Codul de Practici și Proceduri certSIGN

SSL DV CA Clasa 3 G2

pentru certificate SSL DV

Versiunea 1.23

Data: 20 Februarie 2026

Notă importantă

Adresa: Bulevardul Tudor Vladimirescu nr. 29 A,
AFI Tech Park 1, București, România
Telefon: 004-021-31.19.901

Web:www.certsign.ro

Istoric document[1]

Vers.	Data Efectivă[2]	Motiv	Persoana care a făcut schimbarea
1.0	Ianuarie 2018	Publicarea primei versiuni	Securitatea informațiilor Ofiţer
1.1	Mai 2018	Conformitatea CPP cu recomandările GDPR	Manager de politici PKI
1.2	Iulie 2018	Conformitatea CPP cu CA-Browser Forum, cu privire la validarea dreptului de proprietate sau control al solicitantului asupra domeniului	Manager de politici PKI
1.3	Noiembrie 2018	Actualizare sediu	Manager de politici PKI
1.4	Ianuarie 2019	Evaluare anuală. Actualizări determinate de eliminarea caracterului „_” în numele domeniului / dNSName. Conform CA / Browser Forum BR 1.6.2	Manager de politici PKI
1.5	Ianuarie 2020	Evaluare anuală. Actualizări minore pentru conformitate cu CA / Browser Forum BR 1.6.7 și Mozilla Policy v2.7.	Manager de politici PKI
1.6	Mai 2020	Adăugare metodă de validare 3.2.2.4.2	Manager de politici PKI
1.7	Mai 2020	Remediere actualizări OCSP, valabilitate SSL 1 an	Manager de politici PKI
1.8	Septembrie 2020	Adăugare 7.2 CRL cf. CAB BR v1.7.2	Manager de politici PKI
1.9	Ianuarie 2021	Evaluare anuală	Manager de politici PKI
1.10	Mai 2021	Metode dovedire compromitere chei private	Manager Politici PKI
1.11	Septembrie 2021	Ballot SC 48 – FQDN	Manager Politici PKI
1.12	Noiembrie 2021	Actualizări metode validare domeniu	Manager Politici PKI
1.13	Ianuarie 2022	Revizuire anuală	Manager Politici PKI
1.14	Iunie 2022	Actualizări ref. CA Subordonat, motive revocare & valabilitate	Manager Politici PKI
1.15	Octombrie 2022	Actualizari validare identitate, cererea de certificat, CRL Reason	Manager Politici PKI
1.16	Ianuarie 2023	Revizuire anuală	Manager Politici PKI
1.17	Mai 2023	Actualizari diverse, OIDs, links	Manager Politici PKI
1.18	Iulie 2023	Mutare profile (#7) in doc extern	Manager Politici PKI
1.19	Ianuarie 2024	Revizuire anuală	Manager Politici PKI
1.20	15 Ianuarie 2025	Revizuire anuală	Manager Politici PKI
1.21	15 Aprilie 2025	Actualizari metode validare domeniu, ACME, MPIC	Manager Politici PKI
1.22	15 Ianuarie 2026	Revizuire anuală	Manager Politici PKI
1.23	20 Februarie 2026	Actualizari minore	Manager Politici PKI

[1] *Datele din istoric se referă la versiunea în limba engleză a acestui document. Traducerea în limba română are ca dată de creare, aprobare și distribuire Aprilie 2021*
[2] *Data efectivă este ultima zi a lunii*

Acest document a fost creat de către și este proprietatea[3]:

Proprietar	Autor	Data creării
BU Servicii de incredere	Ofițer Securitate Informatică	Ianuarie 2018

Lista de distribuție

Destinaţie	Data distribuirii
Public-Internet	Ianuarie 2018
Public-Internet	Mai 2018
Public-Internet	Iulie 2018
Public-Internet	Noiembrie 2018
Public-Internet	Ianuarie 2019
Public-Internet	Ianuarie 2020
Public-Internet	Mai 2020
Public-Internet	Septembrie 2020
Public-Internet	Ianuarie 2021
Public-Internet	Aprilie 2021
Public-Internet	Mai 2021
Public-Internet	Septembrie 2021
Public-Internet	Noiembrie 2021
Public-Internet	Ianuarie 2022
Public-Internet	Iunie 2022
Public-Internet	Octombrie 2022
Public-Internet	Ianuarie 2023
Public-Internet	Mai 2023
Public-Internet	Iulie 2023
Public-Internet	Ianuarie 2024
Public-Internet	Ianuarie 2025
Public-Internet	Aprilie 2025
Public-Internet	Ianuarie 2026
Public-Internet	Februarie 2026

Acest document a fost aprobat de:

Versiune	Nume	Data
1.0	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2018
1.1	Comitet de Management al Politicilor și Procedurilor	Mai 2018
1.2	Comitet de Management al Politicilor și Procedurilor	Iulie 2018
1.3	Comitet de Management al Politicilor și Procedurilor	Noiembrie 2018
1.4	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2019
1.5	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2020
1.6	Comitet de Management al Politicilor și Procedurilor	Mai 2020

[3] *Datele de creare, distribuire și aprobare se referă la versiunea în limba engleză a acestui document. Traducerea în limba română are ca dată de creare, aprobare și distribuire Aprilie 2021*

1.7	Comitet de Management al Politicilor și Procedurilor	Mai 2020
1.8	Comitet de Management al Politicilor și Procedurilor	Septembrie 2020
1.9	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2021
1.10	Comitet de Management al Politicilor și Procedurilor	Mai 2021
1.11	Comitet de Management al Politicilor și Procedurilor	Septembrie 2021
1.12	Comitet de Management al Politicilor și Procedurilor	Noiembrie 2021
1.13	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2022
1.14	Comitet de Management al Politicilor și Procedurilor	Iunie 2022
1.15	Comitet de Management al Politicilor și Procedurilor	Octombrie 2022
1.16	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2023
1.17	Comitet de Management al Politicilor și Procedurilor	Mai 2023
1.18	Comitet de Management al Politicilor și Procedurilor	Iulie 2023
1.19	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2024
1.20	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2025
1.21	Comitet de Management al Politicilor și Procedurilor	Aprilie 2025
1.22	Comitet de Management al Politicilor și Procedurilor	Ianuarie 2026
1.23	Comitet de Management al Politicilor și Procedurilor	Februarie 2026

Cuprins

1 Introducere

Sistemul PKI certSIGN ROOT CA, care include certSIGN SSL DV CA Clasa 3 G2, este la sfârșitul ciclului de viață, și nu mai emite certificate.

Codul de Practici și Proceduri certSIGN SSL DV CA Clasa 3 G2 pentru certificate SSL DV - (denumit în continuare **CPP**) descrie în detaliu politica de certificare și practicile aplicate de certSIGN pentru emiterea certificatelor **SSL DV** (validare domeniu).

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

- ETSI EN 319 411-1
- CA/B Forum Baseline Requirements (Politica DV 2.23.140.1.2.1)
- CA/Browser Forum Network and Certificate System Security Requirements
- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities — SSL Baseline with 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 Prezentare generală

certSIGN, beneficiari, subiecți și operațiunile asociate ale părților dependente depind de CPP pentru eliberarea certificatelor DV SSL. De asemenea, acest document descrie regulile generale pentru furnizarea de servicii de certificare, cum ar fi înregistrarea subiectului, certificarea cheii publice, rekey-ul certificatelor și revocarea certificatelor.

1.2 Numele și identificarea documentului

Acest document se numește **Codul de Practici și Proceduri certSIGN SSL DV CA Clasa 3 G2 pentru certificate SSL DV**, denumită în continuare CPP.

Documentul este disponibil în format electronic în depozit la adresa https://www.certsign.ro/ro/depozitar

1.3 Participanți PKI

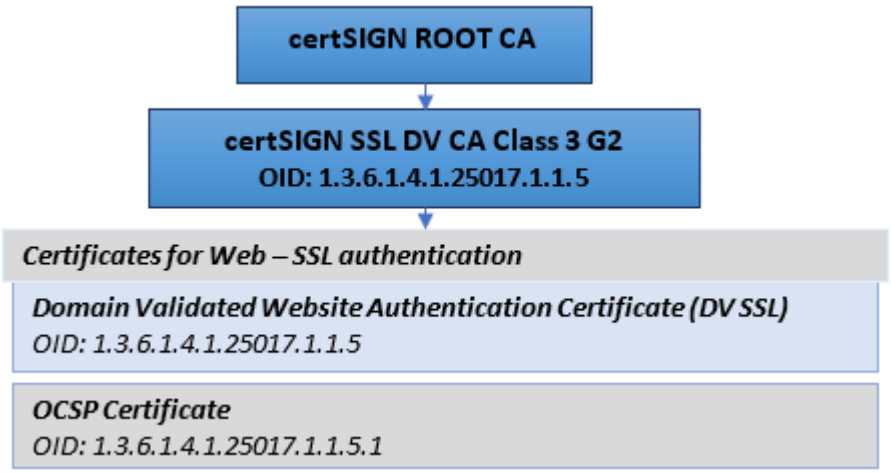
CPP reglementează cele mai importante relații dintre entitățile aparținând certSIGN, echipele de consultanță (inclusiv auditorii) și clienții (utilizatorii serviciilor furnizate):

- certSIGN SSL DV CA Clasa 3 G2
- Autoritatea de Înregistrare,
- Depozitarul,
- Protocolul de stare a certificatului online (autoritatea OCSP),
- Subiecte,
- Beneficiari,
- Terțe părți,
- Furnizori relevanți pentru certSIGN privind emiterea și gestionarea certificatelor digitale.
- Comitet de Management al Politicilor și Procedurilor

certSIGN oferă servicii de certificare pentru fiecare persoană fizică sau juridică care acceptă reglementările prezentului CPP. Scopul acestor practici (care includ procedurile de generare a cheilor, procedura de emitere a certificatelor și securitatea sistemului informațional) este de a asigura utilizatorilor serviciilor certSIGN că nivelurile de credibilitate declarate ale certificatelor emise corespund cu practicile Autorităților de Certificare.

1.3.1 Autoritățile de certificare

Autoritatea de certificare certSIGN SSL DV CA Clasa 3 G2 este o autoritate de certificare Intermediară pentru domeniul certSIGN. Este subordonată certSIGN ROOT CA. certSIGN SSL DV CA Clasa 3 G2 este identificată prin următorul OID: 1.3.6.1.4.1.25017.1.1.5.



Înainte de a începe activitatea, certSIGN SSL DV CA Clasa 3 G2 a trimis o cerere către Autoritatea de certificare primară, certSIGN ROOT CA pentru înregistrare și eliberarea certificatului de cheie publică.

1.3.2 Autoritățile de înregistrare

Autoritatea de înregistrare primește, verifică și aprobă sau respinge cererile de înregistrare și eliberare a certificatelor, rekey-ul certificatului și cererile de revocare. Verificarea cererilor intenționează să autentifice (pe baza documentelor anexate cererilor) atât beneficiarul / subiectul, cât și datele specificate în cerere. Autoritatea de înregistrare poate depune cereri și Autorității de Certificare corespunzătoare pentru a anula o cerere sau a retrage un certificat.

Autoritatea de înregistrare este operată de certSIGN sau de o terță parte delegată, dacă legislația permite acest lucru. Înainte ca certSIGN să autorizeze un terț delegat să îndeplinească o funcție delegată, certSIGN solicită contractual terțului delegat să îndeplinească condițiile specificate în documentul „Cerințe pentru autoritatea de înregistrare delegată pentru certificatele certSIGN SSL DV CA Clasa 3 G2”.

1.3.3 Beneficiari

Beneficiar

Beneficiarul este persoana fizică sau entitatea juridică căreia i se eliberează un certificat și care este legată legal de un Contract de beneficiar sau de Termenii de utilizare. Beneficiarii pot solicita emiterea, revocarea sau rekey-ul certificatelor entității finale pentru subiecții aflați

în grija lor. Un Beneficiar este, de asemenea, responsabil pentru notificarea imediată a certSIGN cu privire la (suspiciunea) compromisul cheii private.

Subiect

Subiectul este entitatea (persoană juridică sau fizică) căreia i se eliberează un certificat și este identificată într-un certificat ca titular al cheii private asociate cu cheia publică din certificat.

Subiectul poate fi:

- Beneficiarul în cazul în care solicită el însuși certificatul,
- O persoană fizică pentru care Beneficiarul solicită certificatul, având un acord juridic obligatoriu sau acționând ca angajator al acestuia
- O persoană juridică pentru care Beneficiarul solicită certificatul

Un subiect este, de asemenea răspunzător de:

- Notificarea imediată a certSIGN cu privire la (suspiciunea) compromisului cheii private;
- Trimiterea cererilor de reînnoire a cheilor și / sau certificatelor la certSIGN în timp util;
- Asigurarea faptului că confidențialitatea cheii lor private este protejată într-un mod care este în concordanță cu acest document;
- Asigurarea faptului că accesul la utilizarea cheii lor private este controlat într-un mod care este în concordanță cu acest document.

1.3.4 Entități partenere

O entitate parteneră, care utilizează serviciile certSIGN, poate fi orice entitate care ia decizii bazate pe corectitudinea conexiunii dintre identitatea unui subiect și cheia publică.

O entitate parteneră este responsabilă pentru modul în care verifică starea actuală a certificatului unui subiect. O astfel de decizie va fi luată de fiecare dată când o entitate parteneră este dispusă să utilizeze un certificat pentru a verifica identitatea sursei sau pentru a crea un canal de comunicare sigur cu subiectul certificatului. O entitate parteneră va utiliza informațiile dintr-un certificat pentru a decide dacă un certificat a fost utilizat în conformitate cu scopul declarat.

1.3.5 Alți participanți

Comitet de Management al Politicilor și Procedurilor este un comitet creat în certSIGN de către consiliul de administrație pentru a supraveghea întreaga activitate a tuturor autorităților de certificare certSIGN și a autorităților de înregistrare. Rolurile și responsabilitățile PPMB sunt descrise în documentația internă.

Furnizori de servicii certSIGN: furnizori externi care susțin activitățile certSIGN în baza unui acord contractual semnat.

Notarii publici: pot efectua identificarea și garanta pentru identitatea reală a subiecților.

1.4 Utilizarea certificatului

Zona de aplicabilitate a certificatului stabilește domeniul de aplicare în care poate fi utilizat un certificat. Acest domeniu este definit de două elemente:

- Primul definește aplicabilitatea certificatului
- Cealaltă este o listă sau o descriere a aplicațiilor permise și interzise.

Entitatea parteneră este responsabilă de stabilirea nivelului de credibilitate necesar unui certificat utilizat într-un anumit scop. Luând în considerare factorii de risc semnificativi, entitatea parteneră va decide ce tip de certificat emis de certSIGN îndeplinește cererile formulate. Subiecții vor cunoaște cererile entităților partenere (de exemplu, aceste cereri ar putea fi publicate ca o politică de semnătură sau o politică de securitate a informațiilor) și apoi să solicite certSIGN să emită certificate corespunzătoare acestor cereri.

1.4.1 Utilizări admise ale certificatului

Certificatele de server SSL DV sunt utilizate pentru a activa protocolul TLS / SSL pe unul sau mai multe site-uri web, al căror domeniu a fost validat de certSIGN.

Se presupune că beneficiarul deține competența și instrumentele necesare pentru a solicita, instala și utiliza certificatul.

Este responsabilitatea beneficiarului, a subiectului și a entității partenere să decidă în ce scop certificatele sunt considerate demne de încredere. O entitate parteneră trebuie să ia întotdeauna în considerare nivelul de asigurare și alte informații din CPP înainte de a decide cu privire la aplicabilitatea certificatului.

1.4.2 Utilizări interzise ale certificatului

Orice utilizare a unui certificat, alta decât utilizarea permisă explicit în CPP, este interzisă.

1.5 Administrarea politicilor

1.5.1 Organizația care administrează documentul

Prezentul document este administrat de către certSIGN TSP (TSP = Prestator de servicii de incredere) prin Comitetul de Management al Politicilor și Procedurilor (PPMB). PPMB include membri superiori ai conducerii, precum și personal responsabil pentru gestionarea operațională a mediului certSIGN TSP PKI.

Nume	SC certSIGN SA Sediu: Bulevardul Tudor Vladimirescu 29 A, Parcul Tehnic AFI 1, București, România Număr de înregistrare: J40 / 484/2006 Cod de înregistrare fiscală: RO 18288250 Sediul social: strada Oltenitei 107A. clădirea C1, parter, sector 4, București, România, PC 041303
Telefon	(+4021) 3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel: 1.5.1 Organizația care administrează documentul

1.5.2 Persoană de contact

Nume	Comitet de Management al Politicilor și Procedurilor (PPMB)
Telefon	(+4021) 3119901
e-mail	office@certsign.ro

Web	www.certsign.ro

Tabel: 1.5.2 Persoană de contact

Procedura de raportare a problemelor legate de certificat

Din cauza unor erori, limitări tehnice sau procedurale sau din alte motive, certificatele pot fi emise greșit de certSIGN (de exemplu, certificatul emis conține informații greșite despre subiect sau organizație). De asemenea, pot exista cazuri când un certificat este utilizat în mod necorespunzător (de exemplu, pentru activități infracționale). Dacă beneficiarii, părțile dependente sau alte terțe părți se confruntă cu astfel de situații, dacă suspectează compromisul cheii private sau alte tipuri de activități frauduloase, utilizarea abuzivă a unui certificat sau o conduită necorespunzătoare sau orice alte aspecte similare legate de certificatele emise de certSIGN, aceștia pot raporta problemele respective la adresa **revokecsgn@certsign.ro**, informând CA emitent cu privire la o cauză rezonabilă pentru revocarea certificatului. certSIGN CA va începe investigarea unui raport privind problema certificatului în termen de douăzeci și patru de ore de la primire și va decide dacă revocarea sau alte acțiuni adecvate sunt justificate pe baza cel puțin următoarelor criterii:

1. Natura presupusei probleme;
2. Numărul de Rapoarte de Probleme de Certificat primite despre un anumit certificat sau beneficiar;
3. Entitatea care face reclamația (de exemplu, o reclamație a unui 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 să pretindă că nu a primit bunurile pe care le-a comandat); și
4. Legislația relevantă.

certSIGN CA menține o capacitate continuă 24x7 de a răspunde intern la un Raport cu Probleme de Certificat cu prioritate ridicată și, după caz, transmite o astfel de reclamație autorităților de aplicare a legii și / sau revoca un certificat care face obiectul unei astfel de reclamații. Rapoartele privind problemele de certificat trebuie trimise la adresa **revokecsgn@certsign.ro**.

1.5.3 Persoana care decide conformitatea CPP cu politica

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

Tabel: 1.5.3 Persoana care decide conformitatea CPP cu politica

1.5.4 Proceduri de aprobare CPP

Comitetul de Management al Politicilor și Procedurilor este responsabil pentru aprobarea CPP. Procedura de aprobare este cuprinsă într-o instrucțiune internă.
Beneficiarii vor respecta CPP-ul implementat și publicat la: http://certsign.ro/repository
Subiecții / Beneficiarii care nu acceptă termenii și reglementările noi, modificate, ale CPP trebuie să facă o declarație adecvată în termen de 15 zile de la data noii versiuni a aprobării

CPP. Acest lucru va duce la rezilierea contractului legat de furnizarea de servicii de certificare și revocarea certificatului emis pe teren.

1.6 Definiții și acronime

1.6.1 Definiții

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

Beneficiar/Solicitant: persoana fizică sau entitatea juridică care solicită (sau solicită reînnoirea) unui certificat. După emiterea certificatului, Solicitantul este denumit Beneficiar. Pentru certificatele emise dispozitivelor, Solicitantul este entitatea care controlează sau operează dispozitivul numit în certificat, chiar dacă dispozitivul trimite cererea de certificat efectivă.

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

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

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

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

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

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

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

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

CAA: De la RFC 6844 (http: tools.ietf.org/html/rfc6844): „Înregistrarea resurselor DNS de autorizare a autorității de certificare (CAA) permite unui titular de nume de domeniu DNS să specifice autoritățile de certificare (CA) autorizate să elibereze certificate pentru acel domeniu. Publicarea înregistrărilor de resurse CAA permite unei autorități publice de certificare să implementeze controale suplimentare pentru a reduce riscul de emisie neintenționată a certificatului. "

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

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

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

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

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

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

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

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

Control: „Control" (și semnificațiile sale corelative, „controlat de" și „sub control comun cu") înseamnă deținerea, directă sau indirectă, a puterii de a: (1) conduce conducerea,

personalul, finanțele sau planurile acestor entitate; (2) controlează alegerea majorității directorilor; sau (3) votează acea parte din acțiunile cu drept de vot necesare pentru „control" conform legii jurisdicției de constituire sau înregistrare a entității, dar în niciun caz mai mică de 10%.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cerere de certificat cu risc ridicat: o cerere care să fie marcată de CA pentru control suplimentar prin referire la criteriile interne și bazele de date menținute de CA, care pot include nume cu risc mai mare de phishing sau alte utilizări frauduloase, nume conținute în cereri de certificate respinse anterior sau certificate revocate , nume enumerate în lista de phishing Miller Smiles sau în lista de navigare sigură Google sau nume pe care CA le identifică utilizând propriile criterii de reducere a riscurilor.

