NomaSign

WHITE PAPER

Evidence you can verify.

How NomaSign seals, signs, and proves documents, and how to check it yourself. Written for IT reviewers, legal teams, and the sceptical partner in any firm evaluating e-signatures.

- Sealed before the first signature
- Verified by Adobe, not by us
- Your documents, your cloud

INSIDE

www.nomasign.com

hello@nomasign.com

Executive summary

When a signed document is challenged, three questions decide everything: what exactly was agreed, when was it agreed, and has anything changed since. Most e-signature platforms answer these questions with a report they generate themselves. NomaSign answers them with cryptographic evidence sealed inside the document, verified by software you already have.

- ✓ Every document is **certified and sealed the moment it is sent**, before the first signature.
- ✓ Every signature is applied as its **own sealed, independently timestamped revision**.
- ✓ An **independent trusted timestamp** closes the completed document.
- ✓ Verification is performed by Adobe (or any PAdES-capable validator) against independently issued certificates and timestamp authorities. **Nothing rests on NomaSign's word.**
- ✓ Documents are **stored in your own cloud**, not ours.

1. The problem with "trust us"

Electronic signing replaced paper's weaknesses with a new one: invisibility. On paper, a crude alteration at least risks being seen. In a PDF, a changed number looks exactly like the original. So every e-signature platform must answer: how do you prove the document is what everyone agreed to?

The common answer is a platform-hosted evidence model: the provider keeps logs on its servers, generates a completion certificate or audit page, and asks you to trust that its records are accurate, complete, and will still exist years from now. That model has a structural weakness: **the party operating the platform is also the party producing the evidence.** For everyday use this works fine, until the one time it matters, when a court or counterparty asks why anyone should accept the operator's own report as proof.

> There is a stronger model, defined by open standards: put the evidence inside the document itself, in a form independent software can verify without consulting the platform at all. This is the model NomaSign uses for every document.

2. The NomaSign sealing model

Three mechanisms, applied in order, all inside the PDF:

2.1 Certified at send, before anyone signs

The moment the sender clicks send, NomaSign applies a **certifying digital signature** to the document (a PDF certification with modification permissions restricted to form-fill and signing). From that instant:

- ✓ The document's baseline is cryptographically locked.
- ✓ The only changes the format permits are the ones signing requires: filling the assigned fields and adding signatures.
- ✓ Any other modification visibly breaks the certification, and validators warn the reader.

This ordering matters. A document protected only after the last signature leaves a window in which what the first signer saw and what the last signer saw cannot be cryptographically distinguished. Sealing before the first signature closes that window: every signer demonstrably signed the same certified baseline.

2.2 One sealed revision per signature

Each signature is applied as an **incremental, individually sealed revision** of the document, with its own embedded timestamp. The consequences:

- ✓ The exact state of the document at every step is preserved and can be viewed ("click to view this version" in Adobe).
- ✓ What changed between revisions is exactly the permitted signing activity, and nothing else.
- ✓ Later signers provably signed over the earlier signatures: the second signature seals a document that already contains the first.

Each signature revision also records contextual details in the signature itself, visible in the reader: on whose behalf it was applied (the verified signer email) and a device identifier.

