CERTIFICATION PRACTICE STATEMENT (CPS) — DEUTSCHE FASSUNG

miPDFsign Cloud CA

Betriebspraktiken zur Umsetzung der Zertifikatsrichtlinie · RFC 3647

BETREIBER	DOKUMENT	WIRKSAM
miPDFsign (Wolfgang Mitterbucher)	Certification Practice Statement	15.07.2026
KONTAKT	**REPOSITORY**	**SETZT UM**
office@mitterbucher.com	cloud-signing.com/api/ca	CP miPDFsign Cloud CA v1.0

Inhalt

> **Sprachfassung.** Diese deutsche Fassung dient der Information. Maßgeblich ist die **englische Fassung** (`CPS-miPDFsign-Cloud-CA.pdf`); bei Abweichungen geht sie vor.

01 Einleitung

Dieses Certification Practice Statement (CPS) beschreibt, **wie miPDFsign** die miPDFsign Cloud CA in Übereinstimmung mit der **Zertifikatsrichtlinie (CP) der miPDFsign Cloud CA** betreibt (Policy-OIDs `1.3.6.1.4.1.66283.2.1` für Organisations-Dokumentsiegel und `1.3.6.1.4.1.66283.2.2` für Personensignaturen; IANA PEN 66283, registriert auf cloud-signing.com). Die CA stellt je Organisation **Dokumentsiegel** aus und — für Organisationen, die sich dafür entscheiden — kurzlebige **Personensignatur**-Zertifikate, die den einzelnen Signator benennen. Beide werden ausschließlich vom serverseitigen Signaturdienst der Plattform unter cloud-signing.com verwendet.

1.1 Hierarchie im Betrieb

CA / Zertifikat	Subject (Muster)	Schlüssel / Gültigkeit
Root-CA	`CN=miPDFsign Cloud Root CA G2, O=miPDFsign Cloud, C=AT`	RSA-4096 · SHA-384 · 20 J.
Issuing-CA	`CN=miPDFsign Cloud Document Signing CA G2, O=miPDFsign Cloud, C=AT`	RSA-4096 · SHA-384 · 10 J. · pathlen 0
Dokumentsiegel	`CN=<Org> Document Seal, O=<Org>, OU=miPDFsign Cloud Organization Seal`	RSA-3072 · SHA-256 · 3 J.

Die CA-Software basiert auf BouncyCastle; sämtliche Zertifikate, Schlüssel, das Ausstellungsregister und der CRL-Zustand werden in der Plattform-Datenbank persistiert. Die CA-Administration erfolgt über die Betreiberkonsole der Plattform (Reiter „CA").

02 Veröffentlichung und Repository

Das Repository wird anonym über TLS unter `https://cloud-signing.com/api/ca` bereitgestellt:

Artefakt	URL
Repository-Index (JSON)	`/api/ca`
Root-CA-Zertifikat	`/api/ca/root.crt` (DER) · `/api/ca/root.pem`
Issuing-CA-Zertifikat	`/api/ca/issuing.crt` (DER) · `/api/ca/issuing.pem`
Vollständige Kette (PEM)	`/api/ca/chain.pem`
CRL — ausgestellte Siegel	`/api/ca/issuing.crl`
CRL — Issuing-CAs	`/api/ca/root.crl`
OCSP-Responder	`/api/ca/ocsp` (GET + POST)
CP · CPS	`/docs/cps.html` (HTML) sowie als PDF-Dokumente

Diese URLs sind in jedes ausgestellte Zertifikat eingebettet (AIA `caIssuers` + `ocsp`, CRL-Verteilungspunkt, certificatePolicies-CPS-Verweis) und werden stabil gehalten. CRLs werden bei Bedarf neu erzeugt, sobald sie älter als 24 Stunden sind, sowie unverzüglich nach einem Widerruf; ihr `nextUpdate` beträgt 7 Tage und bietet damit reichlich Überlappung.

