codegic

Trusted Enrolment & Identity Vetting

Khatim RA Server

IETF and CA/B Forum compliant Registration Authority delivering vetted, automated X.509 certificate enrolment at enterprise scale

4 Protocols
ACME, EST, SCEP, CMP
Automation built in

500+
Enrolment/Sec
Built for Volume

Multi Tenant
One Portal, Many Orgs
Enterprises, Governments, TSPs

PQC
ML-DSA Ready
Future-proof enrolment

X.509 Certificate issuance made simple!

Khatim RA Server is the front door to your certification authority — the layer that decides who deserves a certificate before anything is ever signed. It carries the identity proofing, policy enforcement and approval workflow that a CA should never be asked to perform, so issuance stays fast, automated and defensible from request to revocation.

- Enterprise ready, secure and quick to deploy Registration Authority
- Compatible with WebTrust, IETF RFC 5280 and CA/B Forum requirements
- Automated enrolment over ACME, EST, SCEP and CMP for devices, workloads and websites
- Manual, multi-approval vetting workflows for high-assurance and qualified certificates
- Manages multiple CAs, PKIs and tenant organizations from a single deployment
- Advanced RA insights, live reporting and proactive alerting built in

Khatim RA Server Supports:

- RFC 8555 — ACME for automated TLS/SSL certificate issuance
- RFC 7030 — EST for enrolment over secure transport
- RFC 8894 — SCEP for network devices and endpoints
- RFC 4210 — CMP for certificate management operations
- RFC 5280 — X.509 certificate and CRL profile
- CA/B Forum Baseline Requirements for domain, organization and identity validation
- WebTrust-aligned registration and vetting evidence retention
- TLS/SSL (DV, OV, IV, EV) and S/MIME (MV, OV, SV, IV) certificate policies
- Qualified and Code Signing certificate issuance
- ML-DSA post-quantum key and certificate enrolment

Eight Pillars of Trusted Certificate Enrolment

01

Flexible Enrolment & Vetting Automated, manual or multi-approval vetting configured per certificate type, with every piece of evidence retained and attributable for audit.

02

Automated Protocol Enrolment ACME, EST, SCEP and CMP in one server, so websites, devices and workloads enrol and renew without a human ever touching the request.

03

One Portal, Many Organizations True multi-tenancy with per-organization service plans governing certificate types, quantities, validity and vetting requirements.

04

Standards & CA/B Forum Compliance RFC 5280, WebTrust and CA/B Forum validation rules applied at the point of request, so non-compliant certificates are never issued.

05

Protects Your PKI The RA absorbs validation, vetting and exposure in the DMZ, keeping the CA and its keys out of reach of the requesting population.

06

Post-Quantum-Ready Enrolment Cryptographic agility across RSA, ECDSA and PQC ML-DSA, so registration migrates in step with the hierarchies it serves.

07

RA Insights & Proactive Alerts Live issuance telemetry, expiry visibility and secure event delivery to Splunk, Grafana, Graylog and LogRhythm.

08

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

PILLAR 01 · FLEXIBLE ENROLMENT & IDENTITY VETTING

Decide Who Deserves a Certificate, Before One Exists

The Challenge: A CA Cannot Judge Identity

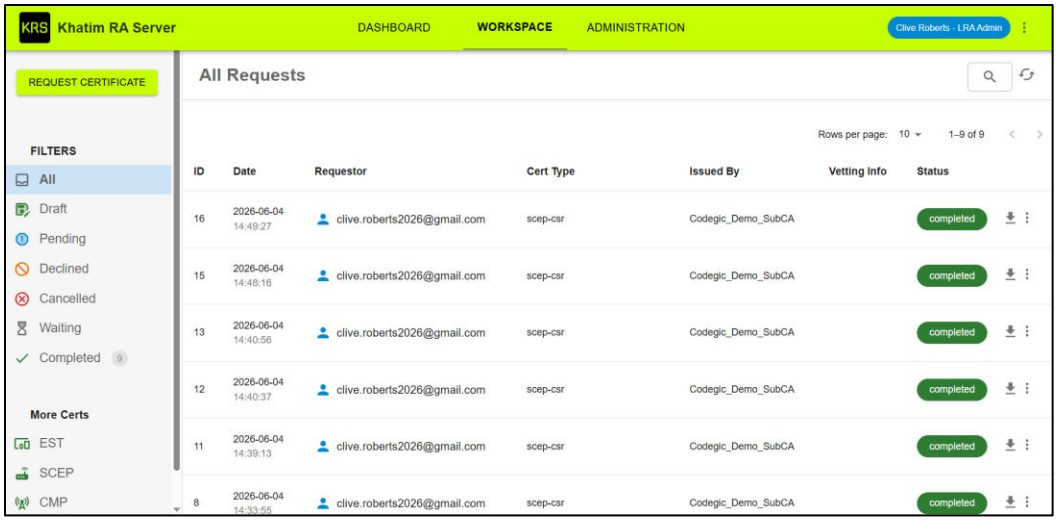
A Certification Authority does exactly what it is told. It has no opinion on whether the requester genuinely controls the domain, works for the organization named in the subject, or is entitled to a certificate at that assurance level. When vetting is handled by spreadsheets, email approvals and institutional memory, three failures follow: the wrong identity gets certified, the right identity waits days for a signature, and when an auditor asks who approved a certificate issued eighteen months ago, nobody can produce the evidence. Registration is where trust is actually established — or quietly lost.

