simplifi

Trust Service Policy

For the issuance of qualified certificates for electronic signatures and seals and for the management of remote signature and seal creation device and timestamping services

This Trust Service Policy defines the high-level principles, commitments, and governance framework under which Simplifi, as a Qualified Trust Service Provider (QTSP), delivers secure and compliant qualified trust services. These services include the issuance and lifecycle management of qualified electronic signatures, qualified electronic seals, and qualified electronic timestamps, in accordance with applicable standards and legislation.

The policy establishes the trust framework and outlines Simplifi's commitments to security, transparency, legal compliance, and the protection of personal data. It sets the foundation for all subordinate documents, including the Certification Practice Statement (CPS), Trust Service Policies, and procedural manuals governing trusted roles, cryptographic systems, and identity verification.

Through this policy, Simplifi affirms its responsibility to operate with integrity, apply best practices in PKI management, and maintain the confidence of subscribers, relying parties, regulators, and the public in the trust services it delivers.

Document information

Version	1.0
Version Date	September 1st, 2025
Approved by	Policies and Procedures Management Committee
Owner of the Document	Trust Service Manager
Document Name	Simplifi Trust Service Policy for the issuance of qualified certificates for electronic signatures and seals and for the management of remote signature and seal creation device and timestamping services
Document OID	1.3.6.1.4.1.63578.1.1.1
Document Classification	Public

Document history

Version	Effective Date	Reason	Author
V 1.0	2025-09-01	Initial publishing	Trust Service Manager

Approval history

Version	Approval Date	Approver Name
V 1.0	2025-09-01	Policies and Procedures Management Committee

Distribution history

Version	Distribution Date	Distribution
V 1.0	2025-09-01	Trust Service Manager

Contents

1. Introduction

1.1. Scope

The Simplifi Trust Service Policy—covering the issuance of qualified certificates for electronic signatures and seals, as well as the management of remote signature and seal creation devices and time stamping services—together with the Simplifi Certification Practice Statement, forms the set of policies and practices that govern Simplifi's trust services and ensure regulatory compliance.
Throughout this document:

- the use of the term "Policy" or "Trust Service Policy" refers to the present document,
- the use of the term "Practice Statement" refers to the Simplifi Certification Practice Statement.

This document supplements the Practice Statement by including the following specific elements:

- identification and authentication mechanism in terms of certificate application
- description of the certificate life cycle
- provisioning of time-stamp service
- practices for the management and protection of cryptographic material for certification authorities and end-users.
- certificate, CRL and OCSP profiles.

The format and content of the Policy follow the recommendations of RFC 3647. The current document follows the standards specified in the Practice Statement.

1.2. Document Name and Identification

The full name of this document is the Simplifi Trust Service Policy for the issuance of qualified certificates for electronic signatures and seals and for the management of remote signature and seal creation device and timestamping services. This document is available in an electronic version at *https://simplifi.ro/policies/*

The present document defines the trust service policy for the issuance of:

- qualified certificates for qualified electronic signatures,
- qualified certificates for qualified electronic seals,
- certificates for electronic timestamp services,

The following table illustrates compliance with policies defined in ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI TS 119 431-1, ETSI EN 319 421 standard

Policy	Identifier	OID	Compliance
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	Certificates for qualified signatures on a Qualified Signature Creation Device (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	Certificates for qualified seals on a Qualified Seal Creation Device (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	Certificates for qualified time stamps
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	EU Server Signing Service Component

1.3. PKI Participants

1.3.1. Certification authority

Within this policy, subordinate CAs are distinguished, serving the issuance of qualified certificates for qualified electronic signatures.

All subordinate CAs are operated by Simplifi under the Simplifi Root CA [G1]1.

Simplifi Root CA [G1] issues certificates for all subordinate CAs.

- **Simplifi Qualified CA Class 3 G1**

Qualified certificates for electronic signature are issued in accordance with QCP-n-qscd policy defined in the ETSI EN 319 411-2.

Qualified certificates for electronic seal are issued in accordance with the QCP-l-qscd policy defined in the ETSI EN 319 411-2.

Qualified certificates for electronic signature (natural person representing legal person) are issued in accordance with the QCP-qscd policy defined in the ETSI EN 319 411-2.

The private keys for electronic signature or electronic seal are stored on a remote QSCD maintained by Simplifi.

Certificates for the electronic Time-Stamping Service Unit (TSU) are issued for TSU purposes, in accordance with the general requirements of ETSI EN 319 411-1.

The list of CAs above may be expanded in the next versions of the present document.

1.3.2. Registration Authorities

A Registration Authority (RA) acts on behalf of the Certification Authority (CA) to perform critical identity verification and certificate enrollment functions. RAs are responsible for ensuring that certificate requests are submitted by duly identified and authorized individuals or entities.

Simplifi may operate as its own Registration Authority or delegate RA functions to authorized third parties, including qualified electronic identification service providers and other entities that meet the requirements set forth in applicable EU and Romanian legislation. These third parties act under formal agreements with Simplifi and operate in accordance with Simplifi's policies, this Practice Statement, and applicable trust service regulations.

[1] Identifier in square brackets is instance numbering and present policy applies to all instances developed in the future

1.3.2.1. Registration Points

An authorized registration point is a legal person. Within each registration point, authorized representatives (natural persons) are designated to carry out initial identity validation. These representatives are formally appointed, properly trained, and act in accordance with established procedures.

1.3.2.2. Registration service

Registration represents an online service for collection and validation of identification means for initial identity validation. It ensures compliance with the internal process adopted by Simplifi, using the necessary mechanisms for verifying both the individual and the presented identity document.

The applicable process may include the following elements or a selected combination thereof to ensure the required level of security:

- Live video verification – the user connects with an agent in real time, presents their identity document, and performs specific actions (e.g., head movements, repeating a phrase).
- Automated document and biometric verification – the system scans the identity document (e.g. OCR, security feature check) and compares the photo with the user's face (live check and matching).
- Reading data from the electronic layer of the document (e.g NFC) – for e-ID cards or chip-enabled passports, data is read and compared with external data sources.

1.3.3. Time-Stamping Authority (TSA)

Simplifi provides time-stamping services that are used solely for the purpose of generating time-stamp tokens. Simplifi operates as a Time-Stamping Authority that responds to time-stamp requests from subscribers (e.g. client applications) as part of a broader trust service infrastructure.

The TSA is responsible for operating one or more Time-Stamping Units (TSUs) that create and sign time-stamp tokens on behalf of the TSA. All TSUs use certificates issued by Simplifi Qualified CA Class 3.

1.3.4. Subjects and subscribers

The subject is defined as the entity identified in the certificate as possessing the private key. Possible types of subjects include:

- a natural person
- a legal person

- a natural person identified in association with a legal person

The subscriber engages in a contractual relationship with Simplifi under the terms of the subscriber agreement. The subscriber is typically the certificate holder (subject) but may also act on behalf of another subject when requesting a certificate. Both natural persons and legal entities are eligible to be subscribers of Simplifi.

A Subscriber is also the entity that requests timestamps from the TSA's service.

1.3.5. Relying parties

A relying party is a natural person or legal entity that relies on the trust services of Simplifi..

1.3.6. Server signing application service

Simplifi delivers a service component using a server signing solution to create electronic signatures or seals on behalf of the Subject

1.3.7. Other participants

The Practice Statement covers the specifics of this item.

1.4. Certificate usage

Simplifi issues following types of certificates:

- qualified certificates for electronic signatures
- qualified certificates for electronic seals

These are issued to entities that have accepted the terms and conditions, along with the provisions set out in relevant documents such as the Practice Statement and this Trust Service Policy.

