simplifi

Declarația de Practici de Certificare Simplifi

Politici și controale operaționale pentru servicii de încredere calificate

Prezenta Declarație de Practici de Certificare (CPS) reglementează emiterea, administrarea și revocarea următoarelor servicii de încredere calificate: certificate calificate pentru semnături electronice, certificate calificate pentru sigilii electronice, marcaje temporale electronice calificate.

Această Declarație de Practici este revizuită periodic de către Managerul Serviciilor de Încredere și este supusă aprobării și auditului de către autoritatea de supraveghere desemnată. Documentul oferă garanții abonaților, părților terțe utilizatoare, autorităților de reglementare și auditorilor privind **integritatea, disponibilitatea și fiabilitatea** serviciilor de încredere calificate furnizate de Simplifi.

Informații despre document

Versiune	1.0
Data versiunii	1 Septembrie 2025
Aprobat de	Comitetul de Management al Politicilor și Procedurilor
Responsabil de document	Manager Servicii de Încredere
Numele documentului	Declarația de Practici de Certificare Simplifi
OID Document	1.3.6.1.4.1.63578.1.1.2
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

Cuprins

1. Introducere

SIMPLIWORKS SRL, care operează sub marca **Simplifi**, este o societate românească înființată la data de **11 aprilie 2022**, având misiunea de a furniza **servicii de încredere cu nivel ridicat de asigurare**, bazate pe principiile fundamentale de **securitate, integritate, confidențialitate și nerepudiere**. Simplifi își propune să construiască o infrastructură de încredere modernă și transparentă, conformă cu standardele stricte aplicabile **semnăturilor electronice calificate**, **sigiliilor electronice calificate** și **marcajelor temporale electronice calificate**, conform **Regulamentului (UE) nr. 910/2014 (eIDAS)**.

În calitate de **Autoritate de Certificare (CA)**, care operează în cadrul unei **infrastructuri cu chei publice (PKI)** dedicate, Simplifi este responsabilă de emiterea, administrarea, revocarea și validarea certificatelor digitale, prin proceduri clar definite și auditate. Arhitectura PKI Simplifi include o **Autoritate de Certificare Rădăcină (Root CA)** și **autorități intermediare subordonate (Intermediate CAs)**, configurate pentru diverse tipuri sau clase de servicii. Fiecare Autoritate de Certificare utilizează **profile de certificate** specifice, adaptate contextului serviciului și nivelului de asigurare solicitat.

Rolul Simplifi, în calitate de **Furnizor Calificat de Servicii de Încredere (QTSP)**, constă în furnizarea de servicii de încredere atât persoanelor fizice, cât și juridice, publice sau private, în deplină conformitate cu legislația **europeană** și **română** aplicabilă. Aceste servicii includ, fără a se limita la:

- Emiterea și gestionarea ciclului de viață al certificatelor calificate și necalificate;
- Generarea și validarea semnăturilor și sigiliilor electronice;
- Publicarea listelor de revocare a certificatelor (CRL) și operarea unui serviciu OCSP (Online Certificate Status Protocol) pentru verificarea în timp real a statutului certificatelor;
- Servicii de marcare temporală.

1.1. Domeniul de aplicare

Declarația de Practici definește principiile care guvernează furnizarea serviciilor de semnătură electronică și desfășurarea operațiunilor autorității de certificare, în conformitate cu cerințele Regulamentului (UE) eIDAS privind furnizarea serviciilor de încredere. De asemenea, asigură conformitatea cu legislația română. Acest document stabilește rolurile, atribuțiile și responsabilitățile tuturor părților implicate și descrie controalele manageriale, operaționale și fizice implementate de SIMPLIWORKS SRL, care operează sub marca Simplifi.

Documentul funcționează ca un cadru unitar pentru furnizarea serviciilor de încredere și de identificare electronică, în conformitate cu politicile specifice adoptate de SIMPLIWORKS SRL, sub marca Simplifi, în calitate de Furnizor Calificat de Servicii de Încredere.

În mod specific, Declarația de Practici acoperă următoarele servicii:

- Emiterea și gestionarea certificatelor pentru semnături electronice;
- Emiterea și gestionarea certificatelor pentru sigilii electronice;
- Emiterea și gestionarea certificatelor pentru infrastructura PKI;
- Furnizarea serviciului de revocare și a informațiilor online privind statutul certificatelor;
- Generarea și gestionarea datelor de creare a semnăturilor electronice în numele Subiectului (semnături și sigilii la distanță);
- Serviciul de marcare temporală.

Practiciile descrise în prezentul document se aplică atât serviciilor de încredere calificate, cât și celor necalificate.

Documentul include o declarație care confirmă că toate serviciile furnizate în baza acestei Declarații de Practici sunt conforme cu următoarele reglementări:

- Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, versiunea consolidată din 18.10.2024;
- Legislația națională română aplicabilă, inclusiv, dar fără a se limita la, Legea nr. 455/2001, Ordonanța de Urgență nr. 38/2020, Legea nr. 214/2024 și deciziile emise de Autoritatea pentru Digitalizarea României (ADR).

Prevederile detaliate privind furnizarea serviciilor de încredere și a serviciilor de identificare electronică sunt definite în documente de politică separate. Fiecare serviciu este clasificat individual ca fiind calificat sau necalificat. Aceste politici sunt public disponibile, conform descrierii din Capitolul 2.1.

Prezenta Declarație de Practici servește drept cadru unitar și cuprinzător pentru practicile interne Simplifi și pentru angajamentele sale publice privind furnizarea serviciilor. Structura documentului respectă RFC 3647 și este aliniată la versiunile aplicabile ale următoarelor standarde:

- ETSI EN 319 401 – Cerințe generale de politică pentru furnizorii de servicii de încredere;
- ETSI EN 319 411-1 și 319 411-2 – Cerințe de politică și securitate pentru furnizorii de servicii de încredere care emit certificate;
- ETSI EN 319 421 – Cerințe de politică și securitate pentru furnizorii de servicii de încredere care emit marcaje temporale;
- ETSI TS 119 431 (Partea 1) – Cerințe de politică și securitate pentru crearea semnăturilor electronice la distanță;
- ETSI EN 319 412 (Parti 1, 2, 3 și 5) – Profile de certificate și reguli de denumire a subiecților.

Pe parcursul acestui document, termenul „Declarație de Practici” se referă la prezentul document.

1.2. Prezentare generală a serviciilor

Serviciile de încredere sunt structurate logic în componente precum CA, RQSCD și TSA, pentru a respecta cerințele prevăzute în clauza 4.3 din ETSI EN 319 411-1 și clauza 4.2 din ETSI EN 319 421:

- **Servicii de înregistrare**
  - **Autoritatea de înregistrare (RA)**: verifică identitatea și, dacă este cazul, atributele specifice ale unui subiect. Autoritatea de înregistrare furnizează servicii de înregistrare pentru serviciile CA.
- **Serviciile Autorității de Certificare (CA)**
  - **Serviciul de generare a certificatelor**: creează și semnează certificate pe baza identității și a altor atribute verificate de serviciul de înregistrare. Acesta include și generarea cheilor.
  - **Serviciul de diseminare**: distribuie certificatele către subiecți și, cu consimțământul acestora, le pune la dispoziția entităților partenere (relying parties). De asemenea, acest serviciu pune la dispoziția abonaților, subiecților și părților terțe condițiile generale, termenii și informațiile publicate privind politicile și practicile furnizorului de servicii de încredere (TSP).
  - **Serviciul de gestionare a revocărilor**: procesează solicitările și notificările referitoare la revocarea certificatelor pentru a determina acțiunea necesară. Rezultatele acestui serviciu sunt distribuite prin intermediul serviciului de verificare a statutului revocării.
  - **Serviciul de verificare a statutului revocării:** oferă informații privind statutul revocării certificatelor către entități partenere și către alte componente.
- **Serviciul de semnare la distanță**
  - **Serviciul de furnizare a dispozitivelor de creare a semnăturii calificate la distanță (Remote QSCD)** gestionează QSCD în numele subiectului, inclusiv întreținerea cheilor și a datelor de semnătură.
  - **Serviciul de creare a semnăturilor electronice** utilizând aplicația de semnare de tip server.
  - **Serviciul de autentificare** - serviciu care oferă autentificarea subiectului pe baza mijloacelor alocate de serviciul de legare a identității.
  - **Serviciul de legare a identității (Identity Linking Service)** - atribuie și asociază metode de autentificare subiectului.
- **Serviciul TSA (Time Stamping Authority)**
  - **Serviciul de furnizare a marcajelor temporale**: generează marcaje temporale

- **Serviciul de management al marcajelor temporale**: monitorizează și controlează funcționarea serviciilor de marcare temporală pentru a se asigura că serviciul furnizat corespunde specificațiilor TSA. Acest component are responsabilitatea instalării și dezinstalării serviciului de furnizare a marcajelor temporale.

Această subdiviziune a serviciilor are scopul exclusiv de a clarifica cadrul serviciilor de încredere și nu impune nicio restricție privind modul de implementare a serviciilor furnizorului de servicii de încredere (TSP).