Khatim RA Server Delivers

Vetting Shaped to Assurance. Vetting policy is configured per certificate type rather than per server, so low-assurance device certificates issue automatically while qualified, organization-validated certificates route to named approvers. Workflows support a single approver or multiple sequential approvals by any number of RA and LRA administrators, and can be disabled entirely where automated validation is sufficient. Assurance level becomes a deliberate policy decision instead of a function of who happened to be available.

Evidence That Survives an Audit. Approvers attach their vetting record in whatever form the check produced it — scanned identity documents, PDFs, photographs, recorded video verification sessions, or free-text notes. Every submission is bound to the request, timestamped and attributed to the operator who made it, and the complete vetting history is retained alongside the issued certificate. When an auditor or relying party asks how an identity was proven, the answer is a record, not a recollection.

- Automated, manual and multi-approval vetting configured per certificate type
- Unlimited RA and LRA approvers with sequential approval workflows
- Vetting evidence captured as PDF, image, video or notes and bound to the request
- Complete attributable vetting history retained for audit and dispute resolution



PILLAR 02 · AUTOMATED PROTOCOL ENROLMENT

Certificates That Enrol and Renew Themselves

The Challenge: Manual Enrolment Does Not Scale — and Expiry Does Not Wait

Certificate populations no longer consist of a few hundred server certificates managed by a team that knows each one. They consist of tens of thousands of workloads, routers, switches, load balancers, mobile devices and containers, on validity periods that have collapsed from years to months. Manual issuance cannot keep pace, and the failure mode is the most expensive one in infrastructure: an expired certificate on a production service, discovered by customers rather than by monitoring. Automation is no longer an efficiency improvement; it is the only viable operating model.

Khatim RA Server Delivers

Four Protocols, One Server. Khatim RA Server implements ACME for websites and TLS endpoints, EST and SCEP for network devices and endpoints, and CMP for full certificate management operations — all from a single deployment sharing one policy engine, one audit trail and one administration console. Clients already built into your operating systems, load balancers, network hardware and orchestration platforms enrol natively. There is nothing proprietary to install and no agent to maintain across the estate.

Automation Under Policy Control. Automated does not mean unrestricted. Every protocol request is evaluated against the same organization, service plan and validation rules that govern manual requests, so an ACME client cannot obtain a certificate its organization is not entitled to, and a SCEP enrolment cannot exceed the validity or quantity its plan allows. Automation removes the operator from the transaction without removing the policy from the decision.

- ACME (RFC 8555) for automated TLS/SSL issuance and renewal
- EST (RFC 7030) and SCEP (RFC 8894) for devices, IoT and network infrastructure
- CMP (RFC 4210) for full certificate management operations
- Every protocol request enforced against organization and service plan policy

