simplifi

Simplifi Certification Practice Statement

Policies and Operational Controls for Qualified Trust Services

This CPS governs the issuance, management, and revocation of the following qualified trust services: Qualified Certificates for Electronic Signatures, Qualified Certificates for Electronic Seals, Qualified Electronic Timestamps.

This CPS is reviewed regularly by the Trust Service Manager and is subject to approval and audit by the designated supervisory authority. It provides assurance to subscribers, relying parties, regulators, and auditors of the **integrity, availability, and reliability** of Simplifi's trust services.

www.simplifi.ro

simplifi

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	Certification Practice Statement
Document OID	1.3.6.1.4.1.63578.1.1.2
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

simplifi

Contents

1. Introduction

SIMPLIWORKS SRL, operating under the umbrella brand **Simplifi**, is a Romanian company established on **April 11, 2022**, with the mission to deliver high-assurance trust services that uphold the core principles of **security**, **integrity**, **confidentiality**, and **non-repudiation**. Simplifi is committed to building a modern and transparent trust infrastructure that meets the rigorous standards required for **Qualified Electronic Signatures**, **Qualified Electronic Seals**, and **Qualified Electronic Time-Stamps**, as defined under the **eIDAS Regulation (EU) No 910/2014**.

As a **Certification Authority (CA)** operating within a dedicated **Public Key Infrastructure (PKI)**, Simplifi is responsible for issuing, managing, revoking, and validating digital certificates through well-defined and auditable procedures. Our PKI design incorporates a **Root Certification Authority**, with subordinate **Intermediate CAs** tailored to distinct types or classes of services. Each Certification Authority uses specific **certificate profiles** adapted to the service context and assurance level required.

Simplifi's role as a **Qualified Trust Service Provider (QTSP)** includes providing trust services to both individuals and organizations, whether private or public, in full compliance with applicable **European** and **Romanian** legislation. These services include, but are not limited to:

- The issuance and lifecycle management of qualified and non-qualified certificates;
- The generation and validation of electronic signatures and seals;
- The publication of Certificate Revocation Lists (CRLs) and maintenance of an Online Certificate Status Protocol (OCSP) service for real-time certificate status information.
- Time-stamping

1.1. Scope

The Practice Statement defines the principles governing the delivery of electronic signature services and the execution of certification authority operations in compliance with the EU eIDAS Regulation requirements related to trust service provision. It also ensures consistency with Romanian legislation. This document establishes the roles, duties, and responsibilities of all involved parties and outlines the management, operational, and physical controls implemented by SIMPLIWORKS SRL, acting under the brand Simplifi.

It functions as a unified framework for delivering trust and electronic identification services according to specific policies adopted by SIMPLIWORKS SRL, acting under the brand Simplifi, in its capacity as a a Qualified Trust service Provider.

Specifically, the Practice Statement covers the following services:

- Issuance and management of certificates for electronic signatures;
- Issuance and management of certificates for electronic seals;
- Issuance and management of certificates for PKI infrastructure

- Provision of revocation service and online status information for certificates.
- Generation and management of electronic signature creation data on behalf of the Subject (remote signatures and seals).
- Time-stamping service.

The practices described herein apply to both qualified and non-qualified trust services.

This document includes a statement confirming that all services provided under the Practice Statement conform to the following regulations:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, consolidated version: 18/10/2024
- Applicable Romanian national legislation, including but not limited to Law no. 455/2001, Emergency Ordinance no. 38/2020, Law number 214/ 2024, decisions of the ADR (Authority for Digitalization of Romania)

Detailed provisions for the delivery of trust and electronic identification services are defined in separate policy documents. Each service is individually categorized as either qualified or non-qualified. These policies are publicly accessible, as described in Chapter 2.1.

This PS serves as a comprehensive and unifying framework for Simplifi's internal practices and publicly declared service commitments. It is structured according to RFC 3647 and aligned with the applicable versions of the following standards:

- ETSI EN 319 401 – General policy requirements for trust service providers;
- ETSI EN 319 411-1 and 319 411-2 – Policy and security requirements for trust service providers issuing certificates;
- ETSI EN 319 421 – Policy and security requirements for trust service providers issuing time-stamps;
- ETSI TS 119 431 (Parts 1) – Policy and security requirements for remote signature creation;
- ETSI EN 319 412 (Parts 1, 2, 3, and 5) – Certificate profiles and subject naming.

Throughout this document, the term "Practice Statement" refers to the present document.

1.2. Services overview

The trust services are logically broken down into the following component services like CA, RQSCD and TSA to address requirements stated in clause 4.3 of ETSI EN 319 411-1 and 4.2 of ETSI EN 319 421:

- **Registration Services**
    - **Registration authority**: verifies the identity and, if applicable, any specific attributes of a subject. The registration authority provides registration for CA services.

- **CA Services**
  - **Certificate generation service**: creates and signs certificates based on the identity and other attributes verified by the Registration service. This includes key generation.
  - **Dissemination service**: disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes TSP's terms and conditions and any published policy and practice information available to subscribers, subjects and relying parties.
  - **Revocation management service**: processes requests and reports relating to revocation to determine the necessary action. The results of this service are distributed through the revocation status service.
  - **Revocation status service:** provides certificate revocation status information to relying parties and other components.
- **Remote signing Service**
  - **Remote QSCD provision service** manages QSCD on behalf of the subject, including maintenance keys and signature data
  - **Service for creation of electronic signatures** using server signing application
  - **Authentication service** - A service that provides subject authentication based on the means assigned by identity linking service
  - **Identity linking service** - assigns and links authentication methods to the subject
- **TSA Service**
  - **Time-stamp provision service**: generates time-stamps
  - **Time-stamping management**: monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the time-stamping provision service.

