. Orice modificare a sistemului necesită aprobarea administratorului de securitate al certSIGN.
- Sistemele certSIGN utilizează aplicaţii pentru crearea copiilor de rezervă a datelor pe baza cărora se poate face în orice moment restaurarea sistemului și auditarea acestuia. Copiile de siguranţă includ toate datele relevante din punct de vedere al securităţii.
- Toate sistemele din care este compusă infrastructura IT pentru furnizarea de servicii de certificare și timestamp sunt monitorizate în mod continuu și toate evenimentele de securitate sunt înregistrate și analizate. Activitățile de sistem anormale care indică o potențială încălcare a securității, inclusiv intruziune în sistemele de rețea sunt detectate și raportate ca alarme pentru a permite certSIGN să detecteze, înregistreze și reactioneze în timp util la orice 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 entitati

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

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

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

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

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

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

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 marcare temporală să își reia activitatea în timp util în cazul unui incident / dezastru.

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

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

Planurile BCP și DRP abordează de asemenea compromiterea, pierderea sau suspiciunea de compromitere a cheii private 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 şi Entităţilor Partenere ce pot apărea ca urmare a deciziei unei Autorităţi de Certificare de a-şi înceta activitatea si include obligativitatea notificarii Subiecților/ Beneficiarilor despre autoritatea care a certificat autoritatea de certificare ce

urmeaza sa isi inceteze activitatea (daca exista) și translatarea responsabilitatilor (servicii furnizate catre Subiecți/ Beneficiari, baze de date, etc) În conformitate cu reglementarile aplicabile catre alta Autoritate de Certificare.

Cerințe asociate transferului responsabilității

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

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

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

În cazul în care certSIGN își încetează activitatea, fără a transfera o parte sau toate activitățile sale, va revoca certificatele afectate după o lună de la notificarea Beneficiarilor și / sau Subiectilor și va iniția procedura de terminare a contractelor încheiate cu partenerii și/sau furnizorii implicați.

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

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

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

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

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

5.9 Lanțul de aprovizionare

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

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

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

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

6 Controale tehnice de securitate

6.1 Generarea și instalarea perechii de chei

Acest capitol descrie procedurile de generare și management a perechii de chei criptografice a unei Autorităţi de Certificare, inclusiv cerințele tehnice asociate. Controalele de securitate corespunzătoare sunt puse în aplicare pentru gestionarea oricăror chei criptografice și a oricărui dispozitiv criptografic pe parcursul ciclului lor de viață. Aceste măsuri de securitate protejează, de asemenea, datele de activare a cheilor criptografice, depozitarele, cheile private și datele de activare pentru cheile private ale 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 siguranţă de către proprietar a cheilor sale. O atenţie deosebită se acordă generării și protecţiei cheii private a certSIGN, care influenţează funcţionarea în siguranţă a întregului sistem de certificare a cheilor publice.

certSIGN Web CA G2 detine cel putin 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.

6.1.1 Generarea perechilor de chei

certSIGN are o procedură documentată pentru efectuarea generării cheilor **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 va elabora un raport al ceremoniei cheilor care va dovedi că a fost efectuată în conformitate cu procedura declarată și că integritatea și confidențialitatea perechii de chei au fost asigurate. Acest raport este semnat de toti participantii, in special 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.

CA-ul:

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

Cheile **certSIGN Web CA G2** 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 și cu distribuirea cunoștințelor:

- Cel puțin trei angajați cu roluri de încredere,
- Ofițerul de securitate,
- un Auditor independent

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

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 de perechi de chei CA este realizată utilizând algoritmul RSA cu lungimea cheii de 4096 biți.

Înainte de expirarea certificatului său de CA, care este utilizat pentru semnarea cheilor Subiecților, CA va genera un nou certificat pentru semnarea perechilor de chei ale Subiecților și va aplică toate măsurile necesare pentru a evita perturbarea operațiunilor oricărei entități care se bazează pe certificatul CA. Noul certificat CA va fi, de asemenea, generat și distribuit în conformitate cu prezentul CPP. Aceste operații trebuie efectuate la un interval de timp adecvat între data expirării certificatului și ultimul certificat semnat pentru a permite tuturor

părților care au relații cu certSIGN (subiecți, Beneficiari, entități partenere, CA-uri mai mari în ierarhia CA etc.) să fie conștienți de această modificare de cheie și să pună în aplicare operațiunile necesare pentru a evita crearea unor inconveniențe și defecțiuni. Acest lucru nu se aplică în cazul în care am înceta operațiunile noastre înainte de data de expirare a propriului nostru certificat de semnare.

Cheile subiecților sunt generate de subiect, prin intermediul aplicațiilor software sau al dispozitivelor criptografice.

CA respinge o cerere de certificat TLS dacă sunt îndeplinite una sau mai multe dintre următoarele condiții:
• perechea de chei nu îndeplinește cerințele stabilite în secțiunea 6.1.5 și / sau în secțiunea 6.1.6
• Există dovezi clare că metoda specifică utilizată pentru a genera cheia privată a fost compromisă;
• CA are la cunoștință despre o metodă demonstrată sau dovedită care expune cheia privată a solicitantului la compromisuri;
• CA a fost informată anterior că cheia privată a solicitantului a suferit un compromis, cum ar fi cele menționate în secțiunea 4.9.1;
• CA are la cunoștință despre o metodă demonstrată sau dovedită pentru a calcula cu ușurință cheia privată a solicitantului pe baza cheii publice (cum ar fi o cheie slabă Debian, consultați https://wiki.debian.org/TLSkeys).
În cazul în care certificatul TLS abonat conține o extensie extKeyUsage care conține valorile id-kp-serverAuth sau anyExtendedKeyUsage, CA-ul NU va genera o pereche de chei în numele abonatului și NU va accepta o cerere de certificat TLS utilizând o pereche de chei generată anterior de CA.

6.1.2 Distribuirea Cheii Private către Beneficiar

Nu efectuăm livrare de chei private către Beneficiar deoarece cheia privată este generată doar Beneficiarului .

6.1.3 Distribuirea Cheii Publice către emitentul certificatului

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

6.1.4 Distribuirea Cheii Publice a Autorității Certificare către Entitățile Partenere

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

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

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

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

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

6.1.5 Marimea cheilor

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

Certificatele digitale emise de certSIGN Web CA G2 utilizează chei RSA de 2048, 3072 sau 4096 biți.

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

Acești algoritmi și aceste dimensiuni de chei sunt permise acum, dar certSIGN își rezervă dreptul de a introduce în viitor alți algoritmi și protocoale decât RSA cu SHA-2 sau lungimi de chei mai lungi. Aceasta poate include algoritmi de 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 pentru certSIGN Web CA G2 Procedurile de verificare includ pași de verificare a faptului că valoarea exponentului public este un număr impar egal cu 3 sau mai mult. Modulul trebuie să aibă următoarele caracteristici: un număr impar, nu puterea unui nr. prim și să nu aibă factori mai mici de 752.

În plus, exponentul public este în intervalul recomandat, între $2^{16}+1$ și $2^{256}-1$.

6.1.7 Scopurile în care pot fi utilizate cheile (cf 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 aplicaţia Beneficiaruluicare face managementul certificatelor.

Folosirea biţilor din câmpul KeyUsage trebuie să respecte următoarele reguli:

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

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

Cheia privata a certSIGN Web CA G2 este utilizata numai în urmatoarele cazuri:

1. Certificate pentru end-useri;
2. Certificate pentru scopuri de infrastructură (Certificatele de verificare a răspunsului OCSP);

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 Beneficiarului, trebuie să o livreze în siguranță Beneficiarului și să impună Beneficiarului să își protejeze cheia privată.

