Codul de Practici și Proceduri certSIGN SSL EV CA Clasa 3 G2 pentru certificate SSL EV

Versiunea 1.17

Data: 31 Iulie 2023

Notă importantă

Adresa: Bulevardul Tudor Vladimirescu nr. 29 A,
AFI Tech Park 1, București, România
Telefon: 004-021-31.19.901
Fax: 004-021-31.19.905

Web:www.certsign.ro

Istoric document

Versiune	Data Efectivă	Motiv	Persoana care a făcut schimbarea
1.0	Ianuarie 2018	Publicarea primei versiuni	Responsabil cu securitatea informațiilor
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 eliminare caracter de subliniere „_" în numele domeniului / dNSName – CA / Browser BR 1.6.2	Manager de politici PKI
1.5	Ianuarie 2020	Evaluare anuală. Actualizări minore pentru conformitatea 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	Actualizare OCSP și re-key	Manager de politici PKI
1.8	Septembrie 2020	Adăugare 7.2 CRL conform 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	September 2021	Ballot SC42/47/48 High Risk Cert. Requests, FQDN, OU	Manager Politici PKI
1.12	Noiembrie 2021	Extensia cabfOrganizationIdentifier	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	Actualizare CRL Reason	Manager Politici PKI
1.16	Ianuarie 2023	Revizuire anuală	Manager Politici PKI
1.17	Iulie 2023	Separare profile cap.7	Manager Politici PKI

Acest document a fost creat și este proprietatea[1]:

Proprietar	Autor	Data creării
Responsabil cu securitatea informațiilor	Responsabil cu securitatea informațiilor	Decembrie 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	September 2021
Public-Internet	Noiembrie 2021
Public-Internet	Ianuarie 2022
Public-Internet	Iunie 2022
Public-Internet	Octombrie 2022
Public-Internet	Ianuarie 2023
Public-Internet	Iulie 2023

Acest document a fost aprobat de:

Versiune	Nume	Data
1.0	Comitetul de Management a Politicilor și Procedurilor	Ianuarie 2018
1.1	Comitetul de Management a Politicilor și Procedurilor	Mai 2018
1.2	Comitetul de Management a Politicilor și Procedurilor	Iulie 2018
1.3	Comitetul de Management a Politicilor și Procedurilor	Noiembrie 2018
1.4	Comitetul de Management a Politicilor și Procedurilor	Ianuarie 2019
1.5	Comitetul de Management a Politicilor și Procedurilor	Ianuarie 2020
1.6	Comitetul de Management a Politicilor și Procedurilor	Mai 2020
1.7	Comitetul de Management a Politicilor și Procedurilor	Mai 2020
1.8	Comitetul de Management a Politicilor și Procedurilor	Septembrie 2020
1.9	Comitetul de Management a Politicilor și Procedurilor	Ianuarie 2021
1.10	Comitetul de Management a Politicilor și Procedurilor	Mai 2021
1.11	Comitetul de Management a Politicilor și Procedurilor	September 2021
1.12	Comitetul de Management a Politicilor și Procedurilor	Noiembrie 2021
1.13	Comitetul de Management a Politicilor și Procedurilor	Ianuarie 2022
1.14	Comitetul de Management a Politicilor și Procedurilor	Iunie 2022

1.15	Comitetul de Management a Politicilor și Procedurilor	Octombrie 2022
1.16	Comitetul de Management a Politicilor și Procedurilor	Ianuarie 2023
1.17	Comitetul de Management a Politicilor și Procedurilor	Iulie 2023

Conţinut

1 Introducere

Codul de Practici și Proceduri certSIGN SSL EV CA Clasa 3 G2 pentru certificate SSL EV (denumit în continuare în acest document sub numele de **CPP**) descrie în detaliu politica de certificare aplicată de CERTSIGN pentru emiterea certificatelor digitale de către Autoritatea de Certificare Intermediară certSIGN SSL EV CA Clasa 3 G2.

Structura și conținutul CPP sunt în conformitate cu recomandările RFC 3647, ultima versiune publicată a "CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" și ultima versiune publicată a "CA/B Forum Guidelines For The Issuance And Management Of Extended Validation Certificates" publicate la http://www.cabforum.org.

1.1 Prezentare generală a CPP

CPP este baza pentru CERTSIGN și Autoritatea de certificare, Autoritatea de înregistrare și funcționarea părților dependente asociate cu privire la emiterea certificatelor calificate pentru autentificarea site-ului web. De asemenea, acest document descrie regulile generale de furnizare a serviciilor de certificare, cum ar fi înregistrarea subiectului, certificarea cheii publice, rekey-ul certificatelor și revocarea certificatelor.

1.2 Numele și identificarea documentului

Documentul se numește **Codul de Practici și Proceduri certSIGN SSL EV CA Clasa 3 G2 pentru certificate SSL EV**. Următorul OID 1.3.6.1.4.1.25017.1.1.6.1 este înregistrat de CERTSIGN pentru includere în toate certificatele SSL EV.

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 auditori) și clienții (utilizatorii serviciilor furnizate):

- Autorități de certificare:
  - certSIGN SSL EV CA Clasa 3 G2
- Autoritatea de Înregistrare,
- Depozitarul,
- Protocolul de stare al certificatului online (OCSP),
- Subiecte,
- Beneficiari,
- Părțile dependente,
- Furnizori relevanți pentru CERTSIGN privind emiterea și gestionarea certificatelor digitale
- Comitetul de Management a Politicilor și Procedurilor

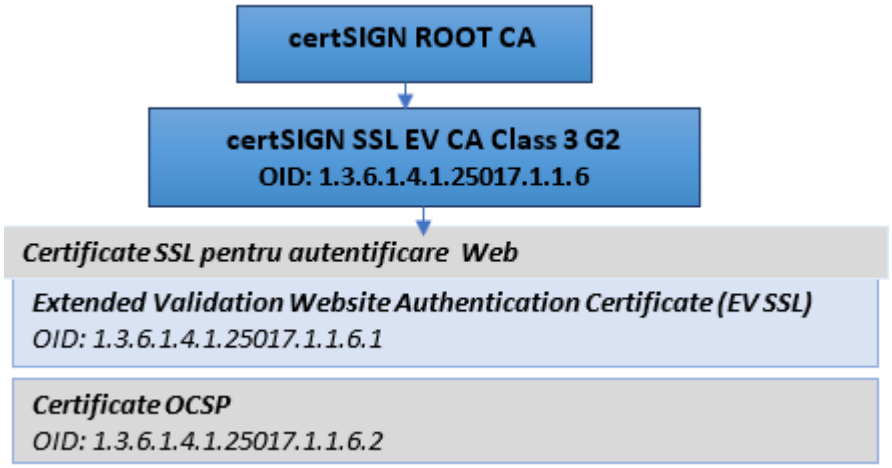
CERTSIGN oferă servicii de certificare pentru fiecare persoană fizică sau juridică care acceptă reglementările prezentului CPP. Scopul acestor practici (care includ procedurile de generare a cheilor, procedura de emitere a certificatelor și securitatea sistemului informațional) este

de a asigura utilizatorilor serviciilor CERTSIGN că nivelurile de credibilitate declarate ale certificatelor emise corespund practicilor Autorității de certificare.

1.3.1 Autorități de certificare

Autoritatea de certificare certSIGN SSL EV CA Clasa 3 G2 este o autoritate de certificare Intermediară pentru domeniul CERTSIGN, subordonată certSIGN ROOT CA.

certSIGN SSL EV CA Clasa 3 G2 este identificat prin următorul OID: 1.3.6.1.4.1.25017.1.1.6.



Autoritatea de certificare certSIGN SSL EV CA Clasa 3 G2 poate înregistra și emite certificate numai serverelor web.

1.3.2 Autoritatea de Înregistrare

Autoritatea de înregistrare primește verifică și aprobă sau respinge cererile de înregistrare și eliberare a certificatului, rekey-ul certificatului și cererile de revocare. Verificarea aplicațiilor intenționează să autentifice (pe baza documentelor anexate cererilor) atât beneficiarul, cât și datele specificate în cerere. Autoritatea de înregistrare poate depune, de asemenea, cereri către autoritatea de certificare corespunzătoare pentru a anula cererea unui subiect și a retrage certificatul acestuia.

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 certSIGN SSL EV CA Clasa 3 G2 pentru certificatele SSL EV SSL”.

1.3.3 Beneficiari

Beneficiar

Beneficiarul este o entitate juridică căreia i se eliberează un certificat și care este obligat legal de un acord de beneficiar sau de Termeni 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 la (suspiciunea) compromisului cheii private.

Subiect

Subiectul este entitatea juridică căreia i se eliberează un certificat și este identificat 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 juridică pentru care Beneficiarul solicită certificatul

Un subiect este, de asemenea răspunzător de:

- Notificarea imediată certSIGN asupra (suspiciunii) compromisului cheii private;
- Trimiterea cererilor de reînnoire a cheilor și / sau certificatelor către 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 Părțile de încredere

O parte de încredere, care utilizează serviciile CERTSIGN, poate fi orice entitate care ia decizii bazate pe corectitudinea conexiunii dintre identitatea unui subiect și cheia publică.

O parte de încredere 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 parte de încredere este dispusă să utilizeze un certificat pentru a verifica identitatea sursei sau pentru a crea un canal de comunicare sigur cu subiectul certificatului. O parte responsabilă 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

Comitetul de Management a 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.

Notari publici: pot efectua identificarea și garanția pentru identitatea reală a subiecților.

1.4 Utilizarea certificatului

Scopul certificatului SSL EV este specificat de câmpurile de utilizare cheie și de utilizare a cheilor extinse găsite în certificatul EV: keyEncipherment, digitalsignature, serverAuthentication și clientAuthentication.

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.

Certificatele SSL EV emise conform acestui CPP sunt utilizate pentru a identifica serverele web accesate prin protocolul TLS sau SSL.

1.4.1 Scopuri de utilizare

Scopurile principale ale unui SSL EV sunt:

1. Identificare entitate juridică care controlează un site web: oferire utilizatorului unui browser de internet o asigurare rezonabilă că site-ul web pe care îl accesează utilizatorul este controlat de o anumită entitate juridică identificată în SSL EV după numele, adresa sediului, jurisdicția Încorporare sau Număr de înregistrare și înregistrare sau alte informații dezambiguizante; și
2. Activează comunicațiile criptate cu un site web: facilitează schimbul de chei de criptare pentru a permite comunicarea criptată a informațiilor pe internet între utilizatorul unui browser de internet și un site web.

Scopurile secundare ale unui SSL EV sunt de a ajuta la stabilirea legitimității unei companii care pretinde că operează un site web și de a oferi un vehicul care poate fi utilizat pentru a ajuta la soluționarea problemelor legate de phishing, malware și alte forme de fraudă a identității online. Furnizând informații mai fiabile de identitate și adresă verificate de terțe părți cu privire la proprietarul companiei, SSL EV poate ajuta la:

1. Face mai dificilă montarea atacurilor de phishing și a altor fraude de identitate online folosind certificate;
2. Asistă companiile care pot fi ținta atacurilor de phishing sau a fraudei de identitate online oferindu-le un instrument pentru a se identifica mai bine utilizatorilor; și
3. Asistă organizațiile de aplicare a legii în investigațiile privind phishingul și alte fraude de identitate online, inclusiv, după caz, contactarea, anchetarea sau acționarea în justiție împotriva subiectului.

1.4.2 Scopuri excluse

SSL EV se concentrează numai pe identitatea subiectului numit în certificat și nu pe comportamentul subiectului. Ca atare, un SSL EV nu este destinat să ofere asigurări sau să reprezinte sau să garanteze în alt mod:

1. Că subiectul numit în SSL EV este implicat activ în a face afaceri;
2. Că subiectul menționat în SSL EV respectă legile aplicabile;
3. Că subiectul menționat în SSL EV este de încredere, onest sau de încredere în relațiile sale comerciale; sau
4. Că este „sigur” să faci afaceri cu Subiectul numit în SSL EV.

1.5 Administrarea politicilor

1.5.1 Organizația care administrează documentul

Prezentul document este administrat de Comitetul de Management a Politicilor și Procedurilor (PPMB) al certSIGN TSP (TSP = Prestator de servicii de incredere). 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
Fax	(+4021) 3119905
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel: 1.5.1 Organizația care administrează documentul

1.5.2 Persoană de contact

Nume	Comitetul de Management a Politicilor și Procedurilor (PPMB)
Telefon	(+4021) 3119901
Fax	(+4021) 3119905
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel: 1.5.2 Persoană de contact

Procedura de raportare a problemelor 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 determină conformitatea CPP cu politica

Nume	Comitetul de Management a Politicilor și Procedurilor
Telefon	(+4021) 3119901
Fax	(+4021) 3119905
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel: 1.5.3 Persoana care determină conformitatea CPP cu politica

1.5.4 Proceduri de aprobare CPP

Comitetul de Management al Politicilor și Procedurilor este responsabil de aprobarea CPP.
Procedura de aprobare este cuprinsă într-o instrucțiune internă.
Subiecții / Beneficiarii vor respecta CPP-ul publicat la: http://certsign.ro/repository
Subiecții / Beneficiarii care nu acceptă termenii și reglementările noi, modificate ale CPP sunt obligați să facă o declarație adecvată în termen de 15 zile de la data noii versiuni a aprobării CPP. Acest lucru duce la rezilierea contractului legat de furnizarea de servicii de certificare și revocarea certificatului emis pe teren.

1.6 Definiții și acronime

Acces - capacitatea de a utiliza și utiliza orice resursă a sistemului informațional.
Controlul accesului - procesul de acordare a accesului la resursele sistemului informațional numai utilizatorilor, aplicațiilor, proceselor și altor sisteme autorizate.
Audit - executarea unei revizuiri și evaluări independente a sistemului, cu scopul de a testa adecvarea controalelor de gestionare a sistemului implementate, pentru a verifica dacă o operațiune a sistemului este efectuată în conformitate cu politica de certificare acceptată și cu reglementările operaționale rezultate, pentru a descoperi posibile lacune de securitate și să recomande modificarea adecvată a măsurilor de control, a politicii de certificare și a procedurilor conexe.
Date de audit - înregistrări cronologice ale activităților sistemului, permițând reconstrucția și analiza succesiunii evenimentelor și modificarea sistemului, asociate evenimentului înregistrat.
Autentifica - pentru a confirma identitatea declarată a unei entități.

Autentificare - controalele de securitate care vizează asigurarea fiabilității datelor transferate, a mesajelor sau a expeditorului acestora sau a controalelor de verificare a autenticității unei persoane, înainte de livrarea unui tip clasificat de informații.
Perioada de activitate a certificatului - perioada cuprinsă între data de începere și data de încheiere a valabilității certificatului sau perioada dintre data de începere a perioadei de valabilitate a certificatului și momentul revocării acestuia
Calea de certificare- calea ordonată a certificatelor, care duce de la un certificat la un punct de încredere ales de un verificator până la un certificat supus verificării. O cale de certificare îndeplinește următoarele condiții:

- Pentru toate certificatele cert (x) incluse în calea de certificare {cert (1), cert (2), ..., cert (n-1)} subiectul certificatului cert (x) este emitentul certificatului cert (x + 1),
- Certificatul certificat (1) este emis de o autoritate de certificare (punct de încredere) de încredere de către verificator,
- cert (n) este un certificat care se verifică.

Fiecare cale de certificare poate fi legată de una sau mai multe politici de certificare sau o astfel de politică poate să nu existe. Politicile atribuite unei căi de certificare sunt intersecția politicilor ale căror identificatori sunt incluși în fiecare certificat, încorporate în calea de certificare și definite în certificatul de extensiePolicies.

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.

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.

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.

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

Revocarea certificatului- definește procedurile privind revocarea unei perechi de chei valide (revocarea certificatului) în cazul în care un acces la perechea de chei trebuie restricționat pentru a preveni posibila utilizare în criptare sau crearea semnăturii electronice. Un certificat revocat este plasat pe lista de revocare a certificatelor (CRL).

Lista de revocare a certificatului (CRL)- lista emisă periodic sau imediat, semnată electronic de către o autoritate, care permite identificarea certificatelor supuse revocării înainte de expirarea perioadei de valabilitate. CRL conține numele emitentului CRL, data publicării, data următoarei actualizări, numerele de serie ale certificatelor revocate și datele și motivele revocării acestora.

Publicarea certificatului și a listei de revocare a certificatelor - Proceduri de distribuire a certificatelor emise și a certificatelor revocate.

Furnizor de servicii de certificare - instituție de încredere (inclusiv dispozitive hardware aflate sub controlul său) parte a părților terțe de încredere care furnizează servicii capabile să creeze, să semneze și să emită certificate sau servicii de non-repudiere.

