

Enterprise Document Signing, On Your Own Terms

KhatimDoc

eIDAS-compliant, self-hosted signing platform delivering e-signatures, natural person digital signatures and organisational seals from one governed, multi-tenant deployment



3 Types

e-Sign, D-Sign, eSeal
One platform

PAdES LT

Proof That Outlives Keys
Archive-grade evidence

Self-Hosted

Your Documents, Your Network
No third-party custody

50+ Languages

Multi-Tenant by Design
Global deployment

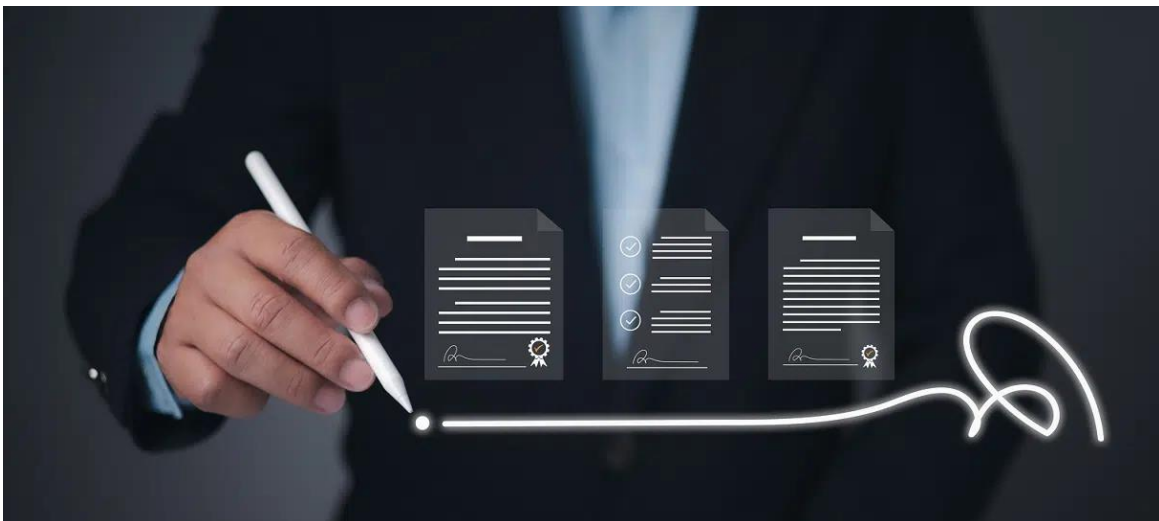
Contract signing made conclusive, not merely convenient!

KhatimDoc is where an agreement stops being a workflow and becomes an instrument — the platform that establishes not merely that somebody clicked, but that a named person, holding a verified credential, consented to a specific document at a specific moment, and can be shown to have done so years later. Signing, sealing and evidence in one deployment you own.

- Enterprise-ready, standards-compliant document signing deployed inside your own network
- e-Signatures, natural person digital signatures and organisational eSeals from one portal
- PAdES-BES, PAdES-T and PAdES-LT signatures that validate natively in Adobe Reader
- Multi-tenant architecture hosting multiple enterprises, teams and brands on one instance
- Signing keys held in smart cards, HSMS, Azure Key Vault or AWS KMS as policy requires
- Complete REST API coverage for ERP, ECM, CRM and custom application integration

KhatimDoc Supports:

- ETSI EN 319 142 — PAdES for PDF documents
- eIDAS — Regulation (EU) 910/2014 on electronic identification and trust services
- ESIGN Act — Electronic Signatures in Global and National Commerce Act
- UETA — Uniform Electronic Transactions Act
- HIPAA — protected health information handling, access control and audit
- FDA 21 CFR Part 11 — electronic records and electronic signatures
- RFC 3161 — trusted timestamping for PAdES-T and PAdES-LT profiles
- RFC 5280 — certificate profile and certification path validation
- RFC 6960 — OCSP revocation checking for signer and issuer certificates
- PKCS#11 — cryptographic token and HSM interface for hardware-held keys
- PKCS#7 / CMS — cryptographic message syntax for signature encoding
- ISO 32000 — PDF document format and embedded signature dictionaries



Ten Pillars of Enterprise Document Signing

01 Three Signature Types, One Platform e-Signatures, natural person digital signatures and organisational eSeals produced, governed and audited by one system.	02 PAdES, Adobe Compatibility & LTV Signatures that validate natively in Adobe Reader and stay provable long after the signing certificate has expired.
03 Enterprise Workflows & Package Signing Multi-document agreements distributed, routed and completed as a single atomic transaction rather than scattered files.	04 Templates, Contacts & Document Gallery A governed central library and pre-configured templates so recurring transactions are assembled once, not every time.
05 Agreement Notices, Consent & Access Disclosure shown and accepted before signing, with PIN, OTP and time-limited access proving who opened the document.	06 Self-Hosted Deployment & Data Sovereignty Documents, keys and logs remain inside your perimeter and your jurisdiction, under controls your auditors can inspect.
07 Multi-Tenancy, Rights & White-Label Branding Multiple enterprises, teams and brands on one instance, each with independent configuration and its own identity.	08 Key Management & Cryptographic Agility Signing keys in smart cards, HSMs or cloud KMS, with algorithms changed at connector level rather than at reinstall.
09 Audit Trail, Tracking & Notifications Live package state, automated reminders and a cryptographically traceable record built to survive challenge.	10 Developer Integration & Deployment REST APIs and webhooks that put signing inside the business process, on any platform your estate already runs.

