simplifi

Politica de Servicii de Încredere

pentru emiterea certificatelor calificate pentru semnături electronice și sigilii, precum și pentru gestionarea dispozitivelor de creare a semnăturilor și sigiliilor la distanță și a serviciilor de marcare temporală

Această Politică de Servicii de Încredere definește principiile generale, angajamentele și cadrul de guvernanță în baza cărora Simplifi, în calitate de Furnizor Calificat de Servicii de Încredere (QTSP), furnizează servicii de încredere calificate securizate și conforme. Aceste servicii includ emiterea și gestionarea ciclului de viață al semnăturilor electronice calificate, sigiliilor electronice calificate și marcajelor temporale electronice calificate, în conformitate cu standardele și legislația aplicabilă. Politica stabilește cadrul de încredere și descrie angajamentele Simplifi privind securitatea, transparența, conformitatea legală și protecția datelor cu caracter personal. Ea reprezintă fundamentul pentru toate documentele subordonate, inclusiv Declarația de Practici de Certificare (CPS), Politicile Serviciilor de Încredere și manualele procedurale care reglementează rolurile de încredere, sistemele criptografice și verificarea identității. Prin această politică, Simplifi își afirmă responsabilitatea de a opera cu integritate, de a aplica cele mai bune practici în managementul PKI și de a menține încrederea abonaților, a părților interesate care se bazează pe servicii, a autorităților de reglementare și a publicului în serviciile de încredere furnizate.

www.simplifi.ro

Informații despre Document

Versiune	1.0
Data versiunii	1 Septembrie 2025
Aprobat de	Comitetul de Management al Politicilor și Procedurilor
Deținătorul documentului	Manager Servicii de Încredere
Numele documentului	Politica de Servicii de Încredere Simplifi pentru emiterea certificatelor calificate pentru semnături electronice și sigilii și pentru gestionarea dispozitivelor de creare a semnăturilor și sigiliilor la distanță și a serviciilor de marcare temporală
OID Document	1.3.6.1.4.1.63578.1.1.1
Clasificare Document	Public

Istoric document

Versiune	Data intrării în vigoare	Motiv	Autor
V 1.0	2025-09-01	Publicare inițială	Manager Servicii de Încredere

Istoric aprobare

Versiune	Data aprobării	Nume approbator
V 1.0	2025-09-01	Comitetul de Management al Politicilor și Procedurilor

Istoric distribuire

Versiune	Data distribuirii	Distribuit de
V 1.0	2025-09-01	Manager Servicii de Încredere

Cuprins

1. Introducere

1.1. Domeniu de aplicare

Politica de Servicii de Încredere Simplifi — care acoperă emiterea certificatelor calificate pentru semnături electronice și sigilii, precum și gestionarea dispozitivelor de creare a semnăturilor și sigiliilor la distanță și a serviciilor de marcare temporală — împreună cu Declarația de Practici de Certificare Simplifi, formează setul de politici și practici care guvernează serviciile de încredere ale Simplifi și asigură conformitatea cu reglementările în vigoare.
Pe parcursul acestui document:

- termenul „Politică” sau „Politica de Servicii de Încredere” se referă la prezentul document,
- termenul „Declarație de Practici” se referă la Declarația de Practici de Certificare Simplifi.

Acest document completează Declarația de Practici prin includerea următoarelor elemente specifice:

- mecanisme de identificare și autentificare în contextul solicitării de certificat,
- descrierea ciclului de viață al certificatului,
- furnizarea serviciului de marcare temporală,
- practici pentru gestionarea și protecția materialului criptografic pentru autoritățile de certificare și utilizatorii finali,
- profiluri pentru certificate, CRL și OCSP.

Formatul și conținutul Politicii urmează recomandările RFC 3647. Prezentul document respectă standardele specificate în Declarația de Practici.

1.2. Numele documentului și identificare

Numele complet al acestui document este Politica de Servicii de Încredere Simplifi pentru emiterea certificatelor calificate pentru semnături electronice și sigilii și pentru gestionarea dispozitivelor de creare a semnăturilor și sigiliilor la distanță și a serviciilor de marcare temporală. Documentul este disponibil în versiune electronică la: https://simplifi.ro/policies/

Prezentul document definește politica de servicii de încredere pentru emiterea:

- certificatelor calificate pentru semnături electronice calificate,
- certificatelor calificate pentru sigilii electronice calificate,
- certificatelor pentru servicii de marcare temporală electronică.

Următorul tabel arata conformitatea cu politicile definite în standardele ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI TS 119 431-1, ETSI EN 319 421

Politica	Identificator	OID	Conformitate
QCP-n-qscd	Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2	0.4.0.194112.1.2	Certificate pentru semnături electronice calificate pe un Dispozitiv Calificat de Creare a Semnăturii (QSCD)
QCP-l-qscd	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)	0.4.0.194112.1.3	Certificate pentru sigilii electronice calificate pe un Dispozitiv Calificat de Creare a Sigiliului (QSCD)
BTSP	itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)	0.4.0.2023.1.1	Certificate pentru mărci temporale calificate
EUSCP	itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3)	0.4.0.19431.1.1.3	Componentă de Serviciu de Semnare la Distanță conform cerințelor UE

1.3. Participanți PKI

1.3.1. Autoritatea de certificare

În cadrul acestei politici, sunt diferențiate autoritățile de certificare subordonate, care deservesc emiterea certificatelor calificate pentru semnături electronice calificate.

Toate autoritățile de certificare subordonate sunt operate de Simplifi sub **Simplifi Root CA [G1]**.

Simplifi Root CA [G1] emite certificate pentru toate autoritățile de certificare subordonate.

- **Simplifi Qualified CA Class 3 G1**

Certificatele calificate pentru semnătura electronică sunt emise în conformitate cu politica **QCP-n-qscd** definită în standardul **ETSI EN 319 411-2**.

Certificatele calificate pentru sigiliul electronic sunt emise în conformitate cu politica **QCP-l-qscd** definită în standardul **ETSI EN 319 411-2**.

Certificatele calificate pentru semnătura electronică (persoană fizică care reprezintă o persoană juridică) sunt emise în conformitate cu politica **QCP-qscd** definită în standardul **ETSI EN 319 411-2**.

Cheile private pentru semnătura electronică sau sigiliul electronic sunt stocate într-un **QSCD** la distanță (Remote Qualified Signature Creation Device), administrat de Simplifi.

Certificatele pentru unitatea de marcare temporală electronică (**Time-Stamping Service Unit – TSU**) sunt emise în scopuri TSA, în conformitate cu cerințele generale ale standardului **ETSI EN 319 411-1**.

Lista autorităților de certificare de mai sus poate fi extinsă în versiunile următoare ale prezentului document.

1.3.2. Autoritățile de înregistrare

O Autoritate de Înregistrare (RA) acționează în numele Autorității de Certificare (CA) pentru a efectua funcții critice de verificare a identității și de procesare a cererilor de certificat. RAs sunt responsabile pentru a se asigura că cererile de certificate sunt depuse de persoane sau entități identificate și autorizate corespunzător.

Simplifi poate opera propria Autoritate de Înregistrare sau poate delega funcțiile RA către terți autorizați, inclusiv furnizori calificați de servicii de identificare electronică și alte entități care îndeplinesc cerințele stabilite prin legislația aplicabilă a Uniunii Europene și a României. Acești terți acționează pe baza unor acorduri formale cu Simplifi și operează în conformitate cu politicile Simplifi, prezenta Declarație de Practici și reglementările aplicabile serviciilor de încredere.

1.3.3. Puncte de Înregistrare

Un punct de înregistrare autorizat este o persoană juridică. În cadrul fiecărui punct de înregistrare, sunt desemnați reprezentanți autorizați (persoane fizice) pentru a efectua validarea inițială a identității.

Acești reprezentanți sunt desemnați formal, instruiți corespunzător și acționează în conformitate cu procedurile stabilite.

1.3.4. Serviciul de Înregistrare

Serviciul de înregistrare reprezintă un serviciu online pentru colectarea și validarea mijloacelor de identificare, în vederea validării inițiale a identității. Acesta asigură conformitatea cu procesul intern adoptat de Simplifi, utilizând mecanismele necesare pentru verificarea atât a persoanei, cât și a documentului de identitate prezentat.

Procesul aplicabil poate include următoarele elemente — sau o combinație selectată dintre acestea — pentru a garanta nivelul de securitate necesar:

- Verificare video live: subiectul se conectează cu un agent în timp real, prezintă documentul de identitate și efectuează acțiuni specifice (de exemplu: mișcări ale capului, repetarea unei fraze).
- Verificare automată a documentului și a biometriei: sistemul scanează documentul de identitate (ex. OCR, verificarea elementelor de securitate) și compară fotografia cu fața subiectului (verificare în timp real și potrivire).
- Citirea datelor din stratul electronic al documentului (ex. NFC): pentru cărți de identitate electronice sau pașapoarte cu cip, datele sunt citite și comparate cu surse de date externe.

1.3.5. Autoritatea de Marcare Temporală (TSA)

Simplifi furnizează servicii de marcare temporală utilizate exclusiv în scopul generării de jetoane de marcare temporală (time-stamp tokens). Simplifi operează ca o Autoritate de Marcare Temporală (TSA), care răspunde cererilor de marcă temporală provenite de la abonați (ex. aplicații client) ca parte a unei infrastructuri extinse de servicii de încredere.

TSA este responsabilă de operarea uneia sau mai multor Unități de Marcare Temporală (TSU), care creează și semnează jetoanele de marcă temporală în numele TSA. Toate TSU-urile utilizează certificate emise de Simplifi Qualified CA Class 3.

1.3.6. Subiecți și abonați

Subiectul este definit ca entitatea identificată în certificat ca deținător al cheii private. Tipurile posibile de subiecți includ:

- o persoană fizică,
- o persoană juridică,
- o persoană fizică identificată în asociere cu o persoană juridică.

Abonatul intră într-o relație contractuală cu Simplifi în baza unui acord de abonament. De regulă, abonatul este titularul certificatului (subiectul), dar poate acționa și în numele unui alt subiect atunci când solicită un certificat.

Atât persoanele fizice, cât și entitățile juridice pot fi abonați ai Simplifi.

Un **abonat** este, de asemenea, entitatea care solicită mărci temporale din partea serviciului TSA.

1.3.7. Entități partenere

O entitate parteneră a serviciului este o persoană fizică sau juridică ce se bazează pe serviciile de încredere furnizate de Simplifi.

1.3.8. Serviciul de semnare pe server

Simplifi furnizează un serviciu care utilizează o soluție de semnare pe server pentru a crea semnături sau sigilii electronice în numele subiectului.

1.3.9. Alți participanți

Aspectele specifice acestui punct sunt detaliate în Declarația de Practici.

1.4. Utilizarea certificatelor

Simplifi emite următoarele tipuri de certificate:

- certificate calificate pentru semnături electronice,
- certificate calificate pentru sigilii electronice.

Acestea sunt emise entităților care au acceptat termenii și condițiile, împreună cu prevederile stabilite în documentele relevante, precum Declarația de Practici (Practice Statement) și această Politică de Servicii de Încredere.

