Cod de Practici și Proceduri

Autoritatea de Certificare DigiSign

Certificate digitale calificate

conform Regulamentului eIDAS și legislației naționale

Categorie:	**Document Public**	Limba:	**Română**
Emis de:	**Organismul de Gestionare a Politicilor DigiSign**		
Verificat de:	**Auditor Intern**	Ediția:	**2**
Aprobat de:	**Director General**	Verisunea:	**1**

OID: **1.3.6.1.4.1.34285.1.1.1.2.3.1.0**

DIGISIGN S.A.

Str. Virgil Madgearu, nr. 2 – 6, sector 1

014135, București, România

+4 031 620 20 00

+4 031 620 20 80

office@digisign.ro

www.digisign.ro

Istoric document

Ediția	Versiunea	Descriere	Data	Autor
1	0	Prima redactare: Codul de Practici și Proceduri al Autorității de Certificare DigiSign, în conformitate cu Regulamentul eIDAS și legislația națională aplicabilă	15 mai 2017	Organismul de Gestionare al Politicilor din cadrul DigiSign
1	1	Actualizări aduse ca urmare a auditului	15 iunie 2017	Organismul de Gestionare al Politicilor din cadrul DigiSign
1	2	Actualizare caracteristici pentru certificatele utilizatorilor finali	17 noiembrie 2017	Organismul de Gestionare al Politicilor din cadrul DigiSign
1	3	Actualizare metode de identificare si adaugare de autoritati noi	22 noiembrie 2018	Organismul de Gestionare al Politicilor din cadrul DigiSign
2	0	Actualizare metode de identificare	15 Octombrie 2019	Organismul de Gestionare al Politicilor din cadrul DigiSign
2	1	Actualizari minore si roluri de încredere	28 Iulie 2020	Organismul de Gestionare al Politicilor din cadrul DigiSign

Cuprins

1. Introducere

DIGISIGN S.A. (denumită în continuare DigiSign) operează o infrastructură de chei publice (denumită în continuare PKI) în vederea furnizării de servicii de încredere, precum: semnături electronice calificate, sigilii electronice calificate și mărci temporale calificate. DigiSign PKI utilizează o Autoritatea de Certificare cu rol de rădăcină, sub care sunt emise Autorități de Certificare intermediare dedicate unei clase sau unui anumit tip de serviciu. În cadrul unei Autorități de Certificare Intermediară sunt definite mai multe profile de certificate pentru a emite un tip de certificat specific unei anumite clase sau aplicabilități.

În calitate de Autoritate de Certificare (denumită în continuare CA), DigiSign emite certificate digitale atât entităților din cadrul sectorului public, cât și celui privat, dar și persoanelor fizice, în conformitate cu regulile, principiile și practicile definte în acest document. În rolul său de CA, DigiSign operează funcții asociate cu operații criptografice care includ, dar nu se limitează la, cereri, emitere, revocare, suspendare, reînnoire de certificate digitale, emiterea și publicarea Listelor de Certificate Revocate (denumite în continuare CRL), precum și menținerea unui serviciu de verificare în timp real al certificatelor, bazat pe protocolul Online Certificate Status Protocol (denumit în continuare OCSP).

DigiSign este unul din principalii Prestatori de Servicii de Încredere Calificate care reușește cu succes să furnizeze servicii de încredere precum semnături electronice calificate, sigilii electronice calificate și mărci temporale calificate, având în același timp și un rol de Terță Parte de Încredere (denumită în continuare TTP) în ceea ce privește crearea și validarea serviciilor respective.

1.1. Informații generale

1.1.1. Identificarea documentului

Acest document reprezintă o declarație publică privind practicile utilizate de DigiSign în calitate de prestator de servicii de încredere calificate, în vederea emiterii, reînnoirii, suspendării, revocării, validării și, în general, administrării cu succes a certificatelor digitale emise. Acest document este denumit Codul de Practici și Proceduri al Autorității de Certificare DigiSign (în continuare CPP) și este structurat în conformitate cu RFC 3647 și standardul ETSI EN 319401. În acest document, dacă nu este specificat altfel, expresia CPP reprezintă prezentul document.

Codul de Practici și Proceduri descrie criteriile stabilite de DigiSign pentru procesul de furnizare a serviciilor de încredere în vederea augumentării nivelul de încredere și siguranță în tranzacțiile electronice. De asemenea, acest CPP descrise practicile utilizate de DigiSign pentru a furniza servicii de încredere calificate, precum semnături electronice calificate, sigilii electronice calificate și mărci temporale calificate, în conformitate cu Regulamentul UE nr. 910/2014 (denumit în continuare Regulamentul eIDAS), legislația națională aplicabilă și standardele relevante în domeniu. Mai mult, acest document descrie regulile implementate de DigiSign în vederea asigurării unui standard înalt de securitate, pentru care DigiSign a obținut certificarea ISO/IEC 27001:2013.

Prin urmare, în termeni generali, acest document descrie:

- principiile, regulile și practicile privind ciclul de viață al certificatelor digitale, precum și controalele operaționale
- sistemele și procesele de încredere utilizate de DigiSign
- chestiuni privind aspectele legale, tehnice și de afacere, comune tuturor tipurilor de certificare (și, prin urmare, comune tuturor politicilor utilizate)
- evaluările și auditurile de conformitate ale soluțiilor DigiSign

- practicile privind administrarea politicilor
- prevederile generale privind obligațiile, răspunderea și garanțiile tuturor participanților în procesul de certificare
- conformitatea cu Regulamentul eIDAS, legislația națională aplicabilă și standardele relevante în domeniu.

Acest CPP face referință și înglobează Politica de Certificare a Autorității de Certificare DigiSign (denumită în continuare CP), care reprezintă un set anume de reguli și principii sub care sunt emise tipuri de certificate digitale aparținând unei comunități anume și/sau unei clase de aplicații cu aceleași cerințe de securitate. Scopul Politicii de Certificare este de a stabili, în termeni generali, ce anume trebuie să facă un participant al DigiSign PKI, precum și aria de aplicabilitate a unui certificat în conformitate cu tipul/clasa acestuia.

1.1.2. Publicare și coordonate de contact

Acest CPP este disponibil public, după cum urmează:

- online la adresa www.digisign.ro sau prin cerere trimisă la office@digisign.ro
- fizic, prin cererea trimisă către sediul DigiSign.

CPP este redactat în două limbi: engleză (varianta originală) și română (varianta tradusă). În eventualitatea unui conflict între cele două versiuni, documentul redactat în limba engleză va prevala.

Atât CPP, cât și CP, sunt administrate de către Organismul de Gestionare a Politicilor din cadrul DigiSign, în conformitate cu cap. 1.4 al acestui document. Mai multe informații în acest sens pot fi obținute prin cerere scrisă trimisă către DigiSign.

Sediul DigiSign și coordonatele de contact sunt:
Adresă: str. Virgil Madgearu, nr. 2 – 6, sector 1, București, 014135, România
Website: www.digisign.ro
E-mail: office@digisign.ro
Telefon: +4 031 620 20 00
Fax: +4 031 620 20 80

1.2. Prezentarea generală a procesului de certificare

Scopul principal al DigiSign PKI este de a furniza în România, dar și în afara granițelor naționale, servicii electronice de încredere bazate pe infrastructuri de chei publice. DigiSign prestează următoarele servicii:

- Servicii de înregistrare – înregistrarea cererilor și verificarea identității și a atributelor specifice titularilor de certificate digitale
- Servicii de emitere – generarea de perechi de chei criptografice, crearea și semnarea certificatelor digitale în baza identității și a altor atribute specifice, verificate prin serviciile de înregistrare
- Servicii de diseminare – diseminarea certificatelor către titularii acestora și, cu acordul titularilor, publicarea certificatelor pentru a deveni opozabile terților
- Servicii de administrare a revocarilor – procesarea cererilor de revocare în vederea stabilirii măsurii corecte ce urmează a fi luată în legătură cu respectiva cerere
- Servicii de publicare a revocărilor – publicarea informațiilor referitoare la statutul de revocat al certificatelor digitale emise
- Servicii de furnizare a dispozitivelor criptografice securizate – verificarea, recomandarea și furnizarea de dispozitive criptografice securizate

În vederea prestării acestor servicii, DigiSign utilizează această declarație publică ca și bază a funcționării Autorităților de Certificare din domeniul său. Mai mult, acest document poate fi considerat baza încrederii utilizatorilor care folosesc serviciile DigiSign deoarece descrie regulile aplicate identificării titularilor de certificate, ale emiterii și reînnoirii de certificate digitale, precum și procedurle utilizate pentru recuperarea în caz de dezastru și continuare a afacerii.

În procesul de certificare sunt identificați diferite entități ce au rol de participanți ai DigiSign PKI, precum:

- Autoritățile de Certificare identificate în structura certificatelor digitale ca și Emitent. Cheia private a unei Autorități de Certificare este utilizată în scopul semnării de certificate digitale, CA-urile având rolul general de a menține responsabilitatea procesului de certificare, asigurând respectarea cerințelor policitilor aferente acestora
- Utilizatorii finali care pot fi titularii certificatelor, beneficiarii acestora sau terțe părți interesate
- Alți participanți precum Autoritățile de Înregistrare, Autoritățile de Validare, Autoritățile de Marcare Temporală, depozitarul DigiSign etc

1.2.1. Ierarhia din cadrul DigiSign PKI

Arhitectura DigiSign PKI este împărțită pe mai multe nivele, în funcție de aria de aplicabilitate a certificatelor digitale, a algoritmului de semnare utilizat și a tipului de circuit aferent (public sau închis).

Nivelul 1 conține Autoritatea de Certificare rădăcină (denumită în continuare ROOT CA) care acționează ca punct de încredere, prin urmare fiecare cale de din lanțul de certificare trebuie să înceapă cu certificatul ROOT CA aferent:

- DigiSign Root Certification Authority (circuit public)
- DIGISIGN PRODUCTION CA V3 (circuit închis)
- DIGISIGN TEST CA V3 (circuit închis)
- DIGISIGN BNR PRODUCTION CA (circuit închis)
- DIGISIGN BNR TEST CA (circuit închis)

Aceste ROOT CA operează exclusiv în mod offline și sunt utilizate pentru a semna CA Intermediare, aferente Nivelului 2, precum și CRL-urile acestora. În cazul în care CA Intermediare din Nivelul 2 sunt compromise, ROOT CA sunt utilizate pentru a revoca certificatele respectivelor CA și pentru a emite un nou certificat.

Nivelul 2 conține Autoritățile de Certificare Intermediare, ale căror certificate sunt semnate direct de către ROOT CA. În ierarhia DigiSign PKI sunt identificate următoarele:

DigiSign Root Certification Authority emite și semnează certificatul pentru CA Intermediar:

- DigiSign Qualified Class 3 CA 2017 (circuit public)

DIGISIGN PRODUCTION CA V3 emite și semnează certificatele pentru CA Intermediare:

- DigiSign for Banking Qualified DS Production CA V4 (circuit închis)
- DigiSign for Banking Simple SSL Production CA V4 (circuit închis)

DIGISIGN TEST CA V3 emite și semnează certificatele pentru CA Intermediare:

- DigiSign for Banking Qualified DS Test CA V4 (circuit închis)
- DigiSign for Banking Simple SSL Test CA V4 (circuit închis)

DIGISIGN BNR PRODUCTION CA emite și semnează certificatele pentru CA Intermediare:

- DigiSign for BNR Qualified DS Production CA (circuit închis)

- DigiSign for BNR Simple SSL Production CA (circuit închis)

DIGISIGN BNR TEST CA emite și semnează certificatele pentru CA Intermediare:
- DigiSign for BNR Qualified DS Test CA (circuit închis)
- DigiSign for BNR Simple SSL Test CA (circuit închis)

Nivelul 3 conține certificatele digitale emise către utilizatorii finali, emise și semnate de către CA Intermediare. Certificatele digitale emise utilizatorilor finali sunt descrise în acest document, în special în capitolul privind utilizarea și aria de aplicabilitate a certificatelor.

Certificatele digitale emise de DigiSign, prin intermediul DigiSign for Banking CAs, sunt restricționate utilizării în ierarhie publică, scopul acestora fiind de a fi utilizate în sistemul SENT operat de TRANSFOND S.A., în baza unui protocol tehnic încheiat între DigiSign și TransFond. Acest protocol este confidențial și nu va fi făcut disponibil public.

Certificatele digitale emise de DigiSign, prin intermediul DigiSign for BNR CAs, sunt restricționate utilizării în ierarhie publică, scopul acestora fiind de a fi utilizate în sistemele ReGIS și SaFIR operate de Banca Nationala a Romaniei, în baza unui protocol tehnic încheiat între DigiSign și Banca Nationala a Romaniei. Acest protocol este confidențial și nu va fi făcut disponibil public.

1.2.2. Participanți ai DigiSign PKI

Participanți ai DigiSign PKI sunt acele entități care îndeplinesc un rol în DigiSign PKI fie prin utilizarea și prin furnizarea serviciilor de certificare. Astfel sunt identificați următorii participanți:
- Autoritățile de Certificare (CA)
- Autoritățile de Înregistrare (RA)
- Autoritățile de Validare (VA)
- Beneficiarii (Subscribers)
- Titularii (Subjects)
- Terțe părți interesate (Relying Parties)
- Alți participanți: Autoritățile de Marcare Temporală (TSA), depozitarul DigiSign etc

A. Autoritățile de Certificare (CA)

A.1. Autoritățile Primare de Certificare

DigiSign utilizează ca și Autoritate Primară de Certificare cu rol de punct de încredere pentru orice parte interesată în serviciile furnizate de DigiSign, respectiv DigiSign Root Certification Authority. O Autoritate Primară de Certificare din domeniul DigiSign operează în baza unui certificat auto-semnat de către ea însăși. Acest tip de CA poate emite și semna certificate doar pentru CA subordonate.

Certificatul auto-semnat nu conține câmpul *certificatePolicies* în structura sa, ceea ce înseamnă că nu există o limită privind calea din lanțul de certificare căreia respectivul certificat îi poate fi atașat.

O Autoritate Primară de Certificare poate furniza servicii de certificare doar sie însăși și CA Intermediare, subordonate acesteia.

A.2. Autoritățile Intermediare de Certificare

Înainte de începerea activității, orice CA intermediară trebuie să trimită o cerere către ROOT CA pentru a fi înregistrată și a i se emit și semna certificatul digital aferent. CA intermediare din domeniul DigiSign sunt identificate după cum urmează:

Autoritate Intermediară de Certificare	OID[1]
DigiSign Qualified CA Class 3 2017	1.3.6.1.4.1.34285.1.2.4.256.2.1.3.42017
DigiSign for Banking Qualified DS Production CA V4	1.3.6.1.4.1.35285.256.10.3.20141030
DigiSign for Banking Simple SSL Production CA V4	1.3.6.1.4.1.35285.256.10.4.20141030
DigiSign for Banking Qualified DS Test CA V4	1.3.6.1.4.1.35285.256.10.5.20141030
DigiSign for Banking Simple SSL Test CA V4	1.3.6.1.4.1.35285.256.10.6.20141030
DigiSign for BNR Qualified DS Production CA	1.3.6.1.4.1.35285.1.2.4.256.1.1.2.3.82017
DigiSign for BNR Simple SSL Production CA	1.3.6.1.4.1.35285.1.2.4.256.1.1.2.3.82017
DigiSign for BNR Qualified DS Test CA	1.3.6.1.4.1.35285.1.2.1.256.1.1.2.0.82017
DigiSign for BNR Simple SSL Test CA	1.3.6.1.4.1.35285.1.2.1.256.1.1.2.0.82017

Table 1 – OID aferente certificatelor CA intermediare

B. Autoritatea de Înregistrare

Autoritatea de Înregistrare (denumită în continuare RA) asistă Autoritatea de Certificare privind identificarea solicitanților de certificate digitale și autentificarea cererilor acestora de înregistrare, reînnoire, suspendare și revocare.

RA primește, verifică și aprobă ori respinge, după caz, cererile de înregistrare, de reînnoire și revocare sau suspendare. Mai mult, RA poate trimite solicitări către CA în vederea anulării unei cereri sau a unui certificat.

RA îndeplinește un rol esențial în procesul de certificare datorită operațiilor de verificare identității solicitanților și autentificare a cererilor înaintate de aceștia. Nivel de asigurare privind identitatea unui solicitant este stabilit de procesul de identificare a acestuia pe care îl realizează RA și este impus de către clasa certificatului solicitat. În cazul celui mai simplu proces de identificare, RA verifica corectitudinea domeniului de care aparține adresa de e-mail introdusă în cerere de către solicitant. În schimb, cel mai riguros și precis proces de identificare a solicitantului presupune prezența în persoană a acestuia la una din RA din cadrul domeniului DigiSign, împreuna cu un act de identitate valid, în original care să dovedească identitatea acestuia. Procesul de identificare a solicitantului poate fi desfășurat fie prin mijloace electronice, fie fizic prin intermediul unui reprezentant al RA.

Pentru a asigura un nivel înalt și calitativ al serviciilor de încredere furnizate, DigiSign se bazează pe o rețea de Autorități de Înregistrare. Specific, RA îndeplinește funcțiile de înregistrare a solicitanților, validare a identității acestora, autentificarea cererilor de înregistrare, verificarea formularelor și documentelor înainte de către solicitanți, precum și

[1] Structura de bază a OID [1.3.6.1.4.1.35285]: 1 – ISO; 3 – Identified Organization; 6 – DOD; 1 – Internet; 4 – Private; 1 – Enterprise; 35285 – Numărul IANNA asignat DigiSign

diseminarea certificatelor digitale și a dispozitivelor criptografice securizate pe care acestea sunt stocate către titulari.

Furnizarea serviciilor specifice RA se desfășoară în conformitate cu prezentul CPP, iar respectarea acestora este asigurată de DigiSign prin încheierea unor contracte specifice. Lista RA autorizate să desfășoare activitățile descrise mai sus, sau cel puțin o parte, este disponibilă public la adresa www.digisign.ro.

C. Autoritățile de Validare

Autoritatea de Validare din cadrul domeniului DigiSign este compusă din trei servicii diferite: validare în timp real a certificatelor emise prin intermediul protocolului OCSP, validarea certificatelor emise prin consultarea Listelor de Certificate Revocate și verificarea certificatelor prin consultarea registrului electronic de evidență a certificatelor emise. Aceste servicii sunt descrise în cadrul cap. 4.10 al prezentului document.

D. Titularii certificatelor digitale

Titularul unui certificat digital este reprezentat de către entitatea înscrisă în câmpul *Subject* din structura certificatului și care nu emite certificate către alte entități, în cazul certificatelor emise către utilizatorii finali. Titularul unui certificat digital emis de CA DigiSign poate fi:

- o persoană fizică
- o persoană fizică identificată în asociație cu o persoană juridică (certificatul conține atribute specifice privind persoana juridică care este legată de persoana fizică)
- o persoană juridică

De asemenea, Autoritățile de Certificare și de Marcare Temporală din cadrul DigiSign pot fi titulari de certificate digitale.

E. Beneficiarii

Beneficiarii sunt reprezentați de către entitățile care înaintează o solicitare către DigiSign în vederea obținerii unuia sau mai multor certificate digitale. În general, Beneficiarul este Titular certificatului însuși, însă sunt cazuri în care Beneficiarul acționează în numele unuia sau a mai multor Titulari distincți, de care este legat (exemplu: Beneficiarul este o companie care solicita certificate pentru angajații săi în vederea participării la tranzacții electronice în numele și pentru companie). Astfel, având în vedere tipul de certificat solicitat Beneficiarul poate fi:

a. în cazul unui certificat digital calificat pentru semnătură electronică
   - persoana fizică însuși, titular al certificatului digital
   - persoana fizică mandatată de către titular
   - persoana juridică de care este legată persoana fizică, titular al certificatului

b. în cazul unui certificat digital calificat pentru sigiliu electronic
   - persoana fizică, reprezentant legal al persoanei juridice
   - persoana fizică, reprezentant autorizat/împuternicit/mandatat de către reprezentantul legal al persoanei juridice

DigiSign emite diferite tipuri de certificate digitale cu diferite tipuri de nivele de asigurare. Beneficiarii trebuie să decidă ce tip de certificat solicită, în funcție de care răspunde cel mai potrivit nevoilor lor. Pentru a fi eligibil de a beneficia de servicii de certificare, Beneficiarii trebuie să respecte cerințele impuse de procedura de obținere a certificatului solicitat, precum și obligațiilor și răspunderii specificate în prezentul document și în Condițiile generale de furnizare a serviciilor de încredere solicitate.