2.3 Closed by an independent trusted timestamp

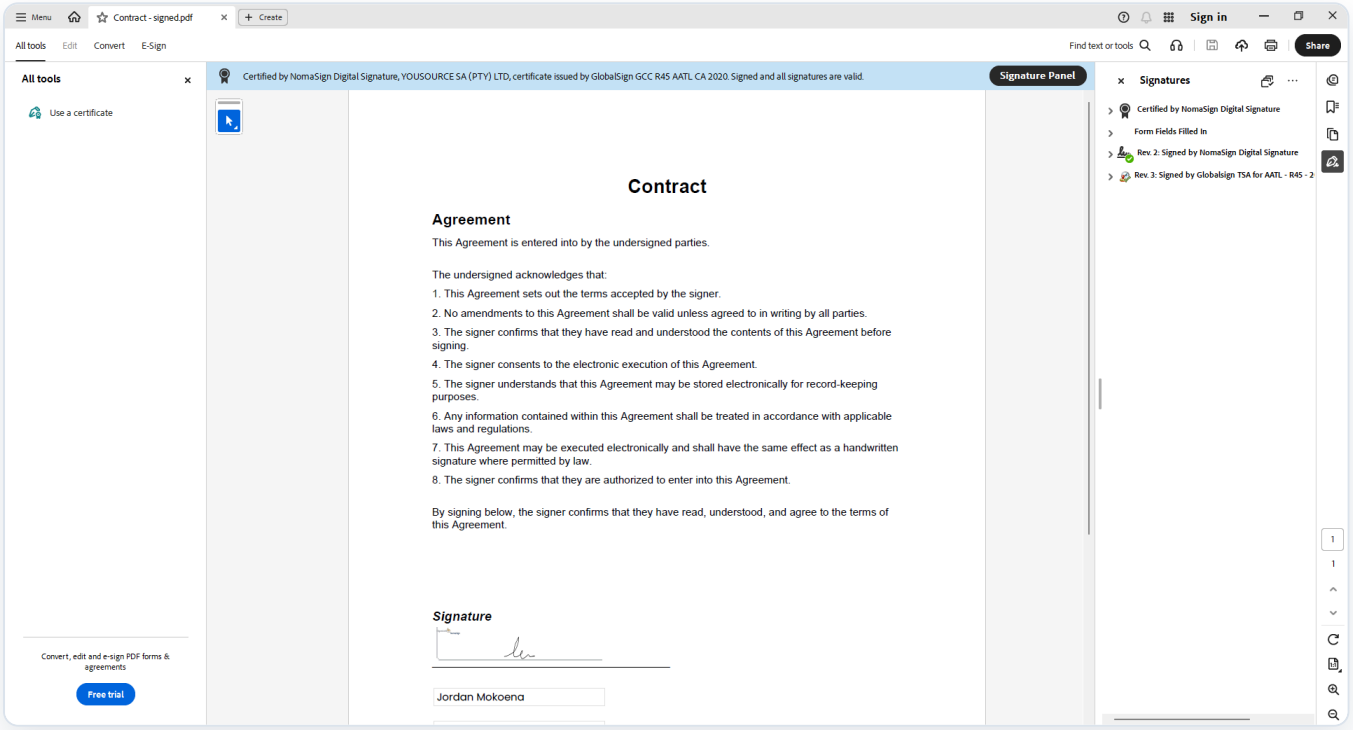
When the last signature is complete, a **document timestamp from an independent timestamp authority** (RFC 3161) is applied. The completion moment is fixed by a third party's clock and certificate, not by NomaSign's server time.

Alongside this, the document embeds long-term validation material (certificate chain and revocation evidence), completing the **PAdES long-term signature structure standardised under the EU's eIDAS framework**. In practice: the signatures remain verifiable for years, even after certificates expire, because everything a validator needs travels inside the file.

3. Verify it yourself: reading the evidence in Adobe

No NomaSign software is involved in verification. Open any completed NomaSign document in Adobe Acrobat Reader:

1. **The banner.** "Certified... Signed and all signatures are valid." Adobe's verdict, computed on your machine.
2. **The signature panel, top entry.** The certification applied at send: "only form fill-in, signing and page adding actions are allowed", with an embedded timestamp, applied before any signature.
3. **The signature revisions.** For each: "document has not been modified since this signature was applied", the embedded timestamp, the trust source (Adobe Approved Trust List), and long-term validation enabled.
4. **The closing entry.** The independent timestamp authority's document timestamp.



The banner and the full revision history, rendered by Adobe

The document's life story: certified, filled, signed, timestamped

The trust chain runs from your PDF reader, to the certificate authorities and timestamp authorities, to the document. **NomaSign is not in that chain at verification time.**

Want to run this check right now? Download a real signed sample at **www.nomasign.com/proof**.