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

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

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

Sunt luate măsuri pentru ca dispozitivele criptografice sigure să nu fie alterate în timpul transportului și în timp ce acestea sunt depozitate la sediul certSIGN.

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

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

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

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

6.2.1 Controalele și standardele modulelor criptografice

Generarea de perechi de chei CA se desfășoară într-un dispozitiv criptografic securizat, care este un sistem de încredere care respectă cel puțin standardele FIPS 140-2 nivel 3 sau Common Criteria EAL 4.

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

Controulul multi-persoană al unei chei private se aplică cheilor private folosite la semnarea certificatelor și a CRL-urilor.

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

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

Acceptarea secretului partajat de către deținătorii săi

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

Protejarea secretului partajat

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

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

Disponibilitatea și ștergerea (transferul) secretului partajat

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

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

Responsibilitățile deținătorului secretului partajat

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

Controlul multiplu nu se aplică cheii private a Beneficiarului .

6.2.3 Custodia Cheii Private

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

Cheile private ale Beneficiarului nu sunt supuse custodiei.

6.2.4 Copia de siguranță a cheii private

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

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

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

6.2.5 Arhivarea Cheii Private

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

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

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

- În cazul creării copiilor de siguranță pentru cheile private 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 utilziat pentru operațiuni standard către un alt modul; situația poate apărea în cazul defectării modulului sau atunci când este necesară distrugerea sa.

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

Introducerea unei chei private într-un modul hardware de securitate al Autorităţii de Certificare **certSIGN Web CA G2** necesită restaurarea cheii de pe carduri în prezenţa unui număr corespunzător de deţinători ai secretului partajat care protejează modulul ce conţine cheile private. Deoarece fiecare Autoritate de Certificare poate deţine o copie criptată a cheii sale private, cheile pot fi de asemenea transferate între module.

Dacă cheia privată a CA a fost comunicată unei persoane neautorizate sau unei organizații care nu este afiliată la CA, certSIGN ROOT CA G2 revocă toate certificatele care includ cheia publică corespunzătoare cheii private comunicate.

6.2.7 Stocarea cheilor private pe modul criptografic

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

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

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

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

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

Operatorii utilizează dispozitive de generare a semnăturii electronice calificate (token-uri/carduri) care respectă cel puțin standardul FIPS 140-2 nivel 3 sau Common Criteria EAL 4. Cheile sunt întotdeauna generate pe dispozitive și nu le părăsesc niciodată. Dispozitivele securizate sunt protejate în timpul transportului de la furnizor la certSIGN, în timpul depozitării și la distribuție.

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

6.2.8 Metoda de activare a cheii private

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

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

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

6.2.10 Metoda de distrugere a cheii private

La sfârșitul durateilor de viață, cheile private ale CA sunt distruse de roluri de încredere din cadrul CA, în prezența a mai mult de un reprezentant al Comitetului de Management al Politicilor și Procedurilor, pentru a se asigura că aceste chei private nu mai pot fi recuperate sau utilizate niciodată.

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

Aceste module hardware sunt tratate într-un mod securizat așa cum s-a descris în cadrul procedurilor interne documentate de distrugere a cheilor. Înregistrările asociate sunt arhivate în siguranță. CMPP autorizează în scris distrugerea cheii private a CA și personalul alocat pentru aceasta activitate.

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

Beneficiarul este responsabil pentru distrugerea cheii private.

6.2.11 Evaluarea Modulului Criptografic

Vezi mai sus.

6.3 Alte aspect legate de managementul perechilor de chei

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

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

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

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

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

6.3.1 Arhivarea cheilor publice

certSIGN își arhivează propriile chei publice de CA și toate cheile publice certificate de certSIGN Web CA G2 sub forma de certificate X509 ce contin cheia.

Vezi capitolul 5.5 pentru conditiile de arhivare.

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

Perioada de folosire a cheilor publice este definită de valoarea câmpului validitate a fiecărui certificat de cheie publică. Aceasta este de asemenea, perioada de valabilitate aplicată cheii private. Perioada maximă de utilizare a cheilor Beneficiarului nu poate depăși perioada de valabilitate a unui certificat, mentionata mai jos.

Perioadele standard maxime de utilizare pentru certificate de CA sunt descrise in Tabelul 6.3.2.1, iar pentru certificate finale in Tabelul 6.3.2.2.

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

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

Detinatorul cheii	Scopul principal al utilizarii cheii
	RSA pentru certificate și semnare CRL

certSIGN Web CA G2	7 ani

Table 6.3.2.1 Perioada maxima de utilizare

Detinatorul cheii	Politica de Certificare	Scopul principal al utilizarii cheii
Entitati juridice	certSIGN Web	397 zile[2]

Table 6.3.2.2. Perioadele maxime de utilzare ale certificatelor Subiectilor

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

6.4 Datele de activare

6.4.1 Generarea și instalarea datelor de activare

Datele de activare sunt folosite în două situații principale:

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

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

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

Atunci când beneficiarii generează cheile private utilizând QSCD, este responsabilitatea lor să genereze și datele de activare (de exemplu codul PIN).

6.4.2 Protejarea datelor de activare

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

[2] După 15 martie 2026, durata va fi mai mică de 200 de zile; după 15 martie 2027 - mai mică de 100 de zile

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

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

6.4.3 Alte aspect ale datelor de activare

Nu este stipulat.

6.5 Controale de Securitate ale computerelor

Acest capitol descrie controalele de securotate ale computerele certSIGN.

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

6.5.1 Cerințe tehnice specifice ale securității calculatoarelor

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

Computerele sunt configurate cu următoarele mecanisme de securitate:

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

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

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

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

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

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

6.5.2 Computer security rating

Sistemul informatic certSIGN respectă cerințele descrise în standardele ETSI EN 319 411-1.

6.6 Controale tehnice specifice ciclului de viață

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

6.6.1 Controale specifice dezvoltării sistemului

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

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

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

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

6.6.2 Controale specifice managementului securității

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

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

6.6.3 Controale de securitate specifice ciclului de viață

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

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

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

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

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

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

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

6.7 Controale de securitate a rețelei

certSIGN 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 reviziuite periodic.
c) Toate sistemele critice pentru funcționarea serviciilor de certificare sunt păstrate într-una sau mai multe zone securizate)
d) Rețeaua dedicată administrării sistemelor IT și rețeaua operațională sunt separate. Sistemele utilizate pentru administrarea implementării politicii de securitate nu sunt utilizate în alte scopuri. Sistemele de producție ale serviciilor de certificare sunt separate de sistemele utilizate în dezvoltare și testare (de exemplu, sistemele de dezvoltare, testare și planificare).
e) Comunicarea între sisteme de încredere distincte se realizează doar prin intermediul unor canaluri de încredere care sunt distincte logic de alte canale de comunicații și oferă identificarea sigură a punctelor terminale și protecția datelor canalului de modificare sau divulgare.
f) Dacă este necesar un nivel înalt de disponibilitate a accesului extern la un anumit serviciu de certificare, conexiunea externă la rețea este redundantă, pentru a asigura disponibilitaea serviciilor, în cazul unui singur eșec.
g) Se realizează o scanare periodica a vulnerabilității adreselor IP publice și private identificate de certSIGN și se înregistrează dovezi că fiecare scanare a vulnerabilității a fost realizată de către o persoană sau o entitate cu abilitățile, instrumentele,

competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.

h) Serviciile de certificare ale certSIGN sunt supuse unui test de penentrare pe sistemele aferente la inițiere și după upgrade-uri de infastructură sau de aplicații sau după modificări pe care certSIGN le consideră importante. Se înregistrează dovezi că fiecare test de penetrare a fost realizat de către o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.