This subdivision of services is only to clarify the trust services framework and places no restrictions on any subdivision of implementing the TSP's services.

1.3. Document Name and Identification

The full name of this document is „ Simplifi Certification Practice Statement”. The electronic version of this document will be published and made accessible at *https://simplifi.ro/policies/*. The Practice Statement can be identified by any party through the following OID: 1.3.6.1.4.1.63578 .1.1.2

Practice statement supports other OIDs:

1.4. PKI Participants

The Practice Statement regulates the most important roles between the following parties:

1.4.1. Certification authorities

Certification authorities (CAs) are operated by Simplifi and issue certificates and revocation lists.

There are the following root certification authorities of Simplifi (Root CAs):

- Simplifi Root CA G1,

The following types of Issuing Certificate Authorities are operated by Simplifi under the Root CA:

- Simplifi Qualified CA Class 3 G1

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

The each trust service policy (policy document) defines the certificates profiles of each authority.

1.4.2. 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.

The responsibilities of a Registration Authority include:

- Identifying and verifying the identity of the **Subject** (certificate holder) in accordance with the certificate policy and applicable assurance level;
- Validating the completeness and accuracy of certificate requests and supporting documentation;
- Handling requests for certificate **issuance, renewal, revocation**, and **suspension**;
- Collecting and securely transmitting identity evidence and application data to the CA;
- When applicable, supporting delivery of cryptographic devices or activation credentials.

Simplifi supports both **on-site** and **remote identity verification**, including the use of **electronic identification** in compliance with **Regulation (EU) No 910/2014 (eIDAS)** and/ or **Romanian national laws**, such as **Law 455/2001, Law 214/2024** and **OUG 38/2020**. For high-assurance trust services, Simplifi relies on certified or notified electronic identification means authorized under national and/ or European frameworks.

The final decision on certificate issuance always resides with the CA, even when RA activities are delegated.

1.4.3. 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.

1.4.4. Relying parties

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

1.4.5. Other participants

Simplifi engages subcontractors, such as data centers, to ensure secure and reliable colocation and operation of server and network equipment.

1.5. Certificate Usage

The scope of this chapter is covered in a specific trust service policy.

1.6. Practice Statement Administration

1.6.1. Organization responsible for administering the document

This Practice Statement is administered by Simplifi:

Strada Gheorghe Țițeica 142, București 014192Romania

1.6.2. Contact

easy@simplifi.ro

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

The Simplifi team is responsible for assessing the completeness and accuracy of the Practice Statement and other documents 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 1.6.2

1.6.4. Approval procedures

The Practice Statement 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 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 1.4.5

1.7. Definitions and Acronyms

Definitions and abbreviations used in this document are provided at the end.

2. Publication and Repository Responsibilities

2.1. Repository

Simplifi will have a repository of:

- Publicly available documents along with previous versions
- All published certificates (both active and revoked) and CRLs
- The electronic version of those will be published and made accessible via URL(s), which will be specified in subsequent versions of this document.

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

2.2. Information published by Simplifi as a Trust Service Provider

The repository at least contains the following documents:

- Practice Statement – current and previous version
- Trust Service Policies - current and previous version
- General Terms & Conditions
- CA Certificates and profiles
- Certificates Revocation Lists (CRLs)
- 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 chapter 9.9,
- 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. Review and modification

The Practice statement and specific trust service policies are reviewed on a yearly basis or in case of significant change in service provisions.

2.5. Access to publication

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

3. Identification and Authentication

The requirements for identification and authentication practices originate from ETSI EN 319 411-1 and ETSI EN 319 411-2. These practices apply to registration of subject in terms of certificate issuance and the processing of revocation requests.

Their description is outlined in a specific trust service policies, available publicly in the repository refered to in Chapter 2.1

4. Certificate Life-Cycle Operational Requirements

The requirements for certificate life-cycle practices originate from ETSI EN 319 411-1 and ETSI EN 319 411-2. These practices apply to certificate management.

Their description is outlined in a specific trust service policy, available publicly in the repository reffered to in Chapter 2.1.

5. Management, Operational and Physical Controls

The chapter outlines the general practices implemented by Simplifi in alignment with ETSI EN 319 401 and ETSI EN 319 411-1, focusing on management, operational, and physical controls.

Simplifi follows a formal risk management process to define and maintain these controls, ensuring they are regularly reviewed and updated. The Simplifi Board of Directors approves the risk assessment and accepts the identified residual risks.

5.1. Physical Security Controls

Simplifi applies robust physical and environmental security measures to protect the integrity, availability, and confidentiality of its trust services infrastructure. These controls align with relevant European standards (including ETSI EN 319 401, EN 319 411-1, and ISO/IEC 27001) and Romanian national regulations.

All trust service systems are hosted in a tier III+ commercial data center with 24/7 physical security, multiple authentication layers, and comprehensive monitoring. The Root Certification Authority (Root CA) is kept offline in secure storage and accessible only through a dual-control procedure.

5.1.1. Site Location and General Controls

- The main infrastructure is hosted in a third-party high-security data center.
- Security guards are present 24/7 at both the data center and Simplifi office buildings.

- Video surveillance (CCTV) covers all access points.
- Data center visitor access requires pre-approval and escort by authorized personnel.
- Audit logging is enforced for all data center physical access events.

