codegic

Trusted Timestamping

Khatim Timestamp Server

High assurance cryptographic, trusted timestamp server with market-leading performance

750+	<1 sec	eIDAS	PQC
Timestamp/Sec	**Time Accuracy**	**Advanced & Qualified**	**ML-DSA Ready**
Built for Speed	*NTP-validated*	*Timestamps for TSPs*	*Future-proof evidence*

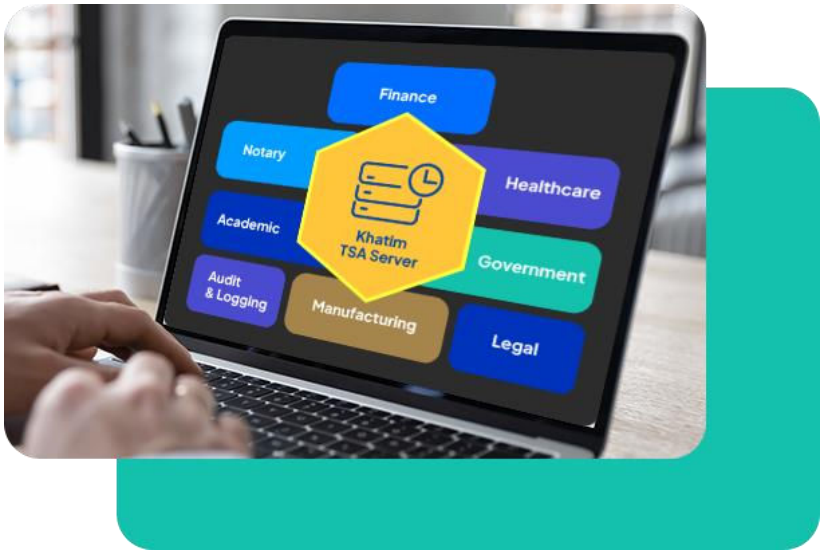
Digital signature preservation made simple!

With the emergence of global standard and regulation for digital signatures, cryptographic timestamping has now become a cornerstone in the evolving digital trust landscape. **Khatim Timestamp Server** (KTS) plays a pivotal role ensuring all of the cryptographic objects identified during digital signature creation remain trusted.

- Enterprise ready, secure and quick to deploy
- Compatible with ETSI & IETF advanced digital signature standards
- Scalable timestamp software securing high valued transactions
- Seamlessly integrate with existing business system & HSMs
- Generates **Advanced** or **Qualified** cryptographic timestamps from multiple trusted time sources

Khatim Timestamp Server issues:

- RFC 3161 timestamp tokens (with RFC 5816 ESSCertIDv2 support)
- Aligned with ETSI TS 101 861, ETSI TS 102 023 and ETSI EN 319 422
- ISO/IEC 18014 time-stamping framework
- CWA 14167-1 trustworthy-system requirements for CA/TSP operations



Ten Pillars of Trusted Timestamping

01
Policies & Access Control
Multiple policies mapped to policy OIDs, signing certificates, hash algorithms and time sources; administrator management and full operator audit trails.

02
Transaction & NTP Logs
Complete request/response transaction logs and precise NTP logs proving what time was received and whether it was trusted.

03
Live Monitoring & Historical Intelligence
Real-time TPS and success/failure telemetry across the cluster, plus deep searchable historical trends from a single pane of glass.

04
Service Plan Management for TSPs
Native quota and plan enforcement, account segmentation and API-driven management to run timestamping as a commercial service.

05
RFC 3161 NTP Integration & ETSI/eIDAS
Multi-source NTP validation, drift thresholds and automated signing holds, aligned to RFC 3161 / 5816 and ETSI EN 319 422.

06
Detailed Logging & Auditing
Every transaction captured with rich metadata, human-readable parsing, powerful search and integrity-safe archival.

07
Post-Quantum Ready Timestamping
Cryptographic agility across RSA, ECDSA and PQC (ML-DSA) so long-term evidence survives the quantum transition.

08
PKCS#11 Integration
Rapid integration with leading HSMs and smart cards over PKCS#11, plus software keystores where HSMs aren’t required.

09
Proactive Alerts & SIEM Integration
Proactive event alerts pushed securely to Splunk, Grafana, Graylog and LogRhythm, with email and daily summary reporting.

10
Military Grade Access Control & GUI
Secure every key function, a full operator audit trail, and unified GUI-based administration from a single pane.

