Signierte PDFs der H&M Software-Netzwerktechnik-GmbH prüfen

Sie haben ein PDF erhalten, das wir — oder eine Firma, für die wir Zertifikate ausstellen — digital signiert haben. Diese Anleitung erklärt, was die Signatur bedeutet, wie Sie sie prüfen und was „vertrauen" dabei heißt.

English version: „Verifying signed PDFs from H&M Software-Netzwerktechnik-GmbH".

Kurz gesagt

- Die Signatur zeigt, **wer** das Dokument signiert hat, dass es **seitdem nicht verändert** wurde und **wann** signiert wurde.
- Ihr PDF-Programm zeigt zunächst **„Gültigkeit unbekannt"**. Das ist kein Fehler: Es kennt uns als Aussteller noch nicht.
- Nach einem einmaligen Schritt — unser **Root-Zertifikat** vertrauen, nachdem Sie seinen Fingerabdruck verglichen haben — steht dort **„gültig"**.

Wer bei uns signiert

Im PDF steht als Unterzeichner	Bedeutung
H&M Software-Netzwerktechnik-GmbH	Das Dokument stammt von uns („herausgegeben").
Michael Lechner (Organisation: H&M Software-Netzwerktechnik-GmbH)	Diese Person hat das Dokument in unserem Namen **freigegeben**.
Name einer anderen Firma, ausgestellt von „H&M Software-Netzwerktechnik-GmbH Document Signing CA"	Ein Bericht aus dem Sensor-Monitoring dieser Firma. Die Firma ist der Unterzeichner; wir haben ihr das Zertifikat ausgestellt.

Ein Dokument kann mehrere Signaturen tragen, z. B. erst „herausgegeben", dann „freigegeben". Jede wird einzeln geprüft.

Was eine Signatur bestätigt — und was nicht

Sie bestätigt:

- Das Dokument wurde mit dem Schlüssel signiert, den wir dem genannten Unterzeichner zugeordnet haben.
- Es wurde danach nicht verändert — auch kein einzelnes Zeichen.
- Mit Zeitstempel: Es lag zu dem angegebenen Zeitpunkt in dieser Form vor.

Sie bestätigt nicht:

- dass der Inhalt richtig ist (z. B. Messwerte),
- eine Vertretungsbefugnis über das hinaus, was im Zertifikat steht.

Unsere Signaturen sind **keine qualifizierten elektronischen Signaturen** im Sinne der eIDAS-Verordnung; wir sind kein qualifizierter Vertrauensdienst. Sie belegen Herkunft und Unversehrtheit technisch. Einzelheiten regelt unsere Certificate Policy.

Was „vertrauen" bedeutet

PDF-Programme kennen von Haus aus nur die Aussteller auf den Listen von Adobe und Microsoft. Wir betreiben eine **eigene** Zertifizierungsstelle und stehen nicht auf diesen Listen. Deshalb fragt Ihr Programm sinngemäß: „Ich kenne den Aussteller nicht — wollen Sie ihm vertrauen?"

Wenn Sie unser **Root-Zertifikat** als vertrauenswürdig eintragen, heißt das:

- Ihr Programm erkennt Signaturen, die mit einem Zertifikat **aus unserer Zertifizierungsstelle** erstellt wurden, als echt an.
- **Nur dafür:** Unsere Zertifizierungsstelle stellt technisch ausschließlich Zertifikate für **Dokument-Signaturen** und **Foto-Siegel** aus — keine für Webseiten, keine für Programme. Das Vertrauen öffnet also keine Tür für anderes.
- Sie können den Eintrag **jederzeit wieder entfernen**.

Entscheidend ist, dass Sie die echte Root eintragen. Vergleichen Sie deshalb vorher den Fingerabdruck — er ist eine Art Prüfsumme des Zertifikats:

Fingerabdruck der „H&M Software-Netzwerktechnik-GmbH Root CA", **SHA-256** (32 Byte, hier auf zwei Zeilen):

```
79:3B:0A:48:3A:9B:26:1D:91:BE:C0:33:C9:47:EB:A4
75:38:DA:48:3D:D4:A8:39:52:EF:3C:5D:F5:C9:0C:AB
```

SHA-1 (zeigt Windows an):

```
AA:97:4E:34:1D:F3:38:6A:07:AF:D0:DD:C1:8E:C3:84:9D:AE:13:49
```

Manche Programme zeigen die Werte mit Leerzeichen statt Doppelpunkten oder in Kleinbuchstaben — es zählt nur die Folge der Zeichen.

Denselben Wert finden Sie unabhängig davon auf **https://mlcgo.eu/pki/**. Stimmt er nicht überein, tragen Sie nichts ein und sprechen Sie uns an. Das Zertifikat selbst: `http://pki.hmsoftware.com/root.cer` (auch unter `http://pki.mlcgo.eu/root.cer`).

