Codul de Practici și Proceduri certSIGN for BNR

Versiunea 1.2

Data: 15 Ianuarie 2026

Notă importantă

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

Telefon: 004-021-31.19.901

Web: www.certsign.ro

Istoric document

Versiune	Data efectivă	Motiv	Persoana care a făcut modificarea
1.0	29 Noiembrie 2024	Publicarea primei versiuni	Responsabil PKI
1.1	15 Ianuarie 2025	Revizie anuala	Manager Politici PKI
1.2	15 Ianuarie 2026	Revizie anuala	Manager Politici PKI

Acest document a fost creat de către și este proprietatea:

Proprietar	Autor	Data creării
certSIGN	Responsabil PKI	Noiembrie 2024

Lista de distribuție

Destinație	Data distribuirii
Public-Internet	Noiembrie 2024
Public-Internet	Ianuarie 2025
Public-Internet	Ianuarie 2026

Acest document a fost aprobat de:

Versiune	Nume	Data
1.0	Comitet de Management al Politicilor și Procedurilor (CMPP)	Noiembrie 2024
1.1	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2025
1.2	Comitet de Management al Politicilor și Procedurilor (CMPP)	Ianuarie 2026

Content

1 Introducere

Codul de Practici și Proceduri certSIGN for BNR (denumit în continuare **CPP certSIGN for BNR** sau **CPP**) descrie politica de certificare și practicile pe care **certSIGN** le aplică în emiterea de certificate digitale către **BNR** (Banca Nationala a Romaniei - BNR) si partenerii acesteia, pentru utilizare în circuit închis.

Structura și conținutul **CPP certSIGN for BNR** respectă în general recomandările RFC 3647, ETSI EN 319 411-1, precum si ale CA/B Forum Baseline Requirements, cu excepții datorate specificului sistemului PKI care este în Circuit Închis – NU este Public.

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

1.1 Descriere Generală

certSIGN, BNR, Beneficiarii, Subiecții și Entitățile Partenere asociate trebuie să respecte prezentul **CPP certSIGN for BNR** pentru emiterea certificatelor pentru autentificare și semnătură electronică și a certificatelor TLS. Documentul descrie, de asemenea, regulile generale de furnizare a serviciilor de certificare, precum înregistrarea Subiecților, certificarea cheii publice, rekey certificate și revocarea certificatelor.

1.2 Denumirea documentului și identificarea

Titlul acestui document este " Codul de Practici și Proceduri certSIGN for BNR", și este denumit în continuare "CPP certSIGN for BNR" sau „CPP".

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

1.3 Participanții PKI

CPP certSIGN for BNR reglementează cele mai importante relații dintre entitățile BNR, echipele de consultanți (inclusiv auditorii) și clienții (utilizatorii serviciilor furnizate) acesteia:

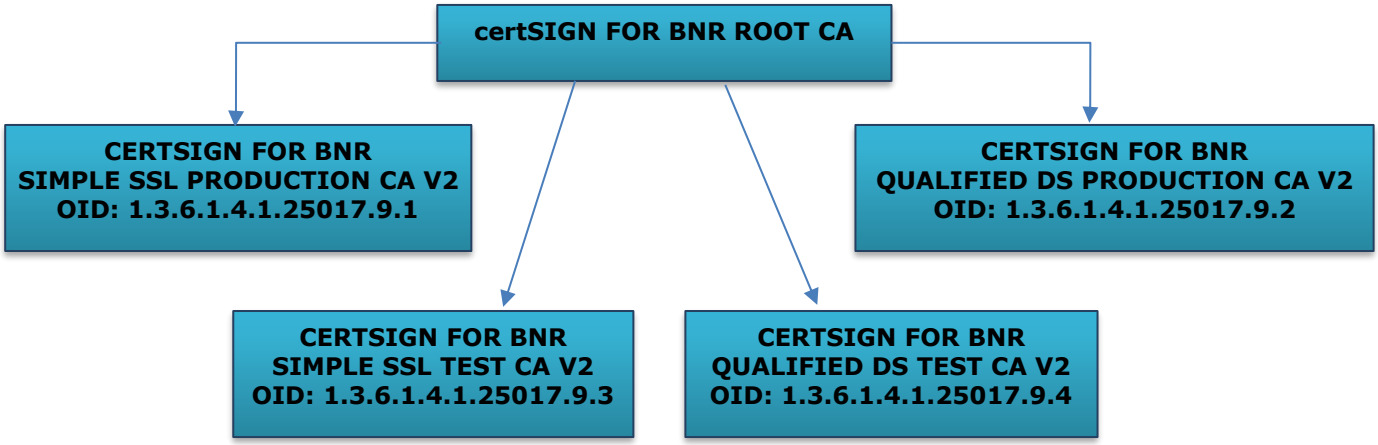
- certSIGN for BNR ROOT CA,
- Autoritățile intermediare subordonate certSIGN FOR BNR ROOT CA,
- Autoritatea de Înregistrare,
- Depozitar/Repository,
- Subiecții,
- Beneficiarii,
- Entitățile Partenere,
- Furnizorii relevanți ai BNR din punct de vedere al emiterii și managementului certificatelor digitale,
- Comitetul de Management al Politicilor și Procedurilor,
- Auditorii.

certSIGN oferă servicii de certificare interne pentru orice persoană fizică sau entitate juridică, din cadrul BNR, care este de acord cu prevederile prezentului CPP. Scopul prezentului CPP (ce include procedurile de generare a cheilor, procedurile de emitere a certificatelor şi securitatea sistemului informaţional) este acela de a garanta utilizatorilor serviciilor **certSIGN** că nivelele de credibilitate declarate ale certificatelor emise corespund practicilor Autorităţilor de Certificare.

1.3.1 Autoritățile de Certificare

certSIGN for BNR ROOT CA este Autoritatea de Certificare primară pentru sistemul PKI cu circuit închis al BNR.

certSIGN for BNR ROOT CA este identificată prin următorul OID: 1.3.6.1.4.1.25017.8.1
Autoritățile de Certificare Intermediare, subordonate **certSIGN FOR BNR ROOT CA**, sunt: certSIGN FOR BNR SIMPLE SSL PRODUCTION CA V2, certSIGN FOR BNR QUALIFIED DS PRODUCTION CA V2, certSIGN FOR BNR SIMPLE SSL TEST CA V2, certSIGN FOR BNR QUALIFIED DS TEST CA V2.



Înainte de începerea activității, certSIGN FOR BNR SIMPLE SSL TEST CA V2 trimite o cerere Autorității de Certificare Primare, **certSIGN FOR BNR ROOT CA** pentru înregistrare și emiterea certificatului de cheie publică. Procesul este similar și pentru certSIGN FOR BNR SIMPLE SSL PRODUCTION CA V2, certSIGN FOR BNR QUALIFIED DS PRODUCTION CA V2 și certSIGN FOR BNR QUALIFIED DS TEST CA V2.

1.3.2 Autoritățile de Înregistrare

Autoritatea de Înregistrare primeşte, verifică și aprobă sau respinge cererile de înregistrare şi emitere de certificate, de rekey certificat sau revocare a certificatelor. Verificarea cererilor are ca scop autentificarea (pe baza documentelor incluse în cereri) atât a beneficiarului/subiectului, cât şi a datelor incluse în cerere. Autoritatea de Înregistrare poate trimite cereri către Autoritatea de Certificare corespunzătoare pentru a anula o cerere sau pentru a revoca un certificat.
Autoritatea de Înregistrare este operată de BNR și de certSIGN.

1.3.3 Beneficiarii

Beneficiar

Beneficiarii sunt persoane fizice care solicită certSIGN prin BNR emiterea unui certificat.
În acest caz, Beneficiarul este Subiectul certificatului emis de certSIGN, în legătură cu organizația la care este angajat, verificată de BNR.
Beneficiarii pot solicita emiterea, revocarea sau rekey-ul certificatelor. Un Beneficiar este responsabil, deasemenea, de notificarea certSIGN imediat după suspiciunea de compromitere a cheii private.

Subiect

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

- Persoana fizică pentru care Beneficiarul solicită certificatul, acesta din urma acționând ca angajator/partener al său,

Un Subiect este responsabil, deasemenea, de:

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

1.3.4 Entitățile Partenere

O Entitate Parteneră este orice entitate care foloseste serviciile de certificare digitală ale certSIGN si ia decizii bazate pe corectitudinea legăturii dintre identitatea Subiectului și cheia publică.
O Entitate Parteneră este responsabilă de modul cum verifică starea curentă a certificatului unui Subiect. O astfel de decizie va fi luată de fiecare dată când o Entitate Parteneră dorește să utilizeze un certificat pentru a verifica o semnătură electronică, identitatea sursei sau autorul unui mesaj sau pentru a crea un canal de comunicare securizat cu Subiectul certificatului. O Entitate Parteneră va utiliza informațiile dintr-un certificat (de exemplu identificatori și calificatori ai politicii de certificare) pentru a decide dacă un certificat a fost utilizat în concordanță cu scopul definit.

1.3.5 Alți participanți

Comitetul de Management al Politicilor și Procedurilor ("CMPP") este un Comitet creat în cadrul certSIGN de către Consiliul de administrație pentru a supraveghea întreaga activitate a Autorităților de Certificare și a Autorităților de Înregistrare ale certSIGN. Rolurile și responsabilitățile CMPP sunt descrise în documentația internă certSIGN.
Furnizorii de servicii ai certSIGN sunt furnizori externi care sprijină activitățile certSIGN pe baza unui acord contractual semnat (de ex. Firmele de curierat).

1.4 Utilizarea certificatului

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

- Unul care defineşte aplicabilitatea certificatului (de exemplu, semnătura electronică, confidențialitate),
- Și unul care presupune o listă sau o descriere a aplicaţiilor permise sau interzise.

Entitatea Parteneră este responsabilă de stabilirea nivelului de credibilitate necesar pentru un certificat utilizat într-un anume scop. Luând în considerare factorii de risc semnificativi, Entitatea Parteneră trebuie să stabilească ce tip de certificat emis de certSIGN întruneşte cerinţele formulate. Subiecţii trebuie să cunoască cerinţele Entităţii Partenere (de exemplu, aceste cerinţe pot fi publicate sub forma unei politici de semnătură sau a unei politici de securitate informatică) şi apoi să solicite certSIGN emiterea de certificate corespunzătoare acestor cerinţe.

1.4.1 Utilizări admise ale certificatului

Certificatele pot fi utilizate în aplicații care satisfac cel puțin următoarele condiții:

- Gestionează în mod corespunzător cheile publice și cheile private,
- Certificatele și cheile publice asociate acestora sunt folosite în concordanţă cu scopul declarat al acestora, confirmat de certSIGN,

- Dispun de mecanisme interne de verificare a stării certificatelor, de creare a căilor de certificare și controlul validităţii (validitatea semnăturii, data expirării etc.),
- Oferă utilizatorului informaţii corespunzătoare despre certificate și despre starea lor.