1.3. Numele și identificarea documentului

Denumirea completă a acestui document este „Simplifi Certification Practice Statement”. Versiunea electronică a documentului va fi publicată la *https://simplifi.ro/policies/*. Declarația de Practici poate fi identificată de orice parte prin următorul OID: 1.3.6.1.4.1.63578.1.1.2

Declarația de Practici susține și alte OID-uri asociate:

Denumirea documentului	Număr OID
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	1.3.6.1.4.1.63578.1.1.1

1.4. Participanți în infrastructura PKI

Declarația de Practici reglementează principalele roluri și relațiile dintre următoarele părți:

1.4.1. Autorități de certificare

Autoritățile de certificare (Certification Authorities – CAs) sunt operate de Simplifi și au rolul de a emite certificate și liste de revocare (CRL).

Următoarea autoritate de certificare rădăcină (Root CA) este operată de Simplifi:

- Simplifi Root CA G1

Sub autoritatea rădăcină, Simplifi operează următoarele tipuri de Autorități de Certificare Emitente (Issuing CAs):

- Simplifi Qualified CA Class 3 G1

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

Fiecare politică de serviciu de încredere (document de politică) definește profilele de certificate aferente fiecărei autorități de certificare.

1.4.2. Autorități de înregistrare

O **Autoritate de Înregistrare (Registration Authority – RA)** acționează în numele **Autorității de Certificare (CA)** pentru a îndeplini funcții esențiale de verificare a identității și de gestionare a procesului de înscriere pentru emiterea certificatelor. Autoritățile de Înregistrare sunt responsabile de asigurarea faptului că cererile de certificate sunt depuse de persoane sau entități identificate și autorizate corespunzător.

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

Responsabilitățile unei Autorități de Înregistrare includ:

- Identificarea și verificarea identității Subiectului (deținătorul certificatului), în conformitate cu politica de certificare și nivelul de asigurare aplicabil;
- Validarea completitudinii și corectitudinii cererilor de certificate și a documentației justificative;
- Gestionarea cererilor de **emitere**, **reînnoire**, **revocare** și **suspendare** a certificatelor;
- Colectarea și transmiterea în condiții de siguranță către CA a dovezilor de identitate și a datelor aferente cererii;
- Atunci când este cazul, sprijinirea livrării dispozitivelor criptografice sau a datelor de activare aferente.

Simplifi sprijină atât procesele de **identificare la fața locului**, cât și pe cele **la distanță**, inclusiv utilizarea mijloacelor de **identificare electronică** conforme cu **Regulamentul (UE) nr. 910/2014 (eIDAS)** și/sau cu legislația națională română, precum **Legea nr. 455/2001**, **Legea nr. 214/2024** și **OUG nr. 38/2020**. Pentru serviciile de încredere cu nivel ridicat de asigurare, Simplifi se bazează pe mijloace de identificare electronică certificate sau notificate, autorizate în cadrul schemelor naționale și/sau europene.

Decizia finală privind emiterea certificatelor aparține întotdeauna **Autorității de Certificare (CA)**, chiar și atunci când activitățile RA sunt delegate.

1.4.3. 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 (Subscriber) intră într-o relație contractuală cu Simplifi în baza acordului de abonat (subscriber agreement). De regulă, abonatul este chiar deținătorul certificatului (subiectul), însă poate acționa și în numele altui subiect atunci când solicită emiterea unui certificat. Atât persoanele fizice, cât și cele juridice pot fi abonați ai Simplifi.

1.4.4. Entități partenere

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

1.4.5. Alți participanți

Simplifi colaborează cu subcontractanți, precum centre de date, pentru a asigura co-locarea sigură și funcționarea fiabilă a echipamentelor de server și de rețea.

1.5. Utilizarea certificatelor

Domeniul de aplicare al acestui capitol este acoperit într-o politică specifică de servicii de încredere.

1.6. Administrarea Declarației de Practici

1.6.1. Organizația responsabilă de administrarea documentului

Prezenta Declarație de Practici este administrată de Simplifi, cu sediul la:

Strada Gheorghe Țițeica 142, București 014192Romania

1.6.2. Contact

easy@simplifi.ro

1.6.3. Entități responsabile pentru validarea principiilor conținute în document

Echipa Simplifi este responsabilă de evaluarea completitudinii și acurateței prezentei Declarații de Practici, precum și a altor documente asociate serviciilor PKI furnizate de Simplifi, asigurând coerența acestora. Toate întrebările și comentariile referitoare la conținutul acestor documente trebuie transmise la adresa specificată în capitolul 1.6.2

1.6.4. Proceduri de aprobare

Declarația de Practici rămâne în vigoare începând cu data indicată ca dată de intrare în efect, până la publicarea unei versiuni valide ulterioare.
Părțile interesate pot transmite comentarii privind modificările propuse în termen de 14 zile lucrătoare de la anunțarea acestora, conform prevederilor din Capitolul 9.10.
Dacă în acest interval nu sunt formulate obiecții semnificative privind conținutul de fond, noua versiune a Declarației de Practici devine efectivă la data indicată în document.

Aprobarea noii versiuni a Declarației de Practici este responsabilitatea conducerii Simplifi. Toate modificările sunt consemnate în istoricul reviziilor. Documentul aprobat este apoi publicat și comunicat către:

- angajați;
- persoane desemnate în roluri de încredere;
- entități partenere (relying parties);
- subiecți și abonați;
- alți participanți definiți în capitolul 1.4.5.

1.7. Definiții și abrevieri

Definițiile și abrevierile utilizate în acest document sunt furnizate la final.

2. Publicare și responsabilități privind depozitarul de informații

2.1. Depozitar

Simplifi va menține un depozitar electronic care va conține:

- documentele publice, împreună cu versiunile anterioare ale acestora;
- toate certificatele publicate (atât active, cât și revocate) și listele de revocare (CRL);
- versiunea electronică a acestor documente, publicată și accesibilă prin URL-urile care vor fi specificate în versiunile ulterioare ale prezentului document.

Depozitarul este destinat următoarelor entități: subiecți, abonați și entități partenere (relying parties).

2.2. Informații publicate de Simplifi ca Furnizor de Servicii de Încredere

Depozitarul conține cel puțin următoarele documente:

- Declarația de Practici – versiunea curentă și versiunile anterioare;
- Politicile Serviciilor de Încredere – versiunea curentă și versiunile anterioare;
- Termeni și Condiții Generale;
- Certificatele Autorităților de Certificare (CA) și profilurile acestora;

- Listele de Revocare a Certificatelor (CRL);
- Informații suplimentare, la decizia internă a Simplifi (de exemplu, notificări privind incidente semnificative).

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

2.3. Frecvența publicării

Publicațiile sunt emise cu următoarea frecvență:

- Declarația de Practici și politicile specifice ale serviciilor de încredere – conform capitolului 9.9.;
- Certificatele tuturor autorităților care operează servicii de încredere în cadrul Simplifi – la fiecare emitere de noi certificate;
- Lista de Revocare a Certificatelor (CRL) – conform Politicii specifice Serviciului de Încredere și profilului certificatului.

2.4. Revizuire și modificare

Declarația de Practici și politicile specifice ale serviciilor de încredere sunt revizuite anual sau ori de câte ori are loc o modificare semnificativă în furnizarea serviciilor.

2.5. Acces la publicații

Simplifi aplică măsuri de securitate logice și fizice pentru a proteja depozitarul împotriva creării, eliminării sau modificării neautorizate a datelor.

3. Identificare și autentificare

Cerințele privind practicile de identificare și autentificare derivă din standardele ETSI EN 319 411-1 și ETSI EN 319 411-2. Aceste practici se aplică procesului de înregistrare a subiecților în vederea emiterii certificatelor, precum și procesării cererilor de revocare.
Descrierea detaliată a acestor proceduri este prezentată în politicile specifice ale serviciilor de încredere, disponibile public în depozitul electronic menționat în Capitolul 2.1.

4. Cerințe operaționale privind ciclul de viață al certificatelor

Cerințele referitoare la practicile privind ciclul de viață al certificatelor derivă din ETSI EN 319 411-1 și ETSI EN 319 411-2. Aceste practici se aplică proceselor de gestionare a certificatelor.
Descrierea lor detaliată este prezentată în politica specifică serviciului de încredere, disponibilă public în depozitul menționat în Capitolul 2.1.

5. Controale de management, operaționale și fizice

Acest capitol descrie practicile generale implementate de Simplifi, în conformitate cu standardele ETSI EN 319 401 și ETSI EN 319 411-1, concentrându-se pe controalele de management, operaționale și fizice.
Simplifi urmează un proces formal de management al riscurilor pentru definirea și menținerea acestor controale, asigurând revizuirea și actualizarea lor periodică. Consiliul de Administrație al Simplifi aprobă evaluarea riscurilor și își asumă riscurile reziduale identificate.

5.1. Controale de securitate fizică

Simplifi aplică măsuri robuste de securitate fizică și de mediu pentru a proteja integritatea, disponibilitatea și confidențialitatea infrastructurii sale de servicii de încredere.
Aceste controale sunt conforme cu standardele europene relevante (ETSI EN 319 401, EN 319 411-1, ISO/IEC 27001) și cu reglementările naționale românești.