5.1.2. Data Center Access Control

Access to trust service systems hosted in the data center is governed by a multi-level access control model:

- **Level 1** – Building Entry: Requires valid identification (e.g., national ID or passport) and visitor registration at reception. CCTV-monitored and manually logged.
- **Level 2** – Floor Access: Controlled via proximity card; restricted to specific floors/zones.
- **Level 3** – Rack Access: Simplifi's infrastructure is hosted in a dedicated half-rack, secured by a PIN code lock. Access is limited to authorized personnel
- **Level 4** – Root CA Access: Root CA systems are kept offline and stored in a physically separate location.

5.1.3. Environmental Protections

- Fire detection and suppression systems are deployed throughout all critical areas.
- HVAC systems regulate temperature and humidity to meet equipment specifications.
- UPS and generators ensure uninterrupted power.
- Servers are placed in elevated positions or raised floors to mitigate flood risk.

5.1.4. Media Handling and Secure Disposal

- Sensitive media (e.g., cryptographic material, backups) is stored in **access-controlled secure cabinets.**
- **Disposal** of electronic and physical media follows strict procedures:
  - Cryptographic keys and HSMs are wiped or physically destroyed.
  - Paper media is shredded.
  - Hardware is sanitized or decommissioned in line with vendor recommendations.

5.1.5. Off-Site Backup and Disaster Recovery

- **Backup data** is replicated to a distinct, secure secondary site.
- Off-site backups are protected against unauthorized access, fire, and water exposure.
- Disaster recovery procedures ensure restoration of services within **48 hours** in the event of a major incident.

5.2. Procedural Controls

5.2.1. Trusted Roles

To improve information security and prevent conflicts of interest, Simplifi has appointed personnel to trusted roles. The assignment of functions to trusted roles follows a clear separation of duties. The specific responsibilities and distribution of these roles are defined in Simplifi's internal documentation.

The following trusted roles are established in Simplifi:

- **CEO/Trust Service Manager** – responsible for correct management of Simplifi, determines directions of development of certification authority, responsible to manage Practice Statement and trust service policies,
- **Security Officer** – supervises implementation and handling of information system security procedures, initiates and supervises cryptographic key and shared secret generation; assigns rights in the field of security and user's access privileges,
- **System Administrator** – installs or supervises the installation of hardware and operating system software; performs initial configuration of the system, HSM devices, and network resources; oversees and carries out the change management process; responsible for the backup process.
- **System Operator** – in cooperation with the System Administrator, and when necessary, under direct supervision, performs operations to maintain service availability.
- **Registration Officer** – verifies subjects' identity and correctness of submitted certification request; authorizes certification request; authorizes the identity proofing policies provided by external identity proofing providers,
- **System auditor** – monitors services to ensure compliance with policies and procedures; verifies the event logs and incident management process.
- **Legal &DPO Officer-** ensures compliance with applicable legislation with respect to eIDAS and GDPR, reviews contractual obligations, terms and conditions, privacy policy, liability clauses etc.

Simplifi's trust services may also involve operational personnel who, although not assigned to trusted roles, perform tasks under supervision and without access to data processing.

5.2.2. Four- eyes principle

For highly security-critical operations, at least two individuals must be involved as a fundamental requirement. This is enforced through technical and organizational controls, including access permissions and knowledge verification.

The following activities require at least two people engagement:

- HSM initialization
- Root CA and subCAs certification keys generations
- CAs keys backup
- Restoration of the certification keys for Root CA, Issuing CAs

5.2.3. Identification and authentication for each role

All trusted roles are formally assigned by the CEO.

All identity checks are performed as a part of HR process.

Simplifi has implemented an onboarding procedure for each individual, which includes issuing personal authentication credentials to the IT systems and physical premises.

Every account is unique and assigned to one specific person, ensuring accountability.

Each person assigned to a trusted role formally accepts the responsibilities associated with it.

5.2.4. Roles requiring separation of duties

Each trusted role is granted only the permissions necessary for the assigned responsibilities. Some roles may be combined or modified within a limited scope. The roles of Security Officer and System Auditor remain strictly separated from all other roles.

Simplifi has a substitution process in place that ensures continuity of operations while maintaining compliance with the required separation of duties.

5.3. Personal Security Controls

5.3.1. Qualifications, experience and clearances

Simplifi's HR policy outlines the requirements for employment and assignment to designated roles. It incorporates a verification process to evaluate candidates' professional qualifications and formal credentials.

Each role is defined by a detailed job profile specifying the required skills and experience. All employees are also made aware of the disciplinary procedures defined in the policy, supporting accountability and compliance with organizational standards.

5.3.2. Personnel verification procedures

Simplifi verifies personnel information in the following areas:

- confirmation of previous employment.
- verification of recommendations.
- confirmation of educational degree.

- verification of criminal records (if applicable)
- identity verification.

Simplifi ensures that personnel will not have access to the trusted functions until the necessary checks are completed.

5.3.3. Training requirements

Simplifi requires trusted roles to meet strict competence and experience criteria at hiring and provides regular training to maintain their qualifications. Training covers at least:

- National and EU regulations.
- Role responsibilities and tasks.
- Information security policies.
- Personal data protection.
- Security controls and procedures based on this document and other policies, focusing on business continuity and recovery procedures.

5.3.4. Training frequency and requirements

Training described in chapter 5.3.3 must be repeated at least every 12 months or whenever significant changes are made to the Practice Statement or other policies.

All personnel involved in the operation of Simplifi's trust services — including those performing roles within the Certification Authority (CA), Registration Authority (RA), and supporting systems — are required to complete structured training before assuming operational, administrative, or security responsibilities.