Există următoarele tipuri de certificate și domeniile lor de aplicabilitate:

a) **Persoană juridică**

Certificate calificate pentru sigilii electronice – certificatele sunt emise persoanelor juridice.Un certificat calificat pentru sigiliu electronic include cel puțin denumirea țării, denumirea subiectului (persoana juridică), numărul de înregistrare, denumirea comună a entității juridice (common name), numărul și seria certificatului.

b) **Persoană fizică reprezentând o persoană juridică**

Certificate calificate pentru semnături electronice – certificatul conține cel puțin denumirea țării, numele subiectului (persoana fizică reprezentând persoana juridică), numărul și seria certificatului, denumirea organizației asociate persoanei fizice.

c) **Persoană fizică**

Certificate calificate pentru semnături electronice – certificatul conține cel puțin denumirea țării, numele subiectului (persoana fizică), seria și numărul certificatului.

Următorul tabel prezintă relația dintre fiecare tip de certificat emis de Simplifi și politica specifică reglementată prin prezentul document:

Tip	Scop	Suport media	Identificator politică	OID Politică ETSI
Persoană juridică	Sigiliu electronic calificat	QSCD la distanță (Remote QSCD)	QCP-l-qscd	0.4.0.194112.1.3
Persoană fizică reprezentând persoană juridică	Semnătură electronica calificată	QSCD la distanță (Remote QSCD)	QCP-n-qscd	0.4.0.194112.1.2
Persoană fizică	Semnătură electronica calificată	QSCD la distanță (Remote QSCD)	QCP-n-qscd	0.4.0.194112.1.2

1.4.1. Utilizări permise ale certificatului

Utilizarea certificatelor emise pentru **persoane juridice** este limitată la crearea de **sigilii electronice calificate** de către persoana juridică și la validarea acestora de către entitățile partenere.

Utilizarea certificatelor de semnătură electronică emise pentru o **persoană fizică ce reprezintă o persoană juridică** este destinată să permită acțiuni cu efect juridic obligatoriu, în care un individ acționează în numele unei organizații. Astfel de certificate sunt limitate la crearea de semnături electronice calificate de către persoana fizică, în cazurile în care efectul juridic al semnăturii este destinat să angajeze persoana juridică reprezentată.

Certificatul personal pentru utilizare în semnături electronice este limitat la crearea de **semnături electronice calificate** de către persoana fizică și la validarea acestora de către entitățile partenere.

1.4.2. Utilizări interzise ale certificatului

Certificatele trebuie utilizate strict în conformitate cu scopul declarat și domeniul de aplicare autorizat. Utilizarea acestor certificate cu încălcarea legislației aplicabile este în mod expres interzisă.

Emiterea certificatului nu constituie o declarație sau garanție privind încrederea în titular, practicile sale comerciale sau starea sistemului asociat, inclusiv absența programelor malițioase (malware) sau a vulnerabilităților.

1.5. Administrarea Politicii

1.5.1. Organizația responsabilă pentru gestionarea acestui document

Această Politică de Servicii de Încredere este gestionată de Simplifi:

Strada Gheorghe Țițeica 142, București 014192, Romania

1.5.2. Contact

easy@simplifi.ro

1.5.3. Entități care determină validitatea principiilor conținute în document

Echipa **Simplifi** este responsabilă pentru evaluarea completitudinii și acurateței prezentului document, precum și a altor documente asociate serviciilor PKI furnizate de Simplifi, precum și pentru asigurarea coerenței acestora. Toate întrebările și comentariile referitoare la conținutul acestor documente trebuie adresate la adresa specificată în **capitolul 1.5.2**.

1.5.4. Proceduri de aprobare

Prezentul document rămâne în vigoare începând cu data specificată ca dată de adoptare, până la publicarea unei versiuni valide ulterioare.

Părțile afectate pot transmite comentarii privind modificările propuse în termen de 14 zile lucrătoare de la anunțarea acestora, conform prevederilor din capitolul 9.10 al Declarației de Practici Simplifi (Simplifi Practice Statement). Dacă în acest interval nu sunt formulate obiecții semnificative privind conținutul substanțial, noua versiune a Declarației de Practici devine efectivă la data indicată în document.

Aprobarea noii versiuni a Declarației de Practici este responsabilitatea managementului Simplifi. Toate modificările sunt înregistrate în istoricul documentului.

Documentul aprobat este apoi publicat și comunicat către:

- angajați,
- roluri de încredere desemnate,
- entități partenere
- subiecți și abonați,
- alte entități participante definite în capitolul 1.4.5 al Declarației de Practici de Certificare Simplifi.

1.6. Definiții și Abrevieri

Definițiile și abrevierile utilizate în prezentul document pot fi consultate în Declarația de Practici de Certificare Simplifi (Simplifi Certification Practice Statement).

2. Publicare și responsabilități Depozitar

2.1. Depozitare

Simplifi deține un depozitar disponibil online, ce conține:

- documentele disponibile public, împreună cu versiunile anterioare, la adresa: *https://simplifi.ro/policies/*.
- toate certificatele publicate, atât cele active, cât și cele revocate (inclusiv Lista de Revocare a Certificatelor), la adresa: *http://simplifi.ro/pki.*
- Raspuns OCSP, la adresa : http://simplifi.ro/*ocsp*

Depozitarul este destinat următoarelor entități: subiecți, abonați, entități partenere.

2.2. Informațiile publicate de Simplifi

Depozitarul conține următoarele documente:

- Declarația de Practici de Certificare– versiunea curentă și versiunile anterioare,
- Politicile Serviciilor de Încredere – versiunea curentă și versiunile anterioare,
- Termenii și Condițiile Generale,
- Profilurile certificatelor, ale listelor de revocare a certificatelor (CRL) și ale răspunsurilor OCSP
- Toate certificatele publicate, atât active cât și revocate
- Listele de Revocare a Certificatelor,
- Raspunsurile OCSP
- Informații suplimentare, în baza deciziilor interne ale Simplifi, de exemplu notificări privind incidente semnificative.

Depozitarul păstrează atât versiunile curente, cât și versiunile istorice ale acestor documente electronice.

2.3. Frecvența publicării

Documentele sunt publicate cu următoarea frecvență:

- Declarația de Practici și politicile specifice ale serviciilor de încredere – conform capitolului 9.10 din Declarația de Practici de Certificare Simplifi,
- Certificatele tuturor autorităților care operează servicii de încredere în cadrul Simplifi – la fiecare emitere a unui certificat nou,
- Lista de Revocare a Certificatelor (CRL) – conform prevederilor din Politica specifică a Serviciului de Încredere și profilul certificatului.

2.4. Accesul la documentele publicate

Simplifi aplică măsuri de securitate logice și fizice pentru a proteja depozitarul împotriva oricărei creări, ștergeri sau modificări neautorizate de date.

3. Identificare și Autentificare

Simplifi se asigură că metodele de verificare a identității utilizate sunt conforme cu cerințele Articolului 24 din Regulamentul (UE) 910/2024, în special pe baza uneia dintre următoarele metode sau, atunci când este necesar, a unei combinații între acestea:

- Art. 24.1a(a): verificarea identității se bazează pe un mijloc de identificare electronică notificat, cu un nivel de asigurare ridicat;
- Art. 24.1a(b): verificarea identității se bazează pe un certificat calificat emis în conformitate cu prevederile Art. 24.1a(a), 24.1a(c) sau 24.1a(d);
- Art. 24.1a(c): verificarea identității utilizează o metodă confirmată de un organism de evaluare a conformității, așa cum este descris în secțiunea 3.2.2;
- Art. 24.1a(d): verificarea identității este efectuată de un Ofițer de Înregistrare, pe baza unei vizite fizice a solicitantului certificatului la un Punct de Înregistrare.

Simplifi elaborează și menține proceduri documentate pentru verificarea și autentificarea identității clienților care solicită certificate și asigură implementarea acestora în conformitate cu cerințele legale și de reglementare aplicabile.

3.1. Nume

3.1.1. Tipuri de nume

În conformitate cu standardul X.509, certificatele conțin informații despre emitent și subiect, identificați prin nume distinctive corespunzătoare.

3.1.2. Nevoia ca Numele să aibă înțeles logic

Numele distinctiv al subiectului este unic pentru toate serviciile de încredere și serviciile de identificare electronică furnizate de Simplifi. Fiecare valoare inclusă în secțiunea de informații despre subiect a certificatului este relevantă și a fost inclusă în mod intenționat.

Secțiunea 3.1.4 specifică datele obligatorii din certificat necesare pentru a asigura identificarea neechivocă a subiectului.

3.1.3. Anonimatul subiectului

Utilizarea pseudonimelor pentru identificarea subiectului nu este permisă în cadrul certificatelor emise.

3.1.4. Reguli pentru interpretarea diferitelor denumiri

Interpretarea câmpurilor de denumire incluse în certificate este conformă cu standardul ETSI EN 319 412 (Părțile 1, 2, 3).

Atributele numelui distinctiv (componentelor DN) din certificate sunt interpretate după cum urmează:

Componentă DN	Interpretation
givenName	Prenumele persoanei fizice. - Conform dovezii utilizate pentru identificare. Se utilizează numai pentru persoane fizice sau personae fizice care reprezintă o persoană juridică
Sn **(surname)**	Numele de familie al persoanei fizice. - Conform dovezii utilizate pentru identificare. Se utilizează numai pentru persoane fizice sau persoane fizice care reprezintă o persoană juridică.
Cn **(commonName)**	Nume comun: sunt utilizate următoarele variante: - Pentru persoane fizice fără pseudonim: „prenume nume”; - Pentru persoane juridice: denumirea oficială a entității juridice (companie, autoritate publică, asociație etc.), redusă la o formă semnificativă dacă este necesar, în cazul depășirii limitei maxime de 64 de caractere.
serialNumber **(serial number)**	Seria și numărul: identificatorul unic al persoanei fizice. Identificatorul pentru o persoană fizică este, de exemplu: - PNORO-1234567890123, sau IDCRO-DZ123456, sau TINRO-1234567890123, pentru identificarea bazată pe codul din Cartea de Identitate Electronică, recunoscut la nivelul Uniunii Europene, conform punctului 5.1.3 din ETSI TS 119 412-1.
O **(organizationName)**	Denumirea oficială a abonatului sau denumirea persoanei juridice (inclusiv forma juridică) de care aparține subiectului sau cu care acesta este afiliat (companie, autoritate publică, asociație etc.), conform dovezii existenței legale; dacă este necesar, denumirea poate fi redusă la o formă semnificativă în cazul depășirii limitei maxime de 64 de caractere. Se utilizează numai pentru persoane juridice sau persoane fizice care reprezintă o persoană juridică.

Componentă DN	Interpretation
OrgID (organizationIdentifier)	Identificator neechivoc al persoanei juridice. Identificatorul pentru o persoană juridică este, de exemplu: - NTRRO-12345678, pentru identificarea bazată pe un identificator din Oficiul Național al Registrului Comerțului (ONRC), recunoscut la nivelul Uniunii Europene conform punctului 5.1.4 din ETSI TS 119 412-1. Se utilizează numai pentru persoane juridice sau persoane fizice care reprezintă o persoană juridică.
C **(countryName)**	Identificarea țării care trebuie menționată corespunde standardului ISO 3166 și este stabilită după cum urmează: Abrevierea internațională pentru numele țării (ex. RO pentru România).

1) *Certificatele electronice calificate pentru persoane fizice includ, cel puțin, următoarele componente DN: "cn", "c", "serialNumber", "givenName" și "surname".*
2) *Certificatele electronice calificate pentru persoane fizice ce reprezintă persoane juridice includ, cel puțin, următoarele componente DN:: "cn", "c", "serialNumber", "givenName", ''surname", "o" și "orgID".*
3) *Certificatele pentru sigiliile calificate pentru persoanele juridice includ, cel puțin, următoarele componente DN: "cn", "c", "o" și "orgID".*

Pot fi adăugate și alte componente suplimentare.
Orice componentă DN suplimentară trebuie să fie conformă cu RFC 5280, RFC 6818 și ETSI EN 319 412.