PILLAR 01 · THREE SIGNATURE TYPES, ONE PLATFORM

A Click Is Not a Signature

The Challenge: One Word Covering Several Different Legal Instruments

Most platforms offer one thing and call it everything. A typed name in a box, a drawn squiggle, a cryptographic signature bound to a credential, and a corporate seal applied by a machine are not variations of a single act. They carry different evidentiary weight, satisfy different regulations and fail in different ways. An organisation equipped only with the first will eventually apply it to something that required the third, and will learn the difference during a dispute rather than during a policy review.

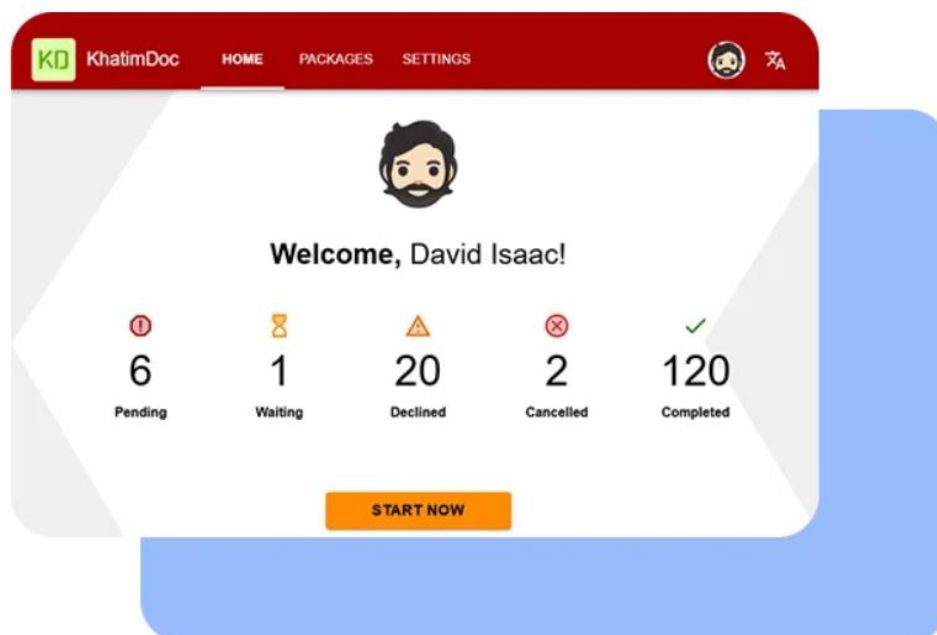
KhatimDoc Delivers

Every Signature Type the Business Actually Needs. KhatimDoc produces e-signatures for internal approvals and low-risk forms, natural person digital signatures bound to a credential held on a smart card, cryptographic token or in an HSM, and organisational eSeals applied on behalf of the entity rather than an individual. Each is created by the same platform, recorded in the same audit trail and presented in the same package viewer. The signing method is selected by template, package or service plan, so the level of assurance follows the document rather than the habits of whoever happened to send it.

Assurance Chosen Deliberately, Not by Default.

Because signing mode is a configuration rather than a product decision, an organisation is never forced to over-engineer a leave request or under-protect a shareholder agreement. Administrators define which modes a team may use and which a given template must use. Every signature — e-Sign, D-Sign or eSeal — produces verifiable metadata including signer identity, certificate serial and issuer, signing time and algorithm identifier, so the record shows not merely that a document was signed but precisely what kind of signature was applied to it.

- e-Signatures, natural person digital signatures and organisational eSeals in one platform
- Signing mode enforced per template, package or service plan
- Smart card, cryptographic token, HSM or cloud-held keys for digital signing
- Signer identity, certificate serial, time and algorithm recorded for every signature



PILLAR 02 · PAdES, ADOBE COMPATIBILITY & LONG-TERM VALIDATION

Verifiable in Adobe Reader Today, Provable Decades From Now

The Challenge: The Recipient Decides Whether Your Signature Is Real

A signature is worth exactly what the party receiving it can verify. If the counterparty opens the PDF and sees a warning triangle, or nothing at all, the cryptography behind it is irrelevant — they will ask for a wet-ink copy. Verification then meets a second deadline nobody plans for. The signer's certificate expires within a year or two, the revocation data that proved it good was published for a week, and the issuing authority may not outlive the contract. The document survives intact. The proof does not survive with it.

