IDeTRUST®

Reference: IDeTRUST-PKI-DSC-2025
Date: 2025/12/01

Declaration of Self-Conformance – IDeTRUST PKI and IDeSIGNER Platform

IDeTRUST GmbH hereby issues this Declaration of Self-Conformance for the IDeTRUST Public Key Infrastructure (PKI) and the IDeSIGNER Digital Signature Generation Platform, jointly constituting the IDeTRUST environment for the issuance and verification of Advanced Electronic Seals in accordance with ISO/IEC 20248 and related standards.

IDeTRUST GmbH affirms that:

1. The IDeTRUST PKI is a two-level X.509 hierarchy consisting of an offline Root Certification Authority and a Domain Authority (DA). The DA issues ISO/IEC 20248-compliant DigSig Certificates (Data Description Certificates) as end-entity eSeal certificates.

2. The IDeSIGNER signing device generates ISO/IEC 20248 Digital Signatures (DigSigs) using FP256BN with SHA-256 via the MIRACL Core library, following Annex D and Annex J requirements of ISO/IEC 20248.

3. All Root and DA operations follow 4-eye dual-custody controls under supervised ceremonies, with strict separation of roles between the IDeTRUST Platform Manager, PKI Security Officer, and Domain Authority representative.

4. All private keys are protected with AES-256 encryption at rest, never stored in plaintext, and used only within controlled execution contexts.

5. PKI operations are performed on a hardened AWS-hosted platform relying on AWS's publicly declared compliance with ISO/IEC 27001, 27017, 27018, 27701, ISO 9001, SOC 1/2/3, and FIPS 140-3 validated components where applicable.

6. All DigSig generation keys are created on the IDeSIGNER under physical security, bound to authorised signing periods, and audited at the end of each signing cycle. Revocation is executed according to ISO/IEC 20248 Annex J when required.

IDeTRUST GmbH declares conformance with the following standards and technical frameworks, directly or indirectly, as applicable to the implementation:

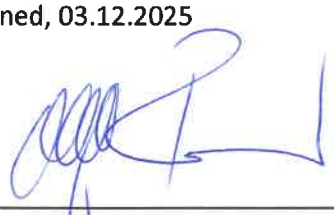
- ISO/IEC 20248 — Digital signature for item identification (DigSig)
- ISO/IEC 15459 — Unique identifiers (IAC/CIN)
- ETSI EN 319 401 — General trust service requirements
- ETSI EN 319 411-1 — Certificate profiles for non-qualified electronic seals
- ETSI EN 319 241 — Trust service policy requirements for electronic seals
- RFC 3647 — Certificate Policy and Certification Practice Statement structure
- AWS compliance declarations including ISO/IEC 27001, 27017, 27018, 27701, ISO 9001, SOC 1/2/3, and FIPS 140-3 validated modules

IDeTRUST GmbH
Managing Director: Olaf Renz
District Court Oldenburg HRB 208243
Stau 125, D-26122 Oldenburg / Germany
VAT Reg. No.: DE291553098
Phone +49 4221 59028-300
Mail info@idetrust.com

IDeTRUST®

This Declaration confirms that the IDeTRUST PKI and IDeSIGNER operate in accordance with the above standards and with the operational, cryptographic, and physical-security controls defined in the attached Self-Conformance Schedule (Annex A).

Signed, 03.12.2025



Name: Olaf Renz
Title: Managing Director
IDeTRUST GmbH

IDeTRUST GmbH
Managing Director: Olaf Renz
District Court Oldenburg HRB 208243

Stau 125, D-26122 Oldenburg / Germany
VAT Reg. No.: DE291553098

Phone +49 4221 59028-300
Mail info@idetrust.com

Annex A — Self-Conformance Schedule

1 Architectural Overview

The IDeTRUST Digital Signature System consists of two integrated components:

The IDeTRUST Public Key Infrastructure (PKI)

- Operated on a hardened, access-controlled Amazon Web Services (AWS) platform
- Contains the offline Root Certification Authority (Root CA) and the online Domain Authority (DA)
- Issues ISO/IEC 20248-compliant DigSig Certificates (Data Descriptions)

The IDeSIGNER Hardware Devices

- Sealed, TPM-anchored, physically secured signing appliances
- Generate FP256BN + SHA-256 DigSigs under the authority of certified Data Descriptions
- Operate according to ISO/IEC 20248 Annex D (key lifecycle, device interface) and Annex J (selective revocation)

Together, these two components provide an end-to-end environment for the secure creation, certification, and verification of Advanced Electronic Seals (DigSigs) for item and product identification.

