

Sign Droid.

Get documents signed — on your infrastructure,
under your brand, with evidence that holds up.

Upload a PDF, place the fields, send tokenised links. Signees sign in the browser with no account, behind an emailed access code and an identity check. What comes back is a completed document carrying an addendum, a consent record, a disclaimer, a full audit certificate, trusted timestamps and a cryptographic seal over the exact archived bytes.

Self-hosted

White-label & custom domains

RFC 3161 timestamps

EN · FR · NL

2 974 tests

327

ENDPOINTS

57

AUDIT ACTION TYPES

5

MAIL PROVIDERS

89%

LINE COVERAGE

THE PROBLEM

Signing is solved. Signing on your own terms is not.

The established signature services work well and cost per envelope, per user, per year — and every contract you send passes through infrastructure you do not control, in a jurisdiction you did not choose, under a brand that is not yours. For an agency reselling to clients, or a firm whose documents are commercially sensitive, both of those are the problem rather than a detail.

Per-envelope pricing

A cost that scales with the thing you want more of, and a renewal conversation every year.

Someone else's tenancy

Contracts, mandates and personnel files processed and stored outside your control.

Someone else's brand

Your client signs on a page carrying a vendor's name, not yours.

Thin evidence

A certificate of completion that proves far less than a dispute will ask of it.

THE SOLUTION

Your servers, your domain, your logo — and a deeper evidence file than the envelope price buys.

White-label to the domain

Branding resolves from the host the visitor arrived on. A signee on your client's own domain sees your client's logo, colours and name — on the login page and the signing page alike, before anyone has logged in.

Evidence, not just a tick

Every completed document carries generated addendum, consent, disclaimer and audit pages, embedded trusted timestamps, per-signee snapshots, and a detached cryptographic seal over the final bytes.

Built to be resold

Tenants, organisations, per-tenant branding, per-organisation mail providers and per-tenant payment credentials — the shape of a product somebody else sells under their own name.

THE FLOW

- 1 Prepare**
Upload one PDF or merge several. Drag signature, text, date, checkbox and dropdown fields onto the pages, assign them to signees, set validation rules and required attestation phrases.
- 2 Send**
Each signee gets a single-purpose tokenised link. Order can be enforced, expiry is per document, and reminders can be sent per document or in bulk.
- 3 Sign**
No account. An emailed six-digit code, an identity check, consent and disclaimer, then draw or type a signature and complete the fields — with progress and a live view of their own audit trail.
- 4 Seal**
Signatures applied, evidence pages appended, timestamps obtained and embedded, snapshots attached, and the whole file sealed with your organisation's key.

PREPARE & SIGN

The editor, the signing room and the evidence.

1 Document preparation

- Upload one PDF, or **merge several into one document** in a chosen order
- Visual field editor: click to place, drag to move, resize by handle, with zoom and a thumbnail rail
- Five field types — signature, text, date, checkbox and dropdown — each with label, instructions, placeholder, default, required flag and length limits
- **Regular-expression validation per field**, with a pattern wizard, a preset library and a live tester
- **Attestation clauses**: require the signee to type a phrase before the field will accept a signature
- Optionally stamp the date and the signee's name beside the signature
- Page reorder, page delete, automatic page numbering
- Templates with pre-placed fields and abstract **signee roles** resolved at instantiation; template content translatable per locale

3 What a completed document carries

- The applied signatures at their placed coordinates
- **Generated addendum, consent, disclaimer and audit-certificate pages**, produced in the document's own language
- The audit certificate lists the history timeline, access log, signature details, entered field data, the verbatim consent wording and timestamp details
- **RFC 3161 trusted timestamps** taken per signature and per document, embedded into the file as attachments
- **Per-signee snapshots attached** — the chain of custody as the document passed between parties
- A detached **4096-bit cryptographic seal** over the exact archived bytes, with the organisation's public key downloadable for verification
- Every stored file hashed; every version retained