3.1.5. Unicitatea denumirilor

Simplifi asigură unicitatea certificatelor emise. În consecință:

- Fiecare pereche **commonName** și **serialNumber** este atribuită în mod exclusiv unei singure persoane fizice;
- Fiecare pereche **commonName** și **organizationIdentifier** este asociată în mod unic unei singure persoane juridice.

3.1.6. Recunoașterea, autentificarea si rolul mărcilor comerciale

Simplifi exclude mărcile comerciale din câmpurile subiectului certificatului. Utilizarea oricărui nume fără dovada clară a deținerii de către abonat este strict interzisă.Simplifi nu își asumă nicio responsabilitate privind soluționarea disputelor legate de deținerea legală a denumirilor, mărcilor comerciale sau a altor identificatori comerciali.

3.2. Validarea inițială a identității

Înregistrarea pentru serviciile Simplifi necesită un proces inițial de verificare a identității, în scopul emiterii de semnături electronice și mijloace de identificare electronică.

Acest proces de înregistrare presupune colectarea datelor de identificare și oferă solicitantului posibilitatea de a se prezenta pentru verificare înainte de emiterea certificatului.

Verificarea inițială a identității se aplică următoarelor categorii:

- persoanelor fizice;
- persoanelor fizice care acționează în numele unei persoane juridice;
- persoanelor juridice.

Înainte de inițierea procedurii de verificare a identității, subiectul trebuie să analizeze și să accepte Termenii și Condițiile de Utilizare și prezenta Politică.

3.2.1. Metoda de dovedire a posesiei cheii private

Simplifi confirmă faptul că subiectul deține sau controlează cheia privată corespunzătoare cheii publice care urmează să fie certificată, prin verificarea semnăturii digitale din cererea de certificat, care trebuie să fi fost generată utilizând acea cheie privată.

3.2.2. Autentificarea unei persoane juridice

Identificarea și autentificarea persoanei juridice se realizează exclusiv în scopul emiterii unui certificat calificat pentru sigiliu electronic.

Reprezentantul autorizat al Punctului de Înregistrare are obligația de a verifica identitatea persoanei juridice și legătura de reprezentare asociată (persoana fizică).

Procedura constă în două părți:

1) Verificarea persoanei juridice include:

- denumirea completă a persoanei juridice,
- țara în care este înregistrată persoana juridică,
- un identificator unic și tipul acestuia (număr din Registrul Comerțului sau cod fiscal – VAT).

Sursa principală de date pentru verificarea persoanei juridice este Registrul Comerțului (Registrul Entităților Juridice din România).

2) Verificarea reprezentantului autorizat (persoană fizică) include:

- calitatea legală de reprezentare,
- denumirea completă și statutul juridic al persoanei juridice reprezentate,
- verificarea rolului și a autorizării persoanei de a acționa în numele persoanei juridice,
- numele complet al persoanei fizice (givenName și surname),
- data și locul nașterii,
- verificarea documentului de identitate.

Dovezile primare pentru verificarea reprezentării pot include:

- o împuternicire legală valabilă,
- validarea semnăturii aplicate pe documente de către o persoană autorizată,
- confirmarea calității de reprezentant prin intermediul bazelor de date guvernamentale.

Validarea identității persoanei fizice în calitate de reprezentant autorizat se realizează în conformitate cu secțiunea 3.2.3.

Identitatea și existența juridică a organizației trebuie revalidate la fiecare 6 ani, începând cu data emiterii primului certificat calificat emis conform prezentei Politici.

3.2.3. Autentificarea unei persoane fizice

Ori de câte ori este necesară identificarea unei persoane fizice pentru emiterea unui certificat sau a unui mijloc de identificare electronică, aceasta se realizează conform procedurii descrise mai jos.

Autoritatea de Înregistrare asigură validarea identității persoanei fizice prin următoarele scenarii:

- **În persoană**: prin prezența fizică a solicitantului la un Punct de Înregistrare, unde dovezile de identitate sunt colectate și verificate de un reprezentant autorizat;
- **De la distanță**): verificarea identității este efectuată în principal de Autorități de Înregistrare de Încredere externe, autorizate de Autoritatea pentru Digitalizarea României (ADR).

Scenariul „în persoană” impune ca subiectul să prezinte unul sau mai multe documente originale de identitate valabile (carte de identitate sau pașaport).

Reprezentantul autorizat al Punctului de Înregistrare poate solicita verificarea autenticității, integrității și confirmarea faptului că documentul prezentat corespunde solicitantului (subiectului).

Scenariul „la distanță” impune ca subiectul să dețină fie un mijloc de identificare electronică notificat emis anterior, fie să prezinte documentul de identitate prin intermediul unui proces de identificare video.

Metodele acceptate în prezent sunt:

- ROeID – mijlocul de identificare electronică notificat al României;
- procesul de identificare video la distanță, furnizat de un prestator extern, care permite verificarea elementelor de securitate ale documentelor de identitate prezentate și validarea corespondenței dintre persoana fizică și documentele acesteia;
- combinația celor două metode (ROeID și procesul de identificare video).

Validarea mijloacelor de identificare electronică este efectuată prin serviciile de înregistrare operate de Autoritatea de Înregistrare.

Fiecare dintre aceste metode asigură că sunt colectate și validate doar datele necesare pentru emiterea certificatului.

Toate dovezile și atestările sunt colectate de Autoritatea de Înregistrare în conformitate cu următoarele principii:

- Identitatea subiectului este verificată în momentul înregistrării;
- Sunt colectate dovezi pentru următoarele date:
    - numele complet (inclusiv prenumele și numele de familie);
    - data și locul nașterii;
    - seria documentului de identitate (dacă este aplicabil);
    - codul numeric personal (CNP);
    - adresa de înregistrare

Autoritatea de Înregistrare înregistrează și păstrează datele de identitate ale tuturor subiecților înregistrați.

3.2.4. Authentificarea unei persoane fizice care reprezintă o entitate juridică

Validarea identității persoanei fizice în calitate de reprezentant autorizat se realizează în conformitate cu secțiunea 3.2.3.

3.2.5. Informații neconfirmate

Certificatul nu conține nicio informație neconfirmată.

3.2.6. Criterii de interoperabilitate

Nu e aplică.

3.3. Identificare și autentificare pentru cererile de reînnoire a cheii

Certificarea și reînnoirea cheii (actualizarea perechii de chei) pot fi inițiate de către subiect în următoarea condiție:

- existența unei cereri de reînnoire (rekey) pentru un certificat activ și neexpirat.

În astfel de cazuri, subiectul trebuie să depună o cerere care să includă solicitarea de generare a unei noi perechi de chei și de emitere a unui nou certificat. Cererile trebuie autentificate prin verificarea unui document semnat digital, semnat de către subiect utilizând cheia privată asociată certificatului curent valabil (neexpirat).

Pentru a facilita reînnoirea în timp util, un e-mail de notificare va fi trimis subiectului cu 45 de zile înainte de expirarea certificatului. Acest mesaj îl va informa cu privire la apropierea termenului de expirare și va descrie pașii necesari pentru finalizarea procesului.

Subiectul poate utiliza ulterior o interfață online pentru a continua procedura. Acest proces impune ca subiectul să își confirme identitatea prin semnarea digitală cu certificatul aflat în curs de expirare.

3.4. Identificare si autentificare pentru cererile de revocare

Cererile de revocare pot fi transmise de subiect, abonat, reprezentanți autorizați, Autoritatea de Înregistrare sau alte roluri de încredere, utilizând canalele definite în Secțiunea 4.9.3.

În funcție de metoda de transmitere, identitatea solicitantului este autentificată după cum urmează:

- **Portalul Simplifi**: subiectul se autentifică utilizând credențialele contului înainte de a trimite cererea de revocare;
- **Cerere semnată**: o cerere de revocare semnată cu o semnătură electronică calificată sau un sigiliu electronic calificat este considerată autentică dacă identitatea semnatarului corespunde subiectului certificatului sau abonatului autorizat;
- **În persoană**: identificarea este realizată pe baza documentelor oficiale de identitate prezentate Autorității de Înregistrare;
- **Canale neautentificate** (de exemplu, e-mail simplu sau formular web): Autoritatea de Înregistrare încearcă să verifice identitatea solicitantului utilizând informațiile de contact furnizate; dacă verificarea eșuează, certificatul poate fi suspendat temporar până la clarificarea situației.

Autoritatea de Înregistrare (RA) este responsabilă de confirmarea legitimității cererii de revocare înainte de executarea acesteia. Procedurile detaliate, inclusiv canalele acceptate și mecanismele de verificare a identității, sunt descrise în Secțiunea 4.9.3.

4. Cerințe operaționale privind ciclul de viață al certificatului

4.1. Cererea de emitere a certificatului

4.1.1. Cine poate depune o cerere pentru emiterea unui certificat

Un certificate poate fi solicitat de catre o persoană fizică, o persoană juridică, sau de către o persoană fizică sau juridică in administrarea careia se află echipamentul sau sistemul pentru care este destinate certificatul.

Autoritatea de Certificare (CA) emite certificate pentru următoarele categorii:

Persoane fizice:

- Certificate personale

Persoane fizice care reprezintă o persoană juridică:

- Certificate asociate organizației reprezentate

Persoane juridice: Certificate emise direct **organizației**

Cererile de certificat pot fi depuse în persoană, la un Punct de Înregistrare. Cererea poate fi inițiată fie de către subiect, fie de către abonat.

4.1.2. Procesul de înregistrare și responsabilități aferente

Procesul de înrolare este coordonat de o entitate desemnată, denumită **Autoritate de Înregistrare (RA)**, care poate fi operată direct de către **Simplifi** sau de către terți autorizați care acționează în numele Simplifi.

Simplifi poate delega identificarea subiecților sau a abonaților către entități externe, inclusiv **furnizori de servicii de identificare la distanță** (precum ROeID, Qoobiss Ontrace sau alți furnizori conformi eIDAS, care respectă integral legislația națională privind identificarea la distanță), cu condiția ca aceștia să aplice **proceduri de identificare care oferă un nivel de încredere** echivalent celor definite pentru RA în prezenta Politică, în Declarația de Practici de Certificare (CPS) și în standardele ETSI aplicabile.

Astfel de servicii externe de identificare pot funcționa în baza:

- unor acorduri contractuale directe cu Simplifi, sau
- recunoașterii reciproce conform eIDAS, ca mijloace de identificare electronică notificate.

Indiferent de delegare, Simplifi își păstrează întreaga responsabilitate – în limitele prevăzute de prezenta Politică – pentru acțiunile sau omisiunile oricărui agent, angajat sau terț implicat în procesul de înregistrare.

Responsibilitățile Autorității de Înregistrare

Autoritatea de Înregistrare (RA) este responsabilă pentru verificarea următoarelor elemente:

- **Identitatea** declarată a subiectului și/sau abonatului;
- **Atributele** declarate (de exemplu: organizație, rol, mandat) ale subiectului și/sau abonatului;
- **Cererea** depusă pentru emiterea certificatului.

Această verificare trebuie efectuată în conformitate cu:

- Procedurile definite în prezenta politică;
- Procedurile interne ale RA stabilite de Simplifi;
- Legislația națională și europeană aplicabilă privind identificarea electronică și serviciile de încredere.

