Garantir

Unlimited CLM + PKI with GaraTrust

The Next Generation of Enterprise Cryptographic Management

Securing Trust at Scale

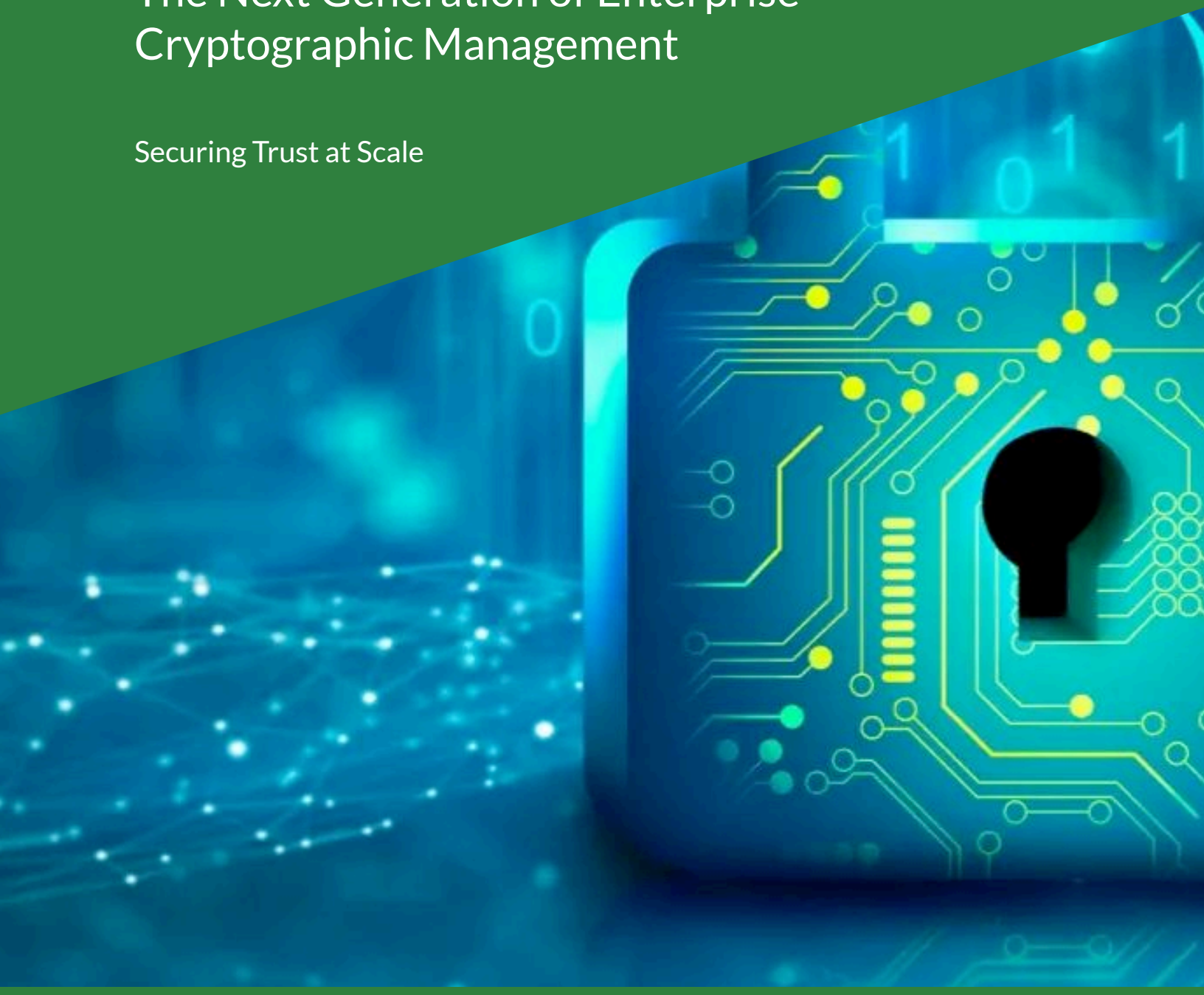
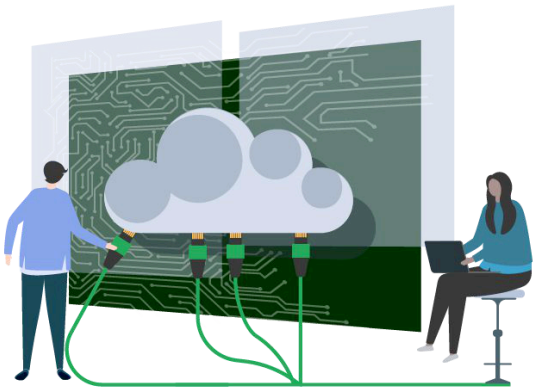