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

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

Mijloacele de protecție a securității rețelei acceptă doar mesajele transmise utilizând protocoalele http, https, NTP, POP3 și SMTP. Evenimentele (log-uri) sunt înregistrate în jurnalele de system și permit supervizarea corectitudinii utilizării serviciilor furnizate de certSIGN.

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

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

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

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

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

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

6.8 Marcare temporala

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).

6.9 Elementele de control specifice modulelor criptografice

Elementele de control ale modulelor criptografice includ cerințele impuse pentru dezvoltarea, producerea și livrarea modulelor. certSIGN nu definește cerințe de proprietate în acest domeniu. Cu toate acestea, certSIGN acceptă și utilizează numai module criptografice care respectă cerințele din capitolul 6.2.

7 Profilul certificatelor, CRL și OCSP

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

7.1 Profilul certificatului

certSIGN Web CA G2 îndeplinește cerințele tehnice stabilite în CABF BR secțiunea 2.2 - Publicarea informațiilor, secțiunea 6.1.5 - Dimensiunile cheilor și secțiunea 6.1.6 - Generarea parametrilor cheii publice și verificarea calității.
Câmpul SerialNumber este un număr nesecvențial mai mare decât zero (0) și mai mic de 2^{159}, care conține cel puțin 64 de biți de la un CSPRNG.
Toate obiectele semnate de o cheie privată certSIGN CA sunt conforme cu cerințele CABF BR #7.1.3.2, RSA sau ECDSA privind utilizarea AlgorithmIdentifier sau a tipului AlgorithmIdentifier-derivat în contextul semnăturilor.

Profilul certificatului CA subordonat

Toate denumirile subiecților sunt codificate conform specificațiilor din secțiunea 7.1.4 și conțin AttributeTypes conform #7.1.2.10.2 "CA Certificate Naming" din CABF BR.
Profilul câmpurilor de bază pentru certificatele certSIGN Web CA G2 este descris în Tabelul 7.1.

Numele campului	Valoarea sau restricțiile valorii	
Version	3	
Serial Number	Unique value greater than zero (0)	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Department (OU) =	certSIGN ROOT CA G2
	Organization (O) =	CERTSIGN S.A.
	Country (C) =	RO
Not before	Universal Time Coordinated based	
Not after	Universal Time Coordinated based	
Subject (Distinguished Name)	CommonName (CN) =	certSIGN Web CA G2
	Organization (O) =	CERTSIGN SA[3]
	OrganizationIdentifier	VATRO-18288250
	Country (C) =	RO
Subject 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 Web CA G2

[3] *CERTSIGN S.A. este aceeasi organizatie ca si CERTSIGN SA. Ambele denumiri sunt interschimbabile intre ele.*

Profilul certificatului de end-user (server)

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

Toate denumirile subiecților sunt codificate în conformitate cu CABF BR secțiunea 7.1.4 și conțin AttributeTypes conform #7.1.2.7.

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

Profilul câmpurilor de bază pentru certificatele end-user TLS emise de certSIGN Web CA G2 este descris în Tabelul 7.2.

Numele campului	Valoarea sau restricțiile valorii	
Version	Version 3	
Serial Number	Valoare unică mai mare decât zero (0) pentru toate certificatele emise de autoritățile de certificare din cadrul certSIGN. Seriile sunt construite folosind un prefix incremental unic constrâns in baza de date care este concatenat cu o secvență aleatorie de 8 octeți Un modul criptografic hardware este utilizat pentru generarea valorii aleatorii.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	CommonName (CN) =	certSIGN Web CA G2
	Organization (O) =	CERTSIGN SA
	OrganizationIdentifier	VATRO-18288250
	Country (C) =	RO
Not before (validity period beginning date)	Universal Time Coordinated based.	
Not after (validity period end date)	Universal Time Coordinated based.	
Subject (Distinguished Name)	Codificate în conformitate cu RFC 5280, pot conține câmpurile prezentate în capitolul 7.1.4 și este în conformitate cu Guidelines for the Issuance and Management of Extended Validation, #7.1.4.2.	
Subject 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).	
Signature	Semnătura certificatului, generată și codificată în conformitate cu cerințele descrise în RFC 5280.	

Table 7.2. Profilul câmpurilor de bază ale certificatelor TLS emise de certSIGN Web CA G2

Profilul de precertificat

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

Câmpurile de bază ale precertificatului:
- **version** codificată este identică, octet cu octet, cu câmpul "versiune" din certificat.
- **serialNumber** codificată este identică, octet cu octet, cu câmpul serialNumber din certificat (ca o excepție de la RFC 5280, secțiunea 4.1.2.2).
- **signature** codificată este identică, octet cu octet, cu câmpul de semnătură din certificat.
- **issuer** codificată este identică, octet cu octet, cu câmpul issuer din certificat.
- **validity** codificată este identică, octet cu octet, cu câmpul validity al certificatului.
- **subject** codificată codificată este identică, octet cu octet, cu câmpul "subject" al certificatului.
- **subjectPublicKeyInfo** codificată codificată este identică, octet cu octet, cu câmpul subjectPublicKeyInfo din certificat.
- **issuerUniqueID** Encoded value este identic octet cu octet cu câmpul issuerUniqueID din certificat sau este omis dacă este omis în certificat.
- **subjectUniqueID** codificată este identică octet cu octet la octet cu câmpul subjectUniqueID din certificat sau este omisă dacă este omisă în certificat.
- **signatureAlgorithm** Valoarea codificată TREBUIE să fie identică byte cu byte cu tbsCertificate.signature.

Field name	Value or value's constraint for Precertificates	
Version	Version 3	
Serial Number	Unique value greater than zero (0. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	CommonName (CN) =	certSIGN Web CA G2
	Organization (O) =	CERTSIGN SA
	OrganizationIdentifier	VATRO-18288250
	Country (C) =	RO
Not before	Universal Time Coordinated based.	
Not after	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, contains countryName and commonName fields.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

Table 7.2.1 Profilul de bază al precertificatelor TLS emise de certSIGN Web CA G2

Profilul de certificat OCSP Responder

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

Field name	Value or value's constraint for OCSP Responder	
Version	Version 3	
Serial Number	Unique value greater than zero (0) for all certificate issued by Certification Authorities within CERTSIGN. It contains a random value of 8 bytes. A hardware cryptographic module is used for generating this value.	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (Distinguished Name)	Common Name (CN) =	certSIGN Web CA G2
	OrganizationIdentifier =	VATRO-18288250
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
Not before	Universal Time Coordinated based.	
Not after	Universal Time Coordinated based.	
Subject (Distinguished Name)	Encoded in accordance with RFC 5280, contains countryName and commonName fields.	
Subject Public Key Info	Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	

Table 7.2.1 Profilul de bază al certificatelor OCSP emise de certSIGN Web CA G2

7.1.1 Numerele de versiune

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

7.1.2 Extensii de certificate

Extensiile profilelor de certificat sunt în conformitate cu CABF BR nr. 7.1.2 "Certificate Content and Extensions" și cu #7.1.2 din Guidelines for the Issuance and Management of Extended Validation Certificates.

Extensii ale profilului de certificat de CA subordonat

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

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

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

Extensia **Certificate Policies** conține cel puțin o "PolicyInformation", care conține exact un identificator rezervat al politicii de certificat.