There are the following types of certificates and their applicability:

a) Legal entity
Qualified certificates for electronic seals - certificates are issued to legal entities. A qualified certificate for an electronic seal includes at least the name of the country, the name of the subject (legal entity), its registration number, legal entity common name and serial number of the certificate.

b) Natural person representing legal entity
Qualified certificates for electronic signatures - certificate contains at least: name of the country, name of the subject (natural entity representing legal entity), serial number of the certificate, organization name associated with natural entity.

c) **Personal**

Qualified certificates for electronic signatures - certificate contains at least: name of the country, name of the subject (natural entity), serial number of the certificate.

The following table presents relation between each type of certificate issued by Simplifi and specific policy regulated by this document:

Type	Purpose	Media	Policy identifier	ETSI Policy OID
Legal person	Qualified electronic seal	Remote QSCD	QCP-l-qscd	0.4.0.194112.1.3
Natural person representing legal person	Qualified electronic signature	Remote QSCD	QCP-n-qscd	0.4.0.194112.1.2
Natural person	Qualified electronic signature	Remote QSCD	QCP-n-qscd	0.4.0.194112.1.2

1.4.1. Appropriate certificate use

The use of legal person certificates is restricted to the creation of qualified electronic seals by a legal person and their validation by relying parties.

The use of electronic signature certificates for a natural person representing a legal person is intended to enable legally binding actions where an individual acts on behalf of an organization. Such certificates are restricted to the creation of qualified electronic signatures by the natural person where the legal effect of the signature is intended to bind the represented legal person.

Personal certificate for electronic signature use is restricted to the creation of qualified electronic signatures by the natural person and its validation by relying parties.

1.4.2. Prohibited certificate use

Certificates shall be employed strictly in accordance with their stated intent and authorized scope. Use of such certificates in violation of applicable law is expressly prohibited.

Issuance does not constitute a representation or warranty of the subject's trustworthiness, business practices, or the condition of the associated system, including its freedom from malware or vulnerabilities.

1.5. Policy Administration

1.5.1. Organization responsible for administrating the document

This Trust Service Policy is administered by Simplifi:

Strada Gheorghe Țițeica 142, București 014192, Romania

1.5.2. Contact

easy@Simplifi.ro

1.5.3. Entities determining the validity of the principles contained in the document

The Simplifi team is responsible for assessing the completeness and accuracy of this document and others related to PKI services provided by Simplifi, as well as ensuring their consistency. All inquiries and comments regarding the content of these documents should be directed to the address specified in specified in chapter 1.5.2.

1.5.4. Approval procedures

The present document remains in effect from its specified start date until a subsequent valid version is published.

Affected parties may submit comments on proposed modifications within 14 working days from their announcement, as outlined in Simplifi Practice Statement chapter 9.10. If no significant objections to the substantive content are raised within this period, the new version of the Practice Statement becomes effective on the date indicated in the document.

Approval of the new version of the Practice Statement is the responsibility of Simplifi management. All changes are recorded in the revision history. The approved document is then published and communicated to:

- employees,
- appointed trusted roles,
- relying parties,
- subjects and subscribers,

other participants defined in Simplifi Certification Practice Statement chapter 1.4.5.

1.6. Definitions and Acronyms

Definitions and abbreviations used in this document can be found in the Simplifi Certificaiton Practice Statement document.

2. Publication and Repository Responsibilities

2.1. Publication Repository

Simplifi has a repository of:

- publicly available documents along with previous versions at: *https://simplifi.ro/policies/*.
- All published certificates, both active and revoked (including the Certificate Revocation Lists), at: *http://Simplifi.ro/pki.*
- OCSP responder, at *http://Simplifi.ro/ocsp*

The repository is intended for the following entities: subjects, subscribers, relying parties.

2.2. Information published by Simplifi

The repository contains the following documents:

- Certification Practice Statement – current and previous version
- Trust Service Policies - current and previous version
- General Terms & Conditions
- Certificate profiles, CRL and OCSP profiles
- All published certificates, both active and revoked
- Certificates Revocation Lists (CRLs)
- OCSP responder
- Additional information, under Simplifi's internal decision, e.g. notifications about significant incidents.

It stores both the current and historical versions of these electronic documents.

2.3. Frequency of publication

Publications are issued with the following frequency:

- Practice Statement and specific trust service policies - see Simplifi Certification Practice Statement chapter 9.10,

- Certificates of all authorities operating trust services within Simplifi - upon every issuance of new certificates,
- Certificate Revocation List (CRL) - according to specific Trust Service Policy and certificate profile

2.4. Access to publications

Simplifi applies both logical and physical security controls to protect the repository against unauthorized data creation, removal, or modification.

3. Identification and Authentication

Simplifi ensures that the supported identity proofing methods comply with the requirements of Article 24 of Regulation 910/2024, specifically on the basis of one of the following methods, or, when needed, a combination thereof:

- Art. 24.1a(a): Identity verification is based on a notified electronic identification means at a high assurance level.
- Art. 24.1a(b): Identity verification is based on a qualified certificate issued in compliance with points 24.1a(a), 24.1a(c) or 24.1a(d)
- Art. 24.1a(c): Identity verification uses a method confirmed by a conformity assessment body, as described in section 3.2.2.
- Art. 24.1a(d): Identity verification is carried out by a Registration Officer based on a physical visit by the certificate applicant to a Registration Point.

Simplifi develops and maintains documented procedures for the verification and authentication of clients applying for certificates and ensures their implementation in accordance with applicable legal and regulatory requirements.

3.1. Naming

3.1.1. Type of names

In accordance with the X.509 standard, certificates contain information about the issuer and subject, identified by their respective distinguished names.

3.1.2. Meaningful names required

The subject's distinguished name is unique across all trust and electronic identification services provided by Simplifi. Each value within the subject information section of the certificate is relevant and intentionally included.

Section 3.1.4 specifies the mandatory certificate data required to ensure unambiguous identification of the subject.

3.1.3. User anonymity

The use of pseudonyms of the subject is not allowed in certificates.

3.1.4. Rules for different names interpretation

The interpretation of the field names included in certificates complies with ETSI EN 319 412 (Parts 1, 2, 3).

The attributes of the distinguished name (DN components) in certificates are interpreted as follows:

DN component	Interpretation
givenName	Given name(s) of the natural person According to the proof used for identification Only used for natural person or natural person representing legal person
Sn **(surname)**	Surname of the natural person - According to the proof used for identification Only used for natural person or natural person representing legal person
Cn **(commonName)**	Common name: The following variants are used: Natural persons without a pseudonym: “givenName surname”. Legal person: Official name of the legal entity (company, public authority, association, etc.), if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded.
serialNumber **(serial number)**	Serial number: The natural person unique identifier. Identifier for a natural person is for example: - PNORO-1234567890123 or IDCRO-DZ123456 or TINRO-1234567890123 for identification based on Carte de Identitate Electronică Code, recognizable on the European Union’s level according to point 5.1.3 ETSI TS 119 412-1

DN component	Interpretation
O **(organizationName)**	Official name of the subscriber or name of the legal person (including legal form) to which the subject belongs or to which he or she is otherwise affiliated (company, public authority, association, etc.) according to the proof of existence; if necessary, reduced to a meaningful name if the maximum number of 64 characters is exceeded. Only used for legal person or natural person representing legal person
OrgID **(organizationIdentifier)**	Unambiguous legal person identifier. Identifier for legal person is for example: - NTRRO-12345678 for identification based on an identifier from a National Trade Register Office (ONRC), recognizable on the European Union's level according to point 5.1.4 ETSI TS 119 412-1 Only used for legal person or natural person representing legal person
C **(countryName)**	The notation of the country to be stated corresponds to ISO 3166 and is set up as follows: International abbreviation for country name (RO for Romania)

1) *Qualified certificates for natural person include, as a minimum, the subject DN components: "cn", "c", "serialNumber", "givenName" and "surname".*
2) *Qualified certificates for natural person representing legal person include, as a minimum, the subject DN components: "cn", "c", "serialNumber", "givenName", ''surname", "o" and "orgID".*
3) *Qualified seals for legal person include, as a minimum, the subject DN components: "cn", "c", "o" and "orgID".*

Further components can be added. Additional DN components must comply with RFC 5280, RFC 6818 and ETSI EN 319 412.