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

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

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

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

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

Pereche de chei: cheia privată și cheia publică asociată.

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

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

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

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

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

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

Companie mamă: o companie care controlează o companie filială.

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

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

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

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

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

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

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

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

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

pentru a descrie un rol sau o funcție, nu implică neapărat un corp separat, dar poate face parte din CA.

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

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

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

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

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

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

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

Cerințe: Cerințele de bază găsite în CABF BR.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.6.2 Acronime

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

Acronim	Original	Traducere
NIST	(US Government) National Institute of Standards and Technology	(Guvernul SUA) Institutul Național de Standarde și Tehnologie
OCSP	Online Certificate Status Protocol	Protocol de stare a certificatelor online
OID	Object Identifier	Identificator de obiect
OV	Organization Validated	Organizație validată
PKI	Public Key Infrastructure	Infrastructură cu cheie publică
PPMB	Policies and Procedures Management Body	Organism de gestionare a politicilor și procedurilor
QSCD	Qualified Electronic Signature Creation Device	Dispozitiv de creare a semnăturilor electronice calificat
QWAC	Qualified Certificate for Website Authentication	Certificat calificat pentru autentificarea site-urilor web
RA	Registration Authority	Autoritatea de înregistrare
RSA	Rivest, Shamir, Adleman asymmetric cryptographic algorithm	Algoritm criptografic asimetric Rivest, Shamir, Adleman
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)	MIME securizat (Extensii multifuncționale de poștă electronică pe Internet)
SSL	Secure Sockets Layer	Secure Sockets Layer
TLS	Transport Layer Security	Securitatea stratului de transport
TSP	Trust Services Provider	Furnizor de servicii de încredere
UTC	Coordinated Universal Time	Timp universal coordonat
VoIP	Voice Over Internet Protocol	Protocol de voce pe internet

2 Responsabilități de publicare și depozitare

2.1 Depozite

Depozitul este disponibil on-line: https://www.certsign.ro/ro/depozitar. Contine:

- Codul de Practici și Proceduri pentru pentru CA SSL DV https://www.certsign.ro/ro/document/certsign-ssl-dv-ca-class-3-g2-codul-de-practici-si-proceduri/
- Certificatele Root CA și ale CA-urilor Intermediare https://www.certsign.ro/ro/resurse/lantul-de-incredere/
- Certificatele Subiecților https://registru.certsign.ro/cgi-bin/pubral/pubra/get_cert
- Listele Certificatelor Revocate https://www.certsign.ro/ro/resurse/lista-certificate-revocate/
- Termeni și condiții pentru utilizarea certificatelor digitale https://www.certsign.ro/ro/document/termeni-si-conditii-generale-pentru-certificate-ssl-dv-si-ov/

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

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

2.2 Publicarea informațiilor de certificare

La eliberarea certificatului digital, certificatul complet și corect este comunicat de certSIGN subiectului pentru care se eliberează certificatul.

Certificatele vor fi disponibile pentru recuperare numai în acele cazuri pentru care a fost obținut consimțământul subiectului, așa cum este descris în documentul Termeni și condiții.

Pentru toate certificatele emise, informațiile despre starea certificatului sunt disponibile prin intermediul CRL-urilor și al serviciului OCSP furnizat de certSIGN 24 * 7 * 365.

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

certSIGN găzduiește 3 pagini web care permit furnizorilor de aplicații software să testeze software cu certificate de beneficiar emise de certSIGN SSL DV CA:

https://testssl-valid.certsign.ro/
https://testssl-expired.certsign.ro/
https://testssl-revoked.certsign.ro/
certSIGN pune la dispoziția părților de încredere termenii și condițiile privind utilizarea certificatelor SSL DV.

Disponibilitate

Disponibilitatea depozitului de documente și a depozitului CRL combinat este concepută pentru a depăși 99,8% din orele de lucru - definite ca 24 de ore pe zi, șapte zile pe săptămână, cu excepția perioadelor de întreținere planificate.

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

În caz de indisponibilitate din cauza unei catastrofe, a eșecului infrastructurii în afara controlului certSIGN sau a oricărui alt motiv, certSIGN SA va depune toate eforturile pentru a restabili disponibilitatea serviciului în termen de 5 zile lucrătoare.

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

2.3 Timpul sau frecvența publicării

Informațiile publicate de certSIGN sunt actualizate cu următoarea frecvență:

CPP – revizuire anuală, respectiv la actualizări, conform Capitol 1.5,

Certificatul autorităților de certificare - după emiterea unui nou certificat;

Certificatele subiecților - după obținerea consimțământului, după fiecare eliberare a unui nou certificat;

Lista certificatelor revocate - vezi Capitolul 7;

Rapoarte de audit efectuate de instituții autorizate - când certSIGN le primește;

Informații suplimentare - după fiecare actualizare.

2.4 Control acces pe depozite

Toate informațiile publicate de certSIGN în depozitul de pe adresa https://www.certsign.ro/ro/depozitar este disponibil pentru public.

certSIGN a implementat mecanisme de protecție logică și fizică împotriva adăugărilor, ștergerilor sau modificărilor neautorizate ale informațiilor publicate în depozit.

Beneficiarii, subiecții și părțile care au încredere au acces numai de citire prin internet la toate depozitele menționate în secțiunea 2.1.

certSIGN poate lua măsuri rezonabile pentru a proteja și preveni împotriva utilizării abuzive a depozitului, a OCSP și a serviciilor de descărcare CRL.

La descoperirea încălcării integrității informațiilor în depozit, certSIGN va întreprinde acțiuni adecvate pentru a restabili integritatea informațiilor, va impune acțiuni legale pentru cei care sunt vinovați și va notifica imediat entitățile afectate.

3 Identificare și autentificare

3.1 Denumire

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

3.1.1 Tipuri de nume

Certificatele emise de certSIGN 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 standardul X.509 (cu referire la recomandările seriei X.500). Denumirile de bază ale subiecților și ale emitenților de certificate plasate în certificatele certSIGN sunt conforme cu denumirile distincte - DN - (cunoscute și sub numele de directoare), create în urma recomandărilor X.500 și X.520. În cadrul DN, este posibil să se definească atributele Serviciului de nume de domeniu (DNS). Acest lucru permite subiecților să utilizeze două tipuri de nume: DN și DNS simultan. Aceasta este o opțiune foarte importantă în cazul emiterii de certificate către serverele administrate de subiect.

Pentru a asigura o comunicare electronică ușoară cu subiectul în certificatele certSIGN, se folosește un nume suplimentar pentru subiect. Acest nume poate conține, de asemenea, adresa de e-mail a subiectului, în conformitate cu recomandările RFC 822.

3.1.2 Nevoia ca numele să aibă înțeles logic

Certificatele SSL, cu excepția certificatelor de tip wildcard și de tip Unified Communications, sunt emise cu un nume de domeniu complet calificat (FQDN) sau cu o adresă IP.

Certificatele SSL conțin un asterisc. Înainte de a emite un astfel de certificat, trebuie să se stabilească dacă asteriscul apare pe prima poziție, în stânga sufixului unui domeniu controlat de organizația de înregistrare a domeniului (adică * .com.ro) sau a sufixului public (adică * .ro, * .edu, „* .com”, „* .co.uk”; pentru detalii, vezi RFC 6454 Secțiunea 8.2) și dacă se întâmplă acest lucru, CA administrat de certSIGN va refuza solicitarea, deoarece domeniul are nevoie să fie deținut sau controlat de beneficiar

Pentru certificatele SSL, în timp ce FQDN sau un nume de domeniu autentificat este plasat în atributul Common Name (CN) al câmpului Subject, acesta poate fi copiat și în extensia Subject Alternative Name, în DNS Name. Denumirea alternativă a subiectului este marcată ca non-critică, în conformitate cu RFC5280.

certSIGN nu emite certificate SSL care conțin „caracter de subliniere” („_”) în numele domeniului / dNSName, aceasta respectând ultima versiune publicată a recomandărilor CA / Browser Forum BR. FQDN cuprinde doar “P-labels” și „Non-Reserved LDH-labels”.

Certificatele SSL pot include adrese IP publice, în conformitate cu RFC 2460 (IP versiunea 6) sau RFC791 (IP versiunea 4).

Tipul certificatelor SSL de comunicații unificate (multi domeniu) pot include domenii nerutabile (de ex. .local) sau IP-uri private (în conformitate cu RFC 1918) în cadrul extensiei Subject Alternative Name. Emiterea de certificate SSL pentru domenii nerutabile, adrese IP private sau adrese IP rezervate (în conformitate cu http://www.iana.org/assignments/ipv4-address-

space/ipv4-address-space.xml și http: // www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml) este considerat învechit. În prezent, nu există certificate emise conform acestor specificații a căror dată de expirare este după 1 noiembrie 2015.

Numele inclus în numele distinctiv al subiectului este semnificativ în limba română, precum și în orice altă limbă care folosește alfabetul latin. Structura numelui distinctiv, aprobat / desemnat și verificat de o autoritate de înregistrare depinde de tipul subiectului.

DN constă din următoarele câmpuri opționale (descrierea câmpului este urmată de abrevierea sa care respectă recomandările X.520

- Câmp CN - Nume de domeniu complet calificat,
- Câmpul C - abrevierea internațională pentru numele țării.

Numele subiectului va fi confirmat de un operator al autorității de înregistrare și aprobat de o autoritate de certificare. certSIGN asigură (în cadrul domeniului său) unicitatea DN-urilor.

3.1.3 Anonimatul sau pseudonimitatea beneficiarilor
Fără stipulare.

3.1.4 Reguli pentru interpretarea diferitelor forme de nume
Interpretarea câmpurilor din certificatele emise de certSIGN se face în conformitate cu profilurile certificatelor descrise în Certificate și Profiluri CRL-uri (Capitolul 7). La crearea și interpretarea DN, se merge la recomandările menționate în capitolul 3.1.2.

3.1.5 Unicitatea numelor
Identificarea fiecărui titular al certificatelor emise de certSIGN se realizează pe baza DN. certSIGN asigură unicitatea DN atribuit fiecărui subiect.

3.1.6 Recunoașterea, autentificarea și rolul mărcilor comerciale
Fără stipulare.

3.2 Validarea inițială a identității

3.2.1 Metoda de a dovedi posesia cheii private
Posesia cheii private, corespunzătoare cheii publice pentru care se solicită generarea certificatului, va fi dovedită prin trimiterea cererii de semnare a certificatului (CSR), conform standardului RSA PKCS # 10, în care va fi inclus cheia publică semnată de cheia privată asociată.

Solicitarea prezentării dovezii de deținere a cheii private nu se aplică în cazul în care, la cererea beneficiarului sau a subiectului, perechea de chei este generată de autoritatea de certificare sau de autoritatea de înregistrare.

3.2.2 Autentificarea organizației și a identității domeniului
Este necesar să se demonstreze că entitatea care solicită certificatul DV SSL are control asupra domeniului la care se referă cererea de certificat.

Procedura de validare a dreptului de proprietate sau control al solicitantului asupra domeniului se bazează pe ETSI EN 319 411-1 și ultima versiune publicată a CA / Browser Forum - Politica de certificat de cerințe de bază pentru emiterea și gestionarea plafonului certificatelor de încredere publică.

3.2.2.1 Identitate

Reprezentanții instituției sunt obligați să prezinte următoarele documente:

- Cerere de cumpărare;

Procedura efectuată de RA pentru verificarea domeniului:

- Verificarea documentelor prezentate de beneficiar,
- Verificarea solicitării, care constă din:
  - Verificarea conformității datelor menționate în cerere cu cele din documentele prezentate,
  - verificarea dovezii deținerii cheii private (dacă cererea presupune o pereche de chei pentru a crea o semnătură electronică) și faptul că numele distinctiv este cel potrivit,
- Verificarea dacă domeniul menționat în certificat este înregistrat de entitatea care depune cererea de certificat sau de cel care a autorizat utilizarea domeniului de către entitatea solicitantă, în conformitate cu CA / Browser Forum - cap. 3.2.2.4.4 (E-mail construit către contactul de domeniu) sau 3.2.2.4.7 (Schimbare DNS).
- Verificarea în registrul de domenii Internet regional (baza de date RIPE pentru beneficiarii europeni) dacă persoana care solicită certificatul SSL este proprietarul sau are dreptul de a utiliza adresa IP rutabilă pentru care este solicitat certificatul.

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

Dacă 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,
- Copiază toate documentele și certificatele utilizate de operator
- În numele Autorității de certificare încheie un contract cu o persoană juridică privind prestarea de servicii de certificare.

Confirmarea este trimisă autorității de certificare care verifică dacă aceasta a fost emisă de o autoritate de înregistrare autorizată.

Procesul de autentificare este înregistrat. Tipul de informații și acțiuni înregistrate depinde de nivelul de credibilitate al certificatului care face obiectul cererii și se referă la:

- Identitatea operatorului Autorității de înregistrare care verifică cererea solicitantului,
- Data verificării,
- Identificatorul operatorului și al solicitantului în cazul în care acesta din urmă este prezent personal la Autoritatea de înregistrare (presupunând că solicitantului i s-a atribuit un astfel de identificator),

N/A

3.2.2.2 DBA (Doing Business As) / Denumire comercială

N/A

3.2.2.3 Verificarea țării

RA verifică țara asociată subiectului utilizând una dintre următoarele:

(a) Atribuirea intervalului de adrese IP în funcție de țară pentru oricare dintre ele

(i) adresa IP a site-ului web, așa cum este indicat de înregistrarea DNS a site-ului web

sau

(ii) adresa IP a subiectului / beneficiarului;

(b) ccTLD (Country Code Top-Level Domain) al numelui de domeniu solicitat;
(c) Informații furnizate de registratorul de nume de domeniu; sau
(d) O metodă identificată în secțiunea 3.2.2.1.
CA a implementat un proces de scanare a serverelor proxy pentru a preveni dependența de adresele IP atribuite în țări diferite de cea în care este de fapt localizat solicitantul.

3.2.2.4 Validarea autorizării sau controlului domeniului

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

certSIGN confirmă că, înainte de emitere, a validat fiecare nume de domeniu complet calificat (FQDN) ce apare in Certificat, folosind cel putin una din metodele de mai jos. certSIGN va efectua verificarea de domeniu pentru fiecare SAN inclus în aplicație. Astfel, mai multe puncte de contact pot fi utilizate și mai multe acțiuni pot fi necesare pentru a demonstra verificarea domeniului pentru toate domeniile solicitate.

certSIGN păstrează înregistrări ale metodei de validare a domeniului, inclusiv numărul de versiune BR relevant, pe care l-au folosit pentru validarea fiecărui domeniu.

3.2.2.4.1 Validarea solicitantului ca contact de domeniu

Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.2 E-mail, fax, SMS sau poştă către contactul de domeniu

Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.3 Contact telefonic cu contactul de domeniu

Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.4 E-mail construit către contactul de domeniu

În toate cazurile, certSIGN va trimite un e-mail construit către contactul de domeniu pentru a confirma că Solicitantul este conștient de această proprietate sau are control asupra 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 la adresa („@”)), urmat de numele de domeniu de autorizare și va include o valoare aleatorie (generată prin mijloace tehnice, unică în fiecare e-mail).

Valoarea aleatorie rămâne valabilă pentru utilizare într-un răspuns de confirmare timp de 30 de zile de la crearea sa.

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

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 validate. Această metodă este potrivită pentru validarea numelor de domenii Wildcard.

3.2.2.4.5 Document de autorizare a domeniului

Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.6 Schimbare asupra site-ului web
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.7 Schimbare DNS
certSIGN va trimite un e-mail persoanei de contact care a depus cererea pentru a confirma că Solicitantul are controlul asupra numelui de domeniu. Poșta electronică va include o valoare aleatorie (generată prin mijloace tehnice, unică în fiecare e-mail) care urmează să fie adăugată în intrarea DNS într-una dintre înregistrările DNS CNAME, TXT sau CAA a domeniului care urmează să fie verificat.
Valoarea aleatorie rămâne valabilă pentru utilizare într-un răspuns de confirmare timp de 30 de zile de la crearea sa.
E-mailul de răspuns trebuie trimis utilizând contul de e-mail utilizat pentru trimiterea inițială, iar certSIGN verifică dacă Valoarea aleatorie este aceeași.
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 validate.
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 domenii Wildcard.

3.2.2.4.8 Adresa IP
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.9 Certificat de testare
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.10 TLS folosind un număr aleatoriu
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.11 Orice altă metodă
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.12 Validarea solicitantului ca contact de domeniu
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.13 E-mail către contactul CAA DNS
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.14 3.2.2.4.13 E-mail către contactul DNS TXT
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.15 Contact telefonic cu contactul de domeniu
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.16 Contact telefonic cu contactul DNS TXT Record
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.17 Contact telefonic cu contactul DNS CAA Phone
Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.18 Modificare convenită la site-ul web v2

Această metodă de validare a domeniului nu este utilizată.

3.2.2.4.19 Modificare convenită la site-ul web - ACME

certSIGN confirmă controlul solicitantului asupra unui FQDN prin validarea controlului domeniului FQDN utilizând metoda ACME HTTP Challenge definită în secțiunea 8.3 din RFC 8555. Acest lucru se realizează prin primirea unui răspuns HTTP de succes la cerere. Tokenul nu este utilizat mai mult de 30 de zile de la crearea sa.
Atunci când certSIGN Web CA urmează 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 multiperspective (MPIC), asa cum se specifică la punctul 3.2.2.9.
Această metodă NU este adecvată pentru validarea numelor de domenii wildcard.

3.2.2.4.20 TLS Folosind ALPN

Această metodă de validare a domeniului nu este utilizată.

3.2.2.5 Autentificare pentru o adresă IP

Niciun certificat autentificat prin adresă IP nu este emis în temeiul acestui CPP.

3.2.2.6 Validarea domeniului wildcard

Înainte de a emite un certificat cu un caracter wildcard (*) într-un CN sau subjectAltName de tip DNS-ID, RA stabilește și urmează o procedură documentată care determină dacă caracterul wildcard apare în prima poziție a etichetei în stânga unui „registry-controlled”sau„ sufix public ”(de ex.„ * .com ”„ * .co.uk ”, vezi RFC 6454 Secțiunea 8.2 pentru explicații suplimentare). Dacă un wildcard se află în interiorul etichetei, imediat în stânga unui sufix controlat de registru sau public, RA refuză emiterea, cu excepția cazului în care solicitantul dovedește controlul său legitim asupra întregului spațiu de nume de domeniu.

3.2.2.7 Precizia sursei de date

Înainte de a utiliza orice sursă de date ca sursă de date fiabilă, certSIGN evaluează sursa pentru fiabilitatea, acuratețea și rezistența la alterare sau falsificare. certSIGN ia în considerare următoarele în timpul evaluării sale:

1. Vârsta informațiilor furnizate,
2. Frecvența actualizărilor sursei de informații,
3. Furnizorul de date și scopul colectării datelor,
4. Accesibilitatea publică și disponibilitatea datelor și
5. Dificultatea relativă în falsificarea sau modificarea datelor.

3.2.2.8 Înregistrările Autorității de Autentificare și Certificare (CAA)

RA verifică înregistrările CAA și urmează instrucțiunile de procesare găsite, pentru fiecare dNSName din extensia subjectAltName a certificatului care urmează să fie eliberat, așa cum se specifică în RFC 8659. Când procesează înregistrările CAA, certSIGN procesează problema, issuewild și etichetele de proprietate iodef, după cum se specifică în RFC 8659. certSIGN respectă marcarea critică și nu emite un certificat dacă întâmpină o etichetă de proprietate nerecunoscută cu acest set de semnalizare. certSIGN tratează un set de înregistrări de resurse CAA care nu conține etichete de proprietate problemă (și, de asemenea, nu conține etichete

de proprietate issuewild atunci când se efectuează procesarea CAA pentru un nume de domeniu wildcard) ca permisiune de emitere, cu condiția să nu existe înregistrări în Setul de înregistrări a resurselor, în caz contrar interzice emiterea. certSIGN nu va emite un certificat decât dacă cererea este consistentă cu Setul de înregistrări a resurselor aplicabil.

Dacă există o înregistrare CAA, atunci trebuie să enumere certSIGN ca CA autorizat. Înregistrarea permisă este certsign.ro. Emiterea se încadrează în TTL al înregistrării CAA sau în 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 va implementat MPIC utilizând cel puțin două (2) perspective de rețea la distanță.

3.2.3 Autentificarea identității individuale

certSIGN nu eliberează certificate SSL persoanelor fizice.

3.2.4 Informații despre beneficiar ne-verificate

Toate informațiile furnizate de către beneficiarul certificatului vor fi verificate prin utilizarea unei surse independente de informații sau a unui canal de comunicare alternativ înainte de a fi incluse în certificat.

