Certificate Policy der H&M Software-Netzwerktechnik-GmbH

H&M Software-Netzwerktechnik-GmbH Version 1.1, Stand 14.11.2026

Diese Richtlinie beschreibt, wie wir Zertifikate ausstellen, verwalten und sperren — und was ein Zertifikat von uns bestätigt und was nicht. Sie richtet sich an unsere Kunden, an alle, die ein von uns zertifiziertes Dokument oder Foto prüfen, und an Prüfer. Die Gliederung folgt RFC 3647 in vereinfachter Form.

1. Einleitung

1.1 Überblick

Die H&M Software-Netzwerktechnik-GmbH betreibt eine eigene Zertifizierungsstelle (PKI). Sie stellt Zertifikate für Schlüssel aus, deren Inhaber wir kennen, und zwar ausschließlich für unsere eigenen Produkte und unsere eigenen Dokumente:

- **Document Signing:** Kunden von MLC Sensor Monitoring erhalten ein Zertifikat auf ihren Firmennamen. Ihr Sensor-Monitoring signiert damit PDF-Berichte (z. B. Mess- und Prüfberichte). Außerdem signieren wir unsere eigenen Dokumente: mit einem Zertifikat auf unseren Firmennamen und mit persönlichen Zertifikaten unserer Beschäftigten für Dokumente, die sie in unserem Namen freigeben.
- **Photo Signing:** Nutzer von MLC Foto-Schutz erhalten ein Zertifikat für ihre C2PA-Siegel („Content Credentials"). In Betrieb seit 12.11.2026.

Wir stellen keine Zertifikate für Webserver (TLS), E-Mail-Verschlüsselung, Code-Signatur oder für Dritte außerhalb unserer Produkte aus.

1.2 Aufbau

```
H&M Software-Netzwerktechnik-GmbH Root CA                  Vertrauensanker, offline
├── H&M Software-Netzwerktechnik-GmbH Document Signing CA  stellt Zertifikate für PDF-Signaturen aus
└── H&M Software-Netzwerktechnik-GmbH Photo Signing CA     stellt Fotozertifikate aus
```

Die **Root CA** stellt nur die beiden Zwischenstellen aus und sperrt sie gegebenenfalls. Jede **Zwischenstelle** ist auf ihren Zweck beschränkt und darf keine weiteren Stellen ausstellen. Wird eine Zwischenstelle kompromittiert, betrifft das nur ihren Zweck.

1.3 Beteiligte

Rolle	Wer
Zertifizierungsstelle (CA)	H&M Software-Netzwerktechnik-GmbH
Registrierungsstelle (Identitätsprüfung)	ebenfalls die H&M Software-Netzwerktechnik-GmbH — es gibt keine externen Registrierungsstellen
Zertifikatsinhaber	Document Signing: der Kunde (juristische Person); für eigene Dokumente die H&M Software-Netzwerktechnik-GmbH selbst und von ihrer Geschäftsführung benannte Beschäftigte (natürliche Personen). Photo Signing: Siegel — wer den Schlüssel auf seinem Gerät besitzt, mit oder ohne MLC-Konto; Identität — der Inhaber eines MLC-Kontos
Vertrauende Dritte	alle, die eine Signatur oder ein Siegel mit einem unserer Zertifikate prüfen

1.4 Zulässige Verwendung

- Kundenzertifikate (Document Signing): ausschließlich zum Signieren von Dokumenten, die das Sensor-Monitoring des Kunden erzeugt.
- Zertifikate der H&M Software-Netzwerktechnik-GmbH (Document Signing): ausschließlich zum Signieren eigener Dokumente der H&M Software-Netzwerktechnik-GmbH — das Firmenzertifikat für Dokumente, die von uns stammen (z. B. diese Richtlinie), ein persönliches Zertifikat für Dokumente, die die genannte Person in unserem Namen freigibt.

- Demo-Zertifikate der H&M Software-Netzwerktechnik-GmbH (Document Signing): ausschließlich zum Vorführen eines unserer Produkte (Vorführungen, Anleitungen, Videos). Damit signierte Dokumente sind **Beispiele**; ihr Inhalt ist erfunden.
- Fotozertifikate (Photo Signing): ausschließlich für C2PA-Siegel aus MLC Foto-Schutz.