PILLAR 01 · POLICIES & ACCESS CONTROL

Flexible Issuance Policies and Governed Administration

The Challenge: One Size Never Fits Every Client

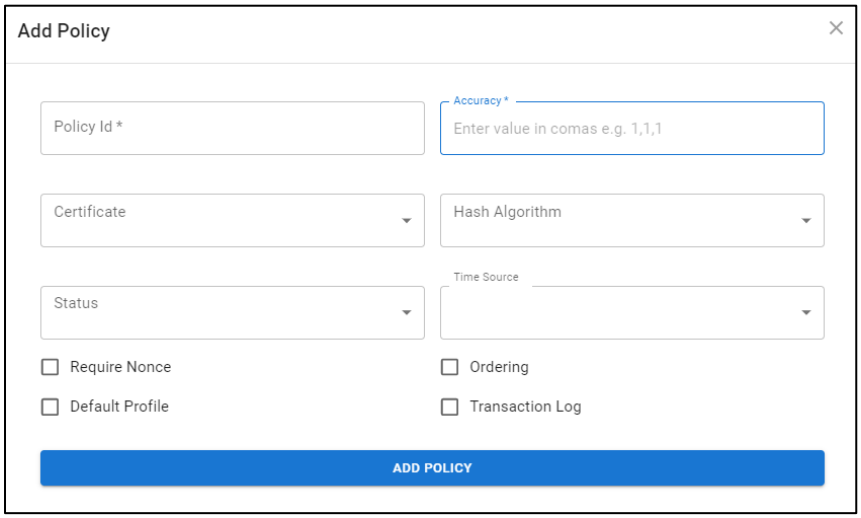
A Trust Service Provider rarely serves a single use case. Different business applications demand different signing certificates, hash strengths, policy identifiers and time sources — and every one of those choices carries legal and compliance weight. At the same time, a TSA is Tier-0 trust infrastructure: the ability to change a policy, rotate a key, or add an operator must itself be controlled and provable. Without policy flexibility, operators are forced into rigid, lowest-common-denominator configurations; without governed access control, changes happen silently and audits fail.

What Khatim Delivers

Multiple, OID-Mapped Policies. Administrators can create multiple timestamp policies, each mapped to a policy OID, a timestamp signing certificate, a hash algorithm, a time source and more. This directly supports the RFC 3161 requirement that each token assert the TSA policy under which it was issued, and the ETSI TS 102 023 / EN 319 422 model where a TSA operates under one or more declared time-stamping policies. Requests referencing an unsupported policy are cleanly rejected with the RFC 3161 unacceptedPolicy status.

Governed Access Control. The Access Control function lets administrators manage other administrators and view operator logs — a full audit trail of every configuration change made by every operator. This separation of duties and traceability of privileged action aligns with the trustworthy-system and personnel-control requirements of CWA 14167-1 and the ETSI EN 319 422 security controls for TSA operation.

- Create and manage multiple issuance policies (unlimited flexibility per client)
- Map each policy to OID, signing certificate, hash algorithm and time source
- Manage administrator accounts and privileges centrally
- Full operator audit trail — who changed what, and when
- Enforce policy conformance at request time (unsupported policies rejected)



PILLAR 02 · TRANSACTION & NTP LOGS

A Complete, Forensic Record of every Timestamp

The Challenge: Failures and Disputes Demand Evidence, Not Guesswork

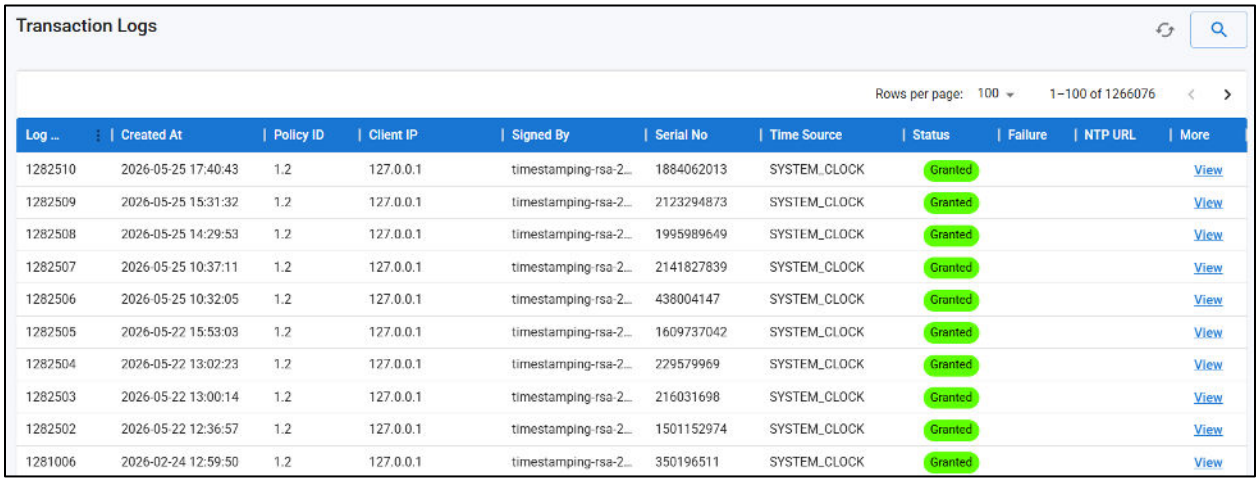
When a timestamp fails or a client disputes a token, “the server was probably fine” is not an answer an auditor or a court will accept. Operators need to see exactly what was requested, what time source was used, which policy applied, and precisely why a request succeeded or failed — down to the RFC 3161 status code.

What Khatim Delivers

Transaction Logs. KTS records the full list of timestamp transactions as they are created, giving administrators the time the request was processed, the incoming message imprint (data hash), success or failure details, the policy used, the detailed request/response, the requestor and host IP addresses, and the time source. Failures are mapped directly to the RFC 3161 status set — badAlg, badRequest, badDataFormat, timeNotAvailable, unacceptedPolicy, unacceptedExtension, addInfoNotAvailable and systemFailure — so root cause is immediate.