Toate sistemele serviciilor de încredere sunt găzduite într-un centru de date comercial de nivel Tier III+, dotat cu securitate fizică 24/7, straturi multiple de autentificare și monitorizare completă. Autoritatea de Certificare Rădăcină (Root CA) este păstrată offline, în depozit securizat, și este accesibilă doar printr-o procedură cu control dual.

5.1.1. Locația sitului și controale generale

- Infrastructura principală este găzduită într-un centru de date terț de înaltă securitate.
- Paza permanentă (24/7) este asigurată atât la centrul de date, cât și la sediile Simplifi.
- Toate punctele de acces sunt supravegheate prin sisteme video CCTV.
- Accesul vizitatorilor în centrul de date necesită aprobare prealabilă și însoțire de personal autorizat.
- Toate evenimentele de acces fizic în centrul de date sunt înregistrate în jurnale de audit.

5.1.2. Controlul accesului în centrul de date

Accesul la sistemele serviciilor de încredere găzduite în centrul de date este reglementat printr-un model de control pe mai multe niveluri:

- **Nivel 1** – Intrare în clădire: necesită identificare validă (ex. carte de identitate, pașaport) și înregistrare a vizitatorului la recepție; monitorizat video (CCTV) și înregistrat manual.
- **Nivel 2** – Acces pe etaj: controlat prin card de proximitate, limitat la anumite zone sau etaje.
- **Nivel 3** – Acces la rack: infrastructura Simplifi este găzduită într-un rack dedicat (jumătate de rack), securizat cu cod PIN; accesul este limitat la personal autorizat.

- **Nivel 4** – Acces la Root CA: sistemele Root CA sunt păstrate offline și stocate într-o locație fizic separată.

5.1.3. Controale legate de mediu

- Sisteme de detecție și stingere a incendiilor sunt instalate în toate zonele critice.
- Sistemele HVAC controlează temperatura și umiditatea conform specificațiilor echipamentelor.
- UPS-uri și generatoare asigură alimentarea neîntreruptă cu energie electrică.
- Serverele sunt montate pe podele tehnice ridicate, pentru a reduce riscul de inundații.

5.1.4. Manipularea mediilor de stocare și eliminarea sigură a deșeurilor

- Mediile sensibile (ex. **materiale criptografice, backup-uri**) sunt stocate în **dulapuri securizate cu acces controlat**.
- Eliminarea mediilor fizice și electronice urmează **proceduri stricte**:
  - Cheile criptografice și HSM-urile sunt șterse complet sau distruse fizic;
  - Documentele pe hârtie sunt tocate;
  - Hardware-ul este curățat de date (sanitizat) sau decomisionat conform recomandărilor producătorului.

5.1.5. Backup extern și plan de recuperare în caz de dezastru

- **Datele de backup** sunt replicate către un sit secundar securizat și distinct.
- Backup-urile externe sunt protejate împotriva accesului neautorizat, incendiilor și expunerii la apă.
- Procedurile de recuperare în caz de dezastru (Disaster Recovery) asigură restabilirea serviciilor în maximum **48 de ore** de la producerea unui incident major.

5.2. Controale procedurale

5.2.1. Roluri de încredere

Pentru a consolida securitatea informațiilor și a preveni conflictele de interese, Simplifi a desemnat personal specializat în roluri de încredere. Atribuirea funcțiilor acestor roluri respectă principiul separării clare a responsabilităților. Responsabilitățile specifice și distribuția acestor roluri sunt definite în documentația internă a Simplifi.

Rolurile de încredere stabilite în cadrul Simplifi sunt următoarele:

- **CEO/Manager Servicii de Încredere** –responsabil de managementul general al Simplifi; stabilește direcțiile de dezvoltare ale autorității de certificare; gestionează Declarația de Practici și politicile serviciilor de încredere,
- **Ofițer de Securitate** – supraveghează implementarea și aplicarea procedurilor de securitate a sistemului informatic; inițiază și supervizează procesele de generare a cheilor criptografice și a secretelor partajate; atribuie drepturi în domeniul securității și al privilegiilor de access ale utilizatorilor.
- **Administrator de Sistem** –instalează sau supraveghează instalarea echipamentelor hardware și a software-ului de sistem; efectuează configurarea inițială a sistemelor, dispozitivelor HSM și resurselor de rețea; coordonează procesul de management al schimbărilor și este responsabil de procedurile de backup.
- **Operator de Sistem** –în colaborare cu Administratorul de Sistem și, atunci când este necesar, sub supravegherea directă a acestuia, efectuează operațiuni pentru menținerea disponibilității serviciilor,
- **Ofițer de Înregistrare** –verifică identitatea subiecților și corectitudinea cererilor de certificare depuse; autorizează cererile de certificare; aprobă politicile de identificare puse la dispoziție de furnizorii externi de validare a identității.
- **Auditor de Sistem** –monitorizează serviciile pentru a asigura conformitatea cu politicile și procedurile; verifică jurnalele de evenimente și procesele de gestionare a incidentelor.
- **Ofițer Juridic și de Protecție a Datelor -** asigură conformitatea cu legislația aplicabilă privind eIDAS și GDPR; revizuiește obligațiile contractuale, termenii și condițiile, politicile de confidențialitate și clauzele de răspundere.

Serviciile de încredere Simplifi pot implica și personal operațional care, deși nu deține un rol de încredere formal, îndeplinește sarcini sub supraveghere directă și fără acces la procesele de prelucrare a datelor.

5.2.2. Principiul celor patru ochi

Pentru operațiunile cu un nivel ridicat de criticitate în materie de securitate, participarea a cel puțin două persoane este o cerință fundamentală.
Această regulă este aplicată prin măsuri tehnice și organizatorice, care includ controlul permisiunilor de acces și verificarea cunoștințelor și autorizărilor persoanelor implicate.

Următoarele activități necesită implicarea a minimum două persoane:

- Inițializarea modulelor HSM;
- Generarea cheilor de certificare pentru Root CA și subordonatele CA (SubCAs);
- Backup-ul cheilor Autorităților de Certificare (CAs);
- Restaurarea cheilor de certificare pentru Root CA și pentru Autoritățile de Certificare Emitente (Issuing CAs).

5.2.3. Identificare și autentificare pentru fiecare rol

Toate rolurile de încredere sunt desemnate în mod formal de către CEO.
Verificarea identității persoanelor este realizată ca parte a procesului de resurse umane (HR).

Simplifi a implementat o procedură de onboarding pentru fiecare persoană desemnată, care include emiterea de credențiale personale de autentificare pentru accesul la sistemele IT și în spațiile fizice.
Fiecare cont de acces este unic și atribuit unei singure persoane, asigurând astfel trasabilitatea și responsabilitatea acțiunilor.

Fiecare persoană desemnată într-un rol de încredere își asumă în mod formal responsabilitățile asociate acelui rol.

5.2.4. Roluri care necesită segregarea atribuțiilor

Fiecărui rol de încredere i se acordă doar permisiunile strict necesare pentru îndeplinirea responsabilităților atribuite. Anumite roluri pot fi combinate sau modificate doar într-un scop limitat și bine definit. Rolurile de Security Officer și System Auditor sunt strict separate de toate celelalte roluri și nu pot fi cumulate.

Simplifi a implementat un proces de substituire controlat, care asigură continuitatea operațiunilor menținând în același timp respectarea principiului separării atribuțiilor.

5.3. Controlul securității personalului

5.3.1. Calificări, experiență și avize

Politica de resurse umane a Simplifi stabilește cerințele pentru angajare și pentru atribuirea rolurilor desemnate. Aceasta include un proces de verificare care evaluează calificările profesionale și documentele oficiale ale candidaților.

Fiecare rol este definit printr-o descriere detaliată a postului, care precizează competențele și experiența necesare. Toți angajații sunt informați cu privire la procedurile disciplinare prevăzute în politică, ceea ce sprijină responsabilitatea individuală și respectarea standardelor organizaționale.

5.3.2. Proceduri de verificare a personalului

Simplifi verifică informațiile privind personalul în următoarele domenii:

- confirmarea locurilor de muncă anterioare;
- verificarea recomandărilor;
- confirmarea studiilor absolvite;
- verificarea cazierului judiciar (dacă este aplicabil);
- verificarea identității.

Simplifi se asigură că niciun angajat nu are acces la funcțiile de încredere până când toate verificările necesare nu au fost finalizate cu succes.

5.3.3. Cerințe de instruire

Simplifi impune ca persoanele desemnate în roluri de încredere să îndeplinească criterii stricte de competență și experiență încă de la angajare și să participe la programe regulate de instruire pentru menținerea calificărilor. Programele de instruire acoperă cel puțin următoarele domenii:

- reglementările naționale și europene aplicabile;
- responsabilitățile și sarcinile specifice fiecărui rol;
- politicile de securitate a informațiilor;
- protecția datelor cu caracter personal;
- controalele și procedurile de securitate bazate pe standardele și politicile interne Simplifi, cu accent pe procedurile de continuitate a afacerii și de recuperare în caz de incident

5.3.4. Frecvența și cerințele instruirii

Instruirea descrisă în capitolul 5.3.3. trebuie repetată cel puțin o dată la 12 luni sau ori de câte ori sunt aduse modificări semnificative Declarației de Practici (CPS) ori altor politici interne.