2 The signing experience

- **No account required** — a tokenised link is the whole entry path
- A layered gate, every step audited: emailed six-digit access code, identity check against the details on file, consent, and disclaimer acknowledgement
- Sign by drawing on canvas — mouse or touch, high-resolution, with undo — or by typing a name
- Field-by-field navigation, live progress, page thumbnails and zoom
- **Refuse to sign, with a reason**, which returns the document to the sender rather than stalling
- The signee can open a live timeline of their own signing events
- Sequential signing with a per-signee order, or all at once
- Session timeout with re-verification, and rate-limited code resends
- Internal counter-signers sign in the application rather than by link

4 Identity hardening

- An optional stricter mode adding an **out-of-band SMS one-time passcode** before signing
- Codes are six digits, ten-minute life, five attempts then lockout, stored only as a hash and compared in constant time
- A per-signee key generated at the identity gate, binding signee, document, field, page, time and image hash
- Safety rails: in strict mode a signee without a phone number blocks dispatch rather than silently downgrading
- Per-signature record of address, user agent, coordinates and browser fingerprint

Positioned honestly. SignDroid produces a simple electronic signature with an unusually deep evidence package, plus an optional hardening mode. It does not issue qualified signatures, and the signature is not embedded as a PDF-native cryptographic signature — the cryptography sits alongside the document, in the seal, the timestamps and the audit record. Where a tender demands a qualified signature, this is not the product.

BRAND, ADMINISTER & OPERATE

The platform around the signature.

5

White-label & tenancy

- Three levels — tenant, organisation, user — with organisation types for customer, internal, partner and trial
- Branding at **two levels**: display name, logo, favicon and five colours, with the organisation overriding the tenant
- **Custom domains** resolved from the request host, so branding applies before login and on the signing page
- The platform name itself is replaced end to end — a signee never sees ours
- Superadmin context switching with an enforced context gate and a remembered favourite

6

Communications

- **Five mail providers per organisation** — Microsoft Graph, Gmail, Zoho, plain SMTP and Outboundly
- Authorisation flows with encrypted secrets, automatic token refresh every ten minutes, and a test-send button
- Six notification types with independent per-organisation switches
- Per-locale email templates with a delivery log recording status, failure reason and retry state
- Reminders on demand, per document or in bulk across everything outstanding

7

Languages, at runtime

- **Three shipped locales — English, French and Dutch — at 3 016 keys each**
- A translation console that adds a language, edits any string and highlights what is missing — **with no redeploy**
- Machine translation built in: fill only the gaps, re-translate a language, or fill across all of them, with a live quota meter
- Audit certificates, consent pages and emails all generated in the document's own language

8

Administration & operations

- **Fifty-seven audit action types** recording actor, address, agent, session and before-and-after values, plus a separate per-signature forensic record
- Document lifecycle with archive, cancel-with-reason, copy, and deletion blocked once signing is under way
- Hourly expiry sweep with per-document failure isolation
- Log viewer with live tail, download, runtime log-level changes and a global switch
- Memory console and a nightly housekeeping sweep that purges expired tokens and reconciles orphaned files
- Per-user, per-table sort preferences; a full dark theme
- Guided first-run setup that installs the schema and can generate and start the service unit
- **Four deployment surfaces** from one artefact, so scheduled work runs on one node rather than all of them

Where the product is today. Subscription billing is present as plan modelling, price calculation across four models, checkout and invoice generation — but charging is a one-off payment per activation, not automatic recurring billing. Multi-factor authentication for administrators, self-service password reset, and data-subject export and erasure tooling are not in this release.

WHO BUYS IT

Signature volume, plus a reason the envelope model does not fit.

Resellers & agencies

The sharpest fit. Per-tenant branding, custom domains, per-tenant payment and mail credentials — everything needed to sell signing under your own name.

Managed service providers

One deployment, many client organisations, each isolated, each on its own domain, each with its own look.

Accountancy & bookkeeping

Engagement letters and mandates at seasonal volume, where per-envelope pricing punishes exactly the months you are busiest.

Human resources & staffing

Employment contracts and onboarding packs, built from templates with named signee roles and enforced signing order.

Real estate

Leases and mandates signed by parties who will never create an account, with an evidence file that survives a dispute.

Legal practice

Client documents that must not pass through a third-party service, with a verbatim consent record and a full audit certificate.

Insurance & intermediaries

Proposals and mandates with an out-of-band passcode step where the value at risk justifies stronger identity proofing.