3.2.5 Validarea autorității

Autentificarea autorizațiilor face parte din procedura efectuată de autoritatea de înregistrare sau de autoritățile de certificare pentru a procesa cererea de certificat pentru o persoană juridică sau pentru un dispozitiv aparținând unei persoane juridice sau fizice. În ambele cazuri, eliberarea certificatului este o confirmare a faptului că o persoană juridică sau un dispozitiv are dreptul de a utiliza cheia privată în numele persoanei juridice.

3.2.6 Criterii de interoperare sau certificare

certSIGN va dezvălui toate certificatele încrucișate care identifică CA ca subiect, cu condiția ca certSIGN să aranjeze sau să accepte stabilirea relației de încredere.

3.3 Identificare și autentificare pentru cereri de re-key

3.3.1 Identificare și autentificare pentru re-key de rutină

Capitolele 4.7 și 4.8 din prezentul document descriu procesul.

3.3.2 Identificare și autentificare pentru re-key după revocare

Se folosește același proces ca și pentru validarea inițială a identității.

3.4 Identificare și autentificare pentru cererea de revocare

Cererile de revocare pot fi trimise prin e-mail direct către emitentul certificatului sau indirect către Autoritatea de înregistrare. De asemenea, solicitările pot fi trimise în alt format decât cel electronic.

- În primul caz, beneficiarul va depune o cerere autentificată de revocare a certificatului. Beneficiarul autentifică solicitarea prin aplicarea unei semnături electronice.
- Beneficiarul nu poate trimite o cerere de revocare electronică și va utiliza o a doua metodă. Cererea de revocare va fi certificată de către autoritatea de înregistrare.

În ambele cazuri, va exista o identificare univocă a identității Beneficiarului. Cererea de revocare poate viza mai multe certificate. Autentificarea și identificarea beneficiarului la Autoritatea de înregistrare se realizează ca în înregistrarea inițială (a se vedea capitolul 3.2). Autentificarea beneficiarului la Autoritatea de certificare constă în verificarea autenticității cererii. Procedura de revocare detaliată este descrisă în capitolul 4.9.
Următoarele entități pot trimite cereri de revocare a certificatului:

- Subiectul care deține cheia privată asociată cu cheia publică din certificat
- Beneficiarul care încheie un acord contractual cu certSIGN pentru eliberarea certificatelor către subiecți
- Autoritatea de înregistrare care poate solicita revocarea fie în numele unui subiect, fie dacă are informații care justifică revocarea certificatului, prin crearea unei cereri autentificate utilizând mecanismele de securitate ale software-ului Autorității de înregistrare
- Roluri de încredere asociate certSIGN SSL DV CA Clasa 3 G2, sub supravegherea Comitetului de Management a Politicilor și Procedurilor (PPMB), prin crearea unei cereri autentificate utilizând mecanismele de securitate ale software-ului Autorității de certificare

4 Cerințele operaționale pentru ciclul de viață al certificatului

Acest capitol descrie procedurile de bază care sunt comune tuturor tipurilor de certificate emise de certSIGN SSL DV CA Clasa 3 G2.
Procedurile detaliate legate de serviciile componente PKI (CA, RA, semnatarii CRL-urilor, răspunsul OCSP etc.) și persoanele / rolurile implicate în procesul operațional al acestor componente sunt descrise în documentația internă confidențială.
certSIGN oferă acces la următoarele servicii:

a. Înregistrare, certificare, rekey;
b. Revocarea certificatului;
c. Verificarea validității certificatului.

4.1 Cererea de certificat

4.1.1 Cine poate depune o cerere de certificat

certSIGN menține o bază de date internă cu toate certificatele revocate anterior și solicitările de certificate respinse anterior din cauza suspectării de phishing sau a altor utilizări sau preocupări frauduloase. certSIGN folosește aceste informații pentru a identifica solicitările ulterioare de certificate suspecte.

Cerere de certificat de către persoane fizice
certSIGN emite certificate:

- Persoanelor fizice, în cazul în care solicită pentru ele însuși certificatul
- Persoanelor fizice (subiecților) pentru care Beneficiarul solicită certificatul, având un acord juridic obligatoriu sau acționând ca angajator al acestuia.

Beneficiarul și subiectul trebuie să respecte prevederile și obligațiile stabilite în formularul de înregistrare, în contractul de beneficiar aplicabil și în Termenii și condițiile privind serviciile de certificare care încorporează acest CPP și Declarațiile publice PKI.
Autoritatea de certificare emite certificate doar ca răspuns la o cerere autentificată din partea Autorității de înregistrare operată de certSIGN sau de o terță parte delegată, dacă legislația permite acest lucru.
certSIGN arhivează informațiile legate de înscriere. Arhiva este întreținută în conformitate cu cerințele definite în CPP și legislația aplicabilă.

Cerere de certificat de către persoane juridice (organizații)
Subiectul trebuie să respecte prevederile și obligațiile stabilite în formularul de înregistrare, în Acordul de beneficiar aplicabil și în Termenii și condițiile privind serviciile de certificare care încorporează acest CPP.

Autoritatea de certificare emite certificate numai ca răspuns la o cerere autentificată din partea Autorității de înregistrare.
certSIGN arhivează informațiile legate de înscriere. Arhiva este întreținută în conformitate cu cerințele definite în CPP și legislația aplicabilă.

4.1.2 Procesul de înregistrare și responsabilitățile

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

Înainte de eliberarea unui certificat, certSIGN obține următoarea documentație de la beneficiar:

1. O cerere de certificat, care poate fi electronică; și
2. Un contract de beneficiar finalizat sau Termeni de utilizare, care pot fi electronici.

certSIGN oferă supraveghere, asistență și audit pentru toate procesele și serviciile RA. RA este responsabilă pentru verificarea următoarelor elemente:

- Cererea de emitere certificat
- Controlul asupra domeniilor pentru care solicită certificat

Procesul de înregistrare se realizează în conformitate cu regulile și metodele descrise în prezentul CPP și în ghidurile și procedurile interne ale RA și legea aplicabilă.
Beneficiarului i se furnizează următoarele informații care fac parte din Contract:

- Formularul de înregistrare
- Adresa online pentru Termenii și condițiile certificatului
- Adresa online pentru CPP
- Statute, avize sau alte documente furnizate de subiect (care urmează să fie definite în contractul de beneficiar)

Prin depunerea unei cereri de emitere Beneficiarul acceptă formal contractul și următoarele:

- Responsabilitatea sa că informațiile furnizate la RA sunt corecte, complete, valabile și actualizate,
- Că certSIGN menține o perioadă de păstrare de 10 ani de la data certificatului emis pentru toate informațiile referitoare la înregistrare și înscriere, cererea de certificat, revocarea certificatului
- Că, în cazul în care certSIGN (ca CA și/sau RA) își încetează activitățile, aceste date pot fi transferate către o terță parte, respectând termenii și condiții de utilizare,
- Recunoaște drepturile, obligațiile și responsabilitățile certSIGN și ale celorlalți participanți la PKI, astfel cum sunt definite în CPP și de legislația națională;
- Că Beneficiarul are obligația de a informa certSIGN cu privire la orice schimbări sau evenimente care pot afecta valabilitatea sau conținutul certificatului

Procesul de înregistrare
Procesul de înregistrare începe la RA.

Operatorul RA face verificarea cererii de certificat.

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 datelor și pentru furnizarea către CA a conținutului corect pentru câmpurile variabile din certificat.

4.2 Procesarea cererii de certificat

Solicitările pot fi trimise on-line.

Cererea de certificat este completată în format electronic:

- Formularul de solicitare (primit prin e-mail sau de pe site-ul web www.certsign.ro) este semnat electronic cu un certificat digital calificat valid (nu revocat sau expirat) emis de certSIGN și trimis la Autoritatea de certificare prin e-mail sau
- Cererea de certificat poate fi completată și plasată pe site-ul https:// shop.certsign.ro

- Cererea de certificat completată în format electronic este trimisă printr-un canal autentificat.

RA verifică înregistrările CAA și urmează instrucțiunile de procesare găsite, pentru fiecare dNSName în extensia subjectAltName a certificatului care urmează a fi emis, conform specificațiilor RFC 6844 modificate prin Errata 5065 (Anexa A). certSIGN nu va emite un certificat decât dacă cererea de certificat este in concordanță cu setul de înregistrări CAA aplicabil.
Dacă există înregistrare 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 efectuează identificarea și autentificarea în conformitate cu procedura definită în capitolul 3.2. și în cadrul documentației confidențiale interne.
RA colectează informațiile de identitate ale Beneficiarului.
Cererea de certificat cu risc ridicat este o cerere pe care CA o semnalează pentru control suplimentar prin referire la criteriile interne și bazele de date menținute de CA, care pot include nume cu risc mai mare de phishing sau alte utilizări frauduloase, nume cuprinse în cereri de certificate respinse anterior sau certificate revocate, nume listate pe lista de phishing-uri Miller Smiles sau pe lista de navigare sigură Google sau nume pe care CA le identifică folosindu-și propriile criterii de atenuare a riscului.

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

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

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

4.2.2 Aprobarea sau respingerea cererilor de certificat

Aprobarea sau respingerea cererilor de certificat este efectuată 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 SSL DV CA Clasa 3 G2 sau din alte motive, la discreția și sub responsabilitatea al RA.

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

4.2.3 Timpul de procesare a cererilor de certificat

certSIGN nu emite certificate imediat după înregistrare. Certificatele trebuie emise de Autoritatea de certificare prin aprobarea cererii de certificat după ce a fost validată de RA, prin urmare certificatele nu sunt disponibile imediat Beneficiarului atunci când certificatele sunt emise de CA.

4.3 Emiterea certificatelor

4.3.1 Acțiunile CA în timpul emiterii certificatului

Certificatul este emis de CA numai după ce a primit o cerere de certificat de la RA. CA și RA sunt sisteme integrate și comunică prin conexiuni de rețea închise. CA procesează numai solicitările care provin din RA de încredere a certSIGN.
CA asigură unicitatea fiecărui certificat pe care îl emite utilizând câmpul *certificateSerialNumber* al fiecărui certificat.

4.3.2 Notificarea emiterii certificatului de către CA către beneficiar

Certificatul este emis ca parte a procesului de înregistrare a certificatului. Beneficiarul primește o notificare de eliberare a 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 Conduită care constituie acceptarea certificatului

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 invalide de la data înregistrării,
- Pierderea dreptului Beneficiarului.

Obligațiile Beneficiarului și ale RA în caz de respingere:

- RA solicită revocarea certificatului
- RA execută revocarea certificatului

4.4.2 Publicarea certificatului de către CA

Vezi capitolul 2.

4.4.3 Notificarea emiterii certificatului de către CA către alte entități

Emiterea certificatului este notificată de certSIGN către alte entități prin publicarea certificatului în depozitar, așa cum este descris în capitolul 2.

4.5 Utilizarea perechii de chei și a certificatului

4.5.1 Utilizarea cheii private și a certificatului de către beneficiar

certSIGN emite certificate pentru cheile furnizate de beneficiari în cererile de certificat.

Subiectul este obligat de condițiile și obligațiile menționate în Contractul de beneficiar, care include prezentul CPP. Beneficiarul va proteja cheile și orice date de activare asociate (de exemplu, parolă, cod PIN etc.) sau alte informații împotriva pierderii, furtului, divulgării, compromisului sau modificării.

Beneficiarul este responsabil personal pentru:

- Utilizarea cheilor numai pentru utilizarea intenționată, așa cum este definită în Politica de certificare și codificată în certificate
- Folosirea de instrumente care pot interpreta corect utilizarea cheii ca fiind codificate în certificat și care respectă condițiile de utilizare a cheii
- Setarea datelor de activare care sunt unice și care sunt conforme cu liniile directoare date în politica de certificare
- Păstrarea confidențială a acestor informații secrete
- Stocarea sigură a oricărui document sau suport care conține transcrieri ale unei părți sau a tuturor datelor de activare asociate
- Nedivulgarea datelor de activare unei alte persoane
- Instalarea certificatului numai pe serverele care sunt accesibile la subiectul (numele) enumerat (e) în certificat și utilizarea certificatului numai în conformitate cu toate legile aplicabile și numai în conformitate cu Acordul beneficiarului sau cu Termenii și condițiile

4.5.2 Utilizarea cheii publice și a certificatului de entități partenere

certSIGN presupune că toate software-urile utilizatorului vor fi conforme cu X.509, protocolul SSL / TLS și alte standarde aplicabile care aplică cerințele generale și cerințele stabilite în acest CPP. certSIGN nu garantează că software-ul unei terțe părți va sprijini sau impune astfel de controale sau cerințe, iar tuturor părților dependente li se recomandă să solicite consiliere tehnică sau juridică adecvată.

Subiecții vor utiliza cheia privată și certificatele:

- În conformitate cu scopul menționat în prezentul CPP și în conformitate cu conținutul certificatului (câmpurile *keyUsage* și *ExtendedKeyUsage*),
- În conformitate cu prevederile acordului dintre Beneficiar și certSIGN,
- Numai în perioada de valabilitate,

Părțile implicate vor utiliza cheile și certificatele publice:

- În conformitate cu scopul declarat în prezentul CPP și în conformitate cu conținutul certificatului (câmpurile *keyUsage* și *ExtendedKeyUsage*),
- În conformitate cu prevederile acordului dintre Beneficiar și certSIGN,
- Numai după verificarea stării lor și verificarea semnăturii Autorității de certificare care a emis certificatul respectiv.

Bazându-se pe o sesiune SSL / TLS care nu poate fi verificată pot rezulta riscuri pe care partea care se bazează le asumă în totalitate și pe care certSIGN nu le asumă în niciun fel.

4.6 Reînnoirea certificatului

4.6.1 Circumstanțe pentru reînnoirea certificatului

Fără stipulare.

4.6.2 Cine poate solicita reînnoirea
Fără stipulare.
4.6.3 Procesarea cererilor de reînnoire a certificatului
Fără stipulare.
4.6.4 Notificarea emiterii de certificate noi către beneficiar
Fără stipulare.
4.6.5 Conduita care constituie acceptarea unui certificat de reînnoire
Fără stipulare.
4.6.6 Publicarea certificatului de reînnoire de către CA
Fără stipulare.
4.6.7 Notificarea emiterii certificatului de către CA către alte entități
Fără stipulare.

4.7 Certificat Re-Key

4.7.1 Circumstanțe pentru certificate re-key
certSIGN efectuează rekey-ul certificatelor pentru certificatele digitale valabile (nu expirate și nu revocate) emise de certSIGN, care nu necesită modificări ale datelor certificatului sau extensii. Procesul de rekey constă în retransmiterea unui certificat cu o nouă pereche de chei pentru a prelungi data de expirare a acestuia, fără a modifica identitatea sau alte extensii ale certificatului.

4.7.2 Cine poate solicita certificarea unei noi chei publice
certSIGN informează întotdeauna subiecții (cu cel puțin 30 de zile înainte) despre apropierea perioadei de expirare.

Rekey se realizează atunci când un subiect care deține un certificat digital valid (nu revocat și nu expirat) generează o nouă pereche de chei și solicită emiterea unui nou certificat pentru a confirma deținerea unei noi chei publice create.
Rekey-ul certificatului se efectuează numai la cererea subiectului și va fi precedat de depunerea unei cereri pe un formular corespunzător completat de beneficiar / subiect.
4.7.3 Procesarea cererilor de re-key a certificatului
Procesul cererii inițiale de certificat va fi modificat după cum urmează:

- Identificarea solicitantului și rezultatele validării din cererile anterioare sunt considerate valide cât timp informațiile validate nu s-au modificat și acele informații sunt obținute dintr-o sursă specificată în secțiunea 3.2 cu cel mult douăsprezece (12) luni înainte de eliberarea certificatului.
- Orice date care s-au modificat trebuie să fie validate ca și cum ar fi o cerere nouă.

4.7.4 Notificarea emiterii de certificate re-key către beneficiar
RA utilizează aceleași procese de notificare ca și pentru un certificat nou solicitat.

4.7.5 Conduita care constituie acceptarea unui certificat 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 re-key de către CA către alte entități
RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.8 Modificarea certificatului
certSIGN nu modifică certificatele emise.
Subiectul sau Beneficiarul, după caz, vor solicita certSIGN să revoce certificatul de îndată ce informațiile incluse în certificat nu mai sunt conforme cu realitatea.

4.8.1 Circumstanța pentru modificarea certificatului
Fără stipulare.

4.8.2 Cine poate solicita modificarea certificatului
Fără stipulare.

4.8.3 Procesarea cererilor de modificare a certificatului
Fără stipulare.

4.8.4 Notificarea emiterii de certificate modificate către beneficiar
Fără stipulare.

4.8.5 Conduită care constituie acceptarea certificatului modificat
Fără stipulare.

4.8.6 Publicarea certificatului modificat de către CA
Fără stipulare.

4.8.7 Notificarea eliberării certificatului modificat de către CA către alte entități
Fără stipulare.

4.9 Revocarea și suspendarea certificatului
Certificatele emise de certSIGN SSL DV CA Clasa 3 G2 pot fi revocate, dar nu sunt niciodată suspendate. Revocarea certificatului este ireversibilă.

Revocarea nu afectează nici tranzacțiile efectuate înainte de revocare, nici obligațiile care rezultă din urmarea prezentului CPP.
Acest capitol precizează condițiile necesare pentru ca o autoritate de certificare să aibă motive pentru revocarea certificatului.

Dacă o cheie privată corespunzătoare unei chei publice conținute într-un certificat revocat rămâne sub controlul subiectului, după revocare ar trebui să fie stocată în siguranță până când este distrusă.
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 Circumstanțe de revocare
Certificatul este revocat în termen de 24 de ore când:
1. Beneficiarul solicită în scris, fără a preciza un motiv, ca CA să revoce un certificat (CRLReason "nespecificat (0)", ceea ce înseamnă că nu se adaugă niciun reasonCode în CRL);
2. Beneficiarul notifică CA că cererea inițială de certificat nu a fost autorizată și nu acordă retroactiv autorizația (CRLReason #9, privilegeWithdrawn);
3. CA obține dovezi că cheia privată a Beneficiarului care corespunde cheii publice din certificat a suferit o compromitere a cheii (CRLReason #1, keyCompromise);

4. CA are cunoștință de o metodă demonstrată sau dovedită care poate calcula cu ușurință cheia de securitate privată a abonaților pe baza cheii publice din certificat (cum ar fi o metodă de calcul a cheii private Debian slabă, a se vedea https://wiki.debian.org/SSLkeys) (CRLReason #1, keyComprompromise);
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).

Certificatul este revocat în termen de 5 zile în cazul în care are loc una sau mai multe dintre 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).

Cheia privată compromisă înseamnă:
(1) acces neautorizat la cheia privată sau un motiv puternic care determină să se creadă așa ceva,

(2) pierderea cheii private sau apariția unui motiv pentru a suspecta o astfel de pierdere,
(3) cheie privată furată sau apariția unui motiv pentru a suspecta un astfel de jaf,
(4) ștergerea accidentală a cheii private.

4.9.2 Cine poate solicita revocarea

Următoarele entități pot trimite cereri de revocare a certificatului:

- Beneficiarul care deține cheia privată asociată cu cheia publică din certificat
- Autoritatea de înregistrare care poate solicita revocarea fie în numele unui subiect, fie dacă are informații care justifică revocarea certificatului
- Roluri de încredere asociate certSIGN SSL DV CA Clasa 3 G2, sub supravegherea Comitetului de Management a Politicilor și Procedurilor (PPMB)

Furnizorii de software pentru aplicații și alte terțe părți pot trimite rapoarte privind problema certificatului informând certSIGN cu privire la o cauză rezonabilă de revocare a certificatului.
Cererea de revocare poate viza mai multe certificate.

4.9.3 Procedura cererii de revocare

CA menține o capacitate continuă 24x7 de a accepta și de a răspunde cererilor de revocare și solicitărilor aferente.

Procedurile de revocare sunt descrise în secțiunea 3.4 din prezentul CPP.
Motivul revocării poate fi doar unul dintre cele specificate la cap. 7.2.
Dacă certSIGN constată că revocarea este adecvată, personalul certSIGN revocă certificatul și actualizează CRL.

4.9.4 Perioada de grație a cererii de revocare

certSIGN efectuează revocarea pe baza best efort, pentru a se asigura că timpul necesar procesării cererii de revocare și pentru publicarea notificării de revocare (CRL actualizat) este cât mai redus posibil.

4.9.5 Timpul în care CA trebuie să proceseze cererea de revocare

certSIGN garantează o perioadă maximă de 24 de ore pentru procesarea unei cereri de revocare a certificatului.
CA decide dacă revocarea sau altă acțiune adecvată este justificată pe baza cel puțin următoarelor criterii:

1. Natura presupusei probleme;
2. Numărul de rapoarte de probleme de certificat primite despre un anumit certificat sau beneficiar; 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 va avea mai multă greutate decât o reclamație a unui consumator care susține că nu a primit bunurile pe care le-a comandat); și
3. Legislație relevantă.

