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

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, **Khatim 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. With blazing fast speed, great user experience, multilingual UI and complying with all security standards Khatim PKI Server simplifies your day to day PKI administration.

Reliable

Secure

Resilient

What makes Codegic the best CA software?

Standards 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

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

Khatim PKI Server accomplishes security 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.

Support all HSMs

Integrate with your existing HSMs using PKCS#11 from all major HSM vendors such as:
– Entrust nShield
– Thales
– Utimaco
– Amazon AWS Cloud HSM
– Microsoft Azure Key Vault

Cross Platform 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

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
– Dilithium (PQC)

Military Grade Access Control

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

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.

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

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

Server can meet the growing needs of your enterprise and ensure that your digital security infrastructure can keep pace with your business growth.

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

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, 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 APIs

Comes with intuitive GUI for easy monitoring of key metrics and data analysis. Management portal is also accessible using API over TLS client authentication.

Ensuring IoT Security

Seamlessly issues digital certificates to IoT devices allowing them to securely authenticate themselves & communicate with other devices & systems.

Management Portal

Comes with intuitive GUI for easy monitoring of key metrics and data analysis. Management portal is also accessible with APIs over TLS client authentication.

Algorithms / Protocols

- RSA (2048/3072/4096/8192)
- ECDSA (NIST_P, SECP (K1,R1), BRAINPOOL (R1,T1) – 160, 192, 224, 256, 384, 521)
- PKCS#11
- PKCS#1 - PKCS#15, PSS
- AD/LDAP, SCEP, CMP
- SMTP, HTTP, HTTP/s, REST
- RFC 5280, 2986, 8666, X.500, SMTP
- X.509 Certificate & CRLs
- SNMP, Syslog
- Dilithium (Post Quantum Cryptography)

Performance

- RSA 2048 bits – 115 TPS
- RSA 4096 bits – 34 TPS
- RSA 8192 bits – 7 TPS
- ECDSA secp256r1 – 200 TPS
- ECDSA secp256r1 – 134 TPS
- ECDSA secp521r1 – 83 TPS
- ECDSA secp521r1 – 80 TPS

* Tested with Entrust HSM XC Solo Base (single instance)

Supported OS / Languages / H/W

- All flavors of Windows Server & Linux *(Centos, Ubuntu, RedHat, Fedora)*
- 10+ Languages including English, Mongolia, Spanish etc.
- 8 GB RAM, 4 vCPU (2.3 GHz), 10 GB Hard disk

Codegic
www.codegic.com
info@codegic.com

Certifications

- ISO 9001:2015
- ISO 14001:2015
- ISO 27001:2022

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 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.

Learn more at www.codegic.com