KhatimDoc Delivers

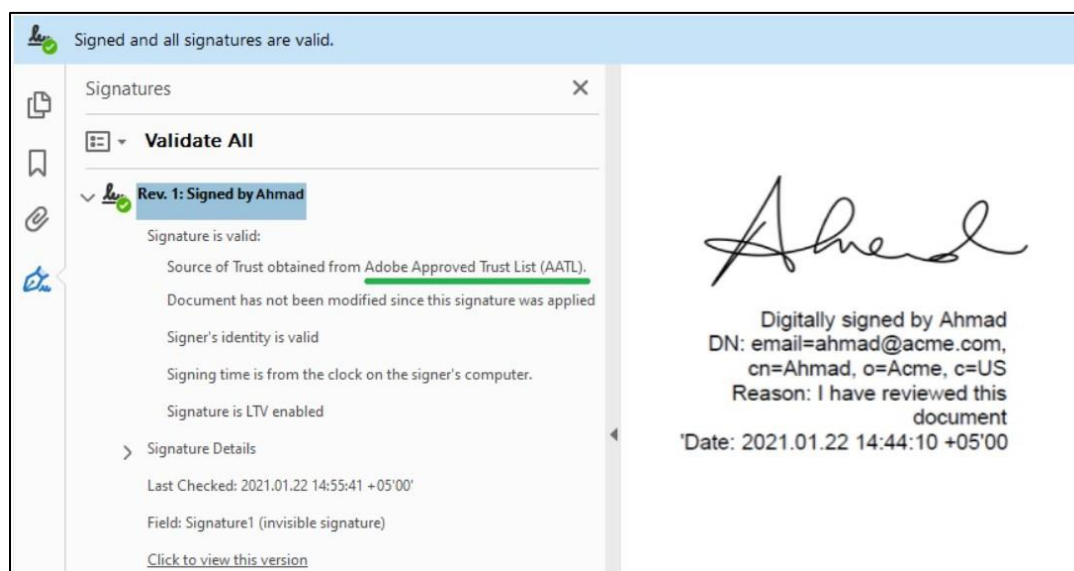
Signatures That Validate Where They Land.

KhatimDoc produces signatures conforming to the PAdES family — PAdES-BES, PAdES-T and PAdES-LT — embedded in the PDF in accordance with ISO 32000. Signed documents open and validate cleanly in Adobe Reader and other standards-compliant viewers, with no plug-in, portal account or vendor-specific application required at the receiving end. The recipient sees a green tick and a named signer in software they already have, which is the difference between a signature that is simply accepted and one that starts a conversation.

Evidence Collected While It Still Exists.

PAdES-T adds an RFC 3161 timestamp from a trusted authority, fixing the moment of signing independently of any clock the parties control. PAdES-LT goes further, embedding the certification path, CRLs and OCSP responses inside the document itself, so the material proving validity travels with the file. A KhatimDoc-signed agreement remains verifiable years after the signer's certificate has expired, the responder has been decommissioned and the issuing authority has been dissolved — because the proof was gathered while the proof still existed.

- PAdES-BES, PAdES-T and PAdES-LT signature profiles selectable per connector
- Native validation in Adobe Reader with no plug-in or vendor viewer required
- RFC 3161 timestamping through Khatim Timestamp Server or a third-party TSA
- Revocation and certification path evidence embedded for long-term verifiability



PILLAR 03 · ENTERPRISE WORKFLOWS & PACKAGE SIGNING

A Contract Is Rarely a Single Document

The Challenge: Real Agreements Arrive in Pieces

A procurement award is a contract, three annexes, a pricing schedule and a compliance declaration. Sent one file at a time to five people it becomes five threads, five reminder chains and five partial records, and it is complete when somebody decides it looks complete. Signers are missed. The annex nobody executed surfaces at renewal. The audit trail lives in an inbox belonging to a person who has since left. Treating a multi-document agreement as a series of unrelated signing events is precisely how the agreement stops being coherent.

KhatimDoc Delivers

The Whole Agreement as One Transaction.

KhatimDoc groups related documents into a package that is distributed, tracked and completed as a single unit. Multiple PDFs, forms and attachments go to multiple reviewers and signers in one action, routed serially where sequence matters or in parallel where it does not, with each recipient's role determining whether they review, approve or sign. The package either completes or it does not. There is no state in which half an agreement has been executed and nobody has yet noticed the other half.

Collaboration Inside the Document. Recipients complete form fields — text, date, number, list and checkbox — apply initials, and sign, approve or decline with a recorded reason, all inside the package rather than in the email traffic around it. Owners may remind, reassign or reissue without fragmenting the record. Access codes, one-time passwords and agreement notice acceptance can be required before a document opens, which raises first-pass completion by settling at send time the questions that would otherwise return as replies.