03 Identifizierung und Authentifizierung

Die Ausstellung ist an einen authentifizierten Plattform-Mandanten gebunden: Die Organisation existiert, ist aktiv und handelt über die authentifizierte Signatur-Pipeline der Plattform. Der Subject DN wird aus dem registrierten Organisationsnamen abgeleitet, RDN-Sonderzeichen werden maskiert. Eine externe Identitätsprüfung findet auf diesem Vertrauensniveau nicht statt; vertrauende Parteien, die geprüfte rechtliche Identitäten benötigen, nutzen stattdessen die qualifizierten Signaturverfahren der Plattform oder von der Organisation beigestellte Zertifikate.

04 Zertifikats-Lebenszyklus im Betrieb

4.1 Ausstellung (automatisch)

Bei der ersten Signatur der Organisation mit dem plattformeigenen Verfahren nach Aktivierung der CA erzeugt die Plattform serverseitig ein RSA-3072-Schlüsselpaar, stellt das Siegel im selben Vorgang über die Issuing-CA aus, speichert den Schlüssel verschlüsselt, trägt das Zertifikat in das Ausstellungsregister ein und schreibt ein Audit-Ereignis (`ca.seal_issued`). Der private Schlüssel verlässt die Plattform zu keinem Zeitpunkt.

4.2 Erneuerung / Schlüsselwechsel (automatisch)

Läuft das aktuelle Siegel innerhalb von 30 Tagen ab oder wurde es widerrufen, löst die nächste Signatur automatisch die Ausstellung eines frischen Siegels mit neuem Schlüssel aus. Zuvor signierte Dokumente bleiben über eingebettete Zeitstempel und LTV-Material prüfbar.

4.3 Widerruf

Der Widerruf steht über drei Kanäle zur Verfügung: **(a)** Betreiber widerrufen Siegel im CA-Reiter der Betreiberkonsole (auditiert als `ca.seal_revoked`); **(b)** Zertifikatsnehmer-Organisationen widerrufen ihr **eigenes** Siegel im Self-Service über den Verwaltungsbereich; **(c)** jedermann — Zertifikatsnehmer wie vertrauende Partei — kann einen Widerrufsantrag über das öffentliche Formular unter `https://cloud-signing.com/ca/report` (auch aus dem Repository-Index verlinkt) oder per office@mitterbucher.com einreichen. Öffentliche Meldungen werden gegen das Register erfasst, alarmieren den Betreiber und werden innerhalb von **24 Stunden** bearbeitet. Die CRL wird bei einem Widerruf unverzüglich neu erzeugt, und OCSP-Antworten spiegeln ihn sofort wider (beide lesen dasselbe Register). Die Gründe folgen RFC 5280; eine Suspendierung wird nicht angeboten.

4.4 Löschung bei Kontolöschung

Beim Löschen eines Mandanten werden dessen Dokumente, Vorgänge, Benutzer, Kontakte und Audit-Trail vollständig entfernt. Ausgestellte Zertifikate werden **pseudonymisiert statt gelöscht**: Subject DN, E-Mail des Signators und das Zertifikat selbst werden gelöscht, während Seriennummer, ausstellende CA, Gültigkeitszeitraum und Sperrstatus erhalten bleiben. Das Register beantwortet damit weiterhin OCSP-Anfragen und führt Sperrungen zu diesen Seriennummern — jede jemals von dieser Organisation erzeugte Signatur behält ihre Sperrauskunft —, ohne dass der verbleibende Datensatz noch eine Person benennt. Der gelöschte Inhaber lässt sich aus dem Register auch durch den Betreiber nicht rekonstruieren.

Die **Siegel-Gültigkeitsdauer** ist konfigurierbar (`Ca:SealValidity`; Standard 3 Jahre). Die CA unterstützt gleichermaßen **kurzlebige Siegel** (z. B. 10 Minuten — ein Siegel je Signatursitzung): Die Gültigkeit zum Signaturzeitpunkt bleibt über den eingebetteten RFC-3161-Zeitstempel und das LTV-Material nachweisbar, und der Widerruf verliert für solche Siegel weitgehend an Bedeutung.