Jede andere Verwendung ist nicht vorgesehen; die Zertifikate sind technisch entsprechend beschränkt (Abschnitt 7).

1.5 Kontakt

H&M Software-Netzwerktechnik-GmbH, Schönachstraße 27, 86972 Altenstadt, Deutschland E-Mail: contact@hmsoftware.com · Telefon: +49 151 2263 9995 Vertreten durch die Geschäftsführerin Sabine A.G. Lechner; Amtsgericht München, HRB 139185.

Sperranträge und Hinweise auf Missbrauch an dieselbe Adresse (Abschnitt 4.4).

1.6 Kennungen (OIDs)

Unsere Kennungen liegen unter der IANA Private Enterprise Number **67396** (`1.3.6.1.4.1.67396`) der H&M Software-Netzwerktechnik-GmbH.

OID	Bedeutung
`1.3.6.1.4.1.67396.1.1`	diese Certificate Policy
`1.3.6.1.4.1.67396.1.2.1`	Zeitstempel-Policy, Version 1 (Abschnitt 7)

Zeitstempel unseres Dienstes tragen die Zeitstempel-Policy. Zeitstempel und Zertifikate mit Kennungen unter `2.999` stammen aus unserem Testbetrieb und haben keinerlei Aussagekraft.

2. Veröffentlichung

Was	Wo
Root-Zertifikat, Zwischenzertifikate	`http://pki.hmsoftware.com/root.cer`, `…/document-ca.cer`, `…/photo-ca.cer` (DER; daneben `.pem`); gleiche Dateien unter `http://pki.mlcgo.eu/…`
Sperrlisten (CRL)	`http://pki.hmsoftware.com/crl/root.crl`, `…/crl/document-ca.crl`, `…/crl/photo-ca.crl`; gleiche Dateien unter `http://pki.mlcgo.eu/crl/…`
Fingerprint der Root und Import-Anleitung	hmsoftware.com/zertifikate/ und mlcgo.eu — beide nennen denselben SHA-256-Fingerprint
Diese Richtlinie	pki.hmsoftware.com und hmsoftware.com/zertifikate/

Die Adressen der Zertifikate und Sperrlisten stehen fest in jedem Zertifikat und ändern sich nicht. Es sind zwei unabhängig betriebene Orte (`pki.hmsoftware.com` und `pki.mlcgo.eu`) mit identischem Inhalt; ist einer nicht erreichbar, nutzen Prüfprogramme den anderen. Fotozertifikate nennen `pki.mlcgo.eu` zuerst, alle anderen `pki.hmsoftware.com`. Sie werden bewusst über `http://` ausgeliefert, wie es RFC 5280 vorsieht; ihr Inhalt ist signiert, eine Verfälschung auf dem Transportweg würde bei der Prüfung auffallen.

Wer unsere Root importiert, sollte den Fingerprint vorher auf **beiden** Seiten vergleichen.

3. Identifizierung

3.1 Namen in Zertifikaten

- **Kundenzertifikat:** `CN` und `O` = Firmenname des Kunden mit Rechtsform, wie im Vertrag mit uns; `C` = Land des Firmensitzes. Keine Personennamen, keine E-Mail-Adressen.
- **Zertifikate der H&M Software-Netzwerktechnik-GmbH für eigene Dokumente:**
  - **Firma:** `CN` und `O` = H&M Software-Netzwerktechnik-GmbH, `C=DE`.
  - **Person:** `CN` = Vor- und Nachname wie im Ausweis, `O` = H&M Software-Netzwerktechnik-GmbH, `C=DE`. Keine Funktion oder Titel, keine E-Mail-Adresse.
  - **Demo:** `CN` = Produktname mit dem Zusatz „– Demo“ (z. B. `MLC Sensor Monitoring – Demo`), `O` = H&M Software-Netzwerktechnik-GmbH, `C=DE`. Für Vorführungen stellen wir **nie** ein Zertifikat auf eine erfundene oder fremde Firma aus.
- **Fotozertifikate** (zwei je Schlüssel, wie im C2PA-Standard üblich):

  - **Siegel:** `O=H&M Software-Netzwerktechnik-GmbH, CN=MLC Foto-Schutz`, dazu der Fingerprint des Schlüssels als Seriennummer. Es nennt das **Programm**, mit dem gesiegelt wurde — keine Person.
  - **Identität:** `CN` und `O` = öffentlicher Anzeigename des MLC-Kontos, wie der Inhaber ihn angegeben hat; nur mit seiner Einwilligung. Keine E-Mail-Adressen.
- In Kunden- und Fotozertifikaten erscheint die H&M Software-Netzwerktechnik-GmbH nur als **Aussteller**, nie als Inhaber (Ausnahme: das Siegelzertifikat nennt unser Programm).