2 System Description (Security & Operational Architecture)

2.1 PKI Structure

The IDeTRUST Public Key Infrastructure (PKI) is a two-level hierarchical X.509 trust structure:

1. IDeTRUST Root Certification Authority (Root CA)
   - Offline, air-gapped
   - Self-signed
   - Certifies a single Domain Authority (DA)
2. ISO/IEC 20248 Domain Authority (DA)
   - Certified directly by the Root CA
   - Issues DigSig Certificates (Data Descriptions) as end-entity certificates
   - Does not create subordinate CAs

All DigSig Certificates issued by the DA are strictly non-CA certificates, compliant with ISO/IEC 20248 eSeal structures.

2.2 Use of ISO/IEC 20248

The Domain Authority certifies its Data Descriptions (DDDs) using the X.509 profile and extension requirements mandated by ISO/IEC 20248, which define:

- DigSig metadata
- Canonical data schema
- Multilingual structures
- Verification and revocation fields

Each DDD Certificate is an Advanced Electronic Seal under the eIDAS definition and binds a trusted data model to a public key for offline verifiable signature creation.

2.3 IDeSIGNER Hardware Signing Device

The IDeSIGNER is a sealed hardware appliance used exclusively for the generation of ISO/IEC 20248 Digital Signatures (DigSigs). It is based on an OnLogic FR202 (Raspberry Pi compute module) and relies on a Trusted Platform Module (TPM) for platform identity and secure key-transport functions.

The TPM is not used to perform FP256BN+SHA-256 asymmetric operations, as this curve is not supported by TPM hardware and RSA/ECC P-curves are too large for compact barcode and RAIN RFID deployments. Instead:

- The TPM stores the platform key, used for device authentication, secure transport, and binding of ephemeral 20248 signing keys to the device.
- The device's internal storage is fully disk-encrypted.
- The operating system is executed from a RAM-disk, ensuring no persistent plaintext secrets are stored.
- All DigSig signing keys (FP256BN) are generated using the MIRACL Core library, held in user-space protected by the encrypted environment and physical security of the IDeSIGNER.

The IDeSIGNER depends on physical security, tamper-evident controls, and strict operational procedures.

2.3.1 Key Generation and Commissioning Process (ISO/IEC 20248 Annex D)

The key generation and commissioning process is manual and physically controlled:

Step 1 — Secure Pre-Commissioning

In a secure facility:

1. The IDeSIGNER is provisioned for the number of Data Descriptions (DDDs) it will serve.
2. For each DDD:
   - The device generates a new FP256BN keypair (MIRACL Core).
   - The public key is exported using the ISO/IEC 20248 Annex D interface.
3. Signing keys are retained internally and never leave the device.
4. The device remains unusable for signing until the assigned signing period begins.

Step 2 — Certification of Public Keys

1. The exported public keys are certified by the Domain Authority with the relevant DDD.
2. The certified DigSig Certificates (DDD Certificates) are pushed back to the device using the ISO/IEC 20248 Annex D protocol.

3. The signing period in each DDD Certificate is deliberately set to start after the device is shipped and installed.
   This ensures:
   – No DigSigs can be produced before the authorised period.
   – The device can generate only DigSigs within the certified validity window.

Step 3 — Time-Bound Trust Anchor

IDeTRUST uses a trust-anchor per calendar year, aligning with:

– manual commissioning,
– physical deployment cycles,
– and time-based revocation in ISO/IEC 20248 Annex J.

Each IDeSIGNER is bound to the trust anchor appropriate for its designated annual signing period.

2.3.2 Missing / Compromise Handling

Before the Signing Period Begins

If the IDeSIGNER goes missing or is suspected to be compromised before the start of its signing period:

– All DDD Certificates assigned to that device are revoked in full.

This prevents the creation of any valid DigSigs for that period.

During the Signing Period

If an IDeSIGNER goes missing or is suspected to be compromised during an authorised signing period:

– DigSigs generated after the suspected breach date are revoked.
– The revocation uses ISO/IEC 20248 Annex J (Time-Interval revocation).
– DigSigs created before the event remain valid and verifiable.

If an IDeSIGNER is misused for a deterministic period of time, i.e. because of a calling system misuse:

– Only DigSigs generated during the misuse-period date are revoked.
– The revocation uses ISO/IEC 20248 Annex J (Time-Interval revocation, and known DigSigs which resulted from the misuse).
– DigSigs created before and after this misuse-period remain valid and verifiable.