05 Infrastrukturelle, organisatorische und betriebliche Kontrollen

- **Schlüsselspeicherung:** Die privaten Schlüssel der Root- und Issuing-CA liegen in einem externen Schlüsseldienst (KMS, OpenBao Transit) auf einer getrennten, gehärteten Maschine; sie sind *non-exportable* und verlassen den KMS nie — signiert wird ausschließlich per delegiertem, authentifiziertem und protokolliertem Aufruf. Kurzlebige End-Entity-Schlüssel (Siegel/Personensignatur) werden je Vorgang erzeugt und, soweit überhaupt persistiert, mit dem Data-Protection-Schlüsselring der Plattform verschlüsselt.
- **Zugriff:** CA-Reiter und CA-API sind auf die Rolle *PlatformAdmin* beschränkt; Betreiberkonten verwenden starke Passwörter und TOTP-Zwei-Faktor-Authentifizierung.
- **Protokollierung:** Ausstellungs- und Widerrufsereignisse werden dem mandantenbezogenen, anfügeorientierten Audit-Trail mit Akteur, Zeitstempel, Subject und Seriennummer hinzugefügt.
- **Incident Response:** Ein veröffentlichtes Runbook (`docs/ca/incident-response.md`) klassifiziert Vorfälle (Kompromittierung von Siegel / Issuing-CA / Root, Repository-Ausfall, Fehlausstellung) mit Sofortmaßnahmen — Widerruf, Hierarchie-Pause (die CA kann sofort deaktiviert werden; das Signieren fällt ohne Ausfall zurück), Schlüsselwechsel — sowie Kommunikationspflichten und Post-Mortems. Erstreaktionsziel: 24 Stunden.
- **Backups:** Datenbank-Backups enthalten ausschließlich verschlüsseltes Schlüsselmaterial; der Data-Protection-Schlüsselring wird getrennt gespeichert und gesichert (in Produktion Redis-persistiert).

5.8 Einstellung des Betriebs

Für den Betrieb dieser CA besteht **keine garantierte Mindestlaufzeit** — miPDFsign Cloud ist ein nicht-qualifizierter Vertrauensdienst ohne aufsichtsrechtliche Fortführungspflicht. Wird der Dienst eingestellt, gilt: die Einstellung wird mit angemessenem Vorlauf (Richtwert 60 Tage) angekündigt und es werden keine neuen Zertifikate mehr ausgestellt; es wird eine abschließende, langdatierte CRL veröffentlicht; das öffentliche Repository (Root-Zertifikat und finale CRL) wird nach Best-Effort weiter bereitgestellt oder an einen statischen Host übergeben; die CA-Signaturschlüssel werden im KMS kryptografisch vernichtet; widerruf- und nachweisrelevante Registerdaten werden im gesetzlich gebotenen Umfang aufbewahrt. Bereits erstellte **PAdES-LT/LTA-Signaturen bleiben davon unberührt prüfbar**, weil Zeitstempel und Widerrufsnachweise im Dokument eingebettet sind — die Gültigkeit zum Signaturzeitpunkt hängt nicht vom Weiterbetrieb dieser Dienste ab (vgl. §4.4 zur Löschung, §7.4 zu OCSP).

06 Technische Sicherheitskontrollen

Algorithmen und Gültigkeiten werden exakt gemäß den Vorgaben der CP (dort Abschnitt 6) betrieben: RSA-4096 / SHA-384 für beide CAs, RSA-3072 / SHA-256 für Siegel; Gültigkeiten von 20 / 10 / 3 Jahren. Seriennummern tragen 159 Bit CSPRNG-Entropie. Es gibt keine Schlüsselhinterlegung und keinen

Schlüsselexport. Alle Endpunkte sind ausschließlich über TLS erreichbar. Die CA-Schlüssel sind Software-Schlüssel, verschlüsselt im Ruhezustand; die Migration auf ein HSM ist vor jeder Bewerbung um die Aufnahme in öffentliche Vertrauensspeicher (AATL, „Stufe 3") vorgesehen.