Informațiile referitoare la revocarea certificatului sunt stocate în baza de date certSIGN.
Certificatele revocate sunt plasate în Lista de revocare a certificatelor (CRL) în conformitate cu frecvența de emitere a CRL.
Ca o excepție, în caz de dezastru, dacă cererea de revocare nu poate fi confirmată în termen de 24 de ore, certSIGN nu va revoca certificatul. si va stoca motivele..

4.9.6 Cerințe de verificare a revocării pentru entitățile partenere

Părțile implicate vor utiliza toate resursele furnizate de certSIGN (CRL, OCSP) pentru a verifica starea unui certificat înainte de a se baza pe acesta.

4.9.7 Frecvența emiterii CRL

O nouă CRL este publicată în depozit după fiecare revocare a certificatului, în maximum o zi. Dacă compromiterea cheii este motivul revocării, noul CRL este emis imediat după procesarea cererii de revocare. Perioada de disponibilitate a CRL este de 48 de ore și este actualizată zilnic.

4.9.8 Latență maximă pentru CRL-uri

CRL-ul acestei autorități de certificare și a tuturor autorităților sale de emitere subordonate este emis în conformitate cu capitolul 4.9.7 și publicat fără întârziere.

4.9.9 Disponibilitatea verificării on-line a revocării/stării

Răspunsurile OCSP sunt semnate de un răspuns OCSP al cărui certificat este semnat de CA care a emis certificatul a cărui stare de revocare este verificată.

Certificatul de semnare OCSP conține o extensie de tip id-pkix-ocsp-nocheck, așa cum este definită de RFC6960.CA acceptă o capacitate OCSP utilizând metoda GET pentru certificatele emise în conformitate cu cerințele CA/B Forum Baseline Requirements.

Pentru starea certificatelor de beneficiar, CA actualizează informațiile furnizate printr-un protocol de stare a certificatului online (OCSP -Online Certificate Status Protocol) listate, la fiecare oră. Răspunsurile OCSP de la acest serviciu au un timp de expirare maxim de 24 de ore.

Pentru statutul certificatelor CA Intermediare:

CA actualizează informațiile furnizate printr-un protocol de stare a certificatului online (OCSP) cel puțin:

- La fiecare douăsprezece luni și
- În termen de 24 de ore de la revocarea unui certificat CA Intermediar.

Dacă răspunsul OCSP primește o cerere pentru statutul unui certificat care nu a fost emis, atunci respondentul nu răspunde cu un status „ good” pentru astfel de certificate.

certSIGN monitorizează răspunsul OCSP pentru cererile de numere de serie "neutilizate" ca parte a procedurilor sale de răspuns de securitate.
Responderul OCSP oferă răspunsuri definitive cu privire la numerele de serie ale certificatelor "rezervate", ca și cum ar exista un certificat care să corespundă precertificatului [RFC6962]. Un număr de serie de certificat în cadrul unei cereri OCSP reprezintă una dintre următoarele trei opțiuni:
1. "assigned " dacă un certificat cu acel număr de serie a fost emis de către CA emitentă, utilizând orice cheie curentă sau anterioară asociată cu acel subiect CA; sau
2. " reserved " dacă un precertificat [RFC6962] cu acest număr de serie a fost emis de către
   (a) CA emitentă; sau
   (b) un certificat de semnare a precertificatului [RFC6962] asociat cu CA emitentă;
3. " unused " dacă nu este îndeplinită niciuna dintre condițiile anterioare.

4.9.10 Cerințe de verificare a revocării on-line
No stipulation.

4.9.11 Alte forme de anunțare a revocării disponibile
Fără stipulare.

4.9.12 Cerințe speciale legate de compromisul cheii

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

- Încetează imediat utilizarea certificatului,
- Începe imediat revocarea certificatului,
- Șterge certificatul de pe toate dispozitivele și sistemele,
- Informează toate părțile dependente de acest certificat.

Compromisul cheii private poate avea implicații asupra informațiilor protejate cu această cheie. Subiectul va decide cum să trateze 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 de suspendare
Fără stipulare

4.9.14 Cine poate solicita suspendarea
Fără stipulare

4.9.15 Procedura cererii de suspendare
Fără stipulare

4.9.16 Limite pentru perioada de suspendare
Fără stipulare

4.10 Servicii de stare a certificatului

4.10.1 Caracteristici operaționale
Serviciile de stare a certificatului certSIGN sunt CRL și OCSP. Accesul la aceste servicii se face prin intermediul site-ului web „www.certsign.ro” și „ocsp.certsign.ro”. Serviciile de stare a certificatului furnizează informații despre starea certificatelor valide. Integritatea și autenticitatea informațiilor de stare sunt protejate printr-o semnătură digitală a CA-ului respectiv.
Intrările de revocare dintr-un răspuns CRL sau OCSP nu sunt niciodată eliminate.

4.10.2 Disponibilitatea serviciului
Serviciile de certificare sunt disponibile 24 de ore pe zi, 7 zile pe săptămână.

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

CA operează și își menține capacitatea CRL și OCSP cu resurse suficiente pentru a asigura un timp de răspuns de zece secunde sau mai puțin în condiții normale de funcționare.

4.10.3 Caracteristici opționale
Serviciile de stare a certificatului certSIGN nu includ și nu necesită funcții suplimentare.

4.11 Încetarea abonamentului
Încetarea abonamentului are loc după:

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

Din motive de conformitate legală, certSIGN și toate autoritățile de înregistrare păstrează toate datele și documentația subiectului pentru o perioadă de 10 ani de la încetarea unui abonament.

4.12 Custodie și recuperare chei
certSIGN nu permite custodia cheii (key-escrow) pentru certificatele SSL.

4.12.1 Politica și practicile esențiale pentru custodie și recuperare
Fără stipulare.

4.12.2 Politica și practicile privind încapsularea și recuperarea cheilor de sesiune
Fără stipulare.

5 Facilități, management și controale operaționale
În calitate de furnizor de servicii de certificare, certSIGN plasează securitatea în centrul activităților sale. Pentru a se asigura că toate activele, activitățile și serviciile sale sunt sigure, certSIGN a implementat, întreține și îmbunătățește continuu un sistem de management al securității informațiilor certificate ISO 27001: 2013. În conformitate cu cerințele acestui cadru de securitate, toate activitățile de securitate încep cu o evaluare a riscurilor pentru a identifica și clasifica toate activele informaționale, pentru a evalua riscurile la care sunt expuși și pentru a determina controalele tehnice, manageriale, organizatorice și procedurale necesare. certSIGN menține un inventar al tuturor activelor informaționale și le atribuie o clasificare conformă cu evaluarea riscurilor.

Toate acele controale legate de activele și activitățile CA și RA sunt conforme cu cerințele aplicabile din următoarele standarde:

- ETSI EN 319 401, Cerințe politice generale pentru furnizorii de servicii de încredere
- ETSI EN 319 411-1, Politici și cerințe de securitate pentru furnizorii de servicii de încredere care emit certificate; Partea 1: Cerințe generale
- Cerințe ale forumului CA/B Forum Baseline Requirements
- 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

Sistemul computerizat de rețea, terminalele operatorului și resursele informaționale ale certSIGN sunt situate în zone dedicate, protejate fizic împotriva accesului neautorizat, distrugerii sau întreruperii funcționării acestora. Aceste locații sunt monitorizate. Fiecare intrare și ieșire, precum și fluctuațiile de putere, sunt înregistrate în jurnalul de evenimente (jurnalele de sistem). Temperatura și umiditatea sunt monitorizate și controlate.

5.1.1 Amplasarea și construcția sediului

certSIGN CA se află în București, România, la următoarea adresă: Bulevardul Tudor Vladimirescu nr. 29A, AFI Tech Park 1, București, România.

Toate operațiunile certSIGN CA și RA se desfășoară într-un mediu protejat fizic, cu controale bazate pe evaluarea riscurilor care sunt menite să descurajeze, să prevină, să detecteze și să contracareze materializarea riscurilor asupra activelor sale. De asemenea, menținem facilități de recuperare în caz de dezastru pentru operațiunile noastre CA și RA, facilități care sunt protejate de controale de securitate fizică similare cu cele implementate la instalația noastră principală. Toate controalele de securitate fizică implementate de certSIGN sunt conforme cu standardele ISO 27001 și 27002 și sunt descrise în detaliu în politicile și procedurile de securitate. Unele dintre cele mai importante controale de securitate sunt:

- Un perimetru clar definit și protejat prin care sunt monitorizate toate intrările și ieșirile;
- Componentele critice sunt protejate cu mai multe perimetre
- Un sistem de control al accesului configurat pentru a permite accesul numai acelor indivizi autorizați în mod corespunzător și autorizați în mod specific să intre în zonă;
- Monitorizare electronică controlată pentru intruziuni neautorizate în orice moment;
- Personalul care nu se află pe lista de acces este însoțit și supravegheat corespunzător;
- Un jurnal de acces la site este menținut și inspectat periodic;

Fiecare echipament este întreținut corect pentru a asigura disponibilitatea și integritatea sa continuă.

5.1.2 Acces fizic

Accesul fizic este controlat și monitorizat de un sistem de alarmă integrat. Sistemul de prevenire a incendiilor, sistemul de detectare a intruziunilor și sistemul de alimentare de urgență sunt instalate.

Programul de lucru certSIGN este de luni până vineri între orele 9.00 și 18.00. În afara acestui interval de timp, inclusiv de sărbătorile legale, accesul la sediul certSIGN este permis numai persoanelor autorizate de conducerea certSIGN.

Vizitatorii sunt însoțiți permanent de personalul autorizat.

Spațiile certSIGN sunt împărțite în:

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

Zonele IT sunt echipate cu un sistem de securitate monitorizat construit pe bază de mișcare, intruziune și foc. Accesul în această zonă este acordat numai personalului autorizat. Monitorizarea drepturilor de acces se realizează pe baza cardurilor electronice și a cititoarelor corespunzătoare, montate lângă zona de intrare. Fiecare intrare și ieșire din zonă este înregistrată automat în jurnalul de evenimente.

Accesul în zona operatorilor este permis numai pe baza unui card electronic și a cititorului corespunzător al acestuia. Deoarece toate informațiile sensibile sunt protejate prin utilizarea dulapurilor securizate, în timp ce accesul la terminalul operatorului sau al administratorului necesită autorizare prealabilă, securitatea fizică implementată este considerată adecvată.

Cheile din zonă sunt accesibile numai personalului autorizat. Zona poate fi ocupată exclusiv de personalul certSIGN și de persoane autorizate, acestora din urmă urmând să li se acorde acces doar însoțite.

Persoanele nesupravegheate nu sunt permise în această zonă. Programatorii și dezvoltatorii nu au acces la informații sensibile. Dacă un astfel de acces este necesar, este necesară prezența administratorului de securitate. Proiectele implementate și software-ul lor sunt testate pe mediul de dezvoltare al certSIGN.

5.1.3 Alimentare electrică și aer condiționat

Sistemul de ventilație este disponibil în toate zonele. În zonele serverului, unitățile de aer condiționat sunt redundante și temperatura este monitorizată. Atunci când apar avarii de curent, sursele de alimentare de urgență (UPS) permit activităților să continue până la intervenția automată a generatorului de rezervă în clădire. Infrastructura de energie electrică este concepută astfel încât, dacă se pierde puterea principală a clădirii, toate activitățile pot continua cel puțin 24 de ore folosind generatorul de energie de rezervă. Fiecare server, echipament de rețea și toate computerele angajaților care efectuează activități importante pentru operațiunile CA și RA sunt, de asemenea, conectate la UPS-uri. Componentele principale ale sistemului de protecție fizică de securitate sunt, de asemenea, conectate la UPS-uri și la generatorul de energie de rezervă.

5.1.4 Expunerea la apă

Riscul de inundație în zona serverelor este atenuat prin plasarea tuturor echipamentelor în rafturi la cel puțin 15 cm de nivelul podelei. În plus, toate camerele de date sunt monitorizate de senzori de umiditate.

5.1.5 Prevenirea și protecția împotriva incendiilor

Locația certSIGN beneficiază de un sistem de prevenire și stingere a incendiilor, în conformitate cu standardele și reglementările corespunzătoare din acest domeniu. Ușile camerelor de date sunt certificate ignifug și toate pasajele din pereți sunt sigilate cu substanțe ignifuge.

5.1.6 Stocare media

În conformitate cu cerințele politicii de clasificare a informațiilor, mediile care conțin date sau informații de rezervă sunt manipulate și stocate în siguranță în cadrul instalației principale. Mediile de rezervă sunt, de asemenea, stocate în siguranță într-o locație separată de locația media originală, cu aceeași securitate ca locația principală. Mediile care conțin date sensibile sunt scoase din funcțiune în siguranță atunci când nu mai sunt necesare.

5.1.7 Eliminarea deșeurilor

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

Când nu mai este necesar, HSM-urile vor fi zero-izate pentru a preveni orice posibilitate de reutilizare a cheilor private CA și vor fi returnate la inventarul criptografic.

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

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

5.1.8 Backup off-site

Copiile cardurilor criptografice sunt stocate într-o cutie de valori în afara locației principale certSIGN.

Stocarea în afara locației cuprinde, de asemenea, arhive, copii actuale ale informațiilor procesate de sistem și kituri de instalare ale aplicațiilor certSIGN. Permite recuperarea de urgență a fiecărei funcții certSIGN în termen de 48 de ore în locația de recuperare în caz de dezastru a certSIGN.

5.2 Controale procedurale

5.2.1 Roluri de încredere

Toate rolurile implicate în furnizarea serviciilor de certificare certSIGN sunt atribuite angajaților certSIGN.

Toți angajații certSIGN se angajează sub semnătură să nu aibă interese contradictorii cu certSIGN, să păstreze confidențialitatea informațiilor și să protejeze datele personale.

certSIGN asigură o separare a sarcinilor pentru funcțiile critice, pentru a preveni utilizarea malițioasă de orice persoană, a sistemelor CA, fără detectare.

Securitatea informațiilor procesate de certSIGN și a serviciilor sale este asigurată prin controale procedurale legate de controlul accesului. Astfel, accesul la informații și funcțiile sistemului de aplicații este restricționat în conformitate cu politica de control al accesului. certSIGN gestionează drepturile de acces ale operatorilor, administratorilor și auditorilor de sistem. Administrarea include gestionarea contului de utilizator și modificarea sau eliminarea în timp util a accesului. Sunt furnizate controale de securitate suficiente pentru separarea rolurilor de încredere identificate, inclusiv separarea funcțiilor de administrare și operare a securității. În special, utilizarea programelor de utilitate a sistemului este restricționată și controlată.

certSIGN poate atribui următoarele roluri de încredere uneia sau mai multor persoane:

- **Ofițer de securitate** - Responsabilitatea generală pentru implementarea practicilor și politicilor de securitate.
- **Administrator de sistem** - Autorizat să instaleze, să configureze și să întrețină sistemele de încredere ale Autorității de certificare pentru înregistrare, generare de certificate, furnizarea dispozitivelor subiect și gestionarea revocării. Instalează hardware și sisteme de operare; instalează și configurează echipamentul de rețea.
- **Operator de sistem** - Responsabil pentru operarea sistemelor de încredere ale Autorității de certificare în fiecare zi. Autorizat să efectueze backup și recuperare a sistemului. Are acces la certificatele subiecților; revocă certificatele subiecților; asigură continuitatea copiilor de rezervă și a arhivelor bazelor de date și crearea jurnalelor de sistem; gestionează baze de date; are acces la informații confidențiale despre subiecți / beneficiari, dar nu are permisiunea de a accesa fizic alte resurse ale sistemului; transferă copii de arhivă și copii de rezervă curente la sediul desemnat.
- **Ofițeri de înregistrare**: Responsabil pentru verificarea informațiilor necesare pentru emiterea certificatului și aprobarea cererilor de certificare;
- **Ofițeri de revocare:** Responsabil pentru modificările stării certificatului de funcționare;

- **Auditor de sistem** - Autorizat să acceseze arhivele și jurnalele de audit ale sistemelor de încredere ale Autorității de certificare. Responsabil pentru efectuarea auditului intern, conformitatea unei autorități de certificare cu acest CPP; această responsabilitate se extinde și asupra Autorității de înregistrare, care operează în cadrul certSIGN.

Rolul auditorului nu poate fi combinat cu niciun alt rol în certSIGN. Nicio entitate care a atribuit un alt rol diferit de un auditor nu poate prelua responsabilitățile auditorului.

Angajații sunt desemnați oficial în funcții de încredere de către Comitetul de Management al Politicilor și Procedurilor (PPMB). Principiul „cel mai mic privilegiu" se aplică la atribuirea drepturilor de acces rolurilor de încredere.

5.2.2 Numărul de persoane necesare pentru fiecare sarcină

În cazul în care este necesar un control dual sau multiplu, sunt prezente cel puțin două persoane distincte, cu roluri relevante de încredere, pentru a putea efectua operația.

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

5.2.3 Identificare și autentificare pentru fiecare rol

Fiecare angajat certSIGN care acționează într-un rol de încredere este identificat și autentificat pentru a accesa infrastructura pentru a-și îndeplini rolul prin intermediul acreditării de autentificare de cel puțin 2 factori.

Fiecare cont atribuit:

- este unic și atribuit direct unei anumite persoane,
- nu este împărtășit cu nicio altă persoană,
- este restricționat după funcție (care decurge din rolul îndeplinit de o anumită persoană) pe baza sistemului software certSIGN, a sistemului de operare și a controalelor aplicației.

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

5.2.4 Roluri care necesită separarea atribuțiilor

certSIGN implementează și impune separarea rolurilor și a atribuțiilor pentru rolurile de administrator, operator și auditor pentru a se asigura că aceeași persoană nu poate deține mai multe roluri. Toate aceste roluri au descrieri de posturi, cu competențe specifice și cerințe de experiență, definite din punctul de vedere al rolurilor îndeplinite. Separarea atribuțiilor și principiile minimului privilegiu sunt în vigoare. Sensibilitatea poziției pe baza sarcinilor determină nivelurile de acces, screeningul de fond și instruirea și conștientizarea angajaților.

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

5.3 Controlul personalului

certSIGN se asigură că persoana care își îndeplinește responsabilitățile de serviciu, care decurg din rolul acționat într-o autoritate de certificare sau o autoritate de înregistrare:

- A absolvit cel puțin școala secundară,

- A înțeles și a semnat un acord care descrie rolul său în sistem și responsabilitățile sale corespunzătoare,
- A fost supus unei pregătiri avansate privind gama de obligații și sarcini, asociate cu poziția sa,
- A fost instruit în domeniul protecției datelor cu caracter personal și al protecției informațiilor confidențiale și private,
- A semnat un acord care conține clauze legate de protecția informațiilor sensibile ale certSIGN și confidențialitatea și confidențialitatea datelor Beneficiarului,
- Nu îndeplinește sarcini care pot duce la un conflict de interese între o autoritate de certificare și o autoritate de înregistrare care acționează în numele acesteia.

Rolurile și responsabilitățile de securitate, așa cum se specifică în politica de securitate a informațiilor certSIGN, sunt documentate în fișele postului sau în documentele disponibile tuturor personalului implicat.

5.3.1 Calificări, experiență și cerințe de autorizare

certSIGN se asigură că toți angajații implicați în furnizarea serviciilor de certificare certSIGN sunt verificați înainte de angajare în ceea ce privește calificările, cunoștințele experților, experiențele și autorizațiile necesare și sunt adecvate pentru a li se atribui roluri de încredere și pentru a îndeplini funcția specifică aferentă postului. Personalul managerial deține expertiză și instruire în tehnologia PKI și experiență în managementul securității informațiilor și managementul riscurilor suficient pentru îndeplinirea funcțiilor de management.

5.3.2 Proceduri de verificare a antecedentelor

certSIGN se asigură că verificările relevante sunt efectuate potențialului personal prin intermediul rapoartelor de stare emise de o autoritate competentă, declarații ale terților sau autodeclarații semnate.

5.3.3 Cerințe de instruire

Personalul care îndeplinește roluri și sarcini care decurg din angajarea în certSIGN trebuie să urmeze următoarele instruiri cu privire la:

- Cerințele Codului de Practici și Proceduri,
- Proceduri și controale de securitate utilizate de Autoritatea de certificare și Autoritatea de înregistrare
- Amenințări frecvente la procesul de verificare a informațiilor (inclusiv phishing-ul și alte tactici de inginerie socială) și cerințele CA/B Forum Baseline Requirements
- Responsabilitățile care decurg din rolurile și sarcinile îndeplinite în sistem,

La finalizarea instruirii, participanții semnează un document care confirmă familiarizarea cu Codul de Practici și Proceduri, alte documente relevante și acceptarea restricțiilor și obligațiilor asociate.

CA-ul se asigură că personalul însărcinat cu atribuții de specializare în validare menține un nivel de calificare care îi permite să îndeplinească aceste sarcini în mod satisfăcător. CA documentează că fiecare specialist în validare deține abilitățile cerute de o sarcină înainte de a permite specialistului în validare să îndeplinească acea sarcină. CA solicită tuturor specialiștilor în validare să treacă un examen asigurat de CA cu privire la cerințele de verificare a informațiilor prezentate în CPP și în cerințele CA/B Forum Baseline Requirements.

