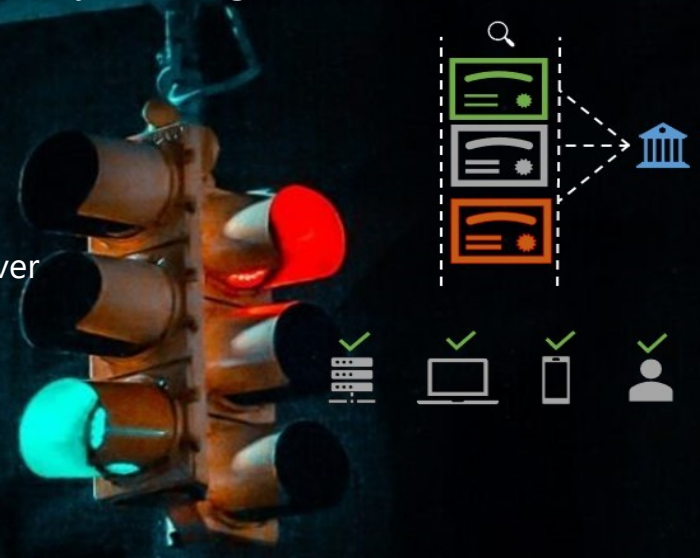
Khatim OCSP Server

High Assurance, Resilient, OCSP server with industry-leading speed

- Compatible with IETF 6960, 5019 standards
- Get Advanced OCSP insights, reporting & alerting
- Enterprise ready, secure and quick to deploy OCSP server
- Provide real-time or CRL based revocation
- Supports both for online &, off-line CAs and PKIs



Purpose of an OCSP Server

The Online Certificate Status Protocol (OCSP) server aka Validation Authority is an essential tool for verifying the revocation status of X.509 digital certificates. By checking the revocation status of a certificate, one can ensure that the certificate is still valid and can be trusted. The use of OCSP servers reduces the overheads associated with traditional Certificate Revocation Lists (CRLs) and provides a more efficient and scalable method for certificate validation. Selecting the right OCSP server is hence a crucial step in your digital transformation journey providing timely access to critical business services.

"OCSP provides a pivotal role in establishing Digital Trust"

Reliable **Secure** **Resilient**

What makes Codegic the best OCSP Server vendor?

Built for Speed

In the realm of validating digital certificates, time is of the essence. Khatim OCSP server offers market-leading performance designed to cater to high-volume OCSP processing. With proper configurations get 2000+ TPS.

Secured Processing

Establishing a high level of security and assurance is crucial in any business. Khatim OCSP server achieves this by utilizing military-grade security measures for all its functions, including key management, OCSP signing, administration, and transaction management.

Keeping it simple

Complicated OCSP systems can lead to confusion and increase the likelihood of errors. Khatim OCSP server, boasts user-friendly web GUI for administrators, making deployment, integration & testing much quicker than other solutions.

Key Features

Cross Platform Deployments

The Khatim OCSP server is platform-independent, making it compatible with both Windows and Linux. It can be easily deployed in various environments. You can deploy in different environments be it on-**premise**, **private** or **public cloud**, VMs or physical machines.

Proactive Alerts & Traceability

Khatim OCSP 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 as: Splunk, Grafana, Greylog, LogRhythm etc.

Military Grade Access Control

Trusted resources access key functions via powerful, multi factor authentication using military-grade TLS Client authentication.

Admin Friendly GUI

Control your OCSP server administration with GUI based interfaces. From key generation, policy handling to transaction viewing & downloading of request can be done from a single pane of glass.

Standards Compliant

Khatim OCSP Server adheres to the industry standards set by **IETF** and **CA/B Forum** for OCSP response, which includes RFC 6960 and 5019 profiles. This allows seamless integration with a wide range of business applications such as Adobe Acrobat, Microsoft Office, web browsers & web servers.

Logging & Auditing

Khatim OCSP server logs and saves all incoming transactions and configurations for thorough analysis. Administrators can easily download and review request/responses in real-time for server status checks and troubleshooting purposes. All updates made to the system is also recorded providing with integrity to ensure reliable audits.

Cryptographic Agility

Khatim OCSP server supports diverse cryptographic requirements such as:

– RSA (1024, 2048, 4096, 8192)
– ECDSA (192, 224, 256, 320, 384, 512)
– SHA-256, 384 and 512 hashing algorithms
– Dilithium (PQC)

Support any HSM & CAs

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.

Unlimited Scalability

Khatim OCSP server can form a cluster of multiple OCSP servers to minimize latency. New OCSP servers can be added without stopping the running instances, resulting in high throughput.

Serve Multiple CAs & PKIs

Have multiple CAs or PKIs? A single deployment of Khatim OCSP Server can handle multiple Certification Authorities, PKI, local or remote CAs. Easily setup multiple OCSP policies by identifying OCSP signing certificate, CA to serve, whether to add extended revocation information and more.

Provides Real-time Revocation

Khatim OCSP Server offers a range of options for revocation checking, including real-time by accessing the list of issued digital certificates by the CA. It can also pull CRLs issued external CAs (over HTTP or LDAP) to respond to incoming OCSP requests, making it compatible with both online and offline CAs.

Management Portal

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

OCSP Insights & Reporting

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

Drop-in OCSP Server

Upgrade to Khatim OCSP Server and eliminate performance bottlenecks while reusing your existing OCSP keys. Say goodbye to legacy OCSP servers effortlessly.

Algorithms / Protocols

- RSA
- ECDSA
- PKCS#11
- SNMP, Syslog
- SMTP, HTTP, HTTP/s, REST
- RFC 2560, 6960, 5019, 4387
- Dilithium (Post Quantum Cryptography)

Performance

- RSA 2048 - 1700 TPS and up to 2400 TPS

* Tested with Entrust HSM XC Solo Mid (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