Training ensures that each individual has the knowledge, competence, and awareness necessary to carry out their duties in compliance with:

- The current Certification Practice Statement (CPS) and related Trust Service Policies
- Internal security and operational procedures applicable to their roles;
- The software, hardware, and cryptographic systems used by CAs and RAs;
- Regulatory and legal obligations under eIDAS, Romanian legislation, and applicable standards.

Training topics include:

- Principles, structure, and requirements of Simplifi's CPS and Trust Service Policies;
- Operational procedures and security controls implemented across CA/RA systems;
- Responsibilities and restrictions associated with assigned roles;
- Incident response procedures in the event of a system failure, security event, or policy breach;
- Handling of cryptographic material, secure authentication, and dual-control requirements.

Upon completion of training, participants sign a formal acknowledgment of understanding and acceptance of responsibilities, including compliance with the CPS, Trust service policies, and internal security policies.

Retraining and awareness updates:

- Retraining is recommended at least once every 12 months, or earlier if:
  - Significant updates are made to the Practice Statement, Policies, or internal procedures;
  - The employee assumes a new role with additional security responsibilities;
  - A major incident or audit reveals deficiencies that require targeted training.

Simplifi maintains records of all completed training sessions and signed acknowledgments. Managers and personnel in security-sensitive or compliance-critical roles also receive additional security awareness training specific to risk management, incident response, and legal obligations under the applicable trust service frameworks.

5.3.5. Job rotation frequency and sequency

Not applicable.

5.3.6. Sanctions for unauthorized actions

Personnel are bound by contractual employment obligation to carry out their duties according to internal rules.

5.3.7. Independent contractor requirements

Independent contractors are subject to the same privacy protection and confidentiality conditions. Under a signed contract, the persons or consultants are subject to the same verification procedure as the defined by HR policy.

5.3.8. Documentation available to personnel

Personnel of Simplifi has access to the following documents:

- Certification Practice Statement,
- 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
- Extracts from documentation corresponding to performed role, including emergency procedures,
- range of responsibilities and obligations associated with the acted role in the system.

5.4. Audit logging procedures

5.4.1. Types of events recorded

Simplifi generates and stores logs events related to trust services and electronic identification service. The logs contain at least the following information:

- system start-up and shutdown
- System crashes and hardware failure
- outbound and inbound network traffic
- activities regarding user administration and permission management, access (including privileged access) to systems and applications
- activities performed with administrator accounts;
- changes to critical configuration files and backups;
- security relevant logs;
- use and performance of system resources;
- physical access to facilities, where appropriate;
- access and use of network equipment and devices; and
- environmental events, where appropriate;
- registration information gatherd by registration authority
- events relating to the life-cycle of certificates and keys
- events relating to the time-stamp service
    - routine clock re-calibrations and synchronizations
    - TSU keys and certificates management
    - Incidents with time-shifting

The records include information at least such as:

- type of event
- event identifiers
- date and time of the event
- source of log
- status

Only authorized persons from the Simplifi staff have access to the information in the records.

The primary sources of logs are applications and systems related to trust services and electronic identification systems. Audit logs are collected and recorded with protection against both external and internal modification and unauthorized access.

5.4.2. Frequency of processing log

The logs and monitoring are regularly checked for discrepancies. Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

5.4.3. Retention time for records

The audit logs which covers directly the provision of the trust service will be stored for 10 years.

5.4.4. Protection of records

Simplifi retains audit logs in dedicated storage systems. To preserve their integrity and confidentiality, security controls are in place, including access monitoring with authorization requirements and encrypted storage media to prevent unauthorized access.

The entire Simplifi infrastructure and trust services are synchronized with Coordinated Universal Time (UTC), with updates occurring at least once daily.

Once the retention period expires, all records are securely migrated to archival storage, with the process being both monitored and traceable.

In the event of legal proceedings, Simplifi can retrieve and present the necessary evidence.

5.4.5. Backup of records

Logs records are regularly backed up and securely stored in accordance with established procedures including specific schedule.

5.4.6. Audit log accumulation system

Each application automatically collects and transmits log entries to the logging system.

In the case of registration points, paper records may also be collected, which must be properly documented.

The logging functions are initiated automatically when the system starts and are continuously maintained throughout the entire operational period of the system.

In the event of any malfunction of automated monitoring systems or the logging system, such incidents are subject to the incident management procedure.

5.4.7. Notification system to event-causing subject

Simplifi's IT systems are constantly monitored. A dedicated team constantly monitors Simplifi Trust Services to track performance and detect security events.

If any activity affects system security, the system automatically sends alerts to at least the Security Officer and System Administrator.

If a significant incident is detected, the incident management process includes notifying the supervisory authority and, if needed, informing the affected subject.

5.4.8. Vulnerability assessment

Simplifi has implemented a vulnerability management procedure and a risk management procedure. In accordance with these procedures, all assets, including software and operating systems supporting the provision of services covered by this document, are required to undergo a vulnerability analysis.

Risk analysis is conducted at least once a year, as well as when introducing new services, implementing major architectural changes, or in the event of an incident.

The entire infrastructure is subject to vulnerability scanning at least once per quarter, carried out by an independent expert. If any vulnerabilities are detected, the vulnerability management procedure is activated to address and mitigate the identified risks.