Pentru a evita un conflict de interese, Beneficiarii și DigiSign, în calitate de prestator de servicii de încredere calificat, sunt și vor rămâne entități diferite. Această regulă întâlnește o excepție în ceea ce privește entitățile care desfășoară toate sau o parte din activitățile specifice RA și care, prin urmare, pot avea calitatea de Beneficiar al serviciilor de încredere prestate de DigiSign atunci când solicită certificate digitale pentru sine sau pentru persoanele fizice care sunt asociate cu respectiva entitate.

D. Entitate Parteneră

O entitate parteneră poate fi reprezentată de o persoană sau de un dispozitiv, care se bazează pe un certificat digital emis de DigiSign sau pe o operațiune criptografică realizată cu un certificat digital emis de DigiSign.

O entitate parteneră utilizează cheia publică a certificatului fie pentru a valida o semnătură electronică, fie pentru a valida o marcă temporală, ori pentru a interoga identitatea titularului certificatului respectiv. De asemenea, o entitate parteneră poate utiliza cheia publică a unui certificat digital emis de DigiSign în vedera creării unui canal de comunicare securizat între el și titularul certificatului prin operțiuni criptografice de tip criptare/decriptare.

În vederea verificării unui certificat digital, o entitate parteneră trebuie întotdeaună să verifice emitentul respectivului certificat pentru a stabili dacă politicile acestuia răspund nivelului de asigurare de care entitatea parteneră are nevoie pentru a accepta respectivul certificat. Mai mult, entitatea parteneră trebuie sa verifice statusul certificatului în vederea stabilirii dacă acesta este valid și utilizat corespunzător, prin accesarea serviciilor de validare puse la dispoziție de DigiSign (exemplu: OCSP, CRL, registrul electronic de evidență a certificatelor emise). Acestea verificării trebuie realizate de entitatea parteneră întotdeauna înainte de a se baza pe orice informație inclusă în respectivul certificat.

Acceptând un certificat digital emis de DigiSign ca fiind compatibil cu nivelul de încredere solicitat, o entitate parteneră acceptă implicit respectarea obligațiilor și răspunderii ce ii revin conform prezentului document.

Entitatea Parteneră poartă răspunderea pentru operația de verificare și pentru modul de verificare a certificatului digital pe care urmează să se bazeze ca fiind de încredere, respectiv ca răspunzând nivelului de asigurare de care acesta are nevoie. Entitatea Parteneră trebuie să utilizeze informațiile cuprinse în structura certificatului doar după o verificare a acestora, în special pentru a stabili dacă respectivul certificat a fost utilizat în conformitate cu scopul și aria de aplicabilitate declarate.

E. Alți participanți

Pe lângă participanții descriși mai sus, la procesul de certificare participă și entități cu un rol deosebit, precum Autoritățile de Marcare Temporală și depozitarul DigiSign.

Depozitarul este administrat de DigiSign și este public disponibil la adresa www.digisign.ro, reprezentând o interfață web unde sunt cuprinse următoarele informații, dar fără a se limita la:

- politicile, practicile și declarațiile publice ale DigiSign
- informațiile privind serviciile de încredere furnizate de DigiSign
- registrul electronic de evidență al certificatelor emise și ale mărcilor temporale
- cheile publice ale Autorităților de Certificare din cadrul DigiSign

Depozitarul DigiSign este descris în prezentul document pe parcursul următoarelor capitole. Autoritatea de Marcare Temporală DigiSign nu face subiectul prezentului CPP.

Informații detaliate privind declarația publică referitoare la politicile și practicile utilizate în furnizarea serviciului de marcare temporală se găsesc în Politica și Codul de Practici și Proceduri al Autorității de Marcare Temporală DigiSign, publicat și disponibil la adresa www.digisign.ro.

1.3. Tipuri de certificate

Un certificat digital (comun numit *certificat*) reprezintă date în format electronic care leagă în mod criptografic identitata unei entități de o cheie publică. Un certificat digital permite unei entități să aparticie la tranzacții electronice, în vederea dovedirii indentității acesteia altor participanți la astfel de tranzacții. Diferite tipuri de certificate sunt utilizate în medii electronice ca și echivalentul unei cărți de identitate electronice.

Marca temporală are rolul de a lega criptografic o anumită formă a unei informații electronice de un anumit moment de timp, stabilind astfel dovada faptului că forma informației respective a existat la un moment anume de timp.

Certificatele digitale emise în conformitate cu acest CPP pot fi utilizate pentru diferite scenarii, precum semnarea electronică, sigiliarea electronică, marcarea temporală sau autentificare. Totuși, nivelul de importanță a unei informații procesate sau protejate de un certificat digial variază în funcție de anumiți factori. Prin urmare, orice Enitate Parteneră are obligația de a evalua în mod corespunzător un certificat digital, în funcție de mediul și aplicația în care se utilizează certificatul și riscurile asociate, luând o decizie informată și corectă în legătură cu utilizarea efectivă a unui anumit tip de certificate, emis în conformitate cu acest CPP.

1.3.1. Utilizarea corespunzătoare a unui certificat

Utilizarea corespunzătoare a unui certificat subliniază scopul acestuia pentru care poate fi folosit de către utilizatori. Acest scop este împărțit în două elemente: aria de aplicabilitate a certificatului și aplicațile permise sau interzise în legătură cu care se poate utiliza certificatul.

Acest CPP face referire la certificatele digitale care pot fi utilizate în procesare și asigurea securității informației cu un nivel ridicat de încredere. Nivelul de încredere necesar trebuie evaluat de către utilizatori înainte de a utiliza un certificat digital.

Următorul tabel descrie succint utilizările corespunzătoare ale certificatelor digitale, în funcție de nivelul de încredere al acestora. Descrierea are status de recomandare și nu este limitativă.

Nr. Crt.	Nivel de încredere	Politica de Certificare	Utilizare corespunzătoare
1	Ridicat	Calificat	Clasa de certificat digitale calificate asigură cel mai înalt nivel de încredere în ceea ce privește identitatea titularilor acestora. Acest nivel este corespunzător unui mediu unde compromitarea datelor are un risc major și unde producerea unui incident are implicații critice. Acest tip de certificate sunt în general recomandate pentru a asigura protecția tranzacțiilor de valoare nelimitată și a tranzacțiilor cu un risc semnificativ privind frauda.

			Certificatele digitale calificate pentru semnătură electronică pot fi utilizate pentru autentificare și crearea și validarea de semnături electronice și mărci temporale. Certificatele digitale calificate pentru sigiliu electronic pot fi utilizate pentru autentificare și crearea și validarea de sigilii electronice și mărci temporale.

Enitățile Partenere sunt responsabile pentru identificarea nivelul de importanță a informațiilor procesate sau protejate de un certificat digital, identificând astfel și nivelul de încredere necesar aferent certificat digital. Având în vedere factorii de risc semnificativ, Entitățile Partenere trebuie să decidă care este tipul de certificat care răspunde corespunzător cerințelor necesare. Utilizatorii trebuie să identifice cerințele Enitităților Partnere (spre exemplu, dacă semnătura electronică necesară trebuie să fie calificată) și apoi să solicite DigiSign emiterea unui certificat digital corespunzător cerințelor respective.

1.3.2. Aria de aplicabilitate recomandată

DigiSign emite diferite tipuri de certificate, în funcție de aria de aplicabilitate a acestora, după cum urmează:

a. Certificatele Autorităților de Certificare – utilizarea acestora nu este restricționată la o anumită arie; aplicabilitatea poate rezulta din valorile extensiilor certificatului care stabilesc cum va fi utilizată cheia privată sau care este rolul acesteia (spre exemplu, certificatul ROOT CA poate fi utilizat pentru semnarea certificatelor altor autorități subordonate și nu pentru certificatele utilizatorilor finali)

b. Certificatele Autorităților de Marcare Temporală – sunt emise serviciului de marcare temporală, care, ca și răspuns pentru o solicitare, emite mărci temporale care leagă anumite date electronice (documente, mesaje, semnături etc) de un anumit moment de timp, determinând astfel secvența de date în timp.

c. Certificatele Autorităților de Validare – sunt emise pentru serviciul de validare în timp real a certificatelor, în conformitate cu protocolul OCSP și furnizează informații referitoare la statusul certificatelor.

d. Certificatele emise utilizatorilor finali:

- **demo/testare**: aceste certificate au ca scop utilizarea lor de către utilizatorii finali pentru sesiune de demonstrare sau testare a funcționalităților certificatelor cu anumite aplicații**.** Utilizarea acestor certificate poate fi customizată conform cerințelor utilizatorilor (spre exemplu pentru autentificare, criptare etc)
- **criptare**: acest tip de certificate este destinat utilizării doar în scopul de a cripta sau decripta informații electronice, în vederea asigurării confidențialității informației
- **autentificare**: acest tip de certificate este destinat autentificării titularului certificatului într**-**un anume sistem
- **semnătură/sigilu**: acest tip de certificate este destinat creării și validării semnăturilor sau sigiliilor electronice, după caz.
- **semnătură calificată/sigiliu calificat**: acest tip de certificate este destinat creării și validării semnăturilor calificate sau sigiliilor calificate, după caz, asigurând astfel valoare legală
- **semnare de cod**: acest tip de certificate este destinat programatorilor de cod software în vederea protejării codului software împotriva falsificării**.**

1.3.3. Utilizări necorespunzătoare sau interzise

Este interzisă utilizarea unui certificat digital emis de CA DigiSign cu alt scop decât cel declarat în prezentul document.
Indiferent de nivelul de încredere al unui certificat digital, acesta nu oferă nici o garanție referitoare la titularul certificatului precum acesta ar acționa cu bună credință, ca este cinstit sau onest în afacerile sale, ori că el sau afacerile sale sunt conforme legislației aplicabile. Un certificat digital confirmă doar faptul că informațiile conținute în acesta au fost verificate în conformitate cu prevederile prezentului document în momentul în care certificatul a fost emis (spre exemplu, certificatele pentru semnare de cod nu confirmă faptul că codul software semnat este sigur pentru instalare sau că nu conține viruși).

1.4. Administrarea documentului

Acest capitol descrie procedurile implementate de DigiSign în vederea redactării și administrării politicilor de certificare și ale codurilor de practici și proceduri din domeniul DigiSign. Acest capitol privește procedurile referitoare la aprobarea acestor documente, precum și natura schimbărilor care pot interveni și care conduc la actualizarea respectivelor documente.

1.4.1. Responsabil

Politicile de certificare și codurile de practici și proceduri din domeniul DigiSign sunt administrate de DIGISIGN S.A. prin Organismul de Gestionare al Politicilor.

Organismul de Gestionare al Politicilor este format din managementul DIGISIGN S.A. Procedura de adăugare sau eliminare a unor membrii din acest organism este determinată și organizată prin documente interne care nu sunt destinate publicului.

1.4.2. Contact

Organismul de Gestionare al Politicilor poate fi contactat la următoarele coordonate:
DIGISIGN S.A.
Str. Virgil Madgearu, nr. 2 – 6, sector 1, București, 014135, România
+4 031 620 20 00 (tel)
+4 031 620 20 80 (fax)
office@digisign.ro
www.digisign.ro

1.4.3. Publicare și notificare

Prezentul document este disponibil public, în format electronic la adresa www.digisign.ro, pentru a fi consultat de către orice parte interesată. În vederea accesării documentului nu sunt necesare credențiale speciale de acces. Acest document poate fi furnizat și prin cerere scrisă adresată la office@digisign.ro sau fizic la coordonatele de contact de mai sus.

DigiSign poate publica până la trei versiuni ale documentelor de acest tip: versiunea curentă aplicabilă, versiunea scoasă din vigoare și versiunea care este în curs de aprobare, dacă este cazul. Statusul versiunii este evidențiat în prima pagina a documentului. Toți participanții PKI trebuie să verifice statusul documentului și să ia în considerare versiunea care curentă aplicabilă, fiind versiunea pe care aceștia trebuie să o respecte.

Versiunea care are statusul spre aprobare reprezintă noua versiune emisă de DigiSign și care este publicată pentru comentarii timp de 30 de zile, dacă este cazul.

Acest CPP este la prima ediție, fiind redactat atât în limba engleză cât și în limba română.

2. Publicarea și responsabilitățile depozitarului

Depozitarul DigiSign este public disponibil pentru a fi consultat la adresa www.digisign.ro, nefiind necesare credențiale speciale pentru accesarea acestuia, și conține:

- CP și CPP ale Autorităților de Certificare și Marcare Temporală din domeniul DigiSign, precum și PKI Disclosure Statement
- Condițiile generale de furnizare a serviciilor de încredere, în funcție de tipul acestora
- Certificatele ROOT CA și Intermediate CA din domeniul DigSign, împreună cu CRL aferente acestora
- Informațiile publice din certificatele digitale emise utilizatorilor finali
- Alte documente relevante, precum certificările și evaluarile DigiSign etc

Disponibilitatea depozitarului DigiSign este construită să depășească 99% din programul de lucru, fiind accesibil publicului 24 de ore din 24, 7 zile din 7, excluzând perioadele de mentenanța programată care sunt anunțate în prealabil cu 24 de ore înainte.

În cazul în care se identifică indisponibilitatea depozitarului datorită unui dezastru natural, precum evenimentul unei catastrofe, DigiSign va depune toate diligențele posibile pentru a restaura disponibilitatea serviciilor în 5 zile lucrătoare.

DigiSign asigură autenticitatea informațiilor publicate în depozitar prin implementarea unor mecanisme de protecție logică și fizică împotriva modificărilor, adăugirilor sau ștergerilor neautorizate. DigiSign poate lua măsuri apropriate în ceea ce privește protecția și prevenirea utilizării abuzive a depozitarului, a serviciului OCSP sau CRL.

În cazul în care DigiSign identifică o breșă de securitate (spre exemplu, integritatea depozitarului a fost afectată sau compromisă în orice fel), va lua măsuri corespunzătoare pentru a restabili integritatea depozitarului în cel mai scurt timp posibil și va notifica de îndată entitățile afectate și organismele responsabile. DigiSign își rezervă dreptul de a iniția acțiuni în justiție împotriva celor răspunzători pentru producerea unor astfel de evenimente.

DigiSign publică informații în depozitar cu următoarea frecvență:

Tipul de informații	Frecvența
Politici	În conformitate cu cap. 1.4
Condiții generale de furnizare a serviciilor	După actualizarea și aprobarea acestora
Certificate ale ROOT CA și Intermediar CA	După emiterea acesora
Certificate ale utilizatorilor finali	După emiterea acestora și acceptul titularilor
Certificări, evaluări și rapoarte de audit	După primirea acestora
Alte informații	De fiecare dată când este necesar

3. Identificare și autentificare

Acest capitol descrie regulile generale privind verificarea identității solicitanților care aplica pentru obținerea unui certificat digital emis de DigiSign. Acestea au ca baza informațiile incluse în certificate și identifică mijloacele necesare pentru a asigura faptul că respectivele informații sunt precise, corecte și credibile la momentul emiterii certificatului.

Verificarea este se realizează în mod obligatoriu în momentul emiterii certificatului, în baza cererilor de înregistrare sau modificare privind orice serviciu de încredere calificat solicitat.

3.1. Numele

DigiSign emite certificate digitale în conformitate cu standardul X.509 v3, ceea ce presupune ca emitentul certificatului și RA care acționează în numele emitentului, verifică și aprobă numele subiectului în conformitate cu cerințele specificate în standardul X.509 v3.

Numele subiectului și ale emitentului unui certificat sunt plasate în structura acestuia în conformitate cu construcția Numelui Distinctiv (denumit în continuare DN), cunoscute și sub denumirea de nume de directoare, create conform recomandărilor seriei X.500, IETF RFC 5280 și standardelor relevante emise de ETSI.

Numele subiectului și ale emitentului unui certificat au o însemnătate în limba română și în orice altă limbă de origine latină. Structura DN, aprobată, desemnată și verificată de către RA, depinde de tipul subiectului.

Numele subiectului este confirmat, după verificare, de către un opreator RA și aprobat de către un operator CA. DigiSign asigura în cadrul domeniului propriu, unicitatea DN-urilor. Pe parcursul ciclului de viată a unei CA din cadrul DigiSign, DN-ul nu va reasignat unei alte entități în afară de cea inițială căruia i-a fost asignat.

Pentru persoanele fizice, DN este construit din următoarele câmpuri, obligatorii sau opționale, după caz:

Câmp	Descriere
C	Prescurtarea internațională a numelui țării (RO pentru România), conform ISO 3166-1 alpha-2
S	Regiunea sau districtul de care aparține subiectul
L	Localitatea/orașul de care aparține subiectul
CN	Numele subiectului
O	Denumirea organizației de care aparține subiectul
OU	Denumirea departamentului de care aparține subiectul
T	Denumirea funcției subiectului
SN	Numele de familie al subiectului
G	Prenumele subiectului
P / Psyeudonym	Pseudonimul subiectului utilizat într-un anumit mediu sau care se dorește a fi utilizat pentru a nu divulga numele său real
SN	Codul de identificare alocat subiectului

Pentru persoanele juridice, DN este construit din următoarele câmpuri, obligatorii sau opționale, după caz:

Câmp	Descriere
C	Prescurtarea internațională a numelui țării (RO pentru România), conform ISO 3166-1 alpha-2
O	Denumirea organizației
OU	Denumirea departamentului din cadrul organizației
S	Regiunea sau districtul de care aparține organizația
L	Localitatea sau orașul de care aparține organizația
CN	Numele organizației
organizationIdentifier	Identificatorul alocat organizației

Posibilitatea de a opta pentru utilizarea unui pseudonim le este atribuită solicitanților sub condiția ca acesta să nu facă referire la expresii consacrate a fi necorespunzătoare sau care presupun uzurparea frauduloasă a unui nume cunoscut, or parodierea unei persoane.

3.2. Validarea inițială a identității

DigiSign verifică identitatea solicitantului înainte de emiterea certificatului digital. Procesul de validare diferă în funcție de tipul certificatului și aria de aplicabilitatea a acestuia, fiind desris în cele ce urmează. În cazul în care rezultatul procesului de validare este pozitiv, DigiSign verifică ca cererea înaintată de solicitantă să fie corectă, autorizată și completă, în conformitate cu dovezile prezentate privind identitatea.

Pentru ca DigiSign să poată desfășura activitatea de verificare, solicitantul are obligația de a furniza dovezi privind identitatea presupusă. Dovezile pot fi sub formă electronică sau în format fizic, însă în ambele cazuri RA verifică validitatea și autenticitatea acestora.

În cazul în care titularul certificatului nu coincide cu beneficiarul acestuia (spre exemplu, o companie care solicită certificate pentru angajații săi în vederea participării la diferite tranzacții electronice în numele companiei), beneficiarul are obligația de a furniza date de identificare a acestuia și dovezi privind autorizarea de a solicita servicii în numele titularului, precum, cel puțin:

- Denumirea sau numele complet al beneficiarului
- O dovadă a acordului titularului de i se furniza serviciile de certificare
- Atunci când beneficiarul este o persoană juridică, dovada precum acesta poate reprezenta legal respectiva persoană juridică și că este autorizat să solicite un certificat pentru acea persoană juridică
- Dacă beneficiarul nu este o persoană juridică, acesta va fi reprezentat de către persoana fizică autorizată să solicite și să reprezinte respectiva persoană juridică

Fiecare titular de certificat care solicită un certificat digital, înainte de emiterea acestuia, are obligația:

- să completeze formularul online de înregistrare ori un document care poate fi descărcat de la adresa www.digisign.ro, dacă este cazul
- să furnizeze dovezi privind identitatea acestuia
- să genereze o pereche de chei criptografice asimetrice (software sau într-un dispozitiv criprografic securizat în cazul certificatelor calificate) și să furnizeze dovezi către RA privind deținerea perechi respective de chei; alternativ, să delege RA sau CA pentru a-i fi generată perechea de chei în beneficiul acestuia
- să sugereze un nume distinctiv
- dacă este cazul, să completeze și să genereze un formular care să conțină și cheia publică și dovada corespondenței dintre aceasta și cheia privată pe care o deține
- opțional, să se prezinte la RA și să furnizeze documentele necesare (daca acest aspect este impus prin politica de certificare al respectivului tip de certificat)
- să încheie un acord cu DigiSign (prezentul CPP va face parte integrantă din respectivul acord)

În funcție de nivelul de încredere asociat certificatului, solicitantul poate avea obligația de a furniza mai multe sau mai puține evidențe, după caz. În confirmitate cu acest CPP, DigiSign emite certificate digitale calificate cu un nivel ridicat de încredere, stabilind în continuare condițiile în care aceste certificate pot fi emise.

