Verifying signed PDFs from H&M Software-Netzwerktechnik-GmbH

You have received a PDF that we — or a company we issue certificates to — signed digitally. This guide explains what the signature means, how to check it, and what "trusting" our certificate involves.

Deutsche Fassung: „Signierte PDFs der H&M Software-Netzwerktechnik-GmbH prüfen".

In short

- The signature shows **who** signed the document, that it **has not been changed** since, and **when** it was signed.
- At first your PDF reader shows **"Signature validity is unknown"**. That is not an error: it does not know us as an issuer yet.
- After one step — trusting our **root certificate** once you have compared its fingerprint — it shows **"valid"**.

Who signs for us

Shown as signer in the PDF	Meaning
H&M Software-Netzwerktechnik-GmbH	The document comes from us ("issued").
Michael Lechner (organisation: H&M Software-Netzwerktechnik-GmbH)	This person **approved** the document on our behalf.
Another company's name, issued by "H&M Software-Netzwerktechnik-GmbH Document Signing CA"	A report from that company's sensor monitoring. The company is the signer; we issued its certificate.

A document can carry several signatures, e.g. first "issued", then "approved". Each one is checked on its own.

What a signature confirms — and what it does not

It confirms:

- The document was signed with the key we assigned to the named signer.
- It has not been changed since — not a single character.
- With a timestamp: it existed in this form at the stated time.

It does not confirm:

- that the content is correct (e.g. measured values),
- any power of representation beyond what the certificate states.

Our signatures are **not qualified electronic signatures** under the eIDAS Regulation; we are not a qualified trust service provider. They prove origin and integrity technically. Details are set out in our Certificate Policy.

What "trust" means

PDF readers only know the issuers on Adobe's and Microsoft's lists out of the box. We run our **own** certification authority and are not on those lists. So your reader is effectively asking: "I don't know this issuer — do you want to trust it?"

When you mark our **root certificate** as trusted, this means:

- Your reader accepts signatures made with a certificate **from our certification authority** as genuine.
- **Only that:** our certification authority is technically limited to certificates for **document signatures** and **photo seals** — none for websites, none for software. Trusting it opens no door to anything else.
- You can **remove** the entry at any time.

What matters is that you trust the real root. Compare its fingerprint — a kind of checksum of the certificate — first:

Fingerprint of "H&M Software-Netzwerktechnik-GmbH Root CA", **SHA-256** (32 bytes, split over two lines here):

```
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 (shown by Windows):

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

Some programs show the values with spaces instead of colons or in lower case — only the sequence of characters matters.

You will find the same value independently at **https://mlcgo.eu/pki/en.html**. If it does not match, do not trust anything and contact us. The certificate itself: `http://pki.hmsoftware.com/root.cer` (also at `http://pki.mlcgo.eu/root.cer`).

Reading the result

Shown	Meaning	What to do
"Signature validity is unknown" with "Document has not been modified"	Signature fine, issuer not yet known.	Trust the root (below).
"Valid"	Signer confirmed, document unchanged.	—
"Invalid" or "Document has been modified"	The document was changed after signing.	Ask the sender for the original. Do not forward it as a new file, "print to PDF" or re-save it — that breaks every signature.

Checking with Adobe Acrobat Reader (Windows and Mac, free)

Acrobat keeps its own list of trusted certificates. To add the root straight from the PDF:

1. Open the PDF → open the **Signatures** panel on the right (or click "Signature Panel" at the top).
2. Right-click the signature → **Show Signature Properties…**
3. **Show Signer's Certificate…**
4. On the left, select the **top entry** of the chain: "H&M Software-Netzwerktechnik-GmbH Root CA".
5. **Details** tab → compare "SHA256 digest" (older versions only show "SHA1 digest") with the matching value above.
6. **Trust** tab → **Add to Trusted Certificates…** → confirm → tick **"Use this certificate as a trusted root"** → OK → OK.
7. Close and reopen the PDF → **"Signature is valid"**.

With the downloaded file you can also use **Preferences** → **Signatures** → **Identities & Trusted Certificates** → **More…** → **Trusted Certificates** → **Import**.

Checking with Microsoft Edge (Windows)

Edge checks against the Windows certificate store:

1. Download `root.cer` and double-click it → **Install Certificate…**
2. **Current User** → Next → **Place all certificates in the following store** → Browse → **Trusted Root Certification Authorities** → Next → Finish.
3. Windows warns and shows a **SHA-1 thumbprint** — compare it with the value above → Yes.
4. Close Edge completely, reopen it, open the PDF → **"Valid"**.

Chrome, Firefox and macOS Preview do not show PDF signatures; use Acrobat Reader for those.

Timestamps

Our signatures carry a timestamp, usually from our own timestamping service. It proves when the document was signed — and keeps the signature verifiable **even after the certificate has expired**. Acrobat then says "Signature includes an embedded timestamp" and validates as of that time. As long as the root is not trusted, Acrobat calls the timestamp "not verified" — that goes away with the step above.

Frequently asked questions

Do I have to trust the root? No. Even without it you can see that the document has not been changed since it was signed. The root is only needed for your reader to confirm the signer.

It says "HM" instead of "H&M". A display quirk of some Windows dialogs that swallow the "&". The certificate correctly says "H&M".

"Revocation checking was not performed". Appears while the root is not trusted or the computer has no internet access. Our revocation lists are at `http://pki.hmsoftware.com/crl/` and `http://pki.mlcgo.eu/crl/`.

How do I remove the root again? Acrobat: Preferences → Signatures → Identities & Trusted Certificates → More… → Trusted Certificates → select the root → Remove. Windows: `certmgr.msc` → Trusted Root Certification Authorities → Certificates → delete.

Contact

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