Aplicațiile pentru care se consideră că Certificatul este de încredere vor fi decise chiar de către Entitățile Partenere, pe baza naturii și scopului (inclusiv utilizarea cheii) Certificatului, inclusiv orice limitare aplicabilă în scris în Certificat.

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

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

1.4.2 Utilizări interzise ale certificatului

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

1.5 Administrarea politicii

1.5.1 Organizația care administrează documentul

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

Nume	certSIGN S.A. Sediu: Bd. Tudor Vladimirescu, nr. 29 A, AFI Tech Park 1, București, România Nr. înregistrare Registrul Comerțului: J2006000484402 Cod de înregistrare fiscală: RO 18288250 Sediu social: Str. Olteniței, nr. 107A, clădirea C1, etaj 1, camera 16, Sector 4, București, România, CP 041303
Telefon	(+4021)3119901
e-mail	office@certsign.ro
Web	www.certsign.ro

Tabel: 1.5.1 Organizația ce administrează documentul

1.5.2 Persoana de contact

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

Tabel: 1.5.2 Persoana de contact

Procedura de raportare a certificatelor cu probleme

Din cauza unor erori, limitări tehnice sau procedurale, ori din alte motive, pot exista certificate emise greșit de certSIGN (ex. certificatul emis conține informații eronate despre subiect sau

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

1. Natura presupusei probleme.

2. Numarul de rapoarte de certificate cu probleme primite despre un anumit Certificat sau Beneficiar.

3. Entitatea care raportează (de exemplu, o reclamatie din partea unui angajat al unei autorități de aplicare a legii potrivit căreia un site Web este implicat în activități ilegale ar trebui să aibă mai multă greutate decât o reclamație a unui consumator care susține că nu a primit bunurile comandate); și

4. Legislația relevantă.

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

1.5.3 Persoana care decide conformitatea CPP cu politica

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

Tabel: 1.5.3 Persoana ce decide conformitatea CPP cu politica

1.5.4 Procedurile de aprobare a CPP

Comitetul de Management al Politicilor și Procedurilor este responsabil de aprobarea CPP. Procedura de aprobare este descrisă într-un document de instrucțiuni interne.

Subiecții/Beneficiarii trebuie să respecte CPP-ul în vigoare, publicat la adresa https://www.certsign.ro/ro/depozitar/.

1.6 Definiții și acronime

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Subiect (Entitate finală): entitate identificată într-un certificat ca fiind deținătorul cheii private asociate cheii publice din certificat
CA subordonat - autoritate de certificare al cărei certificat este semnat de Root CA sau de un alt CA subordonat
Beneficiar – persoană juridică sau fizică legată prin contractul cu un furnizor de servicii de încredere de toate obligațiile Beneficiarului
Prestator de servicii de încredere – o persoană fizică sau juridică ce furnizează unul sau mai multe servicii de încredere, fie ca furnizor de servicii de încredere calificate, fie ca furnizor de servicii de încredere ne-calificate;

CA	Autoritate de certificare
CPP	Cod de Practici și Proceduri
CRL	Lista de Certificate Revocate
CARL	Lista de Revocare a Autorității de Certificare
DN	Nume distinctiv
HW	Hardware
NIMB	Institutul Național de Metrologie București
PKI	Infrastructură cu Cheie Publică
CMPP	Comitet de Management al Politicilor și Procedurilor
QSCD	Dispozitiv de Creare a Semnăturilor Electronice Calificate
RA	Autoritate de Înregistrare
RSA	Algoritmul criptografic asimetric Rivest, Shamir, Adleman
UTC	Timpul Universal coordonat

2 Publicare și responsabilități Depozitar

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

2.1 Depozitare

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

- Codul de Practici și Proceduri pentru CA-urile operate de certSIGN
- Certificatele certSIGN FOR BNR ROOT CA și ale CA-urilor intermediare
- Listele Certificatelor Revocate
- Temenii și condițiile privind utilizarea certificatelor digitale

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

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

2.2 Publicarea informațiilor de certificare

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

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

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

Disponibilitate

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

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

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

2.3 Timpul sau frecvența publicării

Informațiile publicate de certSIGN sunt actualizate cu următoarea frecvență:

- CPP – vezi Capitolul 1.5,

- Certificatele Autorităților de Certificare – după emiterea unui nou certificat;
- Certificatele Subiecților – la obținerea consimțământului, după fiecare emitere a unui nou certificat;
- Lista certificatelor revocate este creată fie o dată la 24 de ore, fie atunci când un certificat este revocat;
- Informațiile suplimentare – după fiecare actualizare.

2.4 Controlul accesului la Depozitare

Toate informațiile publicate de certSIGN în Depozitar la adresa https://www.certsign.ro/ro/depozitar/ sunt accesibile angajatilor și partenerilor BNR.

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

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

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

La descoperirea unor breşe ce afectează integritatea informaţiilor din Depozitar, certSIGN va lua măsurile corespunzătoare pentru a restabili integritatea informaţiilor, va trage la răspundere pe cei vinovaţi și va notifica imediat entităţile afectate.

3 Identificarea și autentificarea

3.1 Denumirea

3.1.1 Tipuri de nume

Certificatele emise de certSIGN sunt conforme cu standardul X.509 v3. Aceasta înseamnă că certSIGN și Autoritatea de Înregistrare (BNR) care acționează în numele emitentului aprobă numele Subiectului în conformitate cu prevederile standardului X.509 (cu referire la recomandările seriei X.500). Denumirile Subiecților și ale emitenților de certificate din certificatele BNR sunt în conformitate cu structura de nume Distinctive Name (DN) – (cunoscute și ca structuri de tip Directory Name), create conform recomandărilor X.500 și X.520.

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

3.1.2 Nevoia ca Numele să aiba înțeles logic

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

DN constă în câmpuri obligatorii și opționale, conform recomandărilor RFC 5280 și X.520, in acord cu Protocolul Tehnic dintre certSIGN si BNR, specificat în Anexele 1 si 2 (documente separate de acest CPP)

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

3.1.3 Anonimitatea sau pseudonimitatea Beneficiarilor

N/A.

3.1.4 Reguli de interpretare a diferitelor formate de nume

Interpretarea câmpurilor din certificatele emise de certSIGN se face în concordanţă cu profilele de certificate descrise în Profilul certificatelor şi al CRL-urilor (Capitolul 7). Caracterele speciale din nume se preiau din documentul de identitate: fie din MRZ, fie din campurile de nume, in conformitate cu standardele precizate in procedurile interne ale certSIGN. Crearea şi interpretarea DN-ului vor fi realizate conform recomandărilor specificate în Capitolul 3.1.2.

3.1.5 Unicitatea numelor

Pentru certificate de semnare/sigilare:

Unicitatea numelui este asigurată prin utilizarea numărului serial al Subiectului atribuit de CA.

3.1.6 Recunoașterea, autentificarea și rolul mărcilor înregistrate

Nu se aplică.

3.2 Validarea Inițială a Identității

3.2.1 Dovada Posesiei Cheii Private

Perechea de chei este generată de Autoritatea de Certificare sau de Autoritatea de Înregistrare certSIGN.

3.2.2 Autentificarea identității organizației

Autentificarea identității organizației

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

3.2.2.1 Identitatea

BNR notifică certSIGN, printr-o adresa scrisă sau printr-un e-mail semnat digital şi criptat sau e-mail ce conţine ca ataşament un document semnat digital şi criptat, asupra participanţilor (instituţii/persoane juridice) care sunt autorizaţi de către Banca Naţională a României să participe in PKI, comunicând pentru fiecare nou participant următoarele date:

- numele complet al instituţiei/persoanei juridice;
- adresa sediului social;
- copii ale fişelor administratorilor de securitate desemnaţi de participant.

BNR va transmite la certSIGN copia fiecărei noi fişe de administrator de securitate avizată. certSIGN a încheiat contracte cu fiecare participant prin care se achiziţionează produsele şi serviciile certSIGN necesare conectării şi utilizării serviciilor oferite de SEP.

3.2.2.2 DBA (Doing Business As)/ Nume Comercial

N/A

3.2.2.3 Verificarea țării

RA accepta emiterea doar pentru România.

3.2.2.4 Validarea Autorizării sau Controlului Domeniului

Autorizarea este validată de către BNR conform cu #3.2.2.1.

3.2.2.5 Autentificarea pentru o Adresă IP

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

3.2.2.6 Validarea unui Domeniu Wildcard

N/A

3.2.2.7 Acuratețea Sursei Datelor

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

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

3.2.2.8 Inregistrarile Autorității de Autentificare si Certificare (CAA)

N/A

3.2.3 Autentificarea identității persoanelor fizice

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

- act de identitate sau pașaport, în cazul cetățenilor români

Verificarea identității persoanelor fizice trebuie realizată:

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

Toate documentele necesare identificării persoanelor fizice vor fi prezentate reprezentanților Autorității de Înregistrare în original sau în copie însoțită de acceptarea Termenilor și condițiilor de furnizare a serviciilor de certificare și CPP.
certSIGN își rezervă dreptul de a nu furniza certificate calificate în cazul în care există indicii rezonabile privind valabilitatea sau veridicitatea documentelor prezentate de către Subiect (carte de identitate sau pașaport deteriorate sau care nu întrunesc cerințele minime de securitate).

3.2.4 Informații neverificate cu privire la Beneficiar

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

Adresa de e-mail și numărul de telefon reprezintă informații neverificate ale Subiectului.

3.2.5 Validarea autorității

certSIGN a stabilit un proces care permite unui Beneficiar să specifice persoanele care pot solicita certificate. Dacă un Beneficiar specifică, în scris, persoanele care pot solicita un certificat, certSIGN nu va accepta nici o cerere de certificat care este în afara acestei specificații.

certSIGN verifică (prin BNR) dacă persoana fizică are drepturi, funcții sau permisiuni specifice, inclusiv mandatul de a acționa în numele entității juridice, pentru a obține un certificat.

3.2.6 Criterii pentru interoperare

N/A.

3.3 Identificarea și autentificarea pentru cererile de re-key

3.3.1 Identificarea și autentificare pentru re-key de rutină

Capitolul 4.7 al acestui document descrie acest proces.

3.3.2 Identificarea și autentificarea pentru re-key după revocare

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

3.4 Identificarea și autentificarea pentru cererile de revocare

Următoarele entități pot trimite cereri de revocare a certificatelor:

- Subiectul care este deținătorul cheii private asociate cheii publice din certificat va trimite cererea de revocare
    - Subiectul comunică telefonic şi prin e-mail semnat digital sau e-mail ce conţine ca ataşament un document semnat digital către BNR şi administratorii de securitate ai Beneficiarului decizia de revocare a certificatului, precizând motivele care au stat la baza revocării.
- Beneficiarul care încheie un acord contractual cu certSIGN pentru emiterea de certificate Subiecților va trimite cererea de revocare
    - pe baza formularului „Cerere pentru revocarea de certificate digitale”- transmis de Beneficiar prin adresa scrisă si/sau numai prin e-mail semnat digital sau e-mail
- Autoritatea de Înregistrare care poate cere revocarea fie în numele unui Subiect, fie fiindca deține informații care justifică revocarea certificatului utilizând mecanismele de securitate ale software-ului Autorității de Înregistrare.