PILLAR 03 · MULTI-TENANCY & SERVICE PLAN GOVERNANCE

One Portal for Every Organization You Serve

The Challenge: One PKI, Many Constituencies

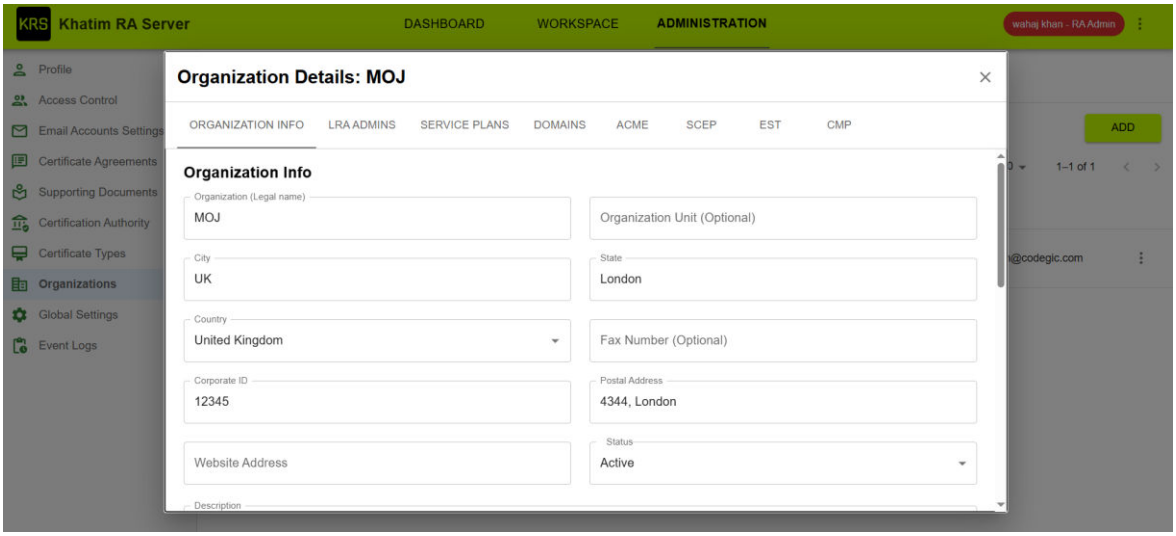
Almost nobody issues certificates to a single, uniform population. A government programme serves ministries and agencies. A Trust Service Provider serves subscribing enterprises. A group holding serves subsidiaries in different jurisdictions with different regulatory obligations. Each needs its own certificate types, its own limits and its own approvers — and none should see another's requests. Solving this by deploying a separate RA per constituency multiplies licences, infrastructure, patching and audit scope, and guarantees that policy drifts apart the moment the second instance is stood up.

Khatim RA Server Delivers

Isolation Without Duplication. A single Khatim RA Server deployment hosts many organizations, each with its own administrators, requesters, certificate catalogue and transaction history, and each unable to see the others. Local Registration Authority administrators are scoped to their own organization, so delegated administration reaches the people closest to the identities being vetted without extending their authority anywhere else. One deployment to license, patch, monitor and audit.

Service Plans as Policy. Each organization is bound to a service plan that defines precisely what it may do: which certificate types it can request, how many, at what validity periods, whether vetting is required and which agreements must be accepted first. Plans make entitlement explicit and enforceable rather than a matter of trust in the requester, and make subscription management — onboarding, uplift, renewal and expiry — an administrative action rather than an engineering one.

- Unlimited organizations from a single RA deployment with full data isolation
- Delegated LRA administration scoped to each organization
- Service plans governing certificate type, quantity, validity and vetting requirement
- Agreement acceptance and subscription lifecycle handled in-product



PILLAR 04 · STANDARDS & CA/B FORUM COMPLIANCE

Compliance Enforced at the Point of Request

The Challenge: Non-Compliance Is Discovered Too Late

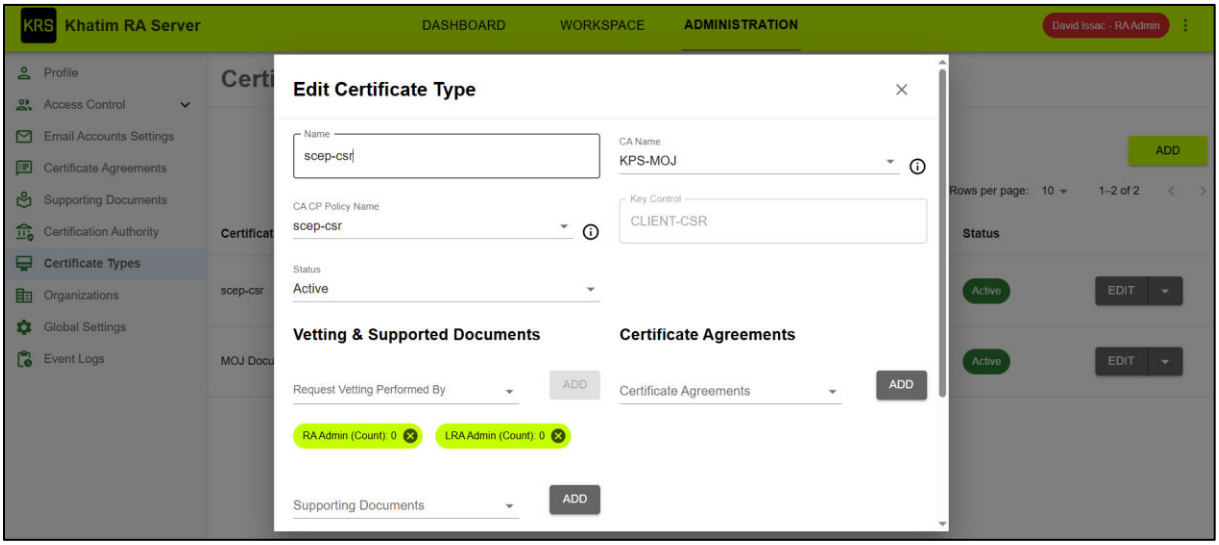
A certificate that violates a profile requirement is not rejected at issuance — it is issued, deployed, and discovered months later by a browser that distrusts it, an auditor sampling the estate, or a root programme conducting a review. By then remediation means mass revocation, emergency re-issuance across production systems, and an incident report. Public trust programmes are unforgiving here: a single mis-issuance can put an entire hierarchy's participation at risk. The only safe place to enforce a profile is before the CA ever sees the request.

