codegic

Trusted Signature Validation & Long-Term Proof

Khatim Verification Server

ETSI and eIDAS compliant signature validation authority delivering policy-driven, long-term verification of advanced electronic signatures at enterprise scale

8 Formats
AdES, ASiC, PKCS, C2PA
One validation engine

EU LOTL
Trusted Lists
eIDAS out of the box

LTV
Proof That Outlives Keys
Archive-grade evidence

PQC
ML-DSA Ready
Future-proof verification

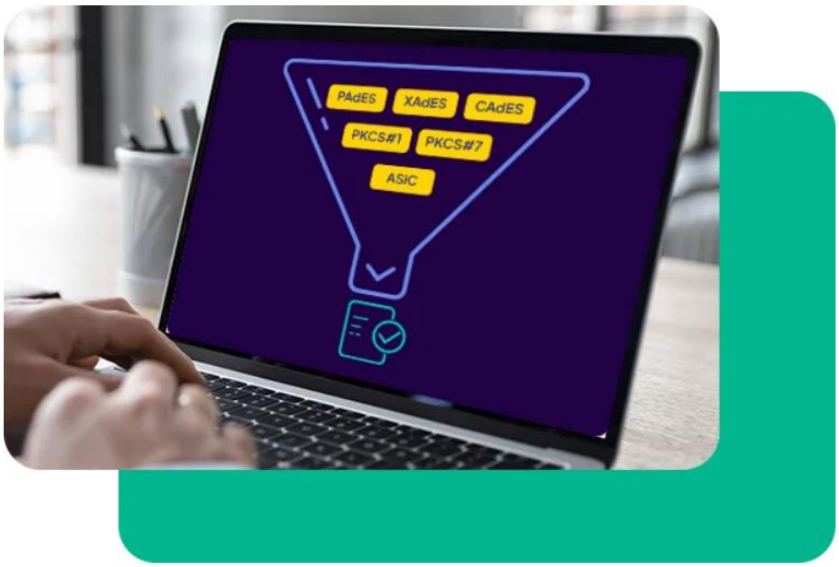
Digital signature validation made conclusive!

Khatim Verification Server is where a signed document stops being a claim and becomes evidence — the layer that establishes not merely that a signature computes, but that it can be trusted, and still proven years from now. It carries the trust anchoring, revocation checking, policy enforcement and long-term evidence collection that turn a cryptographic check into a defensible legal conclusion.

- Enterprise ready, standards-compliant and quick to deploy signature validation service
- Compliant with eIDAS, ETSI EN 319 102-1 validation procedures and IETF signature standards
- Validates PAdES, XAdES, CAdES, JAdES, ASiC and PKCS signatures, plus C2PA content credentials, from one engine
- Trust anchored to the EU List of Trusted Lists or your own custom stores
- Long-term validation with revocation, timestamp and trust path evidence collected and retained
- Advanced verification insights, live reporting and proactive alerting built in

Khatim Verification Server Supports:

- ETSI EN 319 102-1 — procedures for the validation of AdES digital signatures
- ETSI TS 119 102-2 — standardised signature validation reports
- ETSI EN 319 142 — PAdES for PDF documents
- ETSI EN 319 132 — XAdES for XML data and e-invoices
- ETSI EN 319 122 — CAdES for binary content
- ETSI TS 119 182 — JAdES for JSON and API payloads
- ETSI EN 319 162 — ASiC signature containers
- ETSI TS 119 612 and TS 119 615 — Trusted Lists and their interpretation
- eIDAS — Regulation (EU) 910/2014 and Regulation (EU) 2024/1183
- RFC 5280, RFC 5652, RFC 6960, RFC 3161 and FIPS 204 ML-DSA verification
- C2PA — content credentials and provenance manifests for images and video



Nine Pillars of Trusted Signature Validation

01

Every Advanced Signature Format
PAdES, XAdES, CAdES, JAdES, ASiC and PKCS parsed and validated by one engine, so no format needs a verification tool of its own.

02

Content Provenance & C2PA
Content credentials in images and video validated end to end, with manifest integrity, trust chains and ingredient analysis exposing how media was actually made.

03

EU Trusted Lists & LOTL
Trust anchored to the European List of Trusted Lists or your own custom stores, refreshed and monitored automatically.

04

Verification Policies You Control
Accepted algorithms, key sizes, formats and trust sources defined per policy, so each application validates to the rules that actually govern it.

05

Revocation & Trust Path Building
Full chain construction with OCSP and CRL checking for every signer, timestamp and responder certificate found in the signature.

06

Long-Term Validation
Signatures stay provable after certificates expire, algorithms weaken and issuers disappear, because the evidence is collected while it still exists.

07

Post-Quantum-Ready Verification
Cryptographic agility across RSA, ECDSA and PQC ML-DSA, so the verifier is ready before the first post-quantum signature arrives.

