codegic

Trusted Real-time Validation

Khatim OCSP Server

IETF and CA/B Forum compliant OCSP responder delivering real-time certificate validation at enterprise scale

1,000+
OCSP Responses/Sec
Built for Speed

5 RFCs
Full Protocol Coverage
6960, 5019, 2560, 4387, 5280

Multi-CA
One Deployment, Many PKIs
Online & Offline CAs

PQC
ML-DSA Ready
Future-proof validation

Certificate validation made simple!

Khatim OCSP Server is the Validation Authority at the centre of your digital trust estate, answering in milliseconds whether an X.509 certificate is still to be trusted. It removes the overhead of distributing and parsing large Certificate Revocation Lists and replaces it with a fast, scalable, auditable service that every relying party in your organization can depend on.

- Enterprise ready, secure and quick to deploy OCSP server
- Compatible with IETF RFC 6960 and 5019 standards and CA/B Forum requirements
- Real-time or CRL-based revocation for online, offline CAs and PKIs
- Manages multiple CAs and PKIs from a single OCSP deployment
- Advanced OCSP insights, live reporting and proactive alerting built in
- Signs every response with keys protected in an HSM or cloud KMS

Khatim OCSP Server Supports:

- RFC 6960 — Online Certificate Status Protocol
- RFC 5019 — Lightweight OCSP profile for high-volume environments
- RFC 2560 — Legacy OCSP client compatibility
- RFC 4387 — Certificate store access via HTTP
- CA/B Forum Baseline Requirements for response profiles
- Real-time revocation from the issuing CA
- CRL-based revocation over HTTP and LDAP
- Extended revocation information
- Multi-CA and multi-policy validation
- ML-DSA post-quantum response signing

Eight Pillars of Trusted Real-time Validation

01
Built for Speed
High-volume OCSP processing at 1,000+ TPS with clustered responders that scale out without stopping running instances.

02
IETF & CA/B Forum Compliance
Full RFC 6960, 5019, 2560 and 4387 coverage, so Adobe Acrobat, Microsoft Office, browsers and web servers validate revocation easily with no client-side change.

03
Serve Multiple CAs & PKIs
One deployment validates for many Certification Authorities - local, remote, online or entirely offline - each with its own policy and signing identity.

04
HSM-Backed Response Signing
Response signing keys stay inside certified HSMs over PKCS#11 or inside Azure Key Vault, AWS CloudHSM and Google Cloud HSM.

05
Post-Quantum-Ready Validation
Cryptographic agility across RSA, ECDSA and PQC ML-DSA, so your Validation Authority migrates alongside the CAs it serves.

06
OCSP Insights & Live Reporting
Real-time TPS and response-status telemetry across the cluster, deep historical trends and automated daily summary reports from a single pane of glass.

07
Proactive Alerts & SIEM Integration
Event alerts pushed securely to Splunk, Grafana, Graylog and LogRhythm, with email notification and daily digests for governance.

08
Access Control, RBAC & Unified GUI
Least-privilege operator roles with military-grade multi-factor TLS client authentication on every key function, a full attributable audit trail, and unified GUI administration.

PILLAR 01 · OCSP SERVER BUILT FOR HIGH-VOLUME VALIDATION

Answer Millions of Trust Questions in Milliseconds

The Challenge: Validation Sits on the Critical Path

Every TLS handshake, signed document, VPN login and smart-card authentication pauses while something asks whether a certificate is still trusted. That question sits directly on the critical path, so validation latency becomes application latency. Certificate Revocation Lists make this worse: as certificate populations grow into the hundreds of thousands, lists swell to sizes clients download slowly and parse badly. And when a responder saturates or becomes unreachable, relying parties either fail closed and block legitimate business, or fail open and accept certificates nobody has actually checked.