Utilizarea serviciilor de indentificare la distanță

Simplifi poate efectua verificarea identității utilizând **servicii de identificare la distanță**, în special pentru fluxuri de lucru complet digitale. Aceste servicii pot include:

- **sesiuni de identificare video,**
- **scanarea documentelor de identitate electronice (eID) cu potrivire biometrică,**
- **validarea unei semnături electronice calificate la distanță (QES-onboarding),**
- **verificări automate ale identității integrate cu scheme naționale de identificare (de exemplu, ROeID)** sau alți furnizori conformi eIDAS, care respectă în totalitate legislația națională privind identificarea la distanță.

Astfel de sesiuni de identificare pot fi:

- **inițiate de Simplifi (de exemplu, în timpul procesului online de onboarding), sau**
- **delegate integral unui furnizor de servicii de identitate, caz în care Simplifi primește datele de identitate verificate după finalizarea cu succes a procesului.**

În toate cazurile, Simplifi se asigură că metoda de identificare la distanță utilizată este conformă cu cerințele:

- ETSI EN 319 411-1 și ETSI EN 319 411-2,
- ETSI TS 119 461, atunci când este necesar,
- Regulamentului eIDAS, inclusiv Articolului 24 (1a),
- Ghidurilor emise de Autoritatea pentru Digitalizarea României (ADR).

Informațiile furnizate subiectului/ abonatului

Înainte sau în timpul procesului de înrolare, subiectului sau abonatului i se furnizează:

- Termenii și condițiile aplicabile,

- Adresa URL unde pot fi accesați termenii, condițiile și documentele aferente,
- O copie sau un link către prezenta Politică, către Declarația de Practici de Certificare (CPS) și către notificările relevante.

Prin acceptarea acestor termeni, subiectul sau abonatul recunoaște și este de acord că:

- este responsabil pentru acuratețea și completitudinea informațiilor furnizate în scopul înregistrării;
- Simplifi păstrează toate datele de înregistrare și de înrolare pentru o perioadă minimă de 10 ani de la data expirării sau revocării certificatului;
- în cazul în care Simplifi își încetează activitatea în calitate de Autoritate de Certificare (CA) sau Autoritate de Înregistrare (RA), aceste înregistrări pot fi transferate legal unui succesor sau unei terțe părți desemnate;
- a luat cunoștință de drepturile, obligațiile și responsabilitățile sale, astfel cum sunt definite de Simplifi, de acordurile aplicabile și de legislația în vigoare;
- are obligația de a informa prompt Simplifi cu privire la orice eveniment sau modificare care ar putea afecta valabilitatea certificatului.

Procedura de înrolare

Procesul de înrolare începe la nivelul Autorității de Înregistrare (RA), fie:

- direct, prin personalul RA intern al Simplifi,
- prin intermediul RA-urilor delegate,
- sau prin integrarea cu furnizori de servicii de identificare la distanță, conform descrierii de mai sus.

Autoritatea de Înregistrare (RA) este responsabilă pentru:

- colectarea și validarea documentației și a dovezilor de identitate,
- efectuarea verificărilor inițiale și finale,
- asigurarea faptului că datele de înregistrare verificate sunt complete și corecte înainte ca cererea de certificat să fie transmisă către Autoritatea de Certificare (CA).

RA poartă întreaga responsabilitate pentru corectitudinea:

- datelor de identitate care urmează a fi încorporate în certificat,
- atributelor și rolurilor declarate (de exemplu, reprezentant legal),
- nivelului de asigurare aferent procesului de identificare.

4.2. Procesarea cererii de certificat

4.2.1. Realizarea funcțiilor de identificare și autentificare

Identificarea și autentificarea subiectului sau abonatului trebuie finalizate înainte de emiterea certificatului. După ce identitatea subiectului a fost verificată cu succes, procesul de emitere a certificatului poate începe. O descriere detaliată a procedurii de validare inițială a identității este furnizată în Capitolul 3.2 al prezentei Politici.

4.2.2. Aprobarea sau respingerea cererilor de certificat

La finalizarea procesului de înregistrare, CA sau RA își rezervă dreptul de a refuza emiterea certificatului în cazuri precum: lipsa sau insuficiența informațiilor furnizate, eșecul verificărilor de consistență sau securitate ori existența unor dubii neclarificate privind identitatea subiectului sau abonatului.

4.2.3. Timpul de procesare a cererilor de certificat

Simplifi depune toate eforturile pentru a se asigura că, odată primită cererea de certificat, Autoritatea de Certificare (CA) o analizează și emite certificatul cât mai curând posibil.

4.3. Emiterea certificatului

4.3.1. Acțiunile Autorității de Certificare în timpul emiterii certificatului

După procesarea cererii de certificat și verificarea finală a datelor transmise, Autoritatea de Certificare procedează la emiterea certificatului. Fiecărui certificat i se atribuie un număr de serie unic.Perioada de valabilitate a certificatului nu va depăși perioada de valabilitate a Autorității de Certificare emitente.

4.3.2. Notificarea subiecților și abonaților de către Autoritatea de Certificare privind emiterea certificatului

Subiectul și abonatul sunt notificați cu privire la emiterea certificatului, în conformitate cu metodele stabilite în termenii și condițiile aplicabile.

4.4. Acceptarea certificatului

4.4.1. Actiuni care constituie acceptarea certificatului

Este responsabilitatea subiectului să se asigure că toate informațiile incluse în certificatul emis sunt complete, corecte și actualizate. În cazul în care subiectul descoperă orice inexactitate sau neconcordanță, acesta trebuie, fără întârzieri nejustificate, să informeze punctul de contact desemnat, menționat în clauza 1.5.2 a prezentei Politici.

Consimțământul și acceptarea sunt înregistrate în sistemele Simplifi.

4.4.2. Publicarea certificatului de către Autoritatea de Certificare (CA)

A se vedea Capitolul 2.

4.4.3. Notificarea emiterii certificatului de către Autorități de Certificare ale altor entități

Nu se aplică.

4.5. Utilizarea perechii de chei și a certificatului

4.5.1. Utilizarea cheii private și a certificatului de către abonat și/sau subiect

Subiecții sunt obligați să utilizeze cheile lor private și certificatele strict în conformitate cu:

- scopurile definite în prezentul document, în Declarația de Practici de Certificare (CPS) și în termenii și condițiile aplicabile;
- extensiile KeyUsage și extendedKeyUsage, astfel cum sunt specificate în fiecare certificat, în concordanță cu profilurile de certificat aplicabile.

În situațiile în care sunt utilizate dispozitive locale de creare a semnăturii sau credențiale de autentificare pentru activarea cheilor private, subiectul este responsabil pentru asigurarea stocării securizate a acestora și pentru protejarea împotriva accesului neautorizat.

Subiecții pot utiliza perechile de chei pentru semnare în vederea generării de semnături electronice în diverse formate acceptate.

Simplifi stochează și administrează în siguranță certificatele și cheile private corespunzătoare într-un RQSCD (Dispozitiv de creare a semnăturii la distanță calificat), care respectă toate standardele relevante aplicabile.

Serviciul de semnătură bazat pe server (sistemul de semnătură la distanță) implementează măsuri tehnice de protecție pentru a preveni utilizarea certificatelor expirate.

4.5.2. Utilizarea cheii private și a certificatului de către entități partenere

Entitatea parteneră este obligată să utilizeze certificatul și cheia publică în mod legal și în conformitate cu:

- prezenta Politică și Declarația de Practici de Certificare (CPS);
- Termenii și Condițiile aplicabile.

O entitate parteneră poate avea încredere în certificat doar dacă sunt îndeplinite toate condițiile următoare:

- certificatul este utilizat în conformitate cu scopurile permise, definite în extensiile certificatului;

- lanțul de certificare este validat complet și cu succes până la certificatul rădăcină de încredere;
- certificatul este verificat ca nefiind revocat, prin consultarea Listei de Revocare a Certificatelor (CRL) corespunzătoare sau prin confirmarea pozitivă a stării sale prin serviciul OCSP (Online Certificate Status Protocol).

4.6. Reînnoirea certificatului

Reînnoirea certificatelor utilizând aceeași pereche de chei nu este permisă. Pentru menținerea valabilității certificatului, este acceptată utilizarea mecanismului de reînnoire a cheii (Certificate Re-key) – a se vedea clauza 4.7.

4.7. Reînnoirea perechii de chei a certificatului

O actualizare a cheii (key update) este inițiată atunci când subiectul sau abonatul (acționând în numele unui subiect înregistrat anterior) solicită generarea unei noi perechi de chei și emiterea unui nou certificat care să lege identitatea subiectului de noua cheie publică. Actualizarea cheii se aplică în mod specific certificatului indicat în cerere. Certificatul nou emis păstrează conținutul originalului, cu excepția următoarelor diferențe:

- o nouă pereche de chei generată,
- un nou număr de serie,
- o nouă perioadă de valabilitate a certificatului.

4.7.1. Circumstanțele pentru reînnoirea perechi de chei

Certificarea și reînnoirea cheii (actualizarea cheii) pot avea loc atunci când subiectul solicită reînnoirea unui certificat valabil în prezent.

Dacă, pe durata perioadei de valabilitate a unui certificat, algoritmii criptografici recomandați sau parametrii aferenți utilizați de dispozitivul calificat de creare a semnăturii sau sigiliului electronic devin învechiți sau nu mai respectă standardele de securitate aplicabile, Autoritatea de Certificare (CA) poate iniția emiterea unui nou certificat calificat. Noul certificat va fi asociat unui dispozitiv calificat de creare a semnăturii și sigiliului electronic care respectă cerințele de securitate actuale.Într-un astfel de caz, subiectul va fi obligat să finalizeze procesul de reînnoire a cheii (re-key) în conformitate cu instrucțiunile furnizate de CA.

4.7.2. Cine poate solicita certificarea unei noi chei publice

Cheile sunt actualizate numai la cererea subiectului sau a abonatului și, prin urmare, procesul trebuie să fie precedat de depunerea unei cereri corespunzătoare.

4.7.3. Procesarea cererilor de reinnoire a cheii certificatului

Autoritatea de Înregistrare (RA) utilizează aceleași procese ca și în cazul unei cereri de certificat nou.

4.7.4. Notificarea abonatului privind emiterea noului certificat

Autoritatea de Înregistrare (RA) utilizează aceleași procese ca și în cazul unei cereri de certificat nou.

4.7.5. Acțiuni care constituie acceptarea unui certificat reinnoit

Autoritatea de Înregistrare (RA) utilizează aceleași procese ca și în cazul unei cereri de certificat nou.

4.7.6. Publicarea certificatului reinnoit de către CA

Nu se aplică

4.7.7. Notificarea emiterii certificatului de către CA altor entități

Nu se aplică

4.8. Modificarea certificatului

Modificarea certificatului este posibilă doar ca parte a procesului de reînnoire a cheii (re-key), descris în Capitolul 4.7.

4.9. Revocarea certificatului

Simplifi asigură disponibilitatea 24/7 a serviciilor de revocare a certificatelor.Revocarea unui certificat este echivalentă din punct de vedere juridic cu invalidarea acestuia și conduce la încetarea automată a relației contractuale dintre abonat și Simplifi.

Orice semnături electronice create după publicarea revocării sunt considerate nevalabile. După revocare, subiectului îi este strict interzis să utilizeze certificatul pentru semnături electronice, sigilii electronice sau marcare temporală.

