Reference: IDeTRUST-PKI-DSG-PS-2025
Date: 2025/12/01

Entity legal name: IDeTRUST GmbH – Germany

DigSig Generation Practice Statement (DSG PS)
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) – Certification rules for entities authorized to issue DigSig Certificates and DigSigs
- DigSig Certificate Generation Practice Statement (DSG PS) – This document

---

1 Introduction

This document defines the practices and procedures for the generation of DigSigs under ISO/IEC 20248 by a certified Domain Authority (DA). It covers both the certification and publication of DigSig Data Descriptions (DDD) and the secure generation of DigSigs using certified DigSig Certificates.

This document is structured in alignment with RFC 3647 and complements the DSCA CPS and DSDA CPS. *A*

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.

2 Practice Administration

This DSG PS shall be reviewed annually in conjunction with the key ceremony and update cycle.

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

3 DigSig Generation Lifecycle

The DA must follow these steps as defined in ISO/IEC 20248:

1. **Determine the Use Case**: Define the scope and application of the DigSig (e.g., vehicle ID, permit, label).
2. **Develop the DDD**: Specify the structured format and fields to be signed.

3. **Generate the Key Pair**: Create the ECC key pair for signing (typically FP256BN + SHA-256).
   - To prevent operational disruptions, the following year's DDDs should be certified with new keys and published in advance.
   - Even if the DDD remains unchanged, a new key pair shall be used for the new signing period.
4. **Select a CID**: Assign a unique DigSig Certificate ID (CID) as per ISO/IEC 20248.
5. **Certify the DDD**: Bind the DDD to the key via a DigSig Certificate signed using the DA certificate.
6. **Publish the Certificate**: Make the DigSig Certificate available to:
   - Authorised DigSig Generators
   - The DA's official DigSig Repository (WebAPI)
7. **Generate DigSigs**: Produce DigSigs using the certified DDD and key.

4 Handling DDD Updates

DDD updates involved two classes of changes:

- Changes to signed data or encoding: The DDD shall be certify anew.
  - A new CID shall be assigned.
  - A new key pair shall be generated.
  - The DDD shall be certified and published as a new DigSig Certificate.
- No change to signed data or encoding, i.e. the descriptions of the DigSigs and the fields of the DigSig.
  - The updated DDD may be recertified using the existing key pair.

The signing period for any given DDD is one calendar year.

5 DigSig Generator Requirements

All DigSig Generators shall implement the DigSig Encoder Generator Interface (DSEG) defined in Annex D of ISO/IEC 20248.

5.1 Implementations

IDeTRUST provides three validated implementations:

1. **SaaS-Based Generator (IDeSIGNER Cloud)**
   - Hosted and secured online
   - One secure encapsulation per DDD
   - Communicates via encrypted API channel
2. **Hardware-Based Generator**
   - Dedicated device with embedded DSEG-only interface
   - Status display (e.g. for verification, diagnostics)
   - Cannot be field-configured
   - May host multiple DDDs
   - Must operate within a secured, access-controlled private network
3. **Access-Controlled Manual Generator**
   - Web-based interface secured by authentication and access logging
   - Designed for low-volume, high-trust environments
   - Hosted by the DA or IDeTRUST
   - Suitable for ad hoc or special-purpose DigSig generation

5.2 Security Requirements for Hardware Devices

- Devices must reside in a physically and digitally secure environment
- Operator access and provisioning must be vetted
- DDD private keys are generated and stored exclusively within the TPM 2.0 secure element of an approved device
- Signing occurs in RAM; keys are decrypted into RAM using the device TPM
- Keys and their associated DDDs (via the DigSig Certificate) are hardware-bound and cannot be exported
- No field installation and replacement of private keys are permitted
- Replicated IDeSIGNER devices are commissioned by TPM-to-TPM duplication: DDD private keys are exported from the source device as TPM duplication blobs, encrypted under the destination device's TPM migration key and imported into the destination TPM. At no point are DDD private keys available in plaintext outside a TPM. Disk encryption is used solely to protect at-rest system data and does not affect the secrecy of DDD keys.