CERTIFICATE POLICY (CP) — DEUTSCHE FASSUNG

miPDFsign Cloud CA

Richtlinie für Organisations-Dokumentsiegel-Zertifikate · RFC 3647

RICHTLINIEN-VERANTWORTUNG	DOKUMENT	WIRKSAM
miPDFsign (Wolfgang Mitterbucher)	Certificate Policy (CP)	15.07.2026
KONTAKT	**REPOSITORY**	**BEGLEITDOKUMENT**
office@mitterbucher.com	cloud-signing.com/api/ca	CPS miPDFsign Cloud CA

Inhalt

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

01 Einleitung

1.1 Überblick

Diese Zertifikatsrichtlinie (Certificate Policy, CP) legt die **Anforderungen** fest, die für Ausstellung und Verwendung von **Organisations-Dokumentsiegel-Zertifikaten** innerhalb der **miPDFsign Cloud CA** gelten — der internen Public-Key-Infrastruktur der E-Signatur-Plattform unter cloud-signing.com. Wie diese Anforderungen umgesetzt werden, beschreibt das Begleitdokument **Certification Practice Statement (CPS)**. Beide Dokumente folgen dem Rahmen von RFC 3647 und orientieren sich an ETSI EN 319 411-1 (Policy NCP).

1.2 Name und Kennzeichnung des Dokuments

Diese Richtlinie regelt zwei Zertifikatsarten, die jeweils durch eine eigene Zertifikats-Policy-OID unter dem miPDFsign-OID-Bogen `1.3.6.1.4.1.66283.2` gekennzeichnet sind:

Policy-OID	Zertifikatsart	Inhaber
`1.3.6.1.4.1.66283.2.1`	miPDFsign Cloud Organisations-Dokumentsiegel	die Organisation des Zertifikatsnehmers (juristische Person)
`1.3.6.1.4.1.66283.2.2`	miPDFsign Cloud Personensignatur	der einzelne Signator (natürliche Person)

Es handelt sich um getrennte Policies, weil sich Inhaber und **Identitätsprüfungsniveau unterscheiden** (Abschnitt 3); eine vertrauende Partei MUSS beide allein anhand des Zertifikats unterscheiden können. Die **IANA Private Enterprise Number 66283** ist auf **cloud-signing.com** registriert und wird von miPDFsign betrieben. Zertifikate, die eine dieser OIDs führen, MÜSSEN dieser CP entsprechen.

1.3 PKI-Beteiligte

- **Zertifizierungsstelle:** eine zweistufige Hierarchie — eine Root-CA (offline-artig betrieben), die ausschließlich Issuing-CA-Zertifikate und Root-CRLs signiert, sowie eine Issuing-CA, die Endteilnehmer-Dokumentsiegel, CRLs und OCSP-Antworten signiert. Beide werden ausschließlich von miPDFsign betrieben.
- **Registrierungsstelle:** wird durch die Plattform selbst wahrgenommen; externe Registrierungsstellen sind unter dieser Richtlinie nicht zulässig.
- **Zertifikatsnehmer:** Kunden-Organisationen von miPDFsign Cloud. Zertifikatsnehmer DÜRFEN KEINEN Zugriff auf den privaten Schlüssel haben; Schlüssel werden ausschließlich innerhalb der Plattform erzeugt, gespeichert und verwendet.
- **Vertrauende Parteien:** jede Partei, die ein von der Plattform gesiegeltes PDF prüft.

1.4 Zertifikatsverwendung

Zertifikate nach dieser CP DÜRFEN ausschließlich für digitale Signaturen auf PDF-Dokumenten verwendet werden, die von miPDFsign Cloud erzeugt wurden. Sie MÜSSEN jede andere Verwendung (TLS, Code-Signierung, E-Mail) über ihr KeyUsage-/ExtendedKeyUsage-Profil (Abschnitt 7) technisch ausschließen. Dokumentsiegel sind elektronische **Siegel** der Organisation, Personensignatur-Zertifikate elektronische

Signaturen einer natürlichen Person — beide fortgeschrittener Art auf **Plattform-Vertrauensniveau** und **keine** qualifizierten Zertifikate im Sinne der eIDAS-Verordnung. Wo eine qualifizierte Signatur oder eine rechtlich geprüfte Identität verlangt wird, MÜSSEN Zertifikatsnehmer eines der qualifizierten Verfahren der Plattform verwenden (ID Austria, A-Trust, Swisscom).