Aprobator de certificate - O persoană fizică care este fie Solicitantul, angajat de Solicitant, fie un agent autorizat care are autoritate expresă să îl reprezinte pe Solicitant pentru a (i) acționa ca Solicitant de Certificat și pentru a autoriza alți angajați sau terțe părți să acționeze ca solicitant de certificat și (ii) să aprobe cererile SSL EV transmise de alți solicitanți de certificate.

Solicitant de certificat - O persoană fizică care este fie Solicitantul, angajat de Solicitant, un agent autorizat care are autoritate expresă să îl reprezinte pe Solicitant, fie o terță parte (cum ar fi un furnizor de servicii Internet sau o companie de găzduire) care completează și trimite o Cerere SSL EV în numele aplicantul.

Cerere de confirmare - O comunicare adecvată în afara benzii care solicită verificarea sau confirmarea faptului în cauză.
Persoana care confirmă - O poziție în cadrul organizației solicitantului care confirmă faptul particular în cauză.
Semnator de contract - O persoană fizică care este fie Solicitantul, angajat de Solicitant, fie un agent autorizat care are autoritate expresă să îl reprezinte pe Solicitant și care are autoritate în numele Solicitantului să semneze Acorduri de Beneficiar.
Certificat încrucișat–– certificat de cheie publică eliberat unei autorități de certificare, care conține diferite nume ale emitentului și ale subiectului; o cheie publică a acestui certificat poate fi utilizată exclusiv pentru verificarea semnăturii electronice. Este clar indicat faptul că certificatul aparține Autorității de certificare.
Certificare încrucișată- procedura de eliberare a unui certificat de către o autoritate de certificare către o altă autoritate de certificare, care nu este afiliată direct sau indirect cu autoritatea emitentă. De obicei, se emite un certificat încrucișat pentru a simplifica construirea și verificarea căilor de certificare care conțin certificate emise de diferite CA. Emiterea unei certificări încrucișate poate fi efectuată pe baza unui acord reciproc, între două autorități de certificare care își eliberează reciproc certificate.
Modul criptografic - set format din hardware, software, microcod sau combinația acestora, efectuând operațiuni criptografice (inclusiv criptare și decriptare), executate în zona acestui modul criptografic.
Numele distinct (DN) - set de atribute care formează un nume distinct al unei entități juridice / private și care o distinge (adică entitatea) de alte entități de același tip.
Semnatura electronica- transformarea criptografică a datelor permițând destinatarului datelor să verifice originea și integritatea datelor, precum și protecția expeditorului și destinatarului împotriva falsificării de către destinatar; semnăturile electronice asimetrice pot fi generate de o entitate prin intermediul unei chei private și a unui algoritm asimetric, de exemplu RSA.
Entitate finală - entitate autorizată care utilizează certificatul ca subiect sau ca parte de încredere (nu se aplică autorităților de certificare).
Sistem informatic - întreaga infrastructură, personal și componente utilizate pentru asamblare, prelucrare, stocare, transmisie, publicare, distribuție și gestionare a informațiilor.
Transformări de stare cheie - starea unei chei poate fi modificată numai atunci când apare una dintre următoarele transformări (conform ISO / IEC 11770-1):

- Generare - proces de generare cheie; generarea cheilor trebuie efectuată în conformitate cu procedurile acceptate de generare a cheilor; procesul poate include procedura de testare, care vizează aplicarea regulilor cheie de generare,
- Activare - rezultă că cheia devine valabilă și disponibilă pentru performanța operațiunii criptografice,
- Dezactivare - constrângerea unei chei; situația poate apărea din cauza expirării perioadei de valabilitate a unei chei,
- Reactivare - permite utilizarea în continuare a cheii în starea de indisponibilitate pentru operarea criptografică,
- Distrugere - are ca rezultat încetarea ciclului cheie de viață; această noțiune înseamnă distrugerea cheii logice, dar se poate aplica și distrugerii cheii fizice.

Obiect - obiect cu acces controlat, de exemplu un fișier, o aplicație, zona memoriei principale, asamblarea și datele personale păstrate.

Identificator de obiect (OID) - identificator alfanumeric / numeric înregistrat în conformitate cu standardul ISO / IEC 9834 și care descrie în mod unic un obiect specificat sau clasa acestuia.
Cheie privată- una dintre cheile asimetrice aparținând unui subiect și utilizată numai de acel subiect. În cazul sistemului de chei asimetric, o cheie privată descrie transformarea unei semnături. În cazul sistemului de criptare asimetric, o cheie privată descrie transformarea decriptării. Cheia privată este (1) cheia al cărei scop este decriptarea sau crearea semnăturii, pentru utilizarea exclusivă a proprietarului; (2) acea cheie dintr-o pereche de chei cunoscută doar de proprietar.
Procedura pentru operațiuni în situație de urgență - procedura fiind alternativa unei căi de procedură standard și executată la apariția unei situații de urgență.
Punct de încredere- cea mai de încredere autoritate de certificare, în care un subiect sau o parte de încredere are încredere. Un certificat al acestei autorități este primul certificat din fiecare cale de certificare creat de un subiect sau de o parte care se bazează. Alegerea punctului de încredere este de obicei pusă în aplicare de politica de certificare care guvernează funcționarea entității care emite un certificat dat.
Dovada deținerii cheii private- informații transmise de un subiect într-un mod care să permită destinatarului să verifice validitatea legăturii dintre expeditor și cheia privată, accesibilă de către expeditor; metoda de a dovedi deținerea cheii private depinde de obicei de tipul de chei folosite, de exemplu, în cazul cheilor de semnare este suficient să prezentați text semnat (verificarea cu succes a semnăturii este dovada deținerii cheii private), în timp ce în cazul de criptare a cheilor, subiectul trebuie să poată decripta informațiile criptate cu o cheie publică aflată în posesia sa. certSIGN efectuează verificarea asocierilor între perechile de chei utilizate pentru semnare și criptare numai la nivelul Autorității de înregistrare și certificare.
Cheie publică- una dintre cheile din perechea de chei asimetrice a subiectului care poate fi disponibilă publicului. În cazul sistemului de criptografie asimetrică, cheia publică definește transformarea verificării semnăturii. În cazul criptării asimetrice, o cheie publică definește transformarea criptării mesajelor.
Certificat de cheie publică- o structură de date care conține cel puțin numele sau identificatorul unei autorități de certificare, identificatorul unui subiect, cheia publică a acestuia, perioada de valabilitate, numărul de serie și cel atribuit de către autoritatea de certificare. Un certificat poate fi în una dintre cele trei stări de bază: așteptarea activării, activ și inactiv.
Infrastructură cu cheie publică (PKI)- arhitectură, tehnici, practici și proceduri care sprijină în mod colectiv implementarea și operarea sistemelor de criografie cu cheie publică bazate pe certificate; PKI constă din hardware, software, baze de date, resurse de rețea, proceduri de securitate și obligații legale legate împreună, care colaborează pentru a furniza și implementa servicii de certificat, precum și alte servicii, asociate cu infrastructura (de exemplu, timbru).
Certificat calificat pentru semnătură electronică - un certificat pentru semnături electronice, eliberat de un furnizor de servicii de încredere calificat și care îndeplinește cerințele stabilite în anexa I la Regulamentul (UE) 910/2014;
Certificat calificat pentru sigiliul electronic - un certificat pentru un sigiliu electronic, eliberat de un furnizor calificat de servicii de încredere și care îndeplinește cerințele stabilite în anexa III la Regulamentul (UE) 910/2014;

Dispozitiv de creare a semnăturii electronice calificat înseamnă un dispozitiv de creare a semnăturilor electronice care îndeplinește cerințele stabilite în anexa II la Regulamentul (UE) 910/2014
Certificat calificat pentru autentificarea site-ului web înseamnă un certificat de autentificare a site-ului web, eliberat de un furnizor de servicii de încredere calificat și care îndeplinește cerințele stabilite în anexa IV;
Regulamentul (UE) nr. 910/2014- REGULAMENTUL (UE) nr. 910/2014 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93 / CE
Certificat revocat - certificat de cheie publică plasat pe lista de revocare a certificatului.
Solicitant - Subiect în perioada dintre depunerea unei cereri către o autoritate de certificare și finalizarea procedurii de eliberare a certificatului
Parte de încredere - destinatarul care a primit informații care conțin un certificat sau o semnătură electronică asociată verificată cu o cheie publică inclusă în certificat și care trebuie să decidă dacă acceptă sau respinge semnătura pe baza încrederii pentru certificat.
Cheie secreta - cheie aplicată în tehnici de criptografie simetrică și utilizată numai de un grup de subiecți autorizați.
Deținător secret comun - titularul autorizat al unui card electronic, utilizat pentru stocarea secretului comun.
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.
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.
Politica de semnătură - soluții detaliate, inclusiv soluții tehnice și organizaționale, care definesc metodele, domeniul de aplicare și cerințele de confirmare și verificare a unei semnături electronice, a căror executare permite verificarea validității semnăturii.
Secret împărtășit - o parte dintr-un secret criptografic, de ex. O cheie distribuită între n persoane de încredere (jetoane criptografice, de ex. Carduri electronice) într-un mod, care necesită m părți ale secretului (unde m <n) pentru a restabili cheia distribuită.
State de cheie privată - cheile private pot avea una dintre cele trei stări de bază (conform standardului ISO / IEC 11770-1):

- **Se așteaptă activarea (gata)** - cheia a fost deja generată, dar nu este accesibilă pentru utilizare;
- **Activ** - cheia poate fi utilizată în operațiuni criptografice (de exemplu, pentru crearea de semnături electronice)
- **Inactiv** - cheia poate fi utilizată exclusiv pentru decriptare și perechea sa publică pentru verificarea semnăturii electronice.

Token - element de date utilizat pentru schimbul între părți și care conține informații transformate prin intermediul tehnicilor criptografice. Tokenul este semnat de un operator al Autorității de înregistrare și poate fi utilizat pentru autentificarea titularului său în contactul cu o autoritate de certificare.

Terță parte de încredere (TTP) - instituție sau reprezentantul său de încredere de către o entitate autentificată, o entitate care efectuează verificarea și alte entități din zona operațiunilor asociate securității și autentificării.
Validarea certificatelor de cheie publică- verificarea stării certificatului, permițând validarea dacă certificatul este revocat sau nu. Această problemă poate fi rezolvată de singura entitate interesată pe baza CRL sau printr-o cerere, direcționată către serverul OCSP.
Certificat valid - certificatul de cheie publică este valabil numai atunci când (1) a fost emis de o autoritate de certificare, (2) a fost acceptat de subiect și (3) nu a fost revocat.
Perioada de valabilitate: Înainte de 2020-09-01, perioada de timp măsurată de la data emiterii certificatului până la data de expirare. Pentru certificatele emise la sau după 2020-09-01, perioada de valabilitate este definită în RFC 5280, secțiunea 4.1.2.5: perioada de timp de la notBefore la notAfter, inclusiv.

CA	Autoritatea de certificare
CP	Politica de certificare
CAA	Autorizarea autorității de certificare
ccTLD	Codul țării Domeniul de nivel superior
CPP	certificat Declarație de practică
CRL	Lista revocării certificatului
DN	Nume distins
DNS	numele domeniului
EV	Validare extinsă
gTLD	domeniu generic de nivel superior
IANA	Autoritatea numerelor atribuite prin internet
ICANN	Internet Corporation pentru nume și numere atribuite
LRA	Autoritatea de înregistrare locală
OSCP	Protocol de stare al certificatului on-line
OV	Organizare validată
PKI	Infrastructură de cheie publică
PPMB	Comitetul de Management a Politicilor și Procedurilor
PRA	Autoritatea de înregistrare primară
PSE	Mediul de securitate personală
QSCD	Dispozitiv de creare a semnăturii electronice calificat
QCP-w	Politica de certificare calificată pentru autentificarea site-ului web
SSL EV	Certificat calificat pentru autentificarea site-ului web
RSA	Rivest, Shamir, Adleman algoritm criptografic asimetric
TLD	Domeniul de nivel superior
TLS	Securitatea stratului de transport
TSP	Furnizor de servicii de încredere
TTP	Terță parte de încredere

2 Responsabilități de publicare și depozit

2.1 Depozite

Depozitul este disponibil on-line: http://www.certsign.ro/repository. Contine:

- Politica de certificat și Declarația de practică a certificatului pentru CA-urile operate de certSIGN
- Certificatele ROOT CA și certificatele CA Intermediare
- Certificatele subiectelor
- Liste de revocare a certificatelor
- Termeni și condiții pentru utilizarea certificatelor digitale
- Șabloane pentru contracte cu subiecții și beneficiarii

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

- Facă toate eforturile necesare pentru a vă asigura că toate certificatele publicate în depozit aparțin subiecților înregistrați în certificate și subiecții și-au dat acordul cu privire la aceste certificate,
- Asigure că certificatele autorităților de certificare, ale autorității de înregistrare aparținând domeniului certSIGN, precum și certificatele subiectului sunt publicate și arhivate la timp,
- Asigure publicarea și arhivarea politicii de certificare, a CPP, a listelor aplicațiilor și a dispozitivelor recomandate,
- Permite accesul la informații despre starea certificatului prin publicarea listelor de revocare a certificatelor (CRL), prin intermediul serverelor OCSP sau a întrebărilor către HTTP,
- Asigură accesul constant la informații în depozitul pentru autoritățile de certificare, autoritatea de înregistrare, subiecți și părțile care se bazează,
- Publică CRL-uri sau alte informații în timp util și în conformitate cu termenele menționate în Politica de certificare,
- Asigură accesul securizat și controlat la informațiile din depozit.

Răspunderea pentru serviciul Repository și consecințele serviciului aparțin certSIGN (vezi Capitolul 9).

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* publicate la http://www.cabforum.org. În eventuale neconcordanțe între acest document și acele cerințe, respectivele Cerințele au prioritate față de acest document.

CERTSIGN găzduiește pagini web care permit furnizorilor de aplicații software să testeze software cu certificate de beneficiar emise de certSIGN SSL EV CA Clasa 3 G2:

https://testssl.certsign.ro/

CERTSIGN pune la dispoziția părților de încredere termenii și condițiile privind utilizarea certificatelor SSL EV.

2.3 Timpul sau frecvența publicării

Informațiile publicate de CERTSIGN sunt actualizate cu următoarea frecvență:

- Politica de Certificare și CPP – revizuire anuală și 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 revocării certificatelor - 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 accesibil prin http://www.certsign.ro/repository. Depozitul este disponibil public și internațional, 24 * 7 * 365

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

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

Capitolul descrie regulile generale pentru identificarea beneficiarului, reguli care se aplică la emiterea unui SSL EV de către CERTSIGN.

Verificarea este obligatorie efectuată în etapa înregistrării și modificării beneficiarului, precum și la cererea CERTSIGN în cazul oricărui alt serviciu de certificare.

3.1 Denumire

Numele subiectului dintr-un SSL EV sunt conforme cu convenția de numire, așa cum este stabilită în Ghidurile EV și BR, "*Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates",* publicate de CA / Browser Forum.

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).
Certificatele emise în conformitate cu prezentul CPP sunt semnificative numai dacă numele care apar în certificate pot fi înțelese și utilizate de către părțile care se bazează. Numele utilizate în certificate trebuie să identifice într-un mod semnificativ site-ul web căruia îi sunt atribuite.

Atributul Distinguished Name este unic pentru subiectul căruia îi este emis. Pentru fiecare SSL EV, este emis un număr de serie unic în spațiul de nume al certSIGN SSL EV CA Clasa 3 G2.

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). Numele de bază ale subiecților și ale emitenților de certificate plasate în certificatele certSIGN sunt conforme cu numele 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.

3.1.2 Nevoia ca numele să aibă înțeles logic

Pentru certificatele SSL, numele FQDN poate fi plasat în atributul Common Name (CN) din câmpul Subject. Dacă este prezent în CN, acesta trebuie 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 versiunea actuală a recomandărilor CA / Browser Forum BR. FQDN cuprinde doar "P-labels" și „Non-Reserved LDH-labels".

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.

Pentru persoanele juridice, DN constă din următoarele câmpuri opționale (descrierea câmpului este urmată de abrevierea sa care respectă recomandările X.520):

- Câmpul C - abrevierea internațională pentru numele țării (RO pentru România),
- Câmpul O - numele organizației,
- Câmpul OU - numele departamentului organizației[1],
- Câmpul S - județ / district în care funcționează organizația,
- Câmpul L - orașul de reședință al subiectului,
- Câmpul CN - numele de domeniu al instituției,
- Câmpul Phone - număr de telefon,
- Identificator organizare câmp - Un identificator oficial unic al beneficiarului ca persoană juridică

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

Nu se aplică.