Table of Contents

Executive Summary

Digital certificates and cryptographic keys are the foundation of modern enterprise security. They enable the authentication of identities, encrypted communications, and data protection across systems, applications, and workflows. As organizations scale across cloud, DevOps, and AI-Driven environments, the number and complexity of these cryptographic assets have grown exponentially.

At the same time, regulatory and industry standards are tightening. Organizations face mounting pressure to implement short-lived certificates, stronger authentication, and more resilient controls to address threats emerging from quantum computing, AI, and agentic systems. These forces are creating an inflection point for operations and security where unmanaged cryptographic sprawl now extends through multiple layers of the enterprise. Cloud workloads, SaaS platforms, on-prem systems, DevOps pipelines, IoT devices, and software supply chains all rely on these assets.



Each environment often implements it's own isolated cryptographic processes, leading to misconfigurations, key exposure, outages, and compliance violations. The result is costly: increased complexity and risk with reduced visibility. Traditional certificate lifecycle management (CLM) and public key infrastructure (PKI) solutions often exacerbate the problem, offering fragmented architectures, limited automation, and unpredictable pricing models that penalize scale and innovation.

Garantir's GaraTrust platform redefines enterprise cryptography with properly protected, non-exportable keys. By unifying CLM and PKI within a single cohesive architecture, GaraTrust automates the time-intensive process of discovery, issuance, renewal, revocation, and monitoring of cryptographic assets across a wide array of systems, platforms, and identities. This allows for centralized visibility, continuous compliance, and zero certificate outages.

Beyond solving CLM and PKI management challenges, Garantir's unlimited-use, flat-fee pricing removes cost barriers, aligns security operations with business growth, and frees budget for other critical security initiatives.

By consolidating operations onto a single unified platform, Garantir reduces operational complexity, eliminates cryptographic sprawl, shortens time-to-value, and maximizes ROI—empowering security teams to focus on innovation, not maintenance.

The Enterprise Cryptography Challenge

Modern enterprises manage hundreds of thousands of certificates across web servers, APIs, mobile devices, cloud workloads, and IoT endpoints. Each certificate represents a potential single point of failure.

Without full lifecycle visibility and automation, expired or misconfigured certificates cause costly outages, compliance violations, and reputational damage. Shrinking certificate lifespans and the coming post-quantum era multiply that risk, pushing the limits of current security operations.

Enforcing granular controls requires new software

Some resources are managed by third-parties

Challenging to apply identity to locally-stored files

The Failure of Legacy Solutions

Security teams are forced to ration certificates and react to outages because traditional solutions are fundamentally constrained by complexity and cost. Legacy solutions fail to scale due to:

- **Per-Certificate Pricing:** This model penalizes growth. Teams avoid managing every certificate to keep costs down, creating dangerous blind spots and leaving critical systems exposed.
- **Fragmented Toolsets:** Require manual workflows across disparate teams for CLM and PKI, leading to errors and delays.
- **Limited Automation:** Forces manual renewals and replacements, which is the primary cause of certificate outages.
- **Rigid Integrations:** Fail to natively support modern cloud and DevOps environments.
- **Poor Crypto Agility:** Delays adoption of new algorithms and essential post-quantum standards.

The GaraTrust Platform: Unified CLM & PKI

GaraTrust brings all cryptographic functions together in a single, modular platform. It consolidates Certificate Lifecycle Management, Private PKI, key management, and signing to simplify enterprise operations to improve resilience. **GaraTrust is the single source of truth for all enterprise cryptography.**

Core capabilities include:

- **Automated CLM:** Full lifecycle automation for discovery, issuance, renewal, revocation, and monitoring.
- **Unified Key Management:** All certificates and private keys are centrally managed within a hardware security module (HSM).
- **Policy-Based Security:** Administrators can enforce granular policies, including MFA, just-in-time access, and approval workflows, from one interface.
- **Private PKI:** Fully integrated private PKI with HSM-backed root and subordinate certificate authorities (CAs).
- **Crypto Agility:** Built-in support for all current standards such as RSA and ECC, as well as emerging post-quantum algorithms including ML-DSA, LMS, and more.