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

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

CA Certificate **Extended Key Usage** conține id-kp-serverAuth key.
Extensiile certificatelor pentru certSIGN Web CA G2 sunt descrise în Tabelul 7.3.1

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://pkipro.certsign.ro/certsign-rootg2.crt	Ne-Critic
Basic Constraints	Subject type=CA, Path length constraint=0	Critic
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critic
Authority Key Identifier	82212d66c6d7a0e015ebce4c0977c4609e546e03	Ne-Critic
Subject Key Identifier	Unique identifier	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
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)	Non-critical
CRL Distribution Points	http://pkipro.certsign.ro/certsign-rootg2.crl	Ne-Critic

Table 7.3.1 Extensii ale certSIGN Web CA G2

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

AuthorityInfoAccess conține una sau mai multe AccessDescriptions. Fiecare AccessDescription conține doar o AccessMethod permisă, iar fiecare Access location este codificată ca fiind de tipul GeneralName specificat.
Extinderea **Authority Key Identifier** conține doar câmpul keyIdentifier, identic cu câmpul subjectKeyIdentifier al CA emitente.
Extensia **Certificate Policies** conține cel puțin un "PolicyInformation" și conține exact un singur identificator de politică de certificat rezervat:
Pentru certificate DV:

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

Pentru certificate OV:

- *{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)} (**2.23.140.1.2.2**)*

Pentru certificate EV/QWAC:

- *{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines(1)}(**2.23.140.1.1**)*

Valori permise ale **policyQualifiers**, id-qt-cps (OID: 1.3.6.1.5.5.7.2.1), URL HTTP sau HTTPS pentru declarația privind practicile de certificare a autorității de certificare emitente.
End-user TLS Certificate **Extended Key Usage** conține cheia id-kp-serverAuth.
Subject Alternative Name este prezent și conține cel puțin un dNSName. dNSName conține fie un nume de domeniu complet calificat, fie un nume de domeniu cu caractere wildcard pe care CA l-a validat în conformitate cu secțiunea 3.2.2.4 din CABF BR. Numele de domeniu wildcard sunt validate, pentru DV si OV, în conformitate cu secțiunea 3.2.2.2.6 din CABF BR. Intrarea dNSName nu conține un nume intern. Numele de domeniu complet calificat sau porțiunea FQDN a numelui de domeniu wildcard conținută în intrare este compusă în întregime din etichete P sau etichete LDH nerezervate, unite între ele printr-un caracter U+002E FULL STOP (".). Eticheta de domeniu de lungime zero care reprezintă zona rădăcină a sistemului de nume de domeniu Internet NU este inclusă.

Valori de utilizare a cheilor (***Key Usage)***: digitalSignature, și opțional, doar pentru chei publice RSA: keyEncipherment.

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

DV profile
Certificatul end-user TLS cu Validare de Domeniu conține extensiile descrise în Tabelul 7.4a.

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.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/certsign-webcag2.crt	Non-critical
Key Usage	digitalSignature (bit 0), Key Encipherment (bit 2)[4]	Critical
Authority Key Identifier	Unique identifier	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=2.23.140.1.2.1	Non-critical

[4] *Permitted only if the certificate's subjectPublicKeyInfo identifies an RSA public key. Forbidden for ECC public key.*

Extension	Value or Value constraint	Extension status
	[1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.6 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.5.5 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	
CRL Distribution Points	http://pkipro.certsign.ro/certsign-webcag2.crl	Non-critical
Subject Alternative Name	This extension MUST contain one or more host Domain Name(s) owned or controlled by the Subscriber and to be associated with the Subscriber's server. Such server MAY be owned and operated by the Subscriber or another entity (e.g., a hosting service).	Non-critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)	Non-critical

Tabel 7.4a. Extensii certificat TLS DV

OV profile

Certificatul end-user TLS cu Validare de Organizatie conține extensiile descrise în Tabelul 7.4b.

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.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/certsign-webcag2.crt	Non-critical
Key Usage	digitalSignature (bit 0), Key Encipherment (bit 2)[5]	Critical
Authority Key Identifier	Unique identifier	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical

[5] *Permitted only if the certificate's subjectPublicKeyInfo identifies an RSA public key. Forbidden for ECC public key.*

Extension	Value or Value constraint	Extension status
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=2.23.140.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.7 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.5.2 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://pkipro.certsign.ro/certsign-webcag2.crl	Non-critical
Subject Alternative Name	This extension MUST contain one or more host Domain Name(s) owned or controlled by the Subscriber and to be associated with the Subscriber's server. Such server MAY be owned and operated by the Subscriber or another entity (e.g., a hosting service).	Non-critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)	Non-critical

Tabel 7.4b. Extensii certificat TLS OV

EV profile

Certificatul end-user TLS cu validare extinsa conține extensiile descrise în Tabelul 7.4c.

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.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/certsign-webcag2.crt	Non-critical
Key Usage	digitalSignature (bit 0), Key Encipherment (bit 2)[6]	Critical
Authority Key Identifier	Unique identifier	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey	Non-critical

[6] *Permitted only if the certificate's subjectPublicKeyInfo identifies an RSA public key. Forbidden for ECC public key.*

	(excluding the tag, length, and number of unused bits).	
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=2.23.140.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.4 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [3]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.5.6 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://pkipro.certsign.ro/certsign-webcag2.crl	Non-critical
Subject Alternative Name	This extension MUST contain one or more host Domain Name(s) owned or controlled by the Subscriber and to be associated with the Subscriber's server. Such server MAY be owned and operated by the Subscriber or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV.	Non-critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)	Non-critical
cabfOrganization Identifier	cabfOrganizationIdentifier: 2.23.140.3.1 {joint-iso-itu-t(2)international-organizations(23) ca-browser-forum(140) certificate-extensions(3) cabf-organization-identifier(1) }	Non-critical

Tabel 7.4c. Extensii certificat TLS EV

QWAC profile

Certificatul end-user TLS calificat QWAC conține extensiile descrise în Tabelul 7.4d.

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.certsign.ro [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/certsign-webcag2.crt	Non-critical

Key Usage	digitalSignature (bit 0), Key Encipherment (bit 2)[7]	Critical
Authority Key Identifier	Unique identifier	Non-critical
Subject Key Identifier	The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Non-critical
Certificate Policies	Certificate Policies [1]Certificate Policy: Policy Identifier=2.23.140.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [2]Certificate Policy: Policy Identifier=0.4.0.2042.1.4 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [3]Certificate Policy: Policy Identifier=0.4.0.194112.1.4 [3,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository [4]Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.3.1.5.1 or 1.3.6.1.4.1.25017.3.1.5.4 [4,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Non-critical
CRL Distribution Points	http://pkipro.certsign.ro/certsign-webcag2.crl	Non-critical
Subject Alternative Name	This extension MUST contain one or more host Domain Name(s) owned or controlled by the Subscriber and to be associated with the Subscriber's server. Such server MAY be owned and operated by the Subscriber or another entity (e.g., a hosting service). Wildcard certificates are not allowed for QWAC.	Non-critical
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)	Non-critical
Qualified Certificate Statements	esi4-qcStatement-1: 0.4.0.1862.1.1 esi4-qcStatement-6: 0.4.0.1862.1.6 id-etsi-qcs-QcType 3: 0.4.0.1862.1.6.3 esi4-qcStatement-5: 0.4.0.1862.1.5 URL=https://www.certsign.ro/repository Language=en id-etsi-psd2-qcStatement: 0.4.0.19495.2* id-psd2-role-psp-as: 0.4.0.19495.1.1*	Non-critical