4. The audit trail question

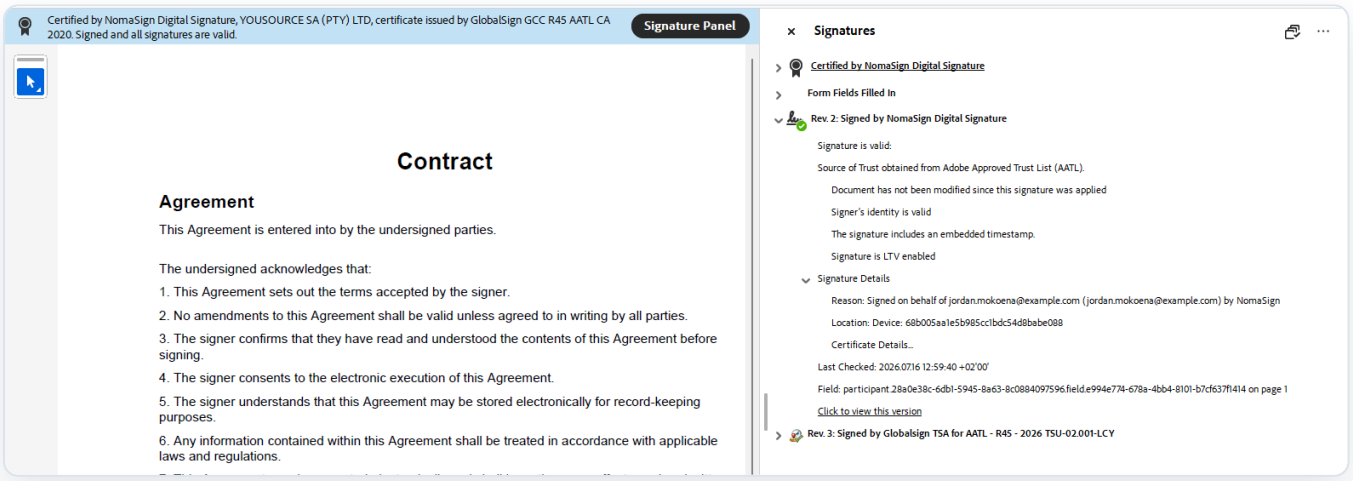
Ask a hard question of any signed PDF with a tidy audit page at the back: **who produced that page, and how do you know it is true?** A generated audit report is an account of events, written by the platform that hosted them. It is useful for readability. It is not, by itself, evidence.

There is also a subtler technical point. A certified document permits only form-fill and signing. **Appending pages after completion would modify the document.** A visibly appended audit page and an intact certification cannot both be fully preserved; something has been traded away.

NomaSign's position

- ✓ **The evidence is the revision history itself:** the certified baseline, the sealed and timestamped signature revisions, and the independent closing timestamp. This is what we recommend relying on, and it is what a validator actually checks.
- ✓ On certified documents, NomaSign does **not** append an audit page. The audit data (signing events, verified email, IP address, device fingerprint, timestamps) is embedded within the document's structure so a human-readable report can be generated on demand, without disturbing the certification.
- ✓ Where a readable report is wanted for convenience, it is exactly that: convenience. The cryptography carries the proof.

> The trustworthy audit trail is not a page describing what happened. It is the sealed revision history that makes lying about what happened impossible.



A signature revision expanded: signer email, device, AATL trust source, embedded timestamp, LTV enabled

5. Identity: layers of assurance

Document integrity and signing time are proven cryptographically for every document, as described above. Signer identity is a layered matter, and honesty about the layers is part of a serious security story.

Standard (every document)

- ✓ Signing links are private to each recipient, and email possession is verified with a one-time code (OTP) before signing when enabled.
- ✓ Each signing event records the verified email address, IP address, and a device fingerprint, embedded with the signature revision.
- ✓ These are strong practical identity signals, comparable to the industry standard for e-signatures, and they sit on top of, not instead of, the sealed revision history.