3.2 Prüfung der Identität

- **Document Signing:** Wir stellen nur für Kunden aus, mit denen ein Vertrag über MLC Sensor Monitoring besteht. Der Firmenname wird mit dem Vertrag abgeglichen. Eine darüber hinausgehende Prüfung (z. B. Handelsregisterauszug oder Ausweis des Unterzeichners) findet nicht standardmäßig statt.
- **Zertifikate der H&M Software-Netzwerktechnik-GmbH:** Das Firmenzertifikat stellt die Geschäftsführung aus. Ein persönliches Zertifikat nur für Beschäftigte, die die Geschäftsführung dafür benannt hat; den Namen prüft sie persönlich anhand des Ausweises. Ein Demo-Zertifikat stellt die Geschäftsführung für ein bestimmtes Produkt aus.
- **Photo Signing:** Das Siegelzertifikat bestätigt nur einen Schlüssel, dessen Besitz nachgewiesen wurde. Ein MLC-Konto ist dafür nicht nötig. Ist der Schlüssel mit einem Konto verbunden, prüfen wir zusätzlich, dass weder der Schlüssel noch das Konto gesperrt ist. Das Identitätszertifikat gibt es nur mit einem MLC-Konto mit bestätigter E-Mail-Adresse; es bestätigt zusätzlich den öffentlichen Anzeigenamen dieses Kontos. **Es findet keine Ausweis- oder Identitätsprüfung statt.** Der Anzeigename ist eine Angabe des Inhabers.

3.3 Besitz des Schlüssels

- **Document Signing:** Den Schlüssel erzeugen **wir im Auftrag des Kunden** (Abschnitt 6.1); der Besitz ergibt sich aus der Übergabe. Schlüssel für persönliche Zertifikate der H&M Software-Netzwerktechnik-GmbH erhält nur die genannte Person. Der Schlüssel eines Demo-Zertifikats liegt nur in der Vorführumgebung des Produkts — nie zusammen mit dem Firmenzertifikat.
- **Photo Signing:** Der Antrag wird mit dem zu zertifizierenden Schlüssel signiert (Besitznachweis über eine einmalige Challenge). Den privaten Schlüssel bekommen wir nie zu sehen.

4. Lebenszyklus eines Zertifikats

4.1 Antrag und Ausstellung

- **Document Signing:** Der Kunde beauftragt die Signierfunktion im Rahmen seines Vertrags. Wir prüfen Vertrag und Firmennamen, erzeugen Schlüssel und Zertifikat und spielen beides verschlüsselt (PKCS#12, AES-256) in sein Sensor-Monitoring ein. Eine Selbstbedienung gibt es nicht.
- **Zertifikate der H&M Software-Netzwerktechnik-GmbH:** auf Anordnung der Geschäftsführung, Ausstellung wie beim Kunden.
- **Photo Signing:** Die App beantragt das Siegelzertifikat automatisch beim Einrichten, auch ohne MLC-Konto, und erneuert es selbst. Wir fragen bei der MLC Photo Registry nach, ob der Schlüssel dort eingetragen ist: Ist er gesperrt oder das Konto gesperrt, stellen wir nichts aus; ist die Registry nicht erreichbar, auch nicht. Das Identitätszertifikat stellen wir nur aus, wenn der Schlüssel mit einem Konto verbunden ist und der Inhaber der Veröffentlichung seines Anzeigenamens zugestimmt hat. Neue Siegelzertifikate ohne Konto geben wir je Absender und insgesamt nur in begrenzter Zahl pro Tag aus.

Jede Ausstellung wird vor der Herausgabe automatisch gegen die Kette und die Regeln aus RFC 5280 geprüft und in ein nur ergänzbares Protokoll eingetragen.