3.1.5. Uniqueness of the names

Simplifi ensures the uniqueness of issued certificates. Accordingly:

- Each **commonName** and **serialNumber** pair is exclusively assigned to a single natural person.

- Each **commonName** and **organizationIdentifier** pair is uniquely associated with a single legal person.

3.1.6. Recognition, authentication and role of trademarks

Simplifi excludes trademarks from certificate subject fields. The use of any name without demonstrable ownership by the subscriber is strictly forbidden. Simplifi disclaims any responsibility for adjudicating disputes related to the legal ownership of names, trademarks, or trade identifiers.

3.2. Initial identity validation

Registration for Simplifi services requires an initial identity verification process to issue electronic signatures, and electronic identification credentials.

This registration process involves collecting identity data and enabling the individual to present themselves for verification prior to certificate issuance.

The initial identity verification applies to:

- Natural persons,
- Natural persons acting on behalf of legal person
- Legal person themselves.

Before starting the identity verification procedure, the subject must review and acknowledge the Terms of Service and this Policy.

3.2.1. Method to prove possession of key

Simplifi confirms that the Subject possesses or controls the private key corresponding to the public key to be certified by verifying the digital signature on the certificate request, which must have been generated using that private key.

3.2.2. Authentication of a legal person

Identification and authentication of the legal person is conducted only for issuance of qualified certificate for electronic seal.

The authorized representative of Registration Points is obligated to verify the identity of the legal person and the associated representation (natural person).

The procedure consists of two parts:

1) Verification of legal person includes:

- The full name of the legal person
- country of the registration of the legal person
- A unique identifier and its type (the National Trade Register or VAT number)

The primary source of data for legal person verification is the Romanian Registry of Legal Entities

2) Verification of the authorized representative (natural person) includes:

- Legal representation
- Full name and legal status of the associated legal person
- Verification of the individual's role and authorization to act on behalf of the legal person
- Full name of the natural person (givenName and surname)
- Date and place of birth
- Identity document verification

The primary evidence for verifying representation may include:

- A valid power of attorney
- Validation of the signature created on documents by an authorized person
- Confirmation of the representation through government databases

Natural person's identity validation as the authorized representative is carried out in accordance with section 3.2.3.

The organization's identity and legal existence shall be **revalidated every 6 years**, starting from the date of issuance of the first qualified certificate under this Policy.

3.2.3. Authentication of a natural person

Whenever identification of a natural person is required for the issuance of any certificate or electronic identification means, it is carried out in accordance with the procedure described below.

Registration Authority provides identity validation of natural entity through the following use cases:

- **In-person**: by the physical presence of the applicant at a Registration Point with identity evidence collected and validated by an authorized representative
- **Remote**: Identity proofing is primarily performed by external Trusted Registration Authorities, authorized by the Romanian ADR (Autoritatea pentru Digitalizarea României).

In-person use case requires from the Subject to provide one or more valid original identity document (ID card or passport).

The authorized representative of RP can request to verify its authenticity, integrity and to confirm that it corresponds to the applicant (subject).

The remote use case requires the Subject to either possess a previously issued electronic identification means (notified) or present ID document via video identification process. Currently acceptable methods are:

- ROeID (notified Romanian eID means)
- Remote Video identification process provided by external provider that allow the verification of security elements for the presented identity documents and validation the the matching between the natural person and documents
- Combination of both (ROeID and Video identification process)

The validation of eID means is made by the registratrion services which is operated by RA.

Each of these methods ensures that only the data needed to issue a certificate is collected and validated.

All evidence and attestations are collected by the Registration Authority in line with the following statements:

- The subject's identity is verified at the time of registration.
- Evidence is collected for the following data:
    - full name (including surname and given names).
    - date and place of birth,
    - ID document serial number (if applicable)
    - Personal Identification Number
    - Registration Address

Registration Authority records and preserves identity data of all registered subjects.

3.2.4. Authentication of a natural person representing legal person

Natural person identity validation of the authorized representative is carried out in accordance with section 3.2.3.

3.2.5. Unconfirmed information

The certificate does not contain any unconfirmed information.

3.2.6. Criteria of interoperability

Not applicable.

3.3. Identification and authentication for re-key requests

Certification and rekey (key update) may be initiated by the subject under the following condition:

- A rekey request for an active, non-expired certificate.

In such cases, the subject must submit an application that includes a request for the generation of a new key pair and the issuance of a new certificate. The request must be authenticated by verifying a digitally signed document, signed by the subject using the private key associated with the currently valid (non-expired) certificate.

To facilitate timely renewal, an email notification will be sent to the subject 45 days prior to the certificate's expiration. This message will inform them of the approaching expiry and outline the necessary steps to complete the process.

Subjects may then use an online interface to proceed. This process requires the subject to confirm their identity by digitally signing with the certificate that is nearing expiration.

3.4. Identification and authentication for revocation requests

Revocation requests may be submitted by the Subject, the Subscriber, authorized representatives, the Registration Authority, or other trusted roles, using the channels defined in Section 4.9.3.

Depending on the submission method, the requester’s identity is authenticated as follows:

- **Simplifi Portal**: The Subject authenticates using their account credentials before submitting a revocation request.
- **Signed Request**: A revocation request signed with a qualified electronic signature or seal is considered authenticated if the signer’s identity matches the certificate Subject or authorized Subscriber.
- **In-person**: Identification is performed based on official identity documents presented to the Registration Authority.
- **Unauthenticated channels** (e.g., plain email or web form): The Registration Authority attempts to verify the requester’s identity using the provided contact information. If verification fails, the certificate may be suspended until the situation is clarified.

The Registration Authority is responsible for confirming the legitimacy of the revocation request prior to execution. Detailed procedures, including accepted channels and identity verification mechanisms, are described in Section 4.9.3.

4. Certificate life-cycle operational requirements

4.1. Certificate application

4.1.1. Who can submit a certificate application

A certificate may be requested by a natural person, a legal person, or a natural or legal person managing the equipment or system for which the certificate is intended.

The Certification Authority (CA) issues certificates for the following categories:

Natural persons:

- Personal certificates

Natural persons representing legal person:

- Certificates linked to the represented organization

Legal person: Certificates issued directly to the **organization**

Certificate applications may be submitted in person at a Registration Point. The application can be initiated by either the Subject or the Subscriber.

4.1.2. Registration process and responsibilities

The enrollment process is coordinated by a designated entity referred to as the **Registration Authority (RA)**, which may be operated directly by **Simplifi** or by authorized third parties acting on behalf of Simplifi.

Simplifi may delegate the identification of Subjects or Subscribers to external entities, including **remote identification service providers** (such as **ROeID**, **Qoobiss Ontrace**, or other eIDAS-compliant providers that fully respect all national legislation for remote identification), provided they apply **identification procedures offering an equivalent level of assurance** to those defined for the RA in this Policy, the Certification Practice Statement (CPS) and applicable ETSI standards.

Such external identification services may operate under:

- Direct contractual agreements with Simplifi, or
- Mutual recognition under eIDAS as notified electronic identification means

Regardless of delegation, Simplifi retains full responsibility—within the limits of this Policy-for the actions or omissions of any agent, employee, or third party involved in the registration process.