Tot personalul implicat în operarea serviciilor de încredere Simplifi — inclusiv persoanele care îndeplinesc funcții în cadrul Autorității de Certificare (CA), Autorității de Înregistrare (RA) sau sistemelor de suport — trebuie să finalizeze o instruire structurată înainte de a prelua responsabilități operaționale, administrative sau de securitate.

Scopul instruirii este de a garanta că fiecare persoană deține cunoștințele, competențele și nivelul de conștientizare necesare pentru a-și îndeplini atribuțiile în conformitate cu:

- Declarația de Practici de Certificare (CPS) curentă și politicile serviciilor de încredere asociate;
- procedurile interne de securitate și operare aplicabile rolului respectiv;
- software-ul, hardware-ul și sistemele criptografice utilizate de Autoritățile de Certificare și Autoritățile de Înregistrare;
- obligațiile legale și de reglementare prevăzute de Regulamentul eIDAS, legislația română și standardele aplicabile.

Temele de instruire includ:

- principiile, structura și cerințele Declarației de Practici (CPS) și ale Politicilor Serviciilor de Încredere Simplifi;
- procedurile operaționale și controalele de securitate implementate în cadrul sistemelor CA/RA;
- responsabilitățile și restricțiile asociate rolurilor atribuite;
- procedurile de răspuns la incidente în caz de defecțiune a sistemului, eveniment de securitate sau încălcare a politicilor;
- manipularea materialului criptografic, autentificarea securizată și cerințele privind controlul dual.

La finalizarea instruirii, participanții semnează o declarație formală de înțelegere și acceptare a responsabilităților, confirmând respectarea Declarației de Pracitici, a politicilor serviciilor de încredere și a politicilor interne de securitate.

Reinstruire și actualizări de conștientizare:

- Reinstruirea este recomandată cel puțin o dată la 12 luni sau mai devreme dacă:
  - sunt aduse actualizări semnificative Declarației de Practici, Politicilor sau procedurilor interne;
  - angajatul preia un nou rol cu responsabilități suplimentare de securitate;
  - un incident major sau un audit relevă deficiențe care necesită instruire specifică.

Simplifi menține evidențe ale tuturor sesiunilor de instruire finalizate și ale declarațiilor semnate de participanți. Managerii și personalul care ocupă roluri critice din punct de vedere al securității sau conformității beneficiază suplimentar de sesiuni de conștientizare

privind securitatea, axate pe managementul riscurilor, răspunsul la incidente și obligațiile legale prevăzute de cadrul aplicabil al serviciilor de încredere.

5.3.5. Frecvența și secvența rotației posturilor

Nu se aplică.

5.3.6. Sancțiuni pentru acțiuni neautorizate

Personalul este obligat, prin contractul de muncă, să își îndeplinească atribuțiile în conformitate cu regulamentele interne. Nerespectarea acestora poate atrage sancțiuni disciplinare, civile sau penale, în funcție de gravitatea faptei.

5.3.7. Cerințe pentru contractanții independenți

Contractanții independenți sunt supuși acelorași condiții de confidențialitate și protecție a datelor ca și angajații. În baza unui contract semnat, persoanele sau consultanții externi sunt supuși aceleiași proceduri de verificare stabilite prin politica de resurse umane (HR).

5.3.8. Documentație disponibilă personalului

Personalul Simplifi are acces la următoarele documente:
Declarația de Practici de Certificare (CPS);

- Politica Simplifi privind serviciile de încredere pentru emiterea certificatelor calificate pentru semnături și sigilii electronice, gestionarea dispozitivelor de creare la distanță a semnăturilor și sigiliilor electronice și serviciile de marcare temporală;
- Extrase din documentația corespunzătoare rolului îndeplinit, inclusiv proceduri de urgență;
- Aria de responsabilități și obligațiile asociate rolului exercitat în sistem.

5.4. Proceduri de audit și jurnalizare

5.4.1. Tipuri de evenimente înregistrate

Simplifi generează și stochează jurnale (loguri) ale evenimentelor asociate serviciilor de încredere și serviciilor de identificare electronică. Aceste jurnale conțin cel puțin următoarele informații:

- pornirea și oprirea sistemelor;
- blocări de sistem și defecte hardware;
- trafic de rețea de intrare și de ieșire;
- activități legate de administrarea utilizatorilor și gestionarea permisiunilor, inclusiv accesul (privilegiat sau nu) la sisteme și aplicații;
- activități efectuate prin conturi de administrator;

- modificări ale fișierelor de configurare critice și ale copiilor de siguranță.
- jurnale relevante pentru securitate;
- utilizarea și performanța resurselor de sistem;
- accesul fizic la instalații, acolo unde este aplicabil;
- accesul și utilizarea echipamentelor și dispozitivelor de rețea;
- evenimente de mediu (temperatură, umiditate etc.), acolo unde este aplicabil;
- informațiile de înregistrare colectate de autoritatea de înregistrare (RA);
- evenimente legate de ciclul de viață al certificatelor și cheilor criptografice;
- evenimente legate de funcționarea serviciului de marcare temporală (TSA);
    - recalibrări și sincronizări de rutină ale ceasului sistemului;
    - gestionarea cheilor și certificatelor unității de marcare temporală (TSU);
    - incidente asociate modificărilor sau deplasărilor neautorizate ale timpului (time-shifting).

Înregistrările includ cel puțin următoarele informații:

- tipul evenimentului;
- identificatorii evenimentului;
- data și ora producerii evenimentului;
- sursa jurnalului (logului);
- starea evenimentului.

Doar persoanele autorizate din cadrul echipei Simplifi au acces la informațiile conținute în aceste înregistrări.

Sursele primare ale jurnalelor sunt aplicațiile și sistemele asociate serviciilor de încredere și serviciilor de identificare electronică.
Jurnalele de audit sunt colectate și înregistrate cu măsuri de protecție împotriva modificărilor interne sau externe și împotriva accesului neautorizat.

5.4.2. Frecvența procesării jurnalelor

Jurnalele și activitățile de monitorizare sunt verificate în mod regulat pentru a identifica eventualele neconcordanțe.Jurnalele de audit sunt revizuite periodic pentru a detecta orice dovadă de activitate malițioasă, precum și după fiecare operațiune importantă.

5.4.3. Perioada de păstrare a înregistrărilor

Jurnalele de audit care acoperă în mod direct furnizarea serviciilor de încredere sunt păstrate pentru o perioadă de 10 ani.

5.4.4. Protecția înregistrărilor

Simplifi păstrează jurnalele de audit în sisteme de stocare dedicate. Pentru a le asigura integritatea și confidențialitatea, sunt implementate controale de securitate, inclusiv monitorizarea accesului și cerințe de autorizare și stocarea pe suport criptat, pentru a preveni accesul neautorizat.

Întreaga infrastructură și serviciile de încredere Simplifi sunt sincronizate cu Timpul Universal Coordonat (UTC), actualizarea având loc cel puțin o dată pe zi.

La expirarea perioadei de păstrare, toate înregistrările sunt migrate în siguranță în arhivă, procesul fiind monitorizat și trasabil.

În cazul unor proceduri legale, Simplifi poate recupera și prezenta dovezile necesare.

5.4.5. Copiere de siguranță a înregistrărilor

Înregistrările jurnalelor sunt copiate periodic și stocate în siguranță, în conformitate cu procedurile stabilite, care includ un calendar specific de backup.

5.4.6. Sistemul de colectare a jurnalelor de audit

Fiecare aplicație colectează automat și transmite înregistrările de log către sistemul central de jurnalizare.
În cazul punctelor de înregistrare, pot fi colectate și documente pe suport de hârtie, care trebuie arhivate și documentate corespunzător.

Funcțiile de jurnalizare sunt inițiate automat la pornirea sistemului și sunt menținute continuu pe întreaga durată de funcționare a acestuia.

În cazul unei defecțiuni a sistemelor automate de monitorizare sau de jurnalizare, incidentul este tratat conform procedurii de management al incidentelor.

5.4.7. Sistem de notificare a subiectului în cazul unui eveniment

Sistemele IT ale Simplifi sunt monitorizate continuu. O echipă dedicată supraveghează permanent serviciile de încredere Simplifi pentru a urmări performanța și a detecta evenimentele de securitate.

Dacă este identificată o activitate care poate afecta securitatea sistemului, acesta trimite automat alerte cel puțin către Ofițerul de Securitate și Administratorul de Sistem.

În cazul detectării unui incident semnificativ, procesul de management al incidentelor include notificarea autorității de supraveghere și, dacă este necesar, informarea subiectului afectat.

5.4.8. Evaluarea vulnerabilităților

Simplifi a implementat o procedură de management al vulnerabilităților și o procedură de management al riscurilor. Conform acestor proceduri, toate activele — inclusiv software-ul și sistemele de operare care susțin furnizarea serviciilor acoperite de acest document — trebuie să fie supuse unei analize de vulnerabilitate.