A. Certificate care nu asigură nici un nivel de încredere

Emiterea certificatelor digitale fără care nu asigură nici un nivel de încredere presupune o verificare superficială a identității solicitantului. În acest caz, RA verifică doar domeniul adresei de e-mail specificată în cererea solicitantului. Nu sunt verificate alte date înainte de emiterea unui astfel de certificat.

B. Certificate care asigură un nivel scăzut de încredere

Pentru emiterea unui certificat digital cu un nivel scăzut de încredere, solicitanții trebuie să furnizeze dovezi privind identitatea pe care și-o asumă, în funcție de tipul de solicitant:

- dacă solicitantul este o persoană fizică, va trebui să depună la RA evidențe privind cel puțin:
  - numele său complet
  - data și locul nașterii, în referință cu un act de identitate recunoscut conform legislației naționale aplicabile, și alte atribute care pot fi utilizate în a distinge respectiva persoana fizică de alta cu același nume.
- dacă solicitantul este o persoană fizică reprezentant al unei persoane juridice, va trebui să depună la RA evidențe privind cel puțin:
  - numele său complet
  - data și locul nașterii, în referință cu un act de identitate recunoscut conform legislației naționale aplicabile, și alte atribute care pot fi utilizate în a distinge respectiva persoana fizică de alta cu același nume.
  - denumirea completă și statusul legal al persoanei juridice
  - orice informație relevantă privind identificarea respective persoane juridice
  - asocierea dintre persoana fizică și persoana juridică și acordul respectivei persoane juridice privind atributele specifice ale persoanei fizice care dovedesc legătura dintre aceasta și persoana juridică
- dacă solicitantul este o persoană juridică, va trebui să depună la RA evidențe privind cel puțin:
  - denumirea completă a persoanei juridice
  - dacă este cazul, asocierea dintre persoana juridică și entitatea identificată în legătură cu această persoană juridică și care apare în câmpul certificatului referitor la organizație

Emiterea unui certificat digital cu un nivel scăzut de încredere implică un proces de verificare a identității care privește cel puțin:

- RA colectează evidențele privind identitatea solicitantului (ex: o copie a actului de identitate) și, dacă este cazul, evidențe privind atributele specifice ale acestuia
- RA verifică ca datele colectate din cererea solicitantului corespund datelor din evidențele furnizate de solicitant
- Dacă rezultatul acestei verificări este pozitiv, RA aprobă cererea de emitere a certificatului și solicită CA emiterea acestuia
- Dacă rezultatul acestei verificări este negativ, RA refuză cererea de emitere a certificatului și notifică solicitantul referitor la decizia luată.

C. Certificate care asigură un nivel substanțial de încredere

Pentru certificatele digitale care asigură un nivel substanțial de încredere, solicitanții trebuie să facă dovadă identității pe care și-o asumă, conform celor descrise în cazul certificatelor care asigură un nivel scăzut de încredere. În plus față de acestea, solicitantul trebuie să depună evidențele necesare la RA, personal sau prin terț împuternicit prin împuternicirea încheiată la un notar public autorizat, conform legislației naționale aplicabile.

Emiterea unui certificat digital care asigură un nivel substanțial de încredere implică un proces al verificării identității solicitantului care privește cel puțin:

- RA colectează evidențele privind identitatea asumată de solicitant și, dacă este cazul, evidențe privind atributele specifice ale acestuia;
- RA verifică ca datele colectate din cererea solicitantului corespund datelor din evidențele furnizate de solicitant;
- Dovezile prezentate de solicitant sunt verificate de RA în prezența fizică a solicitantului (solicitantul se va prezenta personal la RA, cu excepția cazului în care acesta împuternicește un terț, caz în care terțul trebuie să se prezinte personal la RA cu o împuternicire notarială și un act de identitate valid, în original) sau, indirect, prin mijloace care asigură un nivel de încredere cel puțin echivalent cu prezența fizică a solicitantului;
- Dacă rezultatul acestei verificări este pozitiv, RA aprobă cererea de emitere a certificatului și solicită CA emiterea acestuia
- Dacă rezultatul acestei verificări este negativ, RA refuză cererea de emitere a certificatului și notifică solicitantul referitor la decizia luată.

D. Certificate care asigură un nivel înalt de încredere (certificate calificate)

Pentru certificatele digitale calificate care asigură un nivel înalt de încredere se vor aplica regulile descrise în cazul anterior. În plus, se vor aplica următoarele reguli:

a. Pentru certificatele digitale calificate pentru semnătura electronică, emise în numele persoanelor fizice, identitatea persoanei fizice și, dacă este cazul, atributele specifice ale acesteia, vor fi verificate după cum urmează:
   - prin prezența în persoană a respectivei persoane fizice la una din RA din cadrul domeniului DigiSign, sau
   - prin prezența în persoană a respectivei persoane fizice la un notar public autorizat, sau
   - prin mijloace care asigură un nivel de încredere cel puțin echivalent cu prezența fizică a solicitantului și pentru care DigiSign asigură echivalența, precum identificarea și autentificarea solicitantului prin intermediului unui certificat digital calificat activ emis de DigiSign, sau
   - prin mijloace de identificare ce oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică, sau
   - de către o parte terță, cu respectarea legislației naționale în vigoare, aplicabilă în domeniul certificării/atestării identității.

b. Pentru certificatele digitale calificate pentru sigiliu electronic, emise în numele persoanelor juridice, identitatea persoanei juridice și, dacă este cazul, atributele specifice ale acesteia, vor fi verificate după cum urmează:
   - prin prezența în persoană a persoanei fizice autorizate de persoana juridică, la una din RA din cadrul domeniului DigiSign, sau
   - prin prezența în persoană a persoanei fizice autorizate de persoana juridică la un notar public autorizat, sau
   - prin mijloace care asigură un nivel de încredere cel puțin echivalent cu prezența fizică a solicitantului și pentru care DigiSign asigură echivalența, precum identificarea și autentificarea solicitantului prin intermediului unui certificat digital calificat activ emis de DigiSign, sau
   - prin mijloace de identificare ce oferă un nivel de asigurare echivalent din perspectiva fiabilității cu prezența fizică, sau
   - de către o parte terță, cu respectarea legislației naționale în vigoare, aplicabilă în domeniul certificării/atestării identității.

Pentru certificatele digitale calificate, cheia privată va fi întotdeauna generată printr-un dispozitiv de creare a semnăturilor electronice calificate (denumit în continuare QSCD). O entitate poate genera cheia privată în QSCD de unul singur sau poate delega DigiSign să genereze cheia privată în QSCD în numele său. În cazul din urmă, DigiSign asigură faptul că QSCD și cheia privată generată sunt trimise în siguranță către entitatea solicitantă, în

conformitate cu cap. 6.1. – Generarea și instalarea cheii private. În cazul în care entitatea își generează singura cheia privată, aceasta trebuie să facă dovada faptului că dispozitivul pe care s-au generat cheile este un dispozitiv QSCD, precum și dovada privind generarea cheilor conform standardelor recomandate de DigiSign.

3.3. Identificarea și autentificarea cererilor de reînnoire

Procedura privind reînnoirea certificatelor este descrisă în cadrul capitolului 4.5 al acestui document.

Toate cererile privind reînnoirea certificatelor vor fi înaintate către DigiSign prin completarea formularului corespunzător. Cererile sunt procesate de RA care asigură corectitudinea și complementaritatea acestora.

Toate cerințele descrise în cadrul cap. 3.2. al acestui document, privind evidențele și procedurile impuse a fi urmate pentru a dovedi identitatea, se aplică și în cazul cererilor de reînnoirea a certificatelor. În particular, se aplică și următoarele cerințe suplimentare:

- RA verifică existența și validiatea certificatului inițial, iar în cazul reînnoirii prin mijloace electronice, certificatul trebuie să fie valid, nerevocat și nesuspendat, iar cererea să fie înaintată către DigiSign cu cel puțin 5 zile înainte de expirarea certificatului;
- RA se asigură de faptul că solicitantul a citit și a fost de acord cu condițiile generale de furnizare a serivicului de încredere calificat (chiar dacă acestea nu au suferit modificări de când au fost acceptate și semnate la emiterea certificatului inițial), prin verificarea că acestea au fost semnate corespunzător de către solicitant

În cazul în care datele inițiale care au stat a baza emiterii certificatului au suferit modificări, solicitanul trebuie să înainteze către DigiSign și evidențe privind noile informații, în conformitate cu cap. 3.2. al acestui document.

3.4. Identificarea și autentificarea cererilor de revocare sau suspendare

Cererile de revocare și/sau suspendare pot fi trimise către DigiSign fie prin mijloace electronice (e-mail la helpdesk@digisign.ro, fax la 031 620 20 00), fie prin mijloace fizice precum cereri trimise prin servicii poștale sau de curierat către sediul DigiSign.

După primirea unui cereri de revocare și/sau suspendare, semnată, identitatea solicitantului este verificată în sensul conformității datelor trimise prin cerere cu datele declarate prin alte mijloace. Doar în cazul în care RA obține un rezultat pozitiv în ceea ce privește procesul de verificare al identității solicitantului și ale datelor trimise, înaintează la rându-i o solicitare către CA de revocare sau suspendare a certificatului respectiv.

Toate cererile privind revocarea sau suspendarea unui certificat sunt, înainte de a se iniția orice acțiune – acceptare sau respindere a cererii – verificate și autentificate în ceea ce privește solicitantul și dreptul acestuia de a înaintata cererea.

4. Cerințe operaționale - Ciclul de viață al unui certificat

Acest capitol descrie procedurile privind înregistrarea, identificarea și autentificarea solicitantului și emiterea unui certificat digital calificat.

DigiSign pune la dispoziția oricărei părți interesate informațiile privind serviciile de încredere pe care le furnizează și care se bazează pe certificate digitale. Deși nu fac subiectul acestui document, DigiSign a publicat și informațiile privind produsele și serviciile adiționale pe care le furnizează, precum certificate SSL, servicii de marcare temporală, dispozitive criptografice securizate și aplicații software pentru crearea și validarea semnăturilor electronice.

DigiSign publică aceste informații într-o manieră inteligibilă, acestea fiind puse la dispoziția publicului în format electronic la adresa www.digisign.ro, precum și în format fizic, ca urmare a unei cereri scrise în acest sens. Toate aceste informații sunt disponibile public ca oricare parte interesată să poată lua o decizie informată înainte de înaintarea unei cereri către DigiSign. Mai mult, DigiSign a pus la dispoziția publicului departamentul HelpDesk, 24 de ore din 24, 7 zile din 7, pentru a oferi suport părților interesate în ceea ce privește serviciile și produsele furnizate de DigiSign.

În plus, la sediul DigiSign, clienții au oportunitatea să beneficieze și de servicii de consultanță, precum și de completarea și transmiterea unor formulare privind satisfacția. Sediul DigiSign are program cu publicul de luni până vineri, între orele 09:00 și 17:00, cu excepția sărbătorilor naționale legale.

4.1. Formular de înregistrare

Înainte de trimiterea cererii de emitere a certificatului digital calificat, solicitantul trebuie să completeze și să trimită către DigSign formularul de înregistrare aferent cererii acestuia. În vederea facilitării procesului de înregistrare a solicitantului și pentru a reduce numărul posibilelor erori de redactare, DigiSign a dezvoltat o interfață WEB care conține formulare standard de înregistrare. Această interfață prezintă solicitantului, într-o modalitate eficientă și inteligentă, diferite tipuri de formulare care au rolul de a colecta informațiile necesare înregistrării. Formularele dispun de câmpuri dinamice și customizate în funcție de preferințele solicitantului, precum tipul de certificat solicitat.

Prin intermediul acestor formulare de înregistrare, solicitantul trebuie să specifice tipul de certificat dorit și datele care vor fi înscrise în structura certificatului. De asemenea, prin completarea formularului de înregistrare, solicitantul autorizează DigiSign în ceea ce privește datele personale ale acestuia, în vederea furnizării de către DigiSign a serviciilor de încredere solicitate și pentru îndeplinirea obligațiilor stipulate în prezentul document.

Formularul de înregistrare va conține cel puțin următoarele:
- Datele care vor fi înscrise în structura certificatului
- Datele personale de identificare ale solicitantului
- Datele personale de identificare ale persoanei autorizate să reprezinte solicitantul (spre exemplu, persoana fizică autorizată de către reprezentantul legal al persoanei juridice pentru a o reprezenta)
- Datele de facturare și livrare

După completarea și trimiterea formularului de înregistrare, solicitantul primește a adresa de e-mail indicată de acesta în formular, o serie de documente care conțin termenii și condițiile de furnizare a serviciului solicitat, precum obligațiile părților, răspunderea acestora, drepturilor lor și alte informații relevante.

DigiSign procesează informațiile colectate prin intermediul formularelor de înregistrare în conformitate cu prevederile legale în ceea ce privește prelucrarea datele personale. În acest sens, DigiSign prelucrează date cu caracter personal ale solicitanților în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea dispozițiilor de drept intern, ale Regulamentului nr. 679/2016 privind protecţia persoanelor fizice în ceea ce

privește prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date și al altor dispoziții de drept al Uniunii referitoare la protecția datelor.

4.2. Cererea de emitere

DigiSign nu ia în considerare datele trimise prin formularele de înregistrare dacă solicitantul nu le confirmă prin trimiterea către Digi Sign a cererii de emitere a certificatului.

Cererea de emitere a unui certificat digital calificat este formată din documentele necesare procesului de emitere, semnate și datate de către solicitant, precum și validarea identității acestuia de către RA, în conformitate cu regulile specificate în acest document. Detalii privind acestea sunt specificate în cadrul cap. 3 al acestui document.

Cererea de emitere a unui certificat digital calificat poate conține și cheia publică. În acest caz, cheia publică trebuie trimisă către DigiSign de așa manieră încât aceasta să poate fi asociată criptografic cu alte date specificate în cerere, în special cu datele de identificare ale solicitantului. O cerere de emitere poate conține și solicitarea aplicantului de a i se genera o pereche de chei criptografice în numele său.

O cerere de emitere a unui certificat digial calificat poate fi înaintată către DigiSign de orice persoană care se conformează regulilor și procedurilor impuse de DigiSign, în cazul în care nu se specifică astfel prin prevederi legale. DigiSign își rezervă dreptul de a refuza cererea de emitere a unui certificat digital calificat persoanelor care nu au capacitate deplină de exercițiu sau care sunt identificate ca lipsindu-le capabilitățile de a citi și/sau scrie.

Cererile de emitere pot fi înaintate de către solicitant operatorilor RA sau, dacă este cazul, operatorilor CA. Atunci când trimite cererea către RA, operatorul verifică cerera și decide dacă aprobă și trimite cererea către CA sau dacă respinge cererea și o trimite înapoi către solicitant pentru a fi remediată, dacă este posibil.

O terță parte poate înainta către DigiSign o cerere de emitere a unui certificat în numele solicitantului, doar în cazul în care acesta înaintează totodată și un document justificativ (spre exemplu o împuternicire) din care să rezulte faptul că terțul este împuternicit de către solicitant pentru a înainta către DigiSign cererea în numele acestuia. Acest document trebuie prezentat în forma impusă de legislația națională aplicabilă, spre exemplu autentificată la un notar public autorizat.

4.3. Procesul de emitere al certificatului

DigiSign accepta solicitări trimise în mod individual și electronic. Formularele de înregistrare se trimit prin mijloace electronice, prin intermediul interfeței WEB, utilizând protocoale securizate (HTTPS), la adresa www.digisign.ro. Orice solicitant care dorește să completeze un formular de înregistrare, accesează www.digisign.ro și completează formularul aferent solicitării acestuia, conform instrucțiunilor. Formularul de înregistrare poate fi completat de către un operator RA la cererea expresă a solicitantului și atât timp cât acest lucru este posibil.

Înainte de a-și începe activitatea, operatorii RA din cadrul DigiSign sunt instruiți corespunzător și devin subiecți ai unor evaluari periodice conduse de DigiSign în vederea asigurării unui nivel ridicat de încredere în procesul operațional.

Cererile de emitere a certificatelor digitale calificate pot fi înaintate către DigiSign fie fizic, fie prin mijloace electronice corespunzătoare, această posibilitate din urmă fiind disponibilă doar în cazul reînnoirii certificatelor digitale care îndeplinesc condițiile specificate în acest document.

Cererile de emitere a certificatelor digitale calificate pot fi înaintate către DigiSign prin una din următoarele modalități:

- personal, de către solicitant, fie la sediul DigiSign, fie la unul din reprezentantii RA din cadrul domeniului DigiSign
- de către un terț autorizat în acest sens, care se conformează regulilor specificate în acest document în ceea ce privește identificarea și autentificarea cererii
- prin intermediul serviciilor de curierat sau poștale, dacă sunt îndeplinite cerințele specificate în acest document în ceea ce privește identificarea și autentificarea cererii

Fiecare cerere de emitere a unui certificat digital calificat este primită și verificată de către RA după cum urmează:

- operatorul RA primește cererea și o înregistrează corespunzător
- operatorul RA verifică datele înscrise în cerere și identifică solicitantul
- operatorul RA verifică posesia cheii private, dacă este cazul
- operatorul RA verifică și alte date care pot să nu fie prezente în cerere, dar care sunt esențiale pentru procesul de emitere al certificatului
- în urma verificărilor efectuate, operatorul RA confirmă identitatea solicitantului și legătura dintre acesta și datele cuprinse în cerere; în cazul unor nonconformități, operatorul RA respinge cererea
- cerera confirmată de către RA este trimisă către CA.

Înainte de emiterea certificatului, CA verifică respectiva cerere ca fiind confirmată (aprobată) de către RA în prealabil.

4.4. Emiterea certificatului

Cererile de emitere sunt examinate de către RA în termen de maxim 5 zile lucrătoare. Această perioadă depinde de acuratețea informațiilor trimise de către solicitant și de cooperarea acestuia privind remediera eventualelor nonconformități. În cazul în care datele lipsă sau incorecte nu sunt remediate în timp util sau dacă anumite documente necesare lipsesc, perioada de timp de 5 zile lucrătoare se extinde în conformitate cu perioada de timp în care se remediază neregularitățile.

Ulterior confirmării cererii de emitere de către RA, CA emite certificatul digital calificat conform următoarei proceduri:

- Solicitarea confirmată de RA este trimisă către serverul CA emitent
- Dacă solicitare conține și cerere de generare a perechii de chei criptografice în numele solicitantului, serverul inițiază procedura prin intermediul dispozitivului aferent
- Se testează calitatea cheii publice generate
- Dacă acțiunile se încheie cu succes, serverul emite și semnează certificatul
- Certificatul este stocat în baza de date
- CA pregătește răspunsul care conține certificatul emis și îl trimite către solicitant
- Dacă acțiunile nu sunt încheiate cu succes, CA respinge solicitarea.

DigiSign își rezervă dreptul de a refuza emiterea unui certificat digital oricărui solicitant, fără a-și asuma răspunderea pentru posibilele daune sau pierderi produse ca urmare a acestui refuz. În acest caz, DigiSign va restitui solicitantului plata certificatului (dacă plata s-a efectuat înainte de emiterea certificatului), cu excepția cazului în care solicitantul a furnizat date false. Refuzul de emitere a unui certificat se poate datora:

- Suspiciunilor sau certitudinilor privind utilizarea de date false de către solicitant

- Utilizarea resurselor DigiSign într-o manieră perturbatoare prin trimiterea unui număr nejustificat și excesiv de cereri și solicitări de interogare a sistemelor DigiSign
- Alte motive întemeiate.

Informațiile privind deciziile luate de către CA (aprobare sau respindere a solicitării de emitere) sunt trimise către utilizator împreună cu motivele care au stat la baza respectivei decizii. Un solicitant poate înainta o nouă cerere către DigiSign în cazul în care a fost refuzat, sub condiția ca motivele refuzului să fi fost rezolvate între timp.