5.3.4 Frecvența și cerințele reinstruirilor
Instruirile descrise în capitolul 5.3.3 trebuie repetate sau completate întotdeauna în situațiile în care se fac modificări semnificative la operațiunile certSIGN.

5.3.5 Frecvența și secvența de rotație a posturilor
Fără stipulare.

5.3.6 Sancțiuni pentru acțiuni neautorizate
certSIGN va lua măsuri împotriva celor responsabili de încălcarea politicilor sau procedurilor, a acțiunilor neautorizate, a utilizării neautorizate a autorității și a utilizării neautorizate a sistemelor. Aceasta poate include, printre altele, revocarea privilegiilor, acțiuni disciplinare, sancțiuni reglementate de legislația muncii din România, proceduri civile sau penale.

5.3.7 Cerințele contractorului independent
Personalul contractual (servicii externe, dezvoltatori de subsisteme sau aplicații etc.) este supus aceleiași proceduri de verificare ca și angajații certSIGN (a se vedea capitolele 5.3.1, 5.3.2, 5.3.3 și 5.4.1). În plus, atunci când își îndeplinesc sarcina la sediul certSIGN, personalul contractual trebuie să fie escortat de un angajat certSIGN, cu excepția celor care au fost autorizați de ofițerul de securitate și care pot accesa informații clasificate interne sau în conformitate cu legile în vigoare.

5.3.8 Documentația furnizată personalului
certSIGN pune la dispoziția personalului următoarele documente:

- CPP,
- Lista responsabilităților și obligațiilor asociate cu rolul acționat în sistem
- Politici și proceduri de securitate

Alte documente relevante (proceduri operaționale, instrucțiuni de lucru, manuale) necesare personalului pentru a-și îndeplini funcțiile specifice de serviciu legate de furnizarea serviciilor de certificare certSIGN sunt distribuite în cursul formării inițiale, al instruirilor anuale și ori de câte ori este altfel adecvat.

5.4 Proceduri de înregistrare a datelor de audit
Pentru a gestiona eficient sistemele și aplicațiile utilizate de certSIGN în activitatea sa de furnizor de servicii de certificate, dar și pentru a audita acțiunile angajaților și clienților, sunt înregistrate toate informațiile despre evenimente importante, specifice generate de sisteme și aplicații. Informațiile respective, cunoscute în mod colectiv ca jurnale, sunt păstrate în așa fel încât să poată fi accesate de părțile creditoare, de auditori și de autoritățile statului în orice moment în care au nevoie de ele, pentru a furniza dovezi ale funcționării corecte a serviciilor în scopul legal proceduri sau pentru a detecta încercări de a compromite securitatea certSIGN. Evenimentele înregistrate sunt salvate și păstrate într-o locație secundară.

Ori de câte ori este posibil, jurnalele sunt create automat. Dacă acest lucru nu este posibil, vor fi utilizate jurnale pe hârtie. Fiecare înregistrare dintr-un jurnal creat automat sau manual este păstrată sau dezvăluită în timpul unui audit, dacă este necesar. Acuratețea timpului 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). Ora utilizată pentru înregistrarea evenimentelor necesare în jurnalul de audit este sincronizată cu UTC cel puțin o dată pe zi.

5.4.1 Tipuri de evenimente înregistrate

Fiecare activitate critică din punctul de vedere al securității certSIGN este înregistrată în jurnalele de evenimente și arhivată. Arhivele sunt stocate pe suporturi de stocare care nu pot fi șterse sau distruse cu ușurință (cu excepția cazului în care sunt transferate în mod fiabil pe suporturi pe termen lung) în perioada de timp în care trebuie să fie păstrate. Jurnalele de evenimente certSIGN conțin înregistrări ale tuturor activităților generate de componentele software din sistem. Aceste înregistrări sunt împărțite în trei categorii distincte:

- **Jurnale de sistem** - să conțină informații despre solicitările clientului și răspunsurile serverului (sau invers) la nivelul protocolului de rețea (de exemplu http, https); datele înregistrate sunt: adresa IP a stației sau serverului, operațiuni efectuate (de exemplu: căutare, editare, scriere etc.) și rezultatele acestora (de exemplu, introducerea cu succes a unei înregistrări în baza de date),
- **Erori** - conțin informații despre erori la nivelul protocoalelor de rețea și la nivelul modulelor aplicațiilor;
- **Jurnale de Audit** - conțin informații specifice serviciilor de certificare, de exemplu: cerere de înregistrare și certificare, cerere rekey, acceptare certificat, eliberare certificat și CRL etc.

Jurnalele de mai sus sunt comune fiecărei componente instalate pe un server sau pe o stație de lucru și au o capacitate predefinită. Când această capacitate este depășită, se creează automat o versiune de jurnal. Jurnalul anterior este arhivat și șters de pe disc.

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

CA înregistrează cel puțin următoarele evenimente:
1. Evenimentele legate de ciclul de viață al certificatelor și cheilor CA, inclusiv:
   - generarea, salvarea, stocarea, recuperarea, arhivarea și distrugerea cheilor;
   - cereri de certificate, reînnoire și cereri de recheie și revocare;
   - aprobarea și respingerea cererilor de certificate;
   - evenimente de gestionare a ciclului de viață al dispozitivelor criptografice;
   - generarea listelor de revocare a certificatelor;
   - Semnarea răspunsurilor OCSP

Introducerea de noi profiluri de certificat și retragerea profilurilor de certificat existente.2. Evenimentele de gestionare a ciclului de viață al certificatului de abonat, inclusiv:
   - Cereri de certificate, reînnoire și cereri de rechemare și revocare;
   - toate activitățile de verificare prevăzute în prezentele cerințe și în Declarația privind practicile de certificare ale CA;
   - aprobarea și respingerea cererilor de certificate;
   - emiterea de certificate;
   - generarea listelor de revocare a certificatelor;
   - semnarea răspunsurilor OCSP.
3. Evenimente de securitate, inclusiv:
   - încercări reușite și nereușite de acces la sistemul PKI;

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

Fiecare înregistrare automată sau manuală conține următoarele informații:

- Tip de eveniment,
- Identificatorul evenimentului,
- Data și ora evenimentului,
- Identificatorul persoanei responsabile cu evenimentul.

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 (e) de solicitant pentru a susține înregistrarea;
- Înregistrarea datelor unice de identificare, a numerelor sau a unei combinații a acestora (de exemplu, carte de identitate a solicitantului sau pașaport) a documentelor de identificare, dacă este cazul;
- Locația de stocare a copiilor cererilor și a documentelor de identificare, inclusiv a contractului de subiect / beneficiar semnat
- Orice opțiuni specifice din acordul subiectului / beneficiarului (de exemplu, consimțământul publicării certificatului)
- Identitatea entității care acceptă cererea;
- Metoda utilizată pentru validarea documentelor de identificare,

Accesul la jurnale este permis exclusiv ofițerului de securitate, personalului desemnat special și auditorilor, prin cerere adresata pe email sau in format hartie catre CISO.

Confidențialitatea informațiilor despre subiect este menținută.

5.4.2 Frecvența procesării jurnalelor

Jurnalele sunt procesate continuu și / sau în urma oricărei alarme sau evenimente anormale. Jurnalele sunt arhivate și copiate în mod regulat.

5.4.3 Perioada de păstrare a jurnalelor de audit

Înregistrările evenimentelor sunt stocate în fișiere pe discul de sistem până când ating capacitatea maximă permisă. În acest timp, acestea sunt disponibile on-line, la cererea fiecărei persoane autorizate sau proces. După depășirea capacității permise, jurnalele sunt păstrate ca arhive și pot fi accesate exclusiv off-line, de la o anumită stație de lucru.

Jurnalele arhivate ale jurnalelor sunt păstrate cel puțin 10 ani.

5.4.4 Protecția jurnalului de audit

Fișierele jurnal sunt protejate corespunzător de un mecanism de control al accesului. Este implementată o protecție adecvată împotriva modificării și ștergerii jurnalelor de audit, astfel încât nimeni să nu poată modifica sau șterge înregistrările de audit decât după transferul pe suportul de stocare pe termen lung în scopul arhivării. Numai ofițerul de securitate, personalul desemnat special sau un auditor pot revizui un jurnal de evenimente. Accesul la jurnalul de evenimente este configurat astfel încât:

- Doar entitățile de mai sus au dreptul să citească înregistrările jurnalului,
- Platforma centrală de jurnalizare arhivează sau șterge automat fișiere (după arhivarea lor) care conțin evenimente înregistrate,
- Este posibil să se identifice orice încălcare a integrității; acest lucru asigură că înregistrările nu conțin goluri sau falsuri,
- Nicio entitate nu are dreptul să modifice conținutul unui jurnal.

Mai mult, controalele de protecție a jurnalelor sunt astfel implementate încât, chiar și după arhivarea jurnalelor, este imposibil să ștergeți înregistrările sau jurnalul în ansamblu înainte de expirarea timpului global de păstrare a jurnalului.

5.4.5 Proceduri de backup pentru jurnalul de audit

Politicile de securitate certSIGN impun ca jurnalul de evenimente să aibă o copie de rezervă periodică. Aceste copii de rezervă sunt stocate în locații auxiliare ale certSIGN. Fișierele jurnal și pistele de audit sunt copiate în conformitate cu procedurile interne.

5.4.6 Sistem de colectare a auditului (intern vs. extern)

Toate jurnalele generate de servere, dispozitive de rețea, echipamente de securitate, aplicații sunt trimise continuu către o platformă centrală, al cărei scop este:

- Colectarea
- Stocarea
- Analiza
- Corelarea
- Arhivarea
- Back-up pe termen lung

5.4.7 Notificare către subiectul cauzator de evenimente

Fără stipulare.

5.4.8 Evaluări ale vulnerabilității

Întreaga infrastructură este supusă evaluării vulnerabilității ca parte a procedurilor interne de evaluare a riscurilor și de gestionare a riscurilor de la certSIGN.

Pentru a se asigura că toate activele, activitățile și serviciile sale sunt sigure, certSIGN a implementat, întreține și îmbunătățește continuu un sistem de management al securității informațiilor certificate ISO 27001: 2013. În conformitate cu cerințele acestui cadru de securitate, toate activitățile de securitate încep cu o evaluare a riscurilor 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 conformă 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, divulgare, utilizare necorespunzătoare, modificare sau distrugere a oricăror date de certificat sau procese de gestionare a certificatelor;
2. Evaluează probabilitatea și daunele potențiale ale acestor amenințări, ținând seama de sensibilitatea datelor certificatelor și a proceselor de gestionare a certificatelor; și
3. Evaluează suficiența politicilor, procedurilor, sistemelor informaționale, tehnologiei și a altor aranjamente pe care CA le are pentru a contracara astfel de amenințări.

5.5 Arhivarea înregistrărilor

Este necesar ca toate datele și fișierele legate de înregistrarea informațiilor asociate securității sistemului, cererile transmise de subiecți/beneficiari, informații despre subiecți/beneficiari, certificate emise și CRL-uri, cheile utilizate de autoritățile de certificare și înregistrare și întreaga corespondență între certSIGN iar Subiectul/Beneficiarii ar trebui să fie supuși arhivării.

Depozitarul on-line conține certificatele active și poate fi utilizat pentru a efectua unele servicii externe ale Autorității de certificare, cum ar fi verificarea validității unui certificat, publicarea certificatelor pentru proprietarii acestora (restaurarea certificatelor) și entitățile autorizate.

Arhiva conține certificate expirate, inclusiv certificate revocate. Arhiva certificatului revocat conține informații despre un certificat, motivul revocării, data la care certificatul a fost plasat pe CRL. Arhiva este utilizată pentru soluționarea litigiilor privind documentele vechi semnate electronic de un subiect.

Copiile de rezervă sunt create și păstrate în afara locației certSIGN.

5.5.1 Tipuri de date arhivate

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

- Toate certificatele pentru o perioadă de 10 ani de la expirarea lor
- Arhivele jurnalelor de log-uri sunt păstrate 10 ani.
- Jurnale de eliberare și revocare a certificatelor pentru o perioadă de 10 ani de la eliberare / revocare
- CRL-uri pentru 10 ani după publicare
- Următoarele timp de 10 ani după ce orice certificat bazat pe aceste înregistrări încetează să mai fie valabil:
    - jurnalul tuturor evenimentelor legate de ciclul de viață al cheilor gestionate de CA, inclusiv orice perechi de chei de subiect generate de CA.
    - termeni și condiții semnate privind utilizarea certificatului

5.5.2 Perioada de păstrare 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 pierderii datelor din arhivă
- Confidențialitatea datelor arhivate și menținerea integrității în timpul perioadei sale de reținere,

Arhivele sunt accesibile numai personalului autorizat.

5.5.4 Procedurile de backup ale arhivei
Backup-ul datelor arhivei se face în conformitate cu politicile și procedurile interne de backup.

5.5.5 Cerințe pentru marcarea temporală a înregistrărilor
certSIGN asigură înregistrarea timpului precis de arhivare a tuturor evenimentelor, înregistrărilor și documentelor menționate mai sus. Acest lucru se realizează prin sincronizarea tuturor sistemelor cu serverele de timp. Acuratețea timpului 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).

5.5.6 Sistem de colectare a arhivelor (intern sau extern)
Sistemele de colectare a arhivelor certSIGN sunt interne.

5.5.7 Proceduri pentru obținerea și verificarea informațiilor arhivate
Arhivele sunt accesibile angajaților autorizați ai certSIGN și auditorilor desemnați. Înregistrările sunt păstrate în format electronic sau pe suport de hârtie.

Beneficiarul / Subiectul poate obține acces la înregistrările de înregistrare aferente și la alte informații referitoare la subiectul certificatului.

5.6 Schimbarea cheilor
Procedurile de schimbare a cheilor permit tranziția lină de la certificatele CA expirate la certificatele CA noi. Spre sfârșitul duratei de viață a cheii private CA, certSIGN încetează să mai folosească cheia privată CA expirată pentru a semna certificate (cu cel puțin un an înainte de expirare) și folosește cheia privată veche doar pentru a semna CRL-uri. Se pune în funcțiune o nouă pereche de chei de semnare CA și toate certificatele și CRL-urile emise ulterior sunt semnate cu noua cheie de semnare privată. Atât vechea, cât și noua pereche de chei pot fi active simultan. Acest proces de schimbare a cheii ajută la minimizarea oricăror efecte adverse cauzate de expirarea certificatului CA. Noul certificat de cheie publică CA corespunzător este furnizat beneficiarilor și părților dependente prin metodele de livrare detaliate în capitolul 6.1.4.

5.7 Compromitere și recuperare în caz de dezastru
Acest capitol descrie procedurile efectuate de certSIGN în situații anormale (inclusiv dezastre naturale) pentru a restabili un nivel de serviciu garantat. Astfel de proceduri sunt executate în conformitate cu planul de continuitate a activității și de recuperare în caz de dezastru acceptat.

5.7.1 Proceduri de gestionare a incidentelor și a compromiterilor

certSIGN are un proces pentru Managementul Crizelor implementat printr-o procedură de gestionare a incidentelor de securitate pentru a răspunde rapid și coordonat la incidente și pentru a limita impactul încălcărilor de securitate. Angajaților li se atribuie roluri de încredere pentru a urmări alertele de evenimente de securitate potențial critice și pentru a se asigura că incidentele relevante sunt raportate în conformitate cu procedura. Defecțiunile critice sunt procesate pe baza aceleiași proceduri.

Procedura de gestionare a incidentelor de securitate specifică, de asemenea, modalitatea de a notifica părțile competente, în conformitate cu normele de reglementare aplicabile, despre orice încălcare a securității sau pierderea integrității care are un impact semnificativ asupra serviciului de încredere furnizat și asupra datelor cu caracter personal menținute în acesta, în termen de 24 de ore de la identificarea încălcării.

În caz de incident de securitate, se utilizează proceduri interne. Procedurile includ notificarea organului de supraveghere, CSIRT sau alte autorități competente.

În cazul în care încălcarea securității sau pierderea integrității este susceptibilă să afecteze negativ o persoană fizică sau juridică căreia i-a fost furnizat serviciul de certificare, vom notifica, de asemenea, persoanei fizice sau juridice încălcarea securității sau pierderea integrității fără întârzieri nejustificate.

Toate jurnalele de evenimente de securitate sunt analizate continuu prin mecanisme automate pentru a identifica dovezi ale activității rău intenționate și a alerta personalul desemnat cu privire la eventuale evenimente critice de securitate.

Toate incidentele și / sau evenimentele de compromis sunt documentate și toate înregistrările asociate sunt arhivate așa cum este descris în secțiunea 5.5 din 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

5.7.2 Resursele de calcul, software-ul și / sau datele sunt corupte

Politica de securitate a certSIGN ia în considerare următoarele amenințări care influențează disponibilitatea și continuitatea serviciilor furnizate:

- Corupția fizică a sistemului informatic certSIGN, inclusiv corupția resurselor de rețea - această amenințare abordează corupțiile provenite din situații de urgență,
- Software-ul și aplicația funcționează defectuos, făcând datele inaccesibile - astfel de corupții se adresează sistemului de operare, aplicațiilor utilizatorilor și executării de software rău intenționat, de exemplu viruși, viermi, troieni,
- Pierderea serviciilor de rețea, importante pentru activitatea certSIGN. Întreruperea alimentării și deteriorarea conexiunilor de rețea,

- Corupția unei părți a infrastructurii de rețea internă, utilizată de certSIGN pentru furnizarea de servicii - corupția poate implica obstrucționarea clienților și refuzul (neintenționat) al serviciilor.

Pentru a preveni sau a limita rezultatele amenințărilor de mai sus:

- Politica de securitate a certSIGN include un plan de continuitate a activității și de recuperare în caz de dezastru,
- În cazul corupției care restricționează funcționalitatea certSIGN, în termen de 48 de ore va fi activată o facilitate de urgență, care ar trebui să înlocuiască toate funcțiile semnificative ale unei autorități de certificare până la restaurarea serviciilor facilității primare. Distanța dintre facilitățile primare și cele de urgență este suficient de mare pentru a evita ca dezastrele potențiale care apar la locul primar să afecteze și locul de urgență.
- Instalarea versiunii software actualizate în producție este posibilă numai după efectuarea unor teste intensive pe un mediu de testare, efectuate în strictă conformitate cu procedurile dezvăluite. Fiecare modificare a sistemului necesită acceptul administratorului de securitate certSIGN.
- Sistemele certSIGN utilizează aplicații pentru crearea copiilor de rezervă ale datelor, permițând recuperarea sistemului în orice moment și efectuarea auditului. Copiile de rezervă includ toate datele relevante din punct de vedere al securității.
- Toate sistemele din infrastructura IT utilizate pentru furnizarea de servicii de certificare și timestamp sunt monitorizate continuu și toate evenimentele de securitate sunt înregistrate și analizate. Activitățile anormale ale sistemului care indică o potențială încălcare a securității, inclusiv intruziunea în sisteme și rețea, sunt detectate și raportate ca alarme pentru a permite certSIGN să detecteze, să înregistreze și să reacționeze în timp util la orice încercări neautorizate și / sau neregulate de accesare a resurselor sale.
- Sensibilitatea oricărei informații colectate sau analizate este luată în considerare prin protejarea acesteia împotriva accesului neautorizat.
- Pentru a detecta orice discontinuitate în operațiunile de monitorizare, este monitorizată și pornirea și oprirea funcțiilor de înregistrare
- De asemenea, sunt monitorizate disponibilitatea tuturor componentelor importante ale infrastructurii TIC utilizate pentru furnizarea serviciilor de certificare, precum și disponibilitatea serviciilor critice.
- certSIGN abordează orice vulnerabilitate critică care nu a fost abordată anterior, în termen de 48 de ore de la descoperirea sa. certSIGN pregătește și implementează un plan de atenuare pentru noile vulnerabilități, dacă acest lucru este rentabil în comparație cu impactul acestora sau documentează decizia că vulnerabilitatea nu necesită remedierea.

5.7.3 Proceduri de compromis pentru cheia privată a entității

Compromisul cheii (cheilor) private CA sau a datelor de activare asociate implică revocarea imediată a certificatului cheii (cheilor) compromise.

În caz de compromis cu cheia privată CA sau suspiciunea unui astfel de compromis, vor fi întreprinse și următoarele acțiuni:

- Notificarea compromisului către toți subiecții / beneficiarii și alte entități cu care certSIGN are acorduri sau altă formă de relații stabilite, printre care părți de încredere și alți furnizori de servicii de încredere. În plus, aceste informații vor fi puse la dispoziția altor părți dependente prin intermediul mass-media și a poștei electronice
- Notificare publicului larg prin mai multe canale, inclusiv un mesaj pe depozitul CA al certSIGN și pe site-ul web, un comunicat de presă în mass-media
- Un certificat corespunzător cheii compromise este plasat pe lista de revocare a certificatelor
- Toate certificatele semnate de CA-ul deteriorat sunt revocate și este prezentat un motiv adecvat pentru revocare
- Autoritatea de certificare generează o nouă pereche de chei și un nou certificat
- Sunt generate noi certificate pentru subiect

Noile certificate pentru subiecți li se transmit gratuit.