4.2 Gültigkeit und Erneuerung

Zertifikat	Gültigkeit
Root CA	25 Jahre
Zwischenstellen	5 Jahre; die Nachfolgerin wird rund ein Jahr vor Ablauf ausgestellt
Kundenzertifikat und Zertifikate der H&M Software-Netzwerktechnik-GmbH (Document Signing)	2 Jahre
Foto-Siegel	90 Tage, automatische Erneuerung
Foto-Identität	1 Jahr, automatische Erneuerung

Ein Zertifikat endet nie nach seinem Aussteller. Kundenzertifikate werden vor Ablauf durch **neue** Zertifikate mit neuem Schlüssel ersetzt; das alte wird danach mit dem Grund „superseded" gesperrt.

Signaturen bleiben nach Ablauf prüfbar: Unsere Produkte holen beim Signieren einen Zeitstempel nach RFC 3161 — von unserem eigenen Zeitstempeldienst (Abschnitt 7) oder von einem unabhängigen Dienst (derzeit DigiCert). Er belegt, dass die Signatur zu einem Zeitpunkt entstand, an dem das Zertifikat gültig war.

4.3 Gründe für eine Sperrung

Wir sperren ein Zertifikat, wenn

- der Inhaber es beantragt,
- der Vertrag endet bzw. das Konto gelöscht oder gesperrt wird,
- sich Firmenname oder Rechtsform ändern,
- der private Schlüssel kompromittiert sein könnte (z. B. Server eingebrochen, Schlüsseldatei samt Passwort weitergegeben),
- das Zertifikat entgegen dieser Richtlinie ausgestellt oder verwendet wurde,
- es durch ein neues ersetzt wurde,
- bei einem persönlichen Zertifikat der H&M Software-Netzwerktechnik-GmbH: die Person scheidet aus oder ist nicht mehr zur Freigabe in unserem Namen benannt.

4.4 Sperrantrag

Sperren beantragen können der Inhaber (bzw. vertretungsberechtigte Personen des Kunden) und wir selbst. Antrag per E-Mail oder Telefon (Abschnitt 1.5) mit Firmen- bzw. Kontoname und, wenn bekannt, Seriennummer. Hinweise auf Missbrauch nehmen wir von jedem entgegen und prüfen sie.

Wir bearbeiten Sperranträge unverzüglich, in der Regel am selben Werktag. Bei Verdacht auf Kompromittierung sperren wir sofort und informieren den Inhaber. Eine Sperrung ist endgültig.

Für Fotozertifikate nennen Sie statt eines Namens den **Fingerprint** des Schlüssels (Form `xxxx-xxxx-xxxx-xxxx`), den die App anzeigt. Wir sperren dann den Schlüssel: Seine Zertifikate werden gesperrt, und er erhält keine neuen. Das gilt ebenso, wenn wir Missbrauch feststellen, etwa massenhafte Anträge.

Fotozertifikate gleichen wir zusätzlich täglich automatisch mit der MLC Photo Registry ab: Ist dort der Schlüssel oder das Konto gesperrt, sperren wir beim nächsten Abgleich beide Zertifikate. Ist ein Schlüssel nur nicht mehr eingetragen, sperren wir sein Identitätszertifikat, wenn er an drei aufeinanderfolgenden Tagen fehlt — so führt eine vorübergehende Störung nie zu einer endgültigen Sperrung. Das Siegelzertifikat braucht kein Konto; dass ein Schlüssel nicht eingetragen ist, ist dafür kein Sperrgrund. Es läuft nach spätestens 90 Tagen aus. Ein in der Registry nur ausgemustertes Gerät (lange ungenutzt, vom Nutzer entfernt oder wegen des Geräte-Limits) ist kein Sperrgrund: Es erhält keine neuen Zertifikate, die vorhandenen laufen aus, und damit gesetzte Siegel bleiben gültig. Aus demselben Grund sperrt der automatische Abgleich nie ungewöhnlich viele Zertifikate auf einmal; solche Fälle prüfen wir von Hand.