[7] *Permitted only if the certificate's subjectPublicKeyInfo identifies an RSA public key. Forbidden for ECC public key.*

	id-psd2-role-psp-pi: 0.4.0.19495.1.2* id-psd2-role-psp-ai: 0.4.0.19495.1.3* id-psd2-role-psp-ic: 0.4.0.19495.1.4* *These extensions may be present only in certificates issued with OID 1.3.6.1.4.1.25017.3.1.5.4	
cabfOrganization Identifier	cabfOrganizationIdentifier: 2.23.140.3.1 {joint-iso-itu-t(2)international-organizations(23) ca-browser-forum(140) certificate-extensions(3) cabf-organization-identifier(1) }	Non-critical

Tabel 7.4d. Extensii certificat TLS QWAC

Extensiile profilului de precertificat

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

Extensii ale profilului de certificat OCSP Responder

Extensia **Authority Key Identifier** are doar câmpul **keyIdentifier**, identic cu câmpul **subjectKeyIdentifier** al autorității de certificare emitente.
OCSP Responder Extended Key Usage este doar OCSP Signing (1.3.6.1.5.5.7.3.9).
certSIGN include extensia id-pkix-ocsp-nocheck (OID **OCSP Signing**: 1.3.6.1.5.5.7.7.48.1.5).
Această extensie are un extnValue OCTET STRING care este exact octetul 0500 codificat hexagonal, reprezentarea codificată a valorii NULL ASN.1, astfel cum este specificat în RFC 6960, secțiunea 4.2.2.2.2.2.1.
OCSP Responder Key Usage este doar digitalSignature.
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	Unique identifier	Ne-Critic
Subject Key Identifier	Unique identifier	Ne-Critic
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	Ne-Critic
OCSPNoCheck	-	Ne-Critic

Table 7.5. Extensiile certificatelor pentru certificatele OCSP

7.1.3 Obiecte de identificare a algoritmului

SubjectPublicKeyInfo

Câmpul SubjectPublicKeyInfo indică o cheie RSA folosind identificatorul de algoritm rsaEncryption (OID: 1.2.840.113549.1.1.1.1), cu un parametru NULL explicit.
AlgorithmIdentifier pentru cheile RSA este identic, octet cu octet, cu următorii octeți codificați hexagonal: 300d06092a864886f70d0101010500.
Pentru ECDSA, se vor utiliza identificatorii și codificările specificate în #7.1.3.1.1.2 din CABF BR.

Identificatorul algoritmului de semnătură

Toate obiectele TLS semnate de o cheie privată certSIGN CA sunt conforme cu cerințele din CABF BR #7.1.3.2, RSA sau ECDSA privind utilizarea AlgorithmIdentifier sau a tipului

AlgorithmIdentifier-derivat în contextul semnăturilor. În cazul certSIGN, algoritmul utilizat este sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.1.11).

7.1.4 Formulare de nume

Codificarea numelui

Continutul campurilor din certificatele TLS îndeplinesc cerințele din sectiunea 3.1, ultima versiune publicată a CAB Forum BR, și pentru EV/QWAC, ultima versiune publicată a ghidului CAB Forum EV.
Numele Emitentului, pentru toate căile de certificare posibile, trebuie să fie identic octet-cu-octet cu Numele Subiectului din certificatul emitentului. Atributele Subiectului nu pot conține doar metadate precum ‘.’ , ‘ - ’ , și ’ ’ (adică spațiu) pentru a indica faptul că valoarea nu există, este incompletă, sau nu este aplicabilă.

Pentru fiecare cale de certificare validă (conform definiției din RFC 5280, secțiunea 6):
- Pentru fiecare certificat din calea de certificare, conținutul codificat al câmpului Issuer Distinguished Name al unui certificat este identic, octet cu octet, cu forma codificată a câmpului Subject Distinguished Name al certificatului CA emitent.
- Pentru fiecare certificat TLS CA din calea de certificare, conținutul codificat al câmpului Subject Distinguished Name al unui certificat este identic octet cu octet între toate certificatele ale căror Subject Distinguished Names pot fi comparate ca fiind egale în conformitate cu RFC 5280, secțiunea 7.1, inclusiv certificatele expirate și revocate.

Codificarea TLS Subject

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

Atributul "Subscriber TLS Certificate Common Name"

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

7.1.5 Constrangeri privind numele

Nu este stipulat.

7.1.6 Obiecte de identificare a politicii certificatelor

Obiectele de identificare a politicii certificatelor utilizate la nivel de certSIGN Web CA G2 sunt descrise în Tabelul 7.6 și Tabelul 7.7.

Numele si OID-ul politicii de certificare	Identificatorii politicilor incluse
certSIGN Web CA G2 DV 1.3.6.1.4.1.25017.3.1.5.5	***Certificate cu Validare de Domeniu pentru autentificare web*** *{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)}* (***2.23.140.1.2.1***) *itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6)****(0.4.0.2042.1.6)*** {certSIGN}.{id-CA-policy}(3.1.5).{id-Web-CA DV}(5) =***1.3.6.1.4.1.25017.3.1.5.5***
certSIGN Web CA G2 OV 1.3.6.1.4.1.25017.3.1.5.2	***Certificate cu Validare Organizatie pentru autentificare web*** *{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-validated(2)}* (***2.23.140.1.2.2***) *itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)****(0.4.0.2042.1.7)*** {certSIGN}.{id-CA-policy}(3.1.5).{id-Web-CA OV}(2) =***1.3.6.1.4.1.25017.3.1.5.2***
certSIGN Web CA G2 EV 1.3.6.1.4.1.25017.3.1.5.6	***Certificate cu Validare Extinsă pentru autentificare web*** *{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1) }* ***(2.23.140.1.1)*** *itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcp (4)****(0.4.0.2042.1.4)*** {certSIGN} .{id-CA-policy}(3.1.5).{id-Web-CA EV}(6) =***1.3.6.1.4.1.25017.3.1.5.6***
certSIGN Web CA G2 QWAC 1.3.6.1.4.1.25017.3.1.5.1	***Certificate calificate pentru autentificare web*** *{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1) }* ***(2.23.140.1.1)*** *itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcp (4)****(0.4.0.2042.1.4)***

Numele si OID-ul politicii de certificare	Identificatorii politicilor incluse
	{certSIGN} .{id-CA-policy}(3.1.5).{id-Web-CA QWAC}(1) =***1.3.6.1.4.1.25017.3.1.5.1*** *{itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web/QEVCP-w (4)}* ***(0.4.0.194112.1.4)***
certSIGN Web CA G2 QWAC PSD2 1.3.6.1.4.1.25017.3.1.5.4	***Certificate calificate pentru autentificare web cu PSD2*** *{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) ev-guidelines (1) }* ***(2.23.140.1.1)*** *itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcp (4)****(0.4.0.2042.1.4)*** {certSIGN} .{id-CA-policy}(3.1.5).{id-Web-CA QWAC PSD2}(4) =***1.3.6.1.4.1.25017.3.1.5.4*** *{itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web/QEVCP-w (4)}* ***(0.4.0.194112.1.4)***

Table 7.6. Identificatorii politicii și numele lor

7.1.7 Utilizarea extensiei Constrângeri de politică

Nu se aplică.

7.1.8 Sintaxa și semantica atributelor de politică

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

7.1.9 Semantica de procesare pentru extensia Politici critice de certificare

Nu este stipulat.

7.2 Profilul CRL

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

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

Câmpul **revokedCertificates** este prezent dacă CA a emis un certificat care a fost revocat și dacă intrarea corespunzătoare nu a apărut încă în cel puțin o CRL programată în mod regulat după perioada de valabilitate a certificatului revocat. CA va elimina o intrare pentru un certificat corespunzător după ce acesta a apărut în cel puțin o CRL programată periodic după perioada de valabilitate a certificatului revocat.Profilul CRL este descris în Tabelul 7.8.