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

Nu se aplică.

3.2 Validarea inițială a identității

Înainte de a emite un SSL EV, CA se asigură că toate informațiile despre organizația subiectului din certificat sunt conforme cu cerințele și au fost verificate în conformitate cu procedurile prescrise în acest CPP, cu liniile directoare EV publicate de CA/B Forum și cu meciurile informațiile confirmate și documentate de RA în conformitate cu procesele sale de verificare. Astfel de procese de verificare sunt destinate să realizeze următoarele:

1. Verifică existența și identitatea solicitantului, inclusiv;
   a. Verifică existența legală și identitatea solicitantului (așa cum este stipulat în Orientările EV),
   b. Verifică existența fizică a solicitantului (prezența companiei la o adresă fizică) și
   c. Verifică existența operațională a solicitantului (activitatea comercială).
2. Verifică autorizația solicitantului pentru SSL EV, inclusiv;
   a. Verifică numele, titlul și autoritatea semnatarului contractului, aprobatorului de certificat și
3. Solicitant certificat;

[1] Interzis în cazul în care certificatul este eliberat la sau după 1 septembrie 2022

a. Verifică dacă semnatarul contractului a semnat contractul de abonament; și
b. Verifică dacă un aprobator de certificat a semnat sau a aprobat în alt mod solicitarea SSL EV.

4. Verifică dacă solicitantul este un titular înregistrat sau are controlul exclusiv al numelui de domeniu care urmează să fie inclus în SSL EV.

3.2.1 Metoda de a dovedi posesia cheii private

RA efectuează teste de probă a posesiei pentru CSR-uri create folosind algoritmi reversibili asimetrici (cum ar fi RSA) prin validarea semnăturii pe CSR prezentată de solicitant cu cererea SSL EV.

3.2.2 Autentificarea identității entității juridice

RA care operează sub certSIGN SSL EV CA Clasa 3 G2 va efectua o verificare a oricăror identități organizaționale prezentate de un Solicitant sau Beneficiar. Determină dacă identitatea organizațională, existența legală, existența fizică, existența operațională și numele de domeniu furnizate împreună cu o aplicație SSL EV sunt în concordanță cu cerințele stabilite în Ghidurile EV publicate de CA / Browser Forum. Informațiile și sursele utilizate pentru verificarea aplicațiilor SSL EV pot varia în funcție de jurisdicția solicitantului sau a beneficiarului. Conform prezentului CPP, CERTSIGN va accepta numai aplicații SSL EV de la entități pentru care existența poate fi confirmată în România.

În România, autoritatea cu drepturi de înregistrare pentru companiile comerciale din toată România este Oficiul Național al Registrului Comerțului, https://www.onrc.ro/index.php/en/

certSIGN PPMB poate, la discreția sa, să actualizeze practicile de verificare pentru a îmbunătăți procesul de verificare a identității organizației. Orice modificare a practicilor de verificare va fi publicată în conformitate cu procedurile standard de actualizare a SPC.

3.2.2.1 Starea organizației

CERTSIGN verifică dacă beneficiarul este o organizație existentă și legitimă.

Ca dovadă că este o organizație existentă și legitimă, CERTSIGN cere și verifică cel puțin următoarele documente:

- Pentru organizațiile publice / guvernamentale, un extras recent certificat (vechi de până la o lună) în guvernul comerțului, Camera de Comerț sau orice lege, act sau un decret guvernamental care prevede reprezentantul (sau reprezentanții) competent;
- Pentru organizațiile private, un extras recent certificat (până la o lună) din Registrul comerțului național.

Ca dovadă că este o organizație legală, TSP verifică dacă este în ultima listă UE a persoanelor teroriste interzise și de prevenire a organizațiilor, publicată de Consiliul European.

Aceste liste pot fi găsite pe web:

http://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX:32017D1426

CERTSIGN nu va emite certificat SSL EV unei organizații care se află pe această listă.

3.2.2.2 Numele Organizatiei

CERTSIGN verifică dacă numele organizației care este inclus în certificat, este corect și complet și corespunde cu numele organizației înregistrate de beneficiar

Ca dovadă a corectitudinii denumirii oficiale declarate, CERTSIGN va obține și verifica cel puțin următoarele documente:

Organizații private: Un extras recent certificat (până la o lună) din Registrul Comerțului al Camerei de Comerț. Mai mult, în dovezile furnizate, entitatea organizațională ar trebui să se distingă de orice alte organizații cu același nume. Un extras din Registrul comerțului național conține aceste informații

Entități guvernamentale: Informațiile de mai sus referitoare la existența legală și identitatea unei entități guvernamentale pot fi furnizate și de o entitate guvernamentală superioară din aceeași subdiviziune politică ca solicitantul (de exemplu, un secretar de stat poate verifica existența legală a unui departament de stat specific),

Organizații internaționale: Existența legală și identitatea pot fi confirmate:

(a) Cu referire la documentul constitutiv în baza căruia a fost constituită Organizația Internațională; sau
(b) direct cu guvernul unei țări semnatare (adică de la o agenție guvernamentală corespunzătoare sau din legile țării respective sau verificând dacă guvernul țării are misiunea de a-l reprezenta la Organizația Internațională); sau
(c) Direct împotriva oricărei liste actuale de entități calificate pe care Forumul CAB le poate menține
www.cabforum.org. În cazurile în care Organizația Internațională care solicită SSL EV este un organ sau agenție - inclusiv o organizație neguvernamentală (ONG) a unei Organizații Internaționale verificate, atunci CERTSIGN poate verifica solicitantul Organizației Internaționale direct cu umbrela verificată Organizația Internațională a cărei solicitantul este un organ sau o agenție.

3.2.2.3 Adresa organizației

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

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

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

- Pentru verificarea publică / guvernamentală se efectuează împotriva serviciului public de verificare online de pe mfinante.ro (Ministerul Finanțelor);
- Pentru organizațiile private și necorporate un extras recent certificat (până la o lună) din Registrul comerțului național.

În cazul în care adresa din documentele justificative corespunde cu adresa cererii, CERTSIGN va considera că este suficientă dovada că aceasta este adresa la care organizația își desfășoară activitatea.

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

- Verificați dacă afacerea solicitantului se află la adresa exactă specificată în cererea SSL EV (de exemplu, prin semnalizare permanentă, confirmarea angajaților etc.) ;;
- Identificați tipul de facilitate (de exemplu, birou într-o clădire comercială, reședință privată, vitrina etc.) și dacă acesta pare a fi o locație permanentă de afaceri;;

- Indicați dacă există un semn permanent (care nu poate fi mutat) care identifică solicitantul;
- Indicați dacă există dovezi că Solicitantul desfășoară activități comerciale în desfășurare pe site (de exemplu, că nu este vorba doar de un e-mail, căsuță poștală etc.) și
- Includeți una sau mai multe fotografii ale (i) exteriorului site-ului (afișând semnalizări care indică numele solicitantului, dacă este prezent și afișează adresa străzii dacă este posibil) și (ii) zona interioară de recepție sau spațiul de lucru ..

Ca alternativă, CERTSIGN va accepta o declarație a notarului care indică adresa specificată

este adresa la care organizația își desfășoară activitatea

3.2.2.4 Verificarea telefonului organizației

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

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

- Apelează numărul de telefon și obține un răspuns afirmativ suficient pentru a permite unei persoane rezonabile să concluzioneze că Solicitantul este accesibil prin telefon la numărul apelat; și
- Confirmă numărul de telefon general al organizației, așa cum este listat în cea mai recentă versiune a (Pagini Aurii) (online) - https://www.paginiaurii.ro/;

Alternativ, în timpul unei vizite la fața locului, persoana care efectuează vizita la fața locului poate suna la numărul de telefon furnizat și poate încheia vorbind cu persoana prezentă pe site-ul solicitantului în timpul vizitei - care este, de asemenea, la telefon cu persoana care sună - că Solicitantul este accesibil telefonic la numărul apelat; cu condiția ca numărul confirmat să nu fie un telefon mobil.

3.2.2.5 Existența operațională

Beneficiarii SSL EV trebuie să îndeplinească cerința „existenței operaționale”, care se presupune dacă Solicitantul a funcționat de trei (3) ani sau mai mult. Dacă există de mai puțin de trei ani, după cum se indică în evidențele Agenției Guvernamentale, atunci acestea trebuie să fie listate în informațiile curente furnizate de o sursă de informații calificată independentă sau trebuie să aibă un cont de depozit la cerere activ curent cu o instituție financiară reglementată, care poate fi înființată cu documentația autentificată primită direct de la o instituție financiară reglementată care să verifice dacă Solicitantul are un cont de depozit la cerere activ la instituție.

3.2.2.6 Validarea autorizării sau controlului domeniului

Liniile directoare impun solicitantului:

a. Este titularul înregistrat al numelui de domeniu; sau

b. I s-a acordat dreptul exclusiv de a utiliza numele de domeniu de către titularul înregistrat al numelui de domeniu; și că Solicitantul este la curent cu înregistrarea sau controlul exclusiv al numelui de domeniu.

Verificarea autorizației și a identității reprezentantului persoanei juridice care depune cererea în numele acestei entități se face în conformitate cu capitolul. 3.2.2.4.2 și 3.2.2.4.4, CA / Browser Forum BR:

CERTSIGN va trimite un e-mail construit către contactul de domeniu pentru a confirma că Solicitantul este conștient de această proprietate sau 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 („@")), urmată de numele de domeniu de autorizare sau la adresa de e-mail de contact a domeniului 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.

3.2.3 Autentificarea identității entității naturale

RA care operează sub certSIGN SSL EV CA Clasa 3 G2 va efectua o verificare a identității și autorității semnatarului contractului, a aprobatorului de certificat și a solicitantului de certificat asociat cu cererile SSL EV, care sunt trimise de un solicitant sau un beneficiar. Pentru a stabili acuratețea unei identități individuale, AR trebuie să efectueze verificarea identității și a autorității în concordanță cu cerințele stabilite în Ghidurile EV publicate de CA / Forumul browserului.

certSIGN PPMB poate, la discreția sa, să actualizeze practicile de verificare pentru a îmbunătăți procesul de verificare a identității organizației. Orice modificare a practicilor de verificare va fi publicată în conformitate cu procedurile standard de actualizare a SPC.

3.2.4 Informații despre beneficiar ne-verificate

CERTSIGN nu include informații neconfirmate despre beneficiar în certificate. CERTSIGN nu este responsabil pentru informațiile despre beneficiar non-verificate transmise către CERTSIGN sau transmise în alt mod cu intenția de a fi incluse într-un certificat. 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

Pentru certificatele eliberate la cererea agentului unui Beneficiar, atât agentul, cât și Beneficiarul vor despăgubi și solidar CERTSIGN, precum și companiile sale mamă, filialele, directorii, ofițerii, angajații, agenții și contractanții.

Beneficiarul va controla și va fi responsabil pentru datele pe care un agent al Beneficiarului le furnizează CERTSIGN. Beneficiarul trebuie să notifice prompt CERTSIGN cu privire la orice denaturări și omisiuni făcute de un agent al Beneficiarului. Datoria acestui articol este continuă.

Autoritatea persoanelor fizice - semnatari de contracte, aprobatori de certificate și solicitanți de certificate - de a acționa în calitate de agenți ai beneficiarului este confirmată prin primirea unei scrisori de autoritate SSL EV / Acord principal de la beneficiar semnat de o persoană cu autoritate (de exemplu, o „persoană care confirmă") .

(1) Cerere de confirmare. Persoanele care au o astfel de autoritate sunt contactate de CERTSIGN printr-o comunicare adecvată, în afara celor uzuale, care solicită verificarea sau

confirmarea faptului particular în cauză, adică autorizarea persoanei în calitate de semnatar de contract, aprobator de certificat sau solicitant de certificat.

(A) Destinatar. Solicitarea pentru scrisoarea / acordul de autoritate SSL EV este adresată către:

a. Un post din cadrul organizației solicitantului care se califică ca persoană confirmatoare (de exemplu, secretar, președinte, director executiv, director financiar, director financiar, director general, director general, etc.) și care este identificat după nume și titlu într-un extras actual al Registrului comerțului național , un aviz juridic verificat, o scrisoare contabilă verificată sau contactând Departamentul de resurse umane al solicitantului prin telefon sau poștă (la numărul de telefon sau la adresa sediului solicitantului, verificat în conformitate cu liniile directoare); sau
b. Agentul înregistrat al solicitantului, persoana principală înregistrată sau sediul social în jurisdicția de încorporare sau înregistrare, așa cum este listat în evidențele oficiale ale agenției guvernamentale, cu instrucțiuni ca acesta să fie transmis unei persoane confirmatoare corespunzătoare; sau
c. O persoană desemnată, verificată că se află în linia directă de management deasupra persoanei verificate

Semnatar sau aprobator de certificat contactând Departamentul de Resurse Umane al Solicitantului prin telefon sau poștă (la numărul de telefon sau la adresa sediului solicitantului, verificat în conformitate cu Orientările EV).

(B) Mijloace de comunicare. Pe baza (A) de mai sus, Cererea de confirmare este îndreptată către persoana care confirmă într-un mod rezonabil de probabil să ajungă la această persoană. Următoarele opțiuni sunt acceptabile:

(i) În cazul în care cererea / Acordul principal al autorității EV este trimisă prin poștă pe hârtie, aceasta se adresează:

(a) la adresa verificată a sediului solicitantului;

(b) la adresa comercială a unei astfel de persoane confirmatoare specificată într-un extras curent din Registrul comerțului național, un aviz juridic verificat sau o scrisoare contabilă verificată; sau

(c) la adresa agentului înregistrat sau a sediului înregistrat al solicitantului listată în evidențele oficiale ale jurisdicției de încorporare sau înregistrare.

(ii) În cazul în care cererea pentru Scrisoarea / Acordul principal al autorității SSL EV este trimisă prin e-mail, aceasta se adresează adresei de e-mail a Persoanei care confirmă, furnizată de Departamentul de resurse umane al solicitantului în conformitate cu (A) de mai sus, sau așa cum este listat în extrasul din Registrul comerțului național, un aviz juridic verificat sau o scrisoare contabilă verificată.

(iii) În cazul în care solicitarea pentru Scrisoarea / Acordul principal al autorității SSL EV se face prin apel telefonic, atunci persoana care confirmă este contactată apelând numărul de telefon principal verificat de la locul de activitate al solicitantului, solicitând să vorbească cu această persoană și cu persoana respectivă. preluarea apelului se identifică ca pe o persoană.

(iv) Când o cerere pentru scrisoarea / acordul de autoritate SSL EV este trimisă prin fax, atunci aceasta este trimisă la numărul de fax listat într-o sursă actuală de informații guvernamentale calificate, o sursă de informații calificată independentă, un aviz juridic verificat sau un Scrisoare contabilă verificată cu coperta faxului adresată în mod clar Persoanei care confirmă.

(2) Răspuns de confirmare. Primirea de către CERTSIGN a Scrisorii / Acordului Master al Autorității SSL EV de la Persoana care confirmă este verificată prin telefon, e-mail sau altă comunicare scrisă între CERTSIGN și Persoana care confirmă.

(3) Verificarea numelui, titlului și autorității semnatarului contractului și aprobatorului de certificat. Liniile directoare impun ca CERTSIGN să verifice numele, titlul și autoritatea semnatarilor contractului și a aprobatorilor de certificate. Scrisoarea / Acordul principal al autorității SSL EV îndeplinește aceste obiective prin furnizarea unei confirmări independente din partea solicitantului a unui astfel de nume, titlu și autoritate, așa cum este subliniat mai sus. Atestările din Scrisoarea / Acordul principal al autorității SSL EV includ autoritatea de angajare și semnare a semnatarului contractului și autoritatea de angajare și aprobare a aprobatorului de certificat.

(4)În conformitate cu secțiunea 22 (d) (3) din Orientări, CERTSIGN se poate baza pe o persoană confirmatoare confirmată pentru a-și confirma propriile informații de contact: adresa de e-mail, numărul de telefon și numărul de fax. CERTSIGN se poate baza, de asemenea, pe aceste informații de contact verificate pentru corespondența viitoare cu persoana care confirmă dacă:

(i) Domeniul adresei de e-mail este deținut de solicitant și este adresa de e-mail a persoanei care confirmă și nu un alias de e-mail de grup.

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

3.2.6 Criterii de interoperare
Nu se aplică.

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
Consultați secțiunile 4.9.1 până la 4.9.3 pentru informații despre procedurile de revocare a certificatelor.

