simplifi

PKI Disclosure Statement

Summary of Simplifi's Certification Services, Practices, and User Obligations

The PKI Disclosure Statement provides a concise and user-friendly summary of Simplifi's Certification Practice Statement (CPS). It outlines the essential terms, conditions, and responsibilities relevant to subscribers, relying parties, and other stakeholders who use Simplifi's qualified trust services.

The PKI Disclosure Statement describes, in non-technical language, the scope of services offered — including qualified electronic signatures, qualified electronic seals, and qualified timestamps — as well as the conditions for certificate issuance, usage, suspension, and revocation. It also clarifies Simplifi's liability limitations, dispute resolution mechanisms, and applicable laws.

While the PDS is not a substitute for the full CPS, it ensures that users and relying parties can easily understand their rights and obligations when using Simplifi's trust services.

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	PKI Disclosure Statement
Document OID	1.3.6.1.4.1.63578.1.1.3
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

This PKI Disclosure Statement (PDS) is published in accordance with the requirements of European standard ETSI EN 319 411-1 and describes the certification services provided by Trust Service Provider Simplifi.

This document does not replace the Practice Statement and Trust Service Policies which are available on the Simplifi website: *https://simplify.com/policies/.*

2. TSP Contact Info

SIMPLIWORKS SRL

Strada Gheorghe Titeica 142, 3rd Floor, 014192, Bucharest, Romania

Phone: +4 031 82 81 141

E-mail: easy@simplifi.ro

3. Certificate type, validation procedures and usage

3.1. Certificate type

This section covers the electronic signature, electronic seal and electronic time stamp services provided by Simplifi.

Certificates are issued in accordance with ETSI EN 319 411-1/2 and relevant applicable standards. The terms and conditions for these services are published on the Simplifi website.

Simplifi issues:

- Qualified certificates to natural person for advanced or qualified electronic signature
- Qualified certificates to natural person representing legal person for qualified
- Qualified certificates for electronic seals
- Certificates for electronic timestamp services

Certificates are Qualified certificates and are issued and stored on a Qualified Signature/Seal Creation Device or Secure Signature Creation Device.

Simplifi maintains its own Time Stamp Authority (TSA) that issues TSA CA certificates used to certify Simplifi Time Stamp Units responsible for issuing time-stamping tokens.

3.2. Validation procedures

Qualified certificates are issued to individuals after they have undergone an identity verification procedure in accordance with ETSI EN 319 411-1 and ETSI EN 319 411-2 standards.

The following documents are accepted as valid proof of identity:

- ID card
- Passport

3.2.1. Identity verification by authorized representative of Simplifi

The subject's identity can be verified using one of the following two methods:

- in-person verification via Registration Point;
- remotely through electronic identifications means recognized and accepted by Simplifi

3.3. Usage

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

Simplifi issues certificates for qualified electronic signatures to ensure their legal validity. A qualified electronic signature has the same legal validity as a handwritten signature and is uniquely linked to the signatory.

Simplifi issues electronic timestamp tokens that are legally recognized as certified dates. These timestamps are mainly used to provide a reliable time reference for long-term

qualified electronic signatures, although they can also be used in any situation requiring a reliable time stamp.

Simplifi issues qualified certificates for electronic seals, which are used to authenticate electronic documents and confirm their integrity and origin, ensuring that the content remains unchanged from the moment of sealing.

4. Reliance limits

The use of each certificate is strictly limited to the purposes specified in the key usage extensions and extended key usage extensions, where applicable, as specified in the certificate metadata.

All audit-related data, including registration data processed TSP, are archived for a period of seven years after the expiry of the relevant certificate.

5. Subscriber and subject obligations

By applying for a certificate and accepting the relevant terms and conditions, the subscriber/subject agrees to comply with the Trust Services Policy, Practice Statement and terms of provision of trust services published by Simplifi.

The Subject and Subscriber are required to:

- Comply with all terms and conditions applicable to Simplifi trust services.
- Provide truthful and accurate data during the registration process.
- Immediately notify Simplifi if there are any issues, changes, or errors with their certificate.
- Ensure the confidentiality, integrity and exclusive use of credentials used for signature creation, preventing any unauthorized access or disclosure of information.
- Stop using revoked or expired certificates.
- Suspend the use of trust services if there are any indications that the Simplifi system has been compromised.
- Immediately request a revocation in the event of actual or suspected compromise of private keys.

6. Certificate status checking obligations on relying parties

Relying parties on information from certificates issued by Simplifi are responsible for confirming that such certificates have not been revoked.

Verification can be performed by viewing the certificate revocation list (CRL) available at the specified certificate URL or through the OCSP (Online Certificate Status Protocol) service.

Relying parties concerned are responsible for the following checks:

- validity of certificate;
- validity of the chain of certificates, up to the root certificate;
- revocation status of the certificate;
- limitations on any use of the certificate;

Relying parties are obliged to protect any personal information of the subject included in the certificate.

7. Limitation of liability

Simplifi is not liable for the conduct of third parties, subscribers or any individuals or organizations not under its direct control.

Simplifi shall not be liable for:

- losses or damage caused by Subject's failure to maintain the confidentiality of private key
- incorrect or improper verification of certificates by Relying parties
- Inability to fulfil obligations due to technical failures or security breaches related to the Supervisory Authority, Trusted List or other public authorities.
- Any event, according to Practice Statement, that is causes by by Force Majeure

8. Applicable Agreements

8.1. Terms and conditions

All services offered by Simplifi are governed by the applicable Terms and Conditions, which are available on the following website: *https://simplify.com/policies/*.

8.2. Practice Statement and Trust Service Policy

The current and historical versions of the document are published on the following website: *https://simplify.com/policies/*.

9. Privacy Policy

Privacy policy is available on the following website: *https://simplify.com/policies/.*

10.Refund Policy

Subscribers have the right to request fee refund only if Simplifi fails to fulfil its duties and obligations under the terms of provision of trust services, Trust Services Policy, Practice Statement and this document.

11.Applicable Law

Simplifi is a legal entity in Romania. Simplifi is regulated by Romanian Law.

12.Licenses, trademarks and audits

Simplifi operates under valid licenses and in compliance with all applicable legal and regulatory frameworks.

The company does not verify the use of registered trademarks but reserves the right to refuse to issue a certificate or seek its revocation in the event of a dispute.

In accordance with Article 20 of the eIDAS Regulation, independent audits are conducted at least once a year to confirm compliance with both procedural rules and legal obligations.

13.Identification of this document

The document has been registered within Simplifi and has following OID: 1.3.6.1.4.1.63578.1.1.3