5.5. Records Archival

5.5.1. Types of archives

Simplifi archives all data related to:

- The registration information – all documents and data used in process of identity proofing
- all request submitted by users of Simplifi services including certificates application
- all events relating to the life cycle of keys managed by the CA, including any subject key pairs generated by the CA
- CRLs
- Terms and conditions agreed by the Subject/Subscriber
- Others documents related to the trust service and electronic identification service provision.

5.5.2. Retention period of archives

Archived data (paper and electronic) is stored for a minimum 7 years after any certificate based on these records ceases to be valid.

5.5.3. Protection of archive

Simplifi stores archives in dedicated storage. To ensure integrity and confidentiality, Simplifi has implemented security controls, including monitored access that requires authorization and encryption of media storage to prevent unauthorized access.

During the preservation period, Simplifi monitors the media on which archived data is stored to ensure data availability throughout the required retention period.

Archival storage in an external archiving service is permitted.

5.5.4. Backup archives procedures

Simplifi has implemented a backup process for archives to ensure data recovery in the event of primary media failure. This mechanism guarantees the ability to restore archives from backup copies.

Detailed procedures for archiving, backup creation, and data recovery are outlined in the internal documentation.

5.5.5. Requirements for time-stamping the archives

Archives are kept by third-party providers that ensured accurate time-representation.

5.5.6. Archive storage

The archive collection system is an internal system (solution) of Simplifi and then place them to external service maintained by third-party providers.

5.5.7. Archival information access and verification status

Access to the archive is granted only to individuals holding trusted roles and is possible only after successful authorization.

To verify the integrity of archived data, periodic tests are conducted, and the data is compared with the original records. This process may be carried out under the supervision of the system administrator and the security officer and must be documented in the event log.

5.6. Key Changeover

The key changeover procedure applies to the keys of certification authorities (Root CA, CA, subordinate CAs). The key exchange process is conducted in a manner that ensures the maintenance of the agreed minimum certificate validity period.

Before the expiration of any certification authority certificate, a new PKI is established. As part of this process, a new pair of keys and a certificate for the new certification authority are generated.

During the transition period, both the old and new certification authorities operate concurrently until the old authority's certificate expires. The new certification authority assumes the role of the expiring one and handles all certificate-related activities, including issuance, suspension, revocation, and CRL generation.

The expiring certification authority continues to process only the revocation of certificates issued under its own infrastructure and generates CRLs until its operational activity ceases upon certificate expiration.

The new certification authority's certificate is promptly published in the repository to ensure business and trust continuity.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and compromise handling procedures

Incident handling and threat response are governed by procedures outlined in the Business Continuity Plan and the incident management process.

Simplifi reviews and tests these procedures at least once a year to confirm their effectiveness and suitability.

Incidents can be reported using internal or external forms, or by sending an email to easy@simplifi.ro

The Incident Evaluation Team responds based on the severity of the incident, with a maximum response time of 24 hours on business days.

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

All information concerning the corruption of computing resources, software, and/or data is communicated to the Security Officer, who then assigns the necessary tasks according to established incident, risk and change management procedures.

These procedures are designed to assess the severity of an incident, investigate the incident thoroughly, minimize its impact, and implement measures to prevent recurrence in the future.

5.7.3. CA Private Key compromise or loss of calibration of a TSU clock

Key compromise is handled according to Incident Management documentation. Because it also qualifies as a disaster, the business continuity plan is triggered.

In the event of a compromise, suspected compromise, or loss of integrity affecting a Certification Authority (CA) or Time-Stamping Authority (TSA), Simplifi follows a defined set of immediate response actions:

- The operating authority is immediately terminated.
- If the Time-Stamping Authority is compromised, suspected to be compromised, or loses calibration, Simplifi halts the issuance of timestamps until secure and accurate operations are restored through corrective measures.
- The Certification Authority generates a new cryptographic key pair.

- All certificates issued under the compromised CA are revoked and added to the Certificate Revocation List (CRL) with the appropriate reason for revocation.
- The specific certificate corresponding to the compromised key is also placed on the CRL with an appropriate termination reason.
- Affected users are promptly notified through mass communication channels, including announcements on the Simplifi website and email.
- Relying parties are also informed through the same communication channels.
- New certificates are issued to all affected users.
- Replacement certificates are provided at no cost to the users; all expenses are covered by Simplifi.
- An immediate analysis of the incident is conducted, and a formal report is prepared detailing the cause of the compromise.

In the event of a compromise or suspected compromise of Time-Stamp Unit (TSU) keys, or if a time desynchronization occurs between the TSU and its trusted time source, Simplifi will provide subscribers with all necessary information to identify any incorrectly issued time-stamps - provided that doing so does not violate subscriber privacy or compromise the security of Simplifi's services. This information will include, at a minimum, the name of the qualified time-stamp authority and the time window during which the improper issuance occurred.

If the cryptographic algorithms or parameters used by Simplifi's certification authorities are deemed no longer sufficient to maintain the required trust level, Simplifi will notify all certificate holders through public announcements, including publication via mass media and electronic mail.

5.7.4. Business Continuity Management

Simplifi maintains a comprehensive Business Continuity Plan (BCP) that outlines potential risks, remediation strategies, and acceptable recovery times. A key element of the BCP is the inclusion of measures to prevent the recurrence of incidents that may have triggered the activation of the plan.

Simplifi regularly performs risk analyses to identify potential risks and determine appropriate countermeasures within its business operations and processes. Upon identifying risks, Simplifi implements suitable technical and organizational measures to address and mitigate them. These risks are systematically reviewed and updated as necessary. The board of directors is responsible for approving risk treatment plans and accepting residual risks.