3.4 Identificare și autentificare pentru cererea de revocare
Un beneficiar poate solicita revocarea SSL EV în orice moment, cu condiția ca beneficiarul să poată valida către RA care a procesat cererea SSL EV a beneficiarului că beneficiarul este organizația căreia i-a fost emis SSL EV. RA va autentifica o cerere a unui beneficiar de revocare a SSL EV a acestora, cerând codul de revocare primit de beneficiar la aplicația SSL EV și / sau o parte din informațiile furnizate de beneficiar cu aplicația SSL EV. După primirea

și confirmarea acestor informații, RA va procesa cererea de revocare, după cum se stipulează la 4.9.

4 Cerințe operaționale privind ciclul de viață al certificatului

Acest capitol descrie procedurile de bază care sunt comune tuturor tipurilor de certificate de subiect în cadrul procesului de certificare.
Procedurile detaliate referitoare la serviciile componente PKI (CA-uri, RA-uri, semnatari CRL-uri, răspuns OCSP, autoritate de marcare a timpului etc.) și personalitățile / rolurile aferente implicate în procesul operațional al acestor componente sunt descrise în documentația internă confidențială.
Următoarea secțiune oferă o descriere a acestor documente care pot fi divulgate public.
În general, procesul de certificare începe cu subiectul: trimiterea indirectă a unei cereri (după confirmarea originală a cererii de către autoritatea de înregistrare). Pe baza cererii, Autoritatea de certificare ia o decizie cu privire la furnizarea / respingerea serviciului solicitat. Solicitările trimise trebuie să conțină informațiile necesare pentru identificarea corectă a subiectului și a beneficiarului.
certSIGN oferă acces la următoarele servicii de bază:

a. înregistrare, certificare, rekey;
b. revocarea certificatului;
c. verificarea disponibilității certificatului.

Program de lucru
Serviciile sunt prestate atât online, cât și la ghișeu. Serviciile online sunt prestate continuu, în timp ce cele de la ghișeu sunt prestate de luni până vineri, între orele 9 și 18. Pentru toate clasele de certificate, serviciile de revocare a certificatelor sunt prestate în maxim 24 de ore de la solicitare.

4.1 Cerere de certificat

Pentru a obține un SSL EV, un Solicitant trebuie:

a. Să genereze o pereche de chei sigură și criptografică,
b. Să fie de acord cu toți termenii și condițiile CPP și ale Acordului contractual și
c. Să completeze și să trimită o cerere SSL EV, oferind toate informațiile solicitate de un RA.

Următoarele roluri ale solicitantului (consultați Ghidurile EV pentru o definiție a fiecărui rol) sunt necesare pentru eliberarea unui EV SSL:

- Solicitant de certificat - Solicitarea SSL EV trebuie să fie semnată și transmisă de un Solicitant de certificat autorizat.
- Aprobator de certificat - Cererea SSL EV trebuie să fie revizuită și aprobată de un aprobator de certificat autorizat.
- Semnatar de Contract - Un acord de contractare aplicabil SSL EV solicitat trebuie să fie semnat de un semnatar de contract autorizat.

O persoană poate fi autorizată de solicitant să îndeplinească unul, două sau toate aceste trei roluri. Un solicitant POATE autoriza, de asemenea, mai multe persoane să îndeplinească fiecare dintre aceste roluri.
După finalizarea de către Solicitant a cererii SSL EV și acceptarea termenilor și condițiilor prezentului CPP și a Acordului de abonament, RA urmează procedurile descrise în capitolele 3.2.2, 3.2.3, 3.2.5 pentru a efectua verificarea informațiilor conținute în aplicația SSL EV. În cazul în care verificarea efectuată de un RA are succes, RA poate solicita, la propria sa discreție, emiterea către Solicitant a unui SSL EV de la certSIGN SSL EV CA Clasa 3 G2. Dacă

un RA refuză să solicite emiterea unui SSL EV, RA trebuie (i) să depună eforturi rezonabile din punct de vedere comercial pentru a notifica solicitantul prin e-mail cu privire la orice motive ale refuzului și (ii) să ramburseze cu promptitudine orice sume care au fost plătite în legătură cu aplicația SSL EV.
În cazul verificării cu succes a unei cereri SSL EV, RA va trimite o cerere către un CA EV pentru emiterea unui SSL EV și va notifica Solicitantul prin e-mail odată ce un SSL EV a fost emis de CA EV. Solicitantului i se va furniza o adresă URL care poate fi utilizată pentru recuperarea SSL EV.

4.1.1 Autorizarea autorității de certificare

CERTSIGN verifică înregistrările autorizației autorității de certificare (CAA) în conformitate cu RFC 6844 ca parte a procesului de verificare a domeniului.
Dacă există o înregistrare CAA care nu listează CERTSIGN ca CA autorizată, un RA va verifica utilizarea numelui de domeniu în ciuda înregistrării CAA.

4.1.2 Cine poate depune o cerere de certificat

certSIGN SSL EV CA Clasa 3 G2 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. Aceste informații sunt utilizate pentru a identifica solicitările ulterioare de certificate suspecte.

4.1.3 Procesul de înscriere și responsabilitățile

Procesul de înscriere este gestionat de o entitate specifică care este denumită Autoritatea de înregistrare sau RA sub responsabilitatea CERTSIGN.
CERTSIGN asigură infrastructura și resursele operaționale pentru funcționarea RA. CERTSIGN oferă, de asemenea, supraveghere, asistență și audit pentru toate procesele și serviciile RA.
RA este responsabilă pentru verificarea următoarelor elemente:

- Identitatea revendicată a Beneficiarului,
- Atributele revendicate ale Beneficiarului,
- Dreptul Beneficiarului la certificatul (certificatele) solicitat (e)

Procesul de înscriere se realizează în conformitate cu regulile și metodele descrise în prezentul CPP și în orientările și procedurile interne ale RA.
Următoarele roluri de solicitant sunt necesare pentru eliberarea unui SSL EV:

- Solicitant de certificat - Formularul de cerere SSL EV TREBUIE să fie trimis de un Solicitant de certificat autorizat.
- Aprobator de certificat - Formularul de cerere SSL EV TREBUIE să fie aprobat de un aprobator de certificat autorizat.
- Semnatar de Contract - Un acord de beneficiar aplicabil pentru SSL EV solicitat TREBUIE să fie semnat de un semnatar de contract autorizat.

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

1. O cerere de certificat, care poate fi electronică; și
2. Un acord contractual executat sau Termeni de utilizare, care pot fi electronici.

Beneficiarului i se furnizează următoarele informații care formează Acordul de beneficiar:

- Formularul de înregistrare
- Termenii și condițiile certificatului

- Adresa de referință online a CPP și CP
- Statute, avize sau alte documente furnizate de Beneficiar (care urmează să fie definite în Acordul Beneficiarului)

Formularul de înscriere semnat este considerat acceptarea formală de către beneficiar a acordului de beneficiar prin care beneficiarul acceptă următoarele:

- Responsabilitatea sa că informațiile furnizate către RA sunt corecte, complete, valabile și actualizate,
- Ca CERTSIGN să mențină o perioadă de păstrare de minimum 10 ani de la data certificatului eliberat, toate informațiile referitoare la înregistrare și înscriere, cererea de certificat, revocarea certificatului
- Că, în cazul în care CERTSIGN (ca CA și RA) își încetează activitățile, aceste date pot fi transferate către o terță parte, respectând aceiași termeni și condiții definite în Acordul de beneficiar,
- Recunoaște drepturile, obligațiile și responsabilitățile certSIGN și ale celorlalți participanți la PKI, astfel cum sunt definite în acordul de beneficiar și de legislația națională;
- Beneficiarul are obligația de a informa certSIGN despre orice schimbări sau evenimente care pot afecta valabilitatea sau conținutul certificatului

Informațiile extrase din CSR PKCS # 10, adică, numele companiei din denumirea organizațională (de exemplu, O = CERTSIGN SA) și numele domeniului din numele comun (CN = www.certsign.ro) conținut în PKCS # 10 CSR este verificat împotriva denumirii juridice complete a organizației (și, dacă este cazul, a oricărui nume asumat) din cerere. Dacă numele comun nu se potrivește, Solicitantul certificatului trebuie să facă corecțiile necesare și să genereze și să trimită din nou un nou PKCS # 10 pentru a continua. (Dacă alte informații nu se potrivesc, un nou PKCS # 10 poate fi sau nu necesar, în funcție de platforma serverului.) Personalul de înregistrare CERTSIGN compară informațiile transmise de Solicitant pentru a se asigura că este în concordanță cu informațiile. primite sub capul de titlu. 3.2.2.4.4, înregistrarea BR CA / Browser Forum înainte de a permite continuarea procesului de aplicare.

4.2 Procesarea cererii de certificat

În timpul procesului de aprobare a certificatului, personalul de înregistrare CERTSIGN folosește controale pentru a valida identitatea beneficiarului și alte informații prezentate în cererea de certificat. Personalul de înregistrare CERTSIGN revizuiește informațiile despre cerere furnizate de solicitant pentru a asigura conformitatea cu liniile directoare.

Următorii pași descriu etapele din Procesarea cererii de certificat:

Pașii 1: Solicitantul de certificat completează formularul de solicitare a certificatului, PKCS # 10 CSR, numele comun, informațiile organizaționale, adresa și informațiile de facturare împreună cu semnătura sa electronică sau formatul fizic cu semnătură scrisă de mână. Solicitantul trimite alte informații solicitate către CERTSIGN, inclusiv numele de contact ale personalului din cadrul organizației care are autoritatea de a aproba cererea și de a semna Acordul contractual. Solicitantul furnizează un ordin de cumpărare pentru a verifica plata pentru procesarea cererii și emiterea SSL EV.

Pasul 2: CERTSIGN verifică toate informațiile care trebuie verificate de Orientări folosind o varietate de surse, inclusiv Registrul Comerțului Național, ICANN, Ministerul Finanțelor,

Scrisori contabile verificate, Avize juridice verificate și Departamentul de resurse umane al solicitantului.

Pașii 3: CERTSIGN solicită și primește o scrisoare de autorizare SSL EV / Acord principal de la solicitant (cu excepția cazului în care o scrisoare de autorizare SSL EV / Acord principal de la solicitant este deja în posesia sa).

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

Pasul 5: aprobatorul de certificat este contactat fie telefonic, fie direcționat către o pagină web prin care se obține aprobarea certificatului de emitere a certificatului.

Pasul 6: Toate semnăturile solicitanților de certificate, aprobatorilor de certificate și contract

Semnatarii sunt verificați prin proceduri de urmărire sau apeluri telefonice. Alternativ, dacă semnăturile sunt efectuate folosind certificate calificate conforme cu UE 910/2014, nu se mai efectuează alte verificări.

Pasul 7: Doi (2) operatori CERTSIGN (un ofițer de înregistrare și un specialist în validare) sunt obligați să aprobe eliberarea certificatului (a se vedea mai jos corelarea încrucișată și due diligence).

Pasul 8: Un sistem securizat este utilizat pentru a trimite cererea de generare a certificatului către certSIGN SSL EV CA Clasa 3 G2 și se creează Certificatul web calificat.

Pasul 9: Solicitantul de certificat este notificat că certificatul a fost creat și este gata pentru descărcare (sau este trimis la Solicitant ca zip într-un e-mail).

4.2.1 Efectuarea funcțiilor de identificare și autentificare

Identificarea și autentificarea unui certificat de subiect. Ofițerii autorității de înregistrare efectuează identificarea și autentificarea utilizatorilor finali conform procedurii definite în capitolul 3.2.
RA colectează și validează informațiile de identitate și atribute ale subiectului și 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.

4.2.2 Aprobarea sau respingerea cererilor de certificat

Înainte de a stabili dacă se aprobă sau se respinge o cerere pentru un SSL EV, CERTSIGN efectuează alte verificări cerute de Ghiduri, inclusiv următoarele:

1. Aplicațiile pentru SSL EV sunt examinate pentru identificarea unor ținte cu risc ridicat de phishing și alte scheme frauduloase. CERTSIGN verifică listele interne și externe adecvate ale numelor organizațiilor care sunt cel mai frecvent vizate în phishing și în alte scheme frauduloase și semnalează automat astfel de solicitări SSL EV pentru control suplimentar înainte de emisiune.
2. Numele individuale, numele solicitanților, locațiile fizice și jurisdicțiile solicitanților pentru SSL EV sunt revizuite pentru a stabili dacă sunt identificate pe orice listă neagră de la guvern, pe lista persoanelor interzise sau pe o altă listă care interzice să facă afaceri cu o astfel de organizație, după cum se specifică la 3.2.2.1 .

Corelarea încrucișată finală și due diligence

Aprobarea emiterii certificatului de către CERTSIGN necesită doi operatori (operator de înregistrare și specialist în validare. (A se vedea secțiunea 5.2.2, numărul de persoane necesare pentru fiecare sarcină și secțiunea 5.2.4, Roluri care necesită separarea atribuțiilor).

(a) Procedurile CERTSIGN garantează că un Operator de înregistrare care nu este responsabil pentru colectarea și revizuirea informațiilor revizuiește toate informațiile și documentația asamblate în sprijinul SSL EV și caută discrepanțe sau alte detalii care necesită explicații suplimentare.
(b) CERTSIGN solicită, obține și documentează explicații suplimentare sau clarificări de la solicitant, aprobator de certificat, solicitant de certificat, surse de informații independente calificate și / sau alte surse de informații, după cum este necesar pentru a rezolva discrepanțele sau detaliile care necesită explicații suplimentare.
(c) CERTSIGN nu emite un SSL EV până când întregul corp de informații și documentație asamblat în sprijinul SSL EV este astfel încât emiterea certificatului nu va comunica informații de fapt inexacte pe care CERTSIGN le cunoaște sau prin exercițiul de descoperire, din informațiile și documentația asamblate. Dacă nu se primesc explicații satisfăcătoare și / sau documentații suplimentare într-un termen rezonabil, CERTSIGN va respinge cererea SSL EV și va notifica solicitantul în consecință.
(d) CERTSIGN îndeplinește cerințele de corelare încrucișată finală și due diligence prin intermediul angajaților aflați sub controlul său și având pregătire, experiență și judecată adecvate în confirmarea identificării și autorizării organizaționale.
(e) În cazul în care o parte sau întreaga documentație utilizată pentru susținerea cererii este într-o altă limbă decât engleza sau româna, un angajat CERTSIGN calificat în această limbă care are pregătirea, experiența și judecata corespunzătoare în confirmarea identificării și autorizării organizaționale îndeplinește cerințele acestei corelări încrucișate finale și a due diligenței. Atunci când angajații CERTSIGN nu posedă cunoștințele lingvistice necesare, CERTSIGN se bazează pe traduceri lingvistice ale porțiunilor relevante ale documentației furnizate de un traducător calificat.

Din când în când, CERTSIGN poate modifica cerințele legate de informațiile solicitate, în funcție de cerințele CERTSIGN, de contextul comercial al utilizării certificatelor sau după cum poate fi impus de lege.

După finalizarea cu succes a tuturor validărilor necesare pentru o cerere de certificat, CERTSIGN va aproba o cerere pentru un SSL EV.

Dacă informațiile din cererea de certificat nu pot fi confirmate, atunci CERTSIGN va respinge cererea de certificat. CERTSIGN își rezervă dreptul de a respinge o cerere pentru un SSL EV dacă, în propria sa evaluare, numele bun și de încredere al CERTSIGN ar putea fi pătat sau diminuat și poate face acest lucru fără a suporta nicio răspundere sau răspundere pentru orice pierdere sau cheltuieli rezultate din astfel de refuz. CERTSIGN își rezervă dreptul de a nu dezvălui motivele unui astfel de refuz.

Solicitanții ale căror cereri au fost respinse pot solicita ulterior din nou.

4.2.3 Timpul pentru procesarea cererilor de certificat

CERTSIGN nu emite certificate imediat după înregistrare. Certificatele trebuie emise de Autoritatea de certificare; prin aprobarea cererii de certificat primite de la RA, prin urmare, certificatele nu sunt disponibile imediat Beneficiarului atunci când certificatele sunt create de CA.

Fiecare cerere de formular este procesată după cum urmează:

- Operatorul Autorității de înregistrare primește cererea Beneficiarului
- Operatorul verifică datele din cerere cu privire la Subiect și Beneficiar
- În urma verificării, operatorul confirmă identitatea dintre datele menționate și cele incluse în cerere; dacă cererea conține date neconforme, este respinsă,
- Cererea confirmată este trimisă autorității de certificare,
- Autoritatea de înregistrare verifică și alte date care nu sunt specificate în cerere, dar sunt necesare și pentru eliberarea certificatului.