Responsibilities of the Registration Authority

The RA is responsible for verifying the following:

- The claimed **identity** of the Subject and/or Subscriber
- The claimed **attributes** (e.g., organization, role, mandate) of the Subject and/or Subscriber
- The **application** submitted for certificate issuance

This verification must be performed in compliance with:

- The procedures defined in this policy
- Simplifi's internal RA procedures
- National and European legislation applicable to electronic identification and trust services

Use of Remote Identification Services

Simplifi may perform identity verification using **remote identification services**, particularly for fully digital workflows. These services may include:

- **Video identification sessions**
- **eID document scanning with biometric matching**
- **Remote qualified electronic signature validation (QES-onboarding)**
- **Automated identity checks integrated with national identity schemes (e.g., ROeID) or** other eIDAS-compliant providers that fully respect all national legislation for remote identification

Such identification sessions may be:

- **Initiated by Simplifi (e.g., during online onboarding), or**
- **Delegated entirely to a identity provider, where Simplifi receives verified identity data upon successful completion.**

In all cases, Simplifi ensures that the applied remote identification method complies with the requirements of:

- ETSI EN 319 411-1 and 2
- ETSI TS 119 461 when required
- The eIDAS Regulation, including Article 24 (1a)
- Applicable supervisory guidance from the Romanian Digital Authority (ADR)

Information Provided to the Subject/Subscriber

Before or during the enrollment process, the Subject or Subscriber is provided with:

- The applicable Terms and Conditions
- The URL where Terms, Conditions, and applicable documents may be accessed

- A copy or link to this Policy, to the CPS and relevant notices

By accepting these terms, the Subject or Subscriber acknowledges and agrees that:

- They are responsible for the accuracy and completeness of the information submitted for registration
- Simplifi retains all enrollment and registration data for a minimum of 10 years from certificate expiration or revocation
- In case Simplifi ceases operations as a CA/RA, these records may be lawfully transferred to a successor or designated third party
- They understand their rights, obligations, and liabilities as defined by Simplifi, applicable agreements, and the law
- They have a duty to promptly inform Simplifi of any event or change affecting certificate validity

Enrollment Procedure

The enrollment process begins at the RA level, either:

- Directly through Simplifi's in-house RA personnel
- Via delegated RAs
- Or through integration with remote identity providers, as described above

The RA is responsible for:

- Collecting and validating documentation and identity evidence
- Performing initial and final verification steps
- Ensuring that verified enrollment data is complete and accurate before the certificate request is submitted to the CA

The RA bears full responsibility for the correctness of:

- The identity data to be embedded in the certificate
- The attributes and roles asserted (e.g., legal representative)
- The assurance level of the identification process

4.2. Certificate application processing

4.2.1. Performing Identification and Authentication Functions

The identification and authentication of the Subject or Subscriber must be completed prior to certificate issuance. Once the Subject's identity is successfully verified, the issuance process can begin. A detailed description of the initial identity validation procedure is provided in Chapter 3.2 of this Policy.

4.2.2. Approval or rejection of certificate applications

Upon completion of the registration process, the CA or RA reserves the right to deny certificate issuance in cases of missing or insufficient information, failed consistency or security validations, or unresolved doubts regarding the identity of the Subject or Subscriber.

4.2.3. Time to process certificate applications

Simplifi makes every effort to ensure that upon receiving the application for a certificate, the CA reviews the application and issues a certificate as soon as possible.

4.3. Certificate Issuance

4.3.1. CA actions during certificate issuance

Following the processing of the certificate request and final verification of the submitted data, the Certification Authority proceeds with the issuance of the certificate. Each certificate is assigned a unique serial number. The validity period of the certificate shall not exceed the validity period of the issuing Certification Authority.

4.3.2. Notification to Subjects and Subscribers by the CA of issuance of a certificate

The Subject and Subscriber are notified of the certificate issuance in accordance with the methods set out in the terms and conditions.

4.4. Certificate Acceptance

4.4.1. Conduct constituting certificate acceptance

It is the Subject's responsibility to ensure that all information included in the issued certificate is complete, correct, and up to date. Upon discovering any inaccuracy or inconsistency, the Subject shall, without undue delay, inform the designated contact point as referenced in clause 1.5.2 of this Policy.

The consent and acceptance is logged.

4.4.2. Publication of the certificate by the CA

Please refer to Chapter 2.

4.4.3. Notification of certificate issuance by the CA to other entities

Not applicable.

4.5. Key Pair and certificate Usage

4.5.1. Subscriber and/or subject private key and certificate usage

Subjects are obligated to use their private keys and certificates strictly in accordance with:

- the purposes defined in this document, the Certification Practice Statement, and the applicable terms and conditions;
- the KeyUsage and extendedKeyUsage extensions as specified in each certificate, in line with the applicable certificate profiles.

Where local signature creation devices or authentication credentials are used to activate private keys, the Subject is responsible for ensuring their secure storage and protecting them from unauthorized access.

Subjects may use their signing key pairs to generate electronic signatures in various supported formats.

Simplifi securely stores and manages certificates and their corresponding private keys in an RQSCD that meets all relevant standards.

The server-based signing service (remote signature system) implements technical safeguards to prevent the use of expired certificates.

4.5.2. Relying party public key and certificate usage

The relying party is required to use the certificate and public key lawfully and in accordance with:

- this Policy and the Practice Statement.
- the Terms and Conditions.

A Relying Party may rely on a certificate if all of the following conditions are met:

The certificate is used in accordance with the permitted usages defined in the certificate extensions;

- The certificate chain is successfully and fully validated up to the trusted root certificate;
- The certificate is verified as not revoked by consulting the relevant Certificate Revocation List (CRL), or its status is positively confirmed via the Online Certificate Status Protocol (OCSP) service.

4.6. Certificate renewal

Renewal of Certificates using the same key pair is not allowed. To maintain the validity of the certificate, the use of the Certificate Re-key mechanism is supported - see clause 4.7.

4.7. Certificate Re-key

A key update is initiated when the Subject or the Subscriber (acting on behalf of a previously registered Subject) requests the generation of a new key pair and the issuance of a new certificate binding the Subject's identity to the new public key. The key update pertains specifically to the certificate indicated in the request. The newly issued certificate retains the content of the original, except for the following distinctions:

- A newly generated key pair,
- A new serial number,
- A new certificate validity period

4.7.1. Circumstance for certificate re-key

Certification and rekey (key update) may occur when a subject requests for rekey of currently valid certificate.

If, during the validity period of a certificate, the recommended cryptographic algorithms or related parameters supported by the qualified electronic signature and seal creation device become obsolete or no longer meet applicable security standards, the Certification Authority (CA) may initiate the issuance of a new qualified certificate. The new certificate will be linked to a qualified signature and seal creation device that complies with the current security requirements. In such a case, the Subject will be required to complete the re-key process in accordance with the instructions provided by the CA.

4.7.2. Who may request certification of a new public key

Keys are updated only after the Subject or Subscriber's request and therefore must be preceded by the submission of an appropriate application.

4.7.3. Processing certificate re-keying requests

RA uses the same processes as for a newly requested certificate.

4.7.4. Notification of new certificate issuance to subscriber

RA uses the same processes as for a newly requested certificate.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

RA uses the same processes as for a newly requested certificate.

4.7.6. Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7. Notification of certificate issuance by the CA to other entities

Not applicable.

4.8. Certificate modification

Certificate modification is possible only as part of the re-key process described in chapter4.7.

4.9. Certificate revocation

Simplifi ensures 24/7 availability of certificate revocation services. Revocation of a certificate is legally equivalent to its invalidation and results in the automatic termination of the contractual relationship between the Subscriber and Simplifi.

Any electronic signatures created after the publication of the revocation are deemed invalid. Upon revocation, the Subject is strictly prohibited from using the certificate for electronic signatures, electronic seals, or timestamping.