To ensure the continuity of service operations, Simplifi ensures backups of all essential data, information, and software. These backups are stored in a secure location at a determined distance from the primary site, allowing for timely restoration of operations in the event of major incidents or disasters.

Backups are regularly tested to verify their effectiveness and compliance with business continuity requirements.

5.8. Termination plan

Simplifi maintains a current and comprehensive termination plan to be enacted in the event of trust service discontinuation, ensuring minimal disruption to subscribers and relying parties.

Before termination, Simplifi will notify all affected stakeholders, including subscribers, relying parties, other trust service providers (TSPs), and relevant supervisory authorities. Additionally, information about the termination will be made publicly available to ensure that all relying parties are informed.

Authorizations granted to subcontractors acting on Simplifi's behalf will be revoked prior to the termination of services.

Where applicable, Simplifi will transfer its obligations to a trusted third party responsible for maintaining essential records—such as revocation data and PKI infrastructure certificates—for a reasonable period. If no records are retained, Simplifi will provide a formal justification.

Before terminating services, all private keys, including backup copies, will be securely destroyed or deactivated to ensure they cannot be recovered or misused.

When feasible, Simplifi will arrange for the migration of active trust services to another qualified TSP to maintain continuity for existing customers.

Financial safeguards are in place to cover all termination-related obligations, including in the event of insolvency or bankruptcy.

Finally, Simplifi will either continue to maintain or transfer to a reliable entity its responsibility for ensuring that its public keys and trust service tokens remain accessible to relying parties for an appropriate duration following service termination.

6. Technical security controls

This chapter describes practices derived from ETSI EN 319 411-1, ETSI EN 319 411-2, and ETSI EN 319 421. The requirements comprehensively cover the description of technical security controls, including primarily:

- The management and protection of cryptographic material (private key generation, dissemination, activation, deletion etc.).

Separate trust service policies provide practices implemented by Simplifi for each trust service.

- IT security management and the lifecycle of security mechanisms.

Common to all services practices are specified in the following subchapters, starting from chapter 6.4

6.1. Key Pair Generation and Installation

The approach to this item is outlined in specific trust service policies, available publicly in the repository referred to in Chapter 2.1

6.2. Private Key Protection and Cryptographic Module Engineering

The approach to this item is outlined in specific trust service policies, available publicly in the repository referred to in Chapter 2.1

6.3. Activation Data

The approach to this item is outlined in specific trust service policies, available publicly in the repository referred to in Chapter 2.1

6.4. Computer security controls

6.4.1. Specific computer security technical

Simplifi ensures that the components of the Trust Service Provider (TSP) system are securely operated and managed with an acceptable level of risk.

Security functions are delivered by the operating system, or through a combination of system software, applications, and physical safeguards.

The TSP's infrastructure includes the following security mechanisms:

- Enforces authenticated logins for all users in trusted roles.
- Applies access controls based on the principle of least privilege.
- Requires strong password policies to prevent unauthorized access.
- Implements multi-factor authentication for enhanced identity verification.
- Uses cryptographic protocols to secure session communications.
- Provides continuous IT system monitoring and alerting mechanisms.
- Maintains security audit capabilities for tracking system activity.
- Implements protections against malicious code, including detection and prevention controls
- Ensures software and firmware integrity is maintained and systems are regularly updated.
- Applies a clean-desk policy and enforces automatic screen locking or session timeout mechanisms.

Access to the server system is always performed under the supervision of an administrator and exclusively through encrypted connections.

6.4.2. Computer security rating

Not applicable.

6.5. Life cycle security controls

The security controls are evaluated by various methods, such as: risk assessment, penetration tests or internal audits.

6.5.1. System development controls

Security requirements analysis is performed during the design and requirements specification stage of every system development project undertaken by Simplifi.

Before any production deployment, acceptance testing is conducted in a non-production environment, followed by formal approval to ensure compliance and readiness.

For cryptographic modules, Simplifi exclusively uses certified products that meet established technical standards (ETSI/CEN). Simplifi does not define its requirements in this regard.

6.5.2. Security management controls

Security controls are implemented within the information security policy of Simplifi.

Current configurations and changes of Simplifi systems are documented according to change management procedures.

6.5.3. Life cycle security controls

The security controls are evaluated by various methods, such as: risk assessment, penetration tests or internal audits.

6.6. Network security controls

Simplifi ensures the following network security controls:

- Network segmentation
    - High security zone with no direct Internet access (Root CA)
    - High security zone with dedicated network with isolated network access (HSM, RQSCD)
    - Normal security zone with controlled Internet Access
- Access control
    - Restricted physical and logical access to network devices

    - Secure Internet communication through VPN tunnels to protect data transmission
- Hardening
    - Configuration hardening through the deactivation of unnecessary ports and services to minimize attack surfaces
- Monitoring
    - Implementation of firewalls to control incoming and outgoing network traffic
    - NOC team (data center level) is responsible for monitoring 24/7 and detection any abnormal events
- Configuration audits
    - Regular internal audits of network configurations to ensure compliance with security policies and best practices.
- Network separation
    - Separation of administrative network from operational activities to isolate critical functions (separate subnets)
    - Clear separation between production and non-production environment
- Regular vulnerability scan of network infrastructure (at least quarterly)
- Deployment of anti-virus protection to detect and prevent malware infection across network endpoints (workstations).

6.7. Time synchronization

All trust services components are regularly synchronized with a reliable time service. Simplifi uses NTP protocol from GPS sources (STRATUM 1) to establish the correct time for:

- Initial validity time of a CA Certificate.
- Revocation of a CA Certificate.
- Posting of CRL updates.
- Issuance of Subject end entity Certificates.