Procesarea solicitării la Autoritatea de certificare

Autoritatea de certificare verifică dacă autoritatea de înregistrare a confirmat solicitările.

4.3 Emiterea certificatului

După primirea și procesarea unei cereri (a se vedea capitolele 4.1 și 4.2), autoritatea de certificare emite un certificat. După eliberarea certificatului, certSIGN îl publică în depozitele corespunzătoare. Perioada de disponibilitate a certificatelor emise depinde de tipul certificatului și de categoria subiectului și este conformă cu perioadele prezentate în tabelul 6.3.2.2.
CERTSIGN informează Beneficiarul despre emiterea certificatului prin trimiterea unui e-mail (la adresa predată de Beneficiar) informații care îi permit Beneficiarului să obțină certificatul. Fiecare certificat emis este publicat în depozitul certSIGN. Publicarea certificatului este echivalentă cu notificarea altor părți care se bazează pe faptul că a fost emis un certificat pentru un subiect.

4.3.1 Acțiuni CA în timpul emiterii certificatului

Certificatul este emis ca parte a procesului de înscriere a certificatului. CA va primi numai cereri de certificat de la RA. CA, RA și procesul de personalizare sunt sisteme integrate și comunică prin conexiuni de rețea închise. CA procesează numai solicitările care provin de la RA de încredere a CERTSIGN.
Pentru fiecare cerere de certificat, CA va efectua următoarele verificări și acțiuni:

- Cererea provine din RA
- CA verifică autorizația solicitantului pentru tipul de cerere și refuză cererile care se referă la profilurile de certificat pentru care solicitantul nu este autorizat.
- CA, de asemenea, corespunde cererii de certificat cu un profil de certificat predefinit. Informațiile variabile din cerere trebuie să se potrivească cu șablonul și setul de reguli ale profilului certificatului.
- CA adaugă informații variabile și variabile la certificat, așa cum este definit în profilul certificatului specificat.

4.3.2 Notificarea emiterii certificatului de către CA către beneficiar

Certificatul este emis ca parte a procesului de înscriere 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

1.1.1 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 certificatelor
- RA execută revocarea certificatului

4.4.1 Publicarea certificatului de către CA

A se vedea capitolul „PUBLICAREA ȘI RESPONSABILITĂȚILE DE REPOZITARE”

4.4.2 Notificarea emiterii certificatului de către CA către alte entități

La primirea unui certificat, Beneficiarul se angajează să verifice conținutul acestuia, în special corectitudinea datelor și complementaritatea cheii publice cu cheia privată pe care o deține. În cazul în care certificatul prezintă defecte sau greșeli care nu pot fi acceptate de beneficiar, beneficiarul va informa imediat autoritatea de certificare cu privire la revocarea certificării.
Certificatul este considerat acceptat în cazul apariției următoarelor evenimente în termen de maximum 3 zile calendaristice de la data primirii certificatului de către beneficiar:

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

Dacă un certificat nu este respins în 3 zile calendaristice de la primirea acestuia, certificatul este considerat acceptat.
Acceptarea certificatului este exclusiv de către Beneficiar, înainte de utilizare și aplicarea sa la orice operațiune criptografică prin care se consideră că a acceptat termenii și condițiile specificate în prezentul CPP, politica de certificare și acordul de furnizare a serviciilor. În cazul depunerii electronice a cererii, avocatul acceptă automat certificatul în momentul solicitării acestui certificat.

Prin acceptarea certificatului, Beneficiarul acceptă regulile CPP și ale Politicii de certificare și este de acord să respecte prevederile acordului încheiat cu CERTSIGN.

4.5 Perechea de chei și utilizarea certificatului

4.5.1 Utilizarea cheii private a beneficiarului și utilizarea certificatului

Beneficiarii își protejează cheile private de accesul personalului neautorizat sau al altor părți terțe.

Beneficiarii vor utiliza cheile private numai în conformitate cu utilizările specificate în extensia de utilizare a cheii.

A se vedea secțiunile 1.4.1, 6.1.7 și 7.1.

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 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.

Părțile care se bazează pe un SSL EV trebuie să adere la protocolul SSL / TLS și să verifice în permanență o semnătură digitală, verificând validitatea unui certificat digital față de serviciul OCSP de la http://ocsp.certsign.ro sau CRL-ul relevant publicat de CERTSIGN.

Părțile de încredere sunt avertizate că o semnătură digitală neconfirmată nu poate fi atribuită ca semnătură validă a Beneficiarului.

Decizia finală privind dacă se bazează sau nu pe o semnătură digitală verificată sau pe securitatea unei sesiuni SSL / TLS este exclusiv cea a părții care se bazează. Bazarea pe o semnătură digitală sau schimbul de informații SSL / TLS ar trebui să aibă loc numai dacă:

- Semnătura digitală sau sesiunea SSL / TLS a fost creată în timpul perioadei operaționale a unui certificat valid și poate fi verificată referindu-se la un certificat validat.
- Partea de încredere a verificat starea de revocare a certificatului făcând referire la CRL-urile relevante, iar certificatul nu a fost revocat.
- Partea de încredere înțelege că un certificat digital este emis unui beneficiar pentru un anumit scop și că cheia privată asociată certificatului digital poate fi utilizată numai în conformitate cu utilizările specificate în acest CPP și conținute în certificat.

Încrederea este acceptată ca fiind rezonabilă în conformitate cu dispozițiile făcute pentru partea care depinde în temeiul prezentului CPP și în cadrul Acordului părții care se bazează. În cazul în care circumstanțele de încredere depășesc asigurările oferite de CERTSIGN în conformitate cu prevederile prezentului CPP, partea care depinde trebuie să obțină asigurări suplimentare.

Garanțiile sunt valabile numai dacă au fost efectuate etapele detaliate mai sus.

Bazându-se pe o semnătură digitală sau o sesiune SSL / TLS care nu pot fi verificate poate rezulta riscuri pe care partea care le asumă le asumă în totalitate și pe care CERTSIGN nu le asumă în niciun fel.

Prin intermediul acestui CPP, CERTSIGN a informat în mod adecvat părțile dependente cu privire la utilizarea și validarea semnăturilor digitale și a sesiunilor SSL / TLS prin intermediul acestui CPP și a altor documentații publicate în depozitul său public disponibil la http://www.certsign.ro/repository sau de asemenea datorită disponibilității CERTSIGN prin adresele de contact specificate în secțiunile 2.2 și 9.11 din acest CPP.

4.6 Reînnoirea certificatului

CERTSIGN nu efectuează reînnoirea certificatului.

4.7 Re-key certificat

În conformitate cu secțiunea 25 (b) (Validarea cererilor de retransmisie) din liniile directoare EV, CERTSIGN se poate baza pe informații verificate anterior pentru a emite un certificat de înlocuire în cazul în care:

i. Data de expirare a certificatului de înlocuire este aceeași cu data de expirare a SSL EV valabil în curs de înlocuire și
ii. Subiectul certificatului certificatului de înlocuire este același cu subiectul certificatului conținut în SSL EV valabil în prezent.

Re-key-ul sau înlocuirea unui certificat înseamnă să solicitați un nou certificat cu același conținut al certificatului, cu excepția unei noi chei publice. Acest lucru se poate întâmpla, de exemplu, dacă beneficiarul șterge din greșeală cheia privată corespunzătoare. (Rețineți că unele platforme de dispozitive, de exemplu Apache, permit utilizarea reînnoită a cheii private.) Dacă celelalte informații de contact ale beneficiarului și cheia privată nu s-au modificat, CERTSIGN poate emite un certificat de înlocuire utilizând același CSR PKCS # 10 ca cel folosit pentru certificatul anterior. În caz contrar, trebuie depus un nou CSR PKCS # 10 și se eliberează un certificat de înlocuire, cu condiția ca beneficiarul să se califice altfel, mai sus. Alte aspecte ale cheii re-key a certificatului (de exemplu, cine poate solicita cheia nouă, notificarea emiterii, comportamentul care constituie acceptarea, și publicarea certificatului) sunt identice cu cele pentru eliberarea inițială a certificatului. A se vedea secțiunile 3.3.1, 4.1, 4.2, 4.3 și 4.4

4.7.1 Circumstanțe pentru re-key-ul certificatului

CERTSIGN efectuează rekeying de certificate care nu au fost revocate înainte de expirarea lor.

CERTSIGN CA și RA lucrează împreună pentru a solicita sau impune din nou chei ale certificatelor de entitate finală la un moment configurabil înainte de expirarea certificatelor.

Perioada de timp și metodele de notificare sunt configurabile.

4.7.2 Cine poate solicita certificarea unei noi chei publice

certSIGN permite procesul de re-key să fie inițiat atât de Beneficiarul certificatului, cât și de CA / RA care gestionează acel certificat adecvat.

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 în timp ce 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 noi către subiect
RA utilizează aceleași procese de notificare ca și pentru un certificat nou solicitat.

4.7.5 Conduită 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 emiterii certificatului de către CA către alte entități
RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

Certificarea cheii și rekey-ul se efectuează atunci când un beneficiar, în numele unui subiect (deja înregistrat), generează o nouă pereche de chei (sau comandă unei autorități de certificare să genereze o astfel de pereche de chei) și solicită eliberarea unui nou certificat pentru confirmarea posesiei a unei noi chei publice create.
Certificarea cheii sau rekey-ul certificatului se efectuează numai la cererea Beneficiarului și va fi precedată de depunerea unei cereri pe un formular corespunzător completat de Beneficiar.
Solicitările vor fi confirmate în cazul în care operatorul Autorității de înregistrare o solicită.
Procedurile de procesare a rekey și cererea de certificare sunt echivalente cu procedurile de procesare pentru cererile de certificat descrise în capitolul 4.2 și procedurile de eliberare a certificatelor descrise în capitolul 4.3. În urma acestui proces:

- Beneficiarul este informat despre eliberarea noului certificat și a numărului său de serie.
- Un nou certificat este publicat în depozitul Autorității de certificare.

Procedura de certificare și rekey a certificatului este la fel de aplicabilă certificatelor unei anumite autorități de certificare, deși într-o astfel de situație toți clienții autorității de certificare vor fi informați cu privire la executarea procedurii.
certSIGN informează întotdeauna Beneficiarul (cu cel puțin 30 de zile înainte) despre apropierea perioadei de expirare. Aceste informații sunt trimise și pentru certificatele Autorității de certificare.

4.8 Modificarea certificatului
CERTSIGN nu permite modificarea detaliilor certificatului pe durata de viață a certificatului. Dacă se modifică orice informații despre certificat, Beneficiarul trebuie să solicite revocarea certificatului original și să solicite emiterea unui nou certificat. CERTSIGN poate, la discreția sa, să crediteze o parte din costul noului certificat în contul Beneficiarului. A se vedea secțiunile 4.1, 4.2, 4.3 și 4.4.

4.9 Revocarea certificatului
Revocarea certificatului are o influență semnificativă asupra utilizării acestuia și asupra obligațiilor Beneficiarului. La scurt timp după revocarea certificatului unui subiect, certificatul

va fi considerat invalid (în curs de revocare). În mod similar, în cazul certificatului Autorității de certificare - anularea validității unui certificat înseamnă retragerea drepturilor de eliberare a certificatului pentru proprietarul său și revocarea tuturor certificatelor eliberate de acesta. 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 conținută într-un certificat revocat rămâne sub Controlul beneficiarului, după revocare, acesta trebuie păstrat în siguranță până când este distrus.

4.9.1 Circumstanțe pentru revocarea certificatului

Un motiv de bază pentru revocarea certificatului unui subiect este pierderea controlului (sau suspiciunea unei astfel de pierderi) asupra cheii private deținute de Beneficiar încălcarea obligațiilor / cererilor incluse în Politica de certificare sau contractul încheiat cu Autoritatea de certificare sau CPP.
Certificatul este revocat atunci când:

- Informațiile din certificat s-au schimbat,
- O cheie privată asociată unei chei publice din certificat sau de pe dispozitivul de stocare a fost compromisă sau există un motiv serios pentru a suspecta că a fost compromisă,
- Beneficiarul solicită revocarea,
- Poate fi revocat de către emitent, certSIGN, de exemplu, dacă un beneficiar nu respectă politica de certificare, CPP sau acordul sau alte documente emise de autoritatea de certificare,
- Autoritatea de certificare își încetează activitatea; în acest caz, toate certificatele emise de această autoritate de certificare înainte de perioada stabilită pentru încetarea serviciilor vor fi revocate împreună cu certificatul autorității de certificare,
- Beneficiarul întârzie sau nu plătește valoarea serviciilor prestate de autoritatea de certificare,
- Cheia privată sau securitatea unei autorități de certificare au fost compromise într-un mod care pune în pericol credibilitatea certificatelor,
- Dreptul CERTSIGN de a emite și gestiona certificate SSL EV în conformitate cu Orientările EV, Regulamentul UE 910/2014 și Cerințele de bază
- În alte cazuri, când Beneficiarul nu respectă regulile acestui CPP, Politica de certificare sau acordul.
- CERTSIGN primește un ordin legal și obligatoriu de la un guvern sau un organism de reglementare pentru revocarea SSL EV;
- CERTSIGN primește o notificare sau devine altfel conștient de faptul că o instanță sau un arbitru a revocat dreptul unui Beneficiar de a utiliza numele de domeniu listat în SSL EV sau că Beneficiarul nu a reușit să își reînnoiască numele de domeniu;
- CERTSIGN determină, la propria sa discreție, că SSL EV nu a fost emis în conformitate cu termenii și condițiile Ghidului EV și QCP-w;
- CERTSIGN determină că oricare dintre informațiile care apar în SSL EV nu sunt corecte;
- CERTSIGN primește o notificare sau în alt mod devine conștient că a existat o altă modificare a informațiilor referitoare la Beneficiar care sunt conținute în SSL EV; sau

- În cazul în care CERTSIGN primește o notificare sau în alt mod constată că un Beneficiar a fost adăugat ca parte refuzată sau persoană interzisă, așa cum este definit în lista UE specificată la 3.2.2.1

Cheia privată compromisă înseamnă: (1) acces neautorizat la cheia privată sau un motiv puternic care determină să 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.
Solicitarea de revocare poate fi trimisă prin intermediul Autorității de înregistrare (acest lucru implică Beneficiarul să contacteze autoritatea) sau direct către o autoritate de certificare (solicitarea poate fi autentificată prin semnătură). Cererea de revocare trebuie să conțină informații care permit autentificarea sigură a beneficiarului de către autoritatea de înregistrare, în conformitate cu prevederile capitolului 3.1.8. Dacă autentificarea identității beneficiarului nu reușește, autoritatea de certificare respinge cererea de revocare.

4.9.2 Cine poate solicita revocarea certificatului

Beneficiarul și părțile sale autorizate în mod corespunzător pot solicita revocarea unui SSL EV (de exemplu, un semnatar de contract, un aprobator de certificat sau un solicitant de certificat identificat de beneficiar în scrisoarea / acordul principal al autorității SSL EV). CERTSIGN poate, dacă este necesar, să solicite, de asemenea, ca cererea de revocare să fie făcută fie de un contact organizațional, de un contact de facturare sau de către solicitantul înregistrării domeniului.

Pentru o entitate care nu este beneficiar, depunerea unui „Raport privind problema certificatului" ("*Certificate Problem Report*") este primul pas în inițierea unei cereri de revocare a certificatului. Aceste entități includ parteneri, furnizori de software de aplicații și alte terțe părți care pot transmite rapoarte către CERTSIGN despre reclamații sau presupuse compromisuri ale cheii private, utilizarea abuzivă a SSL EV sau alte tipuri de fraude, compromisuri, abuzuri sau comportamente inadecvate legate de SSL EV.

Autoritatea de înregistrare acționează cu extremă prudență atunci când procesează cererile de revocare care nu au fost trimise de beneficiar și acceptă numai acele cereri în conformitate cu capitolul 4.9.1.
Atunci când partea care solicită revocarea certificatului nu este proprietarul certificatului (beneficiar), autoritatea de certificare efectuează următoarele:

- Verifică dacă partea respectivă are dreptul de a emite o astfel de cerere
- Solicită o justificare pentru solicitarea respectivă
- Trimite Beneficiarului o notificare privind revocarea sau începerea procesului de revocare.

Fiecare solicitare va fi trimisă:

- Direct către autoritatea de certificare în format electronic cu sau fără confirmarea autorității de înregistrare,
- Direct sau indirect (prin intermediul Autorității de înregistrare) către Autoritatea de certificare, nu în format electronic (document pe hârtie, fax, telefon etc.)