Public sector & non-profit

Self-hosted, on-premise, no per-signature vendor cost, and data that never leaves the organisation.

Multilingual operations

Three shipped languages and a runtime console for the fourth — with the audit certificate itself produced in the signee's language.

WHO USES IT

Platform operator

Organisation admin

Document preparer

External signee

Internal counter-signer

Translator

Installer

The signee is the persona that matters commercially: they never register, never install anything, and never see a vendor's brand — which is what makes a white-label deployment credible to the client whose name is on the page.

AGAINST THE ALTERNATIVES

OPTION	WHY IT FAILS HERE
Hosted signature service	Per-envelope cost, foreign tenancy, their brand on your client's page
Print, sign, scan	No audit trail, no timestamp, and a day of turnaround per party
An emailed PDF with a typed name	No identity gate, no consent record, nothing to produce in a dispute
Building it yourself	The signing room is the easy part; the evidence package is not

TECHNICAL SPECIFICATION

A fat JAR, a service unit and a reverse proxy.

Runtime	Java 21 on Spring Boot 4
Database	PostgreSQL, 42 tables, 26 versioned migrations applied on demand by the setup wizard
PDF	Server-side rendering and assembly; the signing and editing screens work from generated page images
Cryptography	4096-bit organisation and per-signee keys, RFC 3161 timestamping, SHA-256 file hashing
Front end	Server-rendered with vanilla JavaScript, everything vendored — zero third-party origins
API	327 endpoints across 37 API controllers; specification browser available outside production
Storage	Versioned local filesystem, tenant and organisation scoped, path-traversal guarded
Topology	Four deployment surfaces so scheduled work runs on exactly one node
Scale	~55 000 lines of application code, 43 entities, 74 services
Quality	2 974 tests ; 89.1% instruction and 89.5% line coverage against a 70% gate

SECURITY & GOVERNANCE

- Three roles with method-level authorisation; organisation access asserted at 134 call sites
 - **AES-256-GCM at rest** for every configuration secret, with keys derived at 65 536 iterations and start-up refusing a placeholder key
 - bcrypt passwords; five failures in fifteen minutes blocks for fifteen minutes, by address and by name
 - Access tokens held in memory only and re-minted from a hardened cookie; refresh tokens and passcodes stored only as hashes
 - A strict content security policy with no inline scripting, and a **no-referrer policy specifically so a signing link cannot leak**
 - Forwarded headers trusted only when explicitly enabled, guarding host injection and open redirect
 - Single sign-on through Google, configurable per organisation
 - Fifty-seven audit action types plus a per-signature forensic record with verbatim consent text
 - Dependency vulnerability scanning gated at severity seven
- Not in this release:** multi-factor authentication for administrators, SAML or directory single sign-on, password reset, encryption at rest for the document files themselves, and automated retention or erasure. Timestamp verification requires a trust anchor to be configured.

COMMERCIAL

Licensed per installation. Never per envelope.

This is the whole commercial argument. Send ten documents a month or ten thousand; the software costs the same, under your own domain and branding.

REVENUE	PER YEAR	REVENUE	PER YEAR
Up to €500k	€900	€100M	€13,000
€1M	€1,500	€500M	€37,000
€5M	€2,500	€1B	€52,000
€25M	€5,500		

Annual licence on your own turnover, ex VAT. The schedule is marginal like income tax — each slice of turnover is charged at its own rate, so there are no cliffs — with a €900 minimum and any yearly increase capped at 25%. Every tranche carries unlimited users, projects and organisations inside one tenant, self-hosting and support that rises with the tranche. Hosting and hardware are yours, and consultancy, setup, migration and training are quoted separately. Illustrative: a per-envelope vendor at €2 an envelope bills ten thousand signatures €20,000 a year; at €5M turnover this is €2,500.

SignDroid produces simple electronic signatures under eIDAS; it does not issue advanced or qualified electronic signatures, and does not embed PDF-native signatures. Specifications may change.

NEXT STEP

Send yourself a contract.

On your domain, with your logo. Then open the completed file and read the audit certificate that came back with it.

Sales	tim@automatize.eu
Partners	luc@automatize.eu
Web	automatize.eu