- Multiple documents, signers and reviewers processed as a single atomic package
- Serial and parallel routing with role-based review, approval and signing
- Form fields, initials and decline-with-reason captured inside the package
- Reminders, reassignment and reissue without fragmenting the audit record

Package: Construction Invoice

Recipients: Wahaj

Add Fields:

- D-Sign
- E-Sign
- Initials
- Text
- Checkbox
- Dropdown
- Company
- Name
- Phone
- Email

INVOICE

DATE: INVOICE NO:

QUANTITY	DESCRIPTION	UNIT PRICE	LINE TOTAL
2	Generators	\$4800	\$9600
10	Air Conditioners	\$780	\$7800
121	Lighting Bulbs	\$5	\$605
98	Electric Sockets	\$9	\$882
Subtotal			\$18887
Sales Tax			\$3210
Total			\$22097

Signed by Manager:

Documents: Construction Invoice

Stop Re-Uploading the Same Contract

The Challenge: The Same Document, Assembled Differently Every Time

High-volume senders rebuild the same transaction repeatedly — locate the current NDA, upload it, add the same three recipients, place the same fields in roughly the same positions, write the same covering note. It is slow, and slowness is the smaller problem. Each person works from a local copy, copies drift apart, and eventually a customer receives last year's terms carrying this year's date. Version control by convention is not version control; it is an assumption that everyone checked.

KhatimDoc Delivers

A Governed Library, Not a Shared Folder. The central document gallery holds master agreements, standard forms and policy documents as a single source of truth, searchable by name, tag, department or metadata and available to every authorised user without re-upload. Organisation-level items are published centrally while teams maintain their own, and both are stored with the same encryption, access logging and audit trail as documents in active packages. Selecting from the gallery is faster, and more importantly it makes sending a superseded version a deliberate act rather than an accident.

Templates That Carry the Whole Configuration.

A template fixes documents, recipients, roles, rights, field placement and agreement notices in advance, so a recurring transaction becomes a matter of changing what differs and sending. Contacts are maintained at organisation and team level so recipients need never be retyped. Onboarding an employee, issuing a supplier agreement or executing a standard renewal collapses from a sequence of assembly steps into one action, and every instance is configured identically because it was configured once, by somebody who was paying attention.

- Central gallery with search, tagging and metadata for frequently used documents
- Organisation-wide and team-level galleries, templates, contacts and agreement notices
- Templates carrying documents, recipients, roles, rights and field placement
- Same encryption, access control and audit trail as documents in active packages

The screenshot shows the KhatimDoc web application interface. The top navigation bar is green with 'KhatimDoc' on the left, 'HOME', 'PACKAGES', and 'SETTINGS' in the center, and a search bar and user profile 'MK' on the right. A sidebar on the left contains a 'START NOW' button, 'Inbox', 'Sent', 'Drafts', and a 'FILTERS' section with 'Pending' (2), 'Waiting for Others', 'Declined', 'Cancelled', and 'Completed'. The main content area is titled 'Pending' and shows a table of documents. The table has columns for 'Packages', 'Status', and 'Updated'. Two documents are listed: 'SAMPLE CONTRACT AGREEMENT' and '1 page, Employment application - Duplicate'. Both are in 'Pending' status and have a 'SIGN' button.

Packages	Status	Updated
SAMPLE CONTRACT AGREEMENT Muhammad Wahaj, To: Ahmad	Pending	2023-05-23 01:54:49
1 page, Employment application - Duplicate Shahid, To: Wahaj, Shahid	Pending	2023-04-08 01:26:21

Proving They Knew What They Were Signing

The Challenge: Consent Is the Part That Gets Disputed

Signature challenges rarely turn on cryptography. They turn on whether the signer understood the terms, whether disclosure was made before agreement rather than after it, and whether the person who opened the document was the person the sender intended. A signing link forwarded to a shared mailbox, terms displayed after the signature was applied, a disclosure nobody can prove was ever shown — these are the failures that unwind an agreement, and not one of them is detected by verifying the signature itself.

KhatimDoc Delivers

Disclosure Before Agreement, Recorded.

Document owners configure agreement notices presented to recipients before a document can be opened or signed, with acceptance captured as part of the transaction record. A notice may carry terms of use, regulatory disclosure, processing conditions or instructions specific to the package. What results is not merely a signature but an evidenced sequence: the recipient was shown the notice, accepted it, and then signed — which is the sequence regulators such as FDA 21 CFR Part 11 expect to see documented rather than asserted.

The Right Person, Within the Right Window.

Access to a package can be conditioned on a document access PIN, a one-time password delivered by email, or a private notice visible only to the intended recipient, and can be confined to a defined period after which the link no longer opens. Rights are further constrained by role, so who may view, sign, approve or initiate is governed explicitly rather than implied by possession of a URL. Access attempts, successful and otherwise, are logged against the package alongside every other action.

-
- Configurable agreement notices displayed and accepted before document access
 - Document access PIN and email one-time password authentication
 - Private recipient notices and time-limited package access
 - Consent, access and rights events recorded in the package audit trail

A Document You Do Not Hold Is Governed by Someone Else's Terms

The Challenge: Cloud Signing Moves Your Most Sensitive Documents Off-Site

The documents an organisation signs are precisely the ones it can least afford to lose control of — employment terms, settlements, board resolutions, pricing, patient consent, national contracts. Cloud e-signature services store all of it on infrastructure the customer does not operate, in a jurisdiction the customer did not select, under terms the provider may revise. Retention, disclosure obligations, breach exposure and continuity all become somebody else's decisions. For many regulated and public sector organisations that is not a preference; it is a disqualification.