NTP Logs. The NTP logs record precisely what was received from each NTP server — invaluable for auditing and compliance. Administrators can prove to clients what time was obtained, from which NTP server, whether it was trusted, when a system-clock drift occurred, and to what extent. At startup an NTP monitor validates the system clock against configured NTP servers; if drift exceeds the configured threshold (e.g. 1 second) an alert is raised and KTS responds with timeNotAvailable, upholding the ISO/IEC 18014 and ETSI EN 319 422 requirement that tokens only assert time the TSA can vouch for.

- Every request/response captured as it happens
- Message imprint, policy, time source, requestor/host IP recorded
- Failures mapped to RFC 3161 status codes for instant diagnosis
- NTP logs prove the time received, its source, and whether it was trusted
- Drift detection triggers alerts and timeNotAvailable responses



Log …	Created At	Policy ID	Client IP	Signed By	Serial No	Time Source	Status	Failure	NTP URL	More
1282510	2026-05-25 17:40:43	1.2	127.0.0.1	timestamping-rsa-2…	1884062013	SYSTEM_CLOCK	Granted			View
1282509	2026-05-25 15:31:32	1.2	127.0.0.1	timestamping-rsa-2…	2123294873	SYSTEM_CLOCK	Granted			View
1282508	2026-05-25 14:29:53	1.2	127.0.0.1	timestamping-rsa-2…	1995989649	SYSTEM_CLOCK	Granted			View
1282507	2026-05-25 10:37:11	1.2	127.0.0.1	timestamping-rsa-2…	2141827839	SYSTEM_CLOCK	Granted			View
1282506	2026-05-25 10:32:05	1.2	127.0.0.1	timestamping-rsa-2…	438004147	SYSTEM_CLOCK	Granted			View
1282505	2026-05-22 15:53:03	1.2	127.0.0.1	timestamping-rsa-2…	1609737042	SYSTEM_CLOCK	Granted			View
1282504	2026-05-22 13:02:23	1.2	127.0.0.1	timestamping-rsa-2…	229579969	SYSTEM_CLOCK	Granted			View
1282503	2026-05-22 13:00:14	1.2	127.0.0.1	timestamping-rsa-2…	216031698	SYSTEM_CLOCK	Granted			View
1282502	2026-05-22 12:36:57	1.2	127.0.0.1	timestamping-rsa-2…	1501152974	SYSTEM_CLOCK	Granted			View
1281006	2026-02-24 12:59:50	1.2	127.0.0.1	timestamping-rsa-2…	350196511	SYSTEM_CLOCK	Granted			View

PILLAR 03 · LIVE MONITORING & HISTORICAL INTELLIGENCE

Real-time Visibility Across your Timestamp Cluster

The Challenge: A Timestamp Service Should Never Be a Black Box

Modern Trust Service Providers cannot wait for end-of-day reports to discover problems. Operations teams need instant awareness of performance, failures and load distribution.

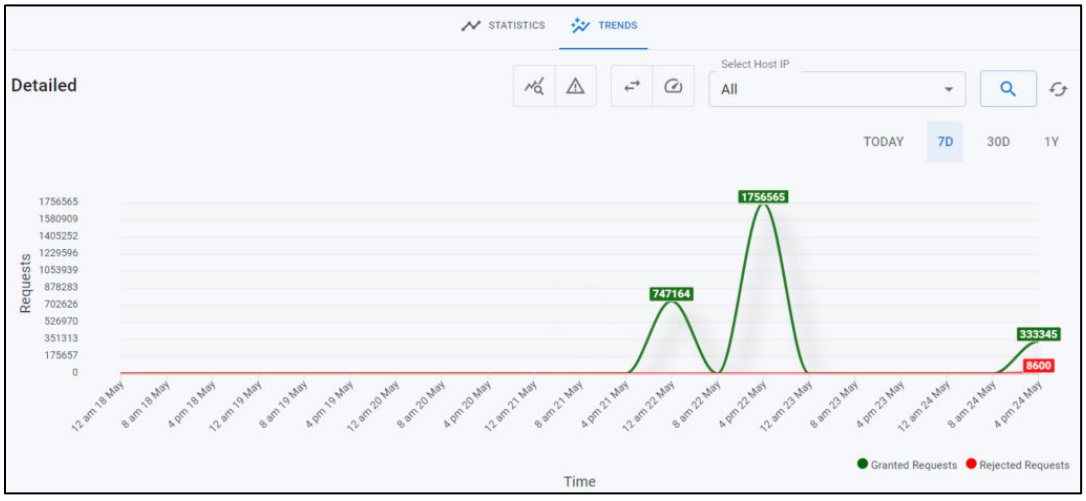
What Khatim Delivers

Native Live Telemetry. A built-in unified live dashboard lets administrators monitor transactions per second (TPS), success rates and failures across clustered timestamp engines from a single screen.