Nume camp	Valoarea sau restricțiile valorii	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	Departament (OU) =	certSIGN ROOT CA G2
	Organization (O) =	CERTSIGN SA
	Country (C) =	RO
ThisUpdate	Date of CRL issuance	
NextUpdate	Date of next expected CRL update	
Revoked Certificates	List of revoked certificates	

Tabel 7.8 Profilul CRL pentru certSIGN Web CA G2

7.2.1 Numerele de versiune

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

7.2.2 CRL și extensiile de intrare CRL

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

Extensiile CRL pentru certSIGN Web CA G2 sunt descrise în Tabelul 7.9.

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Authority Key Identifier	Unique identifier	Ne-critic
CRL Number	Numar secvential care crește în mod monoton	Ne-critic
ExpiredCertsOnCRL	Generalized Time	Ne-critic

Table 7.9. Extensii CRL ale certSIGN Web CA G2

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

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

Table 7.10. Componente revokedCertificates pentru certSIGN Web CA G2

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

1. Nici un motiv furnizat sau nespecificat (RFC 5280 CRLReason # 0)

- În cazul în care codurile de motiv nu se aplică cererii de revocare, solicitantul NU TREBUIE să furnizeze un alt cod de motiv decât "nespecificat".

2. KeyCompromise (RFC 5280 CRLReason # 1)
   - Beneficiarul certificatului TREBUIE să aleagă motivul revocării "keyCompromise" atunci când are motive să creadă că cheia privată a certificatului său a fost compromisă, de exemplu, o persoană neautorizată a avut acces la cheia privată a certificatului său.
3. AffiliationChanged (RFC 5280 CRLReason # 3)
   - Beneficiarul certificatului ar trebui să aleagă motivul revocării "affiliationChanged" atunci când numele subiectului sau alte informații privind identitatea subiectului din certificat s-au schimbat, dar nu există niciun motiv pentru a suspecta că cheia privată a certificatului a fost compromisă.
4. Superseded (RFC 5280 CRLReason # 4)
   - Beneficiarul certificatului ar trebui să aleagă motivul revocării "superseded" atunci când certificatul este înlocuit deoarece: abonatul a solicitat un nou certificat, CA are dovezi rezonabile că nu ar trebui să se bazeze pe validarea autorizării sau controlului domeniului pentru orice nume de domeniu complet calificat sau adresă IP din certificat, sau CA a revocat certificatul din motive de conformitate, cum ar fi faptul că certificatul nu este conform cu cerințele de bază sau cu CPS ale CA.).
5. CessationOfOperation (RFC 5280 CRLReason # 5)
   - Beneficiarul certificatului ar trebui să aleagă motivul revocării "cessationOfOperation" atunci când site-ul web certificat este închis înainte de expirarea certificatului sau dacă Beneficiarul nu mai deține sau nu mai controlează numele de domeniu din certificat înainte de expirarea certificatului..
6. privilegeWithdrawn (RFC 5280 CRLReason #9)[8]
   - 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 Autorităţilor de Certificare afiliate.
Serverul OCSP, care emite confirmări ale stării certificatelor, foloseşte o pereche specială de chei pentru fiecare CA Subordonat și Root CA, generată exclusiv pentru acest scop.
Certificatul serverului OCSP conţine extensia extKeyUsage, descrisă în RFC 5280.

[8] *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 este setată ca fiind ne-critică și semnifică faptul că o Autoritate de Certificare care emite certificatul pentru serverul OCSP confirmă prin semnătura sa delegarea autorizării de a emite confirmări ale stării certificatelor (aparţinând Beneficiarilor acestei autorităţi).
De asemenea, certificatul serverului OCSP conţine extensia OCSPNoCheck, descrisă de RFC 6960. Această extensie este declarată ca fiind ne-critică și semnifică faptul că un client de OCSP care primeşte un răspuns semnat cu cheia privată asociată acestui certificat poate avea încredere în starea certificatului serverului OCSP, nefiind necesară verificarea stării de revocare a acestuia.
Entitatea care primeşte o confirmare emisă de serverul OCSP trebuie să suporte formatul standard de răspuns având identificatorul id-pkix-ocsp-basic.
Informaţiile despre starea certificatului sunt incluse în câmpul certStatus al structurii SingleResponse. Acesta poate avea una dintre următoarele trei valori principale:
- GOOD – indică faptul că certificatul este în stare validă
- REVOKED – indică faptul că certificatul a fost emis și a fost revocat sau certificatul nu a fost emis conform RFC 6960
- UNKNOWN – indică faptul că nu există suficiente informaţii pentru determinarea stării certificatului respectiv
Când răspunsul OCSP conține un cod de eroare (mesaj), răspunsul nu este semnat digital (RCF 6960).

7.3.1 Numarul versiunilor

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

7.3.2 Extensii OCSP

În conformitate cu RFC 6960, serverul OCSP certSIGN acceptă următoarea extensie:

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

8 Auditul de conformitate și alte evaluări

În ceea ce privește auditurile de conformitate și competența, funcționarea consecventă și imparțialitatea conformității organismelor de evaluare care evaluează și certifică conformitatea noastră ca furnizor de servicii de certificare și conformitatea serviciilor noastre de certificare pentru criteriile din Regulamentul 1183/2024 și al actelor de punere în aplicare, conformitatea cu CA/B Forum Baseline Requirements, si cu CA/B Forum EV Guidelines, urmărim cerințele din standardul ETSI EN 319 401 ESTI EN 319 411-1 si ESTI EN 319 411-2 și ne conformam cu:

- cerințele din cea mai recentă versiune a „Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates" si a „CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates".
- cerințele de audit de la cap. 8 din cea mai recentă versiune a „Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates" si a „CA/B Forum Guidelines for the Issuance and Management of Extended Validation Certificates".
- cerințele din partea organismului de supraveghere din România (ADR), deoarece suntem licențiați ca CA în România.

8.1 Frecvența sau circumstanțele de evaluare

Activitățile certSIGN care sprijină furnizarea serviciilor prezentate de CPP 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 EN 319 401, ETSI EN 319 411, CA/B Forum Baseline Requirements si standardele tehnice din Ghidurile CA/B Forum EV.

Auditurile la cerere pot fi realizate la discreția certSIGN, la cererea organismului de supraveghere, astfel cum este definit în Regulamentul UE 1183/2024, 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 1183/2024 și în specificațiile CA/B Forum Baseline Requirements și în specificațiile CA/B Forum EV Guidelines.

8.3 Relația evaluatorului cu entitatea evaluată

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

8.4 Subiectele acoperite de evaluare

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

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

- managementul configuratiei sistemelor
- managementul riscurilor operationale si de securitate (evaluari, rapoarte etc)
- securitate procedurala (actualizare fise post personal cu atributii specifice) ....
- securitatea fizică a certSIGN,
- procedurile de verificare a identităţii Abonaților,

- serviciile de certificare și procedurile de furnizare a serviciilor,
- securitatea aplicaţiilor software și a accesului la reţea,
- securitatea personalului certSIGN,
- jurnalele de evenimente și procedurile de monitorizare a sistemului,
- arhivarea și restaurarea datelor,
- procedurile de arhivare,
- înregistrările referitoare la modificarea parametrilor de configurare pentru certSIGN,
- înregistrările referitoare la analizele și verificările efectuate pentru aplicaţiile software și dispozitivele hardware.

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

8.5 Acțiuni întreprinse ca urmare a deficienței

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

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

8.6 Comunicarea rezultatelor

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

Raportul de audit va prevedea în mod explicit că acoperă sistemele și procesele relevante utilizate pentru emiterea tuturor certificatelor care confirma identificatorii de politica declarati. CA pune la dispoziția publicului raportul de audit în cel mult trei luni de la încheierea perioadei de audit. Raportul de audit va fi în conformitate cu ETSI EN 319 403, capitolul 7.4.4, și cu CABF Baseline Requirements, capitolul 8.6.