Analiza de risc se efectuează cel puțin o dată pe an, precum și în următoarele situații: introducerea de noi servicii, implementarea unor modificări majore de arhitectură, apariția unui incident de securitate.

Întreaga infrastructură este supusă scanării de vulnerabilități cel puțin trimestrial, proces efectuat de un expert independent. Dacă sunt identificate vulnerabilități, se activează procedura de management al vulnerabilităților, pentru remedierea și atenuarea riscurilor constatate.

5.5. Arhivarea înregistrărilor

5.5.1. Tipuri de arhive

Simplifi arhivează toate datele legate de:

- informațiile de înregistrare – toate documentele și datele utilizate în procesul de verificare a identității;
- toate cererile transmise de utilizatorii serviciilor Simplifi, inclusiv cererile de utilizare a certificatelor;
- toate evenimentele legate de ciclul de viață al cheilor gestionate de CA, inclusiv orice perechi de chei generate pentru subiecți de către CA;
- listele de revocare a certificatelor (CRL);
- termenii și condițiile acceptate de Subiect/Abonat;
- alte documente legate de furnizarea serviciilor de încredere și a serviciilor de identificare electronică.

5.5.2. Perioada de păstrare a arhivelor

Datele arhivate (pe suport hârtie și în format electronic) sunt păstrate minimum 7 ani după ce orice certificat bazat pe aceste înregistrări își încetează valabilitatea.

5.5.3. Protecția arhivelor

Simplifi stochează arhivele în spații de depozitare dedicate. Pentru a garanta integritatea și confidențialitatea acestora, Simplifi a implementat măsuri de securitate care includ acces monitorizat, permis doar persoanelor autorizate și criptarea mediilor de stocare pentru a preveni accesul neautorizat.

Pe durata perioadei de păstrare, Simplifi monitorizează mediile de stocare a datelor arhivate pentru a asigura disponibilitatea acestora pe întreaga perioadă necesară.

Este permisă stocarea arhivelor într-un serviciu extern de arhivare, cu condiția respectării acelorași cerințe de securitate.

5.5.4. Proceduri de backup pentru arhive

Simplifi a implementat un proces de backup al arhivelor pentru a asigura recuperarea datelor în cazul unei defecțiuni a mediului de stocare primar. Acest mecanism garantează posibilitatea restaurării arhivelor din copiile de rezervă.
Procedurile detaliate privind arhivarea, crearea copiilor de siguranță și recuperarea datelor sunt descrise în documentația internă.

5.5.5. Cerințe privind marcarea temporală a arhivelor

Arhivele sunt păstrate de furnizori terți care asigură o reprezentare exactă a timpului.

5.5.6. Stocarea arhivelor

Sistemul de colectare a arhivelor este o soluție internă Simplifi, iar ulterior datele sunt transferate către un serviciu extern administrat de furnizori terți.

5.5.7. Accesul la informațiile arhivate și verificarea acestora

Accesul la arhive este permis doar persoanelor care dețin roluri de încredere, fiind posibil numai după o autorizare reușită.
Pentru verificarea integrității datelor arhivate, se efectuează teste periodice, iar datele sunt comparate cu înregistrările originale. Acest proces poate fi efectuat sub supravegherea administratorului de sistem și a ofițerului de securitate, iar toate activitățile sunt documentate în jurnalul de evenimente.

5.6. Schimbarea cheilor

Procedura de schimbare a cheilor se aplică cheilor autorităților de certificare (Root CA, CA, CA subordonate).Procesul de schimbare a cheilor este efectuat astfel încât să se asigure menținerea perioadei minime de valabilitate a certificatelor convenite.

Înainte de expirarea oricărui certificat al unei autorități de certificare, se stabilește o nouă infrastructură PKI. Ca parte a acestui proces, este generată o nouă pereche de chei și un nou certificat pentru noua autoritate de certificare.

Pe durata perioadei de tranziție, atât autoritatea veche, cât și cea nouă funcționează în paralel, până la expirarea certificatului autorității vechi. Noua autoritate de certificare preia rolul celei care expiră și gestionează toate activitățile legate de certificate, inclusiv emiterea, suspendarea, revocarea și generarea CRL-urilor.

Autoritatea de certificare care expiră continuă să proceseze doar revocările certificatelor emise sub propria infrastructură și să genereze listele de revocare (CRL) până la încetarea activității sale operaționale odată cu expirarea certificatului.

Certificatul noii autorități de certificare este publicat prompt în depozitarul public pentru a asigura continuitatea activității și a încrederii.

5.7. Compromiterea și Recuperarea în caz de Dezastru

5.7.1. Proceduri de gestionare a incidentelor și compromiterilor

Gestionarea incidentelor și răspunsul la amenințări sunt reglementate prin procedurile descrise în Planul de Continuitate a Activității și în procesul de management al incidentelor.

Simplifi revizuiește și testează aceste proceduri cel puțin o dată pe an pentru a confirma eficiența și adecvarea lor.

Incidentele pot fi raportate prin formulare interne sau externe, ori prin trimiterea unui e-mail la adresa: easy@simplifi.ro

Echipa de Evaluare a Incidentelor răspunde în funcție de gravitatea incidentului, având un timp maxim de răspuns de 24 de ore în zilele lucrătoare.

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

Toate informațiile referitoare la coruperea resurselor informatice, software-ului și/sau datelor sunt comunicate Ofițerului de Securitate, care atribuie sarcinile necesare în conformitate cu procedurile stabilite de management al incidentelor, riscurilor și schimbărilor.

Aceste proceduri sunt concepute pentru a evalua gravitatea incidentului, a investiga în detaliu cauza acestuia, a minimiza impactul și a implementa măsuri de prevenire pentru a evita reapariția unor incidente similare în viitor.

5.7.3. Compromiterea cheii private a CA sau pierderea calibrării ceasului TSU

Compromiterea unei chei este gestionată în conformitate cu procedurile de Management al Incidentelor. Deoarece un astfel de eveniment este considerat și dezastru operațional, se activează planul de continuitate a activității.

În cazul unei compromiteri, suspiciuni de compromitere sau pierderi de integritate care afectează o Autoritate de Certificare (CA) sau o Autoritate de Marcaj Temporal (TSA), Simplifi urmează un set clar de acțiuni imediate:

- Autoritatea afectată este imediat dezactivată.
- În cazul în care Autoritatea de Marcaj Temporal (TSA) este compromisă, suspectată de compromitere sau își pierde calibrarea, Simplifi oprește emiterea de marcaje temporale până la restabilirea în siguranță a funcționării corecte prin măsuri de remediere.

- Autoritatea de Certificare generează o nouă pereche de chei criptografice.
- Toate certificatele emise sub autoritatea CA compromisă sunt revocate și adăugate în Lista de Revocare a Certificatelor (CRL), cu motivul corespunzător.
- Certificatul asociat cheii compromise este, de asemenea, inclus în CRL, cu un motiv adecvat de terminare.
- Utilizatorii afectați sunt notificați prompt prin canale de comunicare publică, inclusiv anunțuri pe site-ul Simplifi și e-mail.
- Entitățile partenere (Relying Parties) sunt informate prin aceleași canale.
- Noi certificate sunt emise pentru toți utilizatorii afectați.
- Certificatele de înlocuire sunt furnizate fără costuri pentru utilizatori; toate cheltuielile sunt suportate de Simplifi.
- Este efectuată o analiză imediată a incidentului, urmată de întocmirea unui raport formal care detaliază cauza compromiterii.

În cazul compromiterii sau suspiciunii de compromitere a cheilor Unității de Marcaj Temporal (TSU) sau al unei desincronizări a timpului între TSU și sursa sa de timp de încredere, Simplifi va furniza abonaților toate informațiile necesare pentru a identifica orice marcaje temporale emise incorect — cu condiția ca această acțiune să nu încalce confidențialitatea abonaților și să nu compromită securitatea serviciilor Simplifi. Informațiile furnizate vor include, cel puțin numele autorității de marcaj temporal calificate implicate și fereastra de timp în care a avut loc emiterea necorespunzătoare.

Dacă algoritmii sau parametrii criptografici utilizați de autoritățile de certificare ale Simplifi nu mai sunt considerați suficienți pentru a menține nivelul de încredere necesar, Simplifi va notifica toți deținătorii de certificate prin anunțuri publice, inclusiv publicare în mass-media și transmitere prin e-mail.

5.7.4. Managementul Continuității Activității

Simplifi menține un Plan de Continuitate a Activității (BCP) cuprinzător, care descrie riscurile potențiale, strategiile de remediere și timpii acceptabili de recuperare. Un element esențial al planului îl constituie măsurile preventive pentru a evita reapariția incidentelor care au determinat activarea planului.

Simplifi efectuează analize periodice de risc pentru a identifica potențialele amenințări și pentru a determina măsurile tehnice și organizaționale adecvate de prevenire și atenuare a acestora. Riscurile identificate sunt evaluate și actualizate sistematic, iar Consiliul de Administrație este responsabil de aprobarea planurilor de tratare a riscurilor și de acceptarea riscurilor reziduale.