4.5 Sperrlisten

Sperrliste	Gültigkeit	Neu signiert
Root CA	395 Tage	jährlich und bei Sperrung einer Zwischenstelle
Document Signing CA	30 Tage	mindestens wöchentlich und bei jeder Sperrung
Photo Signing CA	30 Tage (7 Tage, sobald der Dienst online läuft)	mindestens wöchentlich bzw. täglich und bei jeder Sperrung

Eine Sperrung erscheint mit der nächsten veröffentlichten Sperrliste, spätestens am Werktag nach der Sperrung. Einen OCSP-Dienst betreiben wir nicht. Vertrauende Dritte sollten bei der Prüfung die Sperrliste abrufen bzw. die in der Signatur eingebettete verwenden.

5. Betrieb und Sicherheit

- **Root-Schlüssel:** wird ausschließlich auf einem Rechner ohne Netzwerkverbindung benutzt, in einer protokollierten Zeremonie mit — wenn möglich — zwei Anwesenden. Er liegt nur verschlüsselt vor, an zwei getrennten Orten. Die Software verweigert Root-Operationen technisch, solange eine Netzwerkverbindung besteht.
- **Schlüssel der Zwischenstellen:** verschlüsselt gespeichert; die Document Signing CA wird nicht als öffentlich erreichbarer Dienst betrieben.

- **Software statt Hardware:** Alle CA-Schlüssel sind Software-Schlüssel, geschützt durch starke Verschlüsselung (age/scrypt) und die genannten Abläufe. Ein Hardware-Sicherheitsmodul (HSM) setzen wir derzeit **nicht** ein; ein späterer Umzug ist ohne Wechsel der Root möglich.
- **Protokoll:** Jede Ausstellung, Sperrung und Sperrliste wird in einem nur ergänzbaren, mit einer Hash-Kette gesicherten Protokoll festgehalten und versioniert gesichert.
- **Sicherung:** Schlüssel und Protokoll werden verschlüsselt bzw. versioniert an getrennten Orten gesichert.
- **Personal:** Zugang zu CA-Schlüsseln haben nur die Geschäftsführung und von ihr benannte Personen.

6. Technische Sicherheit

6.1 Erzeugung und Aufbewahrung der Schlüssel

- **CA-Schlüssel:** erzeugt in der Zeremonie bzw. auf unseren Systemen mit dem Zufallsgenerator des Betriebssystems.
- **Kundenschlüssel (Document Signing):** erzeugt **von uns im Auftrag des Kunden**, nur im Arbeitsspeicher, und als passwortgeschützte PKCS#12-Datei in das Sensor-Monitoring des Kunden eingespielt, das ihn verschlüsselt speichert. **Wir bewahren eine verschlüsselte Kopie** auf, um den Schlüssel bei einem Defekt wiederherstellen zu können. Wir verwenden diese Kopie ausschließlich dafür und für keine eigene Signatur.
- **Schlüssel der H&M Software-Netzwerktechnik-GmbH (Document Signing):** erzeugt wie Kundenschlüssel und verschlüsselt in unserer Schlüsselverwaltung gespeichert. Einen persönlichen Schlüssel benutzt nur die genannte Person.
- **Fotoschlüssel:** erzeugt und gespeichert auf dem Gerät des Nutzers (Schlüsselbund/Keystore). Wir erhalten nur den öffentlichen Schlüssel.

6.2 Algorithmen

Stelle	Algorithmus
Root CA, Zwischenstellen	ECDSA P-384, Signaturen mit SHA-384
Kundenzertifikate, Zertifikate der H&M Software-Netzwerktechnik-GmbH	ECDSA P-256 oder RSA 3072
Fotozertifikate	Ed25519

Seriennummern sind 16 Byte aus einem kryptographischen Zufallsgenerator.

7. Zertifikatsprofile

	Kundenzertifikat (Document Signing)	Foto-Siegel	Foto-Identität	Zeitstempeldienst
Subject	`CN=<Firma>, O=<Firma>, C=<Land>`; persönlich (nur H&M Software-Netzwerktechnik-GmbH): `CN=<Person>, O=H&M Software-Netzwerktechnik-GmbH, C=DE`	`CN=MLC Foto-Schutz, O=H&M Software-Netzwerktechnik-GmbH, C=DE, serialNumber=<Fingerprint>`	`CN=<Anzeigename>, O=<Anzeigename>`	`CN=H&M Software-Netzwerktechnik-GmbH Timestamping Authority, O=H&M Software-Netzwerktechnik-GmbH, C=DE`
Key Usage	digitalSignature, nonRepudiation (kritisch)	digitalSignature (kritisch)	digitalSignature (kritisch)	digitalSignature (kritisch)
Extended Key Usage	documentSigning (RFC 9336), emailProtection	c2pa-kp-claimSigning, emailProtection	wie Siegel	nur timeStamping (kritisch)
Aussteller	Document Signing CA	Photo Signing CA	Photo Signing CA	Document Signing CA
Basic Constraints	kein CA (kritisch)	kein CA (kritisch)	kein CA (kritisch)	kein CA (kritisch)

