IDeTRUST®

Reference: IDeTRUST-PKI-DSCA-CPS-2025
Date: 2025/12/01

Entity legal name: IDeTRUST GmbH – Germany

Certification Practice Statement (CPS) for IDeTRUST ISO/IEC 20248 Root CA
OID: 1.3.6.1.4.1.59938.0.1
(Editor's note: This OID is assigned under the IDeTRUST enterprise arc. The arc 1.3.6.1.4.1.59938.0 is used for IDeTRUST policies for ISO/IEC 20248-based PKI operations.)
Version 1.0 (Current-State)

Effective Date: 2024-12-02

IDeTRUST DigSig PKI Documentation Set

This master index provides access to all certification governance documents maintained by IDeTRUST GmbH for its ISO/IEC 20248-based Public Key Infrastructure (PKI):

- Root CA CPS (DSCA CPS) – This document
- Domain Authority CPS (DSDA CPS) – Certification rules for entities authorized to issue DigSig Certificates and DigSigs
- DigSig Certificate Generation Practice Statement (DSG PS) –Statement governing secure DigSig generation

1 Introduction

1.1 Overview

This Certification Practice Statement (CPS) defines the practices employed by IDeTRUST GmbH in its role as the Root Certification Authority (Root CA) for the IDeTRUST PKI. This PKI exclusively supports ISO/IEC 20248 digital signatures ("DigSigs") and operates on a purpose-specific model distinct from classical TLS or web-based PKIs. The IDeTRUST PKI is closer in architecture to S/MIME, eSeal, and IoT data-signing models.

A DigSig (ISO/IEC 20248) is a verifiable item identifier used in manufacturing, logistics, and document contexts. In addition to the core identifier, a DigSig may include item attributes—often also used for verification purposes. These may describe physical or contextual aspects of the item, such as weight, expiry date, or permitted use. For example, a product DigSig might include an expiry date, while a camping permit DigSig could include the date and campsite.

1.2 PKI Participants

Note: This PKI does not include intermediate CAs. The Root CA issues certificates directly to Domain Authorities. This structure is closer to S/MIME, eSeal, and IoT PKIs than traditional TLS hierarchies.

- Root CA (Trust Anchor): IDeTRUST GmbH
- Domain Authorities (DAs): Entities certified by the Root to issue and operate DigSig Certificates. DAs are CA:TRUE and operate within a defined DAID namespace.
- DigSig Certificates: Operational certificates issued and held by Domain Authorities. A DigSig Certificate certifies a DigSig Data Description (DDD) issued by the Domain Authority as per ISO/IEC 20248.

- DigSig EncoderGenerators: Systems used by Domain Authorities to encode and generate a DigSig as specified with the certified DDD as per ISO/IEC 20248.
- DigSig Verifiers: Systems used by Domain Authorities and independent entities that decode and verify ISO/IEC 20248 DigSigs.

1.3 Certificate Usage

Root CA certificates are used solely to issue Domain Authority certificates. Domain Authorities are authorized to issue and operate DigSig Certificates for DigSig generation. The Root does not issue or manage end-entity certificates in the classical sense.

1.4 Policy Administration

- CPS Maintainer: IDeTRUST GmbH
- Contact: info@idetrust.com
- Repository: https://idetrust.com

2 Publication and Repository Responsibilities

2.1 Repositories

All certificates, CRLs, and policy documents are published at: https://idetrust.com

2.2 Publication of CA Information

The following are published:

- Root CA certificate
- Domain Authority certificates
- CRLs (if applicable)
- This CPS

2.3 Frequency of Publication

- Certificates: upon issuance
- CPS: upon update
- CRLs: not currently issued; reserved for future use

2.4 Access Controls on Repositories

Publicly accessible and read-only.

3 Identification and Authentication

3.1 Naming

- Distinguished Names follow RFC 5280 and ISO/IEC 20248 naming conventions.
- CN for Domain Authorities includes the DAID as per ISO/IEC 15459.

3.2 Initial Identity Validation

- Domain Authorities are manually verified to have a current ISO/IEC 15459 CIN assigned by a current ISO/IEC 15459 Issuing Agent (IAC).
- Domain Authorities are manually verified as legal entities.
- DA must provide a public website and DAID registration proof.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Certificate request is made during the annual key ceremony.

4.2 Certificate Issuance

Issued only after validation of DA identity and public key.