Pentru a asigura continuitatea operațională a serviciilor, Simplifi efectuează copii de siguranță (backup) ale tuturor datelor, informațiilor și aplicațiilor esențiale, stocate într-o

locație sigură, aflată la o distanță determinată de locația principală. Această măsură permite restaurarea rapidă a operațiunilor în cazul unor incidente majore sau dezastre.

Back-up-urile sunt testate în mod regulat pentru a verifica eficiența și conformitatea lor cu cerințele planului de continuitate a activității.

5.8. Plan de Încetare a Activității

Simplifi menține un plan actualizat și cuprinzător de încetare a activității, care se aplică în cazul întreruperii serviciilor de încredere, pentru a asigura un impact minim asupra abonaților și entităților partenere.

Înainte de încetarea activității, Simplifi va notifica toate părțile afectate, inclusiv abonații, entitățile partenere (relying parties), alți furnizori de servicii de încredere (TSP), autoritățile de supraveghere relevante. De asemenea, informațiile privind încetarea serviciilor vor fi făcute publice pentru a garanta că toate părțile interesate sunt informate în mod corespunzător.

Autorizațiile acordate subcontractorilor care acționează în numele Simplifi vor fi revocate înainte de închiderea serviciilor.

Acolo unde este posibil, Simplifi va transfera obligațiile sale către o terță parte de încredere, responsabilă pentru păstrarea în siguranță a înregistrărilor esențiale, cum ar fi datele de revocare și certificatele infrastructurii PKI, pentru o perioadă rezonabilă. Dacă nu sunt păstrate înregistrări, Simplifi va furniza o justificare formală.

Înainte de încetarea serviciilor, toate cheile private, inclusiv copiile de rezervă, vor fi distruse sau dezactivate în siguranță, astfel încât să nu poată fi recuperate sau utilizate în mod abuziv.

Atunci când este posibil, Simplifi va asigura migrarea serviciilor active către un alt furnizor calificat de servicii de încredere (QTSP), pentru a menține continuitatea serviciilor pentru clienții existenți.

Simplifi deține măsuri financiare de siguranță pentru a acoperi toate obligațiile legate de încetarea activității, inclusiv în caz de insolvență sau faliment.

În final, Simplifi va menține sau va transfera responsabilitatea de a asigura că cheile sale publice și tokenurile serviciilor de încredere rămân accesibile entităților partenere pentru o perioadă corespunzătoare după încetarea serviciilor.

6. Controlul securității tehnice

Acest capitol descrie practicile derivate din standardele ETSI EN 319 411-1, ETSI EN 319 411-2 și ETSI EN 319 421. Cerințele acoperă în mod cuprinzător descrierea controalelor tehnice de securitate, incluzând în principal:

- Managementul și protecția materialului criptografic (generarea, distribuirea, activarea, ștergerea cheilor private etc.);

Practici detaliate pentru fiecare serviciu de încredere sunt prevăzute în politicile de servicii de încredere separate implementate de Simplifi.

- Managementul securității IT și ciclul de viață al mecanismelor de securitate.

Practici comune tuturor serviciilor sunt specificate în următoarele subcapitole, începând cu capitolul 6.4.

6.1. Generarea și instalarea perechii de chei

Abordarea acestui element este detaliată în politicile specifice serviciilor de încredere, disponibile public în depozitarul menționat în Capitolul 2.1.

6.2. Protecția cheilor private și ingineria modulelor criptografice

Abordarea acestui element este detaliată în politicile specifice serviciilor de încredere, disponibile public în depozitarul menționat în Capitolul 2.1.

6.3. Date de activare

Abordarea acestui element este detaliată în politicile specifice serviciilor de încredere, disponibile public în depozitarul menționat în Capitolul 2.1.

6.4. Controlul securității informatice

6.4.1. Cerințe tehnice specifice de securitate informatică

Simplifi se asigură că toate componentele sistemului Furnizorului de Servicii de Încredere (TSP) sunt operate și administrate în condiții de securitate, cu un nivel acceptabil de risc.

Funcțiile de securitate sunt furnizate de sistemul de operare sau printr-o combinație de software de sistem, aplicații și măsuri fizice de protecție.

Infrastructura TSP include următoarele mecanisme de securitate:

- impunerea autentificării utilizatorilor pentru toate persoanele care dețin roluri de încredere;
- aplicarea controalelor de acces bazate pe principiul privilegiului minim;

- politici stricte de parolă pentru prevenirea accesului neautorizat;
- implementarea autentificării multi-factor (MFA) pentru verificarea sporită a identității;
- utilizarea protocoalelor criptografice pentru securizarea comunicațiilor de sesiune;
- monitorizarea continuă a sistemelor IT și mecanisme de alertare în timp real;
- capabilități de audit al securității pentru urmărirea activității sistemului;
- protecții împotriva codului malițios, inclusiv mecanisme de detecție și prevenție;
- asigurarea integrității software-ului și firmware-ului și actualizarea regulată a sistemelor;
- aplicarea unei politici de birou curat (clean-desk) și activarea automată a blocării ecranului sau a expirării sesiunii.

Accesul la sistemele serverului se realizează numai sub supravegherea unui administrator și exclusiv prin conexiuni criptate.

6.4.2. Ratingul de securitate informatică

Nu se aplică

6.5. Controlul securității pe parcursul ciclului de viață

Măsurile de securitate sunt evaluate prin diferite metode, cum ar fi: evaluări de risc, teste de penetrare sau audituri interne.

6.5.1. Controlul dezvoltării sistemelor

Analiza cerințelor de securitate este realizată în etapa de proiectare și definire a cerințelor pentru fiecare proiect de dezvoltare de sistem derulat de Simplifi.
Înainte de orice implementare în producție, se efectuează teste de acceptanță într-un mediu de dezvoltare și test, urmate de o aprobare formală pentru a asigura conformitatea și pregătirea sistemului pentru punerea în funcțiune.
Pentru modulele criptografice, Simplifi utilizează exclusiv produse certificate care respectă standardele tehnice stabilite (ETSI/CEN). Simplifi nu își definește cerințe proprii în acest sens.

6.5.2. Controlul managementului securității

Măsurile de securitate sunt implementate în cadrul politicii de securitate a informațiilor a Simplifi.
Configurațiile curente și modificările sistemelor Simplifi sunt documentate conform procedurilor de management al schimbărilor.

6.5.3. Controlul securității pe parcursul ciclului de viață

Măsurile de securitate sunt evaluate prin diferite metode, cum ar fi: evaluări de risc, teste de penetrare sau audituri interne

6.6. Controlul securității rețelei

Simplifi implementează următoarele măsuri de securitate a rețelei:

- Segmentarea rețelei
    - Zonă de securitate ridicată fără acces direct la Internet (Root CA);
    - Zonă de securitate ridicată cu rețea dedicată și acces izolat (HSM, RQSCD);
    - Zonă de securitate normală cu acces controlat la Internet.
- Controlul accesului
    - Acces fizic și logic restricționat la echipamentele de rețea;
    - Comunicare securizată prin Internet utilizând tuneluri VPN pentru protecția transmisiei datelor.
- Consolidare (Hardening)
    - Configurarea echipamentelor de rețea prin dezactivarea porturilor și serviciilor neutilizate, pentru reducerea suprafeței de atac.
- Monitorizare
    - Implementarea de firewall-uri pentru controlul traficului de rețea, atât la intrare, cât și la ieșire;
    - Echipa NOC (la nivelul centrului de date) asigură monitorizarea 24/7 și detectarea evenimentelor anormale.
- Auditarea configurațiilor
    - Audituri interne periodice ale configurațiilor de rețea pentru a verifica respectarea politicilor de securitate și a celor mai bune practici.
- Separarea rețelelor
    - Separarea rețelei administrative de activitățile operaționale pentru izolarea funcțiilor critice (prin subrețele dedicate);
    - Separare clară între mediul de producție și cel de testare/dezvoltare
- Scanare periodică de vulnerabilități a infrastructurii de rețea (cel puțin trimestrial);
- Implementarea protecției antivirus pentru detectarea și prevenirea infecțiilor malware pe stațiile de lucru.

6.7. Sincronizarea timpului

Toate componentele serviciilor de încredere sunt sincronizate periodic cu un serviciu de timp de înaltă precizie. Simplifi utilizează protocolul NTP, conectat la surse GPS (STRATUM 1), pentru a asigura acuratețea orei în următoarele procese:

- Stabilirea orei inițiale de valabilitate a unui certificat CA;
- Revocarea unui certificat CA;
- Publicarea actualizărilor listei de revocare a certificatelor (CRL).
- Emiterea certificatelor pentru subiecți (end entity certificates).

Ajustările de ceas sunt tratate ca evenimente auditate, fiind înregistrate și monitorizate pentru a garanta trasabilitatea și integritatea operațiunilor.