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

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

8.7 Audituri interne

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

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

din certificatele verificate de către terța parte delegată în perioada care începe imediat după prelevarea ultimului eșantion. certSIGN utilizează un proces de Linting pentru a verifica acuratețea tehnică a certificatelor din setul de eșantioane selectate, independent de lintingul anterior efectuat pe aceleași certificate.

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

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

9 Alte elemente de afaceri și legale

9.1 Tarife

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

Serviciile oferite de certSIGN sunt stabilite după cum urmează:

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

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

9.1.1 Tarifele serviciilor de emitere și reînnoire a certificatelor

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 Taxe pentru alte servicii

Prețurile sunt stabilite conform politicii interne de preț.

9.1.5 Politica de rambursare

Plățile pot fi rambursate conform condițiilor contractuale aplicabile..

9.2 Răspunderea financiară

9.2.1 Acoperirea prin asigurare

certSIGN îndeplinește cerințele obligatorii din secțiunea 6.8.2.Responsabilitate Financiară din ETSI EN 319 411-2.

certSIGN are încheiate polițe de asigurare comerciale si profesionale și va acoperi daunele pe care le-ar putea provoca din cauza serviciilor de certificare pentru persoanele care își construiesc etica pe baza efectelor juridice ale certificatelor emise de certSIGN Web CA G2 in limitele stabilite de prezentul CPP, acordurile contractuale incheiate, dupa caz.

9.2.2 Alte active

Nu este stipulat.

9.2.3 Asigurarea sau acoperirea garanției pentru entitățile finale

Pentru certificate DV, OV: certSIGN beneficiază de o asigurare care acoperă răspunderea profesională.

Pentru certificate EV, QWAC: certSIGN îndeplinește cerințele obligatorii din secțiunea 8.4. Asigurare din partea CA / B Forum EV Guidelines.

9.3 Confidențialitatea informațiilor de afaceri

9.3.1 Scopul informatiilor confidentiale

Toate informaţiile referitoare la Beneficiar/Entități Partenere pe care le prelucrează certSIGN sunt obţinute, păstrate şi procesate în concordanţă cu prevederile Regulamentului (UE) nr. 1183/2024. Relaţiile dintre un Beneficiar, o Entitate Parteneră și certSIGN se bazează pe încredere.

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

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

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

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

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

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

Tipuri de informații considerate a fi confidențiale și private

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

- informaţiile furnizate de Beneficiari, în plus faţă de informaţiile care apar in certificate si in Depozitar; dezvăluirea acestor informaţii se face doar cu aprobare scrisă, în prealabil, din partea proprietarului informaţiei sau în alte condiţii prevăzute de lege;
- conţinutul contractelor încheiate cu Beneficiarii sau Entităţile Partenere, conturi bancare, aplicaţiile de înregistrare, emitere, reînnoire, revocare certificate; aceste informații pot fi dezvăluite doar cu aprobarea și în scopul menţionat de proprietarul informaţiilor (de exemplu, Subiectul), cu excepţia informaţiilor incluse în certificate sau din Depozitar, conform prezentului CPP;
- înregistrările corespunzătoare tranzacţiilor din sistem (toate tipurile de tranzacţii, precum și datele pentru controlul tranzacţiilor, aşa numitele loguri ale tranzacţiilor din sistem);
- înregistrările corespunzătoare evenimentelor (log-uri) ce ţin de serviciile de certificare, păstrate de certSIGN;
- rezultatele auditurilor externe vor fi făcute publice;
- planurile în caz de urgenţă;

- informaţiile referitoare la măsurile luate pentru protecţia dispozitivelor hardware şi aplicaţiilor software, informaţiile referitoare la administrarea serviciilor de certificare și la regulile de înregistrare planificate.

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

Dezvăluirea motivului pentru care un certificat a fost revocat

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

Dezvăluirea Informațiilor Confidențiale Reprezentanților Autorităților Legale

Informaţiile confidenţiale pot fi dezvăluite reprezentanţilor autorităţilor legale numai după îndeplinirea tuturor formalităţilor cerute de legislaţia în vigoare în România.

9.3.2 Informații care nu sunt considerate a fi confidențiale

Informaţiile incluse într-un certificat de către Autorităţile de Certificare emitente, în conformitate cu specificaţiile din Capitolul 7 nu sunt confidențiale. Un Beneficiar care aplică pentru obţinerea unui certificat cunoaşte ce fel de informaţii vor fi incluse în certificat şi este de acord cu publicarea acestora.

Cu excepția informațiilor prevăzute la alineatul anterior, informaţiile furnizate de / către Beneficiar pot fi puse la dispoziţia altor entităţi, doar cu acordul scris al Beneficiarului și în scopul menţionat în contractul încheiat cu Beneficiarului.

9.3.3 Responsibilitatea de a proteja informațiile confidențiale

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

9.4 Confidențialitatea datelor cu caracter personal

În prestarea serviciilor de încredere certSIGN prelucrează date cu caracter personal ale Beneficiarului în conformitate cu cerințele Regulamentului (UE) nr. 1183/2024 și cu respectarea dispozițiilor Regulamentului nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date și al altor dispoziții de drept al Uniunii referitoare la protecția datelor.

Scopul prelucrării datelor cu caracter personal este acela de a presta servicii de încredere.

9.4.1 Planul de asigurare a protectiei datelor cu caracter personal

În prestarea serviciilor de încredere, 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. 1183/2024, 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. 1183/2024.
- accesul la serviciile certSIGN se referă la prelucrarea doar a acelor date de identificare, care sunt adecvate, pertinente și necesare pentru a acorda acces la serviciul respectiv

- este asigurată confidențialitatea și integritatea datelor de înregistrare: atunci când sunt schimbate cu beneficiarul / subiectul, atunci când sunt schimbate între componentele sistemului certSIGN, precum și atunci când sunt depozitate.

9.4.2 Informatii considerate ca fiind cu caracter personal

certSIGN tratează toate informațiile despre Abonat, sau despre reprezentanții/persoanele desemnate de Abonat care îl vor reprezenta în scopul eliberării certificatului ca date cu caracter personal.

9.4.3 Informații care nu sunt considerate cu caracter personal

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

9.4.4 Responsabilitatea de a proteja datele cu caracter personal

certSIGN se angajează să păstreze confidențialitatea datelor cu caracter personal atât în timpul prestării serviciilor de încredere, cat și după încetarea valabilității certificatelor. certSIGN nu va divulga date cu caracter personal niciunui tert, pentru niciun motiv, cu exceptia situatiilor in care va fi obligata sa o faca prin lege sau standarde aplicabile sau de catre autoritatile competente.

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

In procesul de emitere a unui certificate digital, Abonatul, persoanele desemnate de sau reprezentanții Abonatului sunt informati despre necesitatea utilizarii datelor cu caracter personal care le apartin, in vederea prestarii serviciului. Dacă persoanele vizate nu sunt de acord ca certSIGN sa le prelucreze datele certSIGN nu poate emite certificatele digitale.

De asemenea, în cazul în care certSIGN va utiliza datele în alte scopuri, Abonatul, persoanele desemnate de acesta sau reprezentanții Abonatului au posibilitatea de a opta explicit pentru utilizarea datelor cu caracter personal pentru alte scopuri comunicate în mod expres de certSIGN prin contract sau în alt mod.

