



Qualified Root CA Certificate Profile

Profiles and parameters for the Root CA Certificate

This document defines the qualified certificate profiles used by Simplifi as a Qualified Trust Service Provider (QTSP). It covers the structure and parameters for the Root CA certificate.

Document information

Version	1.0
Version Date	September 1st, 2025
Approved by	CEO
Owner of the Document	Trust Service Manager
Document Name	Qualified Root CA Certificate Profile
Document OID	1.3.6.1.4.1.63578.1.5.3
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	CEO

Distribution history

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

Contents

Document information	2
Document history	2
Approval history	2
Distribution history	2
1. Introduction	4
2. Technical profile of certificate	4
3. Certificate body	4
3.1. Root CA Certificate.....	4
3.2. CRL Profile.....	5

1. Introduction

The document describes profile for certificates for the Root CA certificate and the associated CRL profile.

2. Technical profile of certificate

Certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280, ETSI EN 319 412-2 and ETSI EN 319 411-2

3. Certificate body

3.1. Root CA Certificate

Root CA Certificate Profile			
Field	Mandatory	Value	Description
Certificate data			
Serial number	Yes	<unique_serial_number>	Unique serial number of the certificate.
Version	Yes	3	
Signature Algorithm	Yes	SHA512	Signature algorithm in accordance to RFC 5280.
Issuer DN			
Common Name (CN)	Yes	Simplifi Root CA G1	Certificate authority name
Organization (O)	Yes	SIMPLIWORKS SRL	Organization name
		VATRO-45938180	Identification of the organization different from the organization name.
Organization Identifier (ORGID)	Yes		Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Country (C)	Yes	RO	Country code: AM – Romania (2 character ISO 3166 country code)
Subject DN			
Common Name (CN)	Yes	Simplifi Root CA G1	Certificate authority name
Organization (O)	Yes	SIMPLIWORKS SRL	Organization name

		VATRO-45938180	Identification of the organization different from the organization name.
Organization Identifier (ORGID)	Yes		Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)
Validity			
Validity period	Yes	20 years	Validity period of certificate from issuance date.
Not before	Yes	<issuance_date_and_time>	First date of certificate validity.
Not After	Yes	<issuance_date_and_time> + 20 years	Last date of certificate validity.
Public key info			
Algorithm	Yes	RSA (4096 Bits)	RSA algorithm in accordance with RFC 4055
Public Key	Yes	<public_key>	Public Key.
Extensions			
Extensions	Values and limitations	Criticality	Mandatory
Key Usage	keyCertSign, keyCrlSign	Critical	Yes
Basic Constraints	Subject Type = CA Path Length Constraint = None	Critical	Yes
Subject Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes

3.2. CRL Profile

CRL			
Field	Mandatory	Value	Description
CRL data			
Version	Yes	2	CRL format version pursuant to X.509.
Signature Algorithm	Yes	SHA512	Signature algorithm in

			accordance to RFC 5280.
Expire Period	Yes	1 year	Time interval during which CRL is valid.
Issue Interval	Yes	1 year	Time interval during which CRL is generated and published
Overlap Time	Yes	7 days	Time interval during which both old and new CRLs are valid.
Issuer DN			
Common Name (CN)	Yes	Simplifi Root CA G1	Certificate authority name
Organization (O)	Yes	SIMPLIWORKS SRL	Organization name
Organization Identifier (ORGID)	Yes	VATRO-45938180	Identification of the organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5.1.4 of ETSI EN 319 412-1.
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)
Extensions			
Extensions	Values and limitations	Criticality	Mandatory
Authority Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
CRL Number	Digit starts from number 1	Non-critical	Yes
ExpiredCertsOnCRL	Yes	Non-critical	Yes