KhatimDoc Delivers

Deployed Inside Your Own Perimeter.

KhatimDoc installs on your infrastructure — on-premise, in a private cloud, on virtual or physical machines, on Windows or Linux — so documents, keys, audit logs and user data remain within your network and your legal jurisdiction. There are no third-party custody of signed instruments and no dependency on an external service remaining available, solvent or contractually agreeable. Where connectivity is constrained or deliberately absent, signing continues to operate within the organisation's own network.

Sovereignty as an Architectural Property.

Because the deployment is yours, data residency, retention periods, backup policy, disaster recovery and encryption at rest are governed by your own standards rather than negotiated as service tiers. Documents are stored under AES-256 encryption with access logging that your auditors inspect directly rather than request. Hybrid arrangements remain available where they suit — cloud key management through Azure Key Vault or AWS KMS, or an external timestamp authority — but they are choices made connector by connector, not conditions of use.

- On-premise, private cloud, virtual or physical deployment on Windows or Linux
- Documents, keys, logs and user data retained within your network and jurisdiction
- AES-256 encryption at rest with retention and backup under your own policy
- Optional hybrid use of cloud key management or external timestamping

PILLAR 07 · MULTI-TENANCY, ROLES, RIGHTS & WHITE-LABEL BRANDING

Many Businesses, Many Brands, One Instance

The Challenge: An Enterprise Is Not a Single Organisation

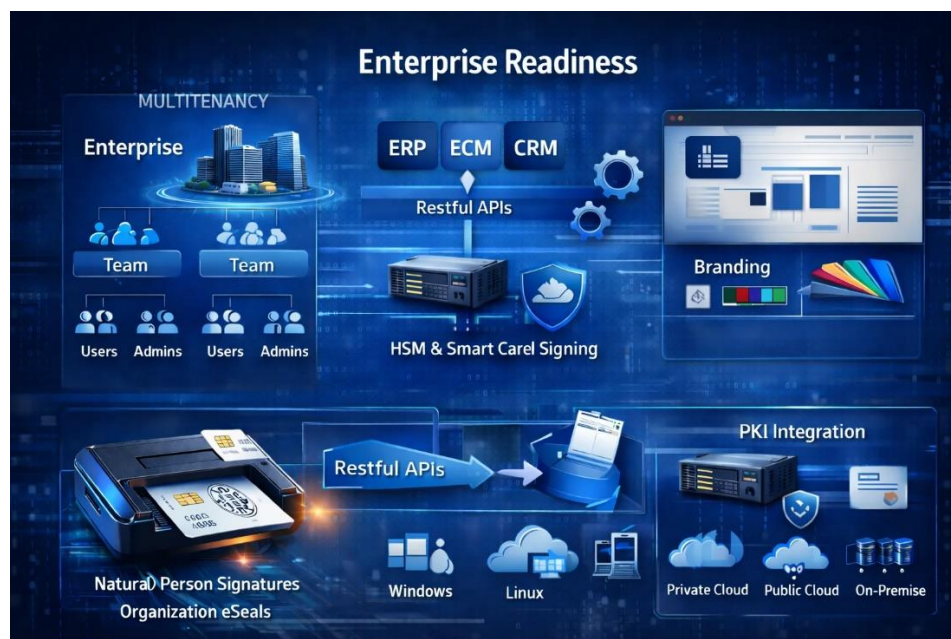
A group with six subsidiaries, a ministry with twelve agencies or a service provider with forty customers cannot operate from one flat account list. Each unit needs its own templates, contacts, notices and signing rules, its own administrators, and frequently its own identity in front of external signers. Solved by deploying separate instances it becomes six upgrade cycles and six sets of certificates. Solved by sharing one account it becomes a governance problem with a support ticket attached to it.

KhatimDoc Delivers

Hierarchy That Matches the Organisation. A single KhatimDoc instance hosts multiple enterprises, each containing multiple teams, each managing its own users, contacts, templates, agreement notices and document gallery — while organisation-level policies and global templates apply across all of them. Rights are assigned through defined roles: enterprise administrators, team administrators, business users and view-only users, governing document access, signing rights, workflow initiation, approval authority and time-bound access.

Your Brand on the Most Trust-Sensitive Email You Send. A signature request is the moment a counterparty decides whether a message is legitimate or a phishing attempt. White-labelling applies your logos, theme colours, interface styling and email notification branding to the portal and to every communication a signer receives, configured per enterprise rather than per installation. A holding company presents each subsidiary under its own identity and a service provider presents its customers under theirs, from one deployment and one maintenance cycle.