- Rolurile de încredere asociate certSIGN CA, sub supravegherea Comitetului de Management al Politicilor și Procedurilor (CMPP) utilizând mecanismele de securitate ale software-ului Autorității de Certificare.

4 Cerințe operaționale privind ciclul de viață al certificatului

Acest capitol descrie procedurile de bază care se aplică tuturor tipurilor de certificate emise de certSIGN CA.
O descriere detaliată a procedurilor referitoare la serviciile componente PKI (CA-uri, RA-uri, CRL Signers, etc.) și persoanele/rolurile implicate în procesul operațional al acestor componente este inclusă în documentația internă confidențială.
certSIGN oferă acces la următoarele servicii:

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

4.1 Cererea de certificat

4.1.1 Cine poate trimite o cerere de certificat

Persoanele Fizice

Pot solicita certificate:

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

Beneficiarul și Subiectul vor respecta prevederile și obligațiile stabilite în Termenii și Condițiile serviciilor de certificare ce încorporează acest CPP.
Autoritatea de Certificare emite certificate doar ca răspuns la o cerere primită de la Autoritatea de Înregistrare operată de certSIGN sau de la o terță parte delegată.
certSIGN arhivează informațiile referitoare la înregistrare. Arhiva este menținută în conformitate cu cerințele definite în CPP și în legislația aplicabilă.

Entitățile Juridice (Organizații)

certSIGN emite certificate pentru sigiliile electronice entităților juridice apartinand BNR. Subiectul va respecta prevederile și obligațiile stabilite în Termenii și Condițiile serviciilor de certificare ce încorporează acest CPP.

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

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

4.1.2 Procesul de înregistrare și responsibilitățile

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

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

În orice situație, certSIGN, în calitate de furnizor de servicii de încredere, răspunde, în limitele prevăzute în prezentul CPP pentru actele sau omisiunile tuturor agenților, angajatilor si colaboratorilor săi implicati în procesul de inregistrare.

RA este responsabilă de verificarea următoarelor elemente, conform procedurilor interne ale certSIGN:

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

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

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

- Termeni și Condiții
- adresa online a Termenilor și Condițiilor privind utilizarea certificatului
- adresa online a CPP, notificări sau alte documente necesar a fi furnizate de Subiect

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

- responsabilitatea sa ca informațiile furnizate către RA sunt corecte, complete, valabile și actualizate,
- că certSIGN păstrează o perioadă de 3 ani de la data expirării/revocării certificatului toate informațiile referitoare la înregistrare și înscriere, la cererea de certificat și la revocarea certificatului,
- că, în cazul în care certSIGN (în calitate de CA și RA) își încetează activitatea, aceste date pot fi transferate către o terță parte,
- recunoaște drepturile, obligațiile și responsabilitățile certSIGN și ale altor participanți la PKI, astfel cum sunt definite în legislațiile naționale,
- că Subiectul/Beneficiarul are obligația de a informa certSIGN cu privire la orice schimbare sau eveniment care poate afecta valabilitatea sau conținutul certificatului.

Procesul de înregistrare

Procesul de înregistrare începe în cadrul RA.
Responsabilitatea entității RA este de a colecta și verifica documentele/informațiile necesare pentru validarea identității și atributelor Subiectului/Beneficiarului, conform procedurilor interne ale certSIGN.

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

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

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

4.2 Procesarea cererilor de certificate

certSIGN acceptă cereri pentru un subiect sau mai mulți. Cererile pot fi trimise fizic și electronic.
BNR transmite către certSIGN, pe suport hârtie, e-mail semnat digital şi criptat sau e-mail ce conţine ca ataşament un document semnat digital şi criptat, formularul ”Cerere pentru emiterea/reînnoirea de certificate digitale”, avizat de BNR.

certSIGN va contacta unul dintre administratorii de securitate ai Beneficiarului şi îi va comunica următoarele informaţii:

- Data şi locaţia la care utilizatorul desemnat se poate prezenta pentru generarea cheilor şi ridicarea certificatelor digitale, dispozitivelor securizate, aplicaţiilor de semnare şi criptare
- Datele de contact ale reprezentantului certSIGN care poate furniza informaţii suplimentare (număr de telefon, adresa email, fax).

4.2.1 Îndeplinirea funcțiilor de identificare și autentificare

RA realizează identificarea și autentificarea în conformitate cu procedura definită în capitolul 3.2 și în documentația internă confidențială.
RA colectează și validează informațiile despre identitatea și despre atributele Subiectului și ale Beneficiarului.

4.2.2 Aprobarea sau respingerea cererilor de certificate

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

4.2.3 Timpul de procesare a cererilor de certificate

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

Certificatele sunt stocate fie pe un dispozitiv securizat de tip token, fie in format software conform cu standardele PKCS#12 si Java Keystore.

4.3 Emiterea certificatelor

4.3.1 Acțiunile CA în timpul emiterii certificatelor

Certificatul este emis de CA numai după primirea unei solicitari de certificat de la RA. CA și RA sunt sisteme integrate și comunică prin conexiuni de rețea închise. CA procesează numai cererile care provin de la RA-ul de încredere al certSIGN.
CA asigură unicitatea fiecărui certificat pe care îl emite utilizând câmpul SerialNumber din fiecare certificat.

4.3.2 Notificarea Subiectului de către CA cu privire la emiterea certificatului

certSIGN notifică BNR prin email semnat digital asupra emiterii noilor certificate pentru participanţi în ziua emiterii.

certSIGN asigură transmiterea către BNR a certificatelor emise.

4.4 Acceptarea certificatului

4.4.1 Conduita care constituie acceptarea certificatului

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

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

- Informația din certificat nu este corectă,
- Informațiile din certificat au devenit nevalide de la data înregistrării,

Obligațiile Subiectului și ale RA în caz de respingere:

- RA cere revocarea certificatelor,
- RA execută revocarea certificatelor.

4.4.2 Publicarea certificatului de către CA

Vezi capitolul 2.

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

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

4.5 Utilizarea perechii de chei și a certificatului

4.5.1 Utilizarea cheii private și a certificatului

Subiectul este responsabil personal pentru:

- utilizarea cheilor numai pentru uzul prevăzut, așa cum este definit în acest CPP și codat în certificate;
- Cheile private care corespund certificatelor emise în baza acestui CPP vor fi utilizate numai pentru a crea semnături electronice sau sigilii electronice.
- Utilizarea de instrumente care pot interpreta în mod corect utilizarea cheii așa cum este ea codificată în certificat și care respectă condițiile cheie de utilizare
- Ștergerea datelor secrete de activare (de exemplu codul PIN) care sunt unice și respectă directivele din CPP
- Păstrând confidențialitatea acestor informații secrete
- Stocarea în siguranță a oricărui document sau a unui mediu care conține transcrierile unei părți sau a tuturor datelor de activare secretă asociate (de exemplu cod PIN)
- Nedezvăluirea datele de activare secretă (de exemplu codul PIN) unei alte persoane.

Cheia privată generată de certSIGN

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

- Distribuirea sigură a datelor inițiale asociate secrete necesare activării (de exemplu codul PIN) către subiect.

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

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

4.5.2 Utilizarea cheii publice și a certificatului unei Entități Partenere

certSIGN presupune că toate aplicațiile software sunt conforme cu standardul X.509 și alte standarde aplicabile ce impun cerințele și seturile de cerinte menționate în acest CPP. certSIGN nu garantează că software-ul oricărei entități partenere va suporta sau impune asemenea controale și cerințe, și toate entitățile partenere sunt sfătuite să identifice suport tehnic și legal adecvat.

Părțile care se bazează pe un certificat verifică în orice moment o semnătură digitală prin verificarea valabilității unui certificat digital cu ajutorul serviciului CRL publicat de certSIGN.

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

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

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

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

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

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

4.6 Reinnoirea certificatului

N/A

4.7 Rekey-ul certificatului

4.7.1 Circumstante pentru rekey-ul certificatului

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

4.7.2 Cine poate solicita certificarea unei noi chei publice

certSIGN informează întotdeauna Subiecții (cu cel puțin 30 de zile înainte) despre apropierea perioadei de expirare.
Rekey-ul se efectuează atunci când un subiect care deține un certificat digital valabil (nu este revocat și nu este expirat) generează o nouă pereche de chei (sau solicită certSIGN să genereze o astfel de pereche de chei) și solicită emiterea unui nou certificat pentru a confirma deținerea unei chei publice nou create.
Rekey-ul certificatului se efectuează numai la solicitarea Subiectului și este precedat de depunerea unei cereri pe un formular corespunzător completat de către Beneficiar/Subiect.

4.7.3 Procesarea cererilor de re-key a certificatelor

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

4.7.4 Notificarea emiterii noului certificat către beneficiar

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

4.7.5 Conduita ce constituie acceptarea unui certificate re-key
RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.7.6 Publicarea certificatului re-key de către CA
RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

4.7.7 Notificarea eliberării certificatului de către CA altor entități
RA utilizează aceleași procese ca și pentru un certificat nou solicitat.

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

4.9 Revocarea și Suspendarea Certificatului
Certificatele emise de certSIGN CA pot fi revocate dar niciodata suspendate. Revocarea certificatelor este un process ireversibil.

Revocarea nu afectează nici tranzactiile efectuate înainte de revocare nici obligațiile ce rezultă din aderarea la prezentul CPP.
Aceste capitol prezintă condițiile necesare pentru ca o autoritate de certificare să revoce un certificat.
Dacă o cheie privată care corespunde unei chei publice conținute într-un certificat revocat rămâne sub controlul Subiectului, după revocare ar trebui să fie stocată în siguranță până când este distrusă.

Certificatele pe termen scurt nu se revocă. În cazul certificatelor pe termen scurt, mecanismul de notificare a problemelor este același mecanism descris la punctul 1.5 in „Procedura de raportare a problemelor legate de certificate”.