7. Profiluri de Certificate și de CRL

Politicile distincte de servicii de încredere definesc profilurile certificatelor, care sunt aliniate la următoarele standarde:

- ETSI EN 319 412-1
- ETSI EN 319 412-2
- ETSI EN 319 412-3
- ETSI EN 319 412-5

Structura acestor profiluri este descrisă în politicile specifice de servicii de încredere, disponibile public în depozitul menționat în Capitolul 2.1.

8. Audit de Conformitate și Alte Evaluări

Serviciile de încredere furnizate de Simplifi sunt auditate pentru a verifica conformitatea cu:

- Regulamentul eIDAS;
- Practicile descrise în prezentul document;
- Legislația română aplicabilă.

Rezultatele auditurilor sunt incluse în raportările de management și au rolul de a demonstra conformitatea, precum și de a sprijini îmbunătățirea continuă a serviciilor.

8.1. Frecvența sau circumstanțele evaluărilor

Un Organism de Evaluare a Conformității (CAB) evaluează conformitatea sistemelor informatice, politicilor, practicilor operaționale, facilităților, personalului și activelor Simplifi, în conformitate cu legislația română, Regulamentul eIDAS și standardele ETSI aplicabile.

Aceste evaluări sunt efectuate cel puțin o dată la doi ani sau ori de câte ori are loc o modificare semnificativă în operațiunile serviciilor de încredere.
În plus, Simplifi a desemnat un auditor de sistem intern, responsabil cu efectuarea verificărilor și auditurilor interne, conform programului intern de audit.

8.2. Calificarea auditorilor

Auditurile externe sunt efectuate de un Organism de Evaluare a Conformității (CAB) acreditat conform ISO/IEC 17065, în conformitate cu ETSI EN 319 403, cu accent pe îndeplinirea cerințelor specificate în Regulamentul eIDAS (UE) nr. 910/2014. CAB-ul este autorizat să efectueze evaluări de conformitate ale Furnizorilor Calificați de Servicii de Încredere și ale serviciilor acestora.

Auditul intern este efectuat de angajați Simplifi sau de terți care dețin experiență și calificare adecvată în domeniul infrastructurilor cu chei publice (PKI), exploatării securizate a sistemelor informatice și securității informației în general.

8.3. Relația auditorului cu Simplifi

Simplifi a selectat un auditor CAB complet independent de organizație.

8.4. Aria de acoperire a auditului

Organismul de Evaluare a Conformității (CAB) auditează toate componentele sistemului informatic utilizat pentru furnizarea Serviciilor de Încredere.

Auditul extern realizat de CAB acoperă întregul domeniu operațional al Simplifi legat de serviciile calificate de certificare, în conformitate cu legislația română și Regulamentul (UE) nr. 910/2014, ținând cont de toate standardele și documentele de standardizare relevante. Evaluarea include următoarele domenii:

- Documentația;
- Arhivele;
- Datele referitoare la emiterea și gestionarea certificatelor calificate;
- Securitatea fizică și informatică, precum și fiabilitatea sistemelor tehnologice și a managementului organizațional.

În paralel, auditurile interne se concentrează asupra următoarelor aspecte:

- Evaluarea operațiunilor Furnizorului de Servicii de Încredere pentru conformitate cu Politicile de Serviciu de Încredere și Declarația de Practici;
- Verificarea modului în care practicile și procedurile documentate sunt aplicate în activitatea curentă
- Revizuirea proceselor efectuate de Autoritatea de Înregistrare (RA).

8.5. Acțiuni întreprinse ca urmare a neconformităților

Rapoartele de audit intern și extern sunt transmise Consiliului de Administrație pentru analiză. Dacă Organismul de Evaluare a Conformității (CAB) identifică abateri sau neconformități, Autoritatea de Supraveghere solicită Simplifi să le corecteze într-un termen specificat. Simplifi se angajează să asigure conformitatea deplină și corectarea în timp util a tuturor neconformităților identificate.

8.6. Comunicarea rezultatelor

Rezultatele auditurilor interne și externe nu sunt publicate.
Totuși, documentul de certificare emis de Organismul de Evaluare a Conformității poate fi publicat pe site-ul web al Simplifi.

9. Alte aspecte comerciale și juridice

9.1. Tarife

Lista serviciilor furnizate de Simplifi și tarifele corespunzătoare sunt publicate pe site-ul oficial *https://www.simplifi.ro*. Plata se poate efectua prin transfer bancar, card bancar sau alte mijloace legale acceptate, în conformitate cu reglementările din România.

9.1.1. Taxe pentru revocare sau acces la informații privind starea certificatelor

Accesul la serviciile de revocare a certificatelor (CRL) și la verificarea starea certificatelor prin OCSP este oferit gratuit pentru toți abonații și entitățile partenere (relying parties). Simplifi își rezervă dreptul de a stabili taxe pentru acces avansat sau de volum ridicat la sistemele de verificare a stării certificatelor, dacă este necesar.

9.1.2. Taxe pentru alte servicii

Simplifi poate percepe taxe pentru activități suplimentare legate de serviciile de încredere, inclusiv, dar fără a se limita la:

- Generarea perechilor de chei pentru abonați sau pentru uz intern;
- Evaluarea sau testarea aplicațiilor terțe pentru compatibilitate;
- Licențierea de instrumente, componente sau API-uri;
- Integrare personalizată, instalare sau servicii profesionale;
- Copii ale politicilor, manualelor sau ghidurilor interne (atunci când nu sunt disponibile public);
- Sesiuni de instruire pentru parteneri sau clienți corporate.

9.1.3. Politica de rambursare

Politica de rambursare a Simplifi este publicată pe site-ul oficial al companiei.
În cazul în care se aprobă o rambursare, abonatul trebuie să solicite revocarea oricărui certificat asociat înainte ca rambursarea să poată fi procesată.

9.2. Responsabilitate financiară

Simplifi menține o acoperire de asigurare și mecanisme interne de protecție pentru a acoperi eventualele răspunderi care pot apărea din operarea serviciilor sale de încredere calificate. În conformitate cu articolul 24(2)(e) din Regulamentul eIDAS, Simplifi este asigurată pentru daunele cauzate de neîndeplinirea obligațiilor legate de serviciile de încredere, până la limita impusă de legislația națională și europeană aplicabilă.

9.3. Confidențialitatea informațiilor de afaceri

Simplifi tratează ca fiind confidențiale toate informațiile comerciale, tehnice și operaționale care nu sunt destinate publicării. Informațiile confidențiale includ, dar nu se limitează la:

- Datele abonaților care nu sunt incluse în certificate;
- Contracte, corespondență și comunicări;
- Jurnalele operaționale și de audit;
- Politici interne de securitate și planuri de recuperare;
- Design de sistem, configurații și proceduri administrative.

Divulgarea acestor informații este permisă numai:

- Cu consimțământul scris explicit al părții afectate;
- Atunci când este impusă prin lege sau printr-o hotărâre judecătorească obligatorie;
- Atunci când divulgarea este necesară pentru executarea serviciilor de către subcontractanți autorizați, aflați sub obligații de confidențialitate.

9.4. Protecția datelor cu caracter personal

Simplifi prelucrează datele cu caracter personal în deplină conformitate cu:

- Regulamentul (UE) 2016/679 (GDPR)**;**
- Regulamentul (UE) 910/2014 (eIDAS)**;**
- **Legislația română aplicabilă și ghidurile emise de ANSPDCP.**

Simplifi acționează în calitate de operator de date și prelucrează datele personale exclusiv în scopul furnizării serviciilor de încredere. Acest lucru include: verificarea identității, emiterea certificatelor, gestionarea ciclului de viață al cheilor criptografice și păstrarea înregistrărilor legale aferente.

Sunt implementate **măsuri tehnice și organizatorice** adecvate pentru a asigura:

- Minimizarea datelor și limitarea scopului prelucrării;
- Confidențialitatea și integritatea datelor în timpul transmiterii și stocării;
- Eliminarea securizată sau arhivarea datelor atunci când acestea nu mai sunt necesare.

Subiecții datelor sunt informați cu privire la modul de utilizare a datelor lor personale înainte de emiterea certificatului și trebuie să își exprime consimțământul informat, acolo unde este necesar. Refuzul de a consimți la prelucrarea datelor obligatorii poate duce la imposibilitatea furnizării serviciului.

Divulgarea datelor cu caracter personal poate avea loc doar în următoarele cazuri:

- Către autorități legal autorizate, în baza unei cereri valide;
- Către auditori sau subcontractanți aflați sub obligații contractuale de confidențialitate;

- Cu consimțământul explicit al subiectului, pentru scopuri specifice (ex. transmiterea adresei poștale, publicarea certificatului).

9.5. Drepturi de proprietate intelectuală

Toate mărcile comerciale, software-ul, documentația și materialele criptografice dezvoltate sau deținute de Simplifi rămân proprietatea intelectuală a acesteia. Utilizarea, reproducerea sau redistribuirea acestor materiale este interzisă fără autorizarea prealabilă în scris a Simplifi. Certificatele și perechile de chei emise persoanelor fizice sunt considerate proprietatea abonatului sau a subiectului, cu excepția cazurilor în care se specifică altfel în certificat sau în contractul aferent.