Die Anzeige verstehen

Anzeige	Bedeutung	Was tun
„Gültigkeit unbekannt", dazu „Dokument wurde nicht geändert"	Signatur in Ordnung, Aussteller noch unbekannt.	Root vertrauen (unten).
„Gültig"	Unterzeichner bestätigt, Dokument unverändert.	—
„Ungültig" oder „Dokument wurde geändert"	Das Dokument wurde nach dem Signieren verändert.	Original beim Absender anfordern. Nicht weiterleiten, nicht „als PDF drucken", nicht neu speichern — das bricht jede Signatur.

Prüfen mit Adobe Acrobat Reader (Windows und Mac, kostenlos)

Acrobat hat einen eigenen Vertrauensspeicher. So tragen Sie die Root direkt aus dem PDF ein:

1. PDF öffnen → rechts das **Unterschriften**-Panel öffnen (oder oben auf „Unterschriftenfenster" klicken).
2. Rechtsklick auf die Signatur → **Signatureigenschaften anzeigen**.
3. **Zertifikat des Unterzeichners anzeigen**.
4. Links in der Kette den **obersten Eintrag** wählen: „H&M Software-Netzwerktechnik-GmbH Root CA".
5. Reiter **Details** → „SHA256-Digest" (ältere Versionen zeigen nur „SHA1-Digest") mit dem passenden Wert oben vergleichen.
6. Reiter **Vertrauen** → **Zu vertrauenswürdigen Zertifikaten hinzufügen** → Rückfrage bestätigen → Haken bei **„Dieses Zertifikat als vertrauenswürdigen Stamm verwenden"** → OK → OK.
7. PDF schließen und neu öffnen → **„Signatur ist gültig"**.

Mit der heruntergeladenen Datei geht es auch über **Einstellungen → Unterschriften → Identitäten und vertrauenswürdige Zertifikate → Weitere… → Vertrauenswürdige Zertifikate → Importieren**.

Prüfen mit Microsoft Edge (Windows)

Edge prüft gegen den Zertifikatspeicher von Windows:

1. `root.cer` herunterladen und doppelklicken → **Zertifikat installieren…**
2. **Aktueller Benutzer** → Weiter → **Alle Zertifikate in folgendem Speicher speichern** → Durchsuchen → **Vertrauenswürdige Stammzertifizierungsstellen** → Weiter → Fertig stellen.
3. Windows warnt und zeigt einen **SHA-1-Fingerabdruck** — mit dem Wert oben vergleichen → Ja.
4. Edge ganz schließen, neu öffnen, PDF öffnen → **„Gültig"**.

Chrome, Firefox und die Mac-Vorschau zeigen keine PDF-Signaturen an; nehmen Sie dafür Acrobat Reader.

Zeitstempel

Unsere Signaturen tragen einen Zeitstempel, meist von unserem eigenen Zeitstempeldienst. Er belegt den Zeitpunkt der Signatur — und sorgt dafür, dass sie **auch nach Ablauf des Zertifikats** prüfbar bleibt. Acrobat zeigt dann „Die Signatur enthält einen eingebetteten Zeitstempel" und prüft zu diesem Zeitpunkt. Ohne vertraute Root nennt Acrobat den Zeitstempel „nicht überprüft" — das verschwindet mit dem Eintrag oben.

Häufige Fragen

Muss ich die Root wirklich eintragen? Nein. Auch ohne sehen Sie, dass das Dokument seit dem Signieren nicht verändert wurde. Die Root braucht es nur, damit Ihr Programm den Unterzeichner bestätigt.

Da steht „HM" statt „H&M". Ein Darstellungsfehler mancher Windows-Dialoge, die das „&" verschlucken. Im Zertifikat steht korrekt „H&M".

„Sperrprüfung wurde nicht durchgeführt". Erscheint, solange die Root nicht vertraut ist oder der Rechner kein Internet hat. Unsere Sperrlisten liegen unter `http://pki.hmsoftware.com/crl/` und `http://pki.mlcgo.eu/crl/`.

Wie entferne ich die Root wieder? Acrobat: Einstellungen → Unterschriften → Identitäten und vertrauenswürdige Zertifikate → Weitere… → Vertrauenswürdige Zertifikate → Root markieren → Entfernen. Windows: `certmgr.msc` → Vertrauenswürdige Stammzertifizierungsstellen → Zertifikate → löschen.

Kontakt

H&M Software-Netzwerktechnik-GmbH, Schönachstraße 27, 86972 Altenstadt E-Mail: contact@hmsoftware.com · Telefon: +49 151 2263 9995