Simplifi publică informații în timp real privind starea certificatelor atât prin intermediul Listelor de Revocare a Certificatelor (CRL), cât și prin intermediul Protocolului Online pentru Starea Certificatului (OCSP). Ambele servicii operează pe baza unei baze de date sincronizate, pentru a asigura verificarea consistentă a stării certificatelor.

4.9.1. Circumstanțe pentru revocare

Un certificat poate fi revocat în oricare dintre următoarele circumstanțe:

- Informații invalide în certificat

- Datele conținute în certificat nu mai sunt corecte sau valabile;
- Simplifi primește o notificare care indică faptul că datele din certificat sunt incorecte.

- Compromiterea cheii sau a dispozitivului
  - Cheia privată asociată certificatului sau dispozitivul securizat (QSCD/SSCD) care o stochează a fost, sau se suspectează că a fost, compromisă;
  - Cheia privată a Simplifi sau sistemele sale au fost compromise, afectând încrederea în certificatele emise.
- Încetarea serviciului sau revocare la inițiativa abonatului
  - Abonatul încetează contractul de servicii cu Simplifi;
  - Dacă abonatul nu inițiază revocarea, aceasta poate fi efectuată de Simplifi, de Autoritatea de Certificare (CA) sau de un reprezentant autorizat al organizației abonatului;
  - Revocarea este solicitată de către abonat sau subiect.
- Acțiune de supraveghere sau reglementare
  - Revocarea este solicitată de către Autoritatea de Supraveghere competentă;
  - Modificările legale, reglementare sau guvernamentale împiedică subiectul să respecte prevederile prezentei Politici.
- Neconformitate contractuală sau de politică
  - Abonatul sau organizația acestuia nu își îndeplinește obligațiile contractuale, inclusiv plata taxelor de serviciu;
  - Simplifi constată că deținătorul certificatului nu respectă prezenta Politică de Certificat sau Declarația de Practici de Certificare (CPS) aplicabilă.
- Slăbiciune criptografică sau risc
  - Algoritmii criptografici sau parametrii utilizați în certificat nu mai sunt considerați securizați, afectând legătura dintre subiect și cheia publică aferentă.
- Încetarea operațiunilor
  - Simplifi își încetează serviciile de certificare;În astfel de cazuri, toate certificatele, inclusiv certificatul propriu al Autorității de Certificare, trebuie revocate înainte de finalizarea perioadei de încetare.
- Circumstanțe extraordinare
  - Orice eveniment, precum dezastre naturale, defecțiuni de sistem sau alte incidente neprevăzute, care împiedică subiectul să își îndeplinească obligațiile conform prezentei Politici.

4.9.2. Cine poate solicita revocarea

Subiectul sau abonatul pot, la discreția lor, să solicite revocarea certificatului subiectului în orice moment. Autoritatea de Certificare (CA) își rezervă dreptul de a revoca un certificat din oricare dintre motivele enumerate în Capitolul 4.9.1.

Autoritatea de Supraveghere poate, în orice moment, să transmită o cerere formală de revocare sau să raporteze evenimente relevante care pot afecta valabilitatea certificatului unui subiect sau a Autorității de Certificare.

De asemenea, entitățile partenere și alte terțe părți pot notifica Simplifi în legătură cu situații justificate care ar putea impune revocarea. În astfel de cazuri, atunci când solicitantul nu este deținătorul certificatului, CA are obligația să:

- evalueze dacă solicitantul deține autoritatea suficientă pentru a cere revocarea; și
- notifice prompt abonatul cu privire la revocarea efectuată sau la inițierea procesului de revocare.

4.9.3. Procedura de solicitare a revocării

Revocarea poate fi inițiată, în conformitate cu prevederile Secțiunii 4.9.2, de către orice parte care are dreptul sau obligația de a o solicita. Simplifi acceptă cereri de revocare prin diverse canale și se asigură că, înainte de efectuarea revocării, sunt realizate verificări corespunzătoare de identificare și autorizare. Procesul este conceput pentru a asigura un echilibru între disponibilitate și securitate, permițând totodată actualizarea promptă a stării certificatelor prin CRL și OCSP.

a) **Revocarea de către subiect**
Subiectul (adică deținătorul cheii private corespunzătoare certificatului) poate solicita revocarea certificatului utilizând una dintre următoarele metode:

- **Prin Portalul Simplifi**: Subiectul se poate autentifica în contul său la *https://www.simplifi.ro* și poate transmite o cerere de revocare după autentificare;
- **Prin formular web**: Subiectul poate completa **formularul de revocare** disponibil la *https://simplifi.ro/revoke*, incluzând:
    - numele complet al solicitantului,
    - numărul de telefon și adresa de e-mail,
    - identificatorul certificatului care urmează a fi revocat,
    - motivul revocării (opțional)
      Notă: Această solicitare este tratată ca neautentificată. Autoritatea de Înregistrare (RA) va verifica identitatea și intenția solicitantului prin contact direct. În lipsa posibilității de validare a identității și intenției, certificatul poate fi suspendat până la clarificarea situației.

- **Prin e-mail:** o cerere de revocare poate fi transmisă la adresa easy@simplifi.ro si trebuie să includă:
    - numele solicitantului,
    - numărul de telefon,
    - numele subiectului sau numărul de serie al certificatului,
    - (opțional) motivul revocării.
      E-mailurile semnate digital utilizând o semnătură electronică calificată (QES) care corespunde subiectului sunt considerate autentificate. Toate celelalte sunt tratate ca neautentificate și supuse verificării.
- **În persoană la Autoritatea de Înregistrare (RA):** Subiectul poate solicita revocarea în persoană, prezentând un document de identitate valabil și un formular de cerere semnat unui reprezentant autorizat al RA.

b) **Revocarea de către abonat**
Abonatul (organizația care a încheiat contractul cu Simplifi) poate revoca orice certificat emis sub responsabilitatea sa prin una dintre următoarele metode:
- **Portal online autentificat;**
- **E-mail semnat digital, utilizând o semnătură electronică calificată (QES) sau un sigiliu electronic calificat (QSeal);**
- **Personal, la Autoritatea de Înregistrare (RA), prezentând un document de identitate valabil și împuternicirea corespunzătoare.**

c) Revocarea de către alte părți autorizate

Autoritatea de Înregistrare (RA): RA poate revoca un certificat pe baza unei cereri verificate sau în caz de compromitere ori încălcare a politicii, utilizând instrumente interne securizate;

Entitățile partenere / Terțe părți: pot transmite cereri de revocare la adresa easy@simplifi.ro, însoțite de dovezi credibile de utilizare abuzivă. RA va verifica cererea și poate suspenda certificatul pe durata investigației;

Roluri de încredere Simplifi (Simplifi Trusted Roles): personalul desemnat în roluri de încredere poate efectua revocarea prin intermediul software-ului CA, în următoarele situații:
- incidente de securitate,
- încălcări ale conformității,
- aplicarea politicilor interne.

Informațiile minime necesare pentru cererile de revocare
Toate cererile de revocare trebuie să includă:

- Numele complet al solicitantului;
- Numărul de telefon de contact;
- Adresa de e-mail (dacă este disponibilă);
- Numele subiectului sau identificatorul certificatului;
- Numărul de serie al certificatului sau DN-ul subiectului (dacă este cunoscut).

Cererile incomplete pot conduce la **suspendarea temporară** a certificatului până la confirmarea identității solicitantului.

Verificarea și măsurile întreprinse de RA
Toate cererile neautentificate sunt transmise către Autoritatea de Înregistrare (RA) pentru verificare. Dacă identitatea sau autoritatea solicitantului nu poate fi confirmată în mod fiabil, certificatul va fi suspendat până la rezolvarea situației. După verificarea cererii, certificatul este revocat, iar RA se asigură că:

- este adăugat fără întârziere în Lista de Revocare a Certificatelor (CRL);
- este marcat ca revocat prin intermediul serverului OCSP;
- este transmisă o notificare de confirmare către solicitant și abonat;
- în cazul refuzului cererii, este furnizat un răspuns motivat.

4.9.4. Perioada de grație pentru cererea de revocare

Abonatul sau subiectul are obligația de a solicita revocarea imediat, de îndată ce constată pierderea sau furtul dispozitivului, ori pierderea controlului asupra credențialelor de autentificare (cum ar fi PIN-uri sau parole).

4.9.5. Timpul în care Autoritatea de Certificare (CA) trebuie să proceseze cererea de revocare

Cererea de revocare a certificatului este procesată de către Simplifi în termen de 24 de ore de la acceptarea acesteia.

După confirmarea cererii de revocare, starea certificatului va fi actualizată în termen de 60 de minute.

4.9.6. Cerința de verificare a revocării de către entitățile partnere

Înainte de a se baza pe informațiile conținute într-un certificat,entitățile partenere trebuie să verifice valabilitatea fiecărui certificat din lanțul de certificare, inclusiv prin verificarea stării și a revocării certificatului, utilizând listele CRL sau serverele OCSP (OCSP responders) specificate în fiecare certificat din lanț.

4.9.7. Frecvența emiterii listelor CRL

Fiecare Autoritate de Certificare (CA) care face parte din infrastructura Simplifi emite o Listă de Revocare a Certificatelor (CRL) separată. CRL-ul este actualizat conform următorului program pentru fiecare nivel al ierarhiei CA:

- la fiecare 24 de ore, pentru Autoritățile Subordonate (Subordinate CAs);
- la fiecare 12 luni, cu excepția cazului în care intervine revocarea unei Autorități Intermediare (Intermediate CA), pentru CA Rădăcină (Root CA).

4.9.8. Latența maximă pentru publicarea listelor CRL

Fiecare CRL este publicată fără întârzieri nejustificate, imediat după generare — de regulă, acest proces se realizează automat, în câteva minute.

4.9.9. Disponibilitatea serviciilor online de verificare a stării certificatelor

Simplifi asigură o verificare continuă și în timp real a valabilității certificatelor, utilizând Protocolul Online pentru Starea Certificatului (OCSP – Online Certificate Status Protocol), implementat în conformitate cu cerințele tehnice din RFC 6960. Acest mecanism permite verificarea eficientă și actualizată a stării unui certificat, fără a fi necesar accesul la Lista CRL.

În condiții normale de operare, timpul de răspuns OCSP nu depășește zece (10) secunde.

Serverul OCSP (OCSP responder), acționând în numele Simplifi, returnează pentru fiecare interogare una dintre următoarele răspunsuri standardizate:

- good – certificatul este în prezent valabil;
- revoked – certificatul a fost oficial revocat;
- unknown – serverul nu deține informații sau nu poate verifica starea certificatului.

Informațiile privind starea OCSP sunt public accesibile, iar punctul de acces al serviciului (endpoint) este inclus direct în certificat. După efectuarea unei revocări, starea certificatului este actualizată și disponibilă prin OCSP în câteva minute.

4.9.10. Cerințele privind verificarea online a revocării

Nu există alte cerințe suplimentare față de cele indicate în Capitolul 4.9.6.

4.9.11. Alte forme de publicarea informațiilor privind revocarea

Nu se aplică.

4.9.12. Cerințe speciale legate de compromiterea cheii

Nu se aplică.

4.9.13. Circumstanțe pentru suspendare

Nu se aplică.

4.9.14. Cine poate solicita suspendarea

Nu se aplică.

4.9.15. Procedura de solicitare a suspendării

Nu se aplică.

4.9.16. Limite privind perioada de suspendare

Nu se aplică.