Atunci când o cheie privată asociată unei chei publice din certificat a fost compromisă sau există un motiv serios pentru a suspecta că a fost compromisă, subiectul sau beneficiarul, după caz, vor solicita CA să revoce certificatul

5.7.4 Capacități de continuitate a afacerii după un dezastru

certSIGN a stabilit într-un plan de continuitate a afacerii și de recuperare în caz de dezastru toate măsurile necesare pentru a asigura recuperarea completă a serviciilor sale în caz de dezastru sau întreruperea oricărei componente sau servicii TIC importante mai mult decât timpul de oprire maxim tolerabil stabilit. Orice astfel de măsuri sunt conforme cu standardele ISO / IEC 27001 și 27002. Pentru fiecare componentă sau serviciu, operațiunile vor fi restaurate în timpul de oprire maxim tolerabil stabilit în planul de continuitate.

Toate datele din sistemele necesare pentru reluarea operațiunilor CA sunt copiate și stocate într-un loc îndepărtat și sigur, adecvat pentru a permite certificarea să revină în timp util la operațiuni în caz de incident / dezastru.

Copiile de rezervă ale informațiilor și software-ului esențial sunt realizate în mod regulat. Sunt furnizate facilități adecvate de backup pentru a se asigura că toate informațiile și software-ul esențial pot fi recuperate în urma unui dezastru sau a unei defecțiuni media. Aranjamentele de rezervă sunt testate periodic pentru a se asigura că îndeplinesc cerințele planurilor de continuitate a activității.

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

Planurile BCP și DRP abordează, de asemenea, compromisul, pierderea sau compromisul suspectat al cheii private a unei CA ca dezastru, iar procesele planificate sunt în vigoare.

După caz, acolo unde este posibil, se vor lua măsuri pentru a evita repetarea unui dezastru.

5.8 Încetarea activității CA sau RA

certSIGN are o reziliere actualizată pentru a minimiza întreruperile pentru subiecți / beneficiari și părțile terțe, care ar putea rezulta dintr-o decizie a unei autorități de certificare de a înceta funcționarea. Planul include obligații de a notifica în prealabil toți subiecții/beneficiarii autorității care a certificat autoritatea de certificare supusă rezilierii (dacă există) și tranziția

responsabilităților (servicii furnizate subiecților / beneficiarilor, baze de date etc.), în conformitate cu reglementările în vigoare către o altă autoritate de certificare.

Cerințe asociate tranziției responsabilităților

Înainte ca autoritatea de certificare să își înceteze activitatea, va:

- Informa (cu cel puțin 30 de zile în avans) pe următorii, despre decizia de a înceta serviciile sale: toți subiecții / beneficiarii care dețin certificate active (neexpirate și nerevocate) emise de această autoritate și alte entități cu care certSIGN are acorduri sau altă formă de relații stabilite , printre care părți de încredere, alți furnizori de servicii de încredere și autorități relevante, cum ar fi organismele de supraveghere. În plus, aceste informații vor fi puse la dispoziția altor părți dependente;
- Revoca certificatele neexpirate care au fost emise.
- Transfera obligațiile către o entitate parteneră pentru menținerea tuturor informațiilor necesare pentru a furniza dovezi ale funcționării serviciilor de certificare pentru o perioadă rezonabilă, cu excepția cazului în care se poate demonstra că certSIGN nu deține astfel de informații. Informațiile se referă la informații de înregistrare, starea de revocare a certificatelor expirate care au fost emise și arhivele jurnalului de evenimente pentru perioada lor de timp respectivă, așa cum se indică subiecților / beneficiarului și părții de încredere;
- Distruge cheile private CA, inclusiv copii de rezervă, sau retragerea din utilizare, astfel încât cheile private să nu poată fi recuperate;
- Acolo unde este posibil, lua măsuri pentru a transfera furnizarea de servicii de certificare pentru clienții existenți către un alt furnizor de servicii de certificare.

certSIGN va menține sau transfera către o entitate parteneră obligațiile sale de a pune la dispoziție cheia sa publică pentru o perioadă rezonabilă.

În cazul în care certSIGN își va înceta activitățile fără un transfer parțial sau total al activităților sale, va revoca certificatele afectate la o lună după ce a notificat Beneficiarii și / sau Subiecții.

certSIGN are un aranjament care să acopere costurile pentru îndeplinirea acestor cerințe minime în cazul în care intră în faliment sau când din alte motive nu poate acoperi singur costurile, pe cât posibil în limitele legislației aplicabile privind falimentul.

Eliberarea certificatului de către succesorul autorității de certificare închise

Pentru a asigura continuitatea serviciilor de eliberare a certificatelor pentru subiecți, o autoritate de certificare reziliată poate semna un acord cu o altă autoritate de certificare care furnizează servicii similare legate de eliberarea certificatelor de înlocuire a certificatelor valide ale autorității de certificare încheiate.

Prin emiterea unui certificat de înlocuire, succesorul Autorității de certificare desființate preia drepturile și obligațiile Autorității de certificare desființate legate de gestionarea certificatelor care rămân în uz.

Arhiva autorității de certificare care își încetează serviciul trebuie predată autorității de certificare primare - certSIGN ROOT CA (în cazul încetării serviciilor certSIGN SSL DV CA clasa 3 G2) sau instituției care a fost semnat contractul cu (în cazul încetării serviciilor certSIGN ROOT CA).

5.9 Lanțul de aprovizionare

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

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

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

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

6 Controale tehnice de securitate

6.1 Generarea și instalarea perechii de chei

Acest capitol descrie procedurile pentru generarea și gestionarea unei perechi de chei criptografice ale unei autorități de certificare, inclusiv cerințele tehnice asociate. Există controale de securitate adecvate pentru gestionarea oricăror chei criptografice și a oricăror dispozitive criptografice pe parcursul ciclului lor de viață. Aceste măsuri de securitate protejează, de asemenea, datele de activare ale cheilor criptografice, depozitelor, cheilor private și datele de activare pentru cheile private ale CA-urilor subiect și ale altor participanți la PKI și alți parametri de securitate critici.

Procedurile de gestionare a cheilor se aplică stocării și utilizării sigure a cheilor deținute de proprietarul acestora. O atenție deosebită este acordată generării și protecției cheilor private certSIGN, influențând funcționarea sigură a întregului sistem de certificare a cheilor publice.

certSIGN SSL DV CA Clasa 3 G2deține cel puțin un certificat semnat de certSIGN ROOT CA. Cheia privată corespunzătoare cheii publice conținute în certificat este utilizată exclusiv pentru semnarea cheilor publice ale subiecților și a listei de revocare a certificatelor necesare funcționării CA.

O semnătură electronică este creată prin intermediul algoritmului RSA în combinație cu rezumatul criptografic SHA-2.

6.1.1 Generarea perechilor de chei

6.1.1.1 Generarea de perechi de chei CA.

certSIGN are o procedură documentată pentru realizarea generării de perechi de chei CA. Această procedură indică următoarele:

- Roluri care participă la ceremonie (interne și externe față de organizație);
- Funcții care trebuie îndeplinite de fiecare rol și în ce faze;
- Responsabilități în timpul și după ceremonie; și
- Cerințe privind dovezile care trebuie colectate în timpul ceremoniei.

După ceremonia cheii, certSIGN produce un raport privind ceremonia cheilor, care demonstrează că a fost efectuat în conformitate cu procedura menționată și că integritatea și confidențialitatea perechii de chei au fost asigurate. Acest raport este semnat de rolul de încredere responsabil cu securitatea ceremoniei de gestionare a cheilor de la certSIGN (de exemplu, ofițer de securitate), în calitate de martor că raportul înregistrează corect ceremonia de gestionare a cheii în timpul desfășurării.

certSIGN CA:

- Pregăteste și va urmeaza un script de generare a cheilor,
- Are un auditor calificat care să asiste la procesul de generare a perechilor de chei ale CA
- Genereaza perechea de chei CA folosind personal cu roluri de încredere în conformitate cu principiile controlului de către mai multe persoane și al cunoașterii separate;
- Generează cheile CA într-un mediu fizic securizat, în cadrul modulelor criptografice care îndeplinesc cerințele tehnice și de afaceri aplicabile, astfel cum sunt prezentate în 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 Scriptul său de ceremonie a cheii.

Cheile certSIGN SSL DV CA Clasa 3 G2 sunt generate într-un mediu securizat fizic de către personalul cu roluri de încredere sub control cel puțin dual:

- Cel puțin trei angajați în roluri de încredere
- Ofițerul de securitate
- Cel puțin un reprezentant al Comitetului de Management al Politicilor și Procedurilor (PPMB)
- Un maestru al ceremoniei cheilor
- Cel puțin un Auditor Calificat, independent și extern

Perechile de chei de CA sunt generate pe stații de lucru desemnate, autentificate și conectate la module de securitate hardware, respectând cerințele FIPS 140-2 Nivelul 3 sau ISO / IEC 15408 EAL 4. Sunt păstrate permanent criptate pe aceste dispozitive.

Acțiunile executate în timpul efectuării generării perechii de chei sunt înregistrate, datate și semnate de fiecare persoană prezentă în timpul generației. Înregistrările sunt păstrate pentru nevoile de audituri și revizuiri comune ale sistemului.

Operatorii Autorității de înregistrare dețin doar chei pentru autentificarea tuturor acțiunilor lor. Aceste chei sunt generate de operator (în prezența ofițerului de securitate) prin intermediul unui software autentificat furnizat de o autoritate de certificare și de un QSCD.

Cheile de subiect generate de CA sunt generate folosind un algoritm recunoscut ca fiind potrivit pentru utilizări, în timpul valabilității certificatului. Generarea de perechi de chei CA se realizează utilizând algoritmul RSA cu o lungime a cheii de 4096 biți.

Înainte de expirarea certificatului CA care este utilizat pentru semnarea cheilor subiect, CA va genera un nou certificat pentru semnarea perechilor de chei subiect și va aplica toate acțiunile necesare pentru a evita perturbarea operațiunilor oricărei entități care se poate baza pe certificatul CA. Noul certificat CA va fi, de asemenea, generat și distribuit în conformitate cu acest CPP. Aceste operațiuni ar trebui să fie efectuate cu un interval de timp adecvat între data de expirare a certificatului și ultimul certificat semnat pentru a permite tuturor părților care au relații cu certSIGN (subiecți, beneficiari, părți de încredere, CA mai mari în ierarhia CA, etc.) să recunoască acest lucru schimbarea cheii și implementarea operațiunilor necesare pentru a evita orice inconvenient și disfuncționalitate.

6.1.1.2 Generarea de perechi de chei RA

Fără stipulare.

6.1.1.3 Generare pereche chei beneficiar

Cheile subiecților sunt generate de subiect, prin intermediul aplicațiilor software sau al dispozitivelor criptografice. CA respinge o cerere de certificat dacă sunt îndeplinite una sau mai multe dintre următoarele condiții:

- perechea de chei nu îndeplinește cerințele stabilite în secțiunea 6.1.5 și / sau secțiunea 6.1.6
- Există dovezi clare că metoda specifică utilizată pentru a genera cheia privată a fost greșită;

- CA este conștient de o metodă demonstrată sau dovedită care expune cheia privată a solicitantului la compromisuri;
- CA a fost informat anterior că cheia privată a solicitantului a suferit un compromis cheie, cum ar fi prin dispozițiile secțiunii 4.9.1.1;
- CA este conștient de o metodă demonstrată sau dovedită pentru a calcula cu ușurință cheia privată a solicitantului pe baza cheii publice (cum ar fi o cheie slabă Debian, consultați https://wiki.debian.org/SSLkeys).

În cazul în care certificatul de beneficiar conține o extensie extKeyUsage care conține fie valorile id-kp-serverAuth sau anyExtendedKeyUsage, CA NU va genera o pereche de chei în numele beneficiarului și NU va accepta o cerere de certificat folosind o pereche de chei generată anterior de CA .

6.1.2 Livrarea cheii private către beneficiar

Fără stipulare.

6.1.3 Livrarea cheii publice către emitentul certificatului

Subiecții își trimit cheile publice generate ca o cerere electronică al cărui format trebuie să respecte protocoalele PKCS # 10 (CSR).

6.1.4 Livrarea cheii publice CA către părțile implicate

Cheile de verificare a semnăturii CA (publice) sunt puse la dispoziția părților dependente într-un mod care asigură integritatea cheii publice CA și autentifică originea acesteia.

Cheile publice ale unei autorități de certificare care eliberează certificate către subiecți sunt distribuite numai sub formă de certificate care respectă recomandările ITU-T X.509 v.3.

CA își publică certificatele plasându-le în depozitul public al certSIGN: https://registru.certsign.ro/cgi-bin/pubral/pubra/get_cert.

Certificatele CA pot fi livrate părților care se bazează pe acestea împreună cu software-ul (sisteme de operare, browsere web, clienți de e-mail etc.), care permite utilizarea serviciilor oferite de certSIGN.

Depozitul de certificate impune controlul accesului la adăugarea, ștergerea sau modificarea informațiilor conexe.

6.1.5 Dimensiuni cheie

certSIGN SSL DV CA Clasa 3 G2 folosește o cheie de 2048 biți pentru certificate și semnarea CRL.

Certificatele digitale emise de certSIGN SSL DV CA Clasa 3 G2 utilizează chei RSA de 2048 biți.

Certificatele digitale sunt semnate utilizând algoritmul RSA în combinație cu rezumatul criptografic SHA-2.

Doar acesti algoritmi si 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 cu lungimi de cheie mai mari. Aceasta poate include algoritmi Elliptic Curve în loc de RSA și alți algoritmi hash.

6.1.6 Generarea parametrilor cheilor publice și verificarea calității

certSIGN are o procedură documentată pentru realizarea generării de perechi de chei CA pentru certSIGN SSL DV CA Clasa 3 G2.

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

6.1.7 Scopuri de utilizare chei (conform X.509 v3 Key Usage)

Scopurile permise de utilizare a cheilor sunt descrise în câmpul KeyUsage (a se vedea capitolul 7.1.1.2) al extensiei standard a unui certificat conform cu X.509 v3. Acest câmp trebuie verificat de aplicația subiecților care gestionează certificatele.

Utilizarea biților din câmpul KeyUsage trebuie să respecte următoarele reguli:

a. digitalSignature: certificat destinat verificării semnăturii electronice,
b. keyEncipherment: destinat criptării cheilor algoritmului simetric, asigurând confidențialitatea datelor,

Cheia privată a certSIGN ROOT CA (CA emitentă pentru certSIGN SSL DV CA Clasa 3 G2) este utilizată numai în următoarele cazuri:

- Certificate auto-semnate pentru a reprezenta CA Root în sine;
- Certificate pentru CA Intermediareși certificate încrucișate.

6.2 Protecția cheii private și controalele tehnice ale modulului criptografic

Fiecare subiect, operator de autoritate de certificare și autoritate de certificare generează și stochează cheia sa privată utilizând un sistem fiabil care previne pierderea cheii private, divulgarea, modificarea sau accesul neautorizat.

certSIGN utilizează dispozitive criptografice sigure adecvate pentru a efectua sarcini de gestionare a cheilor CA. Aceste dispozitive criptografice sunt cunoscute și sub denumirea de module de securitate hardware (HSM).

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

- Cerințe CA/B Forum Baseline Requirements

Se iau măsuri astfel încât dispozitivele criptografice sigure să nu fie manipulate în timpul expedierii și depozitării la sediul certSIGN.

HSM-urile nu părăsesc mediul sigur al spațiilor securizate ale CA. În cazul în care HSM-urile necesită întreținere sau reparații care nu pot fi efectuate în incinte securizate CA (sub controlul dublu al mai multor angajați într-un rol de încredere), acestea sunt dezafectate în siguranță.

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

Cheile private ale CA rămân sub control multi-personal n din m. Custozilor CA li se atribuie sarcina de a activa și dezactiva cheile private ale CA. Cheile CA sunt apoi activate pentru perioade de timp definite.

Cheile de semnare private ale CA stocate pe dispozitivul criptografic securizat al CA vor fi distruse la retragerea dispozitivului.

6.2.1 Standarde și controale ale modulului criptografic

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

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

Controlul mai multor persoane pentru chei private se aplică cheilor private ale CA utilizate pentru semnarea certificatului și a CRL.

Controlul dual al accesului se realizează prin furnizarea de secrete operatorilor autorizați. Secretele sunt stocate pe carduri criptografice sau token-uri, protejate printr-un cod PIN și transferate autentificat proprietarului lor.

Procedura de transfer secret comun trebuie să includă: procesul de generare și distribuire a cheilor, acceptarea unui secret livrat și responsabilitatea rezultată pentru păstrarea acestuia.

Acceptarea secretului împărtășit de deținătorii săi

Fiecare deținător de secrete partajate, înainte de a-și primi secretul, ar trebui să verifice corectitudinea unui secret creat și distribuirea acestuia. Fiecare parte a secretului partajat trebuie să fie transferată titularului său pe un card criptografic sau token protejat de un număr PIN atribuit de către titular și cunoscut doar de acesta. Primirea secretului partajat și crearea corespunzătoare a acestuia sunt confirmate prin semnătură pe un formular adecvat, a cărui copie este păstrată în arhivele Autorității de certificare și de către titularul secretului.

Protecția secretului comun

Deținătorii secretului comun trebuie să își protejeze partea de a nu fi dezvăluită. Titularul declară că:

- Nu va dezvălui, copia sau împărtăși secretul cu nicio altă parte și că nu va folosi acțiunea în mod neautorizat,
- Nu va dezvălui (direct sau indirect) că el / ea este deținătorul secretului,

Disponibilitatea și ștergerea (transferul) secretului comun

Deținătorul unui secret comun ar trebui să permită accesul la acțiunea sa către persoanele juridice autorizate (într-o formă adecvată, semnată de titular la livrarea acțiunii) numai după autorizarea transmiterii secrete. Această situație ar trebui înregistrată în sistemul de securitate ca jurnal de tranzacții adecvat.

În cazul dezastrelor naturale, titularul secretului ar trebui să se prezinte singur la locul de recuperare de urgență al certSIGN, conform instrucțiunilor transmise de emitentul acțiunii. Secretul comun ar trebui să fie livrat de către titular către site-ul de recuperare de urgență personal de către titular într-o manieră care să permită utilizarea acțiunilor pentru restabilirea activității certSIGN la starea sa normală.

Responsabilitățile deținătorului secret comun

Deținătorul secret comun ar trebui să își îndeplinească sarcinile și obligațiile în conformitate cu cerințele prezentei declarații de practică de certificare și într-un mod deliberat și responsabil în orice situație posibilă. Un deținător de secret comun ar trebui să notifice emitentului secretul comun în caz de furt, pierdere, divulgare neautorizată sau încălcare a securității imediat după producerea incidentului. Un deținător secret comun nu poate fi acuzat că și-a neglijat atribuțiile din motive care îi depășesc controlul. Pe de altă parte, el este responsabil pentru dezvăluirea necorespunzătoare a secretului sau pentru omiterea notificării emitentului cu privire la încălcarea securității secretului, rezultată din greșeala, neglijența sau iresponsabilitatea titularului.

Controlul multiplu nu se aplică cheii private a subiectului.

6.2.3 Custodia cheii private

Cheile private ale autorităților de certificare nu sunt supuse custodiei.

Cheile private ale subiectului nu sunt supuse custodiei.

6.2.4 Copia de rezervă a cheii private

CA creează o copie de rezervă a cheii lor private. Copiile sunt utilizate în cazul executării procedurii standard sau de recuperare a cheilor de urgență (de exemplu, după dezastru). Atunci când se află în afara dispozitivului criptografic securizat, cheia privată CA este protejată într-un mod care asigură același nivel de protecție ca cel furnizat de dispozitivul criptografic securizat. Copiile cheilor private sunt protejate de secrete partajate.

certSIGN nu păstrează copii ale cheilor private ale operatorului autorității de certificare.

Cheia de semnare privată CA este copiată, stocată și recuperată numai de către personalul cu roluri de încredere, utilizând cel puțin controlul dublu într-un mediu securizat fizic. Numărul de personal autorizat să îndeplinească această funcție este redus la minimum și în concordanță cu practicile CA.

Copiile cheilor de semnare private ale CA sunt supuse aceluiași sau unui nivel mai mare de controale de securitate ca și cheile utilizate în prezent.

6.2.5 Arhivarea cheii private

Cheile private ale CA utilizate pentru crearea semnăturii electronice nu sunt arhivate - sunt distruse imediat după încetarea executării operațiunii criptografice folosind astfel de chei sau după expirarea certificatului de cheie publică asociat sau după revocarea acestuia.