- Multiple enterprises and teams on a single instance with independent configuration
- Enterprise admin, team admin, business user and view-only roles with granular rights
- Service plans, provisioning and PKI integration governed from the Khatim Admin Portal
- Per-tenant logos, theme colours, interface and email notification branding



PILLAR 08 · KEY MANAGEMENT & CRYPTOGRAPHIC AGILITY

Where the Signing Key Lives Is the Whole Security Argument

The Challenge: A Signature Is Only as Protected as the Key Behind It

Every assurance a digital signature offers rests on one assumption: that nobody but the named signer could have produced it. That assumption fails quietly if the private key sits in a software store on a laptop, is held by a service provider under operational controls the customer has never seen, or is protected by a policy nobody has audited. Meanwhile the algorithms have a shelf life of their own. Key sizes deprecate, hash functions weaken, and regulators revise what they accept. A platform that fixes either decision at installation has made a commitment it cannot revisit.

KhatimDoc Delivers

Keys Held Where Policy Requires. KhatimDoc places signing keys wherever the organisation's security posture dictates: on smart cards or cryptographic USB tokens for local signing by named individuals, in a PKCS#11 HSM appliance for hardware-backed server-side signing and eSeals, or in Azure Key Vault or AWS KMS where cloud-managed custody is preferred. Different signature types route to different key stores through the connector architecture — smart cards for staff, HSM-backed keys for organisational seals, cloud KMS for automated workflows — all within one deployment.

Certificates and Algorithms Under Your Control. Integration with Khatim PKI Server brings certificate issuance, revocation and lifecycle management inside the same estate, so signer credentials are provisioned and withdrawn under your governance rather than purchased per signature from an external provider. Supported algorithms span RSA (2048, 4096, 8192), ECDSA across the standard curve families, and SHA-256, SHA-384 and SHA-512 hashing, changed at connector or policy level without redeployment — so an algorithm migration becomes just a configuration change.

- Smart card, USB token, PKCS#11 HSM, Azure Key Vault and AWS KMS key custody
- Certificate issuance, revocation and lifecycle through Khatim PKI Server integration
- RSA (2048, 4096, 8192), ECDSA and SHA-256 / SHA-384 / SHA-512 support



Every Signature Answers for Itself

The Challenge: Nobody Knows Where the Contract Is

Between sending a document and receiving it back executed, most organisations have no information at all. Whether the recipient opened it, whether it waits on the second signer or the fourth, whether it was declined a week ago and the reason sits unread in somebody's inbox — none of it is visible, so it is chased manually or not at all, and deals slip on inaction rather than disagreement. Then, when an executed agreement is challenged, the evidence needed to defend it must be assembled from systems that were never asked to retain it.

KhatimDoc Delivers

The Package Tells You Where It Is. Owners see live package state, which recipients have viewed, signed, approved or declined, the reason given for any decline, and the date and time of every action, from the package summary rather than from follow-up calls. The built-in notification engine reminds recipients by email of documents awaiting them and alerts owners on completion or exception, so progress depends on the system rather than on somebody remembering to chase it before the end of the quarter.

A Record Built for Challenge. Every action against a package is recorded with full cryptographic traceability: signer identity, certificate serial and issuer, signing time, algorithm identifier, signing method, originating IP address and validation status, together with document version and access history. The consolidated audit trail is viewable from the package summary and exportable for compliance, dispute resolution and regulatory inspection — which is what turns a signed PDF from an assertion into evidence a third party can independently assess.

-
- Live package state with per-recipient viewed, signed, approved and declined status
 - Decline reasons, timestamps and access history retained against the package
 - Email and SMS reminders to recipients, completion and exception alerts to owners
 - Exportable audit trail with certificate, algorithm, time and IP detail per action

Signing Belongs Inside the Process, Not Beside It

The Challenge: The Signing Step Is Where the Automation Stops

An onboarding workflow runs in the HR system, an award runs in procurement, a renewal runs in the core platform — and then a person exports a PDF, opens a separate signing portal, uploads it, retypes the recipients, and later downloads the result and files it back by hand. The automated process has a manual hole in the middle of it, positioned exactly at the step that carries legal weight. Every document passing through that hole is an opportunity for the wrong version, the wrong recipient, or no record at all.

KhatimDoc Delivers

Signing as an API Call. KhatimDoc exposes RESTful APIs covering user enrolment, package creation, document submission, workflow initiation, status query and signed document retrieval, so ERP, ECM, CRM and custom applications can initiate and complete signing without a human intermediary. Webhook callbacks notify the calling system when a package completes or fails, allowing post-signature processing — filing, ledger updates, account provisioning — to run automatically. Sample developer artefacts supplied with the installation shorten the first integration considerably.

Deployable Wherever the Estate Already Runs.

The platform is independent of operating system and hosting model: Windows Server or Linux, on-premise, private or public cloud, virtual or physical machines, with high-availability deployment across multiple instances behind a load balancer. The user portal runs in any modern browser with no client installation on the signer's machine, and the interface is available in over fifty languages, so distributed organisations and external counterparties work in their own language without separate deployments.