How GaraTrust manages certificates and keys throughout their lifecycle to ensure security, speed, and control.

Achieved Outcomes and Business Value

By unifying the technology and disrupting the price model, GaraTrust delivers concrete results that impact security, compliance, and the bottom line.

Outcome Category	Result
Security	Nearly zero certificate outages through proactive automation. Full visibility across hybrid, cloud, and IoT environments.
Financial	High dollar savings compared to tiered licensing models. Budget certainty with predictable annual costs.
Compliance	Seamless regulatory compliance with PCI DSS, HIPAA, NIST, and CNSA 2.0 due to centralized logging and policy enforcement.
Future Readiness	Immediate readiness for post-quantum and complete alignment with Zero Trust security initiatives.

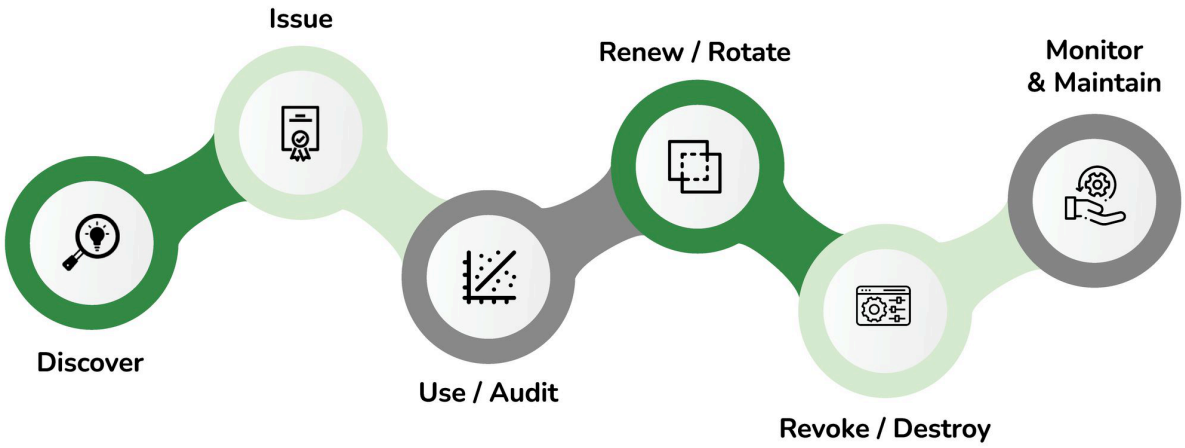
Deep Dive:
Unified CLM & Private PKI

GaraTrust automates every phase of the certificate lifecycle and keeps keys centrally protected at all times.

Certificate Lifecycle Management (CLM) in Practice

Maintaining visibility across thousands of certificates is complex and error-prone. GaraTrust simplifies this with centralized HSM management, automated renewals, and granular security controls.

Function	Description
Discovery	Scans networks, hosts, and APIs to find certificates across the enterprise, eliminating blind spots.
Issue	Integrates with public and private CAs, supporting approvals, and audit logging.
Use/Audit	Enforces access controls and maintains centralized logs for compliance.
Renew/Rotate	Automates renewals and key rotations using lifecycle policies, preventing costly outages.
Revoke/Destroy	Retires certificates and deletes associated keys securely.
Monitor/Maintain	Continuously discovers new assets and brings them under management.



The six essential functions of certificate lifecycle management within GaraTrust.

