Khatim Verification Server

ETSI & eIDAS-Compliant Digital Signature Verification Server

- Ensures compliance with eIDAS, ETSI, and global standards
- Validates timestamps, revocation status, and certificate chains
- Supports long-term validation (LTV) for archived documents
- Supports PAdES, XAdES, JAdES, CAdES, ASiC, PKCS#7, PKCS#1 & more
- User-friendly dashboards for live reporting, alerting, logging, and insights

Purpose of a Digital Signature Verification Server

Verifying the authenticity of digitally signed documents is critical for ensuring trust, compliance, and long-term legal validity. Without proper verification against trusted sources and cryptographic standards, digital signatures lose their evidentiary value. A digital signature verification server ensures that signatures are valid, certificates are trusted, and timestamps are accurate—at the time of validation and into the future.

Khatim Verification Server enables organizations to seamlessly validate digital signatures using ETSI/eIDAS standards, EU Trusted Lists (LOTL/TSL), and trusted timestamping. It integrates easily with existing enterprise systems to verify document integrity, authenticity, signer identity, and signature status across time.

In a cross-border digital ecosystem driven by the eIDAS regulation, Khatim Verification Server becomes essential in building a verifiable, audit-ready trust chain—preserving legal enforceability of documents for years to come.

What makes Khatim Verification Server the best?

Built for Enterprises

Whether integrated with CRMs, ECMs, or ERPs, it delivers rapid and reliable digital signature verification—ideal for high-volume, trust-critical environments.

Fine grained Control

Get full control over acceptable cryptographic algorithms, giving enterprises precise control over digital signature verification.

Secured & Trusted Validations

Enforces strict security for certificate chain validation, revocation checking, and trust list management following ETSI & eIDAS standards.

Unified Monitoring

Gain full visibility with real-time & historical signature verification insights across your infrastructure from a centralized dashboard.

Key Features

Supported Signature Formats

Verifies advanced digital signatures based on IETF and ETSI standards including: XAdES, CAdES, PAdES, JAdES, ASiC, PKCS#7 & PKCS#1 signatures formats. Performs detailed revocation & PKI trust building checks for all of the certificates found against signer, timestamp & OCSP.

Use EU Trust Lists and LOTL

Allows multiple verification policies to handle diverse trust and compliance requirements—such as accepted cryptographic algorithms, signature formats, and trust sources including the EU Trust List, List of Trusted Lists (LOTL) & custom cert stores. This flexibility enables tailored validation for different business applications and regulatory environments.

Cross Platform Deployments

Khatim Verification 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.

Proactive Alerts & Traceability

For traceability, all issues are recorded which can be pushed securely to your central logging systems e.g. Splunk, Grafana, Greylog, LogRhythm etc.

API Integration

Khatim Verification Server offers developer-friendly, Restful APIs for rapid integration with your ECM, CRM, and CMS platforms. All endpoints are secured via TLS client authentication, enabling secure and efficient deployment in minutes.

Logging

Every digital signature verification request is logged with full cryptographic traceability—including certificate chains, CRLs, OCSP responses, timestamps, and trust list sources. Admins can review raw inputs and verification outcomes for diagnostics or audits at any time.

Cryptographic Agility & PQC

Keeping in view businesses having different cryptographic needs, Khatim verification server supports both RSA, ECDSA, PQC cryptography with SHA-256, 384 and 512 hashing algorithms.

Live Reporting

Khatim Verification Server offers live reporting and historical trend analysis, enabling real-time monitoring & usage insights.

Unlimited Scalability

Khatim Verification server can be installed as a cluster of multiple individual verification servers to reduce latency.

Admin Friendly GUI

Manage trust lists, verification policies, and logs through an intuitive web-based interface. From configuring LOTL/TOTL sources to reviewing validation results, all admin functions are accessible in one place.

Algorithms / Protocols

- RSA, ECDSA
- PQC (Dilithium)
- PKCS#11
- RFC 5280
- RFC 3161

Supported OS / Languages / H/W

- All flavors of Windows Server & Linux *(Centos Stream, Ubuntu, RedHat, Fedora)*
- 50 Languages including English, French, Spanish, Arabic, Chinese, Japanese, Italian, Polish, Swedish, Russian & more.
- 8 GB RAM, 2 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