Khatim RA Server Delivers

Validation Before Signature. Khatim RA Server applies CA/B Forum Baseline Requirements and RFC 5280 profile checks to every incoming request — subject and SAN composition, key type and size, validity period, extension consistency and certificate type entitlement — and rejects what does not conform. Compliant requests issue in seconds with no operator involvement. The CA receives only requests it can safely sign, so mis-issuance is prevented structurally rather than detected retrospectively.

Every Certificate Type Your Estate Needs. One RA covers the full commercial and enterprise catalogue: TLS/SSL at DV, OV, IV and EV; S/MIME at MV, OV, SV and IV; Qualified certificates for document signing; code signing; and general X.509 for devices, applications and individuals. Each type carries its own validation depth and vetting requirement, so assurance level and evidence obligation stay correctly paired without a separate registration system per use case.

- CA/B Forum Baseline Requirements validation applied to every request
- RFC 5280 and WebTrust-aligned profile enforcement before issuance
- TLS/SSL (DV, OV, IV, EV) and S/MIME (MV, OV, SV, IV) certificate policies
- Qualified and Code Signing certificate support



PILLAR 05 · PROTECTS YOUR PKI

Your CA Should Never Face the Requester

The Challenge: Exposing the CA Is Exposing Everything

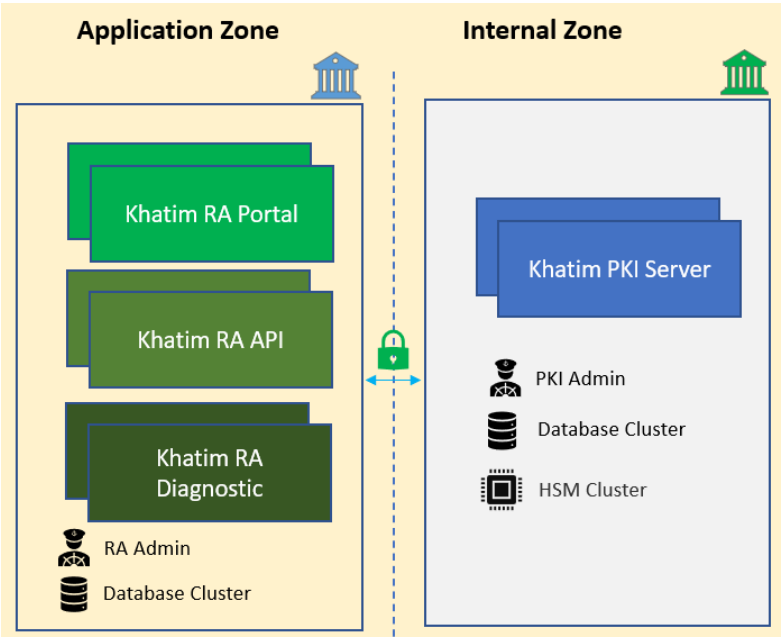
A Certification Authority is Tier-0 infrastructure. Its keys underwrite every certificate the organization has ever issued, and a compromise cannot be contained by revoking a few certificates — it invalidates the hierarchy. Yet certificate requests arrive from the least trusted parts of the estate: internet-facing web servers, mobile devices, third-party integrators, network hardware in branch offices. Any architecture that lets those populations reach the CA directly has placed the most valuable asset in the environment on the same path as its least controlled traffic.

Khatim RA Server Delivers

A Deliberate Line of Defence. Khatim RA Server sits between the requesting population and Khatim PKI Server, absorbing request parsing, protocol termination, validation and vetting so the CA is never directly addressable by requesters. The RA is deployed in the application zone behind the DMZ while the CA, its database and its HSM cluster remain in the internal zone, with only a controlled, authenticated channel between them. The CA does what only a CA should do: sign, revoke and publish.

