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

Entity legal name: IDeTRUST GmbH – Germany

Certification Practice Statement (CPS) for ISO/IEC 20248 Domain Authority certification
OID: 1.3.6.1.4.1.59938.0.2
(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) – Rules for the Root CA
- Domain Authority CPS (DSDA CPS) – This document
- DigSig Certificate Generation Practice Statement (DSG PS) – Statement governing secure DigSig generation

---

1 Introduction

1.1 Overview

This Certification Practice Statement defines the policies and procedures followed by the IDeTRUST Root CA when certifying DigSig Domain Authorities (DSDAs). These DAs are entrusted with certifying DigSig Data Descriptions (DigSigs Certificate) with the associated public key, and generating DigSigs as specified under ISO/IEC 20248.

DigSig Domain Authorities (DAs) are legal entities authorized by the Root CA to issue DigSig Certificates and generate ISO/IEC 20248-compliant DigSigs. In the context of eIDAS, these signatures are classified as advanced electronic seals (eSeals). A DA operates within its own defined domain of accountability, using an assigned Domain Authority Identifier (DAID) derived from its valid assigned ISO/IEC 15459 IAC-CIN.

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 Scope

This CPS applies to:

- The Root CA's procedures for certifying DAs
- The compliance requirements a DA must meet
- The trust and accountability framework for issuing DigSig Certificates and generating DigSigs

1.3 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.

1.4 Certificate Usage

The DA is an X.509 PKI end-entity. DA certificates are used solely to issue the following eSeals within the domain of DA operations: ISO/IEC 20248 DigSig Certificates and DigSigs.

1.5 Terminology and Conventions

See Annex B for definitions.

1.6 Policy Administration

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

2 DSDA Certification Requirements

DAs certified by IDeTRUST must meet the following baseline requirements:

- Be a legally registered entity capable of assuming accountability
- Maintain an active HTTPS website publishing entity details
- Possess a valid IAC-CIN combination under ISO/IEC 15459, establishing the DAID
- Host or delegate a public HTTPS WebAPI for serving:
  - DigSig Certificates
  - Revocation information (if applicable)

3 Identification and Authentication

- DAs must provide proof of legal identity and control over their DAID
- Validation is manual and requires:
  - Certificate request with public key
  - Public disclosure of entity and DAID

4 Certificate Lifecycle Requirements

- Certificates issued by the Root to the DA are valid for one calendar year
- DAs must participate in an annual key ceremony
- New keys and certificates must be generated yearly

5 Technical and Security Controls

- DA certificates use RSA 4096 + SHA-512
- DA may use other algorithms (e.g., ECC FP256BN + SHA-256) for DigSig Certificates, aligned with ISO/IEC 20248
- All keys must be generated and stored securely, either in HSMs or isolated signing environments

6 Policy for DigSig Certificate and DigSig Generation

A DA may only issue DigSig Certificates and DigSigs for which it can assume legal accountability.

- This domain of accountability shall be made transparent via a public “DigSig Best Practice Statement”

  See Annex A for an example format

7 Revocation and Termination

- DAs must implement timestamp-based selective revocation as per ISO/IEC 20248
- Optionally, additional revocation status can be served via CRL or OCSP endpoints

8 Trust Framework and Interoperability

- DAs may be cross-certified by government or eIDAS-qualified roots
- DAs may rely on a dual-certification model where both IDeTRUST and a national PKI certify the same entity

9 Legal and Policy Framework

- DAs must accept liability for their issued DigSig Certificates and DigSigs
- The DSDA CPS may be updated with 30 days’ public notice

Annex A – Sample DigSig Best Practice Statement

In addition to the DigSig Certificate Generation Practice Statement:

- Identifies the entity and its DAID (IAC-CIN)
- Declares its domain of accountability and scope of liability
- Provide the practice/process statement for DDD certification
- Provide the practice/process statement for DigSig Generation
- Provide the practice/process statement for DigSig revocation as per ISO/IEC 20248

Annex B – Definitions and Acronyms

- CA – Certification Authority
- CIN – ISO/IEC 15459 Company Identification Number
- 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
- IAC – ISO/IEC 15459 CIN Issuing Agent
- 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