Khatim RA Server

Powerful & Scalable RA server for complete Certificate Life-cycle management (CLM)

- Flexible Enrollment and Vetting
- Easily integrate using APIs, ACME & SCEP
- Enables low and high assurance X.509 certificates
- Compatible with Web Trust, IETF 5280, CA/B forum standards
- Issue certificates to individuals, devices, and applications

Enterprises, Governments, Trust Service Providers

X.509 Issuance Simplified!

Khatim Registration Authority (RA) Server stands as a robust registration and vetting platform empowering Enterprises, Governments, and Trust Service providers to facilitate tailored enrollment and on-boarding processes for X.509 digital certificates. It facilitates certificate issuance to individuals, devices, and applications via Khatim PKI Server CAs with customizable features. Khatim RA Server enforces stringent identity verification protocols, enhancing the overall security and integrity of the certificate life cycle management (CLM).

"Your Gateway to Trusted Certificate Life Cycle Management"

Authenticate

Validate

Issue

What makes Khatim RA Server standout from the rest?

Built for Enterprises

Khatim RA Server is purpose-built for enterprise scalability and resilience, ensuring reliable validation and vetting for high-volume X.509 certificate issuance across diverse business applications, devices, and individuals. Keeps full track of certificate request life cycle. Be it closed PKI, public or National PKI, one RA fits all!

Multiple Vetting Options

Khatim RA Server provides automated and manual vetting for any type of certificates. For high assurance certificates, manual vetting can be enabled with workflows for single or multiple approvals. During automatic vetting, performs CA/B forum based checks for quick issuance of certificates with zero delays.

IOT, People, Applications

Khatim RA Server provides both programmatic and GUI based interfaces to handle certificate issuance for devices, IOT, people and applications. These could be SSL Certificates (DV, OV, IV, EV), S/Mime (MV, OV, SV, IV), AATL or Qualified Certificates.

Key Features

Protects your PKI

Khatim RA server integrates with Khatim PKI Server handling all the complex user vetting process & acting as the first line of defense before sending the certification request to Khatim PKI. PKI admin can also configure multiple CAs with a single Khatim RA server. This offloads all validations, vetting to Khatim RA Server allowing Khatim PKI Server to manage the core PKI tasks i.e. certificate issuance, revocation etc.

Device Enrollment

Websites and devices need X.509 digital certificates and they need it quickly with no manual intervention. Khatim RA Server supports both ACME (rfc8555) to issue SSL Certificates for websites & SCEP for devices (routers, switches etc.).

Setup Vetting Policies

Khatim RA Server allows customizable manual vetting by any number of RA Admin or LRA Admins or even no vetting for low assurance certificates. All admins can provide their vetting reports in any form, be it PDF, videos, images with notes. The complete vetting history is then maintained for audit purposes.

Catering PKI of all sizes

Khatim RA Server seamlessly manages X.509 certificate issuance, catering to diverse infrastructures and compliance standards, including Closed PKI, Public, and National PKI environments. Whether your needs align with closed, restricted systems or the broader, more public-facing spectrum of PKI, our solution adeptly caters to varying infrastructure requirements, ensuring comprehensive certificate handling across diverse landscapes.

One Portal, multiple Organizations

One Portal, multiple Organizations
Khatim RA Server simplifies managing multiple Organizations and their linked service plans. Service plans helps PKI admins setup what type of certificates an organization needs to create and any limits applied (count, expiry, vetting, agreements etc.) allowing subscriptions management super easy.

Secure GUI based administration

Control your RA server administration with secure GUI based interfaces. Ensures military grade security (AES 256) to your RA server instance for administration using TLS client authentication. From policy management to transaction log viewing all can be done from a single place. For LRA admins and LRA User, authentication is done using user id & password.

Cross Platform Deployments

Khatim RA server is built with platform independence in mind hence supports Windows and Linux alike. You can deploy in different environments be it on-premise, private or public cloud, VMs or physical machines.

Developer Integration

Want to control your RA from your CRM, ECM etc? No issues, with Restful APIs, business applications remain in command of their RA be it configurations, setting up organization, vetting, plans and more.

Unlimited Scalability

Prepare for an unparalleled RA experience with the Khatim RA server! Utilize its clustering feature, enabling multiple RA servers to operate concurrently, minimizing latency. You can seamlessly integrate new RA servers without halting ongoing instances, ensuring the seamless flow of your operations. Bid farewell to sluggish performance and embrace lightning-fast CLM capabilities with Khatim RA server!

Cryptographic Agility

Keeping in view businesses having different cryptographic needs such as, Khatim RA server allows support of the following cryptographic algorithms.

– RSA (2048, 4096, 8192)
– ECDSA (192, 224, 256, 320, 384, 512)
– SHA-256, 384 and 512 hashing algorithms

Proactive Alerts & Troubleshooting

In instances where the Khatim RA server encounters operational disruptions, it proactively alerts administrators, prompting swift action. To ensure comprehensive tracking, all incidents are meticulously logged, providing the option to securely transmit data to central logging systems like Splunk, Grafana, Greylog, LogRhythm, and others for detailed monitoring and analysis.

Reporting & Statistics

Access real-time statistics reflecting your RA performance in the form of graphs. Administrators can delve into various data points such as successful and failed certificate issuance, expired or about-to-expire certificates, alerts, certificate algorithms, and more. Khatim RA Server generates daily summary reports, offering a snapshot of the day's certificate generation details, including certificate types, failures, and alerts, empowering administrators with crucial insights.