1.5 Richtlinienverwaltung

Diese CP wird von miPDFsign gepflegt. Fragen, Beschwerden und Widerrufsanträge: office@mitterbucher.com. Änderungen werden versioniert und im Repository veröffentlicht; wesentliche Änderungen werden frühestens mit ihrer Veröffentlichung wirksam.

02 Veröffentlichung und Repository-Pflichten

Die CA MUSS ein öffentlich zugängliches Repository betreiben, das unter stabilen URLs bereitstellt: die Zertifikate der Root- und Issuing-CA, die Zertifikatskette, aktuelle CRLs, einen OCSP-Responder, diese CP und das CPS. Alle in Zertifikate eingebetteten URLs (AIA, CRL-Verteilungspunkt, CPS-Verweis) MÜSSEN für die gesamte Lebensdauer der Zertifikate, die auf sie verweisen, auflösbar bleiben. CRLs MÜSSEN mindestens alle 24 Stunden sowie unverzüglich nach jedem Widerruf neu ausgestellt werden.

03 Identifizierung und Authentifizierung

3.1 Organisations-Dokumentsiegel

Ein Dokumentsiegel DARF nur an eine Organisation mit aktivem miPDFsign-Cloud-Mandanten ausgestellt werden. Der Subject Distinguished Name MUSS aus dem registrierten Organisationsnamen in der Form `CN=<Organisation> Document Seal, O=<Organisation>, OU=miPDFsign Cloud Organization Seal` abgeleitet werden; RDN-Sonderzeichen MÜSSEN maskiert werden, damit Mandantennamen keine DN-Bestandteile einschleusen können. Die Identität wird über die Konto- und Vertragsbeziehung der Plattform authentifiziert; eine zusätzliche externe Identitätsprüfung ist auf diesem Vertrauensniveau nicht erforderlich. Die Schlüsselerneuerung nutzt dieselbe Authentifizierung; an gesperrte oder gelöschte Mandanten darf kein Zertifikat ausgestellt werden.

3.2 Personensignatur-Zertifikate

Ein Personensignatur-Zertifikat DARF nur für einen Signator ausgestellt werden, der innerhalb eines aktiven Mandanten handelt, der diese Zertifikatsart gewählt hat, und DARF nur diesen Signator benennen — in der Form `CN=<Signator>, E=<E-Mail>, O=<Organisation>, OU=miPDFsign Cloud Personal Signature`. Die Adresse MUSS zusätzlich als `rfc822Name` im `subjectAltName` geführt werden — dem von RFC 5280 §4.1.2.6 dafür vorgesehenen Ort; beide MÜSSEN übereinstimmen. Das Subject MUSS aus dem plattformeigenen Datenbestand zum Signator stammen — dem authentifizierten Konto oder der E-Mail-Adresse, die der Mandant zur Signatur eingeladen hat — und DARF NICHT frei vom Anfragenden vorgegeben werden. RDN-Sonderzeichen MÜSSEN maskiert werden.

> **Aussage zum Vertrauensniveau (für vertrauende Parteien verbindlich).** Die CA bestätigt, *wer für diesen Signaturvorgang von der Plattform authentifiziert oder über sie eingeladen wurde*. Sie bestätigt **nicht** die rechtlich

> geprüfte Identität des Signators: Es wird kein Ausweisdokument geprüft, keine Vor-Ort- oder Video-Identifizierung durchgeführt und kein Register abgefragt. Ein Personensignatur-Zertifikat ist damit ein Nachweis einer plattformauthentifizierten bzw. vom Mandanten erklärten Identität — nicht mehr. Vertrauende Parteien, die eine geprüfte Identität benötigen, MÜSSEN stattdessen eine qualifizierte Signatur verlangen.