DigiSign notifică solicitantul cu privire la emiterea certificatului digital calificat prin e-mail. Această acțiune presupune trimiterea unei notificări prin e-mail în care este precizat faptul că certificatul a fost emis și, în cazul în care emiterea s-a realizat ca urmare a înaintării unei cereri prin mijloace electronice, cheia publică a certificatului respectiv. Notificarea va conține și informații privind utilizarea corespunzătoare a certificatului emis.

4.5. Acceptarea și publicarea certificatului

La primirea certificatului digital calificat, solicitantul are obligația de a-i verifica conținutul, în special în ceea ce privește corectitudinea datelor și complementaritatea cheii publice cu cea privată. Dacă certificatul prezinte orice fel de nereguli privind aceste aspecte, solicitantul are posibilitatea de a-l refuza, fiind obligat să notifice DigiSign de îndată și să solicite revocarea acestuia.

Certificatul digital calificat emis este considerat acceptat de către solicitant din momentul în care acesta realizează prima operațiune criptografică cu acesta sau, în mod implicit, la trecerea a 5 zile de la primirea acestuia, conform condițiilor generale de prestare a serviciului de încredere solicitat.

În cazul în care certificatul este refuzat, solicitantul are obligația de a trimite către DigiSign dispozitivul criptografic securizat pe care este stocat certificatul, o dată cu cererea de revocare a acestuia.

În cazul în care solicitantul înaintează cerera de emitere a certificatului, personal, la sediul DigiSign, certificatul este considerat acceptat în mod implicit, solicitantul semnând în acest sens un proces verbal de recepție.

Fiecare certificat digital calificat acceptat este publicat de către DigiSign în registrul electronic de evidență al certificatelor emise, la adresa www.digisign.ro. O dată publicat în acest registru, certificatul devine opozabil terților.

4.6. Aplicabilitatea certificatelor și utilizarea cheilor

Titularii certificatelor digitale calificate au obligația de a utiliza certificatele și cheile private după cum urmează:

- în conformitate cu scopul declarat al acestora în prezentul document și în conformitate cu conținutul certificatelor
- în conformitate cu prevederile acordurilor încheiate cu DigiSign
- doar în perioada de valabilitate a certificatelor.

Entitățile Partenere au obligația de a utiliza cheia publică a certificatelor digitale calificate emise de DigiSign după cum urmează:

- în conformitate cu prevederile acestui document și a CP

- doar după verificarea corespunzătoare a certificatelor și a emitentului acestora.

4.7. Reînnoirea certificatelor și recertificarea

DigiSign oferă posibilitatea reînnoirii certificatelor și recertificării. Diferența dintre cele două proceduri constă în faptul că reînnoirea certificatelor poate fi realizată doar în cazul în care certificatul inițial este valid (nerevocat și nesuspendat), iar cererea de reînnoire este înantată către DigiSign cu cel puțin 5 zile înainte de expirarea certificatului, precum și sub condiția ca datele esențiale cuprinse în certificatul inițial nu au suferit modificări.

4.7.1. Recertificarea

Recertificarea se aplica solicitanților care dețin un certificat digital calificat, indeferent de statusul acestora și solicită DigiSign emiterea unui nou certificat.

Procedura se aplică în general atunci când solicitanții dețin un certificat digital calificat expirat, revocat, suspendat sau care are mai puțin de 5 zile până când expiră. Procedura se aplică și în cazul în care solicitantul dorește sau se impune modificarea datelor esențiale înscrise în certificatul inițial, precum și în cazul certificatelor inițiale care au suferit alterări ori diferite defecțiuni ale dispozitivelor în care sunt stocate respectivele certificate.

Procedura de recertificare implică același proces ca în cazul emiterii certificatelor, descris în capitolele anterioare și, spre deosebire de procedura de reînnoire, este permisă modificarea datelor esențiale conținute de certificatul inițial. Procedura de recertificare implică de asemenea și procedura de verificare a identității solicitantului descrisă în cap. 3 al acestui document. Regulile privind formularul de înregistrare și cererea de emitere, precum și procesul de emitere și acceptare a certificatului se aplică și în cazul recertificării.

DigiSign își asumă obligația de a informa titularul certificatului despre apropierea datei de expirare a certificatului, începând cu 45 de zile înainte de această dată.

4.7.2. Reînnoirea certificatului

Reînnoirea certificatului digital calificat reprezintă procesul prin care certificatul inițial este înlocuit cu un nou certificat care conține aceleași date privind titularul acestuia, dar care are o nouă perioadă de valabilitate și un nou serial unic. Aceasta procedura se aplica și în cazul solicitării modificării unui certificat emis, dar doar în ceea ce privește datele care nu sunt consideate a fi esențiale, ci pentru datele opționale precum valoarea câmpului *Funcție*.

Pentru ca unui solicitant să i se oferă posibilitatea de a-și reînnoi certificatul, acesta trebuie să îndeplinească un set de condiții:

- certificatul inițial trebuie să fie valid (nerevocat, nesuspendat) și să aibă minimum 5 zile până la expirare acestuia
- solicitantul să nu își fi modificat datele esențiale de identificare a acestuia
- solicitantul să înainteze cererea de reînnoire a certificatului în conformitate cu instrucțiunile publicate la adresa www.digisign.ro
- certificatul inițial care se dorește a fi reînnoit să fi fost emis de CA DigiSign

În vederea reînnoirii certificatului digital calificat, solicitantul completează și trimite formularul de înregistrare aferent prin intermediul interfaței WEB de la adresa www.digisign.ro. Autentificarea cererii se realizează prin intermediul certificatului digital calificat inițial. În cazul în care solicitantul nu mai are acces la certificatul digital calificat inițial, acesta va urma procedura de recertificare descrisă în capitolul anterior.

Cererile de reînnoirea a certificatelor digitale sunt procesate și confirmate de către RA.

4.8. Revocarea unui certificat

Un certificat digital calificat poate avea statusul de valid, suspendat sau revocat. În timp ce suspendarea unui certificat este temporară și reversibilă, revocarea certificatului implică un proces ireversibil. O dată revocat, certificatul nu poate reveni la starea inițială, însă un certificat suspendat poate deveni valid din nou.

Toate cererile privind revocarea unui certificat digital trebuie înaintate către DigiSign în cel mai scurt timp din momentul în cazul producerii oricărei situații prezentate în cap. 4.8.2.

4.8.1. Cine poate solicita revocarea

Următoarele enități pot solicita revocarea unui certificat digital calificat:

- titularul acestuia
- beneficiarul acestuia, în cazul în care diferă de titular, iar titular întotdeauna este informat în acest sens
- un reprezentant autorizat al CA (spre exemplu, Administratorul de Securitate)
- un mandatar al titularului certificatului, sub condiția prezentării unei împuterniciri în acest sens, încheiată la un notar public autorizat
- RA ca fiind delegată de titular în acest sens
- RA în numele său, sub condiția[2] ca aceasta să dețină informații substanțiale care justifică acțiunea.

RA poate înainta în numele său cereri de revocare către CA sub condiția existenței unor informații substanțiale care să justifice cererea (spre exemplu, RA a luat la cunoștință precum cheia privată a fost compromisă) sau în cazul în care certificatul a fost suspendat pe o perioadă care depășește 30 de zile.

4.8.2. Circumstanțe care impun revocarea

Cererea de revocare se impune în cazul în care:

- Cheia privată a fost pierdută, furată sau compromisă[3]
- Titularul nu mai deține controlul absolut al cheii private datorită faptul că datele de activare ale acestia au fost compromise sau pentru orice alt motiv (spre exemplu, compromiterea codului PIN)
- Datele înscrise în certificat nu reflectă datele înscrise în cererea înaintată de către solicitant, fapt ce reiese din verificarea de către solicitant a certificatului în perioada dedicată acceptării acestuia, în conformitate cu procedurile specificate în CPP
- Datele înscrise în certificat nu mai corespund realității sau au fost modificate în orice fel (spre exemplu, schimbarea numelui titularului ca urmare a căsătoriei)
- Părțile decid terminarea acordurilor încheiate între ele

[2] RA din cadrul domeniului DigiSign acționează cu precauție în ceea ce privește procesarea cererilor de revocare care nu sunt înaintate de către titularul certificatului în cauză, și acceptă doar acele cereri care respectă condițiile și regulile impuse prin acest CPP.
[3] Compromiterea cheii private înseamnă: (1) accesul neautorizat la cheia privată sau motive întemeiate pentru care se consideră că s-a accesat neautorizat cheia privată, (2) pierderea cheii private sau motive întemeiate care să determine luarea în considerare a acestui fapt, (3) furtul cheii private sau suspinciune în acest sens, (4) ștergerea cheii private, accidental sau nu.

- Certificatul a fost suspendat pe o perioadă mai mare de 30 de zile
- În orice alt caz în care se identifică o încălcare a prevederilor CP și CPP, ori a acordurilor încheiate între părți.

Certificatele Autorităților de Certificare din cadrul DigiSign pot fi revocate de către CA emitent, iar o astfel de situație se impune în cazul în care:

- CA are motive să considere că datele înscrise în certificat nu mai corespund realității
- Cheia privată a CA sau sistemul informatic a fost compromis, caz în care toate certificatele emise cu respectivul CA vor fi revocate
- Încetarea activității CA, caz în care toate certificatele emise cu respectivul CA vor fi revocate
- CA nu a respectat prevederile CP și CPP, ori a acordurilor încheiate cu utilizatorii.

4.8.3. Procedura de revocare

DigiSign pune la dispoziția părților interesate procedura privind revocarea unui certificat digital calificat pe care solicitantul trebuie sa o urmeze. Procedura este disponibilă la adresa www.digisign.ro sau poate fi solicitată în scris prin e-mail la helpdesk@digisign.ro. Procedura este de asemenea disponibilă în format fizic la sediul DigiSign.

Procedura de revocare implică înaintarea unui formular care conține date despre solicitant, certificatul care se dorește a fi revocat și motivul.

Formularul se înaintează către DigiSign, semnat olograf sau cu semnătură electronică calificată și se trimite prin:

- E-mail la helpdesk@digisign.ro
- Poștă, curier sau fax către coordonatele de contact ale DigiSign.

Revocarea unui certificat digital calificat este definitivă și ireversibilă. DigiSign se obligă să notifice titularul certificatului și, dacă este cazul, beneficiarul acestuia, în legătură cu decizia de revocare, indiferent de cine a solicitat respectiva revocare.

DigiSign depune toate diligențele de a reduce pe cât posibil perioada de timp în care se procesează cererea de revocare și se publică CRL, fără a depăși termenul de 24 de ore.

Pentru ca o cerere de revocare să fie procesată în cel mai scurt timp, aceasta trebuie trimisă direct către DigiSign, prin e-mail sau fax. Cu toate acestea, deși programul cu publicul al RA este limitat, departamentul HelpDesk este disponibil 24 de ore din 24, 7 zile din 7. Astfel, dacă o cerere de revocare este primită în afara programului cu publicul, departamentul HelpDesk o va prelua însă va urma procedura de suspendare a certificatului, urmând ca la reluarea programului cu publicul, RA să continue cu procedura de revocare a certificatului respectiv.

Astfel, perioada maximă de întârziere între recepționarea cererii de revocare și schimbarea statusului valid al certificatului să se realizeze în cel mai scurt timp, informația despre invalidarea certificatului devenind opozabilă terților în maximum 24 de ore.

4.9. Suspendarea certificatului

În timp ce revocarea unui certificat este definitivă și ireversibilă, suspendarea acestuia presupune un proces temporar și reversibil. Toate cererile privind suspendarea unui certificat digital trebuie înaintate către DigiSign în cel mai scurt timp din momentul în cazul producerii oricărei situații prezentate în cap. 4.9.2. al acestui CPP.

4.9.1. Cine poate solicita suspendarea

Entitățile care pot solicita suspendarea unui certificat corespund cu entitățile cărora le este permisă solicitarea revocării unui certificat, în conformitate cu cap. 4.8.1. al acestui CPP.

4.9.2. Circumstanțe care impun suspendarea

Suspendarea se impune în următoarele cazuri:

- La cererea titularului certificatului digital, după o prealabilă verificare a identității acestuia;
- În cazul în care o hotărâre judecătorească dispune acest lucru;
- În cazul în care informațiile cuprinse în certificatul digital nu mai corespund realității;
- În situațiile în care există suspiciuni întemeiate cu privire la faptul că respectivul certificat digital a fost emis prin încălcarea dispozițiilor prezentului CPP;
- În cazul în care titularul certificatului sau beneficiarul acestuia nu achită sau întârzie să achite contravaloarea serviciilor de încredere prestate.

4.9.3. Procedura de suspendare

Procedura de suspendare a certificatului digital calificat coincide cu procedura de revocare. După verificarea cu succes a cererii, CA schimbă statusul certificatului din valid în suspendat.

DigiSign se obligă să notifice titularul certificatului și, dacă este cazul, beneficiarul acestuia, în legătură cu decizia de suspendare, indiferent de cine a solicitat aceasta.

Un certificat digital calificat nu poate avea statusul de suspendat pentru o perioada mai mare de 30 de zile. Dacă au fost depășit acest termen, certificatul se impune a fi revocat. DigiSign va notifica titularul certificatului și, dacă este cazul, beneficiarul acestuia, despre revocarea certificatului.

4.9.4. Procedura de reactivare a certificatului

În cazul în care situațiile care au condus la suspendarea certificatului au încetat, CA poate dispune reactivarea certificatului digital calificat și renunțarea la statusul de suspendat al acestuia. Entiățile care pot solicita reactivarea certificatului coincid cu cele care pot solicita suspendarea acestuia.

După reactivarea certificatului cu succes, acesta este eliminat din CRL, însă perioada în care acesta a fost suspendat rămâne înregistrată în baza de date DigiSign.

4.10. Verificarea unui certificat

Urmare a revocării, suspendării sau reactivării unui certificat, statusul acestuia este modificat și înregistrat în baza de date DigiSign. Fiecare schimbare în statusul unui certificat poate fi urmărită prin: (1) Listele Certificatelor Revocate (CRL), în conformitate cu frecvența de publicare a acestora, (2) serviciile de validare în timp real a certificatelor digitale calificate emise prin OCSP și (3) prin registrul electronic de evidență al certificatelor emise de CA DigSign.

4.10.1. Verificarea prin CRL

Fiecare Autoritate de Certificare din cadrul domeniului DigiSign emite Liste de Certificate Revocate. CRL emise de către CA intermediare sunt publicate o dată la 24 de ore, perioada de valabilitate a acestora fiind de 48 de ore, iar sursa de timp este sincronizată cu UTC. CRL emise de CA rădăcină sunt publicate anual, sub condiția ca nici un certificat emis imediat sub acea rădăcină să nu fie revocat între timp. În ceea ce privește revocarea certificatului unei CA rădăcină, CRL este publicat imediat.

Profilele CRL sunt descrise în detaliu în cadrul cap. 7.2. ale acestui CPP.

Orice entitate parteneră, ca urmare a recepționării unui document semnat electronic, are obligația să verifice cheia publică a certificatului care corespunde cu cheia privată a titularului certificatului cu care a fost creată respectiva semnătură electronică. Entitatea Partneră trebuie să se asigure că respectivul certificat nu era introdus în CRL la momentul semnării. Entitățile Partenere sunt obligate să utilizeze ultima versiune în vigoare a CRL.

Verificarea prin CRL poate fi acceptată ca singura modalitate de verificare a unui certificat doar în cazul în care perioadele de publicare a CRL practicate de DigiSign nu au impact din punct de vedere al pierderilor pe care le-ar putea suferi Entitatea Parteneră care poartă responsabilitatea verificării. Altfel, entitatea parteneră este obligată să utilizeze serviciul de validare în timp real al certificatelor prin intermediul protocolului OCSP.

În cazul în care entitatea parteneră identifică în CRL certificatul pe care îl verifică, aceasta are obligația de a-l respinge, în special dacă motivul revocării este:

a. *unspecified* – necunoscut
b. *keyCompromise* – compromiterea cheii private
c. *cACompriomise* – compromiterea securității CA
d. *cessationOFOperation* – terminarea activității CA
e. *certificateHold* – suspendarea certificatului

Dacă un certificat care urmează să fie verificat este inclus in Lista de Certificate Revocate, entitatea parteneră se angajează să respingă documentul asociat acestui certificat dacă motivul revocării este unul dintre următoarele:

a. *unspecified* – necunoscut
b. *keyCompromise* – compromiterea securitatii cheii private
c. *cACompriomise* – compromiterea securitatii Autoritatii Contractante
d. *cessationOFOperation* – terminarea activitatii Autoritatii Contactante
e. *certificateHold* – suspendarea certificatului
f. *affiliationChanged* – modificarea datelor
g. *superseded* – modificarea cheilor

Decizia finală privind credibilitatea unui certificat cade în responsabilitatea entităților partenere. În luarea acestei decizii, entitățile partenere au obligația de a lua în considerare faptul că motivele de revocare specificate în paragraful anterior, lit. f și g, nu reprezintă compromiterea cheii private a certificatului suspus verificării.

4.10.2. Verificarea prin OCSP

DigiSign pune la dispoziția părților interesate serviciul de verificare a certificatelor în timp real. Acest serviciu se bazează pe protocolul OCSP descris în RFC 6960. Utilizând serviciul de validare prin OCSP sunt obținute date precise privind statusul certificatul (comparând cu verificarea prin CRL).

Acest serviciu funcționează în baza unui model interogare-răspuns. Ca răspuns la o interogare, serverul OCSP furnizează un răspuns care poate conține următoarele informații privind statusul certificatelor:

- *good* – reprezintă un răspuns pozitiv la interogare și se interpretează ca o confirmare a validității respectivului certificat
- *revoked* – reprezintă un răspuns negativ și se interpretează ca o confirmare a faptului că respectivul certificat este revocat
- *unknown* – reprezintă un răspuns neutru și se interpretează ca o confirmare a faptului că DigiSign nu deține nici un fel de informație despre respectivul certificat.

Serviciul de validare prin OCSP este disponibil exclusiv online, pentru orice parte interesată în verificarea în timp real a unui certificat digital califcat emis de DigiSign CA. Statusul certificatelor este furnizat prin acest serviciu în timp real (în momentul interogării) si este bazat pe informațiile înscrise la momentul respectiv în baza de date DigiSign.

4.10.3. Registrul electronic de evindeță

Toate certificatele digitale calificate emise de DigiSign CA și acceptate de către titularii acestora, sunt publicate în registrul electronic de evidență al certificatelor emise de DigiSign CA. Dacă statusul acestora certificate se schimbă după publicarea acestora, informațiile din registru se modifica în conformitate.

5. Gestionarea și controalele operaționale

În ceea ce privește managementul securității, DigiSign se orientează după standardele generale recunoscute în domeniu (ex: ISO 27001) și alte standarde impuse de reglementări și de lege.

Managementul DigiSign a stabilit o politică de securitate care formează baza pentru coerența și completitudinea securității informațiilor și a suportului de management. Documentele de politică si gestionare a securității DigiSign includ controalele de securitate și procedurile de operare pentru facilitățile, sistemele și informațiile din domeniul DigiSign care oferă servicii de încredere. DigiSign efectuează și revizuiește periodic evaluarea riscurilor pentru a evalua riscul afacerii și pentru a determina cerințele de securitate necesare și procedurile operaționale.

Managerul general al DigiSign aprobă politicile și practicile legate de securitatea informațiilor pentru toate serviciile DigiSign. Managementul DigiSign comunică politicile și procedurile de securitate a informațiilor angajaților și părților externe relevante care sunt afectate de aceasta. În plus, managementul DigiSign stabilește abordarea DigiSign pentru a gestiona obiectivele de securitate a informațiilor pentru serviciile de încredere, inclusiv procedurile auditate pentru controlul intern.

DigiSign a obținut cu succes certificarea ISO 27001: 2013.

În continuare, acest capitol descrie cerințele generale privind proprietățile fizice, controalele de securitate organizatorică și de personal. Din motive de siguranță, DigiSign nu va descrie măsurile specifice luate în controalele de securitate. Documentele care descriu punerea în aplicare a controalelor de securitate în cadrul DigiSign sunt considerate confidențiale.

