CERTIFICATE POLICY (CP)

miPDFsign Cloud CA

Policy for organization document-seal certificates · RFC 3647

POLICY AUTHORITY
miPDFsign (Wolfgang Mitterbucher)

DOCUMENT
Certificate Policy (CP)

EFFECTIVE
2026-07-15

CONTACT
office@mitterbucher.com

REPOSITORY
cloud-signing.com/api/ca

COMPANION
CPS miPDFsign Cloud CA

© 2026 Wolfgang Mitterbucher · All rights reserved

Contents

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

© 2026 Wolfgang Mitterbucher · All rights reserved

01 Introduction

1.1 Overview

This Certificate Policy (CP) states the **requirements** that govern the issuance and use of **organization document-seal certificates** within the **miPDFsign Cloud CA**, the internal public-key infrastructure of the e-signature platform at cloud-signing.com. How these requirements are implemented is described in the companion **Certification Practice Statement (CPS)**. Both documents follow the RFC 3647 framework and are oriented toward ETSI EN 319 411-1 (policy NCP).

1.2 Document name and identification

This policy governs two certificate types, each identified by its own certificate-policy OID under the miPDFsign OID arc `1.3.6.1.4.1.66283.2`:

Policy OID	Certificate type	Subject
`1.3.6.1.4.1.66283.2.1`	miPDFsign Cloud organization document seal	the subscriber organization (legal person)
`1.3.6.1.4.1.66283.2.2`	miPDFsign Cloud personal signature	the individual signer (natural person)

The two are separate policies because their subject and their **identity assurance differ** (§3); a relying party MUST be able to tell them apart from the certificate alone. **IANA Private Enterprise Number 66283** is registered to **cloud-signing.com** and operated by miPDFsign. Certificates asserting either OID MUST comply with this CP.

1.3 PKI participants

- **Certification authority:** a two-tier hierarchy — an offline-style Root CA that signs only Issuing-CA certificates and root CRLs, and an Issuing CA that signs end-entity document seals, CRLs and OCSP responses. Both are operated exclusively by miPDFsign.
- **Registration authority:** performed by the platform itself; no external RAs are permitted under this policy.
- **Subscribers:** customer organizations of miPDFsign Cloud. Subscribers MUST NOT have access to the private key; keys are generated, stored and used exclusively inside the platform.
- **Relying parties:** any party validating a PDF sealed by the platform.

1.4 Certificate usage

Certificates issued under this CP MUST be used only for digital signatures on PDF documents produced by miPDFsign Cloud. They MUST technically preclude any other use (TLS, code signing, e-mail) through their key-usage and extended-key-usage profile (section 7). Document seals constitute advanced-style electronic **seals** of the organization; personal signature certificates constitute advanced-style electronic **signatures** of a natural person. Both are issued at **platform assurance level** and are **not** qualified certificates under eIDAS. Where a qualified signature or a legally proofed identity is required, subscribers MUST use one of the platform's qualified methods (ID Austria, A-Trust, Swisscom).

© 2026 Wolfgang Mitterbucher · All rights reserved

1.5 Policy administration

This CP is maintained by miPDFsign. Questions, complaints and revocation requests: office@mitterbucher.com. Amendments are versioned and published in the repository; material changes take effect no earlier than their publication date.

02 Publication and repository responsibilities

The CA MUST operate a publicly accessible repository providing, at stable URLs: the Root and Issuing CA certificates, the certificate chain, current CRLs, an OCSP responder, this CP and the CPS. All URLs embedded in certificates (AIA, CRL distribution point, CPS qualifier) MUST remain resolvable for the lifetime of the certificates that reference them. CRLs MUST be re-issued at least every 24 hours and immediately after any revocation.

03 Identification and authentication

3.1 Organization document seals

A document seal MUST only be issued to an organization holding an active miPDFsign Cloud tenant. The subject distinguished name MUST be derived from the organization's registered account name in the form `CN=<Organization> Document Seal, O=<Organization>, OU=miPDFsign Cloud Organization Seal`; RDN-special characters MUST be escaped so tenant names cannot inject DN components. Identity is authenticated through the platform's account and billing relationship; no additional out-of-band identity vetting is required at this assurance level. Re-key uses the same authentication; no certificate may be issued to a suspended or deleted tenant.

3.2 Personal signature certificates

A personal signature certificate MUST only be issued for a signer acting within an active tenant that has opted into this certificate type, and MUST name only that signer, in the form `CN=<Signer>, E=<email>, O=<Organization>, OU=miPDFsign Cloud Personal Signature`. The address MUST additionally appear as an `rfc822Name` in `subjectAltName`, which is where RFC 5280 §4.1.2.6 places it; the two MUST agree. The subject MUST be taken from the platform's own record of the signer — the authenticated account, or the e-mail address the tenant invited to sign — and MUST NOT be freely supplied by the requester. RDN-special characters MUST be escaped.

> **Assurance statement (binding on relying parties).** The CA attests *who was authenticated by, or invited through, the platform* for this signing operation. It does **not** attest the signer's legally verified identity: no identity document is checked, no face-to-face or video identification is performed, and no register is consulted. A personal signature certificate is therefore evidence of a platform-authenticated or tenant-declared identity, nothing more. Relying parties requiring a proofed identity MUST require a qualified signature instead.