Historical Trends That Explain the Present. Live data tells you what is happening; history tells you why. Deep, searchable historical analytics let teams review behaviour over time and correlate spikes.

Drill Down by Server or Client. In commercial, multi-tenant environments, visibility must go beyond totals. Khatim Timestamp Server filters and analyses by timestamp server IP (per-instance performance), client application name (consumption, behaviour and demand patterns) and individual request/response contribution per source — invaluable for troubleshooting, SLA validation and customer relationship management.

- No third-party tooling — analytics delivered natively from the server
- Filterable historical trends (today / 7d / 30d / 365d / custom)



PILLAR 04 · SERVICE PLAN MANAGEMENT FOR TRUST SERVICE PROVIDERS

Operate Trust like a Service, not a struggle

The Challenge: Cryptography Is Only Half of Running a Timestamp Business

Running a timestamp service is not just about cryptography — it is about delivering predictable, billable and controllable services to customers. Trust Service Providers must manage entitlements, consumption and fair usage across many clients while maintaining strict assurance levels.

What Khatim Timestamp Server Delivers

Native Quota & Plan Enforcement — A Rare Capability. What sets Khatim Timestamp Server apart is that quota enforcement is built directly into the timestamp platform, not bolted on externally. TSPs can define timestamp volumes per customer or application; enforce limits automatically during RFC 3161 requests (unlimited, recurring or fixed); prevent overuse while allowing controlled scaling; track consumption in real time; expose usage via portal or API for billing integration; and adjust allocations instantly without service interruption.

Account Types Designed for TSP Ecosystems. Khatim Timestamp Server supports multiple account models with different authentication mechanisms — Basic Authentication, CMS-based Authentication, and No Authentication — so providers can map real-world customer structures directly into the system. Through the portal or API, TSPs can provision and manage customer accounts, assign plans and quotas, issue credentials securely, track activity per entity, and separate administration from consumption roles.

- Native, in-platform quota enforcement (unlimited / recurring / fixed)
- Real-time consumption tracking, exposed via portal or API
- Instant allocation changes with no service interruption
- Multiple account/authentication models (Basic, CMS, None)
- Separation of administration from consumption roles
- Add servers without stopping instances

PILLAR 05 · RFC 3161, NTP INTEGRATION & ETSI/EIDAS COMPLIANCE

If Time can't be Trusted, neither can the Timestamp

The Challenge: Precise, Provable Time Is the Foundation of Every Token

For an RFC 3161 Timestamp Authority, accurate and provably-correct system time is fundamental — timestamps are legal and technical proof that data existed at a particular instant. Even small clock drift or inconsistent time sources can invalidate long-term evidence or trigger timeNotAvailable errors. Khatim Timestamp Server treats time integrity as a first-class requirement.

What Khatim Timestamp Server Delivers

Standards-Aligned Time Assurance. KTS issues RFC 3161 tokens (with RFC 5816 ESSCertIDv2) and can synchronize using system time, NTP (RFC 1305) or SNTP (RFC 2030). It connects to one or more NTP servers and continuously validates the system clock before issuing tokens, in line with the accuracy and auditability expectations of ETSI TS 101 861, ETSI TS 102 023, ETSI EN 319 422, ETSI EN 319 421 and the ISO/IEC 18014 time-stamping framework.

Multi-Source Validation & Automated Holds. Administrators can configure multiple stratum-2 or stratum-3 NTP endpoints (primary + fallbacks) to avoid a single point of failure, choose "check-all" or "first-pass" modes, set tiebreak rules, tune retries and intervals, and define acceptable drift (ms). If drift exceeds limits or checks fail repeatedly, KTS automatically pauses issuance and raises high-urgency alerts preventing issuance of questionable tokens.

One-of-a-Kind NTP Transaction Log Viewer. Every NTP query/response is recorded in human-readable form — precision, NTP version, stratum, offset, round-trip time, jitter, reachability and last successful check — turning time verification into forensic evidence rather than a buried error code. Statistical dashboards chart offset, drift, precision and pass/fail counts (today / 7d / 30d / 365d / custom), and NTP anomalies are visually correlated with RFC 3161 errors, HSM events and issuance trends for rapid root-cause analysis. Signed NTP transactions can be exported (CSV) and included in timestamping reports for auditors, courts and compliance reviews.

- System time, NTP (RFC 1305) or SNTP (RFC 2030) time sources
- Multiple stratum-2/3 endpoints, check-all / first-pass, tiebreak rules
- Configurable drift threshold with automated signing holds
- Per-server telemetry: offset, stratum, jitter, RTT, reachability

PILLAR 06 · DETAILED LOGGING & AUDITING FOR FULL TRACEABILITY

If it Happened, It's Recorded

The Challenge: Trust Services Must Be Provable

Whether for audits, incident response or customer disputes, operators need a complete and reliable history of what happened. Assumptions are not evidence.