9.6. Responsabilități și garanții

9.6.1. Autoritățile de certificare

Autoritățile de certificare Simplifi (CAs) garantează că toate certificatele respectă standardul X.509 v3 și politica de certificare (CP) aplicabilă. Procedurile CA sunt efectuate în conformitate cu prezenta Declarație de Practici și cu politicile de certificare corespunzătoare.

9.6.2. Autoritățile de înregistrare

Autoritățile de înregistrare (RAs) care operează sub domeniul Simplifi trebuie să respecte toate procedurile interne, politicile aplicabile (CPs) și această Declarație de Practici. Responsabilitățile lor includ verificarea exactă a identității, validarea cererilor de certificare, precum și gestionarea sigură a datelor de înregistrare.

9.6.3. Abonați / Subiecți

Abonații și subiecții trebuie să:

- revizuiască și să accepte Termenii și Condițiile aplicabile;
- protejeze mijloacele de autentificare utilizate pentru activarea cheii private;
- solicite revocarea imediată a certificatului în caz de compromitere sau utilizare neautorizată a cheii;
- asigure acuratețea informațiilor furnizate pentru certificare.

9.6.4. Entități Partenere (Relying Parties)

Entitățile Partenere care se bazează pe serviciile de încredere Simplifi sunt responsabile pentru:

- Verificarea autenticității și valabilității certificatelor înainte de a lua decizii de încredere;

- Verificarea lanțului de certificare, a stării de revocare (prin CRL/OCSP) și a identificatorilor de politică (OID);
- Asigurarea că certificatul este adecvat scopului pentru care este utilizat;
- Utilizarea de software și dispozitive sigure și de încredere pentru validarea certificatelor.

9.7. Limitări ale răspunderii

Simplifi nu va fi răspunzătoare pentru daunele rezultate din:

- Forță majoră sau circumstanțe neprevăzute;
- Neglijența abonatului în protejarea cheilor private sau a mijloacelor de autentificare;
- Utilizarea certificatelor în alte scopuri decât cele prevăzute;
- Utilizarea certificatelor revocate sau expirate;
- Furnizarea de date incorecte de către abonat, dacă acestea au fost declarate ca fiind corecte.

9.8. Despăgubiri

Simplifi nu își asumă nicio responsabilitate pentru utilizarea necorespunzătoare a serviciilor sale de către terți și nici pentru entitățile partenere care nu respectă bunele practici de validare a certificatelor.

9.9. Durata și încetarea valabilității

Prezenta Declarație de Parctici rămâne în vigoare până la momentul în care este înlocuită sau retrasă de către Simplifi. Versiunile actualizate sunt publicate în Depozitarul oficial Simplifi și devin efective la data publicării, cu excepția cazului în care se specifică altfel.

9.10. Notificări și comunicări individuale

Notificările și comunicările legale pot fi transmise prin următoarele mijloace:

- Scrisoare recomandată;
- Curier rapid;
- Poștă electronică (e-mail) – semnată digital, dacă este necesar;
- Mesagerie prin platforme securizate, acolo unde este aplicabil.

9.11. Soluționarea litigiilor

Litigiile vor fi soluționate cu prioritate pe cale amiabilă între părți. Dacă nu se ajunge la un acord în termen de 30 de zile, litigiile vor fi soluționate de **instanțele competente din România**, având **jurisdicție în București**, cu excepția cazului în care părțile convin altfel, în scris.

9.12. Legea aplicabilă

Serviciile de încredere oferite de Simplifi sunt guvernate de:

- **Regulamentul (UE) nr. 910/2014 (eIDAS);**
- **Regulamentul (UE) 2016/679 (GDPR);**
- Legislația relevantă din România și deciziile autorității naționale de supraveghere.

9.13. Conformitate cu legislația aplicabilă

Simplifi confirmă conformitatea deplină cu cadrul juridic european și național aplicabil serviciilor de încredere. Compania este acreditată ca Prestator Calificat de Servicii de Încredere (QTSP) și este supusă auditărilor și evaluărilor periodice pentru menținerea acestui statut.

10. Anexă

10.1. Definiții și Acronime

auditor: persoană care evaluează conformitatea cu cerințele specificate în documentele aplicabile.

autentificare: furnizarea garanției că o caracteristică declarată a unei entități este corectă [SURSĂ: ISO 27002:2022].

Politică de Certificare (CP): set denumit de reguli care indică aplicabilitatea unui certificat pentru o anumită comunitate și/sau clasă de aplicații cu cerințe comune de securitate.

Listă de Revocare a Certificatelor (CRL): listă semnată care indică un set de certificate revocate de emitentul certificatului.

certificat: cheia publică a unui utilizator, împreună cu alte informații, făcută imposibil de falsificat prin criptarea cu cheia privată a autorității de certificare care a emis-o.

Autoritate de Certificare (CA): autoritate în care unul sau mai mulți utilizatori au încredere pentru a crea și atribui certificate.

Timp Universal Coordonat (UTC): scară de timp bazată pe secundă, conform Recomandării ITU R TF.460-6.

zonă de securitate ridicată: locație fizică specifică (vezi ETSI EN 319 401, clauza 7.8) unde este păstrată cheia Root CA.

incident: orice eveniment care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite sau accesibile prin rețele și sisteme informatice.

breșă de securitate a informațiilor: compromiterea securității informațiilor care duce la distrugerea, pierderea, alterarea, divulgarea sau accesul neautorizat la informații protejate transmise, stocate sau prelucrate [SURSĂ: ISO 27002:2022].

Declarație de Practici (Practice Statement): versiunea curentă a documentului care descrie practicile, procedurile și liniile directoare privind furnizarea serviciilor de încredere. Servește ca referință pentru clienți și părțile interesate pentru a înțelege modul de operare al prestatorului de servicii de încredere și standardele la care acesta aderă (prezentul document).

revocare: încetarea permanentă a valabilității unui certificat înainte de data de expirare indicată în acesta.

risc: potențialul de pierdere sau perturbare cauzată de un incident, exprimat ca o combinație între magnitudinea pierderii/perturbării și probabilitatea producerii incidentului.

Root CA: autoritatea de certificare aflată la cel mai înalt nivel în cadrul domeniului TSP și care semnează CA-urile subordonate.

dispozitiv criptografic securizat: dispozitiv care stochează cheia privată a utilizatorului, o protejează împotriva compromiterii și efectuează funcții de semnare sau decriptare în numele utilizatorului.

zonă securizată: zonă (fizică sau logică) protejată prin controale fizice și logice care asigură confidențialitatea, integritatea și disponibilitatea sistemelor utilizate de TSP.

certificat pe termen scurt: certificat a cărui perioadă de valabilitate (de la *notBefore* la *notAfter*) este mai scurtă decât timpul maxim necesar pentru procesarea unei cereri de revocare, conform Declarației de Practici.

subiect: entitatea identificată într-un certificat ca deținător al cheii private asociate cu cheia publică din certificat.

CA subordonată: autoritate de certificare al cărei certificat este semnat de Root CA sau de o altă CA subordonată.

abonat: persoană fizică sau juridică legată printr-un acord cu un prestator de servicii de încredere privind obligațiile de abonat.

ancoră de încredere (trust anchor): entitate în care entitatea parteneră are încredere și pe baza căreia validează certificatele din lanțurile de certificare.

Politică de Servicii de Încredere (Trust Service Policy): set de reguli care indică aplicabilitatea unui serviciu de încredere pentru o anumită comunitate și/sau clasă de aplicații cu cerințe comune de securitate.

Prestator de Servicii de Încredere (TSP): entitate care furnizează unul sau mai multe servicii de încredere.

vulnerabilitate: slăbiciune a unui activ sau a unui control care poate fi exploatată de una sau mai multe amenințări [SURSĂ: ISO 27002:2022].

Certificat calificat UE: certificat calificat, conform definiției din Regulamentul (UE) nr. 910/2014.

Dispozitiv calificat de creare a semnăturii/sigilului electronice (QSCD): conform specificațiilor Regulamentului (UE) nr. 910/2014.

10.2. Abrevieri

Pentru scopurile prezentului document, se aplică următoarele abrevieri:

Abreviere	Descriere
CA	Autoritatea de Certificare (Certification Authority)
CRL	Listă de Revocare a Certificatelor (Certificate Revocation List)
FIPS	Standard Federal de Procesare a Informațiilor (Federal Information Processing Standard)
NCP	Politică de Certificare Normalizată (Normalized Certificate Policy)
NCP+	Politică de Certificare Normalizată Extinsă (Extended Normalized Certificate Policy)
OCSP	Protocol Online de Verificare a Stării Certificatului (Online Certificate Status Protocol)
OID	Identificator de Obiect (Object Identifier)
PKI	Infrastructură cu Cheie Publică (Public Key Infrastructure)
RA	Autoritate de Înregistrare (Registration Authority)
RQSCD	Dispozitiv Calificat de Creare a Semnăturii/Sigilului la Distanță (Remote QSCD)
TSP	Prestator de Servicii de Încredere (Trust Service Provider)
TSA	Autoritate de Marcare Temporală (Time Stamp Authority)
UTC	Timp Universal Coordonat (Coordinated Universal Time)