5.1. Controale de securitate fizică

Controalele de securitate fizică implementate de DigiSign sunt concepute pentru a proteja DigiSign PKI atât software (partea logică) cât și hardware (partea fizică) împotriva utilizării neautorizate. Sistemele informatice, terminalele operatorilor și resursele informatice din cadrul DigiSign sunt dispuse într-o zonă dedicată, protejate fizic împotriva accesului neautorizat, distrugerii sau întreruperii activității. Aceste zone sunt monitorizate permanent și fiecare intrare și ieșire este înregistrată într-un jurnal de evenimente. În plus, stabilitatea alimentării cu energie electrică și a temperaturii sunt monitorizate și controlate în permanență.

5.1.1. Locația

Sediul DigiSign este situat în str. Virgil Madgearu 2 - 6, 014135, Sector 1, București, România.

Sediul DigiSign și Autoritatea de certificare sunt disponibile public în fiecare zi lucrătoare între orele 9:00 și 17:00. În restul timpului, inclusiv zilele nelucrătoare și sărbătorile legale, accesul este permis numai persoanelor autorizate de managementul DigiSign.

5.1.2. Acces fizic

Serviciile de încredere furnizate de DigiSign se bazează pe premise securizate în ceea ce privește găzduirea autorităților DigiSign. DigiSign folosește spații separat fizic în camera de servere, special concepute pentru operarea data center-ului. Echipamentele Autorității de Certificare DigiSign sunt protejate permanent împotriva accesului neautorizat. Dispozitivele DigiSign RA de acces fizic sunt, de asemenea, implementate pentru a minimiza orice risc. Aceste mecanisme de securitate sunt adecvate nivelului de amenințare în spațiul în care sunt instalate echipamentele RA.

Sistemele DigiSign sunt protejate de cinci niveluri de securitate fizică după cum urmează:

a. Accesul la nivelul 1 - necesită un document de identificare (carte de identitate, pașaport etc.) care este prezentat gardianului la recepție. Accesul la acest nivel este automat monitorizat (sistemul video) și înregistrat manual (printr-o carte de registru în care paznicul scrie date despre fiecare persoană care vine și iese din clădire).
b. Accesul la nivelul 2 - necesită un card de proximitate care atunci când este utilizată, este monitorizată și înregistrat automat.
c. Accesul la nivelul 3 - necesită control individual al accesului pentru toate persoanele care intră în zona RA și CA prin utilizarea sistemului de amprente biometrice. Acest nivel de acces este monitorizat automat.
d. Accesul la nivelul 4 - se referă la accesul în interiorul cuștii din data center. Accesul fizic este interzis la acest nivel pentru toți vizitatorii și angajații cu un nivel scăzut de acces. Acest nivel de acces este monitorizat automat.
e. Accesul la nivelul 5 - se referă la accesul biometric la rack-uri care sunt situate în interiorul cuștii și necesită un control individual al accesului. Sala de ceremonii a cheilor necesită control dublu, fiecare folosind doi factori de autentificare: sistemul de amprente biometrice și cardul de proximitate. Acest nivel de acces este monitorizat automat.

5.1.3. Puterea și aerul conditionat

Sediul DigiSign este echipat cu sisteme de încălzire, ventilație și climatizare pentru a controla temperatura și umiditatea relativă, pentru a oferi un mediu de operare adecvat. De asemenea, există sisteme de alimentare pentru a asigura accesul neîntrerupt la energia electrică. Dacă apare o întrerupere a alimentării cu energie electrică, sursa de alimentare

de urgență (UPS) asigură continuitatea activității până la intervenția automată a generatorului de rezervă a energiei din clădire.

5.1.4. Expunerea la apa

DigiSign a luat măsuri de precauție pentru a minimiza impactul expunerii la apă asupra sistemelor informatice. Riscul de inundații în zona serverului este minim datorită poziției sale: distanța de aproximativ 1 metru deasupra solului.

5.1.5. Prevenirea incendiilor

DigiSign a luat măsuri de precauție pentru a preveni și stinge incendiile sau alte daune din cauza expunerii la flacără sau fum. Sediul DigiSign beneficiază de un sistem de prevenire și stingere a incendiilor în conformitate cu standardele și reglementările corespunzătoare din acest domeniu.

5.1.6. Stocarea media

În funcție de sensibilitatea informațiilor, materialele care conțin arhive și datele de rezervă actuale sunt stocate într-o zonă foarte securizată. Accesul în acest domeniu este permis numai persoanelor autorizate. Toate zonele de depozitare sunt protejate împotriva expunerii la incendii și a apei și a pagubelor.

5.1.5. Eliminarea deșeurilor

Eliminarea deșeurilor este pusă în aplicare în mod sigur pentru a împiedica divulgarea neautorizată a datelor sensibile. Hârtia și suporturile electronice care conțin informații importante pentru securitatea DigiSign sunt distruse după expirarea perioadei de păstrare. Modulele de securitate hardware sunt resetate și șterse în conformitate cu recomandările producătorului. De asemenea, aceste dispozitive sunt resetate și șterse atunci când sunt trimise la service sau reparate.

5.1.6. Sediu de rezervă

Mijloacele de rezervă sunt stocate în siguranță într-o locație separată de locația originală și sunt protejate împotriva expunerii la foc și la apă. DigiSign a implementat măsuri pentru a asigura recuperarea completă a serviciilor sale în caz de dezastru, server corupt, software sau date, în termen de 48 de ore. Locațiile de recuperare în caz de dezastre și de dezastre sunt situate în spații izolate suficient de îndepărtate de locația primară și beneficiază de măsuri de securitate echivalente.

5.2. Controale procedurale

Controalele de securitate operaționale implementate de DigiSign pentru activitățile CA și TSA asigură că sistemele CA / TSA sunt sigure și funcționează corect, cu un risc minim de eșec.

Acest capitol descrie o listă de roluri care pot fi definite pentru personalul angajat în DigiSign, precum și responsabilitățile și sarcinile asociate fiecărui rol definit.

5.2.1. Roluri de încredere

DigiSign se asigură că personalul a obținut statutul de încredere și că aprobarea departamentului este acordată înainte ca personalului respectiv să li se încredințeze

dispozitive de acces și credentiale electronice pentru a accesa și a efectua anumite funcții pe sistemele DigiSign.

Următoarele roluri de încredere vor fi administrate cu unul sau mai multe persoane si vor fi aplicate în cadrul DigiSign:

a. Administratori de securitate: sunt responsabili pentru instalarea, configurarea și întreținerea sistemelor de împingere pentru gestionarea serviciilor.
b. Administratori sistem de certificare: sunt responsabili pentru administrarea configurarea, monitorizarea, mentenanța sistemului de certificare.
c. Ofițerii sediului: sunt implicați în operațiunile de zi cu zi, în special în ceea ce privește clădirile și spațiile, cum ar fi: întreținerea clădirilor și terenurilor, sănătatea și siguranța, securitatea fizică și gestionarea spațiului.
d. Auditori interni securitatea informatiei: sunt responsabili de efectuarea unei revizuiri periodice a aderării DigiSign la toate legile, reglementările și standardele aplicabile.
e. Operatori suspendare și revocare: gestionează solicitările de suspendare și revocare ale certificatelor.
f. Operatorii RA: în numele RA, sunt responsabili pentru îndeplinirea sarcinilor prezentate în conformitate cu procedurile DigiSign specificate pentru identificarea și înregistrarea abonaților.

În cadrul DigiSign, rolul auditorului nu poate fi combinat cu niciun alt rol. Nici o entitate care nu are alt rol decât un auditor poate lua responsabilitățile auditorului.

5.2.2. Numărul de persoane necesare pentru a efectua o sarcină delicată

DigiSign menține și aplică proceduri riguroase de control pentru a asigura separarea sarcinilor bazate pe responsabilitățile de serviciu, precum și pentru a asigura că mai multe persoane de încredere trebuie să îndeplinească sarcini delicate.

Următoarele activități necesită minimum două tipuri diferite de persoane de încredere: generarea de chei, backup-ul cheie, restaurarea cheie, gestionarea sistemelor de bază HSM și CA, vizite fizice la data center.

Procesul de generare a cheilor (pentru certificare și semnarea CRL) este una dintre principalele operațiuni care necesită o atenție deosebită. Această activitate necesită prezența a cel puțin două persoane de încredere sau, de asemenea, poate fi observată și de către deținătorii de secrete comune care își păstrează partea lor a cheii într-o locație sigură.

5.2.3. Identificarea și autentificarea pentru fiecare rol

DigiSign a implementat un sistem de control al accesului, care identifică și înregistrează toți utilizatorii într-o manieră demnă de încredere.

Personalul DigiSign este supus procedurilor de identificare și autentificare, după cum urmează:

a. Plasarea pe lista persoanelor autorizate să acceseze facilitățile DigiSign
b. Plasarea pe lista de persoane autorizate să acceseze fizic resursele de sistem și de rețea ale DigiSign
c. Emiterea unei confirmări care să autorizeze îndeplinirea rolului atribuit
d. Atribuirea acreditărilor (cont și parolă) în sistemul informatic al DigiSign

Fiecare cont alocat trebuie să fie unic și atribuit direct unei anumite persoane, nu poate fi împărțit cu nicio altă persoană și trebuie restricționat în funcție de funcția care decurge din rolul unei anumite persoane în sistemul software al DigiSign.

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

5.3. Controlul personalului

Controalele de securitate ale personalului sunt documentate în politici care nu sunt publice și includ subiectele vizate de următoarele subsecțiuni.

5.3.1. Calificări, experiență și cerințe de verificare

DigiSign se asigură că persoanele care își îndeplinesc responsabilitățile au:

a. Au absolvit cel puțin școala secundară
b. Au semnat un acord care descrie rolul său în sistem și responsabilitățile corespunzătoare
c. Au făcut obiectul unei pregătiri avansate privind gama de obligații și sarcini asociate poziției sale
d. Au fost instruit în domeniul protecției datelor cu caracter personal și a protecției confidențiale și a informațiilor private
e. Au semnat un acord care conține o clauză privind protecția sensibilă a informațiilor, confidențialitatea și confidențialitatea datelor subiectului
f. Au fost informati că nu îndeplinește sarcini care ar putea conduce la un conflict de interese între un CA sau un RA care acționează în numele acestuia.

Personalul din conducere dispune de expertiză și formare în domeniul tehnologiei semnaturii electronice și familiarizați cu procedurile de securitate pentru personalul cu responsabilități în domeniul securității și cu experiența în domeniul securității informațiilor și al evaluării riscurilor, suficient pentru a îndeplini funcțiile de management.

DigiSign se asigură că toți membrii personalului implicat în furnizarea de servicii de încredere sunt verificați în ceea ce privește calificările, cunoștințele de specialitate, experiența și clearance-ul necesar și adecvate pentru a ocupa roluri de încredere și pentru a îndeplini funcția specifică a postului respectiv. Astfel de verificări sunt direcționate în mod specific spre lipsa de prezentare de către candidat, adecvarea referințelor validate și orice eliminare considerată adecvată.

5.3.2. Proceduri de verificare a situației

DigiSign realizează sau asigură efectuarea verificărilor relevante pentru personalul potențial prin intermediul rapoartelor de stare emise de autoritatea competentă, declarații ale terților sau declarații propri.

5.3.4. Cerințe de instruire și frecvență de recalificare

Angajații companiei DigiSign au fost instruiți și au toată experiența necesară pentru îndeplinirea atribuțiilor specificate în contractul de muncă și în fișa postului, înainte de a îndeplini orice funcții operaționale sau de securitate.

Personalul care îndeplinește rolurile și sarcinile care decurg din angajarea în DigiSign sau autoritățile locale și regionale trebuie să completeze formarea în ceea ce privește:

a. Reglementările privind Certificate Practice Statements și Certificate Policies
b. Procedurile și controalele de securitate utilizate de CA și RA
c. Software-ul de sistem al CA și RA
d. Responsabilitățile care decurg din rolurile și sarcinile efectuate în sistem
e. Procedurile executate în urma unei defecțiuni sau a unei corupții la un CA / RA

La finalizarea instruirii, toți participanții vor semna un document care să confirme familiarizarea lor cu CPS și CP, precum și acceptarea restricțiilor și obligațiilor asociate.

DigiSign asigură că întreg personalul care îndeplinește îndatoriri de conducere, a primit o instruire cuprinzătoare de conștientizare cu privire la principiile și regulile de securitate din cadrul DigiSign, reglementările și procesele interne, precum și sarcinile pe care trebuie să le îndeplinească.

După finalizarea instruirii inițiale, se efectuează periodic (cel puțin anual) actualizări de instruire pentru toate categoriile de membri ai personalului personalului DigiSign pentru a stabili continuitatea și actualizările în cunoștințele personalului și în proceduri.

5.3.3. Succesiunea și frecvența de rotație a lucrării

Nu se aplică.

5.3.4. Acțiuni și sancțiuni neautorizate

În cazul unei descoperiri sau al unei suspiciuni de acces neautorizat, managementul DigiSign poate suspenda accesul autorului la sistemele DigiSign, dacă făptuitorul este un angajat al DigiSign. Acțiunile disciplinare pentru astfel de accidente vor fi descrise în regulamente adecvate și trebuie să respecte legea aplicabilă.

5.3.5. Cerințele contractorului independent

Persoanele contractante independente (serviciul extern, dezvoltatorii de subsisteme sau aplicații etc.) sunt supuși aceleiași proceduri de verificare ca și angajații DigiSign. În plus, personalul contractual, atunci când își îndeplinește sarcinile la facilitatea DigiSign, trebuie să fie escortat de angajații DigiSign, cu excepția celor care au aprobarea anterioară din partea administratorului de securitate.

5.3.6. Documentația furnizată personalului

DigiSign realizează documentația relevantă sau asigură faptul că documentația relevantă este furnizată membrilor personalului personalului DigiSign, pentru ca aceștia să-și poată îndeplini funcțiile specifice. Distribuirea documentelor va avea loc în timpul formării inițiale, recalificării și ori de câte ori este cazul.

DigiSign oferă personalului său acces la următoarele documente:

a. Certificate Practice Statements si Certificate Policies
b. Gama de responsabilități și obligații asociate cu rolul jucat în sistem
c. Ghiduri și instrucțiuni pentru a-și îndeplini cu succes sarcinile.

5.4. Proceduri de înregistrare conform auditului

5.4.1. Tipuri de evenimente înregistrare

Tipul de date înregistrate de DigiSign include, dar nu se limitează la:

- toate evenimentele legate de înregistrare, inclusiv solicitările de certificat, recheierea sau reînnoirea, menținerea confidențialității informațiilor despre subiect, cum ar fi:
  - documentele prezentate de solicitant pentru a susține înregistrarea
  - înregistrarea documentelor unice de identificare
  - locația de stocare a copiilor aplicațiilor și a documentelor de identificare (de exemplu, acordul de abonament semnat)
  - orice opțiuni specifice din acordul abonatului (de exemplu, consimțământul pentru publicarea certificatului)
  - identitatea entității care acceptă cererea
  - metoda utilizată pentru validarea documentelor de identificare, dacă este cazul
  - numele Autorității de Înregistrare, dacă este cazul.
- toate evenimentele privind ciclul de viață al cheilor CA și certificate emise
- toate evenimentele legate de ciclul de viață al cheilor gestionate de un CA în domeniul DigiSign, inclusiv toate cheile de subiect generate de un CA
- toate cererile și rapoartele privind revocarea, precum și acțiunea care rezultă.

Se înregistrează și evenimente de securitate cum ar fi modificările profilului de securitate, pornirea și oprirea sistemului, erori de sistem și defecțiuni hardware, activitățile firewall și router și încercările de acces la sistemul PKI.

5.4.2. Frecvența de procesare a înregistrărilor

Traseul de audit este auditat când apare un eveniment anormal (ori de câte ori este necesar).

5.4.3. Perioada de păstrare a logurilor de audit

Jurnalele sunt păstrate până la expirarea ultimului certificat emis de un CA în domeniul DigiSign.

5.4.4. Protecția logurilor de audit

Jurnalele pot fi accesate numai de către persoanele autorizate de DigiSign Management. Fiecare modificare a logurilor se face numai cu autorizație.

5.4.5. Proceduri de copiere a logurilor de audit

Jurnalele de audit sunt copiate periodic pe site-ul DR.

5.4.6. Evaluări de vulnerabilitate

Pentru a asigura siguranța activelor DigiSign în tehnologia informației, echipa de securitate informației si risc evaluează periodic poziția de securitate, efectuând evaluări regulate ale vulnerabilității cel puțin de două ori pe an și testarea penetrării cel puțin o dată pe an. Cu rezultatele acestor activități, DIGISIGN poate aplica soluții de securitate sau alte controale compensatorii pentru a îmbunătăți securitatea mediului.

Tehnicile utilizate în timpul evaluărilor de securitate urmăresc să acopere o serie de metodologii și tehnici de atac cât mai largi pentru a identifica toate riscurile cibernetice plauzibile. În acest scop sunt utilizate instrumente automate de scanare, precum și tehnici manuale.

5.5. Arhivarea logurilor

Logurile referitoare la ciclul de viață al certificatului sunt păstrate ca evidențe de arhivă pentru o perioadă de cel puțin 10 (zece) ani, în special pentru certificatele calificate.

Indiferent de mediile de stocare, arhivele sunt protejate în integritate și sunt accesibile numai de personal autorizat. Mass-media care deține datele de arhivă și aplicațiile necesare procesării datelor de arhivă sunt menținute pentru a se asigura că datele de arhivă pot fi accesate pentru perioada de timp necesară.

Înregistrările privind funcționarea serviciilor sunt puse la dispoziția autorităților judiciare și / sau a persoanelor ale căror drepturi de acces la acestea rezultă din lege.

5.6. Compromitere si Disaster Recovery

În cazul unui dezastru, inclusiv compromiterea cheii de semnătură privată sau acreditările serviciului de încredere și eșecul componentelor critice ale sistemelor demne de încredere ale DigiSign, operațiile vor fi restabilite cât mai curând posibil. În acest sens, DigiSign a definit și menține un plan de continuitate a afacerii pentru a acționa în caz de dezastru.

Planul de continuitate a afacerii DigiSign include soluții pentru backup și recuperare de date de sistem, compromitere cheie CA, stare de revocare și compromitere alghoritm.

5.6.1. Incidente și proceduri de manipulare a compromisurilor

DigiSign a implementat un plan de continuitate a afacerii, care acoperă procedurile de evaluare a riscurilor, tratarea incidentelor (incluzând un răspuns la incidente și dezastre), exerciții de recuperare și recuperare.

DigiSign efectuează o evaluare anuală a riscurilor pentru serviciile DigiSign Trust Services pentru a preveni posibilele pericole pentru disponibilitatea operațiunilor DigiSign și pentru a minimiza riscul pierderii controlului asupra serviciilor Trust. Lista situațiilor considerate ca situații de urgență este determinată de evaluarea riscurilor. Rezultatul evaluării riscurilor include cerințele privind planurile de recuperare și scenariile de testare a recuperării.

Planurile de recuperare și scenariile de testare includ cel puțin următoarele amenințări:

- pentru DigiSign CA și DigiSign TSA, cheia privată utilizată pentru furnizarea serviciului este compromisă sau există o suspiciune gravă a acestuia;
- pentru DigiSign TSA, pierderea sincronizării unui ceas de service cu time-stamping.

Procedurile de tratare a incidentelor de securitate a informațiilor, a situațiilor de urgență și a vulnerabilităților critice sunt documentate în procedura internă de raportare și gestionare a incidentelor DigiSign. Obiectivul acestui regulament este reacția imediată și recuperarea disponibilității și protecția continuă a serviciilor DigiSign.

În caz de urgență, DigiSign va informa imediat toți abonații și părțile implicate (sau cel puțin în termen de 24 de ore de la decizia comisiei de criză) despre situația de urgență și soluția propusă prin intermediul canalelor de comunicare a informațiilor publice.

DigiSign va informa fără întârziere, dar în orice caz în termen de 24 de ore de la conștientizarea acesteia, Organismul de Supraveghere din România (Ministerul Comunicațiilor și Societății Informaționale) și, dacă este cazul, alte organisme relevante ca CERT sau Autoritatea Națională pentru Protecția Datelor din Orice încălcare a securității sau pierderea integrității care are un impact semnificativ asupra Serviciului de încredere furnizat sau asupra datelor personale menținute în acesta.

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

Evenimentul de corupție a resurselor informatice, a software-ului și a datelor este gestionat conform politicii interne de gestionare a incidentelor de securitate a DigiSign.