-
- REST APIs for enrolment, package creation, workflow initiation, status and retrieval
 - Webhook callbacks driving automated post-signature processing
 - Windows and Linux, on-premise, private or public cloud, virtual or physical machines
 - Browser-based portal with no client installation, in over 50 languages

AT A GLANCE

Everything Else KhatimDoc Does

Beyond the ten pillars, KhatimDoc carries the operational detail that enterprise signing depends on day to day.

Built-in Document Viewer Review and sign in the browser with no download, plug-in or external application.	Form Fields & Initials Text, date, number, list and checkbox fields plus initials placed anywhere in the document.
Quick Filters & Package Search Locate packages by state, recipient, template or date directly from the dashboard.	50+ Interface Languages English, Arabic, Chinese, French, Spanish, German, Portuguese, Italian, Russian and more.
AES-256 Document Encryption Documents encrypted at rest within your own storage under your own key management.	Retention & Versioning Lifecycle rules and version control maintaining provenance and preventing unauthorised reuse.
Email & SMS Notifications Configurable reminder cadence for pending recipients and alerts for package owners.	Offline Availability Full operation within the corporate network without dependency on internet connectivity.
Connector Architecture Certificate provider, signing and timestamp connectors configured independently per enterprise.	Decline with Reason Recipients record why a document was rejected, captured against the package audit trail.
Service Plans Feature and volume entitlements assigned per enterprise for multi-tenant operation.	Sample Developer Project Reference integration supplied with the installation to accelerate first deployment.

COMPARISON 01 · DEPLOYMENT & CONTROL

Self-Hosted or SaaS: Where Your Documents Actually Live

A signing platform is not only a set of features; it is a decision about custody. The comparison below sets out what changes when signed instruments, keys and audit records remain inside your organisation rather than on infrastructure operated by somebody else.

Dimension	KhatimDoc — Self-Hosted	Typical SaaS e-Signature Service
Deployment Model	On-premise, private cloud or public cloud, operated entirely by your organisation.	Vendor-hosted multi-tenant cloud, operated by the provider.
Data Residency & Control	Documents, metadata and audit logs never leave your network or your jurisdiction.	Stored on provider infrastructure in regions the provider selects.
Attack Surface	Confined to your own perimeter and governed by your own security controls.	Sensitive documents aggregated on an external, high-value target.
Compliance Jurisdiction	Aligned to your national and sector regulation by virtue of deployment.	Bounded by the provider's hosting jurisdiction and contractual terms.
Customisation	Configurable to organisational process, branding and integration requirements.	Limited to the options the vendor chooses to expose.
Enterprise Integration	Direct in-network integration with ERP, ECM and CRM systems.	Cloud-first integration, often requiring additional security review.
Offline Availability	Operates within the corporate network without internet connectivity.	Requires internet connectivity for substantially all operations.
Backup & Recovery	Your policies, your schedules, your retention periods, your restore testing.	Predefined provider protocols and fixed retention windows.
Cost Model	Perpetual licence with predictable annual maintenance.	Recurring subscription tied to seats, envelopes or transaction volume.

COMPARISON 02 · CAPABILITY

Feature Comparison

KhatimDoc matches mainstream e-signature services on the workflow features buyers expect as standard. The difference appears in the cryptography, the key custody and the deployment model — which is where the legal weight of a signature is actually decided.

Capability	KhatimDoc	Typical SaaS Service
Built-in workflows (serial and parallel)	Yes	Yes
e-Signatures and form filling	Yes	Yes
Templates and document tracking	Yes	Yes
User portal and central document gallery	Yes	Yes
Built-in document viewer	Yes	Yes
Advanced digital signatures (PAdES)	Yes	Typically eSeal only, not natural person signing
Native validation in Adobe Acrobat Reader	Yes	Often requires the vendor's own portal
Local signing with smart cards or USB tokens	Yes	Rarely supported
Cryptographic agility (RSA, ECDSA, curve selection)	Yes	Commonly RSA only
Self-hosted deployment	Yes	Cloud only
White-label branding per tenant	Yes	Typically a single brand
Licensing model	Perpetual, paid once	Ongoing subscription

Comparison reflects the capabilities commonly offered by mainstream cloud e-signature services. Individual vendors may differ, and specific tiers may offer additional assurance levels.