Elevated (certificate-based)

NomaSign's signing is **certificate-agnostic**: the cryptographic machinery accepts certificates from any issuer. When a signer or organisation uses their own certificate, identity joins the cryptographic evidence itself: the signature then proves, under the certificate's assurance level, that this person signed this revision at this time. With certificates from recognised trust lists, this reaches advanced or qualified levels (for example AeS and QeS under eIDAS in the EU). South African law defines advanced electronic signatures through accreditation by the South African Accreditation Authority (ECT Act, section 37) [1]. Requirements and accreditation differ by jurisdiction; if your use case needs a specific assurance level, talk to us about the certificate path.

> **It takes two to tango: the platform must handle certificates correctly, and the certificate must carry the required assurance. NomaSign supplies the first and is built to accept the second.**

6. Architecture and data privacy

Your documents live in your cloud

Completed and in-flight documents are stored in your own Microsoft 365 (OneDrive) or Google Workspace (Google Drive). NomaSign does not retain your documents; they transit our service during signing and are delivered to your storage. Practical consequences:

- ✓ Your existing retention, backup, DLP, and access policies apply to signed documents automatically.
- ✓ Offboarding NomaSign does not strand your archive on someone else's servers.
- ✓ A breach model against "the vendor's document store" does not apply: there isn't one.

Signing keys are protected by certified hardware

NomaSign's certificate and signing keys are generated and held in a hardware security module (HSM) validated to FIPS 140-3 Level 3 [2]. Signing operations are performed inside the HSM; private keys are never exposed to application code and never leave the hardware boundary.

Invitations come from your own email

Signing requests are sent from the sender's address, which both improves deliverability (no third-party bulk domain, fewer spam misses) and keeps the communication trail inside your own mail records.

Minimal data at NomaSign

We process account data and signing-session metadata needed to run the service, aligned with POPIA (and GDPR-style principles): the document content itself stays yours, in your storage.

7. Standards summary

Concern	Mechanism	Standard
Document integrity	Certifying signature at send; sealed revision per signature	PDF digital signatures (PAdES)
Signing time	Embedded timestamps; independent closing document timestamp	RFC 3161 TSA
Long-term validity	Embedded chain and revocation evidence	PAdES long-term profiles (eIDAS framework)
Reader trust	Certificates chained to the Adobe Approved Trust List	AATL
Identity (standard)	Verified email (OTP), IP, device fingerprint per event	Platform evidence
Identity (elevated)	Signer/organisation certificates, certificate-agnostic	AeS/QeS under eIDAS; jurisdiction equivalents
Key custody	Signing keys generated and held in certified HSMs	FIPS 140-3 Level 3
Legal recognition (SA)	Electronic signatures for most business documents	ECT Act 25 of 2002

8. An evaluation checklist for any provider

Fair questions to ask of every e-signature platform, including us:

- ✓ When is the document first cryptographically protected: before the first signature, or only after the last?
- ✓ Where does the evidence live: inside the document, or on the provider's servers?
- ✓ Who verifies it: independent software on your machine, or the provider's own portal?
- ✓ Can you view the exact state of the document at each signature?
- ✓ Is the completion time fixed by an independent timestamp authority?
- ✓ Will the signatures still validate in ten years, without the provider's help?
- ✓ Where are your documents stored, and what happens to them if you leave?

> Test the first six in one minute: open a completed document in Adobe and read the signature panel. Our sample is at **www.nomasign.com/proof**.

References

[1] Electronic Communications and Transactions Act 25 of 2002 (South Africa), sections 1 and 37. Official text via the South African government: www.gov.za/documents/electronic-communications-and-transactions-act
[2] FIPS 140-3 Level 3 validation of the underlying HSM platform, per the cloud provider's published security documentation.