Simplifi publishes real-time certificate status information via both Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP). Both services operate on a synchronized database to ensure consistent certificate status verification

4.9.1. Circumstances for revocation

A certificate may be revoked under any of the following circumstances:

- Invalid Certificate Information
    - The data contained in the certificate is no longer accurate or valid
    - Simplifi receives a notification indicating that certificate data is incorrect
- Key or Device Compromise
    - The private key associated with the certificate or the secure device (QSCD/SSCD) storing it has been, or is suspected to have been, compromised.
    - Simplifi's own private key or systems are compromised, undermining the trustworthiness of issued certificates
- End of Service or Subscriber-Initiated Revocation
    - The Subscriber terminates the service agreement with Simplifi.
    - If the Subscriber does not initiate revocation, it may be carried out by Simplifi, the Certification Authority, or an authorized representative of the Subscriber's organization.
    - Revocation is requested by the Subscriber or the Subject.
- Supervisory or Regulatory Action
    - Revocation is requested by the competent Supervisory Body.
    - Legal, regulatory, or governmental changes prevent the Subject from complying with this Policy.
- Contractual or Policy Non-Compliance

    - The Subscriber or their organization fails to fulfill contractual obligations, including payment of service fees.
    - Simplifi determines that the certificate holder has failed to comply with this Certificate Policy or the applicable Certification Practice Statement.
- Cryptographic Weakness or Risk
    - The cryptographic algorithms or parameters used in the certificate are deemed no longer secure, compromising the binding between the Subject and their public key.
- Termination of Operations
    - Simplifi discontinues its certification services. In such cases, all certificates, including the Certification Authority's own certificate, must be revoked prior to the end of the termination period.
- Extraordinary Circumstances
    - Any event, such as natural disasters, system failures, or other unforeseen incidents, that prevents the Subject from fulfilling obligations under this Policy.

4.9.2. Who can request revocation

The Subject or Subscriber may, at their discretion, request the revocation of the Subject's certificate at any time. The Certification Authority reserves the right to revoke a certificate for any reason listed in Chapter 4.9.1.

The Supervisory Body may at any time submit a formal revocation request or report relevant events that may affect the validity of a Subject's or Certification Authority's certificate.

Furthermore, Relying Parties and other third parties may notify Simplifi of justifiable concerns warranting revocation. In such cases, where the requester is not the certificate holder, the CA is required to:

- assess whether the requester holds sufficient authorization to demand revocation, and
- promptly notify the Subscriber of the revocation or of the initiation of the revocation process.

4.9.3. Procedure for revocation request

Revocation may be initiated in accordance with the provisions of Section 4.9.2, by any party with the right or obligation to request it. Simplifi accepts revocation requests through various channels and ensures that appropriate identification and authorization checks are performed prior to revocation. The process is designed to balance availability with security and to enable timely certificate status updates via CRL and OCSP.

a) **Revocation by the Subject**

The Subject (i.e., the holder of the private key corresponding to the certificate) may request certificate revocation using one of the following methods:

- **Via Simplifi Portal**: The Subject may log in to their account at *https://www.simplifi.ro* and submit a revocation request after authentication.
- **Via Web Form**: The Subject may complete the revocation form available at *https://simplifi.ro/revoke*, including:
    - Full name of the requester
    - Contact phone number and email address
    - Identifier of the certificate to be revoked
    - Reason for revocation (optional)

      Note: This is treated as unauthenticated. The RA will verify the identity and intent of the requester via contact. If unsuccessful, the certificate may be suspended until clarified.
- **Via Email**: A revocation request may be emailed to *easy@simplifi.ro*, and must include:
    - Name of requester
    - Phone number
    - Subject name or serial number
    - (Optional) Reason for revocation

      Digitally signed emails using a qualified electronic signature (QES) matching the Subject are considered authenticated. Others are treated as unauthenticated and subject to verification.
- **In Person at RA:** The Subject may request revocation in person by presenting a valid ID and signed request form to an authorized RA.

b) **Revocation by the Subscriber**

The Subscriber (organization contracting with Simplifi) may revoke any certificate issued under their responsibility via:

- **Authenticated Online Portal**
- **Digitally Signed Email (QES or QSeal)**
- **In Person at RA (with ID and mandate)**

c) Revocation by Other Authorized Parties

Registration Authority (RA): The RA may revoke a certificate upon verified request or in case of compromise or policy violation, using secure internal tools.

Relying Parties / Third Parties: May submit revocation requests to *easy@simplifi.ro* with credible evidence of misuse. The RA will verify and may suspend the certificate while investigating.

Simplifi Trusted Roles: Trusted personnel may perform revocation via CA software for:

- Security incidents
- Compliance violations
- Internal policy enforcement

Minimum Required Information for Revocation Requests
All revocation requests must include:

- Full name of requester
- Contact phone number
- Email address (if available)
- Subject's name or certificate identifier
- Certificate serial number or Subject DN (if known)

Incomplete requests may lead to **temporary suspension** until identity is confirmed.

Verification and Action by the RA
All unauthenticated requests are forwarded to the RA for verification. If the requester's identity or authority cannot be reliably confirmed, the certificate is suspended until the matter is resolved. Once verified, the certificate is revoked and:

- Added to the CRL without delay
- Marked as revoked via OCSP
- A confirmation notice is issued to the requester and Subscriber
- If denied, a reasoned response is provided

4.9.4. Revocation request grace period

The Subscriber or Subject is required to request revocation immediately upon detecting the loss or theft of the device, or the loss of control over authentication credentials (such as PINs or passwords).

4.9.5. Time within which CA must process the revocation request

Certificate revocation application is processed by Simplifi within 24 hours of its acceptance.

After confirmation of the request for certificate revocation, its status will be changed within 60 minutes.

4.9.6. Revocation checking requirement for relying parties

Before relying on the information contained in a certificate, the Relying Party shall verify the validity of each certificate in the certification path, including checking certificate status and revocation using CRLs or OCSP responders specified in each certificate in the chain.

4.9.7. CRL issuance frequency

Every certification authority being a part of Simplifi issues a separate Certificate Revocation List. The CRL is updated according to the following schedule for each level of Certification Authority (CA):

- Every 24 hours for Subordinate CAs
- Every 12 months unless there is a revocation of any intermediate CA for the Root CA

4.9.8. Maximum latency for CRLs

Each CRL is published without undue delay as soon as it is created (usually this is done automatically within a few minutes).

4.9.9. On-line revocation/status checking availability

Simplifi ensures continuous, real-time verification of certificate validity using the Online Certificate Status Protocol (OCSP), implemented in accordance with the technical requirements of RFC 6960. This mechanism enables efficient and up-to-date verification without requiring access to the CRL.

Under standard operating conditions, OCSP response time does not exceed ten (10) seconds. The OCSP responder, acting on behalf of Simplifi, returns one of the following standardized responses for each query:

- good – the certificate is currently valid;
- revoked – the certificate has been officially revoked;
- unknown – the responder has no record or cannot verify the certificate's status.

OCSP status information is publicly accessible, and the service endpoint is embedded in the certificate itself. Upon revocation, certificate status is updated and made available via OCSP within a few minutes.

4.9.10. On-line revocation checking requirements

There is no more additional requirement than those indicated in chapter 4.9.6.

4.9.11. Other forms of revocation advertisements available

Not applicable

4.9.12. Special requirements related to key compromise

Not applicable

4.9.13. Circumstances for suspension

Not applicable

4.9.14. Who can request suspension

Not applicable

4.9.15. Procedure for suspension request

Not applicable

4.9.16. Limits on suspension period

Not applicable

4.10. Certificate Status Services

4.10.1. Operational Characteristics

Simplifi provides a certificate status service in the form of a CRL distribution point and OCSP responder. OCSP certificate status request services are accessible over HTTP. The current CRL is published in the repository and available through the CRL distribution point over HTTP.

The formats and protocols of the services are described in sections 7.2 and 7.3 of this policy.

The URL of the OCSP service and CRL distribution point are included in the certificate

4.10.2. Service Availability

The OCSP service and the CRL are available 24 hours a day, 7 days a week.

4.10.3. Operational Features

Not applicable

4.11. End of subscription

The relationship between the Subject and/or Subscriber with the Certification Authority is terminated when the certificate expires or is revoked.

4.12. Key escrow and recovery

Simplifi does not offer key escrow services to Subjects. CA's private keys are never escrowed.

4.12.1. Key escrow and recovery policy and practices

Not applicable

4.12.2. Session key encapsulation and recovery policy and practices

Not applicable

5. Management, Operational, and Physical Controls

5.1. Physical Security Controls

The Practice Statement covers the specifics of this item.