These mechanism provides:

– strict containment,
– forensic traceability,
– and minimal operational impact on legitimate historical DigSigs.

2.3.3 Summary of the Security Model

– TPM provides platform identity and secure key-transport, not signature generation.

- DigSig signing keys use FP256BN + SHA-256 in user-space (MIRACL Core), consistent with ISO/IEC 20248.
- Device storage fully encrypted; runtime executed on RAM disk.
- Keys generated only for the authorised signing period.
- Keys and DDD Certificates delivered via Annex D protocol.
- Time-bound trust anchors and Annex J revocation provide controlled lifecycle management.

2.3.4 Post-Period Return, Audit, and Revocation

At the end of its authorised signing period, the IDeSIGNER is contractually required to be returned to IDeTRUST GmbH for controlled decommissioning and audit. This requirement ensures that:

1. All DigSigs generated during the authorised period can be audited,

   - allowing reconciliation of:
   - expected DigSig counts,
   - issued identifiers,
   - DDD-specific usage, and
   - signing-period boundaries.

2. The integrity of the device and its signing keys can be examined, including:

   - verification of device state,
   - confirmation of encrypted storage intactness,
   - TPM state validation, and
   - inspection of tamper-evident seals.

3. Any discrepancies identified during audit — including suspected misuse, unexpected DigSig output, or inconsistencies with authorised DDD usage — will result in selective revocation, applied as follows:

   - DDD Certificate (DigSig Certificate) revocation, if the discrepancy affects the entire dataset or keypair;
   - Selective DigSig-level revocation under ISO/IEC 20248 Annex J, if discrepancies are restricted to a specific time interval or subset of DigSigs.

4. No new DigSigs can be created after the end of the assigned signing period, and the IDeSIGNER is not reactivated until:

   - the audit is completed,
   - the signing keys are archived or destroyed according to policy, and
   - new signing keys are generated for the next authorised period (if the device is recommissioned).

This return-and-audit requirement closes the operational lifecycle of each IDeSIGNER deployment and ensures full traceability, accountability, and compliance with ISO/IEC 20248 lifecycle controls and the IDeTRUST PKI governance rules.

2.3.5 Hardware Security Module (TPM) Specifications — Nuvoton NPCT750

The IDeSIGNER incorporates a discrete hardware Trusted Platform Module (TPM) based on the Nuvoton NPCT750 TPM 2.0 family.

The module provides the hardware root of trust, secure key storage, sealed storage for platform identity, and protected execution of TPM-bound operations.

The NPCT750 complies with the following internationally recognised security, cryptographic, and environmental standards:

1. Trusted Computing Group (TCG) Compliance

   – Fully compliant with the TCG TPM 2.0, Family “2.0”, Level 0, Revision 1.38
   (Trusted Computing Group TPM 2.0 Library Specification)

2. Common Criteria Evaluation

   – Evaluated to Common Criteria EAL4+
   under an accredited certification authority
   (NPCT7xx family, including NPCT750)

3. FIPS Cryptographic Module Validation

   – FIPS 140-2 validated cryptographic module
   (as part of the NPCT7xx TPM 2.0 hardware security device family)

4. Device & Environmental Standards

   – CE compliant (European Conformity)
   – RoHS compliant (Restriction of Hazardous Substances)
   — ensuring adherence to required environmental and electrical safety standards

5. Functional Characteristics

   – Hardware-based secure key generation
   – Protected NVRAM for key material and platform identity
   – Anti-tamper design characteristics consistent with TPM 2.0 devices
   – Support for measured boot, sealed storage, and platform attestation
   – Integrated cryptographic engine for hashing, random number generation, and integrity operations

6. Operational Use in IDeSIGNER

   – Used to establish the platform root of trust
   – Stores platform identity and binding keys
   – Secures device commissioning and Annex D key-import processes
   – Enforces that DigSig key material is bound to a physically protected device
   – Supports secure return-and-audit lifecycle procedures for each signing period

This hardware security component ensures that the IDeSIGNER has a verified, standards-aligned hardware root of trust, satisfying the expectations for government-grade signing devices under ISO/IEC 20248 deployments.

2.4 Cryptographic Tools and Algorithms (PKI)

The PKI (Root & DA) uses unmodified:

- OpenSSL 3.2.2 (4 June 2024)
  - FIPS-validated algorithms used in non-FIPS mode
  - No custom extensions
  - No third-party cryptographic modules

Algorithms:

- RSA-4096 for Root CA and DA certificates
- AES-256 password-based encryption with SHA-256 hash for key protection
- ECC FP256BN + SHA-256 for DigSig Certificates (as mandated by ISO/IEC 20248)

All private keys at rest are encrypted using AES-256.