4.9.1 Circumstanțele revocării unui certificat
Certificatul se revocă atunci când:

- Informaţia din certificat s-a schimbat,
- O cheie privată asociată unei chei publice din certificat a fost compromisă sau există un motiv serios de a bănui că a fost compromisă,
- Sunt încheiate relațiile de muncă sau acordurile juridice între certSIGN și Subiect,
- Subiectul, deținătorul cheii private asociate cheii publice din certificat, solicită revocarea,
- Subiecții / Beneficiarii nu acceptă noii termeni și reglementările modificate ale CPP,
- Autoritatea de Certificare își încetează activitatea, în acest caz toate certificatele emise de această Autoritate de Certificare, înainte de expirarea perioadei declarate pentru încetarea furnizării serviciilor, trebuie revocate împreună cu certificatul Autorităţii de Certificare,
- Cheia privată sau securitatea certificatului certSIGN au fost compromise într-un mod care amenință credibilitatea certificatelor,
- CA primeste o notificare sau este informat despre orice imprejurare care indica utilizarea ilegala a adresei de email din certificat,
- În alte cazuri în care Subiectul nu respectă regulile prezentului CPP, Termenii și condițiile sau alte acorduri încheiate între părți în legătură cu serviciile furnizate de certSIGN CA.

Cheie privată compromisă înseamnă:
(1) accesul neautorizat la cheia privată sau un motiv întemeiat de a suspecta acest lucru,
(2) pierderea cheii private sau apariţia unui motiv de a suspecta o astfel de pierdere,
(3) furtul cheii private sau apariţia unui motiv de a suspecta un astfel de furt,
(4) ştergerea accidentală a cheii private.

4.9.2 Cine poate solicita revocarea certificatelor

Următoarele entități pot trimite cereri de revocare a certificatelor:

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

Cererea de revocare poate viza mai multe certificate.

4.9.3 Procedura de revocare a certificatelor

Procedura de trimitere a cererii de revocare este descrisă în capitolul 3.4.
Cererea de revocare a certificatului trebuie să identifice cu precizie fiecare certificat, să conțină motivul (motivele) pentru care se solicită revocarea.
Informațiile despre certificatele revocate sunt înscrise pe Lista Certificatelor Revocare emise de certSIGN CA.

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

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

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

4.9.4 Perioada de grație a cererii de revocare

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

4.9.5 Timpul în care CA trebuie să proceseze cererea de revocare

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

Informaţiile despre revocarea de certificat sunt stocate în baza de date a certSIGN. Certificatele revocate sunt plasate în Lista Certificatelor Revocate (CRL) în concordanţă cu perioadele de publicare a CRL.

Ca o excepție, în caz de dezastru, dacă cererea de revocare nu poate fi confirmată în termen de 24 de ore, certSIGN va reprograma cât mai curând posibil analiza cererii și va anunța toate părțile afectate cu privire la motivele întârzierii.

4.9.6 Verificarea cerințelor de revocare pentru Entitățile Partenere

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

4.9.7 Frecvența de emitere a CRL-urilor

Fiecare autoritate de certificare parte a certSIGN emite liste de revocare a certificatelor diferite. Un nou CRL este publicat în Depozitar imediat după fiecare revocare a certificatului sau în maxim o zi. Perioada de disponibilitate a CRL este de 48 de ore și se actualizează zilnic. Lista Certificatelor Revocate (CRL) a Autorității certSIGN Root CA este emisă cel puțin o dată pe an, cu condiția să nu fie revocate certificate ale uneia dintre autoritățile subordonate autorității certSIGN FOR BNR Root CA.

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

4.9.8 Latența maximă pentru CRL-uri

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

4.9.9 Disponibilitatea verificării on-line a revocării/stării

N/A.

4.9.10 Verificarea on-line a cerințelor de revocare

Vezi capitolul 4.9.6 al prezentului document.

4.9.11 Alte forme disponibile pentru anunțarea revocării

Nu se aplică.

4.9.12 Cerințe speciale în cazul compromiterii cheii private

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

- Înceteze imediat utilizarea certificatului,
- Inițieze imediat revocarea certificatului,
- Șteargă certificatul de pe toate dispozitivele și sistemele,
- Informeze toate părțile terte care pot depinde de acest certificat.

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

4.9.13 Circumstanțe pentru suspendare

Nu se aplică.

4.9.14 Cine poate solicita suspendarea

Nu se aplică.

4.9.15 Procedura de solicitare a suspendării

Nu se aplică.

4.9.16 Limitări ale perioadei de suspendare
Nu se aplică.

4.10 Servicii privind starea certificatelor

4.10.1 Caracteristici operaționale
Serviciul de verificare a stării certificatelor este CRL. Accesul la acest serviciu se realizează prin intermediul site-ului web "www.certsign.ro". Serviciul de verificare a stării certificatelor oferă informații despre starea certificatelor valide. Integritatea și autenticitatea informațiilor despre starea lor este protejată prin semnătura electronică a CA-ului respectiv.

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

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

4.11 Încetarea acordului contractual
N/A

4.12 Custodie și recuperare chei
certSIGN nu ofera custodia cheilor pentru certificatele emise de certSIGN CA.

5 Locatie, Management și Controale Operaționale

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

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

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

5.1 Controale fizice

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

5.1.1 Amplasarea și construcția sediului

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

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

5.1.2 Accesul fizic

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

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

Vizitatorii trebuie să fie însoţiţi permanent de personal autorizat.

Zonele ocupate de certSIGN se împart în:

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

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

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

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

5.1.3 Alimentarea cu curent și aerul conditionat

Toate zonele sunt prevăzute cu aer conditionat. În zona serverelor, echipamentele de aer condiționat sunt redundante, iar temperatura este monitorizată atât automat (cu o alertă când un anumit nivel este atins) cât și manual. Din momentul întreruperii alimentării cu energie, sursele de electricitate de urgenţă (UPS) permit continuarea neperturbată a activităţii până la intervenţia automată a grupului electrogen al clădirii. Infrastructura de curect electric este concepută astfel încât la o întrerupere a curentului în cladire toate activitățile să fie disponibile pentru cel puțin 24 de ore cu ajutorul generatorului diesel. Fiecare server, echipament de rețea și toate calculatoarele angajaților care desfășoară activități importante pentru activitățile CA și RA sunt conectate la UPS-uri. Principalele componente ale securitatii fizice sunt de asemenea conectate la UPS-uri și la generatorul diesel.

5.1.4 Expunerea la apă

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

5.1.5 Prevenirea și protecția împotriva incendiilor

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

5.1.6 Depozitarea mediilor de stocare a informaţiilor

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

5.1.7 Aruncarea deșeurilor

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

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

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

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

5.1.8 Stocarea copiilor de siguranță în afara locației

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

5.2 Controale procedurale

5.2.1 Roluri de încredere

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

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

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

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

administrare de securitate și de funcționare. În special, utilizarea de programe utilitare de sistem este limitată și controlată.

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

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

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

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

5.2.2 Numărul de persoane necesare pentru fiecare sarcină

Acolo unde controlul dual sau controlul multiplu este necesar, cel putin doua persoane distincte, cu roluri de incredere relevante sunt prezente pentru a putea indeplinii operatiunea.

Circumstantele ce necesita control dual sau multiplu sunt descrise in documentatia interna confidentiala.

5.2.3 Identificarea și autentificarea pentru fiecare rol

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

Fiecare cont alocat:

- este unic şi alocat direct unei anumite persoane,
- nu este folosit în comun cu nici o altă persoană,

- este restricţionat conform funcţiei (ce reiese din rolul îndeplinit de persoana respectivă) pe baza software-ului de sistem al certSIGN, a sistemului de operare şi a controalelor de aplicaţii.

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

5.2.4 Rolurile care necesită separarea sarcinilor

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

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

5.3 Controlul personalului

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

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

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

5.3.1 Calificări, experință și aprobări necesare

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

5.3.2 Proceduri de verificare a antecedentelor

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

5.3.3 Cerinţele de pregătire a personalului

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

- Cerințele CPP,
- procedurile și controalele de securitate folosite de Autoritatea de Certificare și Autoritatea de Înregistrare
- responsabilităţile ce decurg din rolurile și sarcinile executate în sistem.

După încheierea pregătirii, participanţii semnează un document prin care confirmă familiarizarea lor cu Codul de Practici și Proceduri, Politica de certificare și acceptă restricţiile și obligaţiile impuse.

5.3.4 Frecvența și cerințele stagiilor de pregătire

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

5.3.5 Frecvența și secvența rotației posturilor

Nu se aplică.

5.3.6 Sancțiunile pentru acțiunile neautorizate

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

5.3.7 Cerințele pentru contractanții independenți

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

5.3.8 Documentația oferită personalului

certSIGN ofera personalului său accesul la următoarele documente:

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

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

5.4 Procedurile de înregistrare a datelor de audit

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

de a compromite securitatea certSIGN. Evenimentele înregistrate sunt arhivate și păstrate într-o locație secundară.

Când este posibil, log-urile sunt create automat. Dacă înregistrările nu pot fi create automat, se vor folosi jurnalele de evenimente pe hârtie. Fiecare înregistrarea în log, electronic sau de mână, este păstrată şi dezvăluită atunci când se desfăşoară un audit, dacă este necesar. Acuratețea temporală a log-urilor este asigurată de un server de timp care este sincronizat cu cel putin doua surse de timp care poot fi sateliti GPS sau UTC (NIMB).

5.4.1 Evenimente Înregistrate

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

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

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

Fiecare înregistrare, automată sau manuală, conţine următoarele informaţii:

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

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 cheile de subiect generate de CA sunt înregistrate.

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

Toate evenimentele legate de cererile de înregistrare, inclusiv cererile pentru certificatul de re-key sunt înregistrate.

Toate informațiile de înregistrare, inclusiv următoarele sunt înregistrate:

- tipul de document(e) prezentat de către solicitant la înregistrare;

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

În plus, certSIGN păstrează jurnalele interne ale tuturor evenimentelor de securitate și toate evenimentele operaționale relevante din întreaga infrastructură, oricare ar fi elementul tehnic, dar fără a se limita la:

- Modificări ale politicii de securitate
- Pornirea și oprirea sistemelor;
- Întreruperile;
- Erorile de sistem și de hardware;
- Activitățile firewall-urilor și ale routerelor;
- Încercările de acces în sistemul PKI;
- Accesul fizic al personalului și al altor persoane la părțile sensibile ale oricărui site securizat sau zonă;
- Back-up și restaurare;
- Raportul testelor de recuperare în caz de dezastru;
- Inspecții de audit;
- Actualizări și modificări ale sistemelor, software-ului și infrastructurii;
- Intruziuni de securitate și tentative de intruziune.

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

Confidențialitatea informațiilor Subiectului este menținută.

5.4.2 Frecvența procesării jurnalelor de evenimente

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

5.4.3 Perioada de pastrare a log-urilor de audit

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

Jurnalele arhivate sunt păstrate cel puțin 10 ani.

5.4.4 Protecția jurnalelor de evenimente

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

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

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

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

5.4.5 Procedura de backup a log-urilor de Audit

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

5.4.6 Audit collection system (intern vs. extern)

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

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

5.4.7 Notificarea to event-causing Subiect

Nu se aplica.

5.4.8 Evaluări de vulnerabilitate

Întreaga infrastructură face obiectul evaluării vulnerabilității ca parte a procedurilor de evaluare internă a riscurilor și de gestionare a riscurilor de către certSIGN.