5.1.1. Power and air conditioning

The Practice Statement covers the specifics of this item.

5.1.2. Water exposure

The Practice Statement covers the specifics of this item.

5.1.3. Fire prevention and protection

The Practice Statement covers the specifics of this item.

5.1.4. Media storage

The Practice Statement covers the specifics of this item.

5.1.5. Waste disposal

The Practice Statement covers the specifics of this item.

5.2. Procedural Controls

5.2.1. Trusted roles

The Practice Statement covers the specifics of this item.

5.2.2. Four-eyes principle

The Practice Statement covers the specifics of this item.

5.2.3. Identification and authentication for each role

The Practice Statement covers the specifics of this item.

5.2.4. Roles Requiring Separation of Duties

The Practice Statement covers the specifics of this item.

5.3. Personnel Security Controls

5.3.1. Qualifications, experience and clearances

The Practice Statement covers the specifics of this item.

5.3.2. Personnel testing procedures

The Practice Statement covers the specifics of this item.

5.3.3. Training requirements

The Practice Statement covers the specifics of this item.

5.3.4. Retraining Frequency and requirements

The Practice Statement covers the specifics of this item.

5.3.5. Job rotation frequency and sequency

The Practice Statement covers the specifics of this item.

5.3.6. Sanctions for unauthorized actions

The Practice Statement covers the specifics of this item.

5.3.7. Contracts with the personnel

The Practice Statement covers the specifics of this item.

5.3.8. Documentation available to Personnel

The Practice Statement covers the specifics of this item.

5.4. Audit Logging Procedures

The Practice Statement covers the specifics of this item.

5.4.1. Types of events recorded

The Practice Statement covers the specifics of this item.

5.4.2. Frequency of processing log

The Practice Statement covers the specifics of this item.

5.4.3. Retention time for Records

The Practice Statement covers the specifics of this item.

5.4.4. Protection of records

The Practice Statement covers the specifics of this item.

5.4.5. Backups of records

The Practice Statement covers the specifics of this item.

5.4.6. Audit log accumulation system

The Practice Statement covers the specifics of this item.

5.4.7. Notification system to event-Causing

The Practice Statement covers the specifics of this item.

5.4.8. Vulnerability assessment

The Practice Statement covers the specifics of this item.

5.5. Records Archival

5.5.1. Types of archives

The Practice Statement covers the specifics of this item.

5.5.2. Retention period of archives

The Practice Statement covers the specifics of this item.

5.5.3. Protection of archive

The Practice Statement covers the specifics of this item.

5.5.4. Backup archives procedures

The Practice Statement covers the specifics of this item.

5.5.5. Requirements for time-stamping the archives

The Practice Statement covers the specifics of this item.

5.5.6. Archive storage

The Practice Statement covers the specifics of this item.

5.5.7. Archival information access and verification procedures

The Practice Statement covers the specifics of this item.

5.6. Key Changeover

The Practice Statement covers the specifics of this item.

5.7. Compromise and Disaster Recovery

The Practice Statement covers the specifics of this item.

5.7.1. Incident and compromise handling procedures

The Practice Statement covers the specifics of this item.

5.7.2. Incidents, related to failures in hardware, software and/or data

The Practice Statement covers the specifics of this item.

5.7.3. Private key compromise procedures

The Practice Statement covers the specifics of this item.

5.7.4. Business continuity Management

The Practice Statement covers the specifics of this item.

5.8. TSP Termination

5.8.1. Termination plan

The Practice Statement covers the specifics of this item.

5.9. Time-stamping

5.9.1. Timestamp issuance

Timestamp tokens issued by TSA conform to the format and technical specifications of **ETSI EN 319 422** (the standard for time-stamp profiles). Each timestamp token includes at least the TSA's certificate identifier, the policy OID, a hash of the data provided by the subscriber, and the precise time of issuance, all signed by the TSA's private key (within the TSU). The process of issuing timestamps is securely automated: when a valid request is received, the TSA's system records the current time and produces a signed token. Only

authenticated requests are honored, and the system ensures that no unauthorized timestamps are generated.

The TSA guarantees that every timestamp token it issues contains an accurate representation of time, within the accuracy bounds. The time included in the token is linked to official UTC time sources, ensuring that the timestamp can be universally interpreted correctly. The TSA's signing system is protected against unauthorized access or tampering, so only legitimate timestamps are produced. Each time-stamp token is signed with the TSU's dedicated private key, and the system will automatically reject any attempt to issue a timestamp if the TSU's key is expired or has been revoked. This prevents invalid tokens (e.g., signed with an expired certificate) from ever being generated.

The TSA monitors its timestamp issuance process for anomalies. If the TSA's internal clock were ever detected to be out of sync beyond allowable limits, the TSA would suspend issuance of timestamps until the clock is restored to accuracy. This suspension mechanism protects the reliability of all timestamps issued.

5.9.2. Clock synchronization with UTC

The TSA maintains its time reference (the TSU system clock) in synchrony with Coordinated Universal Time (UTC). The time source is traceable to official UTC(k) laboratories recognized by the Bureau International des Poids et Mesures (BIPM). TSA system regularly synchronizes with at least one UTC(k) time signal, using NTP protocol to achieve an accuracy better than or equal to 1 second relative to UTC.

The TSA's declared accuracy is documented, and all issued timestamps include an indication of the accuracy if required by the profile.

The TSA's clock synchronization mechanism is designed such that the TSU clock will not drift outside the declared accuracy under normal operation. The system continuously monitors the difference between the TSU clock and the trusted UTC source. If the TSU clock deviates beyond the allowed tolerance (for example, by more than 1 second), the TSA will suspend issuance of further timestamps until the clock is resynchronized. Procedures are in place to rapidly detect and correct any clock drift or synchronization failure. All events related to clock synchronization are logged to provide an audit trail.

The TSA also accounts for leap seconds. When a leap second is announced by the relevant authorities (IERS), TSA's systems are prepared to handle the extra second. The leap second adjustment is applied at the end of the day (UTC time) on which it occurs, in accordance with the standard practice (typically June or December). The TSA keeps a record of the exact moment the leap second was inserted or removed, within the stated accuracy, ensuring transparency in how the timestamp times align with UTC during that period. By planning for leap second events and documenting their handling, the TSA maintains continuous synchronization without compromising the service. After any leap second or clock adjustment,

the TSA reconfirms that the time shown in issued tokens remains correct within the declared accuracy. These measures fulfill the requirement that the TSA's clock be reliably synchronized with UTC at all times.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

6.1.1.1. Root CA and subordinate CA

Key pairs for all Simplifi authorities are generated in accordance with a documented generation procedure that ensures the integrity and confidentiality of the keys. The key pair generation takes place at the Simplifi headquarters or secure data center in a physically secure environment, in the presence of at least two authorized individuals in trusted roles, one of whom must be the Security Officer. A report is prepared documenting the activities performed during the key generation process, and this report is signed by all participants involved in the procedure. The Security Officer certifies with their signature that the key generation process was carried out in accordance with the documented procedure, ensuring the confidentiality and integrity of the keys.

The private key used for creating a qualified electronic signature or qualified electronic seal is generated within a qualified signature or seal creation device located in a secure environment managed by Simplifi in accordance with ETSI TS 119 431-1 requirements. The private key generation process takes place entirely within the QSCD device, with no possibility of export, in compliance with the CEN EN 419 241-2 standard. The signer authorizes the key creation operation and its subsequent use remotely — through an assigned authentication and signature operation authorization mechanism, in accordance with the Signature Activation Protocol (SAP) defined in ETSI TS 119 432.

6.1.1.2. Subject key pair generation on remote QSCD (remote device)

Subject private keys are generated and used in a Remote Qualified Signature Creation Device (RQSCD). RQSCD complies with certification against EN 419 241-2 include SCAL2 model.

RQSCD supports cryptographic algorithms and key lengths defined in ETSI TS 119 312.