4.10. Serviciile privind starea certificatelor

4.10.1. Caracteristici operaționale

Simplifi furnizează un serviciu de verificare a stării certificatelor sub forma unui punct de distribuție CRL și a unui server OCSP (OCSP responder). Serviciile de interogare a stării certificatelor prin OCSP sunt accesibile prin HTTP. CRL-ul curent este publicat în repositoriu și este disponibil prin punctul de distribuție CRL (CRL distribution point), de asemenea accesibil prin HTTP.

Formatele și protocolele utilizate de aceste servicii sunt descrise în secțiunile 7.2 și 7.3 ale prezentei politici.

Adresele URL ale serviciului OCSP și ale punctului de distribuție CRL sunt incluse în certificat.

4.10.2. Disponibilitatea serviciului

Serviciul OCSP si lista CRL sunt disponibilie 24 de ore pe zi, 7 zile pe săptămână.

4.10.3. Caracteristici operaționale suplimentare

Nu se aplică.

4.11. Încetarea abonamentului

Relația dintre subiect și/sau abonat și Autoritatea de Certificare (CA) încetează atunci când certificatul expiră sau este revocat.

4.12. Depozitarea si recuperarea cheilor

Simplifi nu oferă servicii de escrow (depozitare) a cheilor pentru subiecți. Cheile private ale CA nu sunt niciodată depozitate.

4.12.1. Politici și practici privind depozitarea și recuperarea cheilor

Nu se aplică.

4.12.2. Politici și practici privind încapsularea și recuperarea cheilor de sesiune

Nu se aplică.

5. Controale de management, operaționale și fizice

5.1. Controale de securitate fizică

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.1.1. Alimentare electrică și aer condiționat

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.1.2. Expunerea la apă

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.1.3. Prevenirea și protecția împotriva incendiilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.1.4. Mediile de stocare

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.1.5. Eliminarea deșeurilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.2. Controale procedurale

5.2.1. Roluri de încredere

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.2.2. Principiul celor patru ochi

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.2.3. Identificarea și autentificarea pentru fiecare rol

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.2.4. Roluri care necesită segregarea atribuțiilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.3. Controale privind securitatea personalului

5.3.1. Calificări, experiență și autorizații

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.3.2. Proceduri de testare a personalului

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.3.3. Cerințe de instruire

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.3.4. Frecvența cerințelor pentru reinstruire

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.3.5. Frecvența și succesiunea rotației posturilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.3.6. Sancțiuni pentru acțiuni neautorizate

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.3.7. Contracte cu personalul

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.3.8. Documentația disponibilă pentru personal

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.4. Proceduri de audit și înregistrare a evenimentelor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.4.1. Tipuri de evenimente înregistrate

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.4.2. Frecvența procesării jurnalelor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.4.3. Perioada de păstrare a înregistrărilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.4.4. Protecția înregistrărilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.4.5. Copii de siguranță ale înregistrărilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.4.6. Sistemul de acumulare a jurnalelor de audit

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.4.7. Sistem de notificare pentru evenimente declanșatoare

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.4.8. Evaluarea vulnerabilităților

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.5. Arhivarea înregistrărilor

5.5.1. Tipuri de arhive

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.5.2. Perioada de păstrare a arhivelor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.5.3. Protecția arhivei

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.5.4. Proceduri pentru copiile de siguranță ale arhivelor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.5.5. Cerințe pentru marcarea temporală a arhivelor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.5.6. Stocarea arhivelor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.5.7. Proceduri de acces și verificare a informațiilor arhivate

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.6. Înlocuirea cheii

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.7. Gestionarea compromiterii și a situațiilor de dezastru

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.7.1. Proceduri pentru gestionarea incidentelor și compromiterilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.7.2. Incidente legate de defecțiuni ale echipamentelor hardware, software și/sau ale datelor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.7.3. Proceduri în caz de compromitere a cheii private

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.7.4. Managementul continuității activității

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.8. Încetarea activității TSP

5.8.1. Plan de încetare

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

5.9. Marcare temporala

5.9.1. Emiterea marcajelor temporale

Token-urile de marcare temporală emise de către TSA (Autoritatea de Marcare Temporală) respectă formatul și specificațiile tehnice prevăzute în ETSI EN 319 422 (standardul pentru profilurile de marcă temporală). Fiecare token de marcare temporală include cel puțin: identificatorul certificatului TSA, OID-ul politicii aplicabile, amprenta hash a datelor furnizate de abonat, și ora exactă a emiterii, toate acestea fiind semnate cu cheia privată a TSA (în cadrul TSU – Time-Stamping Unit). Procesul de emitere a marcajelor temporale este automatizat în mod securizat: atunci când este primită o cerere validă, sistemul TSA înregistrează ora curentă și generează un token semnat. Sunt acceptate numai cererile autentificate, iar sistemul garantează că nu sunt emise marcaje temporale neautorizate.

TSA garantează că fiecare token de marcare temporală emis conține o reprezentare corectă și precisă a timpului, în limitele de acuratețe stabilite. Ora inclusă în token este

aliniată la surse oficiale de timp UTC, asigurând faptul că marcajul temporal poate fi interpretat corect și universal. Sistemul de semnare al TSA este protejat împotriva accesului neautorizat sau a modificărilor nepermise, astfel încât doar marcajele temporale legitime pot fi produse. Fiecare token de marcă temporală este semnat cu cheia privată dedicată a unității TSU, iar sistemul respinge automat orice tentativă de emitere a unui marcaj temporal dacă cheia TSU este expirată sau revocată. Această măsură previne generarea de token-uri invalide (de exemplu, semnate cu un certificat expirat).

TSA monitorizează în permanență procesul de emitere a marcajelor temporale pentru detectarea eventualelor anomalii. Dacă se constată că ceasul intern al TSA este desincronizat peste limitele permise, TSA va suspenda emiterea marcajelor temporale până când sincronizarea exactă este restabilită. Acest mecanism de suspendare asigură fiabilitatea tuturor marcajelor temporale emise.

5.9.2. Sincronizarea ceasului cu UTC

TSA (Autoritatea de Marcare Temporală) menține referința sa de timp (ceasul sistemului TSU – Time-Stamping Unit) sincronizată cu Timpul Universal Coordonat (UTC). Sursa de timp este trasabilă către laboratoare oficiale UTC(k) recunoscute de Bureau International des Poids et Mesures (BIPM). Sistemul TSA se sincronizează periodic cu cel puțin un semnal de timp UTC(k), utilizând protocolul NTP (Network Time Protocol), pentru a obține o precizie mai bună sau egală cu 1 secundă față de UTC.

Precizia declarată de către TSA este documentată, iar toate marcajele temporale emise includ, dacă este prevăzut de profil, o indicație a preciziei.

Mecanismul de sincronizare a ceasului TSA este proiectat astfel încât ceasul TSU să nu se abată în afara toleranței declarate de precizie în condiții normale de funcționare. Sistemul monitorizează în mod continuu diferența dintre ceasul TSU și sursa de timp UTC de încredere. Dacă ceasul TSU se abate peste limita de toleranță permisă (de exemplu, cu mai mult de 1 secundă), TSA suspendă emiterea marcajelor temporale până la restabilirea sincronizării. Există proceduri implementate pentru detectarea rapidă și corectarea oricărei derive sau defecțiuni de sincronizare. Toate evenimentele legate de sincronizarea ceasului sunt înregistrate pentru a furniza o pistă completă de audit.

TSA ia în considerare, de asemenea, secundele intercalare (leap seconds). Atunci când o secundă intercalară este anunțată de autoritățile competente (IERS), sistemele TSA sunt pregătite să gestioneze adăugarea sau eliminarea acestei secunde. Ajustarea secundelor intercalare este aplicată la sfârșitul zilei (ora UTC) în care are loc evenimentul, conform practicii standard (de regulă, în iunie sau decembrie). TSA păstrează o înregistrare exactă a momentului în care secunda intercalară a fost inserată sau eliminată, în cadrul preciziei declarate, asigurând transparență în ceea ce privește alinierea marcajelor temporale la UTC în acea perioadă. Prin planificarea evenimentelor de tip leap second și documentarea

modului de gestionare a acestora, TSA menține o sincronizare continuă, fără a compromite serviciul. După fiecare secundă intercalară sau ajustare a ceasului, TSA reconfirmă că timpul înscris în token-urile emise rămâne corect în limitele preciziei declarate. Aceste măsuri asigură respectarea cerinței ca ceasul TSA să fie sincronizat în mod fiabil cu UTC în orice moment.

6. Controale tehnice de securitate

6.1. Generarea și instalarea perechilor de chei

6.1.1. Generarea perechilor de chei

6.1.1.1. Autoritatea de certificare rădăcină (Root CA) și autoritățile subordonate

Perechile de chei pentru toate autoritățile Simplifi sunt generate în conformitate cu o procedură documentată de generare, care garantează integritatea și confidențialitatea cheilor. Procesul de generare a perechii de chei are loc la sediul Simplifi sau într-un centru de date securizat , într-un mediu fizic securizat, în prezența a cel puțin două persoane autorizate care dețin roluri de încredere, dintre care una trebuie să fie Ofițerul de Securitate (Security Officer). Se întocmește un raport care documentează activitățile desfășurate pe parcursul procesului de generare a cheilor, iar acest raport este semnat de toți participanții implicați în procedură. Ofițerul de Securitate certifică prin semnătura sa că procesul de generare a cheilor a fost efectuat în conformitate cu procedura documentată, asigurând confidențialitatea și integritatea cheilor.

Cheia privată utilizată pentru crearea unei semnături electronice calificate sau a unui sigiliu electronic calificat este generată în cadrul unui dispozitiv calificat de creare a semnăturilor sau sigiliilor (QSCD), localizat într-un mediu securizat administrat de Simplifi, în conformitate cu cerințele ETSI TS 119 431-1. Procesul de generare a cheii private se desfășoară în întregime în interiorul dispozitivului QSCD, fără posibilitatea exportului, în conformitate cu standardul CEN EN 419 241-2. Semnatarul autorizează operațiunea de creare a cheii și utilizarea ulterioară a acesteia de la distanță, prin intermediul unui mecanism de autentificare și autorizare a operațiunii de semnare, în conformitate cu Signature Activation Protocol (SAP) definit în ETSI TS 119 432.

6.1.1.2. Generarea perechii de chei a subiectului într-un QSCD la distanță

Cheile private ale Subiectului sunt generate și utilizate într-un Dispozitiv Calificat de Creare a Semnăturii Electronice la Distanță (RQSCD – Remote Qualified Signature Creation Device). RQSCD este certificat în conformitate cu standardul EN 419 241-2, inclusiv modelul SCAL2.

RQSCD acceptă algoritmii criptografici și lungimile de chei definite în ETSI TS 119 312.

Mediul RQSCD protejează toate cheile generate, asigurându-le confidențialitatea și integritatea. Cheile nu sunt păstrate în afara mediului protejat.

Cheile private ale Subiectului sunt asociate cu identitatea Subiectului înainte de emiterea certificatului.Această asociere de referință este creată după înregistrare și după validarea inițială a identității, așa cum este specificat în Capitolul 3.2 al prezentului document. Procesul tehnic asigură că datele de identificare asociate referinței de identitate a Subiectului corespund datelor înscrise în certificatul emis pentru respectivul Subiect.

RQSCD este inițializat înainte de a genera sau conține orice cheie de semnare. Mecanismele sale tehnice impun participarea a cel puțin doi operatori, iar procesul este efectuat în conformitate cu Capitolul 6.1.1.1.

6.1.2. Livrarea cheii private către subiect

Simplifi **nu livrează** chei private către Subiect.