04 Anforderungen an den Zertifikats-Lebenszyklus

- **Ausstellung:** automatisch, bei der ersten Nutzung des plattformeigenen Signaturverfahrens durch die Organisation nach Aktivierung der CA. Schlüsselerzeugung und Ausstellung MÜSSEN serverseitig in einem Schritt erfolgen; der private Schlüssel DARF die Plattform zu keinem Zeitpunkt verlassen.
- **Erneuerung / Schlüsselwechsel:** Ein neues Siegel mit frischem Schlüssel MUSS automatisch ausgestellt werden, wenn das aktuelle Siegel innerhalb von 30 Tagen abläuft oder widerrufen wurde. Abgelaufene Zertifikate DÜRFEN NICHT verlängert werden.
- **Personensignatur-Zertifikate:** MÜSSEN für jeden einzelnen Signaturvorgang neu und mit frischem Schlüssel ausgestellt werden und MÜSSEN kurzlebig sein (standardmäßig 15 Minuten, niemals mehr als 24 Stunden). Sie DÜRFEN NICHT erneuert oder wiederverwendet werden: Da kein Zertifikat über die Sitzung hinaus gültig bleibt, in der es entstanden ist, gibt es nichts zu erneuern, und ein Widerruf läuft weitgehend ins Leere — die Gültigkeit zum Signaturzeitpunkt wird stattdessen durch den eingebetteten RFC 3161-Zeitstempel und das LTV-Material nachgewiesen. Signaturen mit einem solchen Zertifikat MÜSSEN daher bereits beim Signieren auf **PAdES-LT oder LTA** angehoben werden — die OCSP-Antwort und die Zertifikatskette MÜSSEN im Dokument eingebettet werden. Ohne dieses Material würde die kurze Gültigkeit ihren Zweck verfehlen: Wer das Dokument später prüft, prüft gegen die aktuelle Zeit und fände ein abgelaufenes Zertifikat ohne Nachweis, dass es zum Verwendungszeitpunkt gültig war. Der private Schlüssel MUSS nach dem Signaturvorgang verworfen werden und DARF NICHT gespeichert werden.
- **Löschung von Zertifikatsnehmer-Daten:** Beendet ein Zertifikatsnehmer seinen Mandanten, MUSS die CA von jedem für ihn ausgestellten Zertifikat das *Sperr-Skelett* behalten — Seriennummer, ausstellende CA, Gültigkeitszeitraum und Sperrstatus. Vertrauende Parteien MÜSSEN für Signaturen, die vor der Beendigung entstanden sind, weiterhin eine Sperrauskunft erhalten; eine CA, die eine Seriennummer vergisst, antwortet *unknown* und entwertet damit stillschweigend jede dieser Signaturen. Alles Personenbezogene DARF NICHT aufbewahrt werden: Der Subject Distinguished Name, die E-Mail-Adresse des Signators und das Zertifikat selbst MÜSSEN zu diesem Zeitpunkt gelöscht werden. Personensignatur-Zertifikate benennen eine natürliche Person — dies ist daher eine Löschpflicht und kein Entgegenkommen. Die Aufbewahrung MUSS in der Datenschutzerklärung des Betreibers benannt werden.
- **Widerruf:** Der Betreiber MUSS ein Siegel auf Antrag des Zertifikatsnehmers, bei Mandantenbeendigung oder bei Verdacht auf Schlüsselkompromittierung widerrufen. Die CA MUSS einen öffentlich zugänglichen Widerrufsantrags-Kanal (Webformular und E-Mail) anbieten, der Zertifikatsnehmern *und* vertrauenden Parteien offensteht, und Anträge innerhalb von 24 Stunden bearbeiten. Widerrufe MÜSSEN unverzüglich auf der CRL und in OCSP-Antworten erscheinen. Die Gründe folgen RFC 5280. Ein Widerruf ist unumkehrbar; eine Suspendierung wird nicht angeboten. Zertifikatsnehmer MÜSSEN ihr eigenes Siegel ohne Mitwirkung des Betreibers widerrufen können.

05 Organisatorische und betriebliche Anforderungen

- **Schlüsselschutz:** Die privaten Schlüssel der Root- und Issuing-CA MÜSSEN in einem dedizierten, vom Anwendungssystem getrennten Schlüsseldienst (KMS) *non-exportable* verwahrt werden und DÜRFEN das Anwendungssystem nicht im Klartext verlassen; signiert wird ausschließlich per delegiertem, authentifiziertem und protokolliertem Aufruf. Kurzlebige End-Entity-Schlüssel MÜSSEN, soweit überhaupt persistiert, verschlüsselt gespeichert werden.
- **Zugriffskontrolle:** Die CA-Administration MUSS auf die Plattform-Betreiberrolle beschränkt sein, geschützt durch starke Authentifizierung einschließlich eines zweiten Faktors.
- **Protokollierung:** Jede Ausstellung und jeder Widerruf MUSS in einem anfügeorientierten Audit-Trail mit Akteur, Zeitstempel und Zertifikatsseriennummer festgehalten werden.
- **Betriebskontinuität:** Verschlüsselte Backups MÜSSEN das (verschlüsselte) Schlüsselmaterial umfassen; der Verschlüsselungs-Schlüsselring MUSS getrennt von der Datenbank verwaltet und gesichert werden.
- **Incident Response:** Es MUSS ein dokumentierter Incident-Response-Plan existieren, der Schlüsselkompromittierungen auf jeder Ebene, Repository-Ausfälle und Fehlausstellungen abdeckt — mit einem Erstreaktionsziel von 24 Stunden und definierten Kommunikationspflichten gegenüber Zertifikatsnehmern und vertrauenden Parteien.