6.2.6 Transfer de chei private în sau dintr-un modul criptografic

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

- La crearea copiilor de rezervă pentru cheile private stocate într-un modul criptografic, poate fi necesar ocazional (de exemplu, în cazul corupției sau defecțiunii modulului) să introduceți o pereche de chei într-un alt modul de securitate,
- Când este necesar să se transfere o cheie privată din modulul operațional, utilizată de entitate pentru operațiuni standard, către un alt modul; situația poate apărea în cazul defectării modulului sau dezafectării.

Introducerea unei chei private în modulul de securitate este o operațiune critică, prin urmare, măsurile și procedurile, care împiedică divulgarea, modificarea sau falsificarea cheii, sunt implementate în timpul executării operației.

Introducerea unei chei private într-un modul hardware de securitate al CA necesită restaurarea cheii de pe HSM în prezența unui număr corespunzător de proprietari de secret partajat care protejează modulul care conține cheile private. Datorită faptului că CA poate păstra o copie criptată a cheii sale private, cheile pot fi transferate și între module.

Dacă cheia privată a CA a fost comunicată unei persoane neautorizate sau unei organizații neafiliate cu CA, atunci certificSIGN ROOT CA revocă toate certificatele care includ cheia publică corespunzătoare cheii private comunicate.

6.2.7 Stocare de chei private pe modul criptografic

certSIGN utilizează module de securitate hardware (HSM) pentru a efectua sarcini de gestionare a cheilor CA. Se iau măsuri astfel încât dispozitivele criptografice sigure să nu fie manipulate în timpul expedierii și în timp ce acestea sunt stocate la sediul certSIGN.

Controalele de acces vor fi în vigoare pentru a se asigura că cheile nu sunt accesibile în afara dispozitivelor criptografice sigure dedicate în care sunt stocate cheile de semnare private și copiile CA.

HSM-urile nu părăsesc mediul sigur al spațiilor securizate ale CA.

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

Cheile private ale CA rămân sub control multi-personal n din m. Custozilor CA li se atribuie sarcina de a activa și dezactiva cheile private ale CA. Cheile CA sunt apoi active pentru perioade de timp definite.

Operatorii folosesc dispozitive calificate de creare a semnăturilor electronice (tokenuri / carduri) care respectă cel puțin FIPS 140-2 nivelul 2 sau Common Criteria EAL 4. Cheile sunt întotdeauna generate pe dispozitive și nu le părăsesc niciodată. Dispozitivele securizate sunt protejate de producători la certSIGN, la depozitare în timp ce la certSIGN și distribuite.

6.2.8 Metoda de activare a cheii private

Toate cheile private ale CA sunt introduse în modul după generarea lor, importate într-o formă criptată dintr-un alt modul sau după restaurarea din secretele partajate. Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea se efectuează pe baza unui card criptografic deținut de operator. După introducerea cardului în modulul criptografic și după introducerea numărului PIN, cheia privată rămâne activă până când cardul este scos din modul.

6.2.9 Metoda de dezactivare a cheii private

Toate cheile private ale CA sunt introduse în modul după generarea lor, importate într-o formă criptată dintr-un alt modul sau după restaurarea din secretele partajate. Activarea cheilor private este întotdeauna precedată de autentificarea operatorului. Autentificarea se efectuează pe baza unui card criptografic deținut de operator. După introducerea cardului în modulul criptografic și după introducerea numărului PIN, cheia privată rămâne activă până când cardul este scos din modul.

6.2.10 Metoda de distrugere a cheii private

La sfârșitul vieții, cheile private ale CA sunt distruse de rolurile de încredere ale CA în prezența mai multor reprezentanți ai Comitetului de Management a Politicilor și Procedurilor (PPMB), pentru a se asigura că aceste chei private nu pot fi niciodată recuperate sau utilizate din nou

Cheia privată CA poate fi distrusă prin ștergerea tuturor cardurilor HSM (Operator și Administrator). În plus, HSM-urile permit zeroizarea dispozitivului prin acces fizic și setări pe dispozitiv. Aceasta reinitializează dispozitivul și suprascrie toate datele de pe acesta cu zerouri binare. În cazurile în care această procedură de zeroizare sau reinițializare eșuează, certSIGN va zdrobi, tăia și / sau incinera dispozitivul într-un mod care distruge capacitatea de a extrage orice secret.

Aceste module hardware sunt tratate într-un mod sigur așa cum este descris în procedurile interne documentate de distrugere a cheilor. Înregistrările asociate sunt arhivate în siguranță. Comitetul de Management al Politicilor și Procedurilor (PPMB) autorizează distrugerea cheii private CA și repartizează personalul pentru sarcină.

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

Subiectul este responsabil să distrugă cheia privată.

6.2.11 Capabilitățile modulului criptografic

Vezi deasupra.

6.3 Alte aspecte ale gestionării perechilor de chei

certSIGN utilizează în mod adecvat cheile de semnare privată CA și nu le utilizează după sfârșitul ciclului lor de viață.

Cheia (cheile) de semnare CA utilizate pentru generarea certificatelor și listele de revocare a certificatelor nu vor fi utilizate în alte scopuri.

Cheile de semnare a certificatului trebuie utilizate numai în incinte securizate fizic.

Utilizarea cheii private a CA trebuie să fie compatibilă cu algoritmul hash, algoritmul de semnătură și lungimea cheii de semnătură utilizate pentru generarea certificatelor, în conformitate cu practicile curente (lungimea cheii selectate și algoritmul pentru cheia de semnare CA sunt RSA 4096 biți în acord cu cerințe în ETSI TS 119 312 în scopul semnării CA)

Toate copiile cheilor de semnare private ale CA vor fi distruse la sfârșitul ciclului lor de viață.

6.3.1 Arhivarea cheii publice

certSIGN își arhivează propriile chei publice CA și toate cheile publice certificate de certSIGN SSL DV CA Clasa 3 G2 sub formă de certificat X509 care conține cheia.

Vezi capitolul 5.5 pentru condiții de arhivare.

6.3.2 Perioade operaționale de certificat și perioade de utilizare a perechii de chei

Perioada de utilizare a cheilor publice este definită de valoarea validității câmpului fiecărui certificat de cheie publică. Este, de asemenea, o perioadă de valabilitate a unei chei private. Perioada maximă de utilizare a cheilor subiectului nu poate depăși perioada de valabilitate a unui certificat.

Perioada de valabilitate a certificatului certSIGN SSL DV CA Clasa 3 G2 este de 10 ani.

Perioada de valabilitate a unui certificat de subiect emis de certSIGN SSL DV CA Clasa 3 G2 este de până la 397 zile, pentru certificatele eliberate după 31 august 2020.

Perioadele de utilizare ale certificatelor și cheilor private corespunzătoare pot fi scurtate în cazul revocării unui certificat.

În general, data de începere a perioadei de valabilitate a certificatului respectă data emiterii acestuia. Nu este permisă stabilirea acestei date în viitor sau în trecut.

6.4 Date de activare

6.4.1 Generarea și instalarea datelor de activare

Datele de activare sunt utilizate în două cazuri de bază:

- Ca element al procedurii de autentificare cu unul sau mai mulți factori (așa-numita frază de autentificare, de ex. Parolă, număr PIN etc.),
- Ca parte a secretului comun.

Operatorii și administratorii Autorității de înregistrare și ai Autorității de certificare, precum și alte persoane care îndeplinesc rolurile descrise în capitolul 5.2 utilizează acreditări securizate (tokenuri / carduri) pentru a se identifica și a se autentifica pentru rolurile lor. Cheile lor private care sunt generate pe dispozitive de semnătură electronică calificate sau carduri inteligente HSM de către certSIGN sunt asociate cu datele de activare a utilizatorului (cod PIN) personalizate și distribuite în siguranță. certSIGN se asigură că datele de activare ale operatorilor și administratorilor RA și CA sunt gestionate și protejate în siguranță de către acești participanți prin proceduri interne aplicabile puse la dispoziția acestor participanți.

Secretele partajate utilizate pentru protecția cheii private ale Autorității de certificare sunt generate în conformitate cu cerințele prezentate în capitolul 6.2 și păstrate în cardurile criptografice. Cardurile sunt protejate printr-un număr PIN. Secretele partajate devin date de activare după activare, adică furnizarea numărului PIN corect care protejează cardul. certSIGN se asigură că datele de activare asociate cheilor și operațiunilor private ale CA sunt generate, gestionate, stocate și arhivate în siguranță, așa cum este descris în subsecțiunea relevantă a secțiunilor 6.1 și 6.2. Instalarea și recuperarea perechilor de chei ale CA într-un dispozitiv criptografic sigur necesită controlul simultan a cel puțin doi angajați în roluri de încredere.

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

6.4.2 Protecția datelor de activare

Protecția datelor de activare include metode de control al datelor de activare care împiedică divulgarea acestora. Metodele de control al protecției datelor de activare sunt selectate în funcție de faptul că sunt fraze de autentificare sau dacă controlul este pus în aplicare pe baza cheii private sau a distribuției sale de date de activare în secrete partajate.

Datele de activare utilizate pentru activarea cheii private trebuie protejate prin intermediul controalelor criptografice și a controalelor de acces fizic. Datele de activare vor fi memorate (nu sunt notate) de către entitatea autentificată. Dacă datele de activare sunt scrise, nivelul de protecție al acestora ar trebui să fie același cu datele protejate prin utilizarea unui card

criptografic. Mai multe încercări nereușite de a accesa modulul criptografic ar trebui să ducă la blocarea acestuia. Datele de activare stocate nu vor fi păstrate niciodată împreună cu cardul criptografic.

Subiecții sunt responsabili pentru gestionarea și protecția securizată a datelor lor de activare (adică codul PIN).

6.4.3 Alte aspecte ale datelor de activare

Fără stipulare

6.5 Controale de securitate ale computerelor

Acest capitol descrie controalele de securitate ale computerelor certSIGN.

Subiectul 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 de securitate a computerului

Mecanismele de securitate care protejează sistemele informatice sunt executate la nivel de sisteme de operare, aplicații și protecții fizice.

Calculatoarele sunt configurate cu următoarele mecanisme de securitate:

- Înregistrare autentificată obligatorie la nivel de sistem de operare și aplicații,
- Controlul accesului discreționar,
- Posibilitatea efectuării auditului de securitate,
- Computerul este accesibil numai personalului autorizat, care îndeplinește roluri de încredere în certSIGN,
- Aplicarea segregării datoriei, care decurge din rolul îndeplinit în sistem,
- Identificarea și autentificarea rolurilor și a personalului care îndeplinește aceste roluri,
- Prevenirea reutilizării unui obiect de către un alt proces după ce obiectul a fost eliberat printr-un proces autorizat,
- Protecția criptografică a schimbului de informații și protecția bazelor de date,
- Arhivarea istoricului operațiunilor pe computer și a datelor solicitate de audituri,
- O cale sigură care permite identificarea și autentificarea fiabilă a rolurilor și a personalului care îndeplinește aceste roluri,
- Metode de restaurare cheie (numai pentru module de securitate hardware)
- Monitorizare și alertare în caz de acces neautorizat.

Integritatea sistemelor și informațiilor certSIGN este protejată împotriva virușilor, software-ului rău intenționat și neautorizat.

Suporturile utilizate în cadrul sistemelor certSIGN sunt manipulate în siguranță pentru a proteja suportul de deteriorare, furt, acces neautorizat și perimare.

Procedurile de gestionare a mass-media sunt implementate pentru a proteja împotriva perimării și deteriorării suportului pentru perioada de timp pentru care trebuie păstrate înregistrările.

Datele sensibile trebuie protejate împotriva dezvăluirii prin intermediul obiectelor stocate refolosite (de exemplu, fișiere șterse) fiind accesibile utilizatorilor neautorizați. În acest scop, software-ul special va fi utilizat cu algoritmi de ștergere sigură pentru mediile de stocare,

HSM-urile vor fi zero, dispozitivele criptografice securizate (tokenuri / carduri) vor fi formatate înainte de reutilizare / sau vor fi distruse fizic la sfârșitul ciclului lor de viață.

Pentru toate conturile capabile să provoace direct emiterea certificatelor se aplică autentificarea cu mai mulți factori.

6.5.2 Evaluarea securității computerului

Sistemul de calcul certSIGN respectă cerințele descrise în standardele ETSI: ETSI EN 319 411-1 și CEN CWA 14167 (Cerințe de securitate pentru sistemele de încredere Gestionarea certificatelor pentru semnături electronice).

6.6 Controale de securitate ale 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 de dezvoltare a sistemului

O analiză a cerințelor de securitate se efectuează în etapa de proiectare și specificație a cerințelor proiectelor de dezvoltare a sistemelor întreprinse de certSIGN sau în numele certSIGN pentru a se asigura că securitatea este integrată în sistemele IT.

Fiecare aplicație, înainte de a fi utilizată pentru producția în cadrul certSIGN, este instalată astfel încât să permită controlul versiunii actuale și să prevină instalarea neautorizată a programelor sau falsificarea celor existente.

Reguli similare se aplică înlocuirii componentelor hardware, după cum urmează:

- hardware-ul este furnizat într-un mod care permite trasabilitatea și monitorizarea traseului componentelor până la locul de instalare a acestora,
- livrarea hardware-ului de rezervă se efectuează într-un mod similar cu livrarea hardware-ului original; înlocuirea este efectuată de personal de încredere și instruit.

certSIGN monitorizează versiunile actualizate ale software-ului de Linting dezvoltat de terți și verifică actualizările în termen de cel mult trei luni de la lansarea actualizării. certSIGN efectuează Linting pe corpul certificatelor sale de abonat neexpirate și nerevocate de fiecare dată când actualizează software-ul de Linting.

6.6.2 Controale de gestionare a securității

Scopul controlului de gestionare a securității este de a supraveghea funcționalitatea sistemelor certSIGN, oferind asigurarea că sistemul funcționează corect și în conformitate cu configurațiile acceptate și implementate.

Controalele aplicate sistemului certSIGN permit verificarea continuă a integrității aplicației, a versiunii lor, precum și autentificarea și verificarea originii hardware.

6.6.3 Controale de securitate ale ciclului de viață

Politicile și procedurile de control al modificărilor sunt aplicate pentru versiuni, modificări și remedieri software de urgență ale oricărui software operațional și modificări ale configurațiilor care aplică politica de securitate a certSIGN.

Configurația actuală a sistemelor certSIGN, orice modificare sau versiune nouă, modificare și remedieri software de urgență ale oricărui software operațional, sunt documentate.

certSIGN implementează proceduri de securitate internă pentru a se asigura că:

- Patch-urile de securitate se aplică într-un timp rezonabil după ce acestea sunt disponibile;
- Patch-urile de securitate nu sunt aplicate dacă introduc vulnerabilități sau instabilități suplimentare care depășesc avantajele aplicării acestora;

Motivele pentru care nu se aplică nicio corecție de securitate sunt documentate.

certSIGN implementează o procedură internă de gestionare a capacității care asigură monitorizarea capacității infrastructurii TIC pentru serviciile de certificare și efectuarea unor estimări ale cerințelor de capacitate pentru a se asigura că sunt disponibile puteri de procesare și stocare adecvate.

6.7 Controale de securitate a rețelei

Politicile și procedurile de control al modificărilor sunt aplicate pentru versiuni, modificări și remedieri software de urgență ale oricărui software operațional și modificări ale configurațiilor care aplică politica de securitate a certSIGN.

Configurația actuală a sistemelor certSIGN, orice modificare sau versiune nouă, modificare și remedieri software de urgență ale oricărui software operațional sunt documentate.

certSIGN implementează proceduri de securitate internă pentru a se asigura că:

- Patch-urile de securitate se aplică într-un timp rezonabil după ce acestea sunt disponibile;
- Patch-urile de securitate nu sunt aplicate dacă introduc vulnerabilități sau instabilități suplimentare care depășesc avantajele aplicării acestora;

Motivele pentru care nu se aplică nicio corecție de securitate sunt documentate.

certSIGN implementează o procedură internă de gestionare a capacității care asigură monitorizarea capacității infrastructurii TIC pentru serviciile de certificare și efectuarea unor estimări ale cerințelor de capacitate pentru a se asigura că sunt disponibile puteri de procesare și stocare adecvate.

6.8 Marcarea temporală

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

7 Profil certificate, CRL și OCSP

Profilurile de certificate și profilul Listă de revocare a certificatelor (CRL) sunt conforme cu formatul descris în standardul ITU-T X.509 v.3, în timp ce profilul OCSP respectă cerințele RFC 6960. Informațiile enumerate mai jos descriu semnificația câmpurilor de certificat respective, CRL și OCSP, standarde aplicate și extensii private utilizate de certSIGN.

7.1 Profilul certificatului

Profilul câmpurilor de bază pentru certificatul certSIGN SSL DV CA Clasa 3 G2 este descris în Tabelul 7.1 din documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

Profilul câmpurilor de bază pentru certificatele emise de certSIGN SSL DV CA Clasa 3 G2 este descris în Tabelul 7.2 din documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

7.1.1 Număr de versiune

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

7.1.2 Extensii de certificate

Extensiile de certificate pentru certSIGN SSL DV CA Clasa 3 G2 sunt descrise în Tabelul 7.3 din documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

Certificatul DV SSL conține extensii descrise în Tabelul 7.4 din documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

Certificatul OCSP conține extensii descrise în tabelul 7.5 din documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

7.1.3 Identificatori de algoritm obiect

Conform cu documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

7.1.4 Forme de nume

Conținutul câmpurilor din certificatele DV trebuie să îndeplinească cerințele din secțiunea 3.1 și din ultima versiune publicată a CAB Forum Baseline Requirements Certificate Policy.

Numele Emitentului, pentru toate căile de certificare posibile, trebuie să fie identic octet-cu-octet cu Numele Subiectului din certificatul emitentului. Atributele Subiectului nu pot conține doar metadate precum '.', '-', și ' ' (adică spațiu) pentru a indica faptul că valoarea nu există, este incompletă, sau nu este aplicabilă.

7.1.5 Constrângeri de nume

Fără stipulare.

7.1.6 Identificator de obiect al politicii de certificat

Identificatorii obiectelor politicii certificatelor utilizate la nivelul certSIGN SSL DV CA Clasa 3 G2 sunt descriși în Tabelul 7.6 și Tabelul 7.7, conform cu documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

7.1.7 Utilizarea extensiei de constrângeri de politică

Fără stipulare.

7.1.8 Sintaxa și semantica calificativelor de politici

certSIGN emite certificate cu un calificativ de politică în cadrul extensiei Politici de certificat. Această extensie conține un calificator de pointer CPP care indică CPP.

7.1.9 Prelucrarea semanticii pentru extensia critică de politici de certificat

Fără stipulare.

7.2 Profil CRL

Profilul CRL este descris în Tabelul 7.8 din documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

7.2.1 Numere de versiune

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

7.2.2 CRL și extensii de intrare CRL

Extensiile CRL pentru certSIGN SSL DV CA Clasa 3 G2 sunt descrise în Tabelul 7.9 din documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

Extensiile de intrare CRL (crlEntryExtensions) acceptate de certSIGN conțin câmpuri conform cu documentul extern "certSIGN SSL DV CA Class 3 G2 - Anexa Profile.docx".

7.3 Profil OCSP

Protocolul de verificare a stării certificatului on-line (OCSP) permite evaluarea stării certificatului.

Serviciul OCSP este furnizat de certSIGN în numele tuturor autorităților de certificare afiliate. Serverul OCSP, care emite confirmări de stare a certificatului, folosește o pereche de chei speciale pentru fiecare CA Intermediarși CA ROOT, generată exclusiv în acest scop.

Certificatul de server OCSP trebuie să conțină extensia extKeyUsage, descrisă în RFC 5280.

Această extensie ar trebui setată ca non-critică și înseamnă că o autoritate de certificare care emite certificatul către serverul OCSP confirmă prin semnarea delegării autorizației de a emite conformitatea stării certificatului (a beneficiarilor acestei autorități).

De asemenea, certificatul de server OCSP conține extensia OCSPNoCheck, descrisă de RFC 6960. Această extensie trebuie declarată necritică ceea ce înseamnă că un client OCSP primește un răspuns semnat cu cheia privată asociată acestui certificat poate avea încredere în starea certificatului de server OCSP, fără a fi necesar să îi verificăm starea de revocare.

Entitatea care primește o confirmare emisă de serverul OCSP trebuie să accepte formatul de răspuns standard cu identificatorul id-pkix-ocsp-basic.

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

- GOOD - indică starea validă a certificatului

- REVOKED - indică faptul că certificatul a fost emis și revocat sau certificatul nu a fost emis în conformitate cu RFC 6960

- UNKNOWN - indică faptul că nu există suficiente informații pentru a determina starea certificatului

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

7.3.1 Numere de versiune

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

7.3.2 Extensii OCSP

În conformitate cu RFC 6960, serverul certSIGN OCSP acceptă următoarea extensie:

Nonce- legarea unei cereri și a unui răspuns pentru a preveni atacurile de răspuns. **Nonce** este inclus în **requestExtension** al **OCSPRequest** și repetat în câmpul **responseExtension** al **OCSPResponse**.