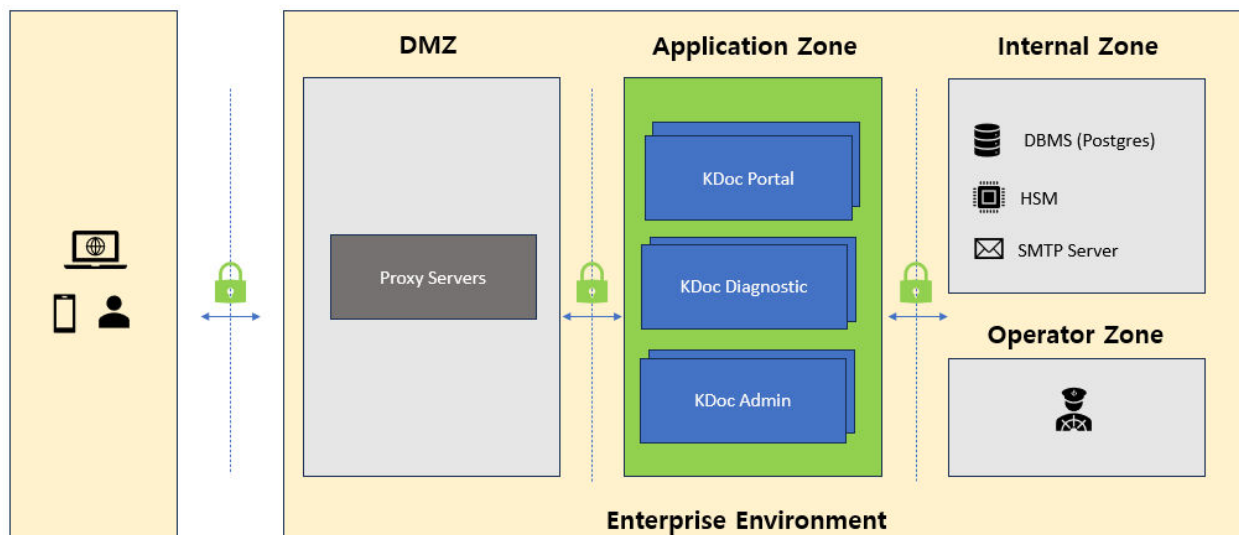
KhatimDoc Architecture

KhatimDoc is a self-hosted enterprise signing platform providing e-signatures, natural person digital signatures and organisational seals to business users, applications and external counterparties. It is built from four core components:

- **KhatimDoc Web Portal**, through which business users assemble packages, place form and signature fields, sign, approve and track progress, and through which external recipients complete the documents sent to them
- **KhatimDoc API**, which delivers RESTful services for enrolment, package creation, workflow initiation, status query and signed document retrieval to ERP, ECM, CRM and custom applications
- **KhatimDoc Admin**, through which enterprises are onboarded and bootstrapped, service plans defined, roles and rights configured, and certificate provider, signing and timestamp connectors established
- **KhatimDoc Storage**, which holds encrypted documents, templates, the document gallery, contacts, configuration, audit records and transactional data

The processing flow is straightforward:

- A package owner assembles documents from upload, the central gallery or a template, and defines recipients, roles, fields and signing mode
- KhatimDoc distributes the package, applying agreement notices, access PINs or one-time passwords where the configuration requires them
- Recipients authenticate, complete form fields and apply e-signatures, digital signatures or approvals within the browser
- KhatimDoc invokes the configured signing connector, producing the signature from a smart card, HSM, Azure Key Vault or AWS KMS held key, and applies an RFC 3161 timestamp where the signature profile requires one
- The completed package is stored encrypted with the full audit record retained, and webhook callbacks notify the calling application that processing has finished



“

We recently had the pleasure of working with the talented team at Codegic to develop an e-signing platform. From the initial consultation to the final delivery, Codegic's team was attentive to our needs and consistently went above and beyond to ensure the success of the project. Their knowledge of the latest technologies and industry best practices was evident in every aspect of their work, and they were able to deliver a high-quality product that met all of our requirements.”

Calvin Tan | Director, Hiend Software Pte Ltd. Singapore



 Algorithms / Protocols	 Supported OS / Languages / H/W
• RSA (2048, 4096, 8192) • ECDSA (192, 224, 256, 320, 384, 512) • SHA-256, SHA-384, SHA-512 • PAdES-BES, PAdES-T, PAdES-LT; PKCS#7 / CMS • PKCS#11, REST, HTTP, HTTP/s, LDAP, SMTP, SMPP, Syslog • Key stores: Smart card, USB token, PKCS#11 HSM, Azure Key Vault, AWS KMS • Standards ○ ETSI EN 319 142 (PAdES), ISO 32000 ○ RFC 3161, RFC 5280, RFC 6960 ○ eIDAS — Regulation (EU) 910/2014 ○ ESIGN Act, UETA ○ HIPAA, FDA 21 CFR Part 11	• All flavours of Windows Server & Linux (Centos Stream, Ubuntu, RedHat, Fedora) • 50+ languages including English, Arabic, French, Spanish, Chinese, German, Portuguese, Italian, Russian & more • 8 GB RAM, 2 vCPU (2.3 GHz), 10 GB hard disk • Oracle, PostgreSQL • Integrates with Khatim PKI Server and Khatim Timestamp Server

Codegic is a security provider specialising in innovative PKI and Digital signatures products and services. Codegic delivers easy to use PKI products for areas like PKI, Document Signing, Timestamping, PKI Monitoring, Digital Certificates issuance and more. We utilise all the latest technologies to help companies and enterprises solve complex security issues that always emerge during their digital evolution journey.

Contact Us Today to see KhatimDoc in action

Facilitating Digital Trust by providing World-Class PKI & Digital Signature Solutions

info@codegic.com

www.codegic.com

USA | UAE | PAK
ISO 27001 · 9001 · 14001 Certified