În cazul **serviciilor de semnare la distanță**, cheia privată este generată și stocată în siguranță în cadrul unui **Dispozitiv Calificat de Creare a Semnăturii (QSCD)**, operat și administrat de Simplifi sau de un furnizor de încredere desemnat. Subiectul nu dobândește posesia sau controlul asupra cheii private în niciun moment.

- Pentru **certificatele pe termen scurt** (de exemplu, semnare la distanță bazată pe sesiune), cheia privată există doar pe durata unei singure sesiuni de semnare și este distrusă sau dezactivată imediat după utilizare. Nu este emis niciun mijloc de autentificare sau mijloc de identitate care să poată fi reutilizat ulterior de către Subiect.

- Pentru **certificatele pe termen lung**, identitatea Subiectului este verificată de către Autoritatea de Înregistrare (RA), iar cheia privată asociată este stocată în siguranță într-un QSCD. În astfel de cazuri, accesul la cheie este posibil numai prin mecanisme de autentificare securizate.

În niciun moment cheia privată nu este extrasă, exportată sau pusă la dispoziția Subiectului în afara procesului securizat de semnare.

6.1.3. Livrarea cheii publice către emitentul certificatului

Nu se aplică.

6.1.4. Livrarea cheii publice către entități partenere

The certificate of the CA contains a public key. The CA certificate is publicly available for relying parties to download. Certificates are available from the public repository.

Certificatul Autorității de Certificare (CA) conține cheia publică. Certificatul CA este disponibil public, pentru ca entitățile partenere să îl poată descărca. Certificatele sunt disponibile în depozitarul public (public repository).

6.1.5. Dimensiunile cheilor

Simplifi utilizează algoritmi criptografici și dimensiuni minime ale cheilor care respectă cerințele prevăzute în standardul ETSI TS 119 312.

Cheile tuturor autorităților de certificare Simplifi sunt chei RSA și au o lungime de cel puțin 4096 biți.

Cheile subiecților sunt, de asemenea, chei RSA și au o lungime de cel puțin 2048 biți.

6.1.6. Generarea parametrilor cheii publice si verificarea calității acestora

Parametrii utilizați pentru generarea cheilor publice respectă cerințele specificate în standardele: ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 și ETSI TS 119 312, în cea mai recentă versiune aplicabilă disponibilă la momentul publicării prezentului document. Înainte de emiterea unui certificat, Autoritatea de Certificare (CA) verifică faptul că cheia publică nu a mai fost utilizată anterior.

6.1.7. Scopurile utilizării cheilor

Scopurile permise pentru utilizarea cheilor sunt descrise în câmpul KeyUsage din extensia standard a unui certificat conform specificației X.509 versiunea 3 (v3).

Utilizarea cheii de semnare a Subiectului:

- digitalSignature (semnarea digitală a documentelor)
- nonrepudiation (nerepudierea semnăturii)

Utilizarea cheii pentru Autoritatea de Certificare Rădăcină (Root CA):

- keyCertSign (semnarea certificatelor)
- keyCrlSign (semnarea listelor de revocare a certificatelor)

Utilizarea cheii pentru Responderul OCSP:

- digitalSignature (semnarea digitală a răspunsurilor OCSP)
- OCSP signing (semnarea răspunsurilor OCSP)

6.2. Protecția cheii private și controlul asupra modulelor criptografice

6.2.1. Standardele si controalele modulelor criptografice

Toate modulele HSM (Hardware Security Module) care protejează cheile infrastructurii CA și PKI sunt certificate conform FIPS 140-2 Level 3.

Modulele criptografice utilizate de Simplifi pentru serviciile de semnare și sigilare la distanță sunt incluse în lista UE a dispozitivelor QSCD și sunt certificate conform standardului EN 419 241-2.

6.2.2. Controlul multipersonal (n din m) asupra cheii private

Modulele criptografice pe care sunt stocate cheile private ale Autorității de Certificare (CA) și cheile subiecților sunt localizate într-un mediu securizat. Pentru activarea respectivei chei private și pentru accesarea cheilor private ale subiecților sunt necesare cel puțin două persoane autorizate.

Secretele partajate sunt stocate pe carduri criptografice, protejate printr-un cod PIN, și sunt transferate în mod securizat către deținătorii acestora care au roluri de încredere.

6.2.3. Depozitarea cheilor private

Nu se aplică.

6.2.4. Copii de siguranță ale cheilor private

Cheile private ale subiecților

Cheile private utilizate de Subiecți pentru semnături electronice calificate la distanță și sigilii electronice calificate sunt generate, stocate și utilizate exclusiv în cadrul unui Dispozitiv Calificat de Creare a Semnăturii Electronice la Distanță (RQSCD – Remote Qualified Signature Creation Device), administrat de Simplifi. Aceste dispozitive sunt implementate utilizând module hardware de securitate certificate (HSM – Hardware Security Modules) și fac parte dintr-un mediu protejat denumit Security World.

Cheile private ale Subiecților nu sunt niciodată exportate sau livrate Subiectului și sunt protejate în așa fel încât doar operațiunile de semnare autorizate pot fi efectuate.Procesele de copiere de siguranță (backup) și restaurare (recovery) ale cheilor private ale Subiecților sunt gestionate în totalitate în cadrul infrastructurii Security World, iar accesul este protejat prin autentificare multifactor (MFA) și control al accesului bazat pe roluri (RBAC – Role-Based Access Control). Nicio cheie privată a Subiectului nu este stocată în afara perimetrului criptografic al RQSCD.

Cheile private ele Autorității de Certificare

Simplifi aplică proceduri distincte de management și copiere de siguranță a cheilor (backup) pentru cheile private ale Autorității de Certificare Rădăcină (Root CA) și Autorității de Certificare Intermediare (Intermediate CA).

Cheile private ale Root CA sunt generate și stocate într-un modul hardware de securitate (HSM) izolat fizic și sunt protejate printr-o cheie de criptare a cheilor (KEK – Key Encryption Key).Cheia KEK este împărțită în părți criptografice (cryptographic shares) distribuite între

mai mulți custozi de chei, în conformitate cu procedurile de ceremonie a cheilor (key ceremony) ale Simplifi. Cheia privată a Root CA nu este niciodată exportată în formă necriptată. Procesele de backup și restaurare necesită acces bazat pe cvorum, sub control dual, într-un mediu securizat și de încredere.

Cheile private ale Intermediate CA sunt protejate în cadrul HSM-urilor care participă la un mediu Security World administrat de Simplifi. Copiile de siguranță sunt realizate prin arhivarea securizată a tuturor datelor Security World. Aceste copii sunt criptate, versionate și stocate offline în facilități fizice securizate. Recuperarea (recovery) este posibilă numai prin utilizarea unui HSM compatibil, sub control dual, de către personal autorizat cu roluri de încredere.

În toate cazurile, operațiunile de backup ale cheilor sunt strict limitate la personalul desemnat cu roluri de încredere, necesită control dual și se desfășoară în medii fizic securizate. Copiile de siguranță beneficiază de un nivel de protecție egal sau superior celui aplicat cheilor operaționale, în deplină conformitate cu ETSI EN 319 411-1 și cu cerințele Regulamentului eIDAS.

Simplifi nu generează și nu păstrează copii ale cheilor private aparținând operatorilor CA, personalului Autorității de Înregistrare (RA) sau oricărui alt participant individual.

6.2.5. Restaurarea cheii private

Restaurarea cheii private necesită prezența Ofițerului de Securitate (Security Officer) și a unui Operator de Sistem desemnat (System Operator) pentru aprobarea dual a importului de configurație.

6.2.6. Arhivarea cheii private

Nu se aplică. Cheile private nu sunt arhivate.

6.2.7. Transferul cheii private în sau dintr-un modul criptografic

Transferul cheilor private ale subiecților nu este permis.

6.2.8. Stocarea cheii private în modulul criptografic

Cheile private sunt generate și stocate într-o zonă securizată a modulului criptografic. Cheile private pot fi stocate în modul necriptat sau criptat, însă indiferent de forma de stocare, acestea nu sunt accesibile din afara modulului criptografic pentru entități neautorizate.

6.2.9. Metoda de activare a cheii private

Cheile private ale subiecților sunt activate de către utilizator, sub controlul exclusive al acestuia/acesteia.

6.2.10. Metoda de dezactivare a cheii private

În cazul unei chei private de semnare a subiectului, dezactivarea este efectuată imediat după crearea unei semnături electronice sau după încheierea sesiunii online (cookie session).

6.2.11. Metoda de distrugere a cheii private

Personalul Simplifi efectuează distrugerea cheii private atunci când certificatul expiră sau este revocat, conform procedurilor de securitate prevăzute de politicile de securitate și de specificațiile producătorului dispozitivului. Aceasta se realizează prin ștergerea cheii private din HSM și, simultan, ștergerea copiilor de siguranță de pe mediile de stocare. La încetarea utilizării HSM-ului, cheile private din dispozitiv sunt șterse.

6.2.12. Nivelul de certificare al modulului criptografic

Acest subiect este abordat în secțiunea 6.2.1.

6.2.13. Arhivarea cheii publice

Declarația de Practici acoperă detaliile referitoare la acest element în capitolul 5.5 „Arhivarea înregistrărilor” (Records Archival).

6.2.14. Perioadele operaționale ale certificatelor și perioadele de utilizare ale perechilor de chei

Perioada de valabilitate a unui certificat este determinată pe baza următoarelor criterii:

- Stadiul tehnologic actual
- Nivelul actual al tehnologiilor criptografice;
- Scopul de utilizare al certificatului avut în vedere.

Perioadele de valabilitate sunt indicate pe fiecare certificat. Perioadele maxime de utilizare ale certificatelor sunt următoarele:

Subiectul certificatului	Perioada maximă de valabilitate
Simplifi Root CA G1	20 ani
Simplifi Qualified CA Class 3 G1	10 ani

Detalii suplimentare sunt prezentate în capitolul 7.

6.3. Date de activare

6.3.1. Generarea și instalarea datelor de activare

Simplifi se asigură că fiecare subiect este identificat și autentificat cu acuratețe înainte de a permite acțiuni care ar putea afecta controlul autorizat asupra oricărei chei de semnare.

Activarea dispozitivului de creare a semnăturii de către subiect necesită utilizarea a doi factori de autentificare separați.

6.3.2. Protecția datelor de activare

Subiectul este responsabil pentru protejarea mijloacelor și/sau dispozitivului de autentificare.

În cazul semnăturilor sau sigiliilor la distanță, datele de activare a semnăturii (SAD – Signature Activation Data) sunt colectate și securizate prin Protocolul de Activare a Semnăturii (SAP – Signature Activation Protocol), utilizat pentru a controla, cu un nivel ridicat de încredere (cel puțin SCAL2 – Sole Control Access Level 2), o anumită operațiune de semnare efectuată de un RQSCD în numele subiectului, aflată sub controlul exclusiv al acestuia. Modulul de Activare a Semnăturii (SAM – Signature Activation Module) este utilizat într-un mediu protejat împotriva manipulării (tamper-protected environment).

Protecția datelor de activare se bazează atât pe controale de acces fizic (aplicate de către CA și Subiect), cât și pe măsuri criptografice de protecție.

6.3.3. Alte aspecte privind datele de activare

Nu se aplică.