9.4.6 Divulgare ca urmare a unui process administrativ sau juridic

certSIGN este exonerat de răspundere pentru dezvăluirea datelor cu caracter personal ale Abonatilor/Beneficiarilor, persoanele desemnate de acestia sau reprezentanții Abonatilor în următoarele situații:

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

9.4.7 Alte circumstante pentru divulgare

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

- ✓ dezvăluirea informațiilor personale față de:
  - auditori în cadrul auditurilor la care certSIGN este supus conform prevederilor Regulamentului (UE) nr. 1183/2024 în condiții de confidențialitate;

- firmele de curierat cu care certSIGN are contract, cu acordul Beneficiarului, în cazul în care acesta a optat pentru transmiterea certificatului la adresa de domiciliu sau la o altă adresă comunicată, cu respectarea acelorași obligații privind securitatea datelor cu caracter personal pe care le are și certSIGN;
- împuterniciți către care am externalizat anumite servicii;
- firmele afiliate certSIGN

✓ informațiile personale care apar în certificate sau în Directoarele publice (Depozitar), cu acordul Beneficiarului;

✓ în orice alte situații justificate cu înștiințarea în prealabil a Beneficiarului.

9.5 Drepturile de Proprietate Intelectuală

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

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

9.6 Reprezentări și garanții

9.6.1 Reprezentările și garanțiile CA

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

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

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

Garanțiile Certificatului le includ în mod specific pe cele menționate în CA/B Forum Baseline Requirements, paragraful 9.6.1, precum si in CA/B Forum EV Guidelines paragraful 9.6.1.

9.6.2 Reprezentările și garanțiile RA

RA are obligația de a respecta cu strictețe CPP, 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-ului aplicabil.

Termenii și condițiile CA conțin dispoziții care impun Beneficiarului obligațiile și garanțiile specificate în cerințele inițiale ale CA / B Forum, paragraful 9.6.3.

9.6.4 Reprezentările și garanțiile Entităților Partenere

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

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

9.6.5 Reprezentările și garanțiile altor participanti

Nu exista prevederi.

9.7 Exonerarea de răspundere privind garanțiile

Cu excepția celor prevăzute în mod expres în altă parte decât în CPP, și în legislația aplicabilă, certSIGN exonerează de răspundere 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 Beneficiarilor și Entităților Partenere.

9.8 Limitarea răspunderii

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

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

certSIGN nu răspunde față de nicio o persoană (beneficiar, subiect, terț, entitate parteneră etc.) in cazul în care datele prezentate la emiterea certificatelor sunt false, inexacte, incomplete sau expirate. certSIGN nu răspunde pentru daunele suportate de Beneficiar sau terți provocate de utilizarea certificatelor emise de CERTSIGN de către Beneficiar.
Fără a aduce atingere celor de mai sus, în cazul în care certSIGN nu a emis sau gestionat Certificatul în conformitate cu cerințele CABF BR/EV, cu politica sa de certificare și/sau cu documentul de Proceduri și Practici de Certificare, certSIGN va acoperi orice daune directe aduse abonaților sau părților terțe pentru revendicări legal recunoscute și probate, limitate la o sumă de două mii de dolari SUA pe Beneficiar sau entitate parteneră per certificat EV.

9.9 Despagubiri

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

certSIGN acționează conform prevederilor paragrafului "9.9 Indemnities" din cerințele inițiale ale Forumului CA / B Baseline Requirements și ale paragraful "9.9 Indemnities" de la CA / B Forum EV Guidelines.

certSIGN răspunde și compensează numai în limitele indicate mai sus.

9.10 Termenii și încetarea

9.10.1 Termenii

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

9.10.2 Incetarea

CPP rămâne în vigoare până la înlocuirea cu o nouă versiune.

9.10.3 Efectul terminării și supraviețuirii

Condițiile și efectul care rezultă din terminarea acestui CPP vor fi comunicate prin intermediul site-ului web certSIGN. Această comunicare va evidenția dispozițiile care pot supraviețui rezilierii acestui CPP și vor rămâne în vigoare. Responsabilitățile de protejare a informațiilor confidențiale și a dater personale trebuie să supraviețuiască încetării, iar termenii și condițiile pentru toate certificatele existente vor rămâne valabile pentru restul perioadelor de valabilitate ale acestor certificate.

9.11 Notificări individuale și comunicarea cu participanții

Toate notificările și alte comunicări care pot sau trebuie date, servite sau trimise în mod obligatoriu în temeiul CPP se vor face în scris și se vor transmite, cu excepția celor prevăzute în mod expres în CPP, fie prin (i) adresa de e-mail înregistrată, confirmare de primire, poșta preplătită, (ii) un serviciu de curierat "în 24 de ore" sau expres recunoscut international, (iii) livrarea În mână sau (v) în format electronic, semnat cu o semnătură electronică calificată și să fie adresată certSIGN, folosind datele de contact furnizate în capitolul 1.5.1 din prezentul document.

9.12 Amendamente

9.12.1 Procedura pentru amendamente

certSIGN este responsabilă, prin Comitetul de Management al Politicilor (CMPP) și Procedurilor, de aprobarea și modificarea prezentului CPP. CPP-se revizuieste cel putin odata pe an.Singurele modificări pe care le poate face CMPP acestor specificații CPP fără notificare sunt modificări minore care nu afectează nivelul de încredere al acestui CPP, de exemplu, corecturi editoriale sau tipografice sau modificări ale detaliilor de contact.

Erorile, actualizările sau modificările a acestui document vor fi comunicate așa cum este menționat în prezentul CPP, secțiunea 1.5.4.

CMPP acceptă, modifică sau respinge modificarea propusă după finalizarea unei faze de revizuire.

Orice modificări la CPP aprobate de CMPP sunt anunțate clienților certSIGN prin publicarea CPP-ului. 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 pot fi diseminate părților interesate la, sau după 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 cu prezentul CPP vor fi soluționate în conformitate cu legile din România.

9.14 Legea aplicabilă
Legea română guvernează aplicabilitatea, construirea, interpretarea, și validitatea prezentului CPP (fără a avea ca efect orice conflict de prevedere a legii care ar determina aplicarea altor legi).

9.15 Conformitatea cu legea aplicabilă
Prezentul CPP și furnizarea serviciilor certSIGN sunt conforme cu legile române relevante și aplicabile și regulamentul EU 1183/2024.

În cazul în care o instanță română sau organismul guvernamental român, cu jurisdicție asupra activităților acoperite de CPS, stabilește că îndeplinirea oricărei cerințe obligatorii este ilegală, atunci o astfel de cerință este considerată reformulată în măsura minimă necesară pentru a face cerința valabilă și legală. Acest lucru se aplică numai operațiunilor sau eliberărilor de certificate care fac obiectul legilor jurisdicției respective. În acest caz, certSIGN va notifica CA /Browser Forum cu privire la faptele, circumstanțele și legea (legile) implicate, astfel încât CA /Browser Forum să poată revizui Ghidul BR și EV în consecință.

9.16 Prevederi diverse
certSIGN asigura accesul nerestrictionat la serviciile furnizate pentru persoanele cu disabilitati in conformitate cu legislatia si standardele in vigoare.

9.16.1 Întregul acord
Nu este stipulat.

9.16.2 Cesiunea
Nu este stipulat.

9.16.3 Anulabilitate
CA acționează conform specificatiilor din "9.16.3 Severability" din cerințele de bază ale CA/B Forum.

9.16.4 Executarea (onorariile avocaților și renunțarea la drepturi)
Nu este stipulat.

9.16.5 Forta Majora
CA actioneaza conform cu legile din României privind forța majoră.

9.17 Alte prevederi
Nu este stipulat.