Clock adjustments are auditable events.

7. Certificate and CRL Profiles

Separate trust service policies provide profiles for certificates. Certificate profiles align with the following standards:

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

Their structure is outlined in a specific trust service policies, available publicly in the repository referred to in Chapter 2.1.

8. Compliance Audit and Other Assessment

Trust services provided by Simplifi are audited for compliance with the:

- eIDAS regulation
- practices outlined in this document
- particularly with Romanian Law.

Audit results are included in management reporting and serve to demonstrate compliance and support service improvement.

8.1. Frequency or circumstances of assessment

A Conformity Assessment Body (CAB) evaluates the compliance of Simplifi's information systems, policies, operational practices, facilities, personnel, and assets in accordance with Romanian law, the eIDAS Regulation, and applicable ETSI standards.

These assessments are conducted at least every two years or whenever a significant change occurs in Trust Service operations.

In addition, Simplifi has designated a system auditor responsible for carrying out internal reviews and audits as defined in its internal audit program.

8.2. Qualification of auditors

External audits are conducted by a Conformity Assessment Body (CAB) accredited according to ISO/IEC 17065, as outlined by ETSI EN 319 403, with a focus on meeting the requirements specified in the eIDAS Regulation (EU) No 910/2014. The CAB is authorized to perform conformity assessments of Qualified Trust Service Providers and their services.

The internal audit is performed by Simplifi employees or third parties with the necessary experience and qualification related to public key infrastructures, secure operation of information technology systems and information security in general.

8.3. Auditor's relationship with Simplifi

Simplifi has chosen an CAB auditor who is entirely independent from the organization.

8.4. Audit scope

The CAB audits all parts of the information system used to provide Trust Services.

The Conformity Assessment Body (CAB) performs a comprehensive audit of all components of the information system used by Simplifi to deliver Trust Services.

This external audit covers the full scope of Simplifi's operations related to qualified certification services, in compliance with Romanian law and Regulation (EU) No. 910/2014, taking into account all relevant standards and standardization documents. The assessment includes the following areas:

- Documentation;
- Archives;
- Data related to the issuance and management of qualified certificates;
- Physical and information security, as well as the reliability of the technological systems and organizational management.;

In parallel, internal audits focus on the following areas:

- Evaluation of the Trust Service Provider’s operations for conformity with the Trust Service Policies and the Practice Statement;
- Verification of how documented practices and procedures are applied in actual operations;
- Review of processes carried out by the Registration Authority;

8.5. Actions taken as a result of deficiency

Internal and external audit reports are delivered to the Board of Directors for review.

If the Conformity Assessment Body (CAB) identifies deviations or non-compliance issues, the Supervisory Body mandates that Simplifi correct these within a specified timeframe.

Simplifi is committed to achieving full compliance and timely correction of non-conformities.

8.6. Communication of results

The results of the performed internal and external audits are not published.

The certification document received by the Conformity Assessment Body may be published on Simplifi’s website.

9. Other business and legal matters

9.1. Fees

The list of services provided by Simplifi and the corresponding fees are published on the official website *https://www.simplifi.ro*. Payment may be made by bank transfer, bank card, or other legally accepted means, in accordance with Romanian regulations.

9.1.1. Revocation or Status Information Access Fees

Access to certificate revocation services (CRL) and certificate status verification via OCSP is provided free of charge for all subscribers and relying parties. Simplifi reserves the right to establish fees for advanced or high-volume access to status verification systems if necessary.

9.1.2. Fees for other services

Simplifi may charge fees for additional trust service-related activities, including but not limited to:

- Key pair generation for Subscribers or internal use;
- Evaluation or testing of third-party applications for compatibility;
- Licensing of tools, components, or APIs;
- Custom integration, installation, or professional services;
- Copies of policies, manuals, or internal guides (when not publicly available);
- Training sessions for partners or enterprise clients.

9.1.3. Refund policy

Simplifi's refund policy is published on its website. In the event a refund is granted, the Subscriber must request revocation of any associated certificate(s) before a refund can be processed.

9.2. Financial Responsibility

Simplifi maintains insurance coverage and internal safeguards to cover liabilities that may arise from the operation of its qualified trust services. In accordance with eIDAS Article 24(2)(e), Simplifi is insured for damages caused by non-compliance with trust service obligations, up to the limit required by national and EU legislation.

9.3. Confidentiality of Business Information

Simplifi treats as confidential all business, technical, and operational information that is not intended for public disclosure. Confidential information includes, but is not limited to:

- Subscriber data not present in certificates;
- Contracts, communications, and correspondence;
- Operational and audit logs;
- Internal security policies and recovery plans;
- System designs, configurations, and administrative procedures.

Disclosure of such information is permitted only:

- With the explicit written consent of the affected party;
- When required by applicable law or a legally binding court order;

- When disclosure is necessary for the execution of services by authorized subcontractors under confidentiality obligations.

9.4. Protection of Personal Information

Simplifi processes personal data in full compliance with:

- **Regulation (EU) 2016/679 (GDPR)**;
- **Regulation (EU) 910/2014 (eIDAS)**;
- Applicable Romanian legislation and ANSPDCP guidance.

Simplifi acts as a data controller and processes personal data strictly for the purpose of delivering trust services. This includes identity verification, certificate issuance, key lifecycle management, and associated legal recordkeeping.