Many CAs Behind One Front Door. A single Khatim RA Server serves multiple Certification Authorities — an internal issuing CA, a device CA, a qualified hierarchy, a legacy PKI awaiting decommission — each with its own certificate types, policies and approvers. Adding a CA becomes a configuration change rather than a new deployment, and every request across every hierarchy passes through the same validation, the same evidence retention and the same audit trail.

- RA terminates all requester traffic; the CA is never directly exposed
- DMZ, application zone and internal zone separation with controlled channels
- Multiple Certification Authorities served from a single RA deployment
- Consistent validation, evidence and audit across every hierarchy



PILLAR 06 · POST-QUANTUM-READY ENROLMENT

Registration That Migrates with Your PKI

The Challenge: Enrolment Is the Constraint Nobody Plans For

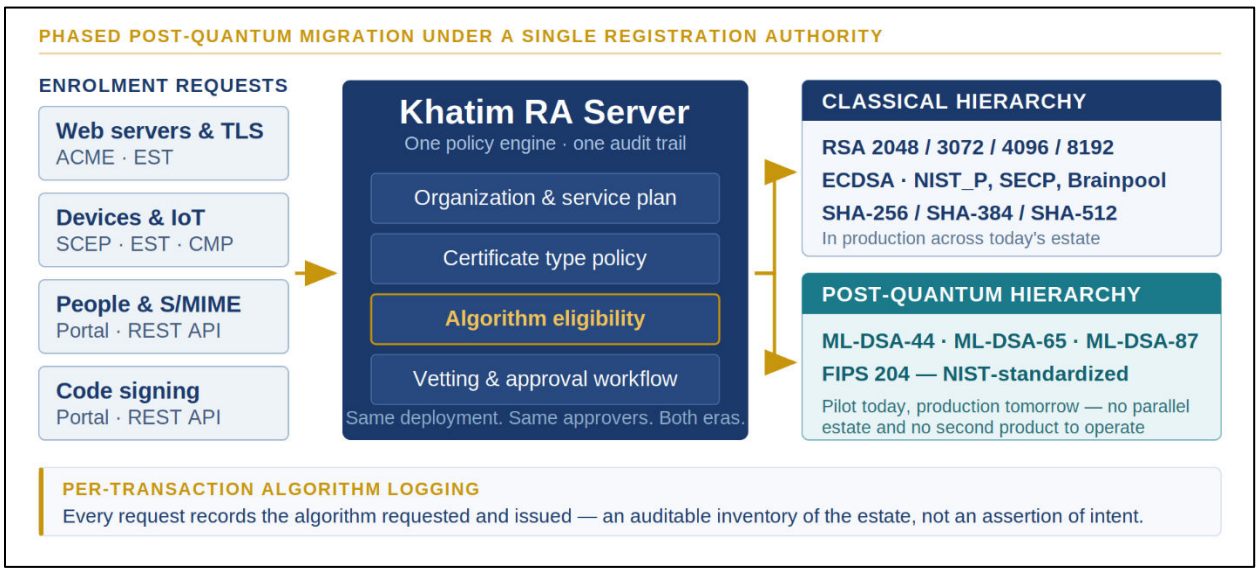
Post-quantum programmes concentrate on the CA — new algorithms, new key generation, new certificate profiles. Registration is assumed to follow. It does not. The moment a hierarchy begins issuing ML-DSA certificates, every request for one has to be parsed, validated, policy-checked and approved by a registration layer that understands the algorithm. An RA that only recognises RSA and ECDSA does not slow one project; it becomes the bottleneck for the entire migration, and the newly capable CA sits idle behind a front door that cannot let anything through.

Khatim RA Server Delivers

Agility Across Classical and Post-Quantum.
Khatim RA Server handles enrolment for RSA (2048, 3072, 4096, 8192), ECDSA across the standard curve families, SHA-256/384/512 hashing, and the NIST-standardized post-quantum signature algorithm ML-DSA (44/65/87). Classical and post-quantum requests are validated, vetted and forwarded through the same deployment, so a PQC pilot hierarchy is served by the infrastructure already running production enrolment — no parallel estate and no second product.

Phased Migration, Recorded as Evidence.
Because algorithm eligibility is a property of the certificate type and service plan, each organization migrates on its own timeline. Legacy applications continue enrolling for RSA while new hierarchies issue ML-DSA, and the same approvers work across both. Every transaction records the algorithm requested and issued, turning migration progress into an auditable inventory of what the estate actually holds rather than an assertion of intent.