07 Zertifikats-, CRL- und OCSP-Profile

7.1 Dokumentsiegel (wie ausgestellt)

Feld / Erweiterung	Wert
basicConstraints (kritisch)	`CA:FALSE`
keyUsage (kritisch)	`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	vorhanden

7.2 Personensignatur-Zertifikat (wie ausgestellt)

Identisch zum Dokumentsiegel, bis auf die beiden Felder, die den Unterschied tragen:

Feld / Erweiterung	Wert
subject	`CN=<Signator>, E=<E-Mail>, O=<Organisation>, OU=miPDFsign Cloud Personal Signature` `CN` ist der Anzeigename des Signators aus dem Datenbestand der Plattform; ist kein Name bekannt, tritt die E-Mail-Adresse an seine Stelle.
subjectAltName	`rfc822Name = <E-Mail>` (nicht kritisch) — der von RFC 5280 §4.1.2.6 dafür vorgesehene Ort. Die Komponente `E=` im DN ist ein PKCS#9-Überbleibsel, das derselbe Abschnitt als veraltet einstuft; sie bleibt erhalten, weil Adobe DN-Komponenten anzeigt, doch der SAN ist die Kopie, die ein Prüfprogramm auswerten soll. Beide führen stets dieselbe Adresse.
certificatePolicies	`1.3.6.1.4.1.66283.2.2` + CPS-URI
Gültigkeit	15 Minuten (konfigurierbar; je Signaturvorgang ausgestellt)
Schlüssel	RSA-3072, je Signaturvorgang erzeugt und danach verworfen — nie gespeichert

Alles Übrige — `CA:FALSE`, `digitalSignature, nonRepudiation`, die Dokumentsignatur-EKUs, CRLDP, AIA und die Schlüsselkennungen — entspricht §7.1, sodass Kettenbildung und Sperrprüfung für beide Arten identisch funktionieren. Ausgestellte Zertifikate werden im Ausstellungsregister erfasst, damit OCSP für ihre Seriennummern antwortet statt *unknown* zurückzugeben.

7.3 CRL

X.509-v2-CRLs mit `cRLNumber` (monoton) und `authorityKeyIdentifier`; `thisUpdate` / `nextUpdate` umfassen 7 Tage; Einträge tragen Gründe nach RFC 5280. Die CRL der Issuing-CA deckt ausgestellte Siegel ab; die CRL

der Root-CA abgelöste Issuing-CA-Generationen.

7.4 OCSP

Der Responder (RFC 6960) antwortet für alle Zertifikate des Ausstellungsregisters. Antworten werden direkt von der Issuing-CA signiert (RFC 6960 §2.6), betten das CA-Zertifikat ein, spiegeln eine vorhandene Anfrage-Nonce zurück (RFC 8954) und sind 24 Stunden gültig. Nicht im Register vorhandene Seriennummern werden mit *unknown* beantwortet; syntaktisch ungültige Anfragen erhalten *malformedRequest*. Unterstützt werden sowohl das POST-Binding (`application/ocsp-request`) als auch das GET-Binding (Base64-Anfrage in der URL).

08 Konformität und Prüfung

Der Betrieb folgt der Struktur von **ETSI EN 319 411-1**, sodass eine externe Konformitätsbewertung ohne Umbau ergänzt werden kann. Zum Stand dieser Version hat keine externe Prüfung stattgefunden; die CA arbeitet selbstdeklariert und weist vertrauende Parteien darauf hin.

09 Sonstige geschäftliche und rechtliche Regelungen

Die Root-CA ist **nicht** in öffentlichen Vertrauensspeichern enthalten (Adobe AATL, EU-Vertrauenslisten, Betriebssystem-Speicher). Vertrauende Parteien, die die Siegel der Plattform als vertrauenswürdig anzeigen möchten, importieren das veröffentlichte Root-Zertifikat bewusst (z. B. Adobe Acrobat → Einstellungen → Vertrauensdienste → `/api/ca/root.crt`). Siegel sind elektronische Siegel fortgeschrittener Art auf Plattform-Vertrauensniveau — keine qualifizierten Zertifikate im Sinne der eIDAS-Verordnung. Die Haftung richtet sich nach den Nutzungsbedingungen von miPDFsign Cloud; anwendbares Recht ist österreichisches Recht. Repository und Widerrufsdienste werden kostenfrei bereitgestellt.