Pentru a se asigura că toate activele, activitățile și serviciile sale sunt sigure, certSIGN a implementat, menține și îmbunătățește continuu sistemul de management al securității informațiilor certificat ISO 27001: 2013. În conformitate cu cerințele prezentului cadru de securitate, toate activitățile de securitate încep cu o evaluare a riscurilor pentru a identifica și a clasifica toate activele informaționale, pentru a evalua riscurile la care sunt expuse și pentru a determina controalele tehnice, manageriale, organizaționale și procedurale necesare. certSIGN menține un inventar al tuturor activelor informaționale și le atribuie o clasificare compatibilă cu evaluarea riscurilor.

5.5 Arhivarea înregistrărilor

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

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

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

Copiile de siguranţă sunt ţinute în afara locaţiei certSIGN.

5.5.1 Tipuri de date arhivate

Următoarele date sunt incluse într-o arhivă de încredere:

- Toate certificatele pentru o perioadă de 3 ani după expirarea acestora
- Jurnalele de log-uri arhivate sunt păstrate timp de 3 ani.
- Log-urile de emitere și revocare a certificatelor pentru o perioadă de 3 ani de la data emiterii / revocării
- CRL-urile sunt păstrate 3 ani de la publicare
- Următoarele, timp de 3 ani de la expirarea valabilității tuturor certificatelor care se bazează pe aceste înregistrări:
    - log-ul tuturor evenimentelor legate de ciclul de viață al cheilor gestionate de CA, inclusiv orice perechi de chei Subiect generate de CA
    - termeni și condiții (semnați) privind utilizarea certificatului.

5.5.2 Perioada de retenție a arhivei

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

5.5.3 Protecția arhivei

certSIGN asigură:

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

Arhivele sunt accesibile exclusiv personalului autorizat.

5.5.4 Procedurile de back-up al arhivei

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

5.5.5 Cerințe privind marcarea temporală a înregistrărilor

certSIGN garantează că ora exactă de arhivare a tuturor evenimentelor, înregistrările și documentelor menționate mai sus este înregistrată. Acest lucru este realizat prin sincronizarea tuturor sistemelor cu serverele de timp. Acuratetea timpuli este asigurata de un server de timp care este sincronizat cu cel putin doua surse de timp care pot fi sateliti GPS sau UTC (NIMB).

5.5.6 Sistemul de colectare al arhivei (intern sau extern)

Sistemele de colectare ale arhivei certSIGN sunt interne.

5.5.7 Proceduri de obținere și verificare a informațiilor arhivate

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

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

5.6 Schimbarea cheilor

Procedurile de Key changeover permit tranzitia usoara de la certificate de CA expirate catre certificate noi. Spre sfârșitul vieții Chei Private a CA, certSIGN încetează să utilizeze cheia privată a CA care expiră pentru a semna Certificate (cu cel puțin un an înaintea expirării) și utilizează vechea cheie privată doar pentru a semna CRL-uri. O nouă pereche de chei de semnare CA este comandată și toate certificatele emise ulterior și CRL-urile, sunt semnate cu noua cheie privată de semnare. Atât vechile, cât și cele noi perechi de chei pot fi active simultan. Acest proces de schimbare a cheilor ajută la minimizarea oricăror efecte negative ale expirării certificatului CA. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed În chapter 6.1.4.

5.7 Compromiterea și recuperare în caz de dezastru

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

5.7.1 Procedurile de administrare a a incidentelor și compromiterilor

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

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

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

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

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

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

certSIGN are un Plan de răspuns la incidente și un Plan de recuperare în caz de dezastru, care includ Planul de Management în situații de Criză, precum și proceduri documentate de

continuitatea afacerii și recuperare în caz de dezastre, proiectate astfel încât să notifice și să protejeze în mod rezonabil furnizorii de aplicații software, beneficiarii și entitățile partenere, în eventualitatea unui dezastru, compromitere a securității sau eșec al afacerii. certSIGN pune la dispoziția auditorilor, la cerere, planurile de continuitate a afacerii și de securitate. Toate procedurile sunt anual testate, revizuite și actualizate.

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

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

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

Pentru a preveni sau limita rezultatele amenințărilor de mai sus:

- Politica de securitate a certSIGN include un Plan de continuitate a afacerii și recuperare în caz de dezastru,
- În cazul apariţiei unui eveniment ce blochează funcţionarea certSIGN, în maxim 48 de ore, va fi activată locaţia auxiliară ce poate substitui toate funcţiile importante ale unei Autorităţii de Certificare până la restaurarea locaţiei principale. Distanța dintre locația primară și cea secundară este suficient de mare pentru ca potențialul dezastru care afectează locația primară să nu afecteze și locatia secundară.
- Instalarea de versiuni noi ale aplicaţiilor software în producţie se poate face numai după testarea intensivă a acestora într-un mediu de test, în conformitate cu procedurile descrise. Orice modificare a sistemului necesită aprobarea administratorului de securitate al certSIGN.
- Sistemele certSIGN utilizează aplicaţii pentru crearea copiilor de rezervă a datelor pe baza cărora se poate face în orice moment restaurarea sistemului și auditarea acestuia. Copiile de siguranţă includ toate datele relevante din punct de vedere al securităţii.

Toate sistemele din care este compusă infrastructura IT pentru furnizarea de servicii de certificare și timestamp sunt monitorizate în mod continuu și toate evenimentele de securitate sunt înregistrate și analizate. Activitățile de sistem anormale care indică o potențială încălcare a securității, inclusiv intruziune în sistemele de rețea sunt detectate și raportate ca alarme pentru a permite certSIGN să detecteze, înregistreze și reactioneze în timp util la orice tentative neautorizate și/sau neobișnuite de a accesa resursele sale.

Sensibilitatea oricăror informații colectate sau analizate este luată în considerare, protejându-le împotriva accesului neautorizat.

Pentru a detecta orice discontinuitate în operațiunile de monitorizare, pornirea și oprirea funcțiilor de logare este, de asemenea, monitorizată

Disponibilitatea tuturor componentelor importante ale infrastructurii TIC utilizate pentru furnizarea serviciilor de certificare, precum și disponibilitatea serviciilor critice sunt, de asemenea, monitorizate.

certSIGN va aborda orice vulnerabilitate critică care anterior nu a fost adresată, într-o perioadă de 48 de ore de la descoperirea sa. Dacă acest lucru este rentabil, având în vedere impactul, va fi creat și pus în aplicare un plan pentru a reduce vulnerabilitatea sau va fi documentată baza factuală în sprijinul deciziei certSIGN că vulnerabilitatea nu necesită remediere.

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

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

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

- Notificarea - asupra compromiterii - a tuturor Subiecților / Beneficiarilor și a celorlalte entități cu care certSIGN are acorduri sau alte forme de relații stabilite, între care Entitățile Partenere și alți Furnizori de Servicii de Încredere. În plus, aceste informații vor fi puse la dispoziția altor Entități Partenere prin intermediul sistemului mass-media și prin poșta electronică.
- Notificarea publicului prin mai multe canale, inclusiv un mesaj în depozitarul certSIGN CA și pe web site, un comunicat de presă în mass-media.
- Un certificat corespunzător cheii compromise este plasat pe Lista Certificatelor Revocate
- Toate certificatele semnate de CA-ul compromis sunt revocate, specificându-se motivul revocării
- Autoritatea de Certificare generează o nouă pereche de chei și un nou certificat
- Se generează noi certificate pentru Subiecţi
- Noile certificate sunt trimise Subiecților în mod gratuit
- Dacă un certificat este revocat din cauza compromisului cheie CA, certSIGN Root CA va emite un CRL nou în termen de 24 de ore de la primirea notificării privind compromisul și va publica CRL-urile online imediat.

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

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

5.7.4 Capacități de Continuitate a afacerii în caz de dezastru

certSIGN a stabilit într-un Plan de Continuitate a afacerii (BCP) și un Plan de recuperare în caz de dezastru (DRP) toate măsurile necesare pentru a asigura recuperarea integrală a serviciilor noastre de certificare și marcare temporală în caz de dezastru, sau în cazul unei discontinuități a oricărei componente TIC ori a unui serviciu important, mai mare decât Downtime-ul Maxim Tolerabil. Orice astfel de măsuri sunt conforme cu standardele ISO/IEC 27001 și 27002. Funcționarea fiecărei componente sau serviciu va fi restaurată în timpul Maxim Tolerabil de Downtime stabilit în planul de continuitate.

Toate datele sistemelor necesare pentru reluarea operațiunilor CA sunt salvate și stocate într-un loc la distanță și în condiții de siguranță, pentru a permite serviciilor de certificare și marcare temporală să își reia activitatea în timp util în cazul unui incident / dezastru.

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

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

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

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

5.8 Încetarea activității Autorității de Certificare sau a Autorității de Înregistrare

certSIGN are un plan la zi de încetare a activității pentru a minimiza efectele negative asupra Subiecților/Beneficiarilor şi Entităţilor Partenere ce pot apărea ca urmare a deciziei unei Autorităţi de Certificare de a-şi înceta activitatea. Planul include obligativitatea notificarii Subiecților/Beneficiarilor asupra autoritatii ce a certificat autoritatea de certificare ce urmeaza sa isi inceteze activitatea (daca exista) și translatarea responsabilitatilor (servicii furnizate catre Subiecți/Abonaţi, baze de date, etc) În conformitate cu reglementarile aplicabile catre alta Autoritate de Certificare.

Cerințe asociate transferului responsabilității

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

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

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

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

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

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

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

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

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

5.9 Lanțul de aprovizionare

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

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

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

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

6 Controale tehnice de securitate

6.1 Generarea și instalarea perechii de chei

Acest capitol descrie procedurile de generare și management a perechii de chei criptografice a unei Autorităţi de Certificare, inclusiv cerințele tehnice asociate. Controalele de securitate corespunzătoare sunt puse în aplicare pentru gestionarea oricăror chei criptografice și a oricărui dispozitiv criptografic pe parcursul ciclului lor de viață. Aceste măsuri de securitate protejează, de asemenea, datele de activare a cheilor criptografice, depozitarele, cheile private și datele de activare pentru cheile private ale Subiecților CA-urilor, și ai altor Participanți PKI, și parametri critici de securitate.

Procedurile de management al cheii se referă la păstrarea și folosirea în siguranţă de către proprietar a cheilor sale. O atenţie deosebită se acordă generării și protecţiei cheii private a certSIGN, care influenţează funcţionarea în siguranţă a întregului sistem de certificare a cheilor publice.

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

O semnătură electronică este creată prin intermediul algoritmului RSA în combinație cu SHA criptografic digest.

certSIGN emite certificate pentru chei stocate in format software.