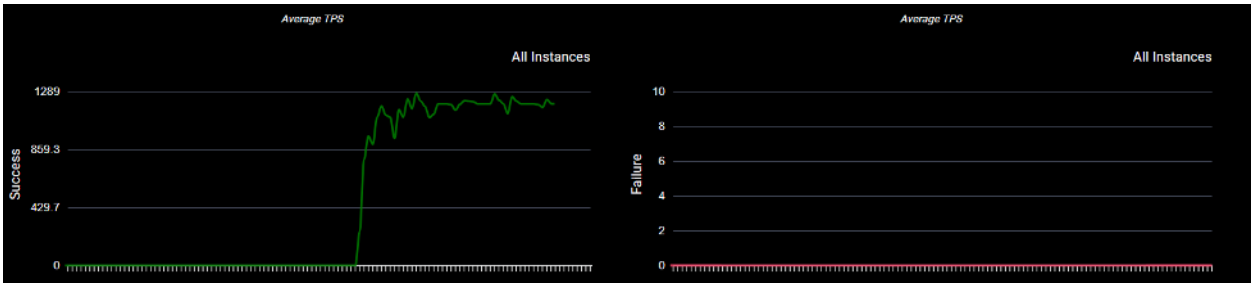
Khatim OCSP Server Delivers

Market-Leading Throughput. Khatim OCSP Server is engineered for high-volume processing, sustaining 1,000+ responses per second with RSA 2048. Responses return in milliseconds rather than the tens of seconds a large CRL download and parse consumes, keeping certificate validation invisible to users and off the critical path of your business transactions.

Drop-In Upgrade Path. Replacing an ageing responder should not mean rebuilding your trust model. Khatim OCSP Server imports and reuses your existing OCSP signing keys and certificates, so relying parties keep validating against the same responder identity while the performance bottleneck disappears behind it. No client-side change, no re-issuance exercise, and no coordinated cutover across every application in the estate.

Cluster Out, Never Down. Multiple instances form a cluster behind a load balancer to minimize latency and absorb peak demand. New responders join the pool without stopping running instances, so capacity grows during business hours and maintenance never means a validation outage. Deploy on-premise, in private or public cloud, on virtual or physical machines - and position responders close to the relying parties that depend on them.

- 1,000+ TPS sustained on a single instance with a high-performance HSM
- Clustered responders scale out with no restarts or downtime
- Deploy on-premise, private or public cloud, VM or physical
- Reuse existing OCSP keys for drop-in legacy replacement



PILLAR 02 · IETF & CA/B FORUM STANDARDS COMPLIANCE

Compliance Your Relying Parties Already Trust

The Challenge: A Non-Standard Response Is No Response

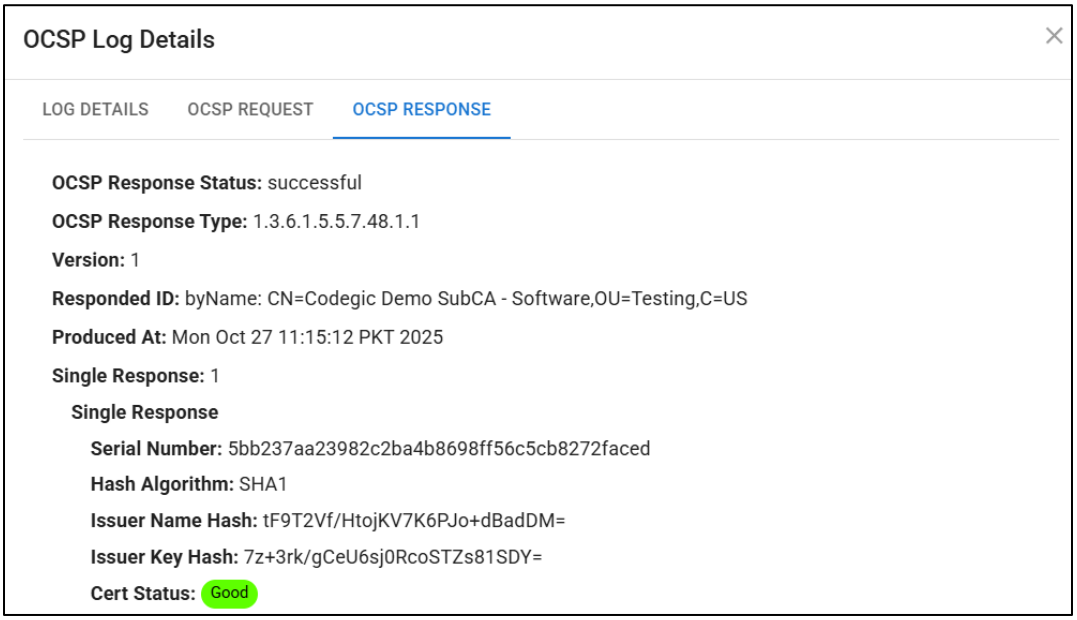
A Validation Authority is only useful if every relying party understands what it says. Acrobat validating a long-term signature, Windows checking a code-signing certificate, a browser completing a handshake, a web server enforcing client authentication - each applies its own strict interpretation of the OCSP specifications. A responder that deviates on response profile, extension handling, signing certificate placement or caching behaviour does not fail loudly; it fails silently, and the certificate is quietly treated as unverified at the exact moment trust was needed most.