Furnizorii de aplicații software 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 de revocare a certificatului

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

Revocarea certificatului poate fi efectuată după cum urmează:

- Beneficiarul trimite către CERTSIGN o cerere de revocare electronică autorizată prin parola primită împreună cu certificatul sau
- Beneficiarul trimite către CERTSIGN o cerere de revocare electronică semnată electronic de Beneficiar cu un certificat calificat valid (care nu este revocat sau expirat) sau
- Beneficiarul furnizează personal cererea de revocare pe hârtie la una dintre autoritățile de înregistrare CERTSIGN, iar autenticitatea documentului pe hârtie este realizată de către autoritatea de înregistrare; după verificarea cu succes a cererii, autoritatea de înregistrare pregătește o cerere de revocare electronică și o înaintează autorității de certificare sau
- Reprezentantul Beneficiarului trimite o cerere de revocare fie pe cale electronică, fie pe hârtie. CERTSIGN contactează Beneficiarul prin telefon pentru a obține confirmarea; certificatul poate fi revocat numai după obținerea confirmării. Numărul de telefon al companiei este cel identificat în procesul de înregistrare inițială.

Informațiile despre certificatele revocate sunt plasate în lista de revocare a certificatelor emisă de autoritatea de certificare. Autoritatea de certificare notifică beneficiarul care solicită revocarea certificatului cu privire la acest lucru sau cu privire la decizia de anulare a cererii împreună cu motivele anulării.
Fiecare cerere de revocare a certificatului va furniza mijloace de identificare univocă a certificatului revocat, va conține motivele pentru care se solicită revocarea, conform cap. 7.2, și trebuie să fie autentificată, conform cap. 3.4.
O cerere de revocare a certificatului are loc după cum urmează:

- CERTSIGN verifică cererea de revocare, inclusiv faptul că este trimisă de o entitate legitimă. Dacă solicitarea este verificată cu succes, Autoritatea de certificare plasează informațiile referitoare la revocarea certificatului în Lista de revocare a certificatului (CRL);
- Autoritatea de certificare notifică beneficiarul cu privire la revocare sau cu privire la decizia de anulare a cererii împreună cu motivele acestei anulare.

Dacă un certificat sau o cheie privată corespunzătoare unui certificat de revocat au fost stocate pe un dispozitiv hardware ca urmare a revocării certificatului, dispozitivul hardware trebuie inițializat în condiții de securitate ridicată.

4.9.4 Perioada de grație a cererii de revocare

certSIGN efectuează revocarea pe baza celui mai bun 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 Timp în care CA trebuie să proceseze cererea de revocare

certSIGN garantează următoarea perioadă maximă pentru procesarea unei cereri de revocare a certificatului,

- Trimis electronic (în formatul corect),
- Trimis ca document pe hârtie,

Așa cum este descris în Tabelul 4.9.5.

Politica de certificare	Perioada de grație admisibilă
certSIGN	În termen de 24 de ore

Tabelul 4.9.5. Perioada maximă 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;
3. 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
4. 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 perioadele de publicare ale CRL.
În momentul revocării certificatului, operatorii Autorității de înregistrare și Beneficiarul implicat sunt informați automat cu privire la această revocare. Informațiile despre starea actuală a certificatului sunt disponibile prin intermediul serviciului de verificare a stării certificatului imediat după perioada de grație menționată. Acest serviciu poate fi solicitat, de exemplu, de către o parte de încredere care verifică disponibilitatea unei semnături electronice aplicate unui document primit de la beneficiar.

4.9.6 Cerințe de verificare a revocării pentru părțile implicate

Părțile de încredere vor utiliza toate resursele pe care CERTSIGN le pune la dispoziție prin depozitul său pentru a verifica starea unui certificat în orice moment înainte de a se baza pe acesta. CERTSIGN actualizează OCSP, CRL-uri în consecință.

4.9.7 Frecvența emiterii CRL

Fiecare parte a Autorității de certificare din CERTSIGN emite diferite liste de revocare a certificatelor. O nouă CRL este publicată în depozit imediat după fiecare revocare a certificatului sau în maximum o zi. Perioada de disponibilitate a CRL este de 48 de ore și este actualizată zilnic.
Lista de revocare a certificatelor (CRL) pentru autoritatea CA CERTSIGN ROOT este emisă cel puțin anual, cu condiția să nu existe revocări de certificate ale uneia dintre autoritățile CA Intermediare.
În cazul revocării certificatului unei autorități afiliate la CERTSIGN, acest certificat este publicat imediat în Lista de revocare a certificatului.

4.9.8 Latență maximă pentru CRL-uri

CRL-ul acestei autorități de certificare și al tuturor autorităților sale de emitere Intermediare 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.

4.9.10 Cerințe de verificare a revocării on-line

CA acceptă o capacitate OCSP utilizând metoda GET pentru certificatele emise în conformitate cu "*Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates*".

Pentru starea certificatelor de beneficiar, CA actualizează informațiile furnizate printr-un protocol de stare a certificatului online cel puțin la fiecare oră. Răspunsurile OCSP de la acest serviciu TREBUIE să aibă un timp de expirare maxim de 24 de ore.

Pentru statutul certificatelor CA Intermediare:

CA actualizează cel puțin informațiile furnizate printr-un protocol de stare a certificatului online

(i) La fiecare douăsprezece luni și
(ii) 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 statut „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.

4.9.11 Alte forme de anunțare a revocării disponibile

În prezent, nu sunt disponibile alte forme de reclame de revocare.

4.9.12 Cerințele speciale legate de compromisul cheii

Dacă un Beneficiar știe sau suspectează că integritatea cheii private a certificatului său a fost compromisă, Beneficiarul va:

- Încetează imediat utilizarea certificatului,
- Începeți imediat revocarea certificatului,
- Ștergeți certificatul de pe toate dispozitivele și sistemele,
- Informați toate părțile care se bazează pe acest certificat.

Compromisul cheii private poate avea implicații asupra informațiilor protejate cu această cheie. Beneficiarul 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
Nu se aplică

4.9.14 Cine poate solicita suspendarea
Nu se aplică

4.9.15 Procedura cererii de suspendare
Nu se aplică

4.9.16 Limite pentru perioada de suspendare
Nu se aplică

4.10 Servicii de stare a certificatului
Nu se aplică

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 „certsign.ro” și al liniei „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.

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 plângere autorităților de aplicare a legii și / sau revoca un certificat care face obiectul unei astfel de plângeri.

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

4.11 Incetarea 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 Beneficiarului pentru o perioadă minimă de 10 ani de la încetarea unui abonament.

4.12 Custodie și recuperare chei
CERTSIGN nu efectuează escrow sau recuperare a cheilor private ale beneficiarului.

5 Facilități, management și controale operaționale

Acest capitol descrie cerințele generale privind controlul, securitatea fizică și organizațională, precum și activitatea personalului, utilizate în CERTSIGN de exemplu în timpul generării cheii, verificării autenticității entității, emiterea și publicarea certificatelor, revocarea certificatului, audit și crearea copiilor de rezervă.

În calitate de furnizor de servicii de certificare, CERTSIGN plasează securitatea în centrul activităților sale. Pentru ca toate activele, activitățile și serviciile sale să fie sigure, CERTSIGN a implementat, menține și îmbunătățește continuu un sistem de management al securității informației certificat 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, General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1, Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2, Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 421, Policy and Security Requirements for Trust Service Providers issuing Time-Stamps

5.1 Controale fizice

Sistemul computerizat de rețea, terminalele operatorului și resursele de informații ale certSIGN sunt situate în zona dedicată, protejate fizic împotriva accesului neautorizat, distrugerii sau perturbării funcționării acestuia. Aceste locații sunt monitorizate. Fiecare intrare și ieșire este înregistrată în jurnalul de evenimente (jurnalele sistemului), stabilitatea puterii, precum și temperatura și umiditatea sunt monitorizate și controlate.

5.1.1 Amplasarea și construcția sediului

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

Toate operațiunile certSIGN CA și RA se desfășoară într-un mediu fizic protejat cu controale bazate pe evaluarea riscurilor care descurajează, previn, detectează și contracarează 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. Printre cele mai importante controale de securitate se numără:

- Un perimetru clar definit și protejat prin care toate intrările și ieșirile sunt controlate;
- Componentele critice sunt protejate cu mai multe perimetre

- Un sistem de control al intrării care admite doar persoanele autorizate în mod corespunzător și autorizate în mod specific să intre în zonă;
- Monitorizare controlată și electronică 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;
- Echipamentul este întreținut corect pentru a asigura disponibilitatea și integritatea sa continuă.

5.1.2 Acces fizic

Accesul fizic în zona certSIGN este controlat și monitorizat de sistemul de alarmă integrat. Sistemul de prevenire a incendiilor, sistemul de detectare a intruziunilor și sistemul de alimentare de urgență sunt utilizate.

Facilitatea CERTSIGN este disponibilă publicului în fiecare zi lucrătoare între orele 9.00 și 18.00. În timpul rămas (inclusiv zilele nelucrătoare), facilitatea este disponibilă numai persoanelor autorizate de conducerea CERTSIGN. Vizitatorii zonelor ocupate de CERTSIGN pot accesa această zonă numai dacă sunt însoțiți permanent de personalul autorizat.

Zonele ocupate de CERTSIGN sunt împărțite în:

- Zone 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 cărților de identitate și a cititorilor corespunzători, montați lângă intrarea în zonă. Fiecare intrare și ieșire din și din zonă este înregistrată automat în jurnalul de evenimente.

Accesul la zona operatorilor este impus prin utilizarea unui card electronic și a cititorului corespunzător al acestora. Deoarece toate informațiile sensibile sunt protejate prin utilizarea seifurilor, în timp ce accesul la terminalul operatorului sau al administratorului necesită autorizare prealabilă, securitatea fizică angajată 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 dacă este însoțit.

Zona de dezvoltare și testare este protejată într-un mod similar cu protecția zonei de operatori și administratori. Persoanelor fără escortă li se permite să ocupe zona. Programatorii și dezvoltatorii nu au acces la informații sensibile. Dacă un astfel de acces este necesar, acesta necesită 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

Toate zonele sunt dotate cu aer condiționat. În zonele serverului, unitățile de aer condiționat sunt redundante și temperatura este monitorizată atât automat (cu o alertă la atingerea unui prag), cât și manual. Din momentul întreruperii alimentării, sursa de alimentare de urgență (UPS) permite continuarea activității până la intervenția automată a generatorului de rezervă în clădire. Infrastructura de energie electrică este concepută astfel încât, dacă se întrerupe

curentul principal al clădirii, toate activitățile pot continua cel puțin 24 de ore datorită generatorului diesel. 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 sunt, de asemenea, conectate la UPS-uri și la generatorul diesel.

5.1.4 Expunerea la apă

Riscul de inundație în zona serverelor este controlat prin rafturi. Toate echipamentele sunt plasate în rafturi, iar distanța de la sol la primul echipament este de minimum 15 cm. 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, suporturile care conțin date sau informații de rezervă sunt manipulate și stocate în siguranță în cadrul facilității primare. Suporturile de rezervă sunt, de asemenea, stocate în siguranță într-o locație separată de locația media originală, cu aceeași securitate ca locația primară. Mediile care conțin date sensibile sunt eliminate în siguranță atunci când nu mai sunt necesare

5.1.7 Eliminarea deșeurilor

Hârtia și suporturile electronice care conțin informații semnificative pentru securitatea CERTSIGN după expirarea perioadei de păstrare sunt distruse. Modulele de securitate hardware sunt resetate și șterse în conformitate cu recomandările producătorului. Aceste dispozitive sunt, de asemenea, resetate și șterse în siguranță atunci când sunt trimise în service sau reparate.

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 cu 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 48 de ore în locația CERTSIGN sau într=o locație auxiliară.

5.2 Controale procedurale

5.2.1 Roluri de încredere

Toate rolurile implicate în furnizarea serviciilor de certificare CERTSIGN sunt ocupate de angajați ai CERTSIGN.

Toți angajații CERTSIGN s-au angajat 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 împiedica o persoană să utilizeze cu răutate sistemele 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, iar administrația include gestionarea contului de utilizator și modificarea sau eliminarea în timp util a accesului. Sunt furnizate controale de securitate pentru computer suficiente pentru separarea persoanelor de încredere identificate, inclusiv separarea funcțiilor de administrare și operare a securității. În special, utilizarea programelor de utilitate a sistemului este restricționată și controlată.

În CERTSIGN, următoarele roluri de încredere ar putea fi echipate cu una sau mai multe persoane:

- **Agent 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 în afara locului certSIGN.
- **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;
- **Specialist în validare**: aplicarea unor proceduri riguroase de control pentru separarea sarcinilor de validare pentru a se asigura că nicio persoană nu poate valida și autoriza singură emiterea unui SSL EV. Un specialist în validare POATE revizui și verifica toate informațiile solicitantului și un al doilea specialist în validare POATE aproba emiterea SSL EV.
- **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 acționează cu un rol diferit de un auditor nu își poate asuma responsabilitățile auditorului.

Angajații sunt desemnați oficial în funcții de încredere de către conducerea superioară responsabilă de securitate care necesită principiul „cel mai mic privilegiu" la accesare sau la configurarea privilegiilor de acces și sunt acceptați de conducere și de persoana respectivă pentru a îndeplini rolul.

5.2.2 Numărul de persoane necesare pentru fiecare sarcină

Procesul de generare de chei - pentru nevoile de certificare și semnare CRL - este una dintre operațiunile care necesită o atenție specială. Generarea necesită prezența a cel puțin trei roluri de încredere, prezența ofițerului de securitate, administratorul autorității de certificare și un număr adecvat de persoane, cu deținerea unui secret comun, atunci când se încarcă cheia criptografică a autorității de certificare în modulul de securitate hardware.

Pentru sarcinile legate de funcțiile critice ale CA, cum ar fi, dar fără a se limita la gestionarea cheilor și, în special, generarea cheilor CA, sunt necesare mai mult de două persoane din motive extinse de securitate și control. Eliberarea certificatelor de către ROOT CA G2 este sub control cel puțin dublu de către personal autorizat și de încredere, astfel încât o persoană să nu poată semna certificate Intermediare pe cont propriu.

5.2.3 Identificare și autentificare pentru fiecare rol

Personalul CERTSIGN este supus procedurii de identificare și autentificare în următoarele situații:

- Plasarea pe lista persoanelor autorizate să acceseze locațiile CERTSIGN,
- Plasarea pe lista persoanelor cărora li se permite accesul fizic la resursele sistemului și de rețea ale CERTSIGN,
- Emiterea confirmării care autorizează îndeplinirea rolului atribuit,
- Atribuirea unui cont și a unei parole în sistemul de informații CERTSIGN.

Fiecare cont atribuit:

- Trebuie să fie unic și atribuit direct unei anumite persoane,
- Nu poate fi partajat cu nicio altă persoană,
- Trebuie restricționat în funcție de funcția (care decurge din rolul îndeplinit de o anumită persoană) pe baza sistemului software CERTSIGN, a sistemului de operare și a controalelor aplicației.

Operațiunile efectuate în CERTSIGN care necesită acces prin resurse de rețea partajate sunt protejate cu mecanisme implementate de autentificare puternică și criptare a informațiilor transmise.

Tot personalul CERTSIGN implicat în furnizarea serviciilor de certificare este identificat și autentificat înainte de a utiliza aplicații critice legate de aceste servicii. În special, administratorilor și operatorilor HSM și operatorilor CA și RA li se eliberează o acreditare (certificate digitale pe tokenuri sau carduri inteligente HSM) pentru a asigura o identificare și autentificare puternică (cu doi factori) înainte de a li se permite să efectueze orice acțiune de încredere. Toate acreditările criptografice sunt stocate în siguranță în cutii individuale.

Toate acțiunile angajaților în roluri de încredere sunt urmărite și se asigură răspunderea deplină.

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 ale posturilor definite din punctul de vedere al rolurilor îndeplinite cu segregarea de atribuții și cel mai mic privilegiu, determinând sensibilitatea poziției pe baza atribuțiilor și nivelurilor de acces, screening-ul de fond și formarea și conștientizarea angajaților. Acestea includ cerințe de abilități și experiență.

