

Khatim PKI Server

Powerful & Scalable CA / PKI server.

- ✔ Compatible with Web Trust, IETF 5280, CA/B forum standards
- ✔ Quickly setup Root CA, Sub CA, online or offline PKIs
- ✔ Seamless integration with PKCS#11 or cloud based HSMs
- ✔ Easy to integrate with business apps using developer friendly APIs
- ✔ User-friendly dashboards for reporting, alerting, logging, and insights

Empowering trust, for a secure tomorrow

Purpose of a CA / PKI

CA / PKI Servers are responsible for managing the complete life cycle of setting up Certification Authorities. It starts by setting up a Root CA followed by Subordinate CAs issuing, validating, and revoking end-entity (users, devices, IOT) X.509 digital certificates & CRLs. This allows all communication and transactions between users and devices to be secure, trusted, and authenticated.

By providing a secure and trusted infrastructure for managing digital certificates and keys, a CA/PKI Server enables organizations to establish a strong foundation of trust in their networked environments. This helps to protect sensitive information, prevent data breaches, and ensure compliance with regulatory requirements.



Fast



Secure



Quick Deploy

What makes Codegic the best Certification Authority software?

Web Trust, CA/B Forum Compliant

Compliant with industry standards is essential in today's business environment. Khatim PKI Server adheres to all the recommended guidelines from WebTrust, CA/B Forum, and IETF standards, meeting the regulatory and market requirements.

Simple PKI management

Complex PKI systems cause confusion and increase the chances of errors. Khatim PKI Server stands out with its user-friendly web-based graphical user interface (GUI) for administrators. This facilitates faster deployment, integration, and testing compared to other solutions available on the market.

Secured Processing & Auditing

Ensuring a high level of security and assurance is paramount in any business. Khatim PKI Server accomplishes this by employing military-grade security measures across all its functions, including key management, CA management, certificate issuance and transaction management.

Key Features

Standard & Compliant

Khatim PKI Server adheres to the industry standards set by Web Trust, IETF and CA/B Forum for Certification Authorities including RFC 5280. Khatim PKI Server helps organizations in joining root certification programs by providing the necessary functionalities and features to meet their requirements.

Cross Platform, Diverse Deployments

The Khatim PKI server is platform-independent, making it compatible with both Windows and Linux. It can be deployed in various environments such as:

- On-premise private or public cloud
- VMs
- Physical machines

Military Grade Access Control

Trusted personnel can only access CA functions via powerful, password less authentication using military-grade TLS Client authentication.

Unlimited Scalability

Khatim PKI Server can be clustered, minimizing latency enabling high throughput. It allows for new servers to be added seamlessly without the need to stop running instances, ensuring uninterrupted service for your business. Khatim PKI Server can meet the growing needs of your enterprise and ensure that your digital security infrastructure can keep pace with your business growth.

Support all HSMs

Integrate with your existing HSMs using PKCS#11 like Entrust nShield, Thales Luna, Protect Server, Utimaco Cryptoserver etc. It also seamlessly integrates with non PKCS#11 based HSM like Microsoft Azure Key Vault, AWS Cloud HSM and Google Cloud HSM.

Cryptographic Agility

Khatim PKI server supports diverse cryptographic requirements such as:

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

Revocation & CRL Issuance

Khatim PKI Server allows quick revocation of existing digital certificates. Configure your CA to issue CRLs at recurring time frames avoiding the hassle of manual CRL issuance.

Reporting & Statistics

Admins can monitor their PKI servers in real-time, and filter data based on CA policies, templates, success/failure, signing algorithm, and more. Khatim PKI server also creates daily summary reports along similar data points providing administrator a snapshot of what types of certificates were generated during the day, any failures and alerts.

Logging & Auditing

Khatim PKI Server saves all incoming transactions and configurations for thorough analysis.

Administrators can easily download and review request/responses in real-time for investigation. All updates made to the system by operators is also recorded providing a reliable audit trail.

Serve Multiple CAs & PKIs

Have multiple CAs or PKIs? A single deployment of Khatim PKI Server can handle multiple Certification Authorities, online/offline CAs making it easy to handle from a single portal.

Proactive Alerts & Troubleshooting

Khatim PKI Server sends proactive notifications to administrators in case of server malfunction. All issues are recorded for traceability and can also be securely pushed to your central logging systems such:

- Splunk
- Grafana
- Greylog
- LogRhythm etc.

365 Protection

Khatim PKI Server lets you issue digital certificate for all the purposes required to ensure a trusted infrastructure. Some of the certificate types are:

- Email / Document Signing
- SSL Client / Server / VPN Authentication
- Code Signing
- Timestamping Certificate
- OCSP

Simplified Migration

Upgrade to Khatim PKI Server for your existing Root CA or Sub CA keys/certificates. Say goodbye to legacy CA servers effortlessly and adopt the new way of managing keys and certificates with more control and insights.

Developer friendly Integration

PKI Admins can either manually issue X.509 digital certificates based on PKCS#10/CSR or allow business applications to request for client-end certificate via Restful programmatic interfaces. Keep your business applications in charge of creating, deleting or revoking digital certificates.

Ensuring IoT Security

Khatim PKI Server seamlessly issues digital certificates to IoT devices, allowing them to securely authenticate themselves and communicate with other devices and systems.

Algorithms

- RSA, ECDSA, PKCS#11, RFC 5280, X.500

Supported OS / Languages / H/W

- All flavors of 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. All Rights Reserved



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