6.1.1 Generarea perechilor de chei

certSIGN are o procedură documentată pentru efectuarea generării cheilor de CA. Această procedură indică următoarele:

- Rolurile care participă la ceremonie (interne și externe organizației);
- Ce funcții trebuie îndeplinite de fiecare rol și în ce fază;
- Responsabilități în timpul și după ceremonie; și
- Cerințe cu privire la dovezile care trebuie colectate in timpul ceremoniei.

După ceremonia cheilor, certSIGN elaboreaza un raport al ceremoniei cheilor care dovedeste că a fost efectuată în conformitate cu procedura declarată și că integritatea și confidențialitatea perechii de chei au fost asigurate de către rolul de încredere responsabil pentru securitatea ceremoniei de gestionare a cheilor certSIGN (de exemplu, ofițer de securitate), ca martor că raportul înregistrează corect ceremonia de gestionare a cheilor în timp ce a fost efectuată.

În toate cazurile, certSIGN:

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

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

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

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

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

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

Generarea perechii de chei CA este realizată folosind algoritmul RSA cu lungimea cheii de 4096 biți.

Înainte de expirarea certificatului său de CA, care este utilizat pentru semnarea cheilor Subiecților, CA va genera un nou certificat pentru semnarea perechilor de chei ale Subiecților și va aplica toate măsurile necesare pentru a evita perturbarea operațiunilor oricărei entități care se bazează pe certificatul CA. Noul certificat CA va fi, de asemenea, generat și distribuit în conformitate cu prezentul CPP. Aceste operații trebuie efectuate la un interval de timp adecvat între data expirării certificatului și ultimul certificat semnat pentru a permite tuturor părților care au relații cu certSIGN (subiecți, abonați, entități partenere, CA-uri mai mari în ierarhia CA etc.) să fie conștienți de această modificare de cheie și să pună în aplicare operațiunile necesare pentru a evita crearea unor inconveniențe și defecțiuni. Acest lucru nu se aplică în cazul în care am înceta operațiunile noastre înainte de data de expirare a propriului nostru certificat de semnare.

Cheile Subiectului sunt generate de catre certSIGN, in format software (container p12 in conformitate cu standardul PKCS12).

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

6.1.2 Distribuirea Cheii Private către Beneficiar

Cheia privată generată de certSIGN

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

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

Cheia privată generată de Subiect

N/A

6.1.3 Distribuirea Cheii Publice către emitentul certificatului

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

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

6.1.4 Distribuirea Cheii Publice a Autorității Certificare către Entitățile Partenere

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

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

Autoritatile de certificare certSIGN isi publica certificatele prin plasarea acestora În depozitarul public disponibil la adresa http://pki.certSIGN.ro/repository.

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

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

6.1.5 Marimea cheilor

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

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

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

6.1.6 Parametrii de generare a Cheilor Publice și verificarea calității

certSIGN are o procedură documentată pentru efectuarea generării de perechi de chei CA pentru toate CA-urile, inclusiv certSIGN CA.

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

6.1.7 Scopurile în care pot fi utilizate cheile (conform câmpului de utilizare a cheilor X.509 v3)

Scopurile în care pot fi folosite cheile sunt descrise în câmpul KeyUsage (vezi Capitolul 7.1.1.2) din cadrul extensiilor standard ale certificatelor X.509 v3. Acest câmp trebuie verificat în mod obligatoriu de aplicaţia Beneficiarului care face managementul certificatelor.

Folosirea biţilor din câmpul KeyUsage trebuie să respecte următoarele reguli:

a) digitalSignature: certificate pentru verificarea semnăturii electronice,
b) nonRepudiation: certificate pentru furnizarea serviciului de ne-repudiere de către persoane fizice, cât şi pentru alte scopuri decât cele descrise la punctele f) și g). Bitul de ne-repudiere poate fi setat numai într-un certificat de cheie publică cu care se

intenţionează verificarea semnăturilor electronice și nu trebuie combinat cu cele descrise la punctele c) - e) şi legate de asigurarea confidenţialităţii,

c) keyEncipherment: folosite pentru criptarea cheilor algoritmilor simetrici, oferind confidenţialitatea datelor,
d) dataEncipherment: folosite pentru criptarea datelor Subiectului, altele decât cele descrise la punctele c) și e),
e) keyAgreement: folosite pentru protocoale de schimbare a cheilor,
f) keycertSIGN: cheia publică este folosită pentru verificarea semnăturii electronice în certificatele emise de entităţi care oferă servicii de certificare,
g) cRLSign: cheia publică este folosită pentru verificarea semnăturilor electronice de pe listele de certificate revocate şi suspendate emise de entităţile care oferă servicii de certificare,
h) encipherOnly: poate fi folosit exclusiv cu bitul de keyAgreement pentru a indica scopul de criptare a datelor în cadrul protocoalelor de schimbare a cheilor,
i) decipherOnly: poate fi folosit exclusiv cu bitul de keyAgreement pentru a indica scopul de decriptare a datelor în cadrul protocoalelor de schimbare a cheilor.

6.2 Protecția cheii private și controalele modulului criptografic

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

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

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

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

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

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

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

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

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

6.2.1 Controalele și standardele modulelor criptografice

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

Cheile Subiectului sunt generate de catre certSIGN, in format software.

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

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

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

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

Acceptarea secretului partajat de către deținătorii săi

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

Protejarea secretului partajat

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

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

Disponibilitatea și ștergerea (transferul) secretului partajat

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

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

Responsibilitățile deținătorului secretului partajat

Deţinătorul secretului partajat trebuie să-şi îndeplinească îndatoririle și obligaţiile conform cerinţelor acestui Cod de Practici și Proceduri, în mod deliberat și responsabil în orice situaţie posibilă. Un deţinător de secret partajat trebuie să anunţe emitentul secretului în cazul furtului, pierderii, dezvăluirii neautorizate sau compromiterii securităţii secretului, imediat

după incident. Un deţinător de secret partajat nu este responsabil pentru neîndeplinirea îndatoririlor/obligaţiilor sale din cauza unor motive ce sunt imposibil de controlat de către acesta, dar este responsabil pentru dezvăluirea inoportună a secretului sau pentru neglijarea obligaţiilor de a notifica emitentul secretului despre dezvăluirea inoportună sau violarea securităţii secretului ca urmare a greşelilor, neglijenţei sau iresponsabilităţii deţinătorului.

Controlul multiplu nu se aplică cheii private a Subiectului.

6.2.3 Custodia Cheii Private

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

Cheile private ale subiectului nu sunt supuse custodiei.

6.2.4 Copia de siguranță a cheii private

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

certSIGN nu păstrează copii ale cheilor private ale operatorilor Autorităţii de Certificare.

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

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

Existenta unei copii de siguranta a cheii private nu se aplică cheii private a Subiectului.

6.2.5 Arhivarea Cheii Private

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

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

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

- În cazul creării copiilor de siguranță pentru cheile private socate într-un modul criptografic, poate fi necesară, ocazional, (de ex. în cazul compromiterii sau defectării modulului) introducerea unei perechi de chei într-un modul de securitate diferit,
- Este necesar transferul de către entitate a unei chei private din modulul operațional utilziat pentru operațiuni standard către un alt modul; situația poate apărea în cazul defectării modulului sau atunci când este necesară distrugerea sa.

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

Introducerea unei chei private într-un modul hardware de securitate al Autorităţii de Certificare **certSIGN CA** necesită restaurarea cheii de pe carduri în prezenţa unui număr

corespunzător de deţinători ai secretului partajat care protejează modulul ce conţine cheile private. Deoarece fiecare Autoritate de Certificare poate deţine o copie criptată a cheii sale private, cheile pot fi de asemenea transferate între module.

6.2.7 Stocarea cheilor private pe modul criptografic

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

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

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

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

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

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

6.2.8 Metoda de activare a cheii private

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

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

6.2.9 Metoda de dezactivare a cheii private

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

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

Cand este stocata in format software, deactivarea cheii private a Subiectului depinde de configuratia software ce o stocheaza.

6.2.10 Metoda de distrugere a cheii private

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

Cheia privată CA poate fi distrusă prin ștergerea tuturor cardurilor HSM (Operator și Administrator). În plus, HSM permit resetarea dispozitivului prin acces fizic și setări pe dispozitiv. Aceasta reinitializează dispozitivul și suprascrie toate datele din acesta cu zerouri binare. În cazurile în care această procedură de resetare sau de reinitializare nu reușește,

certSIGN va zdrobi, arunca și / sau incinera dispozitivul într-o manieră care distruge capacitatea de a extrage orice secret.

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

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

Subiectul este responsabil pentru distrugerea cheii private. Pentru cheile stocate pe dispozitive criptografice hardware (de exemplu QSCD) aceasta poate fi efectuata fie utilizand utilitarul dispozitivului fie prin distrugerea fizica a dispozitivului. Pentru chei stocate in format software Subiectul va sterge (shred) toate copiile pentru a preveni utilizarea neautorizata a cheilor.

6.2.11 Evaluarea Modulului Criptografic

Vezi mai sus.

6.3 Alte aspecte legate de managementul perechilor de chei

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

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

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

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

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

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

6.3.1 Arhivarea cheii publice

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

Vezi capitolul 5.5 pentru conditiile de arhivare.

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

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

Perioada de valabilitate a certificatului certSIGN FOR BNR ROOT CA este de 7 ani.

Perioada de valabilitate a certificatului certSIGN CA este de 3 ani.

Perioada de valabilitate a unui certificat de Subiect este de până la 1 an.

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

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

6.4 Datele de activare

6.4.1 Generarea și instalarea datelor de activare

Datele de activare sunt folosite în două situații principale:

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

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

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

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

Atunci când cheile sunt generate de catre certSIGN, pentru transmiterea datelor de activare (de exemplu codul PIN) catre Subiect, sunt utilizate masuri de securitate adecvate.

6.4.2 Protejarea datelor de activare

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

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

modulul criptografic trebuie să ducă la blocarea acestuia. Datele de activare stocate nu trebuie să fie păstrate împreună cu cardul criptografic.

Subiecții sunt responsabili pentru gestionarea și protejarea sigură a datelor de activare (de exemplu codul PIN) – vezi #6.1.2.

6.4.3 Alte aspect ale datelor de activare

Nu se aplica.

6.5 Controale de Securitate a computerelor

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

6.5.1 Cerințe tehnice specifice ale securității calculatoarelor

Computerele sunt configurate cu următoarele mecanisme de securitate:

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

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

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

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

Datele sensibile sunt protejate împotriva relevării prin obiecte de stocare re-utilizate (de exemplu, fișiere șterse), fiind accesibile utilizatorilor neautorizați. În acest scop, trebuie utilizat un software special, cu algoritmi de ștergere siguri pentru mediile de stocare, HSM-

urile se resetează, dispozitivele criptografice securizate (token-uri / carduri) trebuie formatate înainte de reutilizare / sau distruse fizic la sfârșitul ciclului lor de viață.