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

5.3 Controlul personalului

CERTSIGN se asigură că persoana care 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,
- Este cetățean român,
- 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 privind protecția informațiilor sensibile (din punctul de vedere al securității 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 care acționează pentru furnizarea serviciilor de certificare certSIGN sunt verificați înainte de angajare în ceea ce privește calificările, cunoștințele experților, experiențele și autorizațiile necesare și, după caz, pentru a îndeplini 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 istoricului

CERTSIGN efectuează sau se asigură că verificările relevante sunt efectuate potențialului personal prin intermediul rapoartelor de stare emise de o autoritate competentă, declarații terțe 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:

- Cerințele declarației de practică a certificării (CPP),

- Cerințele politicii de certificare,
- Proceduri și controale de securitate utilizate de o autoritate de certificare și o autoritate de înregistrare
- Amenințări frecvente la procesul de verificare a informațiilor (inclusiv phishing-ul și alte tactici de inginerie socială) și cerințele *"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"*
- Responsabilitățile care decurg din rolurile și sarcinile îndeplinite în sistem,

La finalizarea instruirii, participanții semnează un document care confirmă familiarizarea cu CPP, politica de certificare și acceptarea restricțiilor și obligațiilor asociate.

CA 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 furnizat de CA cu privire la cerințele de verificare a informațiilor prezentate în CPP și în cerințele *"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"*.

5.3.4 Frecvența și cerințele reinstruirilor

Instruirile descrise în capitolul 5.3.3 trebuie repetate sau completate întotdeauna în situația în care se execută modificări semnificative ale CERTSIGN sau ale operațiunii sale de autoritate de înregistrare.

5.3.5 Frecvența și secvența de rotație a posturilor

Nu se aplică.

5.3.6 Sancțiuni pentru acțiuni neautorizate

Încălcările politicilor sau procedurilor, acțiunilor neautorizate, utilizarea neautorizată a autorității și utilizarea neautorizată a sistemelor sunt penalizate de CERTSIGN sau se iau măsuri pentru a se acorda sancțiuni relevante celor responsabili. Aceasta poate include, printre altele, revocarea privilegiilor, disciplina administrativă, sancțiunile reglementate de legislația muncii din România și / sau urmărirea penală.

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 (vezi capitolele 5.3.1, 5.3.2 și 5.3.3). În plus, personalul contractual, atunci când își îndeplinește sarcina la sediile certSIGN, trebuie să fie escortat de certSIGN sau de angajații autorității de înregistrare, cu excepția celor care au aprobarea prealabilă din partea ofițerului de securitate și care pot accesa informații clasificate interne sau în conformitate cu legea din forta.

5.3.8 Documentație furnizată personalului

CERTSIGN trebuie să ofere personalului său acces la următoarele documente:

- Politica de certificare,
- CPP,
- Gama de responsabilități și obligații 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 certificare, dar și pentru a permite auditul acțiunilor angajaților și clienților, toate informațiile despre evenimente importante, specifice generate de sisteme și aplicații sunt înregistrate. Informațiile respective, cunoscute în mod colectiv ca jurnale, trebuie păstrate în așa fel încât să poată fi accesate de părțile care se bazează, auditorii și autoritățile statului în orice moment au nevoie de ele, pentru a furniza dovezi ale funcționării corecte a serviciilor în acest scop. procedurilor judiciare sau pentru a detecta încercările de a compromite securitatea CERTSIGN. Evenimentele înregistrate sunt arhivate 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, fie ea creată automat sau manual, este păstrată și dezvăluită în timpul unui audit, dacă este necesar. Acuratețea în timp a jurnalelor este asigurată de trei servere de timp. Două dintre acestea folosesc ca sursă de timp de referință sateliții GPS și unul este sincronizat cu sistemul care oferă ora oficială a României.

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 medii 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:

- **Intrări de sistem** - să conțină informații despre solicitările clientului și răspunsurile serverului (sau invers) la nivelul protocolului de rețea (de exemplu http, https); datele de înregistrat 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;
- **Audit** - conțin informații specifice pentru serviciile 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.

Fiecare înregistrare automată sau manuală conține următoarele informații:

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

Toate evenimentele legate de ciclul de viață al cheilor CA sunt înregistrate.

Toate evenimentele legate de ciclul de viață al certificatelor sunt înregistrate.

Toate evenimentele legate de ciclul de viață al cheilor gestionate de CA, inclusiv orice cheie de subiect generate de CA sunt înregistrate.

Toate cererile și rapoartele referitoare la revocare, precum și acțiunea rezultată sunt înregistrate.

Toate evenimentele legate de înregistrare, inclusiv cererile de re-key a certificatului, sunt înregistrate.

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,

În plus, certSIGN menține jurnalele interne ale tuturor evenimentelor de securitate și ale tuturor evenimentelor operaționale relevante din întreaga infrastructură, indiferent de serviciul component, inclusiv, dar fără a se limita la:

- Modificări ale politicii de securitate
- Pornirea și oprirea sistemelor;
- Pene de curent;
- Blocări ale sistemului și defecțiuni hardware
- Activități firewall și router
- Încercări de acces la sistem PKI
- Accesul fizic al personalului și al altor persoane la părți sensibile ale oricărui loc sau zonă securizată;
- Back-up și restaurare;
- Raport de testare de recuperare în caz de dezastru;
- Inspecții de audit;
- Actualizări și modificări ale sistemelor, software-ului și infrastructurii;
- Intruziuni de securitate și încercări de intruziune.

Accesul la jurnale este permis exclusiv pentru ofițerul de securitate, administratorii autorităților de certificare și auditori

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 jurnalului 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, administratorii 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,
- Numai ofițerul de securitate poate arhiva sau șterge fișiere (după arhivarea lor) care conțin evenimente înregistrate,
- Este posibil să se identifice orice încălcare a integrității; acest lucru asigură că înregistrările nu conțin lacune 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 de păstrare a jurnalelor.

5.4.5 Proceduri de backup pentru jurnalul de audit

Politicile de securitate CERTSIGN necesită 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
- Arhiva
- Back-up pe termen lung

5.4.7 Notificare către subiectul cauzator de evenimente

Nu se aplică.

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 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.

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, luând în considerare 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 și Subiectul/Beneficiari ar trebui să fie supuse arhivei.

Depozitul 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 off-line conține certificate (inclusiv certificate revocate) expirate cu până la 10 ani înainte de data curentă. Arhiva certificatului revocat conține informații despre un certificat identificat, motivul revocării, data la care certificatul a fost plasat pe CRL. Arhiva este utilizată pentru soluționarea litigiilor, aplicându-se documentelor vechi, semnate electronic de către un subiect.

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

5.5.1 Tipuri de date arhivate

Următoarele date sunt supuse unei arhive de încredere:

- Toate certificatele pentru o perioadă de minimum 10 ani de la expirarea lor
- Jurnalele arhivate ale jurnalelor sunt păstrate cel puțin 10 ani.
- Jurnale de eliberare și revocare a certificatelor pentru o perioadă de minimum 10 ani de la eliberare / revocare
- CRL-uri pentru minimum 10 ani după publicare
- Următoarele timp de cel puțin 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 Emiterea Certificatelor

Toate înregistrările de eliberare a certificatelor (copii ale certificatelor sunt păstrate, indiferent de statutul lor ca expirat sau revocat) sunt păstrate ca înregistrări în arhive electronice și /

sau pe suport de hârtie pentru perioada detaliată mai jos în secțiunea 5.5.2. CERTSIGN poate solicita solicitanților să prezinte documentația adecvată în sprijinul unei cereri de certificat. În astfel de circumstanțe, CERTSIGN păstrează înregistrările menționate în acest CPP.

CERTSIGN înregistrează următoarele informații legate de eliberarea certificatelor ca parte a procesului său de listă de verificare a aprobării certificatului:

- abonamentul PKCS # 10 CSR;
- Documentația existenței organizaționale pentru solicitanții organizaționali, astfel cum este listată în secțiunea 3.2.2;
- Documentația identității individuale pentru solicitanții individuali, astfel cum este listată în secțiunea 3.2.3;
- Verificarea existenței organizaționale și a statutului primit de la baze de date terțe și entități guvernamentale (inclusiv capturi de ecran ale site-urilor web care raportează astfel de informații);
- Validarea adresei poștale (dacă este diferită de cele identificate prin resursele enumerate mai sus);
- Scrisoare de autorizare pentru site-uri web administrate de agenți terți ai Solicitanților (dacă este cazul);
- Depunerea cererii de certificat, inclusiv acceptarea Acordului de beneficiar;
- Numele, adresa de e-mail și adresa IP a persoanei care recunoaște autoritatea solicitantului / beneficiarului colectate în conformitate cu secțiunea 3.2.5;
- Captură de ecran a site-ului web;
- Alte informații relevante de contact pentru solicitant / beneficiar; și
- Copie a certificatelor digitale emise.

5.5.3 Revocarea certificatului

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

5.5.4 Alte informații

CERTSIGN arhivează, de asemenea, următoarele informații despre operațiunile sale CA:

- Versiuni ale acestui CPP
- Obligatii contractuale
- Înregistrări despre configurația echipamentului CA System și accesul și utilizarea CA Private Key
- Date de audit de securitate și conformitate (a se vedea secțiunea 5.4); și
- Orice alte date sau aplicații necesare pentru a verifica conținutul arhivei.

5.5.5 Perioada de păstrare a arhivelor

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

5.5.6 Protecția arhivei

CERTSIGN asigură:

- Implementarea controalelor pentru prevenirea pierderii datelor din arhivă

- Arhivează confidențialitatea datelor și menținerea integrității în timpul perioadei de păstrare,

Arhivele sunt accesibile numai personalului autorizat.

5.5.7 Procedurile de backup ale arhivei

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

5.5.8 Cerințe pentru marcarea temporală a înregistrărilor

Ora sistemului pentru computerele CERTSIGN este actualizată utilizând Network Time Protocol (NTP) pentru a sincroniza ceasurile de sistem cel puțin o dată la opt ore (implicit Windows). Următoarele elemente arhivate din lista de verificare a aprobării certificatului sunt marcate cu data, ora și numele angajatului CERTSIGN care verifică informațiile și face înregistrarea:

- Captură de ecran a stării organizaționale;
- Captură de ecran a site-ului web.

Următoarele înregistrări sunt marcate temporal de către sistemul de administrare a certificatelor atunci când un articol este fie primit automat, fie este înregistrat de către angajatul CERTSIGN:

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

Emiterea certificatului este marcată în timp în funcție de câmpul „Valid From” în conformitate cu profilul certificatului X.509.

Revocarea certificatului este marcată temporal în funcție de câmpul „Data revocării” în conformitate cu profilul listei de revocare a certificatului X.509.

5.5.9 Sistem de colectare a arhivelor (intern sau extern)

Sistemele de colectare a arhivelor CERTSIGN sunt interne.

5.5.10 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 cheie de schimbare 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 secțiunea 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 a implementat o procedură de gestionare a incidentelor de securitate pentru a răspunde rapid și coordonat la incidente și pentru a limita impactul încălcărilor securității. 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 acționate 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 personale menținute în acesta în termen de 24 de ore de la încălcarea fiind identificată.

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 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.

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 unor servicii de rețea importante, importante pentru activitatea CERTSIGN. Se adresează în primul rând întreruperilor de curent și deteriorării conexiunilor de rețea,
- Corupția unei părți a Intranetului, utilizată de CERTSIGN pentru a furniza 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 48 de ore va fi activată o instalație de urgență, care ar trebui să înlocuiască toate funcțiile

semnificative ale unei autorități de certificare până când instalația primară va fi readusă în funcțiune. Distanța dintre facilitățile primare și cele de urgență este suficientă pentru a evita ca dezastrele potențiale care apar la locul principal 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 aplicația care creează copii de rezervă din date, permițând recuperarea sistemului în orice moment și efectuarea unui audit. Copiile de rezervă includ toate datele relevante din punct de vedere al securității.

Toate sistemele care alcătuiau infrastructura IT 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 va aborda 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 cheie privată a Autorității de certificare

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

În cazul compromisurilor cu cheia privată ale autorităților de certificare (afiliate cu certSIGN) 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 părțile de încredere și alți furnizori de servicii de încredere. În plus, aceste informații vor fi puse la dispoziția altor părți dependente prin intermediul sistemului mass-media și al poștei electronice
- Notificare publică 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 fără a percepe taxe.

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 catastrofe toate măsurile necesare pentru a asigura recuperarea completă a serviciilor noastre de certificare și marcare a timpului în caz de dezastru sau întreruperea oricărei componente sau servicii TIC importante mai mult decât perioada de oprire maximă tolerabilă stabilită. 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 de sistem necesare pentru reluarea operațiunilor CA sunt copiate și stocate într-un loc îndepărtat și sigur, adecvat pentru a permite serviciilor de certificare și marcare a timpului să revină la timp 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 un plan de reziliere actualizat. Obligațiile descrise mai jos sunt dezvoltate pentru a minimiza întreruperile pentru subiecți / beneficiari și părțile care se bazează pe acestea care ar putea rezulta dintr-o decizie a unei autorități de certificare de a înceta funcționarea și include obligațiile de a notifica în prealabil toți subiecții / beneficiarii autoritatea care a certificat Autoritatea de certificare supusă rezilierii (dacă există) și tranziției responsabilităților (servicii furnizate subiecților / beneficiarilor, baze de date etc.), în conformitate cu reglementările în vigoare ale altei autorități de certificare.

5.8.1 Cerințe asociate tranziției responsabilităților

Înainte ca o autoritate de certificare să își înceteze activitatea, aceasta:

- Informează (cu cel puțin 30 de zile în avans) următoarele despre decizia de încetare a serviciilor sale: toți subiecții / beneficiarii care dețin certificate active (neexpirate și nerevocate) emise de această autoritate și alte entități cu care certSIGN are acorduri sau alte forme stabilite relații, printre care părți dependente, 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;
- Gestionează starea de revocare pentru certificatele care au fost emise.
- Transferă obligațiile către o parte de încredere pentru menținerea tuturor informațiilor necesare pentru a furniza dovezi ale funcționării serviciilor de certificare

și marcare a timpului pentru o perioadă rezonabilă, cu excepția cazului în care se poate demonstra că nu deținem astfel de informații; Informațiile se referă la informațiile de înregistrare, starea de revocare a certificatelor expirate care au fost emise. și arhive de jurnal de evenimente pentru perioada lor de timp respectivă, așa cum este indicat subiecților / beneficiarului și părții de încredere

- Cheile private CA, inclusiv copii de rezervă, vor fi distruse sau retrase din utilizare, astfel încât cheile private să nu poată fi recuperate;
- Unde este posibil, ar trebui luate 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 parte de încredere obligațiile sale de a pune la dispoziție cheia sa publică pentru o perioadă rezonabilă.

În cazul în care CERTSIGN își va încheia activitățile fără un transfer parțial sau integral 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 devine faliment sau din alte motive nu poate acoperi singur costurile, pe cât posibil în limitele legislației aplicabile privind falimentul.

5.8.2 Emiterea de certificate de către succesorul CA reziliate

Pentru a furniza 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 certificatele de înlocuire emise pentru certificatele autorității de certificare reziliate care rămân în uz.

Eliberând un 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 EV CA Clasa 3 G2).

6 Controale de securitate ale informațiilor tehnice

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 EV CA Clasa 3 G2 deține 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

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

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

După ceremonia cheii, CERTSIGN produce un raport privind ceremonia cheie, 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.

CA:

- Generează cheile CA în cadrul modulelor criptografice care îndeplinesc cerințele tehnice și de afaceri aplicabile, astfel cum sunt prezentate în Declarația de practică de certificare;
- 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 Declarația sa de practică de certificare și (dacă este cazul) Scriptul său de ceremonie a cheii.

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

- Cel puțin trei angajați în roluri de încredere
- Ofițerul de securitate

- Cel puțin un reprezentant al Organismului de Management al Politicilor și Procedurilor (PPMB)
- Un maestru al ceremoniei cheie
- cel puțin un auditor 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 generării perechii de chei sunt înregistrate, datate și semnate de fiecare persoană prezentă în timpul generării. 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.
Cheile subiectului 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;
- AC 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 Livrare de chei private către beneficiar

Nu se aplică.

6.1.3 Livrarea cheii publice către autoritatea de certificare

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 a Autorității de certificare 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: http://www.certsign.ro/repository.

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 chei

CertSIGN SSL EV CA Class 3 G2 folosește o cheie de 2048 biți pentru certificate și semnarea CRL.

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

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

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 parametrilor

CERTSIGN are o procedură documentată pentru realizarea generării de perechi de chei CA pentru certSIGN SSL EV 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 cheie (conform câmpului KeyUsage X.509 v3)

Scopurile permise de utilizare a cheilor sunt descrise în câmpul KeyUsage (a se vedea capitolul 7.1.1.) Al extensiei standard a unui certificat conform cu X.509 v3. Acest câmp trebuie verificat în mod obligatoriu de către aplicația subiecților care gestionează certificatele.