08

Verification Insights & Proactive Alerts
Live validation telemetry, trust list health and secure event delivery to Splunk, Grafana, Graylog and LogRhythm.

09

RBAC, Secure Administration & APIs
Least-privilege administrator, operator and auditor roles under TLS client authentication, with full REST API control for business applications.

PILLAR 01 · MULTI-FORMAT SIGNATURE VERIFICATION

One Engine for Every Signature You Receive

The Challenge: Every Format Is a Different Problem

A PDF signed in Germany, an XML invoice from Italy, a JSON payload from an API gateway and a CAdES-signed archive from an enterprise are four different parsing problems wearing one label. Organizations that solve them one at a time accumulate a library here, an open-source utility there, and a vendor SDK nobody has updated since the developer who chose it left. Each behaves differently at the edges, and the edges are precisely where invalid signatures hide. A signature accepted by one tool and rejected by another has not been verified — it has merely been processed.

Khatim Verification Server Delivers

Every Format, One Validation Engine. Khatim Verification Server validates PAdES for PDF, XAdES for XML, CAdES for binary content, JAdES for JSON and API payloads, ASiC containers for packaged evidence, and PKCS#7/CMS and PKCS#1 hash signatures for everything built before the AdES family existed. All of it runs through a single engine, one policy set, one audit trail and one administration console. The receiving application submits a document and receives a verdict, without needing to know which standard the sender chose. Media files carrying C2PA content credentials are validated by the same engine under the same policies.

Structure Understood, Not Just Bytes Checked. Verification goes past the cryptographic digest into the structure of the signature itself: signed and unsigned attributes, signing certificate references, commitment types, signature policy identifiers, counter-signatures, multiple and sequential signers, and incremental updates in signed PDFs. Conformance level is determined and reported — B-B, B-T, B-LT or B-LTA — so a relying party can tell a bare signature apart from one carrying its own long-term evidence.

- PAdES, XAdES, CAdES, JAdES, ASiC, PKCS#7/CMS and PKCS#1 in one engine
- Multiple, parallel and counter-signatures resolved and reported individually
- Conformance level detected and reported from B-B through B-LTA
- Detailed per-signature validation reports suitable for audit and dispute resolution

PILLAR 02 · CONTENT PROVENANCE & C2PA VERIFICATION

Know Where the Image Actually Came From

The Challenge: Synthetic Media Is Indistinguishable by Inspection

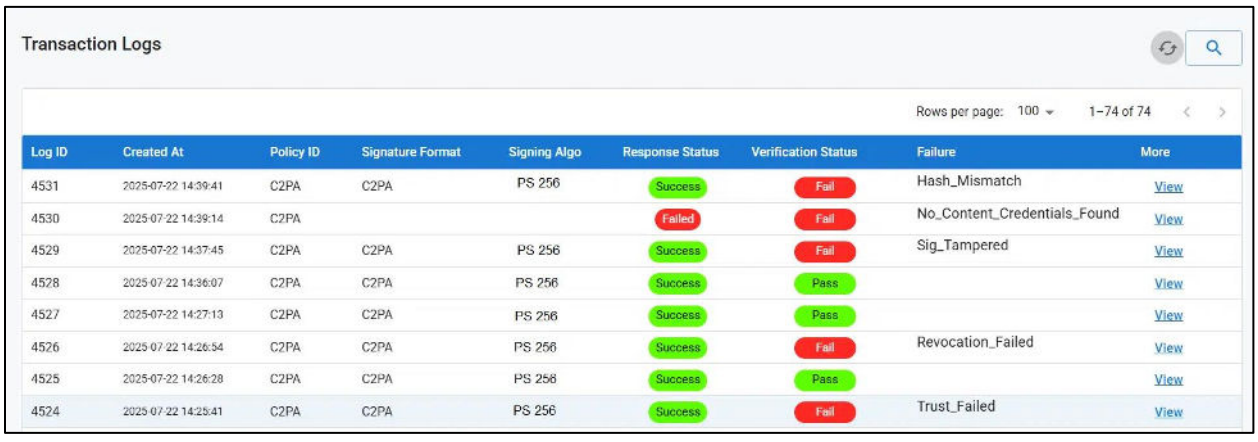
A generated image and a photograph are the same thing to a viewer, and increasingly the same thing to a trained reviewer. Newsrooms publish supplied footage. Legal teams submit photographic exhibits. Brands run campaigns on assets that passed through four agencies and an AI editing tool. Watermarks are stripped, metadata is discarded on upload, and reverse image search proves nothing about what was altered inside the frame. Judging authenticity by looking harder is not a control; it is a hope that the forger was careless.

Khatim Verification Server Delivers

Provenance, Verified Cryptographically. C2PA embeds a digitally signed manifest inside the media file recording who captured or edited it, when, and with which tool. Khatim Verification Server first detects whether content credentials are present at all, then validates the manifest signature, builds and validates the certificate chain to a configured trust anchor, checks revocation over CRL and OCSP, and confirms manifest integrity. Ingredient analysis walks the chain of custody through multi-layered edits and composited sources, so a file assembled from several origins is reported contributor by contributor rather than as a single verdict.