5.8 Einstellung des Betriebs

Für den Betrieb dieser CA besteht **keine garantierte Mindestlaufzeit**; als nicht-qualifizierter Vertrauensdienst unterliegt sie keiner aufsichtsrechtlichen Fortführungspflicht. Wird der Betrieb eingestellt, MUSS: die Einstellung mit angemessenem Vorlauf angekündigt und die Neuausstellung von Zertifikaten beendet werden; eine abschließende, langdatierte CRL veröffentlicht werden; das öffentliche Repository (Root-Zertifikat und finale CRL) nach Best-Effort weiter bereitgestellt oder an einen Dritten übergeben werden; die CA-Signaturschlüssel nachweislich vernichtet werden (im Schlüsseldienst kryptografisch gelöscht); und widerruf- sowie nachweisrelevante Registerdaten im gesetzlich gebotenen Umfang aufbewahrt werden. Die Einstellung DARF die Prüfbarkeit bereits erstellter **PAdES-LT/LTA-Signaturen NICHT beeinträchtigen**, da deren Gültigkeitsnachweis (Zeitstempel und Widerrufsdaten) im Dokument eingebettet ist.

06 Technische Sicherheitsanforderungen

	Root-CA	Issuing-CA	Dokumentsiegel
Schlüsselalgorithmus (mindestens)	RSA-4096	RSA-4096	RSA-3072
Signatur-Hash (mindestens)	SHA-384	SHA-384	SHA-256
Maximale Gültigkeit	20 Jahre	10 Jahre	3 Jahre

Schlüsselhinterlegung (Key Escrow) und Schlüsselexport sind untersagt. Zertifikatsseriennummern MÜSSEN mindestens 100 Bit CSPRNG-Entropie tragen. Repository- und OCSP-Endpunkte MÜSSEN ausschließlich über TLS bereitgestellt werden. Hardware-geschützte CA-Schlüssel (HSM) sind vor jeder Bewerbung um die Aufnahme in öffentliche Vertrauensspeicher (AATL) erforderlich.

07 Anforderungen an Zertifikats-, CRL- und OCSP-Profile

Dokumentsiegel MÜSSEN enthalten: `basicConstraints CA:FALSE` (kritisch); `keyUsage digitalSignature, nonRepudiation` (kritisch) und keine weiteren Schlüsselverwendungen; `extendedKeyUsage id-kp-documentSigning` (RFC 9336; die Microsoft-Dokumentsignatur-EKU KANN ergänzt werden); `certificatePolicies` mit der Policy-OID aus Abschnitt 1.2 und einem CPS-URI-Verweis; einen CRL-Verteilungspunkt; ein AIA mit `caIssuers`- und `ocsp`-Einträgen; sowie Subject-/Authority-Key-Identifier. Issuing-CA-Zertifikate MÜSSEN `pathLenConstraint 0` tragen. CRLs MÜSSEN X.509 v2 mit `cRLNumber` sein; OCSP MUSS RFC 6960 entsprechen, mit Antworten, die von der Issuing-CA oder einem delegierten Responder signiert sind.

08 Konformitätsprüfung

Diese CP ist so strukturiert, dass eine künftige Konformitätsbewertung nach **ETSI EN 319 411-1** möglich ist (z. B. für die Aufnahme in die Adobe Approved Trust List). Bis eine solche Bewertung stattgefunden hat, arbeitet die CA selbstdeklariert; vertrauende Parteien werden über diesen Status durch das CPS und das Repository informiert.

09 Sonstige geschäftliche und rechtliche Regelungen

Die miPDFsign Cloud Root-CA ist **nicht** in öffentlichen Vertrauensspeichern enthalten. Das Vertrauen in diese CA ist allein die Entscheidung der vertrauenden Partei, getroffen durch den bewussten Import des veröffentlichten Root-Zertifikats. Die CA wird ohne Gewähr („as is") bereitgestellt; die Haftung richtet sich nach den Nutzungsbedingungen von miPDFsign Cloud. Anwendbares Recht: Österreich. Entgelte: keine — die Ausstellung ist im Plattform-Abonnement enthalten; das Repository ist kostenfrei.