- RSA 2048/3072/4096/8192 and ECDSA curve support across NIST, SECP and Brainpool families
- PQC ML-DSA enrolment for post-quantum hierarchies
- Per-certificate-type algorithm eligibility for phased, verifier-safe migration
- Per-transaction algorithm logging for audit and cryptographic inventory
-



PILLAR 07 · RA INSIGHTS, REPORTING & PROACTIVE ALERTS

See Every Request as It Happens

The Challenge: Issuance Failures Are Invisible Until They Are Expensive

Registration fails quietly. Nothing announces that a service plan quota was exhausted overnight, that an ACME client has been retrying against a rejected policy for three days, that one organization's requests are queued behind an absent approver, or that four hundred certificates expire next Tuesday. The symptom appears somewhere else entirely — a failed deployment, a blocked onboarding, a production outage attributed to the application team. And when governance asks what was issued last quarter, to whom, and on whose approval, guesswork is not a defensible answer.

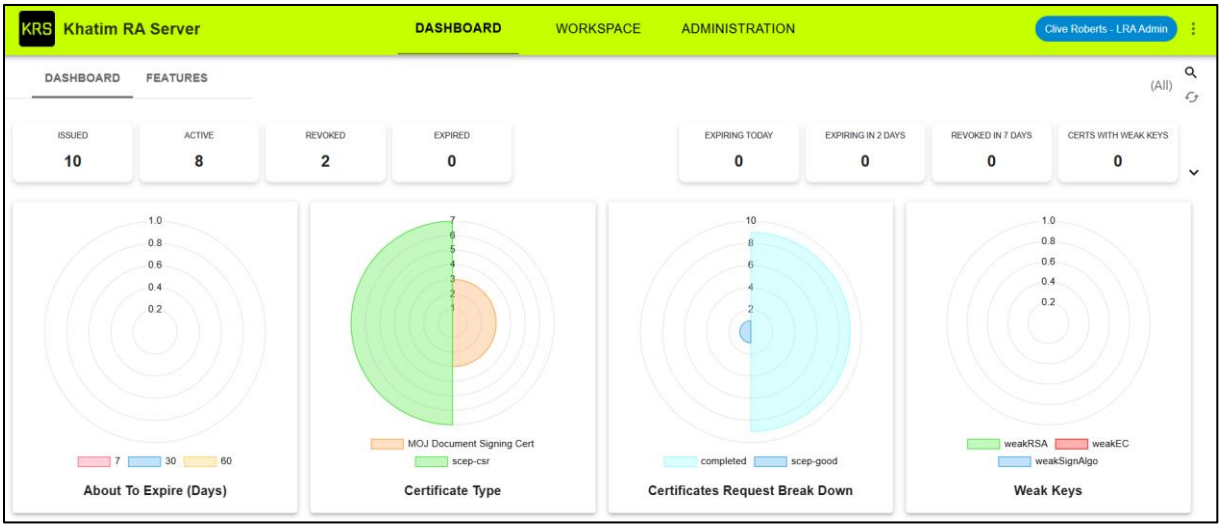
Khatim RA Server Delivers

Live Operational Visibility. Khatim RA Server presents live and historical issuance statistics through interactive dashboards covering successful and failed requests, requests awaiting vetting, certificates approaching expiry, and volumes broken down by organization, certificate type, protocol and signing algorithm.

Administrators watch the whole estate from one screen or drill into a single request to inspect what was submitted, what was validated and what was returned. Automated daily summary reports deliver the same picture to inboxes without anyone logging in.

Alerts Before the Business Notices. When enrolment degrades — a CA unreachable, a protocol endpoint failing, a quota exhausted, an approval queue stalling — administrators are notified proactively rather than discovering it through a support ticket. Every event is recorded for traceability and pushed securely into central logging and SIEM platforms including Splunk, Grafana, Graylog and LogRhythm, so registration telemetry can be correlated with authentication, network and CA activity instead of investigated in isolation.

- Live issuance, failure, pending-vetting and expiry telemetry in one console
- Filter by organization, certificate type, protocol, algorithm and outcome
- Secure event delivery to Splunk, Grafana, Graylog and LogRhythm
- Automated daily summary reports emailed to administrators