5.6.3. Compromitere cheie privată CA

Compromiterea unei chei a CA va duce la revocarea imediată a tuturor certificatelor emise. Într-un astfel de caz, diferiților participanți li se va notifica faptul că CRL-ul nu poate fi neapărat deplin de încredere.

5.6.3. Compromiterea algoritmului

În cazul algoritmilor sau al parametrilor asociați utilizați de DigiSign sau de abonații săi, devin insuficienți pentru utilizarea dorită a acestora, DigiSign va informa toți abonații și părțile implicate ale algoritmului compromis și va programa revocarea oricărui certificat afectat după anunț.

5.7. Terminara CA si RA

Furnizarea serviciilor de încredere se încheie:

a. Cu o decizie a Comitetului executiv al DigiSign
b. Cu o decizie justificată a autorității care exercită supravegherea: Organismul de Supraveghere al României - Ministerul Comunicațiilor și Societății Informaționale
c. Cu o hotărâre judecătorească definitivă și irevocabilă
d. La lichidarea sau încetarea operațiunilor DigiSign.

Inainte ca DigiSign sa inceteze furnizarea unui serviciu de incredere, se vor executa urmatoarele proceduri:

- DigiSign informează despre terminare: toți abonații și părțile implicate, precum și toate entitățile cu care DigiSign are acorduri sau alte forme de relații stabilite
- DigiSign face cel mai bun efort pentru a face aranjamente cu alți furnizori de servicii de încredere pentru a transfera furnizarea de servicii clienților săi existenți
- DigiSign distruge cheile private CA și TSA, inclusiv copiile de rezervă sau cheile retrase din utilizarea în așa fel încât cheile private să nu poată fi retrimise
- DigiSign reinitializează și / sau distruge toate echipamentele hardware legate de serviciile care se termină, în funcție de reglementările de securitate în vigoare
- DigiSign încetează orice autorizație a tuturor subcontractanților de a acționa în numele DigiSign în îndeplinirea oricăror funcții legate de procesul de emitere a serviciilor de încredere.

Notificarea privind încetarea CA a DigiSign va fi publicată în mass-media publică.

DigiSign nu își asumă răspunderea pentru nici o pierdere sau daună ca rezultat al terminării CA, cu condiția ca DigiSign să fi anunțat publicul de reziliere prin intermediul canalelor de comunicații publice cu cel puțin o lună în avans.

DigiSign are un aranjament cu un asigurător care acoperă costurile pentru a îndeplini cerințele minime de mai sus, în cazul în care DigiSign intră în faliment sau din alte motive nu este în măsură să acopere costurile de la sine.

Aceste cerințe se aplică și în cazul rezilierii autorităților de înregistrare delegate.

6. Controale tehnice de securitate

Acest capitol descrie procedurile utilizate pentru generarea și gestionarea perechii de chei criptografice a unei CA și a unui abonat, precum și a cerințelor tehnice asociate.

6.1. Generarea și instalarea perechii de chei

DigiSign utilizează chei criptografice generate și instalate într-o manieră de siguranță și urmează cele mai bune practici din industrie pentru gestionarea ciclului de viață cheie, lungimea cheii și algoritmi.

Toate cheile trebuie generate folosind o metodă aprobată de FIPS sau un standard internațional echivalent (de ex. CC EAL).

6.1.1. Generarea perechii de chei

Generarea de perechi de chei este un proces critic dat fiind faptul că modul în care este generată perechea de chei este esențială pentru siguranța întregului sistem PKI.

a. Cheile Root CA

Perele cheie DigiSign Root CA sunt create în conformitate cu procedurile interne pentru crearea acestui tip de chei. Perechile de chei DigiSign Root CA sunt generate de mai multe persoane de încredere, care acționează în roluri de încredere și utilizează un dispozitiv hardware criptografic securizat (HSM), certificat FIPS 140-2 Level 3, ca parte a unei ceremonii de generare a cheilor scripturilor. Activarea HSM necesită utilizarea unui token de autentificare cu două factori. HSM protejează cheile de compromisuri externe și operează într-un mediu sigur din punct de vedere fizic.

DigiSign urmează o procedură documentată (ceremonie cheie) pentru efectuarea generării de perechi de chei de bază pentru toate părțile sale principale. DigiSign produce un raport care demonstrează că ceremonia a fost efectuată în conformitate cu procedura stabilită și că integritatea și confidențialitatea perechii de chei au fost asigurate. Procedura și raportul nu sunt disponibile publicului.

Fiecare CA Root DigiSign deține un certificat auto-semnat. Cheia privată care corespunde cheii publice conținută în certificatul auto-semnat este utilizată exclusiv pentru a semna cheile publice ale CA-urilor intermediare prin semnarea certificatelor operaționale și a CRL-ului necesare funcționării autorităților. Un scop similar este destinat cheilor private deținute de fiecare CA intermediare, care corespund cheilor publice incluse în certificatele emise de autoritățile centrale pentru fiecare autoritate.

După generarea perechii de chei pentru semnarea certificatului și CRL, distribuția cheilor private și a acestuia activarea în modul de securitate hardware, tastele pot fi utilizate în operațiuni criptografice până când perioada de valabilitate a expirat sau au fost dezvăluite cheile.

Codurile criptografice DigiSign ROOT CA au o durată de viață limitată; dacă perioada a expirat, cheile trebuie să fie actualizate.

b. Cheile Intermediar CA

Cheile CA-urilor intermediare sunt generate în cadrul facilității DigiSign, în prezența unui grup de persoane de încredere. Perechile cheie sunt generate pe stații de lucru desemnate, autentificate care sunt conectate la un certificat HSMS, FIPS 140-2 Level 3. Perechile de chei sunt reținute permanent pe HSM.

Acțiunile executate în timpul generării perechii de chei sunt înregistrate, datate de un semnat de fiecare persoană prezentă în timpul generării. Înregistrările sunt păstrate pentru necesitățile auditurilor și revizuirilor comune ale sistemului.

c. Cheile (utilizatorilor finali) abonaților

Pentru certificatele electronice calificate emise pe QSCD, perechea de chei trebuie întotdeauna generată și stocată în QSCD.

Abonatul are opțiunea de a genera propria pereche de chei. În acest caz, perechea de chei trebuie să fie verificată de DigiSign pentru a se asigura că a fost generată și stocată într-un dispozitiv criptografic securizat (QSCD), care respectă sau depășește standardele de certificare FIPS 140-2 Level 2. Atunci când generarea cheilor este efectuată de către subiect, procesul de solicitare a certificatului asigură faptul că subiectul deține cheia privată asociată cu cheia publică prezentată pentru certificare și că procedura de eliberare a certificatului este corelată în mod sigur cu înregistrarea sau reînnoirea certificatului asociat.

De asemenea, Abonatul poate încredința DigiSign să genereze și să stocheze perechea de chei utilizând aplicații adecvate și dispozitive criptografice securizate (QSCD), certificate FIPS 140-2 Level 2. În acest caz, DigiSign trebuie să trimită în siguranță dispozitivul subiectului.

DigiSign garantează că, în orice moment după generarea unei perechi de chei la cererea subiectului, cheile nu vor fi folosite pentru crearea unei semnături electronice și că Autoritatea de Certificare nu va crea condiții pentru a face disponibilă semnătura unei entități neautorizate, A cheii private.

Pentru certificatele electronice necalificate, folosite în demonstrații sau în scopuri de testare, Abonatul are posibilitatea fie de a genera și de a stoca perechea de chei într-un dispozitiv criptografic securizat, fie în containere PKCS # 12.

6.1.2. Livrarea cheii private către abonat

Dacă subiectul încredințează DigiSign generarea de perechi de chei, cheile sunt astfel distribuite subiectului după cum urmează:

a. Cheile sunt stocate într-un dispozitiv criptografic securizat sau în recipiente PKCS # 12, fiind livrate personal subiectul sau prin poștă recomandată;
b. Informațiile necesare pentru accesarea perechii de chei (cod PIN) sunt transmise subiectului fie personal, fie prin poștă recomandată.

6.1.3. Livrarea cheii publice a subiectului catre CA

Abonații prezintă cheile publice generate ca o solicitare electronică a cărei formă trebuie să respecte protocoalele din PKCS # 10 (CRS).

Cererile prezentate unei autorități de certificare pot solicita, în anumite cazuri, confirmarea emisă de autoritatea de înregistrare.

Prezentarea unei chei publice este consumabilă în cazul în care o pereche de chei este generată la cererea abonatului sau la cererea operatorului autorității de înregistrare de către o autoritate de certificare care emite simultan un certificat pentru perechea de chei generate.

6.1.4. Distribuirea cheii publice CA către părțile învestite

Cheile publice ale autorităților care eliberează certificate pentru subiecți (utilizatori finali) sunt distribuite numai într-un formular de certificat care respectă recomandările ITU-T X.509 v.3. În cazul certificatelor DigiSign ROOT, certificatele sunt semnate automat.

DigiSign CA Cheile publice sunt furnizate în mod sigur potențialilor părți care utilizează următoarele canale:

a. Plasarea în depozitul public al DigiSign; Recuperarea certificatelor cere Abonaților să viziteze site-ul oficial al DigiSign.
b. Distribuția lanțului de încredere DigiSign.

6.1.5. Marimea cheii

DigiSign urmărește publicarea specială NIST 800-133 (2012) - Recomandare pentru generarea de chei criptografice, pentru termenele recomandate și cele mai bune practici privind dimensiunea cheii pentru CA-urile de bază, CA-urile intermediare, precum și pentru certificatele utilizatorilor finali. Astfel, perechile de chei trebuie să aibă o lungime suficientă pentru a preveni deducerea cheii private, folosind procedee de criptanaliză corecte.

DigiSign selectează din următoarele dimensiuni cheie / algoritmi de hash pentru Certificate Root, Certificatele CA emise și Certificate pentru utilizatorii finali, precum și pentru CRL / OCSP Responsabilul statutului certificatului:

- cheie RSA de 2048 biți cu algoritm hash securizat 2 (SHA-2)
- cheie RSA de 4096 biți cu algoritm hash securizat 2 (SHA-2)

6.1.6. Parametrii de generare a cheilor publice

Creatorul unei chei este responsabil pentru verificarea calității parametrilor cheii generate. Acesta este obligat să verifice:

a. Capacitatea de a executa operațiunea de criptare și decriptare, inclusiv crearea semnăturii electronice și verificarea acesteia,
b. Procesul de generare a cheilor, care ar trebui să se bazeze pe generatoare de numere criptografice puternice aleatoare - surse fizice de zgomot alb, dacă este posibil,
c. Imunitate la atacurile cunoscute (se aplică algoritmilor RSA și DSA).

6.1.7. Key usage

Scopurile în care sunt permise a fi utilizate cheile criptografice sunt descrise de către valoarea câmpului KeyUsage din structura certificatului, în conformitate cu standardul X.509 v3. Utilizarea biților câmpului KeyUsage trebuie realizată în conformitatea cu următoarele:

a. digitalSignature: crearea și verificarea semnăturilor electronice
b. nonRepudiation: servicii de non-repudiere și alte scopuri decât cele de la lit. f și g. Acest bit ar trebui setat doar în cheiele publice ale certificatelor care au ca scop verificarea semnăturilor electronice și nu ar trebui combinat cu cele descrise la litera c, d și e și în legătură cu asigurarea confidențialității.

c. keyEncipherment: criptare simetrică
d. dataEncipherment: criptarea datelor, alta decât cea de la lit. c și e
e. keyAgreement: schimbare de chei
f. keycertsign: verificarea semnăturilor aplicate cu certificate ale entităților ce oferă servicii de certificare
g. cRLSign: verificarea semnăturilor electronice din 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 criptarea datelor în procesul de schimb de chei
i. decipherOnly: poate fi folosit exclusiv cu bitul de keyAgreement pentru a indica decriptarea datelor în procesul de schimb de chei.

6.2. Protecția cheii private și controalele modulelor criptografice

DigiSign generează și stochează cheia privată prin utilizarea unui sistem sigur de prevenire a pierderii cheii private, a dezvăluirii acesteia sau modificării și utilizării neautorizat. În cazul în care DigiSign generează cheia privată la cerera solicitantului, DigiSign are obligația de o trimite către solicitant într-un mod sigur și să impună solicitantului protecția cheii private.

6.2.1. Standarde pentru modulele criptografice

Pentru emiterea certificatelor digitale calificate, DigiSign utilizează un modul criptografic securizat de tip HSM, în conformitate cu standardul FIPS 140-2 Level 3. Accesul fizic la acest dispozitiv este restricționat printr-un sistem securizat de control al accesului și nu poate fi accesat decât în prezența a cel puțin două persoane autorizate simultan.

Dispozitivele criptografice securizate utilizate de DigiSign pentru a emite certificate digitale calificate a căror chei criptografice sunt stocate pe un astfel de dispozitiv (QSCD), la cerera solicitantului de a i se genera perechea de chei în numele său, DigiSign asigură utilizarea unor dispozitive care sunt certificate conform standardului FIPS 140-2 Level 2.

6.2.2. Private key control (N out of M)

Serviciile DigiSign utilizează module hardware care impun participarea a mai mult de o persoană pentru a îndeplini activități delicate. Toate instrumentele necesare pentru îndeplinirea acestor activități sunt stocare într-un mod sigur și nu pot fi accesate fără informații de la diferite persoane. Controlul chei private realizat prin participarea a mai mulor persoane se aplica în cazul cheilor certificatelor CA.

Controlul accesului multipul este realizat prin diseminarea de secrete unor operatori autorizați și de încredere. Secretele sunt stocate pe carduri sau dispozitive criptografice, protejate prin coduri PIN și transferate într-un mod sigur și autorizat către titularii acestora.

6.2.3. Private key escrow

Această opțiune nu este disponibilă pentru cheile certificatelor CA sau ale utilizatorilor finali.

DigiSign ar putea furniza aceast serviciu pentru cheile altor tipuri de certificate față de cele care fac obiectul acestui CPP (spre exemplu pentru chei critographice utilizate exclusiv pentru criptare și decriptare), cu scopul de a asigură recuperearea cheilor. În acest caz,

cheile vor criptate și protejate printr-o metodă carea asigură același nivel de securitate sau unul superior ca cel utilizat pentru generarea și stocarea cheilor.

6.2.4. Back-up al cheii private

Pentru Autoritățile de Certificare din cadrul domeniului DigiSign sunt create câte o copie de back-up a chei private. Atunci când cheile sunt transferate într-un alt mediu pentru back-up și recuperare în caz de dezastru, acestea sunt transferate în formă criptată. Aceste copii sunt utilizate pentru execuția procedurilor standard sau de urgență, precum recupererea în caz de dezastru. Acest back-up al cheilor private ale certificatelor CA este realizat de multiple persoane de încredere prin utilizarea dispozitivelor criptografice securizate, urmând un proces standard și înregistrat.

6.2.5. Arhivarea cheii private

DigiSign nu oferă servicii de arhivare a cheii private.

6.2.6. Transferul în sau dintr-un modul criptografic al cheii private

Toate cheile sunt generate prin și într-un modul criptografic. Cheile private sunt exportate din modulul criptografic în dispozitive securizate certificate FIPS 140-2 doar în scopul transferării HSMurilor, stocării offline sau pentru back-up. Cheile private sunt criptate înainte de a fi transferate din modulul criptografic și nu sunt niciodată expuse în ca text simplu. Atunci când sunt transferate între module criptografice, DigiSign criptează cheile private, protejând cheile de criptare împotriva dezvăluirii acestora. Cheile de criptare pentru back-up sunt stocate într-un mod sigur, iar accesul la acestea necesită informații din partea mai multor persoane.

6.2.7. Stocarea cheii private în modulele criptografice

Cheila private ale certificatelor CA sunt generate și stocate în interiorul modulelor criptografice care sunt evaluate și certificate conform standardului FIPS 140-2 Level 3. Cheile private ale certificatelor CA rădăcină sunt stocate în mod offline în interiorul modulelor criptografice, într-un mediu sigur și securizate care poate fi accesat doar prin intermediul informațiilor din partea mai multor persoane.

6.2.8. Activarea cheii private

Cheila private ale certificatelor CA sunt activate conform specificațiilor producătorului modulelor criptografice utilizate. Datele de activare sunt protejate împotriva dezvăluirii.

În ceea ce privește certificatele utilizatorilor, aceștia sunt singurii răspunzători de protejarea cheii private. DigiSign recomandă utilizarea unor coduri PIN și parole puternice sau a unor metode de autentificare echivalente care asigură protecția împotriva accesului și utilizării neautorizate a cheilor private. Utilizatorii nu ar trebui niciodată să dezvăluie, în nici o circumstanță, datele de activare a cheilor private (spre exemplu, codul PIN).

6.2.9. Dezactivarea cheii private

Cheile private ale certificatelor CA sunt dezactivate urmând o procedură de logout pentru dispozitivul HSM atunci când acestanu este utilizat. Cheile private ale certificatelor CA rădăcină sunt dezactivate prin îndepărtarea completă a acestora din partiția de stocare ale dispozitivului HSM. DigiSign niciodată, sub nici o circumstantă, nu lasă dispozitivul HSM activat neblocat sau nesupravegheat.

DigiSign recomandă utilizatorilor să procedeze în același mod în ceea ce privește dezactivarea cheilor private ale certificatelor lor atunci când acestea nu sunt utilizate, aplicând proceuri de delogare și înlăturare a dispozitivului.

6.2.10. Distrugerea cheii private

Personalul autorizat al DigiSign care deține un rol de încredere, distruge într-o manieră sigură cheile private care nu mai sunt în uz. Distrugerea acestora poate implica ștergerea lor din toate partițile de stocare. De asemenea, DigiSign inițializează dispozitivele și modulele de back-up asociate, în conformitate cu procedurile producătorilor acestor dispozitive. Această acțiune inițializează dispozitivul și rescrie datele cu zerori binare. Dacă acestă acțiune eșuează, DigiSign va distruge dispozitivul fizic printr-o manieră de așa natură încât extragerea cheilor private să devină imposibilă (spre exemplu, incinerare).

DigiSign recomandă utilizatorilor să distrugă cheile private printr-o manieră sigură atunci când acestea nu mai sunt utilizate – certificatul este revocat sau expirat.

6.3. Alte aspecte privind managementul cheii private

Tehnic, este posibil ca o cheie privată să fie utilizată și cu scopul de a crea semnături electronice și de a cripta date. Deși această posibilitate există, DigiSign nu recomandă această practică. Conform acestui CPP, este interzisă utilizarea cheilor private de semnare ale CA pentru alte scopuri precum critparea.

Prin urmare, acest capitol va descrie alte aspecte privind managementul cheilor private, precum procedurile de arhivare a cheilor publice și valabilitatea cheilor publice și private utilizate și recomandate de DigiSign.

6.3.1. Arhivarea cheii publice

Scopul arhivării cheilor publice este de a crea posibilitatea verificării semnăturilor electronice generate cu acesta și după momentul în care certificatul respectiv este eliminat din depozitarul DigiSign. Această acțiune este esențială pentru serviciile de non-repudiere, precum seriviciile de marcare temporală sau serviciile de validare certificatelor.

Fiecare CA din domeniul DigiSign, utilizată pentru emiterea certificatelor utilizatorilor finali, arhivează cheia publică a respectivelor certificate. Utilizatorii pot arhiva local cheia publică a certificatelor, mai ales în cazul în care această acțiune este necesară pentru utilizarea certificatului în anumite aplicații.

Arhiva cheilor publice este protejată într-o manieră care asigură protecția împotrivă accesului neautorizat și împiedică acțiuni precum modificarea în orice fel a acesteia. Protecția este asigurată prin metode de autentificare ale entității de arhivare și autorizare ale interogări acesteia.

6.3.2. Valabilitatea cheilor criptografice

Conform acestui CPP, DigiSign utilizează în mod corespunzător cheile private ale certificatelor CA de semnare, fără a depăși perioada de viață ale acestora, așa cum este descris în tabelul următor.

Tipul de certificat	Perioada maximă de utilizare
Certificat CA rădăcină	40
Certificat CA intermediar	25
Certificat utilizator final	5

Tabelul 6.3.2. Valabilitatea cheilor criptografice

6.3.3. Valabilitatea certificatelor

Perioada de valabilitate a certificatelor emise pentru utilizatorii finali de către Autoritățile de Certificare DigiSign este de pana la 3 ani, din momentul emiterii acestora, fără a depăși perioada de valabilitate a autorității emitente.