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

6.5.2 Evaluarea securității calculatoarelor

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

6.6 Controale de securitate specifice ciclului de viață

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

6.6.1 Controale specifice dezvoltării sistemului

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

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

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

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

6.6.2 Controale specifice managementului securității

Scopul managementului securitatii este de a superviza functionalitatea sistemelor certSIGN oferind siguranta ca toate sistemele functioneaza corect si in conformitate cu configuratiile acceptate si implementate.

Controalele applicate sistemelor certSIGN permit verificarea continua a integritatii aplicatiilor, a versiunilor acestora precum si autentificarea si verificarea originii hardware-ului.

6.6.3 Controale de securitate specifice ciclului de viață

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

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

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

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

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

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

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

6.7 Controale de securitate a rețelei

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

a) Sistemele sunt segmentate în rețele sau zone luând în considerare relația funcțională, logică și fizică (inclusiv de locație) dintre sistemele și servicii de încredere. certSIGN aplică aceleași controale de securitate pentru toate sistemele co-localizate în aceeași zonă.
b) Accesul și comunicarea între zone sunt permise doar persoanelor necesare funcționării serviciilor de certificare. Conexiunile și serviciile care nu sunt necesare sunt interzise în mod explicit sau dezactivate. Setul de reguli stabilite sunt reviziuite periodic.
c) Toate sistemele critice pentru funcționarea serviciilor de certificare sunt păstrate într-una sau mai multe zone securizate)
d) Rețeaua dedicată administrării sistemelor IT și rețeaua operațională sunt separate. Sistemele utilizate pentru administrarea implementării politicii de securitate nu sunt utilizate în alte scopuri. Sistemele de producție ale serviciilor de certificare sunt separate de sistemele utilizate în dezvoltare și testare (de exemplu, sistemele de dezvoltare, testare și planificare).
e) Comunicarea între sisteme de încredere distincte se realizează doar prin intermediul unor canaluri de încredere care sunt distincte logic de alte canale de comunicații și oferă identificarea sigură a punctelor terminale și protecția datelor canalului de modificare sau divulgare.
f) Dacă este necesar un nivel înalt de disponibilitate a accesului extern la un anumit serviciu de certificare, conexiunea externă la rețea este redundantă, pentru a asigura disponibilitaea serviciilor, în cazul unui singur eșec.
g) Se realizează o scanare standard a vulnerabilității adreselor IP publice și private identificate de certSIGN și se înregistrează dovezi că fiecare scanare a vulnerabilității a fost realizată de către o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.
h) Serviciile de certificare ale certSIGN sunt supuse unui test de penentrare pe sistemele aferente la inițiere și după upgrade-uri de infastructură sau de aplicații sau după modificări pe care certSIGN le consideră importante. Se înregistrează dovezi că fiecare test de penetrare a fost realizat de către o persoană sau o entitate cu abilitățile, instrumentele, competența, codul de etică, și independența necesare pentru a oferi un raport de încredere.

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

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

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

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

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

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

Sistemul **certSIGN CA** se află într-o zonă de înaltă securitate.

6.8 Marcare temporala

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

7 Profilul certificatelor si al CRL

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

7.1 Profilul certificatului

Profilul câmpurilor de bază pentru certificatul **certSIGN FOR BNR ROOT CA** este descris în Tabelul 7.1.1

Numele campului	Valoarea sau restricțiile valorii	
Versiune	3	
Serie	1001d2004d151531f7ef	
Altoritm de semnare	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Emitent (Nume distinctiv)	CommonName (CN)=	certSIGN FOR BNR ROOT CA
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Nu înainte de	October 17, 2024 2:34:00 PM	
Nu după	October 17, 2036 2:34:00 PM	
Subiect (Distinguished Name)	Common Name (CN) =	certSIGN FOR BNR ROOT CA
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Informații despre cheia publica a subiectului	4096 bits RSA key	
Semnătură	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	

Table 7.1.1 Profilul câmpurilor de bază al certSIGN ROOT CA

Profilul câmpurilor de bază pentru certificatele de CA emise de **certSIGN FOR BNR ROOT CA** este descris în Tabelul 7.1.2.

Numele câmpului	Valoarea sau restricțiile valorii	
Versiune	Version 3	
Serie	Valoare unică mai mare decât zero (0) pentru toate certificatele emise de autoritățile de certificare din cadrul certSIGN. Seriile sunt construite folosind un prefix incremental unic constrâns in baza de date care este concatenat cu o secvență aleatorie de 8 octeți. Un modul criptografic hardware este utilizat pentru generarea valorii aleatorii.	
Algoritm de semnare	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Emitent (Nume distinctiv)	CommonName (CN)=	certSIGN FOR BNR ROOT CA
	Organization (O) =	certSIGN SA
	Country (C) =	RO
Nu înainte de	Universal Time Coordinated based.	
Nu după	Universal Time Coordinated based.	
Subiect (Nume distinctiv)	CommonName (CN) =	*Common Name of the CA*
	Organization (O) =	CERTSIGN SA
	OrganizationIdentifier =	VATRO-18288250
	Organization Unit (OU) =	*Type of certificate (Test/Production)*
	Country (C) =	RO

Numele câmpului	Valoarea sau restricțiile valorii
Cheia publica a subiectului	4096 bits RSA key
Semnătură	Codificate în conformitate cu RFC 5280, pot conține informații despre cheile publice RSA, DSA sau ECDSA (identificatorul cheii, dimensiunea cheii în biți și valoarea cheii publice);

Table 7.1.2. Profilul câmpurilor de bază ale certificatelor emise de certSIGN FOR BNR ROOT CA

Profilul câmpurilor de bază pentru certificatul de end user emis de orice CA intermediar este descris în Tabelul 7.1.3.

Numele campului	Valoarea sau restricțiile valorii	
Versiune	3	
Serie	Valoare unică mai mare decât zero (0) pentru toate certificatele emise de autoritățile de certificare din cadrul certSIGN. Seriile sunt construite folosind un prefix incremental unic constrâns in baza de date care este concatenat cu o secvență aleatorie de 8 octeți. Un modul criptografic hardware este utilizat pentru generarea valorii aleatorii.	
Algoritm de semnare	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Emitent (Nume distinctiv)	Country (C) =	RO
	Organization (O) =	certSIGN SA
	OrganizationIdentifier =	VATRO-18288250
	OrganizationUnit (OU) =	*Type of certificate (Test/Production)*
	CommonName (CN)=	Common Name of the CA
Subiect (Nume distinctiv)	Codificate în conformitate cu RFC 5280, pot conține câmpurile prezentate în capitolul 3.1.2.	
Informații despre cheia publica a subiectului	Codificate în conformitate cu RFC 5280, pot conține informații despre cheile publice RSA, DSA sau ECDSA (identificatorul cheii, dimensiunea cheii în biți și valoarea cheii publice); Dimensiunea cheii RSA este prezentată în capitolul 6.1.5.	
Semnătură	Semnătura certificatului, generată și codificată în conformitate cu cerințele descrise în RFC 5280.	

Table 7.1.3. Profilul câmpurilor de bază pentru certificate end-user

7.1.1 Numerele de versiune

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

7.1.2 Extensii de certificate

7.1.2.1 certSIGN FOR BNR SIMPLE SSL TEST CA V2

Extensiile certificatelor pentru certSIGN FOR BNR SIMPLE SSL TEST CA V2 sunt descrise în Tabelul 7.1.2.1.1

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access	Ne-Critic

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRRootCA.crt	
Basic Constraints	Subiect type=CA, Path length constraint=None	Critic
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critic
Authority Key Identifier	2f38f23a352a3b2bec69306a923930b5f59277bd	Ne-Critic
Subiect Key Identifier	9887f988ee9acaaf6fcbebe0898537c65af68765	Ne-Critic
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=X509v3 Any Policy [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Ne-Critic
CRL Distribution Points	http://pkipro.certsign.ro/CERTSIGNBNRRootCA.crl	Ne-Critic

Tabel 7.1.2.1.1. Extensiile certificatului certSIGN FOR BNR SIMPLE SSL TEST CA V2

Extensiile certificatelor pentru utilizatorii finali sunt descrise in tabelul următor.

Extensiile **certificatelor de autentificare** pentru utilizatori finali:

Extension	Value or Value constraint	Extension status
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRSIMPLESSLtestv2.crt	Ne-Critic
Key Usage	digitalSignature (bit 0) și Key Encipherment (bit a0)	Critic
Authority Key Identifier	9887f988ee9acaaf6fcbebe0898537c65af68765	Ne-Critic
Subiect Key Identifier	KeyIdentifier este compus din hash-ul SHA-1 de 160 biți al valorii lui BIT STRING SubiectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizati).	Ne-Critic
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.9.3 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:	Ne-Critic

Extension	Value or Value constraint	Extension status
	http://pki.certsign.ro/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRSSLTEST/CERTSIGNBNRSIMPLESSLtestv2.crl	Ne-Critic
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	Ne-Critic
Subject Alternative Name	Other Name: RFC822 Name and Principal Name (UPN) *This extension is optional*	Ne-Critic

Tabel 7.1.2.1.2 Extensiile **certificatelor de autentificare** pentru utilizatori finali

7.1.2.2 certSIGN FOR BNR Qualified DS TEST CA V2

Extensiile certificatelor pentru certSIGN FOR BNR Qualified DS TEST CA V2 sunt descrise în Tabelul 7.1.2.2.1

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRRootCA.crt	Ne-Critic
Basic Constraints	Subject type=CA, Path length constraint=None	Critic
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critic
Authority Key Identifier	2f38f23a352a3b2bec69306a923930b5f59277bd	Ne-Critic
Subject Key Identifier	8124fb2ba7ab64573e9923827776800096da3f90	Ne-Critic
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=X509v3 Any Policy [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Ne-Critic
CRL Distribution Points	http://pkipro.certsign.ro/CERTSIGNBNRRootCA.crl	Ne-Critic

Tabel 7.1.2.2.1. Extensiile certificatului certSIGN FOR BNR Qualified DS TEST CA V2

Extensiile certificatelor pentru utilizatorii finali sunt descrise in tabelele următoare.
Extensiile **certificatelor de semnare** pentru utilizatori finali:

Extension	Value or Value constraint	Extension status
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRQUALIFIEDDStestv2.crt	Ne-Critic
Key Usage	digitalSignature (bit 0) și nonRepudiation (bit 1)	Critic
Authority Key Identifier	8124fb2ba7ab64573e9923827776800096da3f90	Ne-Critic
Subiect Key Identifier	KeyIdentifier este compus din hash-ul SHA-1 de 160 biți al valorii lui BIT STRING SubiectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizati).	Ne-Critic
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.9.4 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Ne-Critic
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRDSTEST/CERTSIGNBNRQUALIFIEDDStestv2.crl	Ne-Critic
Extended Key Usage	Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12)	Ne-Critic
Subiect Alternative Name	Other Name: RFC822 Name and Principal Name (UPN) *This extension is optional*	Ne-Critic

Tabel 7.1.2.2.2 Extensiile **certificatelor de semnare** pentru utilizatori finali

7.1.2.3 certSIGN FOR BNR SIMPLE SSL PRODUCTION CA V2

Extensiile certificatelor pentru certSIGN FOR BNR SIMPLE SSL PRODUCTION CA V2 sunt descrise în Tabelul 7.1.2.3.1

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer	Ne-Critic

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
	(1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRRootCA.crt	
Basic Constraints	Subject type=CA, Path length constraint=0	Critic
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critic
Authority Key Identifier	2f38f23a352a3b2bec69306a923930b5f59277bd	Ne-Critic
Subject Key Identifier	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Ne-Critic
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=X509v3 Any Policy [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Ne-Critic
CRL Distribution Points	http://pkipro.certsign.ro/CERTSIGNBNRRootCA.crl	Ne-Critic

Tabel 7.1.2.3.1. Extensiile certificatului certSIGN FOR BNR SIMPLE SSL PRODUCTION CA V2

Extensiile certificatelor pentru utilizatorii finali sunt descrise in tabelele următoare.