Logging & Auditing

The Khatim RA server diligently logs all inbound transactions and configurations for in-depth analysis, encompassing vetting details submitted. This encompasses automated API calls, interactions via ACME, SCEP protocol, or manual inputs. Administrators possess the capability to instantly retrieve and scrutinize request and response data, facilitating real-time troubleshooting whenever necessary.

Architecture

Khatim RA Server consist of 3 core components which are Khatim RA Portal, Khatim RA API and Khatim RA Diagnostic.

Khatim RA Portal

The portal provides a central, secure, GUI based management console to manage all the configurations of the RA. Some of these are setting up organizations, certificate types, vetting configurations, service plans.

Administrators can also view statistics, reports and transaction logs to get a better understanding of how the RA is functioning.

Multiple instances of Khatim RA Portal can also run to achieve a reliable fault tolerant architecture.

Khatim RA APIs

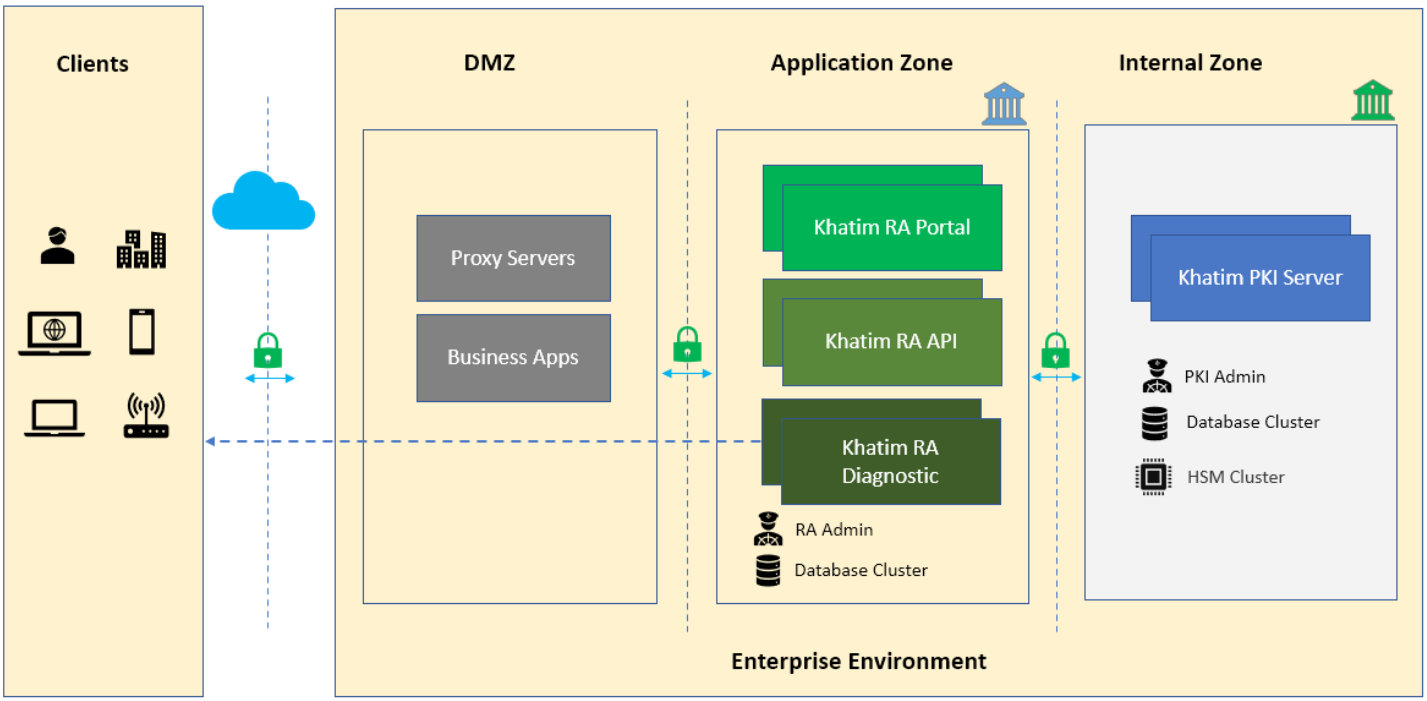
Khatim RA APIs allowing either business apps to interact with RA configurations accessible over the TLS client auth or use the standard API interfaces such as ACME, SCEP etc. accessible over TLS Server auth.

Multiple instances of Khatim RA APIs can also run to achieve a reliable fault tolerant architecture.

Khatim RA Diagnostic

Khatim Diagnostic components provides background processing of events such as notifications, monitoring and daily summary reporting.

Khatim Diagnostic runs in an active-passive mode.



Algorithms / Standards

- RSA
- ECDSA
- ACME
- SCEP
- RFC 5280

Certificate Types

Types

- X.509
- S/Mime (MV, OV, SV, IV)
- TLS/SSL Certificate (DV, OV, IV, EV)
- AATL or Qualified Certificates
- Code Signing

Key Storage

- PFX/PKCS#12
- HSM (At Khatim PKI Server)

Supported OS / Languages / H/W

- Windows Server & Linux (Centos, Ubuntu, RedHat, Fedora)
- Supported Language: English
- 8 GB RAM, 2 vCPU (2.3 GHz), 10 GB Hard disk

Codegic
www.codegic.com
info@codegic.com

codegic

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 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.

Learn more at www.codegic.com