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

The Right People, the Right Rights, All Recorded

The Challenge: The RA Console Is Itself an Attack Surface

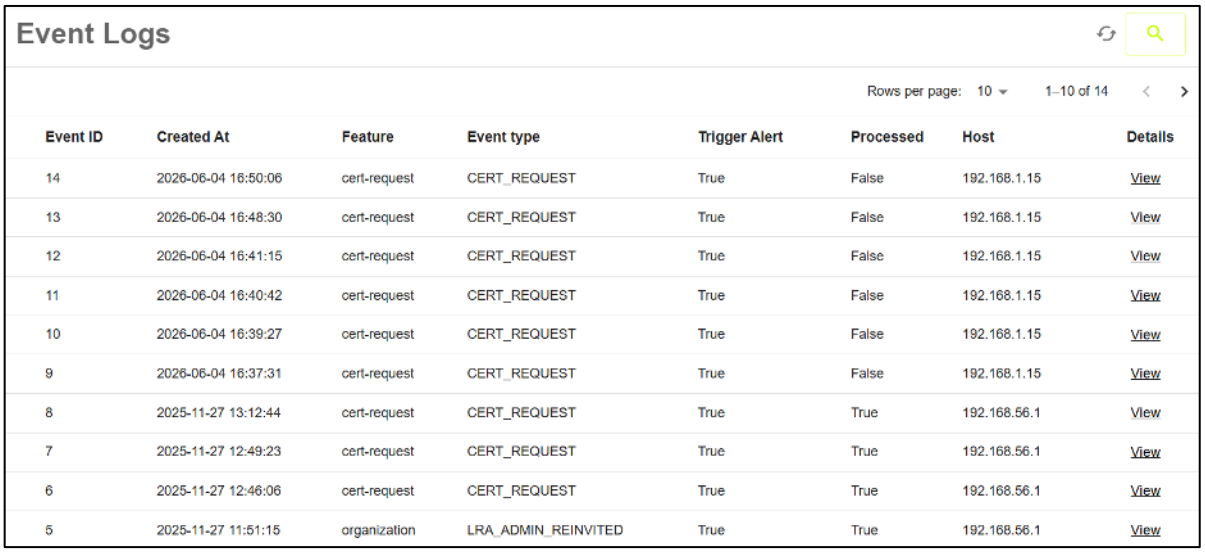
Whoever can alter a vetting policy, create a service plan or approve a request can cause a certificate to be issued to an identity that was never proven — without ever touching the CA. Yet daily operations draw many hands towards that console: local administrators onboarding subscribers, support staff investigating a rejected request, auditors sampling evidence, developers integrating a business application. Where privilege cannot be divided, everyone becomes an administrator by default; and where changes happen without attribution, no audit can reconstruct who authorised what.

Khatim RA Server Delivers

Least Privilege by Role. Access is granted through defined roles rather than a single shared level of power. RA administrators govern global configuration; LRA administrators are confined to their own organization; LRA users submit and track requests; support and audit staff hold read-only visibility into transactions and logs. Administrative access to the RA is protected by military-grade AES-256 and mutual TLS client authentication, while LRA operators authenticate with credentials appropriate to their scope. Privilege becomes a deliberate grant rather than a side effect of holding an account.

Full Control from Your Own Applications. Everything available in the portal is available over REST APIs secured by TLS client authentication — organization onboarding, service plan configuration, certificate request submission, vetting decisions, revocation and reporting. CRM, ECM, ITSM, HR and identity platforms drive registration directly, so certificate issuance becomes a step inside an existing business process rather than a separate system somebody has to remember to visit.

- Distinct RA, LRA administrator, LRA user and read-only audit roles
- AES-256 and mutual TLS client authentication for administrative access
- Full attributable audit trail across every configuration and vetting decision
- Complete REST API coverage for CRM, ECM and business application integration



Event ID	Created At	Feature	Event type	Trigger Alert	Processed	Host	Details
14	2026-06-04 16:50:06	cert-request	CERT_REQUEST	True	False	192.168.1.15	View
13	2026-06-04 16:48:30	cert-request	CERT_REQUEST	True	False	192.168.1.15	View
12	2026-06-04 16:41:15	cert-request	CERT_REQUEST	True	False	192.168.1.15	View
11	2026-06-04 16:40:42	cert-request	CERT_REQUEST	True	False	192.168.1.15	View
10	2026-06-04 16:39:27	cert-request	CERT_REQUEST	True	False	192.168.1.15	View
9	2026-06-04 16:37:31	cert-request	CERT_REQUEST	True	False	192.168.1.15	View
8	2025-11-27 13:12:44	cert-request	CERT_REQUEST	True	True	192.168.56.1	View
7	2025-11-27 12:49:23	cert-request	CERT_REQUEST	True	True	192.168.56.1	View
6	2025-11-27 12:46:06	cert-request	CERT_REQUEST	True	True	192.168.56.1	View
5	2025-11-27 11:51:15	organization	LRA_ADMIN_REINVITED	True	True	192.168.56.1	View