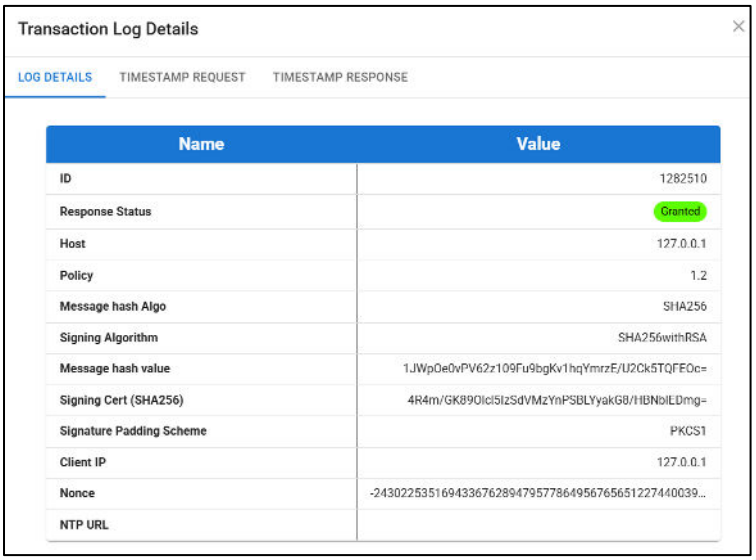
What Khatim Timestamp Server Delivers

Capture Every Transaction. KTS records every incoming request and generated response with rich operational metadata: success or failure status, exact processing time, client IP and host information, applied policy, time source used, and the certificate that signed the response. Nothing is lost; every action is attributable — meeting the event-logging and record-keeping obligations of CWA 14167-1 and ETSI EN 319 422.

Understand Requests in Human Language. Raw ASN.1 is for machines, not investigations. Khatim Timestamp Server transforms timestamp messages into clear, human-readable views so administrators can inspect parsed request/response details, validate policy and algorithm usage, confirm signer identity, and download the original request/response files for external or forensic analysis.

Powerful Search, Export & Integrity-Safe Archival. Advanced multi-parameter search filters logs by Log ID, Nonce, Policy, Host IP, Client IP, Signing Certificate Alias, Serial Number, Time Source, NTP URL, PKI status, failure information, hash algorithm and more. For long-term retention, logs are archived in CSV, packaged, compressed and protected in an integrity-friendly manner for regulatory or contractual needs.

- Full request/response capture with signer, policy, time source and IPs
- Human-readable parsing of ASN.1 request/response structures
- Downloadable originals for forensic analysis
- Multi-parameter search across a dozen-plus attributes



PILLAR 07 · POST QUANTUM READY TIMESTAMPING

Future-Proofing Starts Today

The Challenge: Today's Evidence Must Survive Tomorrow's Computers

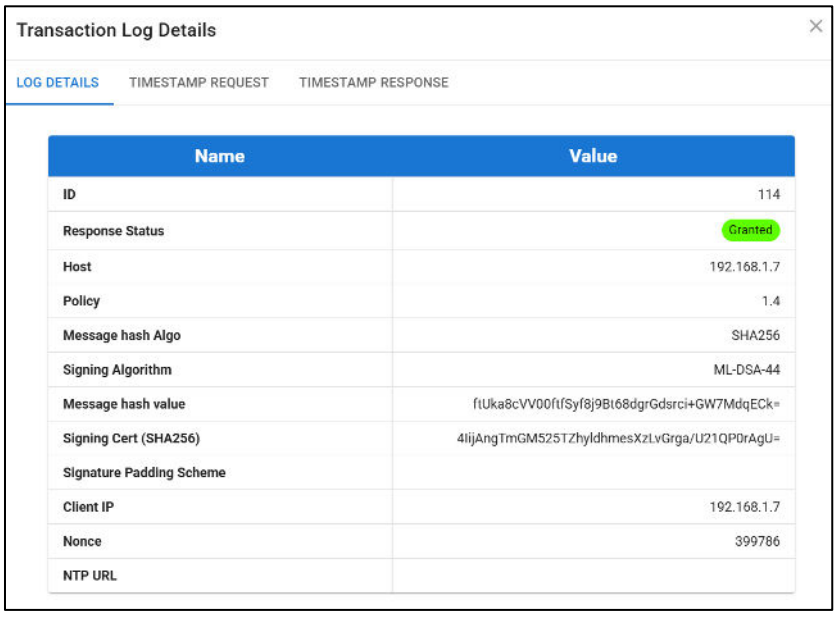
RFC 3161 timestamps often prove that data existed at a specific moment — and many of these proofs must survive years or decades. As quantum computing advances, the classical cryptography underpinning those tokens will eventually face new attack models. Organizations relying on long-term proof (contracts, medical records, financial archives, intellectual property, government data) must begin preparing for cryptographic migration now.

What Khatim Timestamp Server Delivers

Cryptographic Agility with PQC. Recognizing that businesses have different cryptographic needs, Khatim Timestamp Server supports RSA (2048, 3072, 4096, 8192), ECDSA (160, 192, 224, 256, 384, 521), the post-quantum algorithm ML-DSA, and SHA-256/384/512 hashing. This flexibility lets operators maintain compatibility with existing ecosystems while gradually introducing quantum-resistant capabilities — testing, phasing and deploying stronger cryptography without disrupting live services.