	Kundenzertifikat (Document Signing)	Foto-Siegel	Foto-Identität	Zeitstempeldienst
Weitere	Authority/Subject Key ID, AIA und CRL-Verteilpunkt (`http://pki.hmsoftware.com/…` und `http://pki.mlcgo.eu/…`)	wie links	wie links	wie links

Zeitstempeldienst (RFC 3161, `https://pki.mlcgo.eu/tsa`): Policy `1.3.6.1.4.1.67396.1.2.1`, Hash SHA-256, Genauigkeit 1 Sekunde (Systemuhr per NTP). Jeder Stempel wird mit Zeit, Seriennummer und Hash protokolliert — nie mit den gestempelten Daten selbst.

Zwischenstellen: Pfadlänge 0, Extended Key Usage auf ihren Zweck beschränkt. Root: Pfadlänge 1. Einzelheiten veröffentlichen wir auf Anfrage.

8. Prüfungen

Jedes ausgestellte Zertifikat wird automatisch gegen die Regeln aus RFC 5280 geprüft. Die Abläufe dieser Richtlinie prüfen wir intern mindestens jährlich. Eine externe Auditierung (etwa nach ETSI EN 319 411 oder WebTrust) findet **nicht** statt.

9. Rechtliches

9.1 Was ein Zertifikat bestätigt — und was nicht

Ein Kundenzertifikat bestätigt: Der Schlüssel wurde für den genannten Vertragspartner erzeugt und ist ihm zugeordnet. Ein persönliches Zertifikat der H&M Software-Netzwerktechnik-GmbH bestätigt: Die genannte Person ist bei uns beschäftigt und von der Geschäftsführung benannt, Dokumente in unserem Namen freizugeben. Ein Demo-Zertifikat bestätigt nur: Das Dokument wurde in einer Vorführumgebung des genannten Produkts der H&M Software-Netzwerktechnik-GmbH signiert — es ist ein Beispiel, keine Aussage der H&M Software-Netzwerktechnik-GmbH zu seinem Inhalt. Ein Foto-Siegelzertifikat bestätigt: Das Foto wurde mit einem Schlüssel gesiegelt, für den bei uns ein Zertifikat für MLC Foto-Schutz beantragt und dessen Besitz dabei nachgewiesen wurde; der Schlüssel war zum Zeitpunkt der Ausstellung bei uns nicht gesperrt. Es bestätigt **weder eine Person noch ein Konto**. Ein Foto-Identitätszertifikat bestätigt zusätzlich: Der Schlüssel gehört zu einem MLC-Konto mit bestätigter E-Mail-Adresse, und dessen öffentlicher Anzeigename ist der im Zertifikat genannte. Ein Zeitstempel bestätigt, dass die gestempelten Daten zu dem angegebenen Zeitpunkt vorlagen.

Ein Zertifikat bestätigt **nicht** den Inhalt eines signierten Dokuments oder Fotos, die Richtigkeit von Messwerten, die Vertretungsbefugnis einzelner Personen beim Kunden oder die Identität eines Fotografen über das Konto hinaus.

9.2 Kein qualifizierter Vertrauensdienst

Die PKI der H&M Software-Netzwerktechnik-GmbH ist **kein qualifizierter Vertrauensdienst** im Sinne der eIDAS-Verordnung (EU) Nr. 910/2014 und steht nicht auf der EU Trusted List. Signaturen und Siegel mit unseren Zertifikaten sind **keine qualifizierten elektronischen Signaturen oder Siegel**; wir sichern keinen bestimmten rechtlichen Status zu. Sie belegen Herkunft und Unversehrtheit technisch; wie sie rechtlich gewürdigt werden, hängt vom Einzelfall ab.