Private keys are decrypted only in controlled memory during signing operations.

2.5 PKI Platform Security (AWS-Hosted PKI)

The IDeTRUST PKI is hosted on Amazon Web Services (AWS), which is independently certified against the following internationally recognised security and quality standards:

- ISO/IEC 27001 — Information Security Management
- ISO/IEC 27017 — Cloud Security Controls
- ISO/IEC 27018 — Protection of PII in Cloud Environments
- ISO/IEC 27701 — Privacy Information Management
- ISO 9001 — Quality Management Systems
- SOC 1, SOC 2, SOC 3 — Independent Security and Availability Audits
- FedRAMP Moderate / High — U.S. Government Cloud Security Baseline
- PCI DSS Level 1 — Payment Card Industry Security Standard
- FIPS 140-2 / 140-3 Validated Modules — Hardware-validated cryptographic components in the AWS infrastructure

These certifications confirm that AWS provides a secure, professionally audited, globally recognised hosting environment suitable for government-grade digital signature systems and Advanced Electronic Seal (eSeal) operations.

Only standard system utilities are installed:

- OpenSSL
- OpenSSH
- tmux
- Standard Linux core tools

No additional services, runtimes, or databases are used.

2.6 Access Control and Operational Security

Access to the PKI platform is controlled exclusively through:

- OpenSSH_8.7p1
- Key-based authentication
- Strict account controls with role separation

Only two permanent roles have full access to the PKI environment:

1. Platform Manager (PM)
   - Responsible for system administration, configuration, and platform security.
2. PKI Security Officer (PKI-SO)
   - Represents IDeTRUST GmbH for Root CA and DA signing actions.
   - Holds the IDeTRUST half of the dual-custody password.

A third role may be granted temporary, ceremony-only access:

3. Domain Authority Representative (DA-Rep)
   - Provides the second half of the dual-custody password for DA key ceremonies only.
   - Access is via a restricted guest login, active only for the duration of the ceremony.

For Root CA ceremonies, the second password custodian is another IDeTRUST-appointed individual, not the DA-Rep, ensuring strict separation of duties and Root governance.

Operational controls include:

- 4-eye controlled ceremonies conducted through a shared tmux 3.2a session.
- Dual-custody passwords, where:
  - The PKI-SO holds the IDeTRUST half.
  - The DA-Rep or second IDeTRUST officer holds the other half.
- No full password ever appears in plaintext, logs, terminals, or storage.
- Root CA operations are fully offline, supervised, and require two IDeTRUST custodians.
- DA operations require participation of both IDeTRUST and the Domain Authority.
- Audit trails are preserved for all signing and certificate issuance events.

This structure ensures that:

- No single individual can issue a Root or DA certificate.
- Root CA authority always remains within IDeTRUST GmbH.
- DA certification actions require cooperative participation from both trust domains.
- All access is traceable, supervised, and consistent with PKI governance and eIDAS advanced-level requirements.

3 Standards Conformance Statement

The IDeTRUST PKI and IDeSIGNER conform to the following standards, directly or indirectly:

3.1 PKI, eSeal, and Cryptographic Standards

- ISO/IEC 20248 — Digital signature for item identification
- ISO/IEC 15459 — Unique identifiers (IAC/CIN structure)
- RFC 3647 — Certificate Policy / Certification Practice Statement framework
- ETSI EN 319 401 — General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 — Certificate Profiles (non-qualified, advanced eSeal)
- ETSI EN 319 421 — Policy and security requirements for remote signature creation
- ETSI EN 319 241 — eSeal and trust service provider guidance (non-qualified)

Note: The PKI asserts conformance at the Advanced Electronic Seal level, not Qualified.

3.2 Cryptographic Module Trustworthiness

- OpenSSL 3.2.2 (industry-standard, FIPS-validated algorithms available)
- MIRACL Core Library
  - Implementations of FP256BN and BLS signature schemes are used in ISO/IEC 20248 deployments
  - Deterministic behaviour and constant-time primitives are employed

3.3 Platform & Cloud Compliance (AWS)

AWS compliance includes:

- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO/IEC 27701
- ISO 9001
- SOC 1 / SOC 2 / SOC 3
- FIPS 140-3 validated hardware modules (where applicable)

IDeTRUST uses only AWS infrastructure components falling under these declarations.