Built for Long-Term Trust. PQC is not a switch flipped overnight; it is a journey of compatibility, risk management and operational readiness. Khatim Timestamp Server gives providers the agility to move forward confidently while continuing to deliver trusted services today, supporting the migration planning encouraged by evolving eIDAS and ETSI guidance.

- RSA (2048 / 3072 / 4096 / 8192) and ECDSA (160–521) support
- Post-quantum ML-DSA signing for long-term resilience
- SHA-256 / 384 / 512 hashing
- Phase in quantum-resistant crypto without service disruption
- Aligned with long-term-evidence and migration-readiness goals



PILLAR 08 · PKCS#11 INTEGRATION

Connect any HSM

The Challenge: Signing Keys Must Be Protected to the Highest Assurance Level

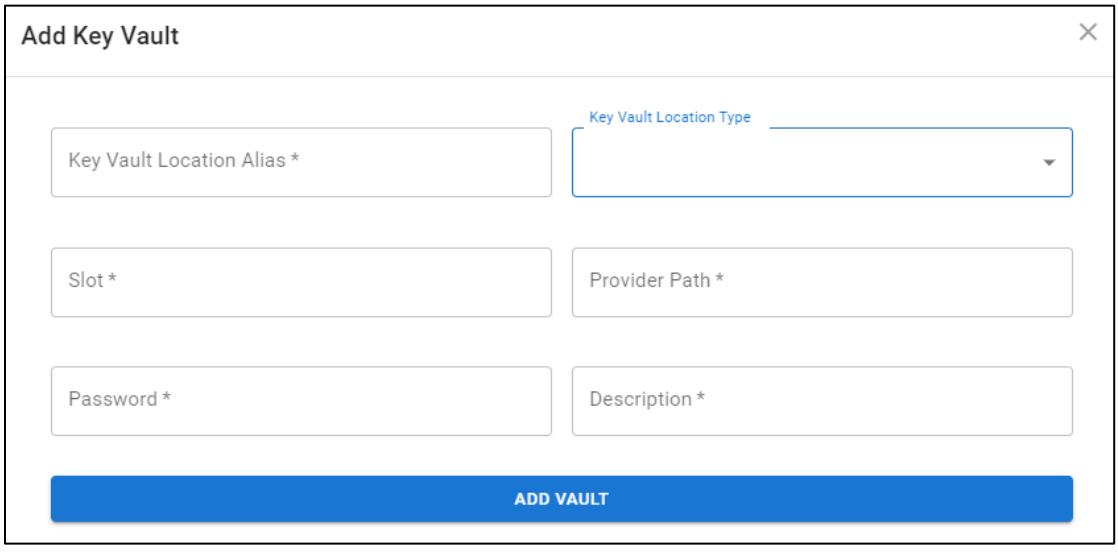
A TSA's signing key is the root of every token's trust. For high-assurance and regulated environments, that key must be generated and held in a certified hardware security module — and the timestamp platform must integrate cleanly with whatever HSM the operator already owns.

What Khatim Timestamp Server Delivers

Broad HSM Support over PKCS#11. Through its Key Vault, KTS configures PKCS#11-based HSMs and smart cards, and can generate cryptographic keys (RSA, ECDSA), CSRs and certificates for timestamping, then import issued certificates back into the system. It integrates quickly with the HSMs operators already run — Entrust nShield, Thales Luna & ProtectServer, Utimaco CryptoServer, Microsoft Azure Key Vault and AWS CloudHSM. This use of certified cryptographic modules supports the secure-key-management requirements of CWA 14167-1 and ETSI EN 319 422 for trustworthy TSA systems.

Software Keystores Where HSMs Aren't Required. Environments that don't require an HSM can still use software-based cryptographic keystores, and timestamp certificates can be certified by an operator's existing CA for quick import and use — keeping deployment fast without compromising the option to raise assurance later.

- PKCS#11 integration with leading HSMs and smart cards
- Supported: Entrust nShield, Thales Luna/ProtectServer, Utimaco CryptoServer, Azure Key Vault, AWS CloudHSM
- Generate keys, CSRs and certificates; import issued certs back
- Software keystore option where HSMs are not required
- Use your existing CA to certify timestamp certificates



PILLAR 09 · PROACTIVE ALERTS & SIEM INTEGRATION

Turn Operational Problems into Early, Actionable Signals

The Challenge: Detecting TSA failures in Realtime

A Timestamp Authority fails quietly. An NTP source drifts, an HSM stops responding, a signing certificate slips past its expiry — and unless someone is watching the right screen at the right moment, the first sign of trouble is a customer complaint or a failed audit. Operations teams cannot babysit a dashboard around the clock, and time-related risk rarely announces itself. What operators need is for the server itself to raise its hand the instant something is wrong, and to route that signal into the tools the security team already lives in.