9.3 Pflichten

- **Inhaber:** Schlüssel und PKCS#12-Passwort schützen und nicht weitergeben; uns Änderungen des Firmennamens und jeden Verdacht auf Kompromittierung unverzüglich melden; das Zertifikat nur wie in 1.4 beschrieben verwenden.
- **Vertrauende Dritte:** den Fingerprint der Root vor dem Import vergleichen; Signatur, Kette, Sperrstatus und Zeitstempel prüfen bzw. ihr Prüfprogramm das tun lassen; die Grenzen aus 9.1 beachten.

9.4 Haftung

Wir haften nach den gesetzlichen Bestimmungen für Vorsatz und grobe Fahrlässigkeit sowie bei Verletzung von Leben, Körper und Gesundheit. Im Übrigen gelten die Haftungsregeln des jeweiligen Vertrags mit dem Kunden. Gegenüber vertrauenden Dritten, mit denen kein Vertrag besteht, übernehmen wir keine darüber hinausgehende Haftung.

9.5 Datenschutz

Zertifikate enthalten nur Firmen- bzw. Kontonamen und Land, keine E-Mail-Adressen. Sie stehen in jedem signierten Dokument bzw. gesiegelten Foto und sind damit für jeden lesbar, der es erhält. Sperrlisten enthalten nur Seriennummern. Unser Protokoll (Seriennummern, Namen, Laufzeiten) ist nicht öffentlich. Für ein Foto-Siegelzertifikat ohne Konto erhalten wir nur den öffentlichen Schlüssel; um missbräuchliche Anträge zu begrenzen, zählen wir Anträge je IP-Adresse 24 Stunden lang im Arbeitsspeicher. Im Übrigen gilt die Datenschutzerklärung auf hmsoftware.com.

9.6 Anwendbares Recht

Es gilt das Recht der Bundesrepublik Deutschland.

10. Änderungen dieser Richtlinie

Änderungen veröffentlichen wir als neue Version an denselben Adressen. Änderungen, die Inhaber oder vertrauende Dritte betreffen, kündigen wir Kunden vorab an.

Version	Datum	Änderung
1.0 (Entwurf)	25.10.2026	erste Fassung, nicht veröffentlicht
1.1	14.11.2026	Zertifikate der H&M Software-Netzwerktechnik-GmbH für eigene Dokumente (Firma und benannte Beschäftigte: 1.1, 1.3, 1.4, 3.1–3.3, 4.1–4.3, 6, 7, 9.1); Photo Signing in Betrieb; ausgemustertes Gerät ist kein Sperrgrund (4.4); eigener Zeitstempeldienst (4.2); Demo-Zertifikate der H&M Software-Netzwerktechnik-GmbH für Vorführungen (1.4, 3.1–3.3, 9.1); Foto-Siegelzertifikat auch ohne MLC-Konto, 90 Tage gültig, Sperrung je Schlüssel (1.3, 3.2, 4.1, 4.2, 4.4, 9.1, 9.5); nach juristischer Durchsicht überall der volle Firmenname; erste veröffentlichte Fassung

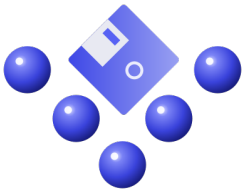
Digitale Signaturen · Digital signatures

Dieses Dokument ist digital signiert. Jede Signatur bestätigt, wer es herausgegeben oder freigegeben hat und dass es seitdem nicht verändert wurde. Prüfen Sie die Signaturen in Ihrem PDF-Programm (z. B. Acrobat Reader, Unterschriften-Panel) — das Bild unten allein ist kein Nachweis. Anleitung: **mlcgo.eu/pki/signaturen-pruefen.pdf**

This document is digitally signed. Each signature confirms who issued or approved it and that it has not been changed since. Check the signatures in your PDF reader (e.g. Acrobat Reader, Signatures panel) — the picture below is not proof on its own. Guide: ***mlcgo.eu/pki/verifying-signatures.pdf***



Digital signiert von / Digitally signed by
H&M Software-Netzwerktechnik-GmbH
Grund / Reason: Herausgegeben / Issued
Datum / Date: 2026.11.14 14:03:12 +01'00'



Digital signiert von / Digitally signed by
Michael Lechner
Grund / Reason: Freigegeben / Approved
Datum / Date: 2026.11.14 14:03:19 +01'00'