6.4. Controale de securitate a sistemelor informatice

6.4.1. Cerințe tehnice specifice privind securitatea sistemelor informatice

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

6.4.2. Clasificarea securității sistemelor informatice

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

6.5. Controale de securitate în ciclul de viață

6.5.1. Controale privind dezvoltarea sistemelor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

6.5.2. Controale de management al securității

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

6.5.3. Controale de securitate pe durata ciclului de viață

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

6.5.4. Controale de securitate a rețelei

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

6.5.5. Sincronizarea timpului

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

6.6. Marcarea temporală

6.6.1. Generarea cheii TSU

Generarea fiecărei chei de semnare a Unității de Marcare Temporală (TSU – Time-Stamping Unit) se realizează într-un mediu fizic securizat, de către personal aflat în roluri de încredere, sub control dual (cel puțin două persoane). Numai persoanele autorizate și strict necesare (conform politicilor interne de securitate ale TSA – Time-Stamping Authority) participă la procesul de generare a cheii TSU, asigurând un control riguros asupra acestei activități critice. Cheile de semnare TSU sunt generate în cadrul unui dispozitiv hardware criptografic de înaltă asigurare, care respectă standarde de securitate recunoscute la nivel internațional. Dispozitivul de generare a cheii îndeplinește următoarea cerință:

• Este certificat conform FIPS 140-3 Level 3 (sau unui standard național echivalent) pentru module criptografice securizate.

TSA utilizează chei RSA de 4096 biți împreună cu funcția de hash SHA-512 pentru generarea semnăturilor digitale ale marcajelor temporale, în conformitate cu seturile de algoritmi identificate de ETSI TS 119 312 pentru semnături electronice/sigilii calificate.

Nicio cheie de semnare TSU nu este vreodată exportată în formă necriptată din modulul criptografic în care a fost generată.

6.6.2. Protecția cheii private a TSU

Confidențialitatea și integritatea cheilor private de semnare ale Unității de Marcare Temporală (TSU – Time-Stamping Unit) sunt protejate prin măsuri stricte de control. Toate cheile private ale TSU sunt stocate și utilizate exclusiv în cadrul unui dispozitiv hardware criptografic securizat (HSM – Hardware Security Module), care oferă un mediu controlat pentru stocarea și utilizarea cheilor. Modulul criptografic utilizat pentru protecția cheilor îndeplinește criterii de asigurare ridicată, conform standardului FIPS 140-3 Level 3, asigurând faptul că dispozitivul este rezistent la manipulare (tamper-resistant) și că cheile nu pot fi extrase sau utilizate fără autorizare.

Dacă o cheie privată TSU necesită copiere de siguranță (backup), aceasta se efectuează în formă criptată și în condiții strict controlate. Orice operațiune de copiere sau duplicare a cheii implică cel puțin două persoane de încredere (control dual) într-un mediu securizat. Copiile de siguranță ale cheilor TSU sunt protejate prin mijloace criptografice, la același nivel de securitate ca și cheia principală.

Regulile de securitate ale Autorității de Marcare Temporală (TSA – Time-Stamping Authority) limitează accesul la cheile private ale TSU exclusiv la funcțiile necesare emiterii marcajelor temporale. Accesul administrativ la modulele HSM este restricționat doar pentru personalul autorizat cu roluri de încredere și se realizează prin autentificare multifactor (MFA). Sunt păstrate jurnale de audit (logs) pentru toate operațiunile care implică materialul criptografic al cheilor TSU. Prin combinarea acestor măsuri, se asigură protecția completă a cheilor private TSU împotriva dezvăluirii neautorizate sau modificării neintenționate.

6.6.3. Certificatul cheii publice a TSU

Cheia publică de verificare a semnăturii fiecărei Unități de Marcare Temporală (TSU – Time-Stamping Unit) este pusă la dispoziția entităților partenere prin intermediul unui certificat de cheie publică X.509, emis de o Autoritate de Certificare (CA – Certification Authority). Acest certificat asociază identitatea TSU-ului cu cheia sa publică și este utilizat de către clienți pentru verificarea semnăturii digitale aplicate pe marcajele temporale. Autoritatea de Marcare Temporală (TSA – Time-Stamping Authority) se asigură că nicio unitate TSU nu emite marcaje temporale până când certificatul cheii publice a acelei TSU nu este emis corespunzător și încărcat în dispozitivul său securizat. Această măsură previne generarea oricărui marcaj temporal nesemnat sau neverificabil.

Certificatul TSU include extensii care identifică utilizarea specifică a cheii pentru marcare temporală (timestamping).

Odată ce certificatul TSU este emis și unitatea TSU este activată, TSA poate începe semnarea marcajelor temporale utilizând cheia privată corespunzătoare.

6.6.4. Reemiterea cheii TSU

Autoritatea de Marcare Temporală (TSA – Time-Stamping Authority) nu efectuează operațiuni de „rekey” (adică reutilizarea unei chei existente pentru un nou certificat) pentru cheile Unității de Marcare Temporală (TSU – Time-Stamping Unit). În schimb, atunci când perechea de chei a unei TSU trebuie înlocuită (de exemplu, la apropierea expirării sau în cazul unei compromiteri), se generează o nouă pereche de chei, iar pentru noua cheie se obține un nou certificat de cheie publică. Această abordare garantează că fiecare cheie TSU este unică și trasabilă la o perioadă de valabilitate specifică, asigurând totodată că niciun material criptografic vechi nu este utilizat dincolo de durata sa de viață prevăzută.

6.6.5. Managementul ciclului de viață al echipamentelor criptografice de semnare

Toate dispozitivele hardware criptografice utilizate pentru semnarea marcajelor temporale sunt gestionate prin proceduri stricte de management al ciclului de viață, pentru a menține integritatea și securitatea acestora. Autoritatea de Marcare Temporală (TSA – Time-Stamping Authority) se asigură că fiecare dispozitiv este expediat, stocat, operat și în cele din urmă dezafectat în condiții de securitate corespunzătoare. La livrarea de la producător, dispozitivul este verificat pentru a se asigura că nu a fost manipulat pe durata transportului; acesta rămâne sigilat sau sub monitorizare până la instalare. În timpul stocării înainte de utilizare, dispozitivul este păstrat într-un mediu securizat, pentru a preveni orice acces sau modificare neautorizată. Instalarea dispozitivului în mediul operațional este realizată de personal autorizat aflat în roluri de încredere, iar în timpul etapelor critice de configurare (cum ar fi încărcarea cheilor TSU), se aplică cel puțin principiul controlului dual (dual control).

La activarea unui nou dispozitiv TSU sau la duplicarea cheii de semnare a unei TSU pe un dispozitiv de rezervă (în scop de echilibrare a sarcinii – load balancing sau continuitate operațională – failover), personalul de încredere urmează proceduri documentate care asigură confidențialitatea cheilor și autenticitatea dispozitivului țintă.

Atunci când un dispozitiv criptografic urmează să fie retras din uz, toate cheile private TSU și materialele sensibile sunt șterse în mod securizat înainte de dezafectare. Ștergerea este efectuată astfel încât datele să nu poată fi recuperate, nici măcar prin tehnici avansate de analiză criminalistică (forensic recovery). Numai după confirmarea ștergerii complete a cheilor, dispozitivul poate fi reutilizat sau eliminat definitiv. Aceste controale ale ciclului de viață îndeplinesc cerințele privind protecția echipamentelor criptografice ale TSA pe întreaga durată — de la punerea în funcțiune până la retragerea din uz.

6.6.6. Sfârșitul ciclului de viață al cheii TSU

Fiecărei chei de semnare a Unității de Marcare Temporală (TSU – Time-Stamping Unit) i se atribuie o perioadă maximă de valabilitate, pentru a asigura reînnoirea periodică a cheilor. Simplifi limitează durata de viață a cheilor private TSU la 5 ani, facilitând astfel adaptarea sigură la noi algoritmi criptografici și o gestionare eficientă a cheilor. O cheie de semnare a unei TSU nu este niciodată utilizată dincolo de perioada de valabilitate a certificatului de cheie publică corespunzător. În practică, data de expirare a certificatului TSU stabilește ultima dată posibilă la care cheia poate fi utilizată pentru semnare; de regulă, TSA retrage cheia puțin mai devreme, pentru a menține o marjă de siguranță.

Autoritatea de Marcare Temporală (TSA – Time-Stamping Authority) implementează măsuri proactive pentru a trece la noile chei TSU cu mult timp înainte ca cele vechi să expire. Aproximativ cu un an înainte de expirarea unei chei TSU, TSA generează o nouă pereche

de chei și obține un nou certificat TSU. Noua TSU (sau noua cheie pe o TSU existentă) este pusă în funcțiune în paralel cu cea veche, astfel încât cererile de marcaj temporal să poată fi prelucrate treptat de noua cheie. Această metodă asigură o tranziție lină (rollover), fără întreruperea serviciului. Odată ce noua TSU devine complet operațională, vechea TSU este dezactivată la expirarea perioadei sale de valabilitate.

După expirarea unei chei TSU sau după încetarea utilizării acesteia, TSA distruge materialul criptografic asociat cheii private TSU în mod securizat și ireversibil. Distrugerea include toate copiile sau copiile de rezervă (backup) ale cheii respective. Prin ștergerea securizată sau distrugerea fizică a hardware-ului care a conținut cheia, TSA garantează că astfel cheia expirată nu poate fi restaurată sau utilizată pentru falsificarea marcajelor temporale. Aceste practici îndeplinesc cerințele privind gestionarea cheilor TSU la sfârșitul ciclului de viață, asigurând că cheile vechi nu devin un risc de securitate.

7. Profilurile certificatelor și ale listelor CRL

Profilurile certificatelor și ale listelor de revocare a certificatelor (CRL – Certificate Revocation Lists) sunt emise în conformitate cu normele ETSI TS 319 412-1 și ETSI EN 319 412 (Părțile 2, 3 și 5).

7.1. Profilul certificatului

Structura profilului certificatului este prezentată în depozitarul public disponibil la adresa:

http://simplifi.ro/policies

7.2. Profilul listei CRL

Structura profilului CRL este prezentată în depozitarul public disponibil la adresa:
http://simplifi.ro/policies

7.3. Profilul OCSP

Structura profilului OCSP este prezentată în depozitarul public disponibil la adresa:
http://simplifi.ro/policies

8. Audit de Conformitate și Alte Evaluări

8.1. Frecvența sau circumstanțele evaluării

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

8.2. Calificarea auditorilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

8.3. Relația auditorilor cu Simplifi

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

8.4. Aria de aplicare al auditului

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

8.5. Acțiuni întreprinse ca urmare a constatării unor neconformități

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

8.6. Comunicarea rezultatelor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9. Alte Aspecte Comerciale și Juridice

9.1. Tarife

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.2. Responsabilitate financiară

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.3. Confidențialitatea informațiilor comerciale

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.4. Confidențialitatea informațiilor cu caracter personal

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.5. Drepturi de proprietate intelectuală

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.6. Declarații și garanții

9.6.1. Obligațiile Simplifi

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.6.2. Obligațiile și garanțiile Autorităților de Înregistrare

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.6.3. Obligațiile și garanțiile Subiecților și Abonaților

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.6.1. Obligațiile și garanțiile Entităților Partenere

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.6.2. Declarațiile și garanțiile altor participanți

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.7. Excluderea garanțiilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.8. Limitarea răspunderii

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.9. Despăgubiri

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.10. Modificări

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.11. Proceduri de soluționare a litigiilor

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.12. Legea aplicabilă

Declarația de Practici acoperă specificațiile detaliate pentru acest element.

9.13. Dispoziții diverse

Declarația de Practici acoperă specificațiile detaliate pentru acest element.