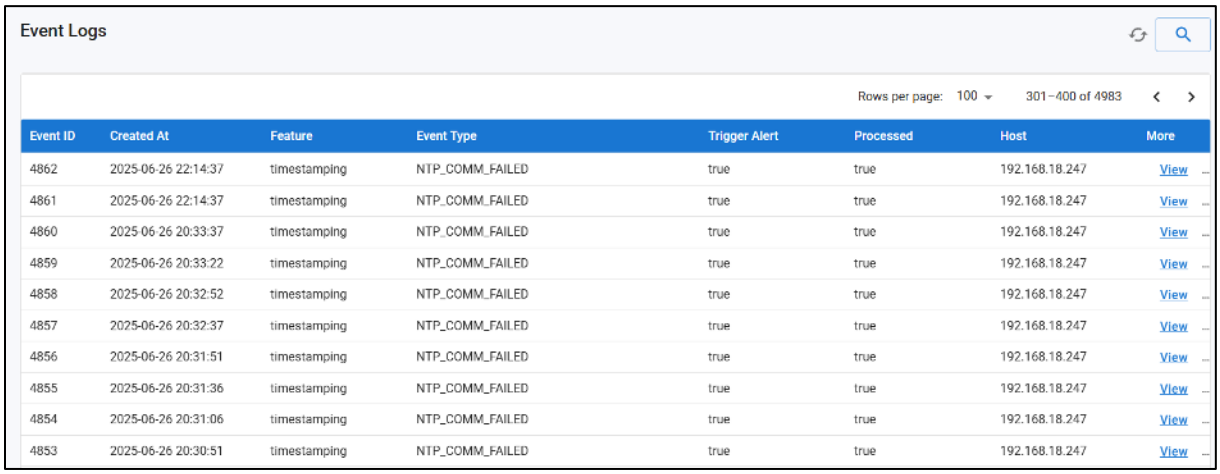
What Khatim Timestamp Server Delivers

Proactive Administrator Notification. When the timestamp server is not operating as it should, Khatim Timestamp Server proactively notifies administrators so they can take immediate action. Alerts fire on the conditions that matter to a TSA — NTP communication failures, drift-threshold breaches and licensing events — so problems are caught before they cascade into failed timestamp issuance.

Email & Daily Summary Reporting. System events are emailed to configured administrators as they are generated and are also consolidated into daily summary reports, giving both real-time awareness and a periodic operational digest for review and record-keeping.

Secure Push to Central Logging & SIEM. For full traceability, every issue is recorded and can be pushed securely to your central logging and SIEM platforms — including Splunk, Grafana, Graylog and LogRhythm — so time-related risk surfaces in the same place your security team already monitors. This keeps the TSA from becoming a blind spot in an otherwise well-instrumented environment.

- Proactive alerts for NTP, HSM, certificate, signing and licensing events
- Secure event forwarding to Splunk, Grafana, Graylog and LogRhythm
- Email notifications sent as events occur
- Daily summary reports for operational review
- Every issue recorded for full traceability



Event ID	Created At	Feature	Event Type	Trigger Alert	Processed	Host	More
4862	2025-06-26 22:14:37	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View
4861	2025-06-26 22:14:37	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View
4860	2025-06-26 20:33:37	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View
4859	2025-06-26 20:33:22	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View
4858	2025-06-26 20:32:52	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View
4857	2025-06-26 20:32:37	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View
4856	2025-06-26 20:31:51	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View
4855	2025-06-26 20:31:36	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View
4854	2025-06-26 20:31:06	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View
4853	2025-06-26 20:30:51	timestamping	NTP_COMM_FAILED	true	true	192.168.18.247	View

PILLAR 10 · MILITARY GRADE ACCESS CONTROL & UNIFIED ADMINISTRATION

Maximum Security, Managed from a Single Pane

The Challenge: The Control Plane Must Be as Trusted as the Signing Key

A TSA's signing key gets the security attention — but the systems around it are just as exposed. Configuration data, transaction records and administrative functions are all attack surface, and if administration is scattered across command lines, config files and separate consoles, mistakes and blind spots multiply. High-assurance environments demand that every sensitive function be both strongly protected at rest and operated from one coherent, auditable place — so security and usability reinforce each other rather than trading off.

What Khatim Timestamp Server Delivers

Military-Grade Protection with AES-256. Khatim Timestamp Server applies military-grade security to every key function of your timestamp instance. Administration, timestamp creation and transaction logging are all protected using AES-256 encryption, ensuring that sensitive configuration and operational data remain confidential and tamper-resistant across the platform

Unified Admin-Friendly GUI. All of this is managed from a single, admin-friendly graphical interface. Key generation, HSM and keystore configuration, policy handling, and transaction and log viewing are performed from one place — giving operators complete control of the server without switching between disparate tools or external consoles, while a console-based interface remains available for headless environments.

Governed, Attributable Access. Access to these functions is controlled through an administrator model with a full operator audit trail, so every privileged action — a policy change, a key operation, an account update — is both secured and attributable to a named operator. This separation of duties and traceability of privileged action supports the trustworthy-system and personnel-control expectations of CWA 14167-1 and ETSI EN 319 422.