Khatim OCSP Server Delivers

Full Profile Coverage. Khatim OCSP Server adheres to the standards set by the IETF and the CA/B Forum, implementing the RFC 6960 protocol and the RFC 5019 lightweight profile designed for high-volume, cache-friendly deployments, alongside RFC 2560 for legacy clients and RFC 4387 for HTTP-based certificate store access. Extended revocation information can be included per policy, so responses carry exactly the evidence a given population of relying parties expects.

Interoperability by Default. Because responses are standards-exact, integration is a configuration exercise rather than a development project. Khatim OCSP Server is validated against Adobe Acrobat, Microsoft Office, mainstream web browsers and web servers, and interoperates with any CA that publishes revocation data it can consume. Business applications continue to use the OCSP client already built into their platform - there is nothing proprietary to install and no SDK to adopt.

- RFC 6960 protocol with the RFC 5019 lightweight profile
- RFC 2560 and RFC 4387 support for legacy and store access
- Validated with Acrobat, Microsoft Office, browsers and web servers
- Extended revocation information configurable per OCSP policy



PILLAR 03 · SERVE MULTIPLE CAs, PKIs & OFFLINE HIERARCHIES

One Responder for Every CA You Operate

The Challenge: Real PKIs Are Never Just One CA

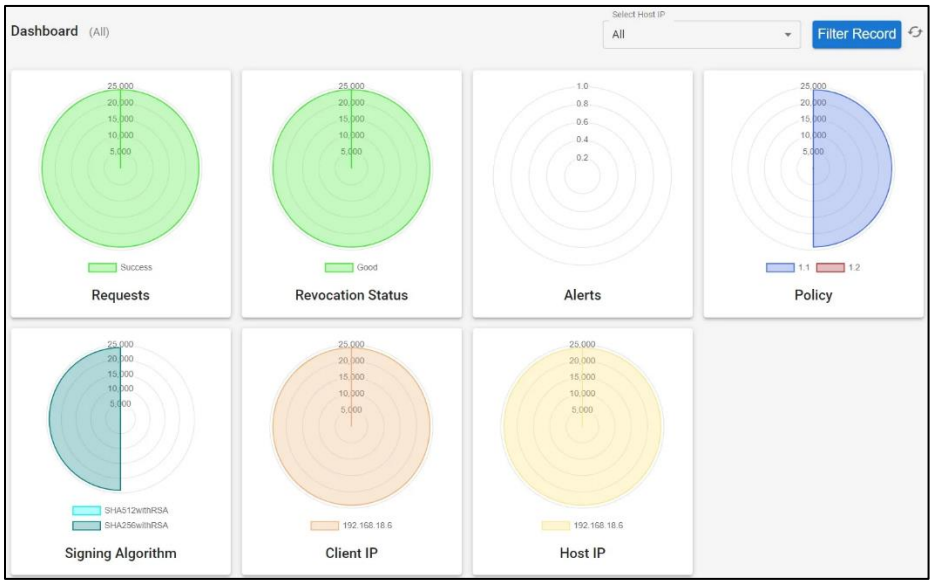
Enterprises rarely run a single Certification Authority. There is an internal issuing CA, a device CA, an offline root, a legacy hierarchy nobody can decommission, and certificates from external commercial CAs in the mix. Standing up a separate responder for each one multiplies licences, hardware, keys, monitoring and audit scope. Worse, offline CAs cannot answer for themselves at all, and external CAs publish only CRLs - so validation coverage ends up uneven, with the least visible parts of the estate the least well served.

Khatim OCSP Server Delivers

A Single Validation Hub. One deployment of Khatim OCSP Server handles multiple Certification Authorities and PKIs, local or remote. Each is configured as its own OCSP policy identifying the CA to serve, the OCSP signing certificate to use, whether extended revocation information is added, and more. Consolidating validation into one hub collapses the licensing, infrastructure and audit footprint while giving every relying party a single, consistent place to ask.