4.3 Certificate Acceptance

Acceptance occurs via physical key ceremony record.

4.4 Certificate Suspension and Revocation

Not supported at Root level; DA-level revocation supported via DigSig time-bound selective revocation.

4.5 Certificate Renewal and Re-key

No re-keying. A new certificate is issued annually.

4.6 Certificate Status Services

- Root certificate is hardcoded in verifiers.
- DA status available via HTTPS.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

Root key material is stored in offline, air-gapped hardware. Access limited to authorized personnel.

5.2 Procedural Controls

- Dual control required for all key ceremonies
- Annual key ceremonies are conducted in November–December, during which Domain Authority keys are generated and certified for the upcoming calendar year

5.3 Personnel Controls

- Background-checked staff
- Confidentiality agreements
- Segregation of duties

6 Technical Security Controls

6.1 Key Pair Generation and Installation

- Root CA keypair is generated on a dedicated, air-gapped Linux system (without graphical interface), used solely for Domain Authority certification.
- The private key is encrypted and secured using a multi-person access control method (four-eyes principle).
- Root and Domain Authority certificates use RSA 4096 with SHA-512.

  Note: The Root CA actively monitors developments in cryptographic best practices. Future upgrades to post-quantum cryptography (e.g., hybrid schemes or quantum-resistant algorithms) will be considered in alignment with evolving international standards and threat models.

- Keys expire automatically at year-end; renewal is performed manually via key ceremony.

6.2 Private Key Protection

- Stored offline
- Encrypted with multi-person access control

6.3 Other Aspects of Key Management

- Root certificate validity is 21 years to ensure DigSigs can remain valid for 20 years after issuance
- No backup of Root private key; regeneration only via new Root

6.4 Activation Data

Not applicable. The Root CA private key is stored offline and accessed only during key ceremonies under four-eyes control. No activation data (e.g., PINs or tokens) is used.

6.5 Computer Security Controls

Signing occurs in air-gapped system with write-only outputs

6.6 Life Cycle Technical Controls

Change control processes documented; all changes approved by policy board

7 Certificate, CRL, and OCSP Profiles

- Root CA and Domain Authority certificates conform to X.509v3.
- Certificate profiles include:
  - BasicConstraints: CA:TRUE
  - KeyUsage: keyCertSign, cRLSign
  - Subject fields include DAID and URI
  - Custom extensions for ISO/IEC 20248 metadata (OID 1.0.20248.1.x)
- No CRLs or OCSP for Root at this stage.

8 Compliance Audit and Other Assessments

- Currently self-audited by IDeTRUST annually.

- Target-state: External audit for eIDAS/QTSP compliance by a qualified conformity assessment body.

9 Other Business and Legal Matters

- Certificates are issued to legal entities assuming accountability.
- Root CA is not liable for misuse by certified DAs unless caused by negligence or breach of CPS.
- Dispute resolution follows German law.
- CPS may be updated with 30 days public notice.

Annex A – Crosswalk to RFC 3647 and ETSI EN 319 401

Section	RFC 3647	ETSI EN 319 401 Equivalent
CPS Structure	RFC 3647 full profile	Policy & Security Requirements (cl. 6–8)
Trust Service Model	Section 1.3–1.4	Clause 5
Entity Identification	Section 3.2	Clause 6.3.2
Certificate Lifecycle	Sections 4–6	Clause 6.3.3–6.3.5
Technical Security Controls	Section 6	Clause 6.4

Note: This CPS follows RFC 3647 structure for modularity and alignment with IETF practice. The table above shows interoperability with ETSI EN 319 401 requirements to support future eIDAS compliance.

Annex B – Definitions and Acronyms

- CA – Certification Authority
- CPS – Certification Practice Statement
- DA – Domain Authority
- DAID – Domain Authority Identifier (from ISO/IEC 15459)
- DDD – DigSig Data Description (the data schema)
- DigSig – Digitally signed data structure conforming to ISO/IEC 20248
- DSCA – DigSig Root Certification Authority
- DSDA – DigSig Domain Authority
- DSGPS – DigSig Certificate Generation Practice Statement
- HSM – Hardware Security Module
- OCSP – Online Certificate Status Protocol
- OID – Object Identifier
- PKI – Public Key Infrastructure
- QSCD – Qualified Signature/Seal Creation Device
- QTSP – Qualified Trust Service Provider
- RFC 3647 – IETF standard for Certificate Policy and CPS frameworks