Appropriate **technical and organizational measures** are implemented to ensure:

- Data minimization and purpose limitation;
- Confidentiality and integrity during transmission and storage;
- Secure disposal or archiving of data when no longer required.

Subjects are informed of the use of their personal data prior to certificate issuance and must give informed consent where required. Refusal to consent to the processing of required data may result in denial of the service.

Disclosure of personal data may only occur in the following cases:

- To legally authorized authorities under valid legal request;
- To auditors or subcontractors bound by confidentiality agreements;
- With explicit subject consent for specific use cases (e.g., mailing address forwarding, certificate publication).

9.5. Intellectual Property Rights

All trademarks, software, documentation, and cryptographic material developed or owned by Simplifi remain its intellectual property. Use, reproduction, or redistribution of such material is prohibited without prior written authorization. Certificates and key pairs issued to individuals are considered the property of the Subscriber or Subject unless stated otherwise in the certificate or agreement.

9.6. Responsabilities and Warranties

9.6.1. Certification Authorities

Simplifi CAs ensure that all certificates conform to the X.509 v3 standard and the applicable Certificate Policy. CA procedures are executed in accordance with this CPS and applicable CPs.

9.6.2. Registration Authorities

RAs acting under Simplifi's domain must comply with all internal procedures, applicable CPs, and this CPS. Their responsibilities include accurate identity verification, request validation, and secure handling of registration data.

9.6.3. Subscribers/Subjects

Subscribers and Subjects must:

- Review and accept the applicable Terms and Conditions;
- Protect their credentials to activate private key
- Request immediate revocation if the key is compromised or misused;
- Ensure the information provided for certification is accurate.

9.6.4. Relying Parties

Relying Parties are responsible for:

- Verifying the authenticity and validity of certificates before trust decisions;
- Checking the certification path, revocation status (via CRL/OCSP), and policy OIDs;
- Ensuring that the certificate is appropriate for the intended use;
- Using secure and reliable software and devices for validation.

9.7. Limitations of Liability

Simplifi shall not be liable for damages resulting from:

- Force majeure or unforeseen circumstances;
- Subscriber negligence in protecting private keys or credentials;
- Use of certificates beyond their intended purpose;
- Use of revoked or expired certificates;
- Inaccurate data provided by the Subscriber, if declared as correct.

9.8. Indemnities

Simplifi assumes no responsibility for improper use of its services by third parties, nor for relying parties who fail to follow certificate validation best practices.

9.9. Term and Termination

This CPS remains in effect until replaced or withdrawn by Simplifi. Updated versions are published on Simplifi's official Repository and take effect upon publication, unless otherwise stated.

9.10. Individual Notices and Communications

Notices and legally required communications may be delivered via:

- Registered mail;
- Express courier;
- Electronic mail (digitally signed if required);
- Secure platform messaging, where applicable.

9.11. Dispute Resolution

Disputes will first be addressed amicably between the parties. If no resolution is reached within 30 days, disputes shall be settled by the **competent Romanian courts**, with jurisdiction in **Bucharest**, unless otherwise agreed in writing.

9.12. Governing Law

Simplifi's trust services are governed by:

- **Regulation (EU) No. 910/2014 (eIDAS)**;
- **GDPR (Regulation (EU) 2016/679)**;
- Relevant Romanian legislation and decisions of the national supervisory authority.

9.13. Compliance with Applicable Law

Simplifi affirms full compliance with applicable European and national legal frameworks governing trust services. The company is accredited as a Qualified Trust Service Provider and undergoes regular audits and assessments to maintain this status.

10. Appendix

10.1. Definitions and Acronyms

auditor: person who assesses conformity to requirements as specified in given requirements documents

authentication: provision of assurance that a claimed characteristic of an entity is correct [SOURCE: ISO 27002:2022]

Certificate Policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

Certificate Revocation List (CRL): signed list indicating a set of certificates that have been revoked by the certificate issuer

certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

Certification Authority (CA): authority trusted by one or more users to create and assign certificates

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6

High security zone: specific physical location of the security zone (see ETSI EN 319 401 clause 7.8) where the Root CA key is held

incident: any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

information security breach: compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed [SOURCE: ISO 27002:2022]

Practice Statement: the current version of Practice Statement document outlining practices, procedures, and guidelines related to providing trust services. It serves as a reference for customers and stakeholders to understand how the trust service provider operates and what standards they adhere to. (present document)

revocation: permanent termination of the certificate's validity before the expiry date indicated in the certificate

risk: potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident

root CA: certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)

secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

secure zone: area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the systems used by the TSP

short-term certificate: certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the Practice Statement

subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

subordinate CA: certification authority whose Certificate is signed by the Root CA, or another Subordinate CA

subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations

trust anchor: entity that is trusted by a relying party and used for validating certificates in certification paths

Trust Service Policy (Policy): set of rules that indicates the applicability of a trust service to a particular community and/or class of application with common security requirements

Trust service provider (TSP): entity which provides one or more trust services

vulnerability: weakness of an asset or control that can be exploited by one or more threats [SOURCE: ISO 27002:2022]

EU Qualified Certificate: Qualified Certificate as specified in Regulation (EU) No 910/2014

Qualified electronic Signature/Seal Creation Device (QSCD): As specified in Regulation (EU) No 910/2014

10.2. Abbreviations

For the purposes of the present document, the following abbreviations apply:

Abbreviation	Description
CA	Certification Authority
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standard
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RQSCD	Remote QSCD
TSP	Trust Service Provider
TSA	Time Stamp Authority
UTC	Coordinated Universal Time