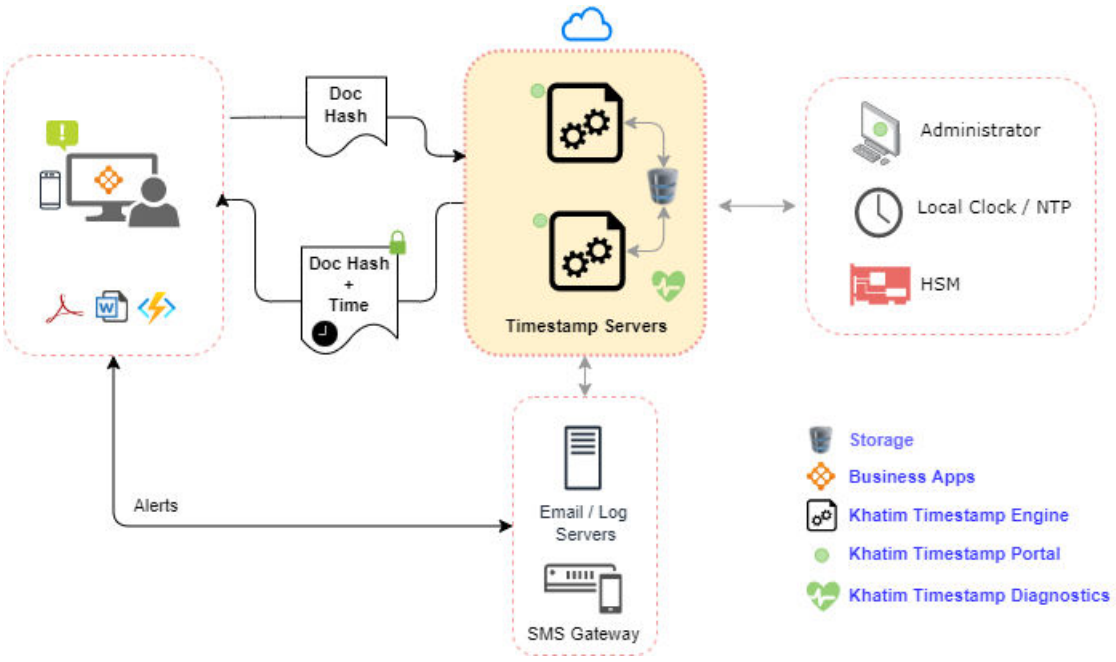
- AES-256 encryption across administration, creation and logging
- Administrator model with full operator audit trail & dual control
- Key generation, policy and transaction management in one GUI
- No disparate tools or external consoles required

Khatim Timestamp Server Architecture

Khatim Timestamp Server provides independent and irrefutable proof of time for business transactions, e-documents and digital signatures. It is built from three core components:

- **Khatim Timestamp Portal**, through which administrators manage configuration, transactions and statistics
- **Khatim Timestamp Engine**, which delivers the timestamp service to business applications
- **Khatim Timestamp Diagnostic**, which performs housekeeping and continuous health checks

The processing flow is straightforward: a business application submits a timestamp request containing a document hash. The server validates the request, obtains trusted time from the system clock or a configured NTP source and returns a digitally signed RFC 3161 timestamp token. For high-volume and high-availability needs, it is deployed as a cluster of individual timestamp servers behind a load balancer - additional servers can be added to the pool without stopping running instances. Signing keys are held in a PKCS#11 HSM, and transaction logs are retained for audit and archival.



> *I couldn't be more pleased with our experience working with Codegic on seamlessly integrating Khatim Timestamp Server into our system. From the beginning, their team displayed a remarkable level of professionalism and expertise that instilled confidence in us.*
>
> *Thanks to Codegic's exceptional service and their robust timestamp server, we've achieved a new level of security and accuracy in our operations. We're excited about the opportunities this opens up for our organization and look forward to continued collaboration. Kudos to the Codegic team for their dedication and top-notch service!"*
>
> **David Stojković** | *Lead Operating System Management, Zagrebačka banka d.d.UniCredit Group, Croatia*

Zagrebačka banka
UniCredit Group

Algorithms / Protocols	Performance	Supported OS / Languages / H/W
• RSA (2048/3072/4096/8192) • ECDSA (NIST_P, SECP (K1,R1), BRAINPOOL (R1,T1) – 160, 192, 224, 256, 384, 521) • PQC – ML-DSA • RFC 5280, 5816, 3161 • PKCS#11, NTP, SNMP, SMTP, Syslog • PKCS#1 - PKCS#15, PSS • HTTP, HTTP/s, REST • ETSI TS 101 861 • ETSI TS 102 023 • ETSI EN 319 422	• RSA 2048 – 394.38 TPS • RSA 4096 – 98.67 TPS • ECDSA secp256r1 – 380+ TPS • ECDSA secp384r1 – 381.5 TPS • ECDSA secp521r1 – 390.1 TPS * Tested with Entrust HSM XC Solo Base (single instance)	• All flavors of Windows Server & Linux (Centos Stream, Ubuntu, RedHat, Fedora) • 50 Languages including English, French, Spanish, Arabic, Chinese, Japanese, Italian, Polish, Swedish, Vietnamese, Russian & more. • 8 GB RAM, 2 vCPU (2.3 GHz), 10 GB Hard disk • Oracle, PostgreSQL

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.

Contact Us Today to see Khatim Timestamp Server in action

Facilitating Digital Trust by providing World-Class PKI & Digital Signature Solutions

info@codegic.com
www.codegic.com
USA | UAE | PAK
ISO 27001 · 9001 · 14001 Certified