Extensiile **certificatelor de autentificare** pentru utilizatori finali:

Extension	Value or Value constraint	Extension status
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRSIMPLESSLprodv2.crt	Ne-Critic
Key Usage	digitalSignature (bit 0) și nonRepudiation (bit 1)	Critic
Authority Key Identifier	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Ne-Critic
Subject Key Identifier	KeyIdentifier este compus din hash-ul SHA-1 de 160 biți al valorii lui BIT STRING SubjectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizati).	Ne-Critic
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.9.1 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:	Ne-Critic

Extension	Value or Value constraint	Extension status
	http://www.certsign.ro/repository	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRSSLPRODUCTIE/CERTSIGNBNRSIMPLESSLprodv2.crl	Ne-Critic
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	Ne-Critic
Subiect Alternative Name	Other Name: RFC822 Name and Principal Name (UPN) *This extension is optional*	Ne-Critic

Tabel 7.1.2.3.2 Extensiile **certificatelor de autentificare** pentru utilizatori finali

7.1.2.4 certSIGN FOR BNR QUALIFIED DS PRODUCTION CA V2

Extensiile certificatelor pentru certSIGN FOR BNR QUALIFIED DS PRODUCTION CA V2 sunt descrise în Tabelul 7.1.2.4.1

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRRootCA.crt	Ne-Critic
Basic Constraints	Subiect type=CA, Path length constraint=0	Critic
Key Usage	keyCertSign (bit 5), cRLSign (bit 6)	Critic
Authority Key Identifier	2f38f23a352a3b2bec69306a923930b5f59277bd	Ne-Critic
Subiect Key Identifier	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Ne-Critic
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=X509v3 Any Policy [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Ne-Critic
CRL Distribution Points	http://pkipro.certsign.ro/CERTSIGNBNRRootCA.crl	Ne-Critic

Tabel 7.1.2.4.1. Extensiile certificatului certSIGN FOR BNR QUALIFIED DS PRODUCTION CA V2

Extensiile **certificatelor de semnare** pentru utilizatori finali:

Extension	Value or Value constraint	Extension status
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.certsign.ro [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRQUALIFIEDDSprodv2.crt	Ne-Critic
Key Usage	digitalSignature (bit 0) și nonRepudiation (bit 1)	Critic
Authority Key Identifier	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Ne-Critic
Subiect Key Identifier	KeyIdentifier este compus din hash-ul SHA-1 de 160 biți al valorii lui BIT STRING SubiectPublicKey (cu excepția etichetei, lungimii și numărului de biți neutilizati).	Ne-Critic
Certificate Policies	Certificate Policies [1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.25017.9.2 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.certsign.ro/repository	Ne-Critic
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://pkipro.certsign.ro/CERTSIGNBNRDSPRODUCTIE/CERTSIGNBNRQUALIFIEDDSprodv2.crl	Ne-Critic
Extended Key Usage	Secure Email (1.3.6.1.5.5.7.3.4) Document Signing (1.3.6.1.4.1.311.10.3.12)	Ne-Critic
Subiect Alternative Name	Other Name: RFC822 Name and Principal Name (UPN) *This extension is optional*	Ne-Critic

Tabel 7.1.2.4.2 Extensiile **certificatelor de semnare** pentru utilizatori finali

7.1.3 Algoritmul identificatorului obiect

Câmpul signatureAlgorithm conține un identificator algoritm criptografic utilizat pentru semnătură electronică creat de o autoritate de certificare pe certificat. În cazul certSIGN, algoritmul utilizat este sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11).

7.1.4 Formulare de nume

Vezi sectiunea 3.1.

7.1.5 Constrangeri privind numele

Nu se aplica.

7.1.6 Identificatorul de obiect pentru politica de identificare

Certificatele de identificare a obiectului de politică utilizate la nivel de certSIGN certSIGN for BNR sunt descrise în Tabelele 7.6 si Table 7.7.

{certSIGN} = *1.3.6.1.4.1.25017.1*

Numele politicii de certificare	Identificatorul politicii
certSIGN FOR BNR SIMPLE SSL PRODUCTION CA V2	{certSIGN}.{id-BNR}(9).{id-policy}(1) *ID=1.3.6.1.4.1.25017.9.1*
certSIGN FOR BNR QUALIFIED DS PRODUCTION CA V2	{certSIGN}.{id-BNR}(9).{id-policy}(2) *ID=1.3.6.1.4.1.25017.9.2*
certSIGN FOR BNR SIMPLE SSL TEST CA V2	{{certSIGN}.{id-BNR}(9).{id-policy}(3) *ID=1.3.6.1.4.1.25017.9.3*
certSIGN FOR BNR QUALIFIED DS TEST CA V2	{certSIGN}.{id-BNR}(9).{id-policy}(4) *ID=1.3.6.1.4.1.25017.9.4*

Tabel 7.6.Identificatorii politicii si numele lor

CA Level	Tip	OID
certSIGN FOR BNR SIMPLE SSL PRODUCTION CA V2	Certificate ne-calificate	*Certificate pentru autentificare* • 1.3.6.1.4.1.25017.9.1
certSIGN FOR BNR QUALIFIED DS PRODUCTION CA V2	Certificate calificate	*Certificate pentru semnare* • 1.3.6.1.4.1.25017.9.2
certSIGN FOR BNR SIMPLE SSL TEST CA V2	Certificate ne-calificate	*Certificate pentru autentificare* • 1.3.6.1.4.1.25017.9.3
certSIGN FOR BNR QUALIFIED DS TEST CA V2	Certificate calificate	*Certificate pentru semnare* • 1.3.6.1.4.1.25017.9.4

Tabel 7.7 Identificatori de obiect pentru politica de certificare

7.1.7 Utilizarea extensiei Constrângeri de politică

Nu se aplica.

7.1.8 Sintaxa și semantica calificărilor de politică

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

7.1.9 Semantica de procesare pentru extensia Politici critice de certificare

Nu se aplica.

7.2 Profilul CRL

Profilul CRL este descris în Tabelul 7.8.

Nume camp	Valoarea sau restricțiile valorii	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer	Common Name (CN) =	Common Name of the CA
	Organization (O) =	certSIGN SA
	Country (C) =	RO
ThisUpdate	Date of CRL issuance	
NextUpdate	Date of next expected CRL update	
Revoked Certificates	List of revoked certificates	

Table 7.8 Profilul CRL pentru certSIGN FOR BNR CA

7.2.1 Numerele de versiune

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

7.2.2 CRL și extensiile de intrare CRL

Extensiile CRL pentru certSIGN for BNR sunt descrise în Tabelul 7.9.

Extensie	Valoarea sau restricțiile valorii	Statusul extensiei
Authority Key Identifier	3ae9ca308a1d14b51aaf1518f7de020f0bad8866	Ne-critic
CRL Number	monotonically increasing sequence number	Ne-critic
ExpiredCertsOnCRL	Generalized Time	Ne-critic

Table 7.9. Extensii CRL ale certSIGN CA

8 Auditul de conformitate și alte evaluări

8.1 Frecvența sau circumstanțele de evaluare

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

8.2 Identitatea / calificările evaluatorului

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

Legat de conformitatea / calificarile evaluatorului, operarea consistenta si impartialitatea atestarii effectuate de corpurile de conformitate ce evalueaza si certifica conformitatea noastra ca si furnizori de servicii de certificare si conformitatea serviciilor noastre de certificare conform Regulamentului 910/2014 si a actelor de implementare, noi urmarim cerintele din standardul ETSI EN 319 403.

8.3 Relația evaluatorului cu entitatea evaluată

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

8.4 Subiectele acoperite de evaluare

Auditurile planificate cuprind, dar nu se limitează la, toate aspectele operațiunilor și serviciilor certSIGN specificate în CPP BNR CA.

8.5 Acțiuni întreprinse ca urmare a deficienței

Organismul de evaluare a conformității raportează deficiențele și neconformitățile detectate către CMPP. certSIGN și organismul de evaluare a conformității analizează concomitent rezultatele raportului și aprobă un plan de corecție și un interval de timp pentru punerea în aplicare a acestuia.

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

8.6 Comunicarea rezultatelor

Organismul de evaluare a conformității comunică raportul de audit conducerii certSIGN și catre CMPP.

9 Alte aspecte

9.1 Termenii și încetarea

9.1.1 Termenii

Prezentul CPP și orice modificări ale acestuia vor intra în vigoare după publicare în Depozitar și în conformitate cu secțiunea 9.2 și vor rămâne în vigoare perpetuu până la incetarea lor în conformitate cu prezenta secțiune.

9.1.2 Încetarea

Prezentul CPP rămâne în vigoare până la înlocuirea cu o nouă versiune.

9.1.3 Efectul terminării și supraviețuirii

Condițiile și efectul care rezultă din terminarea acestui CPP vor fi comunicate prin intermediul site-ului web certSIGN. Această comunicare va evidenția dispozițiile care pot supraviețui rezilierii acestui CPP și vor rămâne în vigoare. Responsabilitățile de protejare a informațiilor confidențiale și a informațiilor personale trebuie să supraviețuiască încetării, iar termenii și condițiile pentru toate certificatele existente vor rămâne valabile pentru restul perioadelor de valabilitate ale acestor certificate.

9.2 Amendamente

9.2.1 Procedura pentru amendamente

certSIGN este responsabilă, prin Comitetul de Management al Politicilor (CMPP) și Procedurilor, de aprobarea și modificarea prezentului CPP. CPP-se revizuieste cel putin odata pe an.

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

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

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

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

9.2.2 Mecanismul de notificare și perioada

Toate modificările aduse prezentului CPP aflate în analiza CMPP vor fi distribuite părților interesate înainte de sau la publicare. Data intrării în vigoare este indicată pe pagina titlului prezentului CPP.