8 Auditul de conformitate și alte evaluări

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

8.1 Frecvența sau circumstanțele evaluării

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

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

Auditurile la cerere pot fi realizate la discreția exclusivă a certSIGN, la cererea organismului de supraveghere, astfel cum sunt definite în Regulamentul UE 910/2014 și CA/B Forum Baseline Requirements, sau pentru a demonstra conformitatea cu cerințele specifice din industrie, legale sau comerciale.

8.2 Identitatea / calificările evaluatorului

Evaluarea va fi efectuată de un organism de evaluare a conformității, astfel cum este definit în Regulamentul UE 910/2014 și în specificațiile CA/B Forum Baseline Requirements.

8.3 Relația evaluatorului cu entitatea evaluată

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

8.4 Subiecte acoperite de evaluare

Auditurile planificate acoperă, dar nu se limitează la toate aspectele operațiunilor și serviciilor certSIGN specificate în prezentul CPP, în conformitate cu următoarea schemă:
„WebTrust for CAs" v2.2.2 sau o versiune mai nouă și „WebTrust for CAs SSL Baseline" v2.8 sau o versiune mai nouă.
Auditurile interne și externe se desfăşoară conform regulilor și procedurilor acceptate pe plan internaţional pentru Autoritățile de Certificare și vizează:

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

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

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

8.5 Acțiuni întreprinse ca urmare a deficienței

Organismul de evaluare a conformității raportează deficiențele și neconformitățile detectate către PPMP. certSIGN și organismul de evaluare a conformității analizează împreună concluziile raportului și convin asupra unui plan de corecție și a unui termen pentru implementarea acestuia.

Se poate realiza un audit de urmărire pentru a verifica acțiunile de remediere.

8.6 Comunicarea rezultatelor

Organismul de evaluare a conformității comunică raportul de audit către conducerea certSIGN și către PPMB.

Raportul de audit va preciza în mod explicit că acoperă sistemele și procesele relevante utilizate la eliberarea tuturor certificatelor care afirmă identificatorii de politici enumerați în secțiunea 7.1.6.1. CA pune la dispoziția publicului Raportul de audit nu mai târziu de trei luni de la sfârșitul perioadei de audit. În cazul unei întârzieri mai mari de trei luni și dacă este solicitat de către un furnizor de software de aplicație, CA furnizează o scrisoare explicativă semnată de auditorul calificat. Raportul de audit va fi conform cu cap.8.6 din CABF Baseline Requirements.

8.7 Auto-audituri

În perioada în care CA emite certificate, CA monitorizează respectarea cerințelor CPP și CA/B Forum Baseline Requirements și își controlează cu strictețe calitatea serviciilor prin efectuarea de auto-audit pe o bază trimestrială, comparativ cu un eșantion selectat aleatoriu din un certificat sau cel puțin trei la sută din certificatele emise de acesta în perioada care începe imediat după prelevarea eșantionului anterior de auto-audit.

9 Alte aspecte juridice și de afaceri

9.1 Tarife

Tarifele/Prețurile pentru serviciile de certificare și tipurile de servicii percepute sunt publicate în lista tarifelor disponibile la adresa http://www.certsign.ro. Prețurile sunt stabilite în conformitate cu politica internă a prețurilor.

Serviciile furnizate de certSIGN sunt stabilite după cum urmează:

- **Servicii de certificare individuală** - prețul este stabilit pentru fiecare serviciu parțial, de exemplu, pentru un certificat individual vândut sau un număr mai mic de certificate,
- **Pachete de servicii de certificare** - prețul este stabilit pentru pachetele de servicii prestate unei singure entități;
- **Servicii de abonament** - prețul este stabilit pentru serviciile prestate periodic; valoarea sumelor plătite depinde de tipul și numărul de servicii accesate și este utilizată în principal pentru serviciile de marcare a timpului și verificarea stării certificatelor prin intermediul protocoalelor OCSP,
- **Servicii indirecte -** prețul este stabilit pentru fiecare serviciu prestat clienților săi de către un partener certSIGN a cărui activitate se bazează pe infrastructura certSIGN.

Plățile se vor face în numerar, prin ordin de plată sau carduri bancare, în conformitate cu prevederile legale în vigoare.

9.1.1 Taxe de eliberare sau reînnoire a certificatului

Prețurile sunt formate în conformitate cu politica internă a prețurilor.

9.1.2 Taxe de acces la certificat

Serviciu gratuit.

9.1.3 Taxe de acces la informații de revocare sau stare

Prețurile sunt formate în conformitate cu politica internă a prețurilor.

9.1.4 Taxe pentru alte servicii

Prețurile sunt formate în conformitate cu politica internă a prețurilor.

9.1.5 Rambursarea taxelor

Plățile pot fi rambursate conform condițiilor contractuale aplicabile..

9.2 Responsabilitatea financiară

9.2.1 Acoperirea prin asigurare

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

9.2.2 Alte bunuri

Fără stipulare

9.2.3 Asigurare sau acoperire de garanție pentru entitățile finale

certSIGN beneficiază de asigurări care acoperă răspunderile profesionale.

9.3 Confidențialitatea informațiilor comerciale

9.3.1 Domeniul de aplicare al informațiilor confidențiale

Toate informațiile legate de subiectul / beneficiarul / entitățile partenere care procesele certSIGN sunt obținute, stocate și prelucrate în conformitate cu prevederile Regulamentului (UE) nr. 910/2014. Relațiile dintre un subiect, un beneficiar, o entitate parteneră și certSIGN se bazează pe încredere.

Un terț poate avea acces doar la informațiile publice disponibile în certificate. Alte date furnizate în cererile trimise către certSIGN nu vor fi dezvăluite de bună voie unei terțe părți sub nicio circumstanță (cu excepția situațiilor juridice).

O parte va fi exonerată de răspunderea divulgării datelor confidențiale dacă:

a) informațiile au fost cunoscute de partea contractantă înainte de a fi primite de cealaltă parte contractantă;

sau

b) informațiile au fost dezvăluite după obținerea acordului scris al celeilalte părți;

sau

c) partea a fost obligată legal să dezvăluie informațiile.

Dezvăluirea oricărei informații către părțile implicate în îndeplinirea obligațiilor lor va fi făcută în mod confidențial și va acoperi numai informațiile necesare pentru îndeplinirea obligațiilor.

Tipuri de informații considerate confidențiale și private

certSIGN, angajații săi și alte entități care desfășoară activități de certificare se angajează să păstreze informațiile secrete atât în timpul, cât și după angajare. Sunt considerate informații private și confidențiale:

- Informații furnizate de subiecți / beneficiari în plus față de informațiile care vor fi trimise pentru a efectua serviciile de certificare; în acele situații dezvăluirea informațiilor primite necesită acordul prealabil scris al proprietarului informațiilor sau în alte condiții conform legii.
- Informații furnizate de / către subiecți / beneficiari (de exemplu, conținutul contractelor încheiate cu subiecții / beneficiarii sau părțile de încredere, conturi bancare, cereri de înregistrare, eliberare, rekeying, revocarea certificatelor - cu excepția informațiilor incluse în certificate sau din depozit, în conformitate cu prezentul CPP); o parte din informațiile menționate mai sus pot fi divulgate numai cu aprobarea și în scopul specificat de către proprietarul informațiilor (de exemplu subiectul),
- Înregistrări ale tranzacțiilor de sistem (toate tipurile de tranzacții, precum și date pentru controlul tranzacțiilor, așa-numitele jurnale de tranzacții de sistem)
- Evidența evenimentelor (jurnale) legate de serviciile de certificare, păstrate de certSIGN,

- Rezultatele auditurilor interne și externe, dacă sunt o amenințare pentru securitatea certSIGN,
- Planuri de urgență,
- Informații despre măsurile luate pentru a proteja dispozitivele hardware și aplicațiile software, informații despre gestionarea serviciilor de certificare și regulile de înregistrare planificate.

Persoanele responsabile de păstrarea confidențialității informațiilor și care respectă regulile privind gestionarea informațiilor poartă răspunderea conform legilor în vigoare.

Divulgarea motivului de revocare a certificatului

Dacă un certificat a fost revocat la cererea unei părți autorizate, altul decât subiectul sau subiectul, informațiile despre revocare și motivele aferente sunt dezvăluite ambelor părți.

Divulgarea informațiilor non-publice către oficialii de aplicare a legii

Informațiile confidențiale pot fi dezvăluite oficialilor de aplicare a legii numai după îndeplinirea tuturor formalităților solicitate de legile române în vigoare.

9.3.2 Informații care nu intră în sfera informațiilor confidențiale

Toate informațiile necesare pentru buna funcționare a serviciilor de certificare nu sunt considerate confidențiale sau private. Se referă în special la informațiile incluse într-un certificat de către autoritatea de certificare emitentă, în conformitate cu specificațiile din capitolul 7. Un subiect / beneficiar care solicită obținerea unui certificat este conștient de tipul de informații incluse în certificat și este de acord cu publicarea lor.

O parte din informațiile furnizate de către sau către Subiect / Beneficiar ar putea fi puse la dispoziția altor entități numai cu acordul scris al Subiectului / Beneficiarului și în scopul declarat în contractul încheiat cu Subiectul / Beneficiarul.

9.3.3 Responsabilitatea de a proteja informațiile confidențiale

certSIGN, angajații săi, precum și entitățile care desfășoară activități de certificare se angajează să păstreze informațiile secrete atât în timpul, cât și după angajare.

9.4 Confidențialitatea informațiilor personale

În furnizarea de servicii de încredere, certSIGN prelucrează datele personale ale subiectului / beneficiarului în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și în conformitate cu dispozițiile interne ale Regulamentului nr. 679/2016 privind protecția persoanelor cu în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și alte dispoziții ale dreptului comun al Uniunii privind protecția datelor.

Scopul prelucrării datelor cu caracter personal este furnizarea de servicii de certificare.

9.4.1 Planul de confidențialitate

În furnizarea de servicii de certificare, certSIGN acționează ca un operator de date cu caracter personal conform paragrafului 7 al art. 4 din Regulamentul nr. 679/2016. Măsurile de securitate solicitate de Autoritatea Națională de Supraveghere a României pentru Prelucrarea Datelor cu Caracter Personal sunt implementate pentru a garanta că:

- Se iau măsuri tehnice și organizatorice adecvate împotriva prelucrării neautorizate sau ilegale a datelor cu caracter personal și împotriva pierderii accidentale sau distrugerii sau deteriorării datelor cu caracter personal.
- Accesul la serviciile certSIGN se referă doar la prelucrarea acelor date de identificare care sunt adecvate, relevante și nu excesive pentru a permite accesul la serviciul respectiv.
- Protecția confidențialității și integritatea datelor de înregistrare: atunci când sunt schimbate cu beneficiarul / subiectul, când sunt schimbate între componentele sistemului certSIGN, precum și atunci când sunt stocate.

9.4.2 Informații tratate ca private

Toate informațiile care conduc la identificarea subiectului sunt considerate informații personale.

9.4.3 Informații tratate ca private

Conținutul certificatelor digitale și al informațiilor accesibile prin intermediul depozitarului sunt informații publice.

9.4.4 Responsabilitatea de a proteja informațiile private

certSIGN și angajații săi se angajează să păstreze confidențialitatea informațiilor personale în timpul serviciilor de certificare și după încetarea certificatului.

certSIGN nu va dezvălui informații personale niciunei terțe părți, din niciun motiv, cu excepția cazului în care este impusă de lege sau de către autoritățile competente.

9.4.5 Notificare și consimțământ pentru utilizarea informațiilor private

În procesul de emitere a unui certificat digital, subiecții / beneficiarii sunt informați cu privire la necesitatea de a utiliza datele lor personale pentru serviciu și la necesitatea consimțământului. Dacă persoanele vizate nu sunt de acord ca certSIGN sa le prelucreze date, nu pot beneficia de serviciile de certificare.

Subiecții / Beneficiarii au, de asemenea, opțiunea de a utiliza datele cu caracter personal în alte scopuri comunicate expres de certSIGN prin contract sau altfel.

9.4.6 Divulgarea conform procesului judiciar sau administrativ

certSIGN este exonerat de răspundere pentru divulgarea datelor cu caracter personal ale subiecților / beneficiarilor în următoarele situații:

- divulgarea informațiilor personale Organismului de supraveghere în conformitate cu legislația aplicabilă;

- către instituțiile și organismele competente, pe baza obligațiilor de drept public pe care certSIGN le are, în conformitate cu prevederile legale.

9.4.7 Alte circumstanțe de divulgare a informațiilor

Constituie excepții de la obligația de a păstra confidențialitatea datelor cu caracter personal care exonerează certSIGN de răspundere, următoarele situații:

- divulgarea informațiilor personale către:

- auditori în cadrul auditurilor la care este supus certSIGN conform prevederilor Regulamentului (UE) nr. 910/2014 sub confidențialitate;
- companiile de curierat cu care certSIGN are un contract, cu acordul Subiectului / Beneficiarului, dacă a optat pentru transmiterea certificatului la adresa de domiciliu sau la o altă adresă comunicată, respectând aceleași obligații privind securitatea datelor cu caracter personal el / are și certSIGN;
- o persoană împuternicită căreia îi externalizez anumite servicii;
- companii afiliate certSIGN

- informații personale care apar în certificate sau în autoritățile publice (depozitar), cu acordul subiectului / beneficiarului.

9.5 Drepturi pentru proprietate intelectuala

Toate mărcile comerciale, brevetele, mărcile, licențele, imaginile grafice etc. utilizate de certSIGN sunt și vor fi proprietatea intelectuală a proprietarilor lor legali. certSIGN se angajează să menționeze acest lucru în conformitate cu cererile impuse de proprietari.

Toate mărcile comerciale, brevetele, mărcile, licențele, imaginile grafice etc., aparținând certSIGN sunt și rămân în proprietatea sa, indiferent dacă sunt împreună cu brevete, modele de utilitate, drepturi de autor sau nu și nu pot fi reproduse sau livrate unei terțe părți fără acordul prealabil scris al certSIGN.

9.6 Reprezentări și garanții

9.6.1 Reprezentările și garanțiile CA.

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

certSIGN garantează că toate cerințele stabilite în CPP aplicabil (și indicate în certificat în conformitate cu capitolul 7) sunt respectate. De asemenea, își asumă responsabilitatea de a asigura o astfel de conformitate și de a furniza aceste servicii în conformitate cu CPP.

Singura garanție oferită de certSIGN este că procedurile sale sunt implementate în conformitate cu CPP și procedurile de verificare în vigoare și că toate certificatele emise cu un identificator de obiect (OID) au fost emise în conformitate cu procedurile relevante, iar CPP ca aplicabil în momentul emiterii.

Garanțiile de certificat includ în mod specific cele specificate în CA/B Forum Baseline Requirements, punctul 9.6.1.

9.6.2 Reprezentările și garanțiile RA

RA are obligația de a respecta scrupulos CPP și procedurile interne relevante certSIGN.

9.6.3 Reprezentările și garanțiile Subiectului

Subiectul acceptă Termenii și condițiile relevante pentru serviciul furnizat de certSIGN.

Subiectul este de acord cu CPP și cu responsabilitățile, obligațiile și obligațiile sale relevante, astfel cum sunt prevăzute în secțiunile relevante ale CPP.

Termenii și condițiile CA conțin dispoziții care impun subiectului însuși obligațiile și garanțiile specificate în CA/B Forum Baseline Requirements, punctul 9.6.3.

9.6.4 Reprezentările și garanțiile Entităților partenere

Exemple de obligații și responsabilități ale părților invocate includ (fără limitare):

- efectuarea cu succes a operațiunilor cu cheie publică ca o condiție prealabilă pentru a se baza pe un certificat certSIGN
- validarea unui certificat certSIGN prin utilizarea (CRL-urilor) sau a serviciilor de validare a certificatelor furnizate de certSIGN
- încetarea imediată a oricărei dependențe de un certificat certSIGN dacă acesta a fost revocat sau expirat
- Luarea la cunoștință a prevederilor prezentului CPP, a garanțiilor și limitelor răspunderii Certsign SA

9.6.5 Reprezentările și garanțiile altor participanți

Fără stipulare.

9.7 Declinarea garanțiilor

Cu excepția cazului în care se prevede altfel în mod expres în CPP și în legislația aplicabilă, certSIGN renunță la toate garanțiile și obligațiile de orice tip, inclusiv orice garanție de comercializare, orice garanție de adecvare pentru un anumit scop și orice garanție de exactitate a informațiilor furnizate (cu excepția cazului în care a provenit dintr-o sursă autorizată) și, în plus, renunță la orice răspundere pentru neglijență și lipsa de îngrijire rezonabilă din partea subiectului, beneficiarilor și părților care se bazează.

9.8 Limitări de răspundere

În limita stabilită de legea României, în niciun caz (cu excepția fraudei sau a unei abateri intenționate de către certSIGN) certSIGN nu va fi răspunzător pentru:

- Orice pierdere de profit, de venit sau afaceri;
- Orice pierdere de date;
- Orice daune indirecte, consecvente sau punitive care rezultă din sau în legătură cu utilizarea, livrarea, licența și executarea sau neexecutarea certificatelor sau a semnăturilor digitale;
- 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.

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

9.9 Indemnizații

certSIGN nu își asumă nicio responsabilitate financiară pentru certificate, CRL-uri și servicii conexe utilizate în mod necorespunzător specificate în acest CPP.

certSIGN acționează așa cum se specifică la punctul „9.9 Despăgubiri de către CA” din CA/B Forum Baseline Requirements

9.10 Termeni și reziliere

9.10.1 Termeni

Prezentul CPP și orice modificări la acesta vor intra în vigoare după publicarea în depozitar și în conformitate cu secțiunea 9.12.2 și vor rămâne în vigoare permanent până la încetarea conform prezentei secțiuni 9.10.

9.10.2 Rezilierea

CPP rămâne în vigoare până când este înlocuit cu o nouă versiune.

9.10.3 Efectul încetării și supraviețuirii

Condițiile și efectul care rezultă din rezilierea acestui CPP vor fi comunicate prin intermediul site-ului web certSIGN la reziliere. Această comunicare va descrie prevederile care pot supraviețui încetării acestui CPP și rămân în vigoare. Responsabilitățile pentru protejarea informațiilor confidențiale și a informațiilor personale private vor supraviețui 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 comunicări cu participanții

Toate notificările și alte comunicări care pot sau trebuie să fie date, servite sau trimise în conformitate cu CPP trebuie să fie în scris și să fie trimise, cu excepția cazului în care sunt prevăzute în mod explicit în CPP, fie prin (i) poștă recomandată, chitanță de retur solicitată, poștale plătit în avans, (ii) un serviciu de curierat „peste noapte” sau de curierat rapid recunoscut la nivel internațional, (iii) livrare manuală (iv) transmisie de fax, considerată primită la livrarea efectivă sau facsimil completat, sau (v) în format electronic, semnată cu o semnătură electronică calificată și să fie adresat certSIGN utilizând datele de contact furnizate în capitolul 1.5.1 din prezentul document.

9.12 Modificări

9.12.1 Procedura de modificare

certSIGN este responsabil prin organismul său de gestionare a politicilor și procedurilor pentru aprobarea și modificarea prezentului CPP. CPP este revizuit cel puțin o dată pe an.

Singurele modificări pe care PPMB le poate face la aceste specificații CPP fără notificare sunt modificări minore care nu afectează nivelul de asigurare al acestui CPP, de exemplu, corecții editoriale sau tipografice sau modificări ale detaliilor de contact.

Erorile, actualizările sau modificările sugerate la acest document vor fi comunicate așa cum sunt identificate în prezentul CPP, secțiunea 1.5.4. O astfel de comunicare va include o descriere a modificării, o justificare a modificării și informații de contact ale persoanei care solicită modificarea.

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

Orice modificare a CPP este aprobată de PPMB și este anunțată clienților certSIGN. Subiecții / Beneficiarii trebuie să respecte numai CPP aplicabil în prezent.

9.12.2 Mecanismul de notificare și perioada
Toate modificările aduse prezentului CPP în curs de examinare de către PPMB vor fi diseminate părților interesate înainte de publicare. Data efectivă este indicată pe pagina de titlu a prezentului CPP.

9.12.3 Circumstanțe în care trebuie modificat OID
Fără stipulare.

9.13 Proceduri de soluționare a litigiilor
Toate disputele asociate prezentului CPP vor fi soluționate conform legilor române.

9.14 Legea aplicabilă
Legile române vor reglementa aplicabilitatea, construcția, interpretarea și valabilitatea prezentului CPP (fără a da efect vreunei prevederi de conflict de legi care ar cauza aplicarea altor legi).

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

9.16 Dispoziții diverse

9.16.1 Întregul acord
Fără stipulare.

9.16.2 Misiune
Fără stipulare.

9.16.3 Separabilitate
CA acționează așa cum se specifică la punctul „9.16.3 Separabilitate” din CA/B Forum Baseline Requirements.

9.16.4 Executare
Fără stipulare.

9.16.5 Forță majoră
AC acționează în conformitate cu legile din România privind forța majoră.

9.17 Alte prevederi
Fără stipulare.