Automated Certificate Management with GaraTrust

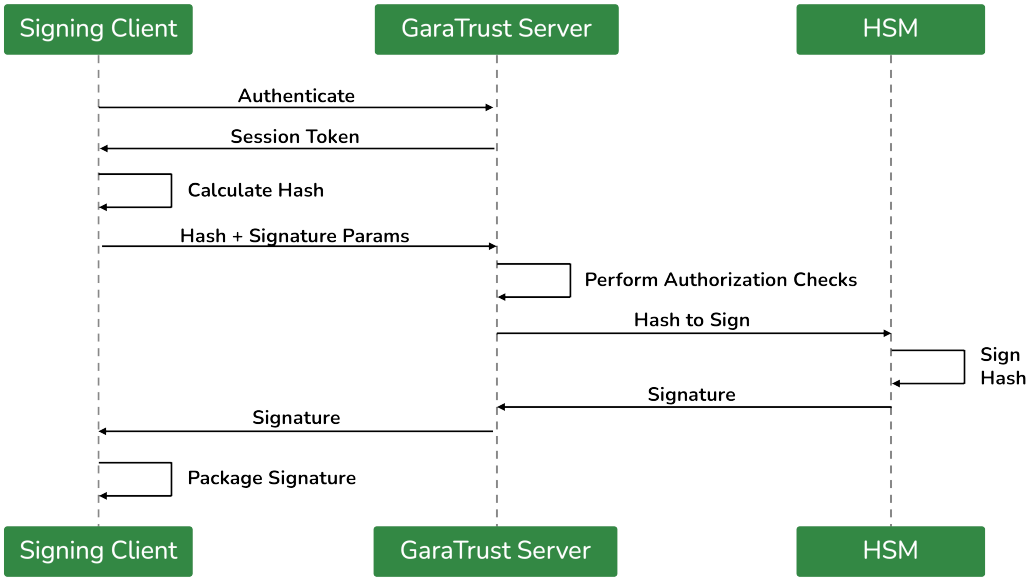
- Certificates are discovered and tracked continuously.
- Renewals occur automatically before expiration, preventing costly outages.
- Private keys remain secured in a non-exportable state within the HSM.
- MFA, device authentication, and approval workflows can be enforced with a few clicks.

THE RESULT: Zero outages, simplified audits, and stronger cybersecurity posture.

Private PKI Simplified

A strong public key infrastructure (PKI) is essential to establishing and maintaining digital trust. GaraTrust enables enterprises to deploy or modernize an organizations PKI efficiently, securely, and with minimal overhead.

- **Protecting the Root of Trust:** The PKI root of trust is among the enterprise's most sensitive assets. GaraTrust keeps root keys secured and non-exportable in a hardware security module (HSM), ensuring hardware-level protection.
- **Design and Deployment Expertise:** Garantir provides the deep experience necessary for thoughtful planning and maintenance, ensuring compliance and adaptability.
- **Full Visibility and Central Management:** GaraTrust delivers a single plane of glass for managing internal and external certificate authorities, policies, and access controls.

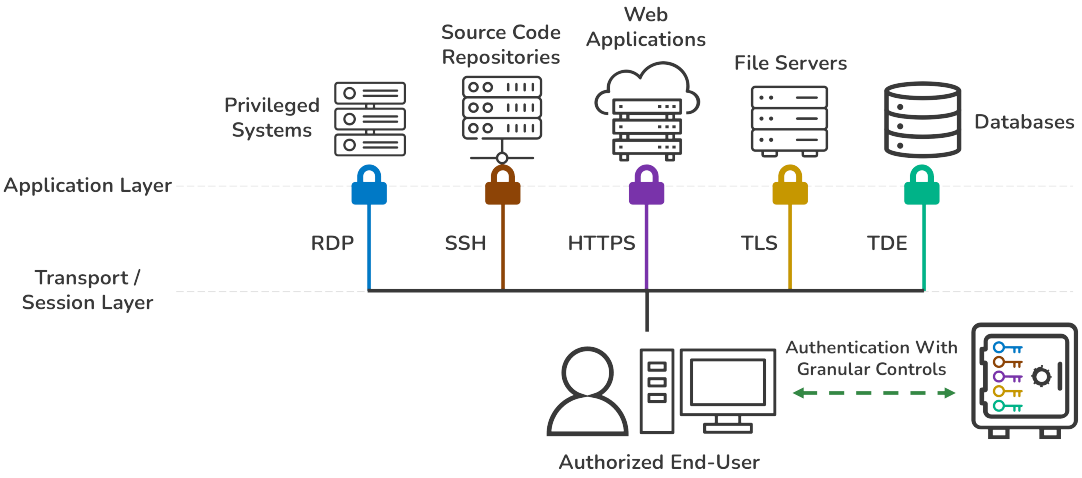


GaraTrust provides a complete PKI and certificate management framework, backed by HSM-secured roots and centralized control.

GaraTrust Design and Architecture Principles

GaraTrust was built for high performance, centralized visibility, and uncompromising key security, supporting any development model: on-premise, in the cloud, or hybrid.