© 2026 Wolfgang Mitterbucher · All rights reserved

04 Certificate life-cycle requirements

- **Issuance:** automatic, upon the organization's first use of the platform's built-in signing method after CA activation. Key generation and issuance MUST occur server-side in one step; the private key MUST never exist outside the platform.
- **Renewal / re-key:** a new seal with a fresh key MUST be issued automatically when the current seal expires within 30 days or has been revoked. Expired certificates MUST NOT be extended.
- **Personal signature certificates:** MUST be issued fresh, with a fresh key, for each individual signing operation, and MUST be short-lived (15 minutes by default, never more than 24 hours). They MUST NOT be renewed or reused: because no certificate remains valid beyond the session that created it, there is nothing to renew and revocation is largely moot — the signature's validity at signing time is instead proven by the embedded RFC 3161 timestamp and LTV material. Signatures made with such a certificate MUST therefore be augmented at signing time to **PAdES-LT or LTA** — the OCSP response and the certificate chain MUST be embedded in the document. Without that material the short validity would defeat the purpose: a verifier checking the document later validates against the current time and would find an expired certificate with no proof it was good when it was used. The private key MUST be discarded after the signing operation and MUST NOT be persisted.
- **Erasure of subscriber data:** when a subscriber terminates their tenancy, the CA MUST retain the *revocation skeleton* of every certificate it issued to them — serial number, issuing CA, validity window and revocation state — because relying parties MUST keep receiving a revocation answer for signatures produced before the termination; a CA that forgot a serial would answer *unknown* and silently degrade every one of those signatures. The CA MUST NOT retain anything that identifies a person: the subject distinguished name, the signer's e-mail address and the certificate itself MUST be erased at that point. Personal signature certificates name a natural person, so this is an erasure obligation, not a courtesy. The retention MUST be declared in the operator's privacy notice.
- **Revocation:** the operator MUST revoke a seal on subscriber request, on tenant termination, or on suspected key compromise. The CA MUST offer a publicly accessible revocation-request channel (web form and email) open to subscribers *and* relying parties, and MUST process requests within 24 hours. Revocations MUST appear on the CRL and in OCSP responses immediately. Reason codes follow RFC 5280. Revocation is irreversible; suspension is not offered. Subscribers MUST be able to revoke their own seal without operator involvement.

05 Management and operational requirements

- **Key protection:** the Root and Issuing CA private keys MUST be held *non-exportable* in a dedicated key service (KMS) separate from the application system, and MUST NOT leave the application system in the clear; signing happens only through a delegated, authenticated and logged call. Short-lived end-entity keys MUST, where persisted at all, be stored encrypted.
- **Access control:** CA administration MUST be restricted to the platform-operator role, protected by strong authentication including a second factor.
- **Audit:** every issuance and revocation MUST be recorded in an append-only audit trail with actor, timestamp and certificate serial.

© 2026 Wolfgang Mitterbucher · All rights reserved

- **Business continuity:** encrypted backups MUST include the (encrypted) key material; the encryption key ring MUST be managed and backed up separately from the database.
- **Incident response:** a documented incident-response plan MUST exist covering key compromise at every tier, repository outage and mis-issuance, with an initial-response target of 24 hours and defined communication duties toward subscribers and relying parties.

5.8 CA termination

There is **no guaranteed minimum term** of operation for this CA; as a non-qualified trust service it is under no supervisory continuity obligation. On termination the operator MUST: announce the shutdown with reasonable notice and cease issuing certificates; publish a final, long-dated CRL; keep the public repository (root certificate and final CRL) available on a best-effort basis or hand it to a third party; provably destroy the CA signing keys (cryptographic deletion in the key service); and retain records relevant to revocation and evidence for the period required by law. Termination MUST NOT impair the verifiability of already-produced **PAdES-LT/LTA signatures**, whose proof of validity (timestamp and revocation data) is embedded in the document.

06 Technical security requirements

	Root CA	Issuing CA	Document seal
Key algorithm (minimum)	RSA-4096	RSA-4096	RSA-3072
Signature hash (minimum)	SHA-384	SHA-384	SHA-256
Maximum validity	20 years	10 years	3 years

Key escrow and key export are prohibited. Certificate serial numbers MUST carry at least 100 bits of CSPRNG entropy. Repository and OCSP endpoints MUST be served exclusively over TLS. Hardware-protected CA keys (HSM) are required before any application for public trust-store membership (AATL).

07 Certificate, CRL and OCSP profile requirements

Document seals MUST contain: `basicConstraints CA:FALSE` (critical); `keyUsage digitalSignature, nonRepudiation` (critical) and no other key usages; `extendedKeyUsage id-kp-documentSigning` (RFC 9336; the Microsoft document-signing EKU MAY be added); `certificatePolicies` asserting the policy OID of section 1.2 with a CPS URI qualifier; a CRL distribution point; an AIA with `caIssuers` and `ocsp` entries; and subject/ authority key identifiers. Issuing-CA certificates MUST carry `pathLenConstraint 0`. CRLs MUST be X.509 v2 with `cRLNumber`; OCSP MUST conform to RFC 6960, with responses signed by the Issuing CA or a delegated responder.

08 Compliance audit

This CP is structured to allow a future conformity assessment against **ETSI EN 319 411-1** (e.g. for Adobe Approved Trust List membership). Until such an assessment has taken place, the CA operates self-declared; relying parties are informed of this status through the CPS and the repository.

© 2026 Wolfgang Mitterbucher · All rights reserved

09 Other business and legal matters

The miPDFsign Cloud Root CA is **not** included in public trust stores. Trusting this CA is solely the relying party's decision, made by deliberately importing the published root certificate. The CA is provided "as is"; liability is governed by the miPDFsign Cloud terms of service. Governing law: Austria. Fees: none — issuance is included in the platform subscription; the repository is free of charge.

© 2026 Wolfgang Mitterbucher · All rights reserved