Utilizarea biților din câmpul KeyUsage trebuie să respecte următoarele reguli:

A) digitalSignature: certificat destinat verificării semnăturii electronice,

b) non-repudiere: certificat destinat furnizării unui serviciu de non-repudiere de către persoane fizice, precum și în alte scopuri decât cele descrise la f) și g). Bitul de non-repudiere poate fi setat numai într-un certificat de cheie publică destinat verificării semnăturilor electronice și nu trebuie combinat cu scopurile descrise la punctele c) - e) și conectat cu asigurarea confidențialității,

c) keyEncipherment: destinat criptării cheilor algoritmului simetric, asigurând confidențialitatea datelor,

d) dataEncipherment: destinat criptării datelor subiectului, altele decât cele descrise la c) și e),

e) keyAgreement: destinat protocoalelor de schimb de chei,

f) keyCertSign: cheia publică este utilizată pentru verificarea semnăturii electronice în certificatele emise de entități care furnizează servicii de certificare,

g) cRLSign: cheia publică este utilizată pentru verificarea semnăturilor electronice pe listele de certificate revocate și suspendate emise de entitățile care furnizează servicii de certificare,

h) encipherOnly: poate fi utilizat exclusiv cu bitul keyAgreement pentru a indica scopul criptării datelor în protocoalele de schimb de chei,

i) decipherOnly: poate fi utilizat exclusiv cu bitul keyAgreement pentru a indica scopul decriptării datelor în protocoalele de schimb de chei.

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

- Certificate auto-semnate pentru a reprezenta CA Root în sine;
- Certificate pentru CA Intermediare și 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 folosind un sistem credibil care previne pierderea cheii private, revelarea, modificarea sau accesul neautorizat. Dacă o autoritate de certificare generează o pereche de chei la cererea subiectului / beneficiarului autorizat, aceasta trebuie să o livreze în siguranță subiectului și să impună subiectul pentru a-și proteja cheia privată.

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

- ETSI EN 319 411-2

Se iau măsuri pentru ca dispozitivele criptografice securizate să nu fie manipulate în timpul expedierii și în timp ce sunt stocate 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). Custodilor CA li se atribuie sarcina de a activa și dezactiva cheile private ale CA. Tastele CA sunt apoi active 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 al unei 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 tokenuri, protejate printr-un cod PIN și transferate autentificate proprietarului lor.

Procedura de transfer secret comun trebuie să includă: procesul de generare și distribuire a cheilor, acceptarea unui secret livrat și responsabilitățile rezultate 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). Când se află în afara dispozitivului criptografic securizat, cheia privată CA este protejată într-un mod care asigură același nivel de protecție pe care îl asigură 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.

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 Transferul cheii 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,
- atunci 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 în 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. 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 Corpului de gestionare 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 a Politicilor și Procedurilor (PPMB) autorizează distrugerea cheii private CA și repartizează personalul pentru sarcină.

Fiecare distrugere a cheii private este înregistrată în jurnalul de evenimente.

Subiectul este responsabil să distrugă cheia privată.

6.2.11 Evaluarea 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 EV CA Clasa 3 G2 sub forma unui 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 de două ori durata de viață a unui certificat, perioadă menționată mai jos.

Valorile standard ale perioadei maxime de utilizare a certificatelor Autorității de certificare sunt descrise în Tabelul 6.3.2.1, în timp ce certificatele subiectului sunt prezentate în Tabelul 6.3.2.2.

Perioadele de utilizare ale certificatelor și cheile 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.

Proprietar cheie	Scopul principal al utilizării cheii
	RSA pentru semnarea certificatului și a CRL
certSIGN SSL EV CA Clasa 3 G2	10 ani

Tabelul 6.3.2.1 Perioada maximă de utilizare a certificatelor CA.

Proprietar cheie	Politica de certificare	Utilizarea cheii principale
Entitati legale	SSL EV	397 zile;

Tabelul 6.3.2.2. Perioadele maxime de utilizare a certificatelor subiectului

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

Operatorii și administratorul Autorității de înregistrare și ai Autorității de certificare, precum și alte persoane care îndeplinesc rolurile descrise în capitolul 5.2 utilizează acreditări sigure (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 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 de un număr PIN, creat în conformitate cu cerințele FIPS-112. 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

Nu se aplică

6.5 Controale de securitate a computerului

Acest capitol descrie controalele de securitate ale computerului 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

Cerințele tehnice, prezentate în acest capitol, se aplică controlului de securitate al unui singur computer și controlului software instalat, utilizat pentru certSIGN. Securitate înseamnă că protecția sistemelor informatice se execută la nivelul sistemului de operare, al aplicației și al protecțiilor fizice.

Calculatoarele situate în autoritățile de certificare și în componentele asociate acestora (de exemplu, autoritatea de înregistrare) sunt echipate cu următoarele mijloace 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 alte procese după eliberarea obiectului de către un proces autorizat,
- Protecția criptografică a schimbului de informații și protecția bazelor de date,
- Arhiva istoricului operațiunilor efectuate pe computer și a datelor solicitate de audituri,
- O cale sigură care permite identificarea și autentificarea credibilă a rolurilor și a personalului care îndeplinește aceste roluri,
- Metode de restaurare cheie (numai în cazul modulelor de securitate hardware) și aplicație și sistem de operare,

- Monitorizarea și alertarea înseamnă în cazul accesului neautorizat la resurse de calcul.

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 mass-media în perioada în care înregistrările trebuie păstrate.

Datele sensibile vor fi protejate împotriva dezvăluirii prin intermediul obiectelor de stocare refolosite (de exemplu, fișiere șterse), accesibile utilizatorilor neautorizați. În acest scop, software-ul special va fi utilizat cu algoritmi de ștergere siguri pentru mediile de stocare, HSM-urile vor fi zero, dispozitivele criptografice securizate (jetoane / 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 ale sistemului de dezvoltare

O analiză a cerințelor de securitate se efectuează în etapa de proiectare și specificație a cerințelor proiectelor de dezvoltare a sistemelor implementate 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.

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 configurația acceptată și implementată.

Controalele aplicate sistemului CERTSIGN permit verificarea continuă a integrității aplicației, a versiunii lor 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 configurației care aplică politica de securitate a CERTSIGN.

Configurația actuală a sistemului Certsign, orice modificări aduse acestora, precum și orice versiuni ale versiunilor, modificărilor și remedierilor 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

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

a) sistemele noastre sunt segmentate în rețele sau zone bazate pe relații funcționale, logice și fizice (inclusiv locație) între sisteme și servicii de încredere. CERTSIGN aplică aceleași controale de securitate tuturor sistemelor co-amplasate în aceeași zonă.

b) accesul și comunicațiile între zone sunt limitate la cele necesare funcționării serviciilor de certificare. Conexiunile și serviciile nu sunt necesare sunt interzise sau dezactivate în mod explicit. Setul de reguli stabilit este revizuit în mod regulat.

c) toate sistemele care sunt esențiale pentru funcționarea serviciilor de certificare sunt păstrate într-una sau mai multe zone securizate

d) Rețeaua dedicată pentru administrarea sistemelor IT și rețeaua operațională sunt separate. Sistemele utilizate pentru administrarea implementării politicii de securitate nu sunt utilizate în alte scopuri. Sistemele de producție pentru serviciile de certificare sunt separate de sistemele utilizate în dezvoltare și testare (de exemplu, sisteme de dezvoltare, testare și etapizare).

e) Comunicarea între sisteme de încredere distincte se stabilește numai prin canale de încredere, care sunt în mod logic distincte de alte canale de comunicare și oferă identificarea asigurată a punctelor sale finale și protecția datelor canalului împotriva modificării sau divulgării.

f) Dacă este necesar un nivel ridicat de disponibilitate a accesului extern la un anumit serviciu de certificare, conexiunea la rețeaua externă este redundantă pentru a asigura disponibilitatea serviciilor în cazul unei singure defecțiuni.

g) se efectuează o scanare regulată a vulnerabilității adreselor IP publice și private identificate de certSIGN și se înregistrează dovezi că fiecare scanare a vulnerabilității a fost efectuată de o persoană sau entitate cu abilitățile, instrumentele, competența, codul de etică și independența necesare pentru a furniza un raport de încredere.

h) serviciile de certificare certSIGN sunt supuse unui test de penetrare a sistemelor conexe la instalare și după actualizarea infrastructurii sau a aplicațiilor sau modificările pe care certSIGN le consideră semnificative. Se înregistrează dovezi că fiecare test de penetrare a fost efectuat de o persoană sau entitate cu abilitățile, instrumentele, competența, codul de etică și independența necesare pentru a furniza un raport fiabil.

Serverele și stațiile de lucru de încredere ale sistemului CERTSIGN sunt conectate printr-o rețea locală (LAN), concepută în mai multe subrețele prevăzute cu acces controlat. Accesul de pe Internet la orice segment este protejat prin intermediul unui firewall inteligent.

Controalele de securitate sunt dezvoltate pe baza firewall-ului și a filtrării traficului pe routere și servicii proxy care protejează domeniile de rețea interne ale CERTSIGN de accesul neautorizat, inclusiv accesul subiecților / beneficiarilor și al terților. Firewall-urile sunt configurate pentru a preveni toate protocoalele și accesele care nu sunt necesare pentru funcționarea CERTSIGN CA.

Mijloacele de protecție a securității rețelei acceptă numai mesajele trimise cu utilizarea protocoalelor http, https, NTP, POP3 și SMTP. Evenimentele (jurnalele) sunt înregistrate în jurnalele de sistem și permit supravegherea corectitudinii utilizării serviciilor furnizate de CERTSIGN. Componentele rețelei locale (de exemplu, ruterele) trebuie păstrate într-un mediu sigur din punct de vedere fizic și logic și configurațiile lor trebuie verificate periodic pentru a se conforma cerințelor specificate de CERTSIGN.

CERTSIGN întreține și protejează toate sistemele CA în cel puțin o zonă securizată și are în vigoare o procedură de securitate care protejează sistemele și comunicațiile dintre sistemele din interiorul zonelor securizate și zonelor de înaltă securitate.

CERTSIGN configurează toate sistemele CA eliminând sau dezactivând toate conturile, aplicațiile, serviciile, protocoalele și porturile care nu sunt utilizate în operațiunile CA.

CERTSIGN acordă acces la zonele securizate și zonele de înaltă securitate numai rolurilor de încredere.

Sistemul CA Root se află într-o zonă de securitate ridicată.

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).

6.9 Controale specifice modulelor criptografice

Controalele modulelor criptografice includ cerințe impuse pentru dezvoltarea, producția și livrarea modulelor. CERTSIGN nu definește cerințele de proprietate în acest domeniu. Cu toate acestea, CERTSIGN acceptă și utilizează numai module criptografice care respectă cerințele din capitolul 6.2.

7 Certificat, CRL și profil 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, au aplicat extensii standard și private utilizate de CERTSIGN.

7.1 Profilul certificatului

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

Profilul câmpurilor de bază pentru certificatele emise de certSIGN SSL EV CA Clasa 3 G2 este descris în Tabelul 7.2 din documentul extern "certSIGN SSL EV 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 EV CA Clasa 3 G2 sunt descrise în Tabelul 7.3.

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

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

7.1.3 Identificatori de algoritm obiect

Identificatorul de algoritm criptografic este descris in #7.1.3 din documentul extern "certSIGN SSL EV CA Class 3 G2 - Anexa Profile.docx".

7.1.4 Forme de nume

Conținutul câmpurilor trebuie să îndeplinească cerințele din secțiunea 3.1 și ghidurile ultimei versiuni publicate ale EV Forum CAB.

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

Nu se aplică.

7.1.6 Identificator de obiect al politicii de certificat

Identificatorii obiectelor politicii certificatelor utilizate la nivelul certSIGN SSL EV CA Clasa 3 G2 sunt descrise în Tabelul 7.6 și Tabelul 7.7 din documentul extern "certSIGN SSL EV CA Class 3 G2 - Anexa Profile.docx".

7.1.7 Utilizarea extensiei de constrângeri de politică

Nu se aplică.

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

Nu se aplică.

7.2 Profil CRL

Profilul CRL este descris în Tabelul 7.8 din documentul extern "certSIGN SSL EV 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 Extensii de intrare CRL și CRL

Extensiile CRL pentru certSIGN SSL EV CA Clasa 3 G2 sunt descrise în Tabelul 7.9 si in #7.2.2 din documentul extern "certSIGN SSL EV CA Class 3 G2 - Anexa Profile.docx".

7.3 Profil OCSP

Protocolul de verificare a stării certificatului on-line (OCSP) este descris in #7.3 din documentul extern "certSIGN SSL EV CA Class 3 G2 - Anexa Profile.docx".

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 extensiile descrise in #7.3.2 din documentul extern "certSIGN SSL EV CA Class 3 G2 - Anexa Profile.docx"

8 Auditul conformității 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 cu criteriile din Regulamentul 910/2014 și actele sale de punere în aplicare și CA/B Forum, Ghiduri CA/B Forum EV, respectăm cerințele din standardul ETSI EN 319 403.

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.

Auditul verifică conformitatea cu prezentul CPP și ETSI 319401, ETSI 319411, CA/B Forum Baseline Requirements, CA/B Forum EV Guidelines technical standards.

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

8.2 Identitatea / calificările evaluatorului

Evaluarea va fi efectuată de un auditor extern independent, în conformitate cu criteriile Programului WebTrust EV pentru criteriile AC.

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 de CPP Web CA.

8.5 Acțiuni întreprinse ca urmare a deficienței

Organismul de evaluare a conformității raportează deficiențelor și neconformităților 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 efectua 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.

8.7 Auto-audituri

În perioada în care CA emite certificate, CA monitorizează respectarea cerințelor sale de bază ale forumului CPP și CA/B 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 Taxe

Taxele 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 emitere și reînnoire a certificatelor digitale

Prețurile sunt stabilite în conformitate cu politica internă a prețurilor.

9.1.2 Taxe de acces la certificat

Serviciu gratuit.

9.1.3 Taxe de acces la informațiile de revocare sau de stare

Prețurile sunt stabilite în conformitate cu politica internă a prețurilor.

9.1.4 Alte taxe

Prețurile sunt stabilite în conformitate cu politica internă a prețurilor.

9.1.5 Rambursarea taxelor

Plăți pot fi rambursate conform condițiilor contractuale aplicabile..

9.2 Responsabilitatea financiară

9.2.1 Acoperirea prin asigurare

CERTSIGN îndeplinește cerințele obligatorii din secțiunea 8.4.Asigurarea din liniile directoare CA/B Forum EV.

CERTSIGN has professional insurance policies in place and will cover any damages it may cause due to certification services for persons building their ethics on the legal effects of certificates issued by certSIGN CAs within the limits set by this CPP, contractual agreements entered into, as applicable.

9.2.2 Alte bunuri

Nu se aplică.

9.2.3 Asigurarea sau acoperirea garanției pentru entitățile finale

CERTSIGN îndeplinește cerințele obligatorii din secțiunea 8.4.Asigurarea din liniile directoare CA/B Forum EV.

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 publice

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 Reprezentări și garanții CA.

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 certificatelor includ în mod specific cele specificate în *"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"*, punctul 9.6.1. și în CA/B Forum EV Guidelines punctul 7.1.

9.6.2 Reprezentări și garanții RA

RA are obligația de a respecta scrupulos CPP, secțiunea relevantă a CP aplicabilă și procedurile interne relevante CERTSIGN.

9.6.3 Reprezentări și garanții ale 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 *"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"*, punctul 9.6.3.

9.6.4 Reprezentări și garanții ale 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 când a expirat
- Luarea la cunoștință a prevederilor prezentului CPP, a garanțiilor și limitelor răspunderii Certsign SA

9.6.5 Reprezentanțe și garanții ale altor participanți
Fără stipulare

9.7 Declinarea garanțiilor
Cu excepția cazului în care se prevede altfel în mod expres în CPP, CP aplicabil 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 (pentru când provine dintr-o sursă autorizată) și, în plus, își declină orice responsabilitate 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 certSIGN) CERTSIGN nu va fi răspunzător pentru:

- Orice pierdere de profit, 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.

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 în paragraful „9.9 Despăgubiri de către AC" din "*Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates" și* în paragraful 18. Răspundere și despăgubire din liniile directoare EV Forum CA / B.

9.10 Termeni și reziliere

9.10.1 Termeni
Prezentul CPP și orice modificări la acesta vor intra în vigoare după publicarea în depozit 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 rezultat în urma rezilierii 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 și 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

Nu se aplică.

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 legii 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 *"Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates"*.

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 dispoziții

Fără stipulare.