The RQSCD environment protects all generated keys to ensure their confidentiality and integrity. Keys are not kept outside of the protected environment.

Subject private keys are linked to the subject before certificate issuance. The reference link is created after registration and initial identity validation specified in the chapter 3.2 of the present document. The technical process ensures that the identification data linked to the subject's identity reference matches the data associated with the subject of the corresponding certificate.

RQSCD is initialized before generating or containing any signing key. Its technical mechanisms require at least two operators. It is done according to chapter 6.1.1.1.

6.1.2. Private key delivery to Subject

Simplifi **does not deliver** private keys to the Subject.

In the case of **remote signing services**, the private key is generated and securely stored within a **Qualified Signature Creation Device (QSCD)** operated and managed by Simplifi or a designated trusted provider. The Subject does not gain possession or control of the private key at any time.

- For short-term certificates (e.g., session-based remote signing), the private key exists only for the duration of a single signing session and is destroyed or disabled immediately after use. No credential or identity means is issued or persisted for reuse by the Subject.
- For **long-term certificates** the Subject's identity is verified by the Registration Authority, and the associated private key is securely stored in a QSCD. In such cases, access to the key is possible only through **secure authentication mechanisms.**

At no time is the private key extracted, exported, or made accessible to the Subject outside of the secure signing process.

6.1.3. Public key delivery to certificate issuer

Not applicable

6.1.4. CA public key delivery to relying parties

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.

6.1.5. Key sizes

Simplifi uses cryptographic algorithms and minimum key sizes that comply with the requirements of the ETSI TS 119 312 standard.

The keys of all certification authorities of Simplifi are RSA keys and have at least 4096 bits.

Keys of the subjects are RSA keys and have at least 2048 RSA bits.

6.1.6. Public key parameters generation and quality checking

Public key-generating parameters meet the requirements specified in the standards: ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI TS 119 312 norms in their latest applicable version available at the moment of publication of the present document.

Prior to issuing a certificate, the CA verifies that the public key has not been used before.

6.1.7. Key usage purposes

Allowed key usage purposes are described in KeyUsage field of standard extension of a certificate complying with X.509 v3.

Subject Signing Key usage:

- digitalSignature
- nonrepudiation

Root CA and Issuing CA key usage:

- keyCertSign
- keyCrlSign

OCSP responder Key usage:

- digitalSignature
- OCSP signing

6.2. Private Key Protection and Cryptographic Module Engineering

6.2.1. Cryptographic module standards and controls

All HSMs protecting CA and PKI infrastructure keys are certified against FIPS 140-2 Level 3.

Cryptographic modules used by Simplifi for remote signature and sealing are present in the list of EU QSCD and are certified against EN 419 241-2.

6.2.2. Private key (n out of m) multi-person control

The cryptographic modules on which the service CA and subject keys are stored is located in the secure environment. At least two authorized people are needed to activate the respective private key and to access the private subject keys.

Shared secrets are stored on cryptographic cards, protected by a PIN number and transferred in a secure manner to their holders in trusted roles.

6.2.3. Private key escrow

Not applicable.

6.2.4. Private key backup

Subject Private Keys

Private keys used by Subjects for qualified remote electronic signatures and electronic seals are generated, stored, and used exclusively within a Remote Qualified Signature Creation Device (RQSCD) managed by Simplifi. These devices are implemented using certified Hardware Security Modules (HSMs) and are part of a protected Security World.

Subject private keys are never exported or delivered to the Subject and are protected in such a way that only authorized signing operations may be performed. Backup and recovery of Subject private keys are handled entirely within the Security World infrastructure, and access is protected by multi-factor authentication and role-based access control. No Subject private keys are stored outside the cryptographic boundary of the RQSCD.

Certification Authority (CA) Private Keys

Simplifi applies distinct key management and backup procedures for Root CA and Intermediate CA private keys.

Root CA private keys are generated and stored in a physically isolated HSM and are protected by a Key Encryption Key (KEK). The KEK is divided into cryptographic shares distributed among multiple key custodians, in accordance with Simplifi's key ceremony procedures. The Root CA private key is never exported in unencrypted form. Backup and recovery require quorum-based access under dual control, in a secure, trusted environment.

Intermediate CA private keys are protected within HSMs that participate in a Simplifi-managed Security World. Backups are performed by securely archiving the Security World data itself. These backups are encrypted, versioned, and stored offline in physically secure facilities. Recovery is only possible using compatible HSM, under dual control by authorized personnel in trusted roles.

In all cases, key backup operations are strictly limited to designated personnel with trusted roles, require dual control, and are performed in physically secured environments. Backup copies are afforded a level of protection equal to or greater than that applied to the operational keys, in full compliance with ETSI EN 319 411-1 and eIDAS requirements.

Simplifi does not generate or retain copies of private keys belonging to CA operators, Registration Authority staff, or any other individual participants.

6.2.5. Key Restoration

Restoration of the private key requires the presence of the Security Officer and a dedicated System Operator for dual approval of configuration import.

6.2.6. Private key archival

Not applicable. Private keys are not archived.

6.2.7. Private key transfer into or from a cryptographic module

Transfer of subject private keys is not allowed.

6.2.8. Private key storage on cryptographic module

The private keys are generated and stored in a secure area of the cryptographic device. Private keys can be stored in the module in plain or encrypted form. Regardless of private key storing form it is not accessible from outside cryptographic module for unauthorized entities.

6.2.9. Method of activating private key

Private subject keys are activated by the user under his/her only sole control.

6.2.10. Method of deactivating private key

In the case of a subject private signing key deactivation is carried out immediately after creation of an electronic signature or after ending the online session (cookie session).

6.2.11. Method of destroying private key

Simplifi staff deals with the destruction of the private key when the certificate expires or is revoked, according to security procedures provided by security policies and device manufacturer specifications. This is accomplished by deleting the private key on the HSM and simultaneously deleting the backups on data media. When use of the HSM is terminated, the private keys in, the device are deleted.

6.2.12. Cryptographic Module Rating

The scope related to this item is addressed in 6.2.1.

6.2.13. Public key archival

The Practice Statement covers the specifics of this item in chapter 5.5 “Records archival”.

6.2.14. Certificate operational periods and key pair usage periods

A certificate validity period is determined based on:

- The state of technology;
- The state of the art for cryptographic technologies;
- The intended use of the certificate.

Validity periods are stated on each certificate. Maximum periods of use of certificates:

Subject of certicate	Maximum validity period
Simplifi Root CA G1	20 years
Simplifi Qualified CA Class 3 G1	10 years

The details are presented in chapter 7.

6.3. Activation Data

6.3.1. Activation data generation and installation

Simplifi ensures that each subject is accurately identified and authenticated prior to permitting actions that could affect the authorized control over any signing key.

Activation of the signature creation device by the subject requires the use of two separate authentication factors.

6.3.2. Activation data protection

The subject is responsible for protecting his or her authentication means and/or device.

In case of remote signatures or seals, SAD is collected and secured by the Signature Activation Protocol, used to control with a high level of confidence (at least SCAL2-Sole Control Access Level 2), a given signature operation, performed by a RQSCD on behalf of the subject, that this under sole control of the subject. Signature Activation Module (SAM) used in a tamper protected environment.

The protection of activation data relies on physical access controls (on the part of both the CA and the Subject) as well as cryptographic safeguards.

6.3.3. Other aspects of activation data

Not applicable.

6.4. Computer Security Controls

6.4.1. Specific computer security technical requirements

The Practice Statement covers the specifics of this item.

6.4.2. Computer security rating

The Practice Statement covers the specifics of this item.

6.5. Life Cycle Security Controls

6.5.1. System development controls

The Practice Statement covers the specifics of this item.

6.5.2. Security management controls

The Practice Statement covers the specifics of this item.

6.5.3. Life cycle security controls

The Practice Statement covers the specifics of this item.