6.4. Datele de activare

Datele de activare reprezintă instrumentul de acces la o anumită cheie privată. Datele de activare pot fi sub forma unei parole, a unui cod PIN, nume de utilizator și parolă aferentă, secret partajat etc, sau o combinație a acestora.

Operatorii RA și CA, precum și persoanele din cadrul DigiSign care dețin un rol de încredere, au obligația să utilizeze parole puternice, imune la atacuri brute, pentru sistemele care implică autentificarea cu o pereche de chei criptografice. DigiSign recomandă utiliatorilor să utilizeze de asemenea parole puternice.

Pentru accesara unei chei private, DigiSign recomandă utilizarea unor factori multipli de autentificare, precum un dispozitiv criptografic și a unor date de autentificare, precum o parolă.

Secretele partajate utilizate pentru protecția cheilor private ale certificatelor CA sunt generate în conformitate cu prevederile acestui CPP și sunt stocate în module criptografice dedicate. Aceste module sunt protejate de un cod PIN, creat în conformitate cu cerințele standardului FIPS 112. Secretele partajate devin date de activare după activarea acestora în sistemul în care urmează a fi utilizate.

Protecția datelor de activare include metode de control al acestor date care previn dezvăluirea lor. Acestea sunt în conformitate cu tipul datelor de activare și depind dacă controlul este impus de cheia privată sau de distribuirea datelor de activare în secrete partajate. Pentru expresiile de autentificare sunt recomandate cerințele standardului FIPS 112, iar în cazul secretele partajate sunt recomandate cerințele standardului FIPS 120.

Este recomandat ca datele de activare utilizate pentru accesara cheilor private sa fie protejate prin intermediul controalelor criptografice și controalelor de acces fizic. Datele de activare nu ar trebui sa fie scrise pe suporturi fizice, iar în cazul în care sunt, nivelul de protecție al respectivelor suporturi ar trebui să fie cel puțin echivalent cu cel al protejării datelor de către modulul criptografic. Încercările excesive de a accesa modulul criptografic care nu sunt finalizate cu succes ar trebui să impună blocarea mdoulului și compromiterea cheii private. Stocarea datelor de activare nu trebuie să fie realizată în același loc cu stocarea modului critpografic.

6.5. Controalele de securitate ale sistemelor de calcul

DigiSign asigură controalele de securitate ale sistemelor de calcul utilizate, în conformitate cu standardele tehnice ETSI EN 319 411-1 și ETSI EN 319 411-2, atunci când aceste standarde impun cerințe suplimentare privind procedurile de certificare, și, de asemnea, în conformitate cu standardul ISO 27001:2013.

Operațiile întreprinse de CA și RA din cadrul DigiSign sunt realizate prin dispozitive hardware și aplicații software de încredere și sigure.

Serverele și computerele sunt rulate printr-un sistem de încredere utilizat de DigiSign, configurat și testat prin cele mai bune practici din domeniu. Sistemele sunt scanate pentru a detecta programe malițioase, fiind protejate împotriva virușilor prin programe dedicate. DigiSign limitează accesul la serverele de producție doar la acele persoane autorizate în acest sens. Aplicațiile generale utilizate de operatori nu sunt configurate pe serverele de producție.

Rețeaua DigiSign din mediul de producție dispune de soluții de firewall pentru a proteja sistemul împotriva încercărilor de accesare neautorizată, atât din interior, cât și din exterior, precum și pentru a limita acele procese ce pot atrage vulnerabiliăți în sistemul de producție. DigiSign impune operatorilor și utilizatorilor săi să utilizeze parole care conțin un minim de caractere alfanumerice combinate cu caractere speciale, precum și schimbarea periodică a acestora. Descrierea detaliată a controalelor de securitate implementate de DigiSign este disponibilă în documentele interne, confidențiale, care nu vor fi puse la dispoziția publicului.

6.6. Controale tehnice privind ciclul de viață

DigiSign asigură implemetarea unor controale perioadeice privind dezvoltarea, managementul și ciclului de viață al sistemelor utilizate, în conformitate cu standardele ETSI EN 319 411-1 și ETSI EN 319 411-2, atunci când aceste standarde impun cerințe suplimentare privind procedurile de certificare, și, de asemnea, în conformitate cu standardul ISO 27001:2013.

Implementarea sistemului DigiSign este în conformitate cu standardele în vigoare privind dezvoltarea și managementul schimbării sistemelor. Fiecare aplicație, înainte de a fi implementată în producție, este testată într-un mediu specific de testare. Acest proces este desfășurat de o echipă de IT împreună cu operatori din diferite departamente. Testarea se realizează în conformitatea cu scenarii prestabilite. Datele din testare nu sunt utilizate în producție și datele din mediul de producție nu sunt utilizate în procesele de testare decât dacă au fost depersonalizate în prealabil.

Reguli similare se aplica și în ceea ce privește componentele hardware și înlocuirea acestora, astfel:

a. componentele hardware sunt implementate de o așa manieră încât să permită identificarea acestora și evaluarea rutei componentelor până la locul instalării acestora
b. livrarea componentelor hardware de înlocuit este realizăt într-o manieră similiară cu livrarea componentelor inițiale, iar procesul de înlocuire este realizat de personal de încredere instruit în acest sens.

Scopul acestor controale de securitate este de a monitoriza permanent funcționalitatea sistemului DigiSign, asigurând operarea corectă a acestuia și în conformitate cu configurațiile acceptate și implementate. Configurația actuală a sistemului DigiSign, precum și rice modificare și actualizare a sistemului, este controlată și înregistrată corespunzător. Controalele aplicate sistemului DiigSign permit verificarea continuă a integrității aplicațiilor, a versiunilor acestora, precum și a autentificării și verificării originii componentelor hardware.

Descrierea detaliată a controalelor implementate de DigiSign este disponibilă în documentele interne, confidențiale, care nu vor fi puse la dispoziția publicului.

6.7. Controalel de securitate ale rețelei

DigiSign asigură controalele de securitate ale rețelei, inclusiv, dar fără a se limita la firewall, detectarea accesului neautorizat, securizarea comunicațiilor dintre participanții PKI care asigură confidențialitatea și autentificarea mutuală, protecția anti-virus, securitatea website-ului, a bazei de date și a altor resurse, acestea fiind implementate în conformitate cu cerințele standardelor ETSI EN 319 411-1 și ETSI EN 319 411-2 standards, atunci când aceste standarde impun cerințe suplimentare privind procedurile de certificare.

Serverele și stațiile de lucru din cadrul sistemului DigiSign sunt conectate la o rețea locală dedicată (LAN), divizată în mai multe sub-rețele unde accesul este controlat. Accesul prin internet la orice segment este protejat prin mijloace de tip firewall inteligent. Controalele de securitate sunt dezvoltate în baza filtrării traficului prin firewall, routere și servicii de proxy.

Măsurile de protecție ale securității rețelei acceptă doar acele mesaje trimise utilizând protocoale HTTP(S), LDAP(S), NTP, POP3(S), IMAP(S) și SMTP(S). Evenimentele (logurile) sunt înregistrate în jurnalele sistemului, permițând monitorizarea utilizării serviciilor furnizate de DigiSign.

Descrierea detaliată a controalelor implementate de DigiSign este disponibilă în documentele interne, confidențiale, care nu vor fi puse la dispozția publicului.

7. Profilul certificatelor, CRL și OCSP

Acest capitol descrie profilele certificatelor, ale CRL și ale OCSP, implementate în DigiSign PKI.

Profilul certiifcatelor și CRL sunt în conformitate cu formatul acestora descris în standardul ITU-T X.509 v.3, în timp ce profilul serviciului OCSP este în conformitate cu cerințele RFC 6960. Certificatele digitale emise de DigiSign CA sunt în conformitate cu specificațiile descrise în ETSI EN 319 412 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Părțile 1, 2, 3 și 5.

7.1. Profilul certificatelor

Conform standardului X.509 V3, un certificat digital reprezină o secvență compusă din următoarele trei secțiuni esențiale: corpul certificatului (tbsCertificate), informații referitoare la algoritmul utilizat pentru semnarea certificatului (signatureAlgorithm), și semnătura electronică a Autorității de Certificare emitentă (signatureValue).

7.1.1. Conținutul certificatului

Conținutul certificatelor include valori ale câmpurilor de bază și ale extensiilor acestora (standard, descrise în norme și private, definite de către CA emitentă). Extensiile definite în structura certificatului, în conformitate cu normele aplicabile, permit asignarea unor atribute adiționale pentru subiectul certificatului, precum și cheia publică, simplificând managementul ierarhiei structurii certificatului. Certificatele digitale emise în conformitate cu standardul X.509 V3 permit definirea unor extensii proprietare, unice pentru un anumit sistem.

a. Câmpurile de bază

DigiSign suportă următoarele câmpuri de bază:

- **Version**: versiunea a treia a formatului certificatului
- **Serial Number**: număr de serial unic pentru CA
- **Signature Algorithm**: identificatorul algoritmului utilizat de CA
- **Issuer**: numele distinct al CA
- **Validity**: perioada de valabilitate, descrisă prin data de începere a valabilității (notBefore) și data de încetare a valabilității (notAfter) certificatului
- **Subject**: numele distinct al subiectului certificatului (titularul acestuia)
- **Subject Public Key Info**: valoara cheii publice și identificatorul algoritmului criptografic asociat cu această cheie.

b. Extensiile

Funcționalitatea fiecărei extensii este definită de valoarea standardului corespondent identificatorului de obiect. Extensiile, în funcție de CA emitentă, pot fi marcate ca critice sau non-critice. Dacă o extensie este marcată ca fiind critică, iar aplicația care utilizează acel certificat nu recunoaște respectiva extensie, atunci certificatul trebuie să fie respins. Pe de altă parte, extensiile care sunt marcate ca fiind non-critice, pot fi omise la verificarea certificatului.

DigiSign suportă următoarele câmpuri privind extensiile standard:

- **AuthorityKeyIdentifier**: identificatorul cheii publice ale certificatului CA utilizat pentru semnarea certificatelor emise – non-critic

- **SubjectKeyIdentifier** – identificatorul cheii subiectului certificatului – non-critic

- **KeyUsage**: descrie utilizarea cheii private - critic
  digitalsignature (0): crearea semnăturilor electronice
  nonRepudiation (1): servicii de non-repudiere
  keyEncipherment (2): schimbarea de chei
  dataEncipherment (3): criptarea de date
  keyAgreement (4): acceptul cheilor
  keycertsign (5): semnarea certificatelor
  CRLsign (6): semnarea CRL
  encipherOnly (7): doar criptare
  decipherOnly (8): doar decriptare

- **ExtKeyUsage**: definește constrângerile privind utilizarea cheii – non-critic. Acest câmp definșete una sau mai multe arii, suplimentar față de utilizare cheii. Acest câmp se interpretează ca o restricție la utilizările cheii permise. DigiSign emite certiifcate care ar putea conține următoarele valori în acest câmp:
  serverAuth – autentificarea web a serverelor TLS;
  clientAuth – autentificarea web a clienților TLS;
  codesigning – semnarea de cod executabil;
  emailProtection – protecție e-mail;
  ipsecEndSystem – protecție protocol IPSEC,
  ipsecTunnel – IPSEC protocol Tunnelling,
  ipsecUser – protecția protocoalelor IP în aplicații,
  timeStamping – asocierea dintre valoarea digest cu sursa de timp furnizată de către o sursă de timp de încredere
  OCSPsigning – servicii de validare a statusului certificatelor emise
  dvcs – confirmarea emisă de o autoritatea notarială, în baza protocolului DVCS
  EncryptedFileSystem – criptarea fișierelor sistemului (EFS), este obligatoriu pentru interogările anumitor aplicații

SmartCardLogon **–** operații de tip logare, autentificare într-un sistem

- **Certificate Policies** – această extensie indică politicile pe care CA emitentă le implementează atunci când emite un certificat – non-critic. Extensia este formată dintr-o lista de informații referitoare la politicile de certificare aplicate (identificator unic, adresa web etc)

c. Qualifiers

Certificatele emise de DigiSign CA pot conține și qualifiers, conform recomandărilor RFC 3280:

- **PolicyMapping**: conține unul sau mai mulți identificatori de politici – non-critic
- **SubjectAlternativeName:** numele alternativ al subiectului – non-critic
- **BasicConstraints**: definește tipul certificatului (CA sau utilizator final) precum și numărul maxim privind calea de certificare – critic
- **CRL DistributionPoints**: definește adresele privind CRLul emis de CA emitent– non-critic
- **AuthorityInfoAccessSyntax**: indică metoda de acces la informațiile publicate de CA emitent – non-critic
- **OCSPNoCheck**: non-critic
- **NetscapeCertType**: non-critic, cu următoarele valori ce pot fi combinate:
  SSLClient (bit 0)
  SSLServer (bit 1)
  S/MIME (bit 2)
  ObjectSigning (bit 3)
  SSL CA (bit 5)
  S/MIME CA (bit 6)
  ObjectSigning CA (bit 7)

d. Identificatorul algoritmului de semnare

Acest câmp – signatureAlgorithm – conține algoritmul criptografic de semnare utilizat de CA emitentă. DigiSign utilizează algoritmul RSA în combinație cu funcțiile SHA-1 și SHA-2.

e. Câmpul semnăturii electronice a CA emitent

Valoara acestui câmp - signatureValue **–** reprezintă rezultatul execuției unei funcții criptografice HASH pentru toate câmpurile certificatului și algoritmul semnării rezultatului obținut cu cheia privată a CA emitentă.

7.1.2. Profile

A. Autoritatea de Certificate Rădăcină

DigiSign ROOT Certification Authority	
Version	V3
Serial Number	16 5e 1c 37 56 d0 2b 77
Signature Algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN = DigiSign Root Certification Authority OU = DigiSign Certification Services O = DigiSign S.A. C = RO
Valid From	Thursday, October 30, 2014 12:40:13
Valid To	Monday, October 30, 2034 12:40:13
Subject	CN = DigiSign Root Certification Authority OU = DigiSign Certification Services O = DigiSign S.A. C = RO
Public Key	
Public Key parameters	05 00
Subject Key Identifier	49 08 ac 07 8c 1f b8 2e 71 b6 5c 4c a2 5e 09 6e 01 2b 6a 4e
Authority Key Identifier	KeyID=49 08 ac 07 8c 1f b8 2e 71 b6 5c 4c a2 5e 09 6e 01 2b 6a 4e
Basic Constraints	Subject Type=CA Path Length Constraint=None
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbrint algorithm	sha1
Thumbrint	f5 e3 24 04 2f f4 5e 1c b9 3a a5 a4 46 8c 59 f2 0f 53 dc 5e

B. Autoritatea de Certificare Intermediară

DigiSign Qualified CA Class 3 2017	
Version	V3
Serial Number	21 00 9b 29 28 2c 68 a6
Signature Algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CN = DigiSign Root Certification Authority OU = DigiSign Certification Services O = DigiSign S.A. C = RO
Valid From	luni, 10 aprilie 2017 13:03:44
Valid To	miercuri, 6 aprilie 2033 13:03:44
Subject	CN = DigiSign Qualified CA Class 3 2017 2.5.4.97 = VATRO-17544945 OU = DigiSign Certification Services

	O = DigiSign S.A. C = RO
Public Key	
Public Key parameters	05 00
Certificate Policies	[1] Certificate Policy: Policy Identifier=1.3.6.1.4.1.34285.256.3.0.2.0.2017 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.digisign.ro/cps
Subject Key Identifier	53 21 f4 13 a6 75 37 49 66 de b3 02 69 9d b0 dc ff 07 19 c7
Authority Key Identifier	KeyID=49 08 ac 07 8c 1f b8 2e 71 b6 5c 4c a2 5e 09 6e 01 2b 6a 4e
Subject Alternative Name	office@digisign.ro
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.digisign.ro/repository/rootcav3.crl
Authority Information Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.5.46.1) Alternative Name: URL=http://ocsp.digisign.ro/ocsp
Basic Constraints	Subject Type=CA Path Length Constraint=0
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Thumbrint algorithm	sha1
Thumbrint	8f c3 82 bc 63 b4 86 0c 97 99 86 1e c8 75 6f cf 7a 07 4f 50

7.2. Profilul CRL

Lista Certificatelor Revocate (CRL) conține trei câmpuri: primul (tbscertList) conține informații privind certificatele revocate, iar următoarele - signatureAlgorithm și signatureValue conțin informații despre identificatorul algoritmului utilizat pentru semnara listei și semnătura electronică a CA emitentă.

Câmpul tbscertList reprezintă o secvență de câmpuri obligatorii și opționale. Cele obligatorii se referă la emitentul CRL, iar cele opționale conține informații despre certificatele emise și extensiile CRL, astfel:

- **Version**: versiunea formatului CRL
- **Signature**: algoritmul utilizat de CA emitent pentru semnara CRL; DigiSign utilizează algoritmii sha1WithRSAEncryption și sha2WithRSAEncryption
- **Issuer**: numele CA emitent
- **ThisUpdate**: data de publicare CRL
- **NextUpdate**: data publicării următorului CRL

- **Revokedcertificates**: lista certificatelor revocate (e posibil să nu conțină valori dacă nu sunt certiifcate revocate) și este formată din trei sub-câmpuri:
  usercertificates – serial unic al certificatului revocat;
  revocationDate – data revocării;
  crlEntryExtensions – informații suplimentare despre certificatul revocat – optional.

- **crlExtensions**: informații suplimentare despre CRL (câmp opțional). Cele mai importante valori posibile ale acestui câmp sunt *AuthorityKeyIdentifier* și *cRLNumber*.

Funcționalitățile și semnificația extensiilor CRL sunt în conformitate cu cele ale certificatelor. Extensiile CRL permise de DigiSign sunt: **ReasonCode** care reprezintă codul motivului revocării și este marcat ca fiind non-critic, astfel:

a. **unspecified** – nespecificat;
b. **keyCompromise** – compromiterea cheii;
c. **cACompromise** – compromiterea cheii CA;
d. **affiliationChanged** – modificarea datelor subiectului;
e. **superseded** – reînnoirea certificatului;
f. **cessationOfOperation** – încetarea activității;
g. **certificateHold** – suspendarea certificatului;
h. **removeFromCRL** – eliminarea certificatului din CRL.

Certificatele revocate sunt păstrate pe o perioadă de timp de 15 ani. După expirarea acestora, sunt scoase din CRL.

7.3. Profilul OCSP

Protocolul OSP utilizat pentru verificarea în timp real a certificatelor digitale emise, permite evaluarea statusului acestora. Serviciul este furnizat de DigiSign în numele CA emitente. Serverul OCSP care emite confirmările statusului certificatului deține o pereche de chei generată exclusiv pentru acest scop.

Certificatul serverului OCSP conține extensia extKeyUsage definită în RFC 3280. Această extensie este marcată ca fiind non-critică și reprezintă confirmarea delegării acestui serviciu de către CA. Certificatul pentru OCSP conține și extensia OCSPNoCheck, descrisă în RFC 6960, marcata ca fiind non-critică.

Entitatea care primește o o confirmare a statusului unui certificat, emisă de serverul OCSP trebuie să suportate răspunsul standard al acestuia, cu identificatorul *id-pkix-ocsp-basic*. Atunci când răspunsul OCSP conține un mesaj de eroare, răspunsul nu este semnat electronic (RCF 6960).

7.3.1. Numărul versiunii

Serverul OCSP al DigiSign emite confirmări ale statusului certificatelor în conformitate cu RFC 6960. Singura valoare pentru versiunea disponibilă este 0, fiind echivalentul versiunii v1.

7.3.2. Statusul certificatelor

Informațiile privind statusul certificatelor sunt incluse în câmpul certStatus a structurii SingleResponse și pot avea următoarele valori:

a. **GOOD** – certificatul este valid
b. **REVOKED** – certificatul este revocat sau nu este emis în conformitate cu RFC 6960

c. **UNKNOWN** – nu sunt suficiente informații pentru ca statusul certificatului să poate fi identificat

7.3.3. Extensii standard suportate

În conformitate cu RFC 6960, serverul OCSP acceptă următoarea extensie: **Nonce**. Aceasta este inclusă în requestExtension a OCSPRequest și reluată în câmpul responseExtension a OCSPResponse.