One Policy, Documents and Media Alike. C2PA verification is enabled inside the same verification policy that governs PAdES, XAdES, CAdES, JAdES and ASiC — one policy, one trust anchor configuration, one set of accepted algorithms, one audit trail. Media is submitted to the same REST endpoint as any signed document with the format declared in the policy parameters, and results return per manifest with issuer, certificate serial, algorithm and status: valid and active, valid as an ingredient, not validated, or no content credentials found. CMS, DAM, editorial and compliance systems receive the same response shape they already handle.

- Detects, validates and reports C2PA content credentials in images and video
- Manifest integrity, signature validation, chain building and CRL/OCSP revocation checking
- Ingredient analysis across multi-layered edits and composited sources
- C2PA and AdES formats governed by one verification policy and one REST endpoint



Log ID	Created At	Policy ID	Signature Format	Signing Algo	Response Status	Verification Status	Failure	More
4531	2025-07-22 14:39:41	C2PA	C2PA	PS 256	Success	Fail	Hash_Mismatch	View
4530	2025-07-22 14:39:14	C2PA			Failed	Fail	No_Content_Credentials_Found	View
4529	2025-07-22 14:37:45	C2PA	C2PA	PS 256	Success	Fail	Sig_Tampered	View
4528	2025-07-22 14:36:07	C2PA	C2PA	PS 256	Success	Pass		View
4527	2025-07-22 14:27:13	C2PA	C2PA	PS 256	Success	Pass		View
4526	2025-07-22 14:26:54	C2PA	C2PA	PS 256	Success	Fail	Revocation_Failed	View
4525	2025-07-22 14:26:28	C2PA	C2PA	PS 256	Success	Pass		View
4524	2025-07-22 14:25:41	C2PA	C2PA	PS 256	Success	Fail	Trust_Failed	View

PILLAR 03 · EU TRUSTED LISTS, LOTL & TRUST ANCHOR GOVERNANCE

Trust You Can Point At

The Challenge: Trust Is Not a Folder of Certificates

Most relying parties anchor trust in a local certificate store that grew by accident — anchors added to unblock a project, none ever removed, none owned by anyone in particular. Then a trust service provider loses qualified status and nothing changes locally. A signature arrives from a member state the organization has never dealt with and there is no answer at all. Meanwhile the European lists update on their own schedule, entirely independently of the trust store. A trust store nobody governs is not a statement of trust; it is an accumulation of past decisions.

Khatim Verification Server Delivers

Anchored to the Source of Truth. Khatim Verification Server retrieves the European List of Trusted Lists, verifies its signature, follows it into each referenced Trusted List and extracts every trust service entry with its type, status and status history. Lists are refreshed on schedule and their signatures re-verified on every fetch. Critically, the status of a trust service is evaluated as it stood at the time of signing rather than at the time of checking, so a signature made under a qualified service does not silently lose its standing when that service is later withdrawn.

Your Own Trust, Governed the Same Way. Not every signature originates in the European Union. Custom trust stores sit alongside the EU lists for national PKIs, government hierarchies, sector schemes and private enterprise CAs, and each verification policy selects which sources apply to it. Trust sources are versioned, attributable and auditable — every addition, removal and refresh recorded against the operator who made it. Administrators are alerted when a list fails to refresh or a trust service changes status, so trust drifts visibly rather than quietly.

- EU LOTL and Trusted Lists fetched, signature-verified and refreshed automatically
- Trust service status evaluated at time of signing, not time of checking
- Custom trust stores for non-EU and private hierarchies
- Alerts raised when a trust service changes status or a list fails to refresh

PILLAR 04 · VERIFICATION POLICIES & CRYPTOGRAPHIC CONTROL

Different Documents Deserve Different Rules

The Challenge: One Validation Rule Cannot Serve Every Document

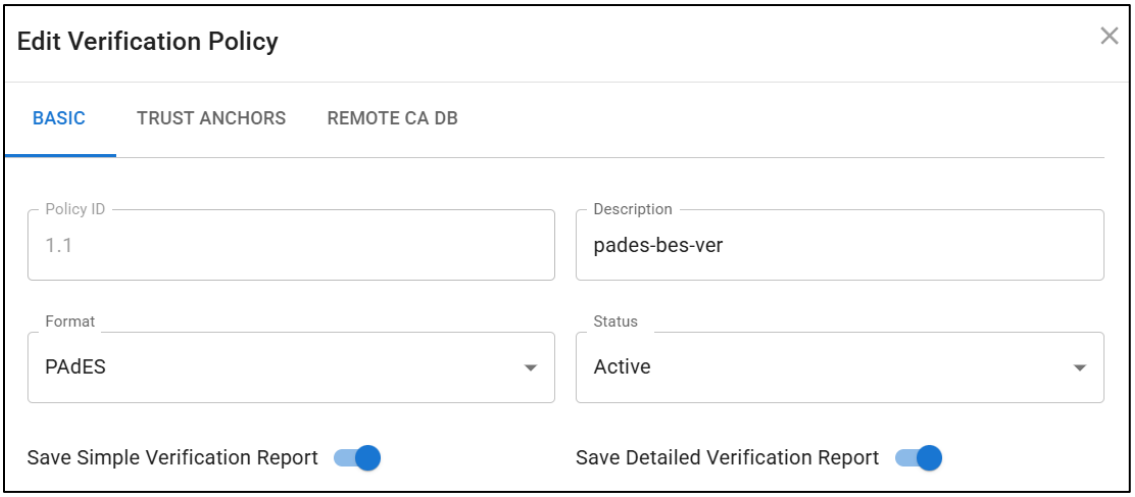
A single global verification setting is either too strict or too permissive, and it is usually both at once. Set it strictly and a decade-old archive signed with SHA-1 is rejected, along with the legal position that depended on it. Set it permissively and a 1024-bit RSA signature on a high-value contract returns the same reassuring green result as a qualified signature under a national scheme. The two documents carry entirely different consequences and are held to an identical bar. One verification setting forces the organization to choose which mistake it prefers.

Khatim Verification Server Delivers

Policy Per Application, Not Per Server. Verification policies are defined independently and bound to the applications, document types or jurisdictions that use them, so one deployment serves an HR onboarding workflow, a cross-border procurement portal and a records archive without compromise between them. Each policy fixes its own trust sources, accepted formats, required conformance level, timestamp requirement and revocation strictness. Adding a business use case is a policy definition rather than a second deployment.

Algorithms as an Explicit Decision. Accepted signature algorithms, minimum key sizes and permitted hash functions are stated per policy rather than inherited from a library default. A policy may require SHA-256 or stronger and RSA 3072 upward for new business, while an archive policy deliberately continues to accept legacy material and flags it as such in the report. Deprecation becomes a scheduled, documented change with a known blast radius instead of a surprise the day a dependency is upgraded.

- Unlimited verification policies bound to applications, document types or jurisdictions
- Accepted algorithms, minimum key sizes and hash functions set explicitly per policy
- Required conformance level enforced from B-B through B-LTA
- Identical policy enforcement whether the request arrives by REST API or portal



PILLAR 05 · REVOCATION CHECKING & PKI TRUST PATH BUILDING

A Valid Signature on an Untrusted Certificate Is Not Valid

The Challenge: The Cryptography Is the Easy Part

Confirming that a digest matches a signature value is arithmetic, and every library does it. The difficulty is everything around it: building a path from the signer's certificate to a governed anchor, and establishing revocation status not only for the signer but for each intermediate, for the timestamp authority's certificate and for the OCSP responder's own certificate. Weak implementations check the signer alone, check revocation as of today rather than as of signing, or treat an unreachable responder as an implicit pass. A verifier that fails open is worse than none, because it produces a green tick.

Khatim Verification Server Delivers

The Whole Chain, Every Certificate. Khatim Verification Server constructs the complete certification path from the signing certificate to a trust anchor governed by the applicable policy, resolving intermediates from the signature, from configured stores and from authority information access where permitted. Every certificate encountered on the way — signer, intermediates, timestamp authority and OCSP responder — is subject to the same revocation and profile checking under RFC 5280. Path construction reports which path was selected rather than leaving the conclusion unexplained.

Revocation at the Right Moment in Time. Revocation is meaningless without a time reference. Khatim Verification Server evaluates status as it stood at the moment of signing, using trusted timestamp evidence to fix that moment, so a certificate revoked long after a document was legitimately signed does not retrospectively invalidate it — and one revoked before signing is never quietly accepted. OCSP and CRL sources are used according to policy, responses are themselves validated, and an unreachable check is reported as indeterminate rather than passed.

- Full path construction from signing certificate to a policy-governed trust anchor
- OCSP (RFC 6960) and CRL checking for signer, timestamp and responder certificates
- Revocation evaluated at time of signing using trusted timestamp evidence
- Unreachable or inconclusive revocation reported explicitly, never silently accepted

Name	Value
Log ID	10
Created At	2026-07-23 14:03:27.248
Policy ID	1.1
Response Status	Success
Verification Status	Fail
Total Signature Count	1
Verification Failure Info	Trust_Failed
Signature Format	PAdES
Signing Algorithm	SHA256withRSAandMGF1
Request Processing Time	261 ms

PILLAR 06 · LONG-TERM VALIDATION & EVIDENTIARY DURABILITY

Provable Decades From Now, Not Only Today

The Challenge: Evidence Expires Faster Than Obligations

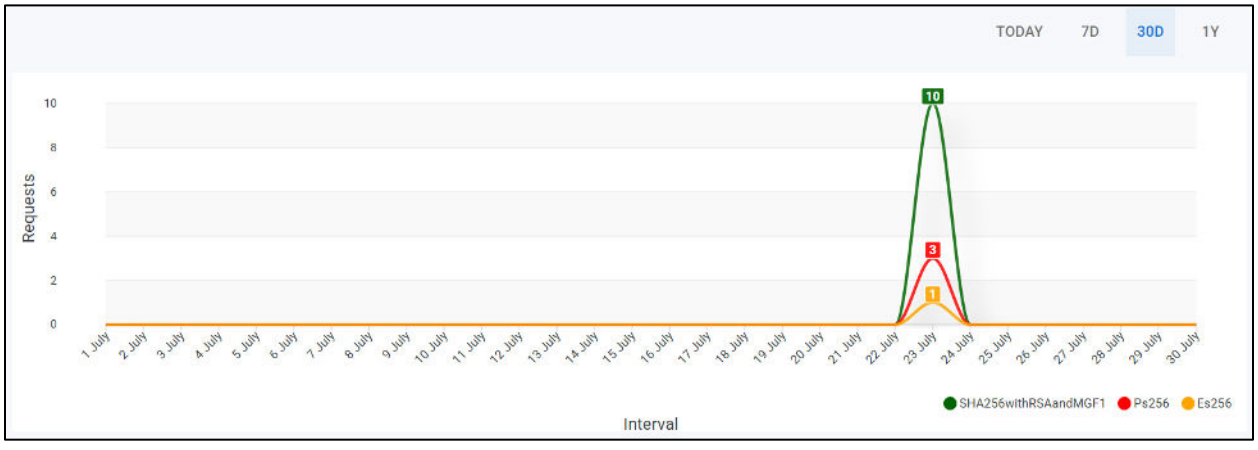
A signed contract might run thirty years, a medical record longer, a pension entitlement a working lifetime. The evidence supporting the signature on it does not. The signer's certificate expires within a year or two. The CRL that proved it was good was published for a week. OCSP responses are retained briefly by design. The issuing authority may be dissolved, its responders decommissioned, its hashing algorithm deprecated. The document survives intact and entirely unhelpful. The ability to prove it does not survive with it — unless somebody collected the proof while the proof still existed.

Khatim Verification Server Delivers

Proof Collected While It Still Exists. Khatim Verification Server performs full long-term validation of B-LT and B-LTA signatures, gathering the complete certification path, CRLs, OCSP responses and timestamp tokens that establish validity, and retaining that material against the transaction. Where signatures arrive without embedded evidence, validation material is collected at first verification and preserved, so a signature received today can be re-proven years after the responders that answered for it have gone. Archive timestamps are recognised and honoured.

Validated Against the Past, Not the Present. Historic validation reconstructs the trust position as it stood at the moment of signing: the trust service status then current, the certificates then valid, the revocation data then published, and the cryptographic acceptance rules then in force. A signature made lawfully in 2019 continues to validate as such in 2039, and a document is not devalued by the ordinary passage of time. The report records both the outcome and the evidence it rested on.

- Long-term validation of B-LT and B-LTA signatures with embedded revocation evidence
- Validation material collected and retained at first verification for later re-proof
- Archive timestamps honoured so signatures survive algorithm deprecation
- Historic validation reproduces the trust position as it stood at signing time



PILLAR 07 · CRYPTOGRAPHIC AGILITY & POST-QUANTUM VERIFICATION

The Verifier Has to Be Ready First

The Challenge: Verification Is Always the Trailing Edge

Post-quantum programmes plan for signing — new algorithms, new keys, new certificate profiles at the CA. Verification is assumed to follow, and it does not follow by itself. An ML-DSA signature has no value until the parties receiving it can validate it, which means every verifier in the chain must understand the algorithm before the first signature is ever produced. At the same time it must keep validating RSA and ECDSA for decades of archived material that will never be re-signed. Migration completes when everyone receiving a signature can verify it.

Khatim Verification Server Delivers

Classical and Post-Quantum, Side by Side. Khatim Verification Server validates signatures made with RSA (2048, 3072, 4096, 8192), ECDSA across the standard NIST, SECP and Brainpool curve families with SHA-256/384/512, and the NIST-standardised post-quantum signature algorithm ML-DSA (44/65/87). Classical and post-quantum signatures are parsed, path-built, revocation-checked and reported through the same engine and the same policies — no parallel estate and no second product.

Agility as a Policy Setting. Because algorithm acceptance is a property of the verification policy, each application migrates on its own timeline. A legacy archive continues accepting what it must while a new cross-border workflow requires post-quantum protection, and both are served by one deployment. Every transaction records the signature and hash algorithms actually encountered, turning verification traffic into a measured inventory of the cryptography your counterparties are really using rather than an assumption about the estate.

- RSA, ECDSA and PQC ML-DSA (44, 65, 87) signature verification from a single engine
- SHA-256, SHA-384 and SHA-512 with explicit control over legacy hash acceptance
- Per-policy algorithm eligibility for phased, verifier-safe migration
- Algorithm recorded per transaction for cryptographic inventory and CBOM reporting

PILLAR 08 · VERIFICATION INSIGHTS, REPORTING & PROACTIVE ALERTS

See Every Verification as It Happens

The Challenge: Failed Verifications Surface Somewhere Else

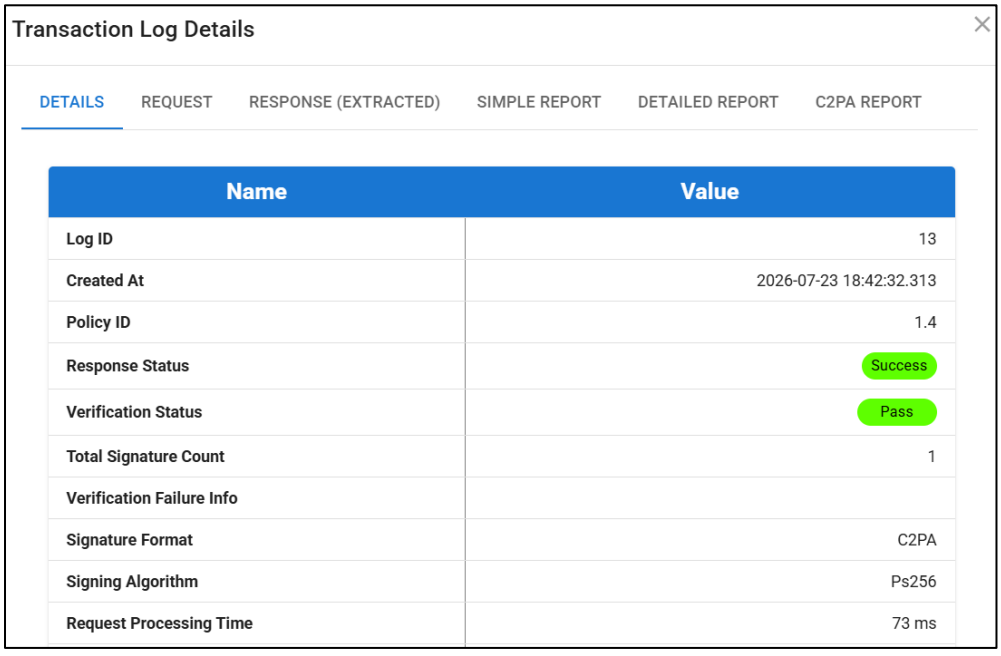
Verification fails quietly and the consequence appears elsewhere entirely. Nothing announces that a trusted list has failed to refresh for three days, that one partner's signatures began failing the morning they changed provider, that an OCSP responder has been unreachable since a firewall change, or that a policy tightened last month is now rejecting a document class nobody tested. The symptom presents as a stalled onboarding, a disputed invoice or a blocked filing. By the time a validation failure has a ticket number, it has been a business problem for a week.

Khatim Verification Server Delivers

Live Operational Visibility. Khatim Verification Server presents live and historical verification statistics through interactive dashboards covering successful, failed and indeterminate results, broken down by verification policy, signature format, signing algorithm, trust source and calling application. Administrators watch the whole estate from one screen or drill into a single transaction to inspect what was submitted, which path was built and what was returned. Automated daily summary reports deliver the same picture to inboxes without anyone logging in.

Alerts Before the Business Notices. When verification degrades — a trusted list refresh failing, an OCSP responder unreachable, a trust service withdrawn, a failure rate climbing for one application — administrators are notified proactively rather than discovering it through a support ticket. Every verification is logged with full cryptographic traceability including certificate chains, CRLs, OCSP responses, timestamps and trust list sources, and events are pushed securely into central logging and SIEM platforms including Splunk, Grafana, Graylog and LogRhythm.

- Live validation, failure and indeterminate telemetry in one console
- Filter by policy, signature format, algorithm, application and outcome
- Secure event delivery to Splunk, Grafana, Graylog and LogRhythm
- Automated daily summary reports emailed to administrators



PILLAR 09 · ROLE-BASED ACCESS CONTROL, SECURITY & APIs

Whoever Sets the Policy Decides What Counts as Valid

The Challenge: Changing the Configuration Changes the Answer

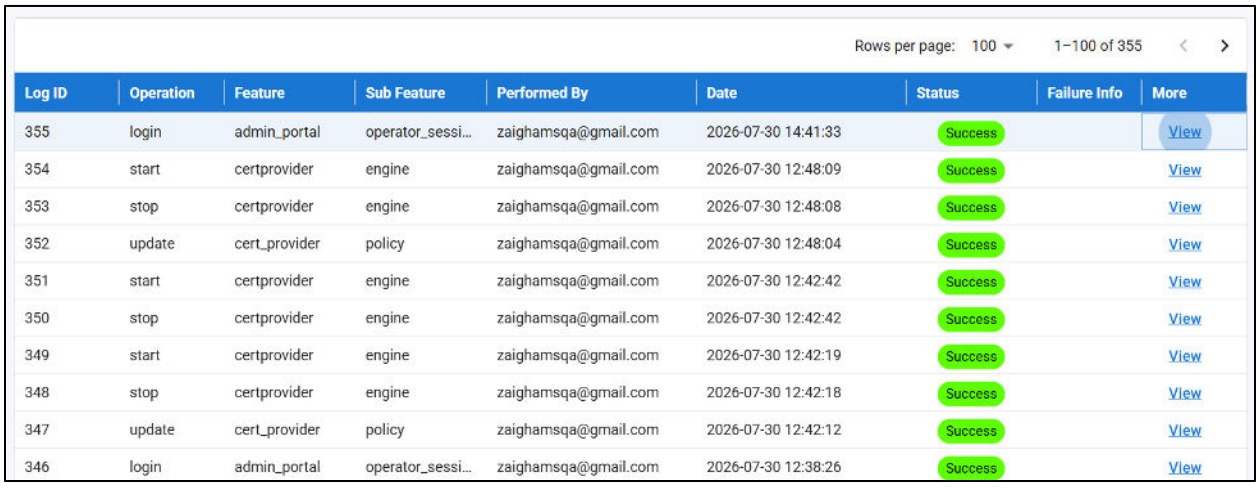
Anyone able to relax a verification policy, lower a minimum key size or add a trust anchor can cause an invalid signature to return a valid result — without touching a certificate, a key or a document. Yet daily operations draw many hands towards that console: integrators onboarding a new application, support staff investigating a rejected file, auditors sampling evidence, developers testing a workflow. Where privilege cannot be divided, everyone becomes an administrator by default. A verification result is only as trustworthy as the control over the configuration that produced it.

Khatim Verification Server Delivers

Least Privilege by Role. Access is granted through defined roles rather than a single shared level of power. Administrators govern policies, trust sources and system configuration; operators submit and review verifications; support and audit staff hold read-only visibility into transactions, reports and logs. Administrative access is protected by military-grade AES-256 and mutual TLS client authentication, and every configuration change — a policy edit, a trust anchor added, an algorithm accepted — is recorded against the operator who made it, with the previous state retained.

Full Control from Your Own Applications. Everything available in the portal is available over REST APIs secured by TLS client authentication — submitting documents and detached signatures for verification, selecting the verification policy, retrieving the detailed validation report, and querying transactions and statistics. ECM, CRM, CMS, ERP and workflow platforms call verification directly, so validating an incoming document becomes a step inside an existing business process rather than a separate system somebody has to remember to visit.

- Distinct administrator, operator and read-only audit roles
- AES-256 and mutual TLS client authentication for administrative and API access
- Full attributable audit trail across every policy and trust source change
- Complete REST API coverage for ECM, CRM, CMS and ERP integration



Rows per page: 100 1–100 of 355

Log ID	Operation	Feature	Sub Feature	Performed By	Date	Status	Failure Info	More
355	login	admin_portal	operator_sessi...	zaighamsqa@gmail.com	2026-07-30 14:41:33	Success		View
354	start	certprovider	engine	zaighamsqa@gmail.com	2026-07-30 12:48:09	Success		View
353	stop	certprovider	engine	zaighamsqa@gmail.com	2026-07-30 12:48:08	Success		View
352	update	cert_provider	policy	zaighamsqa@gmail.com	2026-07-30 12:48:04	Success		View
351	start	certprovider	engine	zaighamsqa@gmail.com	2026-07-30 12:42:42	Success		View
350	stop	certprovider	engine	zaighamsqa@gmail.com	2026-07-30 12:42:42	Success		View
349	start	certprovider	engine	zaighamsqa@gmail.com	2026-07-30 12:42:19	Success		View
348	stop	certprovider	engine	zaighamsqa@gmail.com	2026-07-30 12:42:18	Success		View
347	update	cert_provider	policy	zaighamsqa@gmail.com	2026-07-30 12:42:12	Success		View
346	login	admin_portal	operator_sessi...	zaighamsqa@gmail.com	2026-07-30 12:38:26	Success		View

Khatim Verification Server Architecture

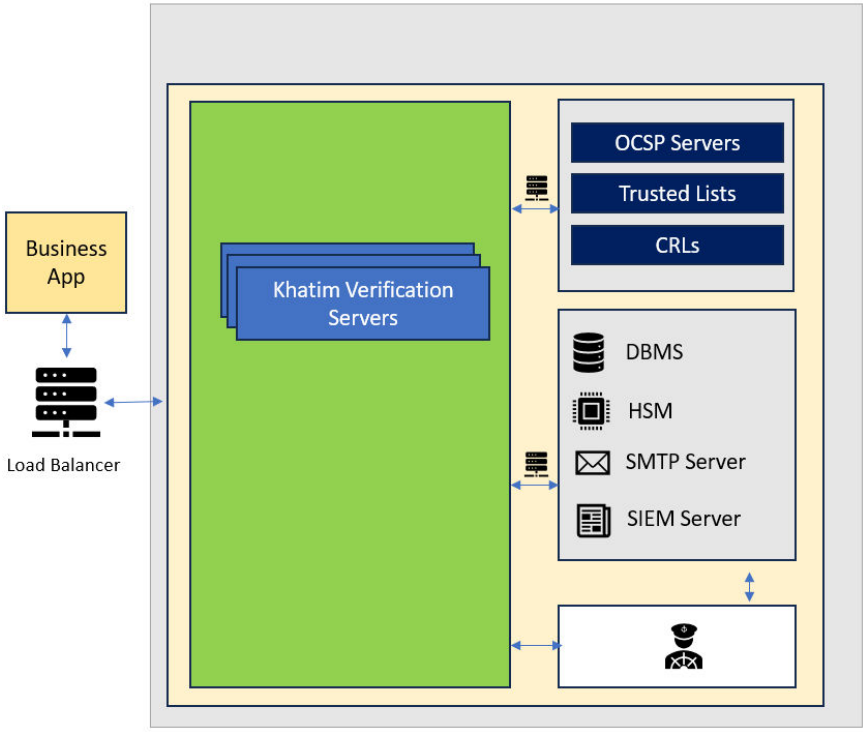
Khatim Verification Server (KVS) is a high-assurance signature validation authority providing policy-enforced verification of advanced electronic signatures for business applications, portals and archives. It is built from four core components:

- **Khatim Verification Portal**, through which administrators manage verification policies, trust sources and trusted lists, transactions, reports and statistics
- **Khatim Verification Engine**, which delivers RESTful verification services to business applications and performs parsing, path building, revocation checking and report generation
- **Khatim Verification Diagnostic**, which performs housekeeping, trusted list refresh, health checks, notifications and daily summary reporting
- **Khatim Verification Storage**, which holds configuration, trust sources, long-term validation material and transactional data

The processing flow is straightforward:

- A business application submits a signed document, detached signature or C2PA media file for verification through the REST API or the portal
- KVS authenticates the caller over OAuth and resolves the applicable verification policy
- KVS parses the signature, validates cryptographic integrity and builds the certification path to a governed trust anchor
- KVS performs revocation checking and trusted list evaluation at the time of signing, collecting long-term validation material
- KVS returns a detailed verification report and retains the full request, evidence and response record for audit

For high-volume and high-availability needs, KVS is deployed as a cluster of Verification Portal and Verification Engine instances behind a load balancer — additional servers can be added to the pool without stopping running instances. It runs on Windows and Linux alike, on-premise, in private or public cloud, on virtual or physical machines. Here is a basic deployment architecture for a Khatim Verification Server.



> *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*

hiend.

Algorithms / Protocols

- RSA (2048, 3072, 4096, 8192)
- ECDSA (NIST_P, SECP (K1,R1), BRAINPOOL (R1,T1) — 160, 192, 224, 256, 320, 384, 521)
- SHA-256, SHA-384, SHA-512; RSASSA-PSS (PS256, PS384, PS512)
- PQC — ML-DSA (44, 65, 87)
- PAdES, XAdES, CAdES, JAdES, ASiC-S / ASiC-E, PKCS#7 / CMS, PKCS#1, C2PA (content credentials)
- REST, HTTP, HTTP/s, LDAP, SMTP, SNMP, Syslog
- Conformance levels: B-B, B-T, B-LT, B-LTA
- **Standards**
  - ETSI EN 319 102-1, TS 119 102-2
  - ETSI EN 319 122 / 132 / 142 / 162, TS 119 182
  - ETSI TS 119 612, TS 119 615 (Trusted Lists)
  - RFC 5280, RFC 5652, RFC 6960, RFC 3161, RFC 5816
  - eIDAS — Regulation (EU) 910/2014 and (EU) 2024/1183
  - C2PA Content Credentials Specification — content provenance manifests
- **Trust Sources:** EU LOTL, Custom trust stores

Supported OS / Languages / H/W

- All flavours of Windows Server & Linux (Centos Stream, Ubuntu, RedHat, Fedora)
- 50 Languages including English, French, Spanish, Arabic, Chinese, Japanese, Italian, Polish, Swedish, Vietnamese, Russian & more.
- 8 GB RAM, 2 vCPU (2.3 GHz), 10 GB Hard disk
- Oracle, PostgreSQL

Codegic is a security provider specializing 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 Khatim Verification Server in action

info@codegic.com
www.codegic.com
USA | UAE | PAK
ISO 27001 · 9001 · 14001 Certified

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