Khatim RA Server Architecture

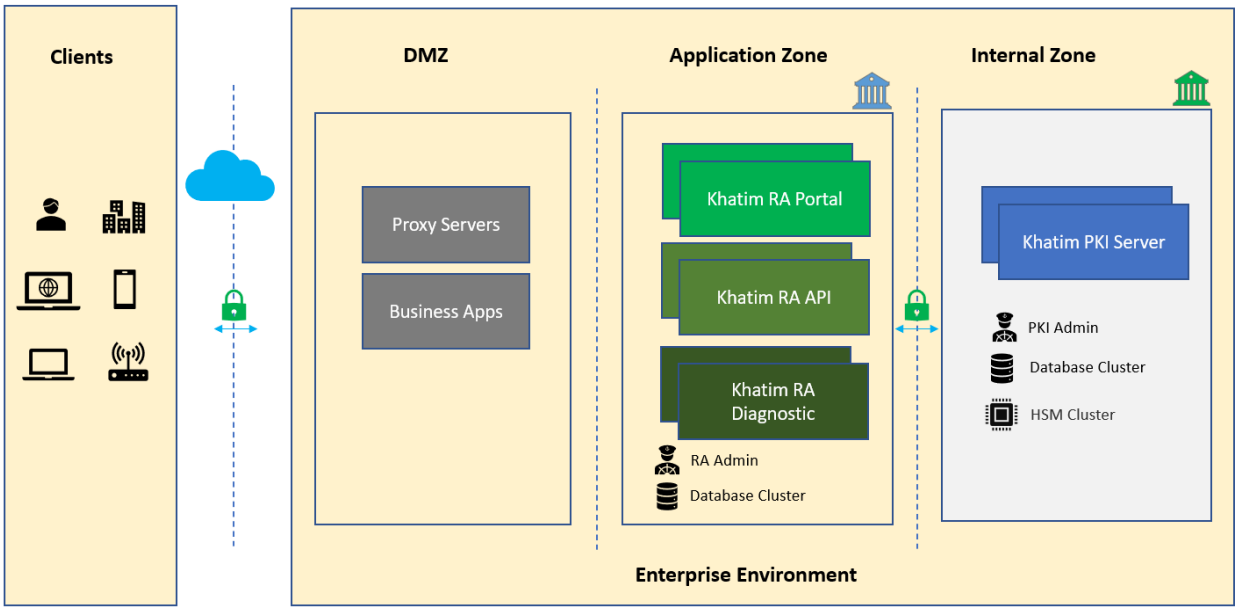
Khatim RA Server (KRS) is a high-assurance Registration Authority providing vetted, policy-enforced certificate enrolment for business applications, devices and individuals. It is built from four core components:

- **Khatim RA Portal**, through which administrators manage organizations, certificate types, vetting configuration, service plans, transactions and statistics
- **Khatim RA API**, which delivers registration services to business applications and terminates the ACME, EST, SCEP and CMP protocol interfaces
- **Khatim RA Diagnostic**, which performs housekeeping, notifications, monitoring and daily summary reporting
- **Khatim RA Storage**, which holds configuration, vetting evidence and transactional data

The processing flow is straightforward:

- A business application, device or administrator submits a certificate request through the API, an enrolment protocol or the portal
- KRS verifies the request against the applicable organization, service plan and validation policy
- KRS applies the configured vetting workflow — automatic, or routed to one or more named approvers with evidence capture
- KRS forwards the approved request to Khatim PKI Server for issuance
- KRS returns the issued certificate to the requester and retains the full request, vetting and response record for audit

For high-volume and high-availability needs, KRS is deployed as a cluster of RA Portal and RA API instances 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 RA Server.



> *We needed the ability to use X.509 Certificate based SSL Client Authentication to provide an additional security layer for our cloud-based applications and Codegic not only quickly provisioned the certificates we needed, but also provided very responsive support when we had questions. Rolling out any PKI project can be hard work, but having a partner like Codegic has made it fast and easy."*
>
> **Kevin de Smidt** | *Head of Technology, CURE International*

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
- PQC — ML-DSA (44, 65, 87)
- ACME (RFC 8555), EST (RFC 7030), SCEP (RFC 8894), CMP (RFC 4210), RFC 5280, RFC 2986, X.500
- REST, HTTP, HTTP/s, LDAP, AD/LDAP, SMTP, SNMP, Syslog
- CA/B Forum Baseline Requirements
- **Certificate Types**
  - X.509 for individuals, devices and applications
  - TLS/SSL (DV, OV, IV, EV)
  - S/MIME (MV, OV, SV, IV)
  - Qualified Certificates
  - Code Signing
- **Key Storage:** PFX / PKCS#12, HSM (at Khatim PKI Server), Smart Cards

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 RA 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