8. Evaluări și audit de conformitate

Acest capitol descrie evaluările și auditurile implementate pentru a asigura că acțiunile întreprinse de DigiSign și entitățile delegate sunt în conformitate cu regulile și practicile asumate, precum Politica de Certificare și CPP.

DigiSign implementează procese de audit intern, dar și extern, conduse de o entitate independentă. Pentru furnizarea serviciilor de încredere calificate, DigiSign este auditată de către un Organism de Evaluare a Conformității.

8.1. Frecvența și circumstanțele care impun auditul

Auditul intern are loc cel puțin anual, iar auditul extern este realizat la cerere, cel puțin o dată la doi ani.

Pentru furnizarea serviciilor de încredere calificate, auditul condus de Organismul de Evaluare a Conformității are loc o dată la doi ani sau de fiecare dată când are loc o schimbare majoră în procesul de furnizare al serviciilor, ori de fiecare dată când este solicitat de către Organimsul de Supraveghere național.

8.2. Identitatea și calificarea auditorului

Auditul intern este condus de departamentul de calitate și audit al DigiSign, în timp ce auditul extern este realizat de către o entitate independentă.

Orice auditor care evaluează sistemul DigiSign trebuie să acționeze cu precizie pentru a asigura faptul că politicile și practicile asumate de DigiSign sunt implementate în mod corspunzător, precum și pentru a detecta orice non-conformitate care ar putea pune în pericol securitatea serviciilor furnizate. DigiSign se obligă să contracteze auditori cu un nivel ridicat de expertiză în domeniul securității, în particular în domeniul auditat.

Serviciile de audit sunt realizate de către companii specializate în acest sens, independente, recunoscute și credibile cel puțin în domeniul tehnologiei informației. Auditul serviciilor de încredere calificate furnizate de DigiSign este condus de un Organism de Evaluare a Conformității, în conformitate cu Regulamentul UE nr. 910/2014.

8.3. Relație auditor – entitate auditată

Enitatea care conduce auditul extern și emite Raportul de Evaluare a Conformității este desemnată de DigiSign sub condiția ca această să fie total independentă de DigiSign.

Auditorul și furnizorul supus auditului trebuie să nu aibă nici un fel de relație care ar pune sub îndoială idenpendența și obiectivitatea auditorului. Această relație include segmentul financiar, legal, social sau orice alt tip de relație din care ar putea rezulta un conflict de interese.

8.4. Subiectele auditate

Toate auditurile sistemului DigiSign sunt realizate în conformitate cu regulamentele și regulile acceptate internațional și privesc cel puțin:

- Securitatea fizică
- Procedurile privind verificarea identității solicitanților
- Procedurile de furnizare a serviciilor de încredere
- Securitatea aplicațiilor software și ale rețelei de acces
- Securitatea privind personalul DigiSign
- Evenimentele de jurnal și procedurile de monitorizare
- Procedurile de arhivare și restaurare
- Planurile de continuitate a afacerii și recuperare în caz de dezastru
- Înregistrările privind modificarea parametrilor de configurare ale sistemelor
- Înregistrările privind verificările și analiza aplicațiilor software și ale dispozitivelor hardware utilizate în cadrul sistemului.

8.5. Măsurile de remediere a deficiențelor

Măsurile de remediere a deficiențelor identificate, dacă este cazul, sunt determinate de natura și întinderea acestor neregularități. Orice determinare a măsurilor este realizată de DigiSign ținând cont de recomandările făcute de echipele de auditori. DigiSign își rezervă dreptul de a decide care este măsura potrivită ce ar trebui implementată pentru a remedia respectiva deficiență, precum și perioada de timp aferentă remedierii.

Privind serviciile de încredere calificate, în conformitate cu prevederile legale aplicabile, măsurile de remediere și perioada de timp aplocată acestora pot fi stabilite de către Organismul de Supraveghere național.

8.6. Comunicarea rezultatului auditului

Rezultatul auditului, în particular Raportul de Evaluare a Conformității este comunicat către managementul DiigSign și Organismului de Supraveghere național care are responsabilitatea confirmării statutului de prestator de servicii de încredere calificat.

9. Alte aspecte legale și de business

9.1. Tarife

Tarifele privind produsele și serviciile furnizate de DigiSign sunt publicate la adresa www.digisign.ro. Plata acestor tarife poate fi realizată în numerar prin ordin de plată, precum și cu cardul, în conformitate cu factura emisă în acest și legislația aplicabilă în vigoare.

9.1.1. Tarife privind serviciile de verificare a certificatelor

Serviciile de verificare a certificatelor, precum și serviciile de revocare și/sau suspendare, sunt gratuite. DigiSign își rezervă dreptul de a stabili tarife privind serviciile de verificare a certificatelor în timp real prin protocolul OCSP, precum și pentru alte servicii conexe.

9.1.2. Tarife privind serviciile conexe

DigiSign își rezervă dreptul de a stabili tarife pentru serviciile conexe, precum:

- Generarea de chei criptografice pentru CA sau utilizatori
- Testarea de aplicații și includerea lor în lista aplicațiilor recomandate
- Acordarea de licențe
- Dezvoltare, implementare și instalare
- Redactare a CP, CPP, instrucțiuni, ghiduri etc
- Cursuri de instruire

9.1.3. Politica de restituire

DigiSign oferă restituirea tarifelor achitate, în confirmitate cu Policita de Restituire publicată la adresa www.digisign.ro. Utilizatorii care dores invocarea acestei politici trebuie să inițieze și procedura de revocare a serviciilor de care au beneficiat.

9.2. Responsabilitate financiară

DigiSign va acoperi prejudiciile pe care le-ar putea cauza cu prilejul desfășurării activității de certificare, tuturor persoanelor care își întemeiază conduita pe efectele juridice ale certificatelor digitale calificate, până la concurența echivalentului în lei (RON) a sumei de 10.000 euro pentru fiecare risc asigurat. Riscul asigurat reprezintă fiecare prejudiciu produs, chiar dacă se produc mai multe asemenea prejudicii ca urmare a neîndeplinirii de către furnizor a unei obligații prevăzute de lege.

9.3. Confidențialitate

Toate informațiile deținute de DigiSign sunt colectate, stocate și procesate în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea dispozițiilor de drept intern, ale Regulamentului nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date și al altor dispoziții de drept al Uniunii referitoare la protecția datelor.
Relațiile dintre participanții DigiSign PKI sunt bazate pe încredere.

O terță parte poate avea acces la informațiile publice din cadrul certificatelor digitale emise. Alte informații care au stat la baza emiterii respectivului certificat nu vor fi puse la dispoziția publicului sub nici o circumstanță, cu excepția situațiilor impuse prin lege.

Partea care dezvăluie informații confidențiale poate fi exonerată dacă:

a. Informația era cunoscută înainte să fie primită de partea care o dezvăluie
b. Informația a fost dezvăluităă după obținerea acordului părții proprietare
c. Partea care o dezvăluie a fost forțată legal în acest sens

Dezvăluirea informațiilor către părți care au obligații în procesul de furnizare a serviciilor de încredere, se va realiza confidențial și se va extinde doar la acele informații necesare îndeplinirii obligațiilor respective.

9.3.1. Informații considerate confidențiale sau private

DigiSign, angajații săi și alte entități parte ale procesului de furnizare a serviciilor de încredere, se obligă să păstreze confidențialitatea informațiilor pe perioada pe care sunt angajați și după această perioadă. Sunt considerate confidențiale sau private următoarele tipuri de informații:

- Informațiile furnizate de utilizatori care nu fac parte din cheia publică a certificatelor
- Documente furnizate de/către utilizatori (contracte, acorduri, oferte etc)
- Înregistrările din sistem privind tranzacțiile efectuate
- Înregistrările de evenimente (loguri)

- Rapoartele auditurilor interne și externe, dacă acestea pot dezvălui informații de natură să provoace o amenințare a securității sistemului DigiSign
- Planurile de urgență
- Informații cu privire la securitatea și protecția dispozitivelor hardware, aplicațiilor software, informații privind managementul serviciilor de încredere și regulile aplicabile.

9.3.2. Informații publice

Toate informațiile necesare funcționării corespunzătoare a serviciilor oferite nu sunt considerate confidențiale sau private. În particular, informațiile publice reprezintă informațiile incluse în certificatele digitale emise și cele publicate la adresa www.digisign.ro. Orice solicitant care aplică pentru obținerea unui certificat digital este considerat a fi luat la cunoștință despre informațiile publice incluse în certificate și este de acord cu publicarea acestora.
O parte din informațiile furnizate de sau către utilizator pot fi dezvăşuite altor entități doar cu acordul scris al utilizatorului sau al DigiSign, după caz, și doar pentru scopul declarat în acordul încheiat între părți.

Următoarele categorii de informații sunt disponibile publicului prin depozitarul DigiSign:
- Politicile și practicile privind furnizarea serviciilor de încredere
- Lista de prețuri privind serviciile și produsele furnizate
- Ghiduri, instrucțiuni și recomandări
- Certificatele digitale emise utilizatorilor
- Certificatele digitale ale CA
- CRL etc

9.3.3. Dezvăluirea motivului revocării unui certificat

Dacă un certificat a fost revocat la cerea unui solicitant autorizat (nu titularul certificatului), informația privind revocarea și motivele acesteia sunt dezvăluite oricărei părți interesate.

9.3.4. Dezvăluirea informațiilor confidențiale autorităților publice

Ca principiu general, nici un document, informație sau evidență cu caracter confidențial, deținută de DigiSign, nu va fi dezvăluită autorităților publice, cu excepția cazului în care acestea dispun de un instrument oficial care să impună dezvăluirea (ex: mandat) sau printr-un decizie a unei instanțe de judecată, chiar dacă respectiva decizie este sau nu contestată deoarece DigiSign nu își asumă obligația de a stabili acest lucru.

9.4. Protecția datelor cu caracter personal

DigiSign asigură protecția confidențialității și integrității datelor cu caracter personal pe care le deține, în special în ceea ce privește transmiterea acestora către utilizatori și între componentele sistemului DigiSign, în conformitate cu cerințele Regulamentului (UE) nr. 910/2014 și cu respectarea dispozițiilor de drept intern, ale Regulamentului nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date și al altor dispoziții de drept al Uniunii referitoare la protecția datelor.

9.5. Drepturi de proprietate intelectuală

Toate mărcile, patentele, licențele, imaginile grafice etc utilizate de DigiSIgn sunt și vor rămâne în proprietatea intelectuală a propietarilor acestora. DigiSign se angajează să

menționeze acest lucru în conformitate cu cererile primite în acest sens. Fiecare cheie privată asociată certificatului utilizatorului este proprietatea titularului acestuia.

9.6. Responsabilități și garanții

A. Autorități de Certificare

Toate certificatele digitale emise de DigiSign sunt în conformitate cu standardul X.509 V3. DigiSign își asumă obligația de a garana aceasta conformitate. Mai mult, DigiSign asigură faptul că toate cerințele acestui CPP și ale CP sunt respectate.

Garanția esențială furnizată de DigiSign se referă la faptul că procedurile implementate sunt în conformitate cu regulile stabilte în CP și CPP. Alte responsabilități specifice vor fi descrise în acordurile încheiate cu utilizatorii.

Dacă nu este specificat altfel în CPP sau legislația aplicabilă, DigiSign declină orice fel de responsabilitate mai ales în ceea ce privește neglijența sau lipsa de responsabilitate a utilizatorilor și entităților partenere.

B. Autoritățile de Înregistrare

Autoritățile de Înregistrare din cadrul DigiSign au obligația respectării prevederilor CP, CPP și ale procedurilor interne.

C. Utilizatorii

Utilizatorii au obligația să accepte și să respecte condițiile generale aplicabile serviciului de încredere solicitat. Dacă utilizatorii nu respectă și nu acceptă aceste condiții generale, DigiSign nu poate furniza serviciul de încredere solicitat. Prin acceptarea condițiilor generale, utilizatori acceptă implicit CP și CPP aplicabile serviciului solicitat, precum și obligațiile și responsabilitățile ce decurg din acestea.

Responsabilitatea principală a utilizatorilor este față de entitățile partenere în sensul utilizării corespunzătoare a serviciilor de încredere furnizate, a cheilor private, a certificatelor aferente acestor servicii și a dispozitivelor QSCD, cu excepția cazului în care utilizatorii pot dovedi că au luat toate măsurile adecvate terminării serviciului de încredere la timp (spre exemplu, revocarea certificatului).

D. Entitățile Partenere

Entitățile Partenere au cel puțin următoarele obligații și responsabilități:

- Să verifice cu atenție fiecare semnătură electronică primită, astfel:
  - Să verifice calea de certificare a certificatului semnatar
  - Să se asigure de faptul că certificatul semnatar este corespunzător emis de o CA care asigură nivelul de încredere de care are nevoie
  - Să se asigure de faptul că nici un certificat din lanțul de certificare nu este revocat sau suspendat
  - Să se asigure de faptul că CA emitent are dreptul de a emite și semna certificatul semnatar
  - Să verifice marca temporală care însoțește semnătura electronică, dacă este cazul

- Să utilizeze doar aplicații software capabile de funcționalități criptografice care asigură un nivel de încredere compabitil cu cel de care are nevoie

- Să refuze o semnătură electronică dacă rezultatul verificării acesteia este negativ sau invalid
- Să verifice semnătura electronică în sensul dacă acesta a fost creată printr-un dispozitiv de creare a semnăturilor calificat și dacă a fost modificată de la momentul aplicării acesteia
- Să accepte doar acele certificate care:
  - Sunt utilizate în conformitate cu scopul declarat al acestora și aria de aplicabilitate aferentă
  - Al căror status este verificat prin serviciile de validare a certificatului puse la dispozite de DigiSign
- Să stabilească condițiile care trebuie îndeplinite de către certificatul semnatar sau semnătura electronică pentru a fi considerate valide

9.7. Limitarea responsabilității

DigiSign nu este responsabilă pentru (a) daunele cauzate de forța majoră și/sau cazul fortuit, (b) de utilizarea necorespunzătoare a serviciilor de încredere calificate, (c) stocarea de date eronate in bazele de date ale DigiSign si includerea acestora in certificate digitale emise Utilizatorului in cazul in care Utilizatorul a declarat ca aceste date sunt corecte, (d) prejudiciile cauzate de furtul sau deteriorarea dispozitivelor criptografice securizate care stochează certificatele digitale, folosirea neautorizata a acestora sau pentru orice fel de neglijenta a Utilizatorului in păstrarea si utilizarea acestora.

9.8. Despăgubiri

DigiSign nu își asumă răspunderea financiară pentru utilizarea necorespunzătoare a certificatelor emise, a listelor CRL sau a altor servicii furnizate.

9.9. Încetare

Acest CPP este în vigoare până la publicarea unei noi versiuni la adresa www.digisign.ro. Modificările aduse acestui document sunt marcate corespunzător prin schimbarea versiunii și a ediției, după caz.

9.10. Comunicări și notificări individuale

Toate comunicările și notificările care ar putea să fie sau sunt necesare a fi date în conformitate cu acest CPP, se vor face în scris și vor fi publicate la adresa www.digisign.ro. Notificările individuale pot fi date după cum urmează:

- Servicii poștale sau de curierat, cu confrimare de primire
- Personal
- Prin e-mail, semnat cu semnătură electronică calificată sau sigiliu calificat, dacă este necesar.

9.9. Procedura de rezolvare a disputelor

Părțile contractante vor încerca rezolvarea oricăror dispute pe calea amiabilă, folosindu-se de orice instrumente de negociere și mediere de care dispun, conform legislației aplicabile în vigoare.

Orice dispută care nu poate fi rezolvată pe cale amiabilă, va fi adresată instanțelor judecătorești compentente din București.

9.10. Legea aplicabilă

Acest CPP se supune legislației naționale aplicabile.

9.11. Conformitatea cu legislația aplicabilă

Serviciile de încredere calificate furnizate de DigiSign sunt în conformitate cu Regulamentul eIDAS și legislația națională aplicabilă. Conformitatea este susținută de certificarea și acreditarea în acest sens a DigiSign ca și prestator de servicii de încredere calificate, de către Organismul de Supraveghere național.

10. Standarde și recomandări

Internet Engineering Task Force (IETF) recommendations:

- **RFC 2822 –** Internet Message Format;
- **RFC 1778** – The String Representation of Standard Attribute Syntaxes;
- **RFC 3647** – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- **RFC 6960** – X.509 Internet Public Key Infrastructure Online certificate Status Protocol – OCSP;
- **RFC 3739** – Internet X.509 Public Key Infrastructure – Qualified certificate Profile;
- **RFC 3161** – Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP). updated by RFC 5816;
- **RFC 5280** – Internet X.509 Public Key Infrastructure certificate and Certificate Revocation List (CRL) Profile);
- **RFC 6818** – Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile;

International Telecomunication Union (ITU), X series recommendations:

- **X.500 –** Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services;
- **X.501** – Information technology - Open Systems Interconnection - The Directory: Models;
- **X.509 V.3** – Certificate Profile for Certificates Issued to Natural Persons;
- **X.520** – Information technology - Open Systems Interconnection - The Directory: Selected attribute types;

Standardele PKCS ale RSA:

- **PKCS#1 –** RSA Cryptography Standard - Definește proprietățile matematice și formatul RSA al cheilor publice și private (ASN.1 codificate în text clar), algoritmii

de bază și schemele de codificare / padding pentru efectuarea criptării și decriptării RSA, generării și verificării semnăturilor;

- **PKCS#7 –** Cryptographic Message Syntax Standard - Folosit pentru semnarea și/sau criptarea mesajelor unei infrastructuri de chei publice. Utilizat și pentru propagarea certificatelor (de exemplu, ca răspuns la un mesaj PKCS # 10). A constituit baza pentru S/MIME, care din 2010 se întemeiază pe RFC 5652, un standard actualizat Cryptographic Message Syntax (CMS). Adesea folosit pentru single sign-on;
- **PKCS#10** – Certification Request Syntax Standard – Formatul mesajelor trimise către Autoritatea de Certificare pentru a solicita certificarea unei chei publice;
- **PKCS#11** – Cryptographic Token Interface – De asemenea cunoscut ca și "Cryptoki". Un API ce defineste o interfață generică pentru dispozitivele criptografice token (vezi de asemenea Modulul de Securitare Hardware). Adesea utilizat pentru single sign-on, Public-key cryptography si disk encryption systems. Dezvoltarea ulterioară a standardului PKCS#11 a fost predată către Comitetul Tehnic OASIS PKCS 11;
- **PKCS#12** – Personal Information Exchange Syntax – Definește formatul unui fișier utilizat în mod obișnuit pentru a stoca cheile private asociate cu certificate de chei publice, protejate de o cheie simetrică bazată pe parolă. PFX este un predecesor al PKCS#12. Acest container poate conține mai multe obiecte încorporate, cum ar fi mai multe certificate. De obicei protejate/criptate cu o parolă. Utilizat ca format pentru Java key Store și pentru a stabilii certificate de autentificare a clienților în Mozilla Firefox. Folosit de către Apache Tomcat.

Other standards:

- **ETSI TS 102 023 –** Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities;
- **ETSI TS 102 042 –** Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates;
- **ETSI TS 101 456** – Electronic Signatures and Infrastructures (ESI); Policy and requirements for certification authorities issuing qualified certificates;
- **ETSI EN 319 411-1** - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
- **ETSI EN 319 411-2** - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- **ETSI EN 319 421** - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- **ISO/IEC 11770-1** – Information technology - Security techniques - Key management - Part 1: Framework.
- **ISO/IEC 13335** – Information technology -- Security techniques -- Management of information and communications technology security.
- **ISO/IEC 15408-1:2005** – Security techniques/Evaluation criteria for IT security/ Part 1: Introduction;
- **ISO/IEC 15408-2:2005** – Security techniques/Evaluation criteria for IT security/ Part 2: Security functional requirements;
- **ISO/IEC 15408-3:2005** – Security techniques/Evaluation criteria for IT security/ Part 3: Security assurance requirements;
- **ISO/IEC 27001:20013** – Information technology – Security techniques – Information security management systems – Requirements.
- **ISO/IEC 27002:20013 –** Information technology – Security techniques – Information security management systems – Code of Practice for Information Security Management;

- **FIPS 140-2** – Security Requirements for Cryptographic Modules
- **CEN CWA 14167** – Security Requirements for Trustworthy Systems Managing certificates for Electronic Signatures;
- **CC EAL 4+** – Common Criteria for Information Technology Security Evaluation