Remote key enforcement ensures applications never handle raw key material. GaraTrust authenticates and authorizes all cryptographic operations centrally, while private keys remain secured in non-exportable form within an HSM or key manager, eliminating common security vulnerabilities.



GaraTrust enforces layered security controls transparently, ensuring compliance and consistent protection.

Minimal Network Usage: Client-side hashing ensures cryptographic operations happen efficiently without transferring large data sets across the network, maintaining high performance.

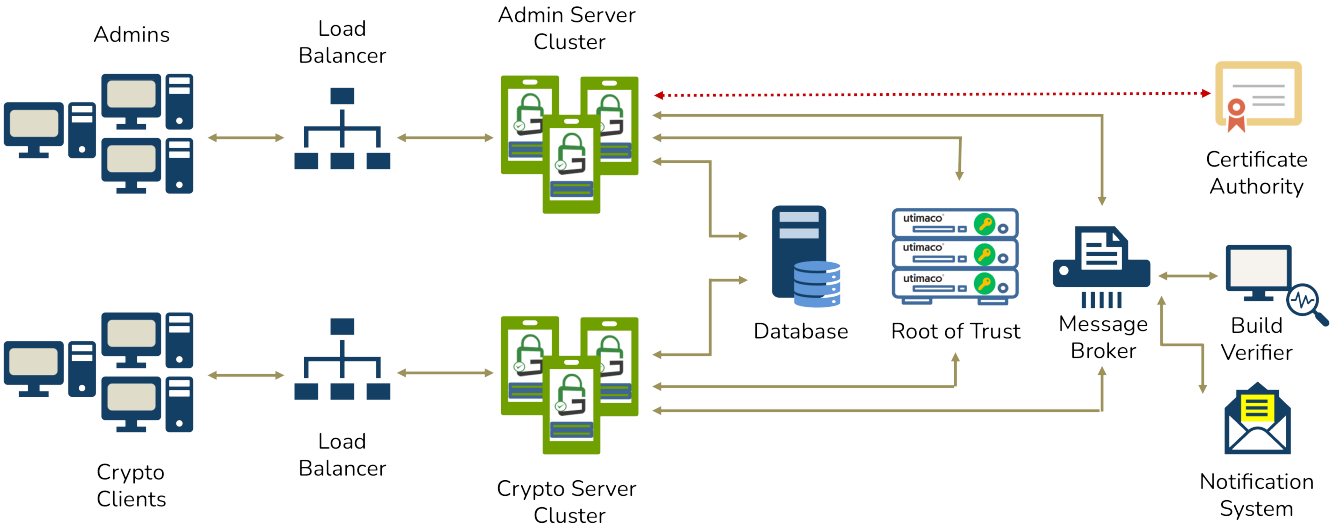
Configurable Security Controls: Security teams can define granular policies, including multi-factor authentication (MFA), just-in-time access, device authentication, and approval workflows.

Open APIs: Every component of GaraTrust exposes an open API for seamless integration with CI/CD pipelines, certificate authorities, and existing enterprise tools.

Real-World Use Cases

GaraTrust supports a wide range of enterprise use cases across every modern IT environment:

- **DevOps and Cloud:** Kubernetes and Istio certificate automation; hybrid cloud environments spanning AWS, Azure, and GCP.
- **Identity:** IoT device identity management for secure provisioning and rotation; **Zero Trust frameworks** ensuring authenticated communication between all entities.
- **Security Operations:** HSM Certificate Management Automation enabling automatic certificate renewal and centralized key control to eliminate outages and simplify audits.
- **Code Integrity:** Enterprise-scale code signing for Windows, macOS, and cross-platform applications.



The full GaraTrust architecture showing its scalable, modular components for enterprise cryptography.

Conclusion

Per-certificate pricing is outdated and puts the enterprise at risk. The future of enterprise cryptography is unified, automated, and predictable.

GaraTrust delivers CLM and PKI in a single, integrated platform that scales with your business without scaling your costs.

Predictable. Secure. Unlimited.

About Garantir

Garantir is a cybersecurity company that provides advanced cryptographic solutions to the enterprise. The Garantir team has worked on the security needs of business of all sizes, from startups to Fortune 500 companies. At the core of Garantir's philosophy is the belief that securing business infrastructure and data should not hinder performance or interrupt day-to-day operations. With GaraTrust, Garantir's flagship cryptographic services platform, private keys remain secured at all times, while a client-side hