CERTIFICATION PRACTICE STATEMENT (CPS)

miPDFsign Cloud CA

Practices implementing the miPDFsign Cloud CA Certificate Policy · RFC 3647

OPERATOR	DOCUMENT	EFFECTIVE
miPDFsign (Wolfgang Mitterbucher)	Certification Practice Statement	2026-07-15
CONTACT	**REPOSITORY**	**IMPLEMENTS**
office@mitterbucher.com	cloud-signing.com/api/ca	CP miPDFsign Cloud CA v1.0

Contents

> **Language versions.** This English version is authoritative. A German convenience translation is published as `CPS-miPDFsign-Cloud-CA.de.pdf` ; in case of discrepancies this English version prevails.

01 Introduction

This Certification Practice Statement (CPS) describes **how miPDFsign operates** the miPDFsign Cloud CA in conformance with the **miPDFsign Cloud CA Certificate Policy (CP)**, policy OIDs `1.3.6.1.4.1.66283.2.1` (organization document seal) and `1.3.6.1.4.1.66283.2.2` (personal signature) — IANA PEN 66283, registered to cloud-signing.com. The CA issues per-organization **document seals** and, for organizations that opt in, short-lived **personal signature** certificates naming the individual signer. Both are used exclusively by the platform's server-side signing service at cloud-signing.com.

1.1 Hierarchy as operated

CA / certificate	Subject (pattern)	Key / validity
Root CA	`CN=miPDFsign Cloud Root CA G2, O=miPDFsign Cloud, C=AT`	RSA-4096 · SHA-384 · 20 y
Issuing CA	`CN=miPDFsign Cloud Document Signing CA G2, O=miPDFsign Cloud, C=AT`	RSA-4096 · SHA-384 · 10 y · pathlen 0
Document seal	`CN=<Org> Document Seal, O=<Org>, OU=miPDFsign Cloud Organization Seal`	RSA-3072 · SHA-256 · 3 y

The CA software is built on BouncyCastle; all certificates, keys, the issuance registry and CRL state are persisted in the platform database. CA administration is performed through the platform-operator console ("CA" tab).

02 Publication and repository

The repository is served anonymously over TLS at `https://cloud-signing.com/api/ca`:

Artifact	URL
Repository index (JSON)	`/api/ca`
Root CA certificate	`/api/ca/root.crt` (DER) · `/api/ca/root.pem`
Issuing CA certificate	`/api/ca/issuing.crt` (DER) · `/api/ca/issuing.pem`
Full chain (PEM)	`/api/ca/chain.pem`
CRL — issued seals	`/api/ca/issuing.crl`
CRL — issuing CAs	`/api/ca/root.crl`
OCSP responder	`/api/ca/ocsp` (GET + POST)
CP · CPS	`/docs/cps.html` (HTML) and as PDF documents

These URLs are embedded in every issued certificate (AIA `caIssuers` + `ocsp`, CRL distribution point, certificatePolicies CPS qualifier) and are kept stable. CRLs are regenerated on demand when older than 24 hours and immediately after a revocation; their `nextUpdate` is 7 days, providing ample overlap.

03 Identification and authentication

Issuance is bound to an authenticated platform tenant: the organization exists, is active and acts through the platform's authenticated signing pipeline. The subject DN is derived from the registered organization name with RDN-special characters escaped. No out-of-band identity vetting is performed at this assurance level; relying parties needing vetted legal identities use the platform's qualified signing methods or organization-supplied certificates instead.

04 Certificate life-cycle operations

4.1 Issuance (automatic)

On the organization's first signature with the built-in method after CA activation, the platform generates an RSA-3072 key pair server-side, issues the seal from the Issuing CA in the same operation, stores the key encrypted, records the certificate in the issuance registry and writes an audit event (`ca.seal_issued`). The private key never leaves the platform.

4.2 Renewal / re-key (automatic)

When the current seal expires within 30 days or has been revoked, the next signature automatically triggers issuance of a fresh seal with a new key. Previously signed documents remain verifiable through embedded timestamps and LTV material.

4.3 Revocation

Revocation is available through three channels: **(a)** operators revoke seals in the CA tab of the operator console (audited as `ca.seal_revoked`); **(b)** subscriber organizations revoke their **own** seal self-service in the administration area; **(c)** anyone — subscriber or relying party — can submit a revocation request via the public form at `https://cloud-signing.com/ca/report` (also linked from the repository index) or via office@mitterbucher.com. Public reports are recorded against the registry, alert the operator and are processed within **24 hours**. The CRL is rebuilt immediately on revocation and OCSP answers reflect it at once (both read the same registry). Reason codes follow RFC 5280; suspension is not offered.

4.4 Erasure on account deletion

Deleting a tenant purges its documents, flows, users, contacts and audit trail. Issued certificates are **pseudonymized rather than deleted**: subject DN, signer e-mail and the certificate itself are erased, while serial number, issuing CA, validity window and revocation state remain. The registry keeps answering OCSP and listing revocations for those serials — every signature the organization ever produced keeps its revocation answer — but nothing in the retained row identifies a person. There is no way for an operator to reconstruct the erased subject from the registry.

Seal lifetime is configurable (`Ca:SealValidity`; default 3 years). The CA equally supports **short-lived seals** (e.g. 10 minutes — one seal per signing session): validity at signing time remains provable through the embedded RFC 3161 timestamp and LTV material, and revocation becomes largely moot for such seals.

05 Facility, management and operational controls

- **Key storage:** the Root and Issuing CA private keys live in an external key service (KMS, OpenBao Transit) on a separate, hardened machine; they are *non-exportable* and never leave the KMS — signing happens only through a delegated, authenticated and logged call. Short-lived end-entity keys (seal / personal signature) are generated per operation and, where persisted at all, encrypted with the platform's data-protection key ring.
- **Access:** the CA tab and CA API are restricted to the *PlatformAdmin* role; operator accounts use strong passwords and TOTP two-factor authentication.
- **Audit:** issuance and revocation events are appended to the tenant-scoped, append-only audit trail with actor, timestamp, subject and serial.
- **Incident response:** a published runbook (`docs/ca/incident-response.md`) classifies incidents (seal / issuing-CA / root compromise, repository outage, mis-issuance) with immediate actions — revocation, hierarchy pause (the CA can be deactivated instantly; signing falls back without outage), re-keying — plus communication duties and post-mortems. Initial response target: 24 hours.
- **Backups:** database backups contain only encrypted key material; the data-protection key ring is stored and backed up separately (Redis-persisted key ring in production).

5.8 CA termination

There is **no guaranteed minimum term** of operation for this CA — miPDFsign Cloud is a non-qualified trust service and is under no supervisory continuity obligation. On cessation: the shutdown is announced with reasonable notice (60 days as a guideline) and no further certificates are issued; a final, long-dated CRL is published; the public repository (root certificate and final CRL) is kept available on a best-effort basis or handed over to a static host; the CA signing keys are cryptographically destroyed in the KMS; and records relevant to revocation and evidence are retained for the period required by law. Already-produced **PAdES-LT/LTA signatures remain verifiable regardless**, because their timestamps and revocation evidence are embedded in the document — validity at signing time does not depend on the continued operation of these services (cf. §4.4 on erasure, §7.4 on OCSP).

06 Technical security controls

Algorithms and validities are operated exactly as required by the CP (section 6 there): RSA-4096 / SHA-384 for both CAs, RSA-3072 / SHA-256 for seals; 20 / 10 / 3-year validities. Serial numbers carry 159 bits of CSPRNG entropy. There is no key escrow and no key export. All endpoints are TLS-only. CA keys are software keys encrypted at rest; migration to an HSM is planned before any application for public trust-store membership (AATL, "Stage 3").

07 Certificate, CRL and OCSP profiles

7.1 Document seal (as issued)

Field / extension	Value
basicConstraints (critical)	`CA:FALSE`
keyUsage (critical)	`digitalSignature, nonRepudiation`
extendedKeyUsage	`id-kp-documentSigning (1.3.6.1.5.5.7.3.36)`, `1.3.6.1.4.1.311.10.3.12`
certificatePolicies	policy OID (CP §1.2) + CPS URI
cRLDistributionPoints	`https://cloud-signing.com/api/ca/issuing.crl`
authorityInfoAccess	calssuers: `…/api/ca/issuing.crt` · ocsp: `…/api/ca/ocsp`
subjectKeyIdentifier / authorityKeyIdentifier	present

7.2 Personal signature certificate (as issued)

Identical to the document seal except for the two fields that carry the difference:

Field / extension	Value
subject	`CN=<Signer>, E=<email>, O=<Organization>, OU=miPDFsign Cloud Personal Signature` `CN` is the signer's display name as the platform holds it, falling back to the e-mail address when no name is known.
subjectAltName	`rfc822Name = <email>` (non-critical) — the place RFC 5280 §4.1.2.6 designates for an address. The `E=` component in the DN is a PKCS#9 leftover that the same section deprecates; it is kept because Adobe renders DN components, but the SAN is the copy a verifier is meant to read. Both always carry the same address.
certificatePolicies	`1.3.6.1.4.1.66283.2.2` + CPS URI
validity	15 minutes (configurable; issued per signing operation)
key	RSA-3072, generated per signing operation and discarded afterwards — never persisted

Everything else — `CA:FALSE`, `digitalSignature, nonRepudiation`, the document-signing EKUs, CRLDP, AIA and the key identifiers — is as in §7.1, so chain building and revocation checking work identically for both types. Issued certificates are recorded in the issuance registry, so OCSP answers for their serials rather than returning *unknown*.

7.3 CRL

X.509 v2 CRLs with `cRLNumber` (monotonic) and `authorityKeyIdentifier`; `thisUpdate` / `nextUpdate` span 7 days; entries carry RFC 5280 reason codes. The Issuing CA's CRL covers issued seals; the Root CA's CRL covers superseded Issuing-CA generations.

7.4 OCSP

The responder (RFC 6960) answers for all certificates in the issuance registry. Responses are signed directly by the Issuing CA (RFC 6960 §2.6), embed the CA certificate, echo the request nonce when present

(RFC 8954) and are valid for 24 hours. Serials not present in the registry are answered *unknown*; syntactically invalid requests receive *malformedRequest*. Both the POST binding (`application/ocsp-request`) and the GET binding (base64 request in the URL) are supported.

08 Compliance and audit

Operations follow the structure of **ETSI EN 319 411-1** so that an external conformity assessment can be added without re-architecting. As of this version, no external audit has taken place; the CA operates self-declared and states this to relying parties.

09 Other business and legal matters

The Root CA is **not** included in public trust stores (Adobe AATL, EU Trusted Lists, operating-system stores). Relying parties who wish to see the platform's seals as trusted import the published root certificate deliberately (e.g. Adobe Acrobat → Preferences → Trust Manager → `/api/ca/root.crt`). Seals are advanced-style electronic seals at platform assurance level — not qualified certificates under eIDAS. Liability is governed by the miPDFsign Cloud terms of service; governing law is Austria. The repository and revocation services are provided free of charge.