6.5.4. Network Security Controls

The Practice Statement covers the specifics of this item.

6.5.5. Time synchronization

The Practice Statement covers the specifics of this item.

6.6. Time-stamping

6.6.1. TSU key generation

Generation of each TSU's signing key is carried out in a physically secure environment by personnel in trusted roles, under at least dual control. Only authorized and necessary individuals (as determined by the TSA's internal security policies) participate in the TSU key generation process, ensuring tight control on this critical activity. TSU signing keys are generated within a high-assurance cryptographic hardware device that meets recognized security standards. In particular, the key generation device is the following:

- A device certified to meet FIPS 140-3 Level 3 requirements (or equivalent national standard) for secure cryptographic modules.

The TSA uses RSA 4096-bit keys with SHA-512 hashing for generating time-stamp digital signatures, in compliance with the algorithm suites identified by ETSI TS 119 312 for qualified electronic signatures/seals.

Each TSU's signing key is never exported in plain form from that module.

6.6.2. TSU private key protection

The confidentiality and integrity of TSU private signing keys are safeguarded through strong controls. All TSU private keys are held and used within secure cryptographic hardware (a Hardware Security Module) that provides a controlled environment for key storage and

usage. The cryptographic module employed for key protection meets high assurance criteria FIPS 140-3 Level 3). This ensures the module is tamper-resistant and that keys cannot be extracted or used without authorization.

If a TSU private key needs to be backed up, the backup is performed in encrypted form and under strictly controlled conditions. Any key backup or key copy operation involves at least two trusted individuals (dual control) in a secure environment. Backup copies of TSU keys are themselves protected by cryptographic means at the same level of security as main asset.

The TSA's security rules restrict access to TSU private keys only to those functions necessary for time-stamp issuance. Administrative access to the HSMs is limited to authorized personnel in trusted roles, and multi-factor authentication is used for such access. Logs are kept of all operations involving TSU key material. These combined measures meet the requirements for protecting TSU private keys against disclosure or alteration.

6.6.3. TSU public key certificate

Each TSU's signature verification public key is made available to relying parties via an X.509 public key certificate issued by a Certification Authority. This certificate binds the TSU's identity to its public key and is used by clients to verify the digital signature on timestamps. The TSA ensures that no time-stamp tokens are issued by a TSU until that TSU's public key certificate is properly issued and loaded into the TSU's secure device. This prevents any unsigned or unverifiable tokens from being produced.

The TSU certificate includes extensions identifying the key's specific usage for timestamping.

Once the TSU's certificate is in place and the TSU is activated, the TSA can begin signing timestamps with the corresponding private key.

6.6.4. Rekeying TSU's key

The TSA does not perform "rekey" operations (re-use of an existing key for a new certificate) for TSU keys. Instead, when a TSU's key pair is due for replacement (e.g., about to expire or if compromised), a brand new key pair is generated and a new public key certificate is then obtained for the new key. This approach ensures that each TSU key is unique and traceable to a specific validity period and that no old key material is extended beyond its intended lifetime.

6.6.5. Life cycle management of signing cryptographic hardware

All cryptographic hardware devices used for timestamp signing are handled with strict life-cycle management procedures to maintain their security integrity. The TSA ensures that each device is securely shipped, stored, operated, and eventually decommissioned. Upon

delivery from the manufacturer, the device is checked to ensure it has not been tampered with in transit; it remains sealed or under monitoring until installation. During storage before use, the device is kept in a secure environment to prevent any unauthorized access or modifications. Installation of the device into the operational environment is performed by authorized personnel in trusted roles, and at least dual control is employed during critical setup steps such as loading TSU keys.

When activating a new TSU device or duplicating a TSU's signing key onto a backup device (for load balancing or failover), trusted personnel follow documented procedures that ensure the confidentiality of keys and the authenticity of the target device.

When a cryptographic device is to be retired from service, all TSU private keys and sensitive material are securely erased from it before decommissioning. The erasure is done in such a way that the data cannot be recovered, even using advanced forensic techniques. Only after confirmed deletion of keys will the device be repurposed or disposed of. These life-cycle controls meet the requirements for protecting the TSA's cryptographic hardware from inception to retirement.

6.6.6. End of TSU key life cycle

Each TSU signing key is assigned a maximum validity period to enforce periodic key renewal. Simiplifi limits the lifetime of TSU private keys to 5 years, which facilitates secure algorithm agility and key management. A TSU's signing key will never be used beyond the validity of its corresponding public key certificate. In practice, the TSU's certificate expiration date dictates the absolute latest date the TSU key can be used for signing; typically, the TSA will retire the key slightly earlier to maintain a safety margin.

The TSA implements proactive measures to transition to new TSU keys well before the old keys expire. Approximately 1 year before a TSU key is due to expire, the TSA generates a new key pair and obtains a new TSU certificate. The new TSU (or new key on an existing TSU) is brought into operation in parallel with the old one, so that time-stamp requests can gradually be served by the new key. This ensures a smooth rollover with no interruption of service. Once the new TSU is fully operational, the old TSU is deactivated when its validity period ends.

After a TSU key is expired or no longer in use, TSA destroys the TSU's private key material in a secure, irreversible manner. This destruction includes all copies or backups of that key. By securely wiping or physically destroying the hardware that contained the key, the TSA guarantees that the expired key cannot be resurrected or used to forge timestamps. These practices fulfill the requirements for end-of-life handling of TSU keys, ensuring that old keys do not become a security liability.

7. Certificate and CRL Profiles

Profiles of certificates and CRLs are issued in line with norms of ETSI TS 319 412-1 and ETSI EN 319 412 (Parts 2,3,5).

7.1. Certificate Profile

The structure of certificate profile is presented in publicly available repository *http://simplifi.ro/policies*

7.2. CRL Profile

The structure of CRL profile is presented in publicly available repository *http://simplifi.ro/policies*

7.3. OCSP Profile

The structure of OCSP profile is presented in publicly available repository *http://simplifi.ro/policies*

8. Compliance Audit and Other Assessment

8.1. Frequency or circumstances of assessment

The Practice Statement covers the specifics of this item.

8.2. Qualification of auditors

The Practice Statement covers the specifics of this item.

8.3. Auditor's relationship with Simplifi

The Practice Statement covers the specifics of this item.

8.4. Audit scope

The Practice Statement covers the specifics of this item.

8.5. Actions Taken as a Result of Deficiency

The Practice Statement covers the specifics of this item.

8.6. Communication of results

The Practice Statement covers the specifics of this item.

9. Other Business and Legal Matters

9.1. Fees

The Practice Statement covers the specifics of this item.

9.2. Financial Responsibility

The Practice Statement covers the specifics of this item.

9.3. Confidentiality of Business Information

The Practice Statement covers the specifics of this item.

9.4. Privacy of Personal Information

The Practice Statement covers the specifics of this item.

9.5. Intellectual Property Rights

The Practice Statement covers the specifics of this item.

9.6. Representations and Warranties

9.6.1. Simplifi obligations

The Practice Statement covers the specifics of this item.

9.6.2. Registration Authorities obligations and warranties

The Practice Statement covers the specifics of this item.

9.6.3. Subjects and subscribers obligations and warranties

The Practice Statement covers the specifics of this item.

9.6.4. Relying Party Obligations and warranties

The Practice Statement covers the specifics of this item.

9.6.5. Representations and warranties of other participants

The Practice Statement covers the specifics of this item.

9.7. Warranty Disclaimer

The Practice Statement covers the specifics of this item.

9.8. Limitations of Liability

The Practice Statement covers the specifics of this item.

9.9. Indemnities

The Practice Statement covers the specifics of this item.

9.10. Amendments

The Practice Statement covers the specifics of this item.

9.11. Dispute Resolution Procedures

The Practice Statement covers the specifics of this item.

9.12. Governing Law

The Practice Statement covers the specifics of this item.

9.13. Miscellaneous Provisions

The Practice Statement covers the specifics of this item.