Real-Time and CRL-Based Revocation. Khatim OCSP Server answers in real time from the CA's issued-certificate list, so status reflects reality with no publication delay — and, critically, the responder knows which serial numbers were actually issued. It never returns "good" for a certificate the CA never issued, satisfying a CA/B Forum requirement that CRL-derived responders cannot structurally meet. For external and offline hierarchies it also pulls CRLs over HTTP or LDAP, making one deployment compatible with online CAs, offline CAs and third-party PKIs alike.

- Multiple CAs, PKIs and hierarchies from one deployment
- Per-CA OCSP policies with their own signing certificate
- Real-time revocation direct from the issuing CA & CRL-based revocation
- External CRL retrieval over HTTP and LDAP for offline CAs



PILLAR 04 · HSM-BACKED OCSP RESPONSE SIGNING

Every Response Signed Inside an HSM

The Challenge: A Responder Is Only as Trusted as Its Key

An OCSP signing key is a statement of authority: whoever holds it can declare a revoked certificate good. If that key sits in a file on a server, the entire revocation model of the PKI rests on host security alone - and a compromise is close to undetectable, because forged responses look exactly like legitimate ones. Regulated industries, QTSPs and government programmes must therefore demonstrate hardware-backed key storage, controlled access, traceable usage and separation of duties for the responder, not only for the CA.

Khatim OCSP Server Delivers

Certified Hardware Protection. Response signing executes inside Hardware Security Modules over PKCS#11. Keys are generated or imported under hardware protection and never leave the cryptographic boundary, delivering strong isolation from the operating system, protection against extraction and tampering, role-based control of key usage, and audit evidence that stands up to regulatory scrutiny.

Cloud KMS Without Compromise. For cloud-hosted and hybrid deployments Khatim OCSP Server integrates directly with non-PKCS#11 key services - Microsoft Azure Key Vault, AWS CloudHSM and Google Cloud HSM - so responders running in the cloud sign with the same hardware-grade assurance as on-premise instances. Validation infrastructure can follow the rest of the estate into the cloud without weakening the key protection story or fragmenting your HSM strategy.

- Entrust nShield, Thales Luna, Utimaco, Kryptus, Futurex, Securosys etc. over PKCS#11
- Azure Key Vault, AWS CloudHSM and Google Cloud HSM support
- Generate or import OCSP signing keys under hardware protection
- Military-grade protection across key management and signing

PILLAR 05 · POST-QUANTUM-READY VALIDATION

Validation That Migrates with Your PKI

The Challenge: Revocation Has to Migrate Too

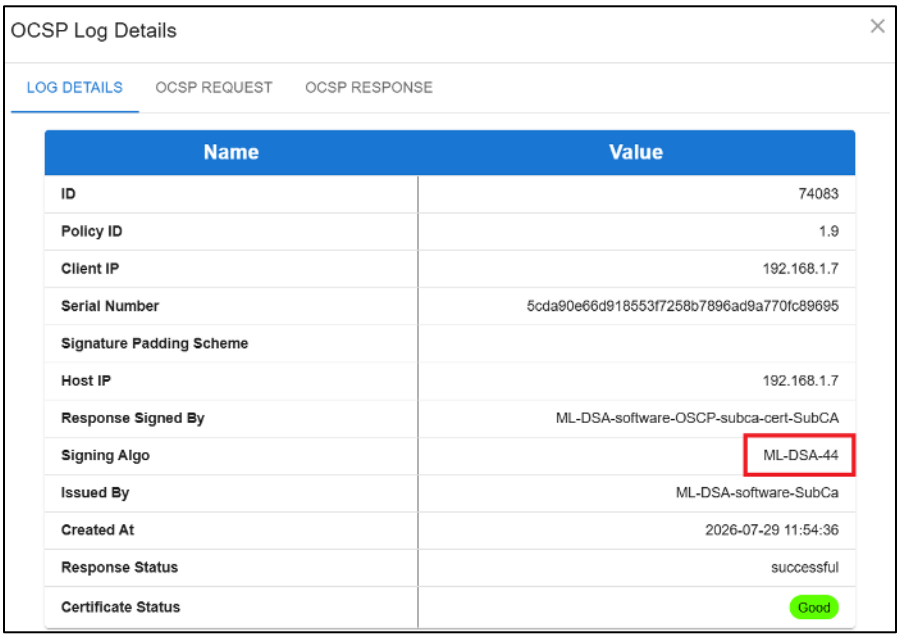
Post-quantum planning concentrates on issuance - new algorithms, new key sizes, new certificate profiles. Validation is routinely forgotten. Yet the moment a CA begins issuing ML-DSA certificates, something has to answer for their revocation status and a responder that can only sign with RSA or ECDSA becomes the constraint that stalls the whole migration. Certificate validity is checked continuously across the entire estate, so an inflexible Validation Authority does not delay one project; it delays every project that depends on the new hierarchy.

Khatim OCSP Server Delivers

Cryptographic Agility Today. Khatim OCSP Server supports RSA (2048, 3072, 4096, 8192), ECDSA (160 through 521), SHA-256/384/512 hashing, and the NIST-standardized post-quantum signature algorithm ML-DSA. Classical and post-quantum response signing coexist in the same deployment, so a PQC pilot hierarchy is validated by the same infrastructure serving production RSA CAs - no parallel estate, no second product, no separate operational model to learn.

Per-Policy Algorithm Selection. Because signing algorithm is a property of the OCSP policy rather than the server, each CA is served with exactly the cryptography its relying parties understand. Legacy applications continue receiving RSA-signed responses while new hierarchies are answered in ML-DSA, enabling phased, verifier-safe rollout. Every transaction records the algorithm used, giving auditors provable evidence of migration progress rather than an assertion of intent.

- RSA 2048/3072/4096/8192 and ECDSA 160 to 521 curve support
- PQC ML-DSA response signing for post-quantum hierarchies
- Per-policy algorithm selection for phased, verifier-safe migration
- Per-transaction algorithm logging for audit and crypto-inventory



PILLAR 06 · OCSP INSIGHTS, LIVE & HISTORICAL REPORTING

See Every Response as It Happens

The Challenge: You Can't Defend What You Can't See

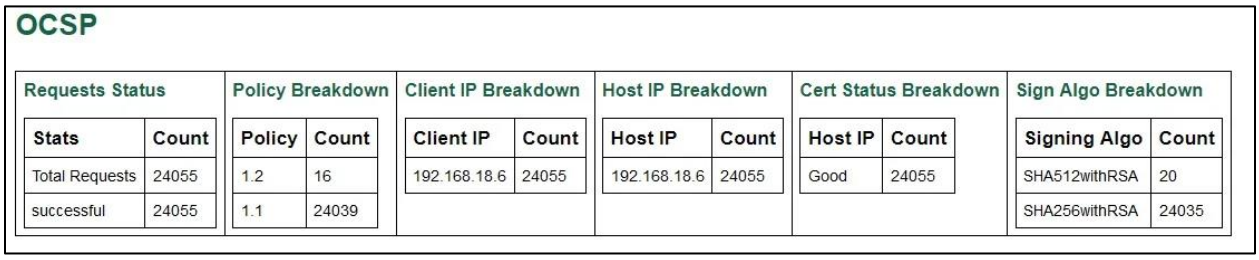
A Validation Authority is infrastructure that fails quietly. Nothing announces that response times have doubled, that a CRL feed stopped refreshing hours ago, that one node in the cluster is answering unknown for a whole hierarchy, or that a signing certificate is weeks from expiry. The symptom surfaces somewhere else entirely - a failed login, a rejected signature, an outage attributed to the application team. And when an auditor asks what the service was doing last Tuesday, guesswork is not an answer.

Khatim OCSP Server Delivers

Real-Time Operational Visibility. Khatim OCSP Server is the first to present live and historical performance statistics for all OCSP clusters from a single pane of glass. Administrators watch transactions per second, success versus failure rates and per-node behaviour update in real time, monitoring the whole cluster from one screen or zooming into a single responder to inspect its request and response stream, recent errors and throughput.

Insight, Not Just Uptime. Data filters by revocation status, OCSP policy, success or failure, signing algorithm and more, turning raw traffic into intelligence: which CAs are queried hardest, which populations generate revoked responses, how demand shifts across the day. Automated daily summary reports arrive with a snapshot of what response types were generated, alongside failures and alerts - supporting capacity planning, SLA reporting and forensic investigation.

- Live TPS, success/failure and per-node telemetry across the cluster
- Filter by revocation status, policy, algorithm and outcome
- Automated daily summary reports emailed to administrators
- Single-pane-of-glass monitoring included, not licensed separately



PILLAR 07 · PROACTIVE ALERTS & SIEM INTEGRATION

Know before Your Relying Parties Do

The Challenge: Problems You Learn About Too Late

When validation degrades, the first notification is usually a user who cannot sign in or an application team reporting a certificate error they cannot explain. By then the SLA is already breached and the incident has been misattributed. Governance makes this harder still: it is not enough for an operator to notice a problem and fix it. Every event needs to be formally recorded, retained, and correlated with the rest of the security estate to be defensible after the fact.

Khatim OCSP Server Delivers

Proactive Notification. When the OCSP server is not working as it should, Khatim OCSP Server proactively notifies administrators so they can act before SLAs are breached. Every issue is recorded for traceability, giving operations an early-warning system rather than an after-the-fact report, and giving auditors a complete incident record. Email notifications reach configured administrators as events are generated, and are consolidated into daily summary reports.

Secure SIEM Delivery. Alerts and event logs are pushed securely into central logging and SIEM platforms - including Splunk, Grafana, Graylog and LogRhythm - with SNMP and Syslog available for existing monitoring frameworks. Validation telemetry lives alongside the rest of your security data, so an OCSP anomaly can be correlated with authentication failures, network events and CA activity instead of being investigated in isolation.

- Proactive administrator alerts before SLAs are breached
- Secure push to Splunk, Grafana, Graylog and LogRhythm
- SNMP and Syslog integration for existing monitoring estates
- Email notification and automated daily summary reporting

PILLAR 08 · ROLE-BASED ACCESS CONTROL, SECURITY & GUI

The Right People, the Right Rights, All Recorded

The Challenge: Administration Is Itself an Attack Surface

Validation infrastructure is Tier-0 trust. Whoever can change an OCSP policy, swap a signing certificate or redirect a CRL source can change what the entire organization believes about certificate validity - without touching a single CA. Yet daily operations pull many hands towards that console: help-desk staff investigating a failed validation, auditors sampling evidence, engineers tuning a policy. Where privilege cannot be divided, everyone becomes an administrator by default - and once changes happen silently, no audit can reconstruct who did what.

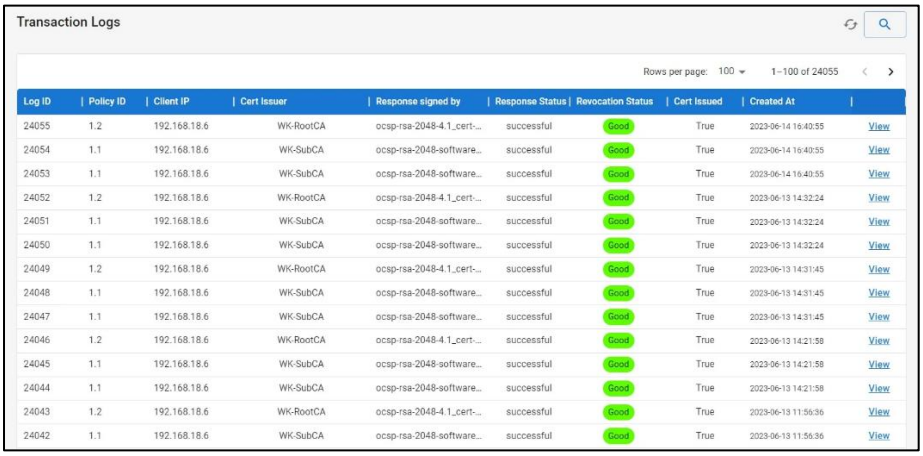
Khatim OCSP Server Delivers

Least Privilege by Role. Access is granted through defined administrator roles rather than a single shared level of power, so each person receives only the rights their job requires. Help-desk and support staff can review transactions and logs to resolve a customer issue without the ability to view or alter configuration; auditors gain read-only visibility; policy, key and keystore operations stay reserved for senior operators. Privilege becomes a deliberate grant instead of a side effect of having an account.

Unified Admin-Friendly GUI. Complicated OCSP systems cause confusion and invite error. Khatim OCSP Server provides a user-friendly web GUI covering key generation, HSM and keystore configuration, OCSP policy handling, transaction viewing and request download from a single pane of glass - making deployment, integration and testing markedly quicker than other solutions on the market.

Hardened, Attributable Administration. Trusted resources reach key functions through powerful multi-factor authentication using military-grade TLS client authentication, so only authorized operators access privileged operations. Every update made to the system is recorded with integrity and attributed to a named operator, delivering the separation of duties and complete audit trail that auditors expect.

- Role-based access control with least-privilege operator separation
- Read-only log and transaction access for support and audit staff
- Multi-factor TLS client authentication on all key functions
- Full attributable audit trail across every configuration change
- Equally accessible by API over TLS client authentication for automated operations



Khatim OCSP Server Architecture

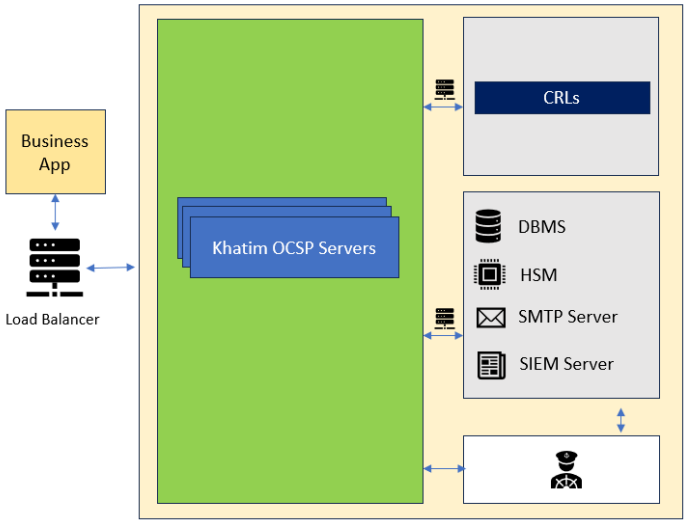
Khatim OCSP Server (KOS) is a high-assurance Validation Authority providing real-time certificate status to business applications, relying parties and devices. It is built from four core components:

- **Khatim OCSP Portal**, through which administrators manage configuration, transactions and statistics
- **Khatim OCSP Engine**, which delivers the OCSP service to business applications
- **Khatim OCSP Diagnostic**, which performs housekeeping and continuous health checks
- **Khatim OCSP Storage**, which holds configuration and transactional data

The processing flow is straightforward:

- A business application sends an OCSP request containing certificate information
- KOS verifies the incoming request against the applicable OCSP policy
- KOS determines status in real time from the issuing CA, or from a monitored CRL
- KOS returns a digitally signed OCSP response of good, revoked or unknown
- Signing keys are held in a PKCS#11 HSM or cloud KMS and transactions are retained in the database for audit and archival

For high-volume and high-availability needs, KOS is deployed as a cluster of individual OCSP servers behind a load balancer - additional servers can be added to the pool without stopping running instances. Here is a basic deployment architecture for a Khatim OCSP Server.



> *Codegic team was immensely helpful in bringing our ideas for phone-based PKI authentication and signing to reality. Codegic was absolutely up to the challenge of bringing the security and accountability of our Authenticity Infrastructure's identity certificates to iOS and Android. They gave us secure solutions when it came to advanced digital signatures (CAdES, JSON signing) and WebCrypto. With top quality support, they are a go to shop for any serious PKI / Digital Signature development.*
>
> **Wes Kussmaul** | *CEO, Reliable Identities, Inc.*

Reliable Identities, Inc.
Identity is the Foundation of Security™

Algorithms / Protocols

- RSA (2048/3072/4096/8192)
- ECDSA (NIST_P, SECP (K1,R1), BRAINPOOL (R1,T1) — 160, 224, 256, 320, 384, 521)
- SHA-256, SHA-384, SHA-512
- PQC — ML-DSA (44, 65, 87)
- RFC 6960, RFC 5019, RFC 2560, RFC 4387, RFC 5280
- PKCS#11, SNMP, SMTP, Syslog, HTTP, HTTP/s, LDAP, REST
- CA/B Forum Baseline Requirements
- **Performance:** RSA 2048 – 390[1] - 2,400 TPS[2]

[1] Tested with Entrust nShield HSM XC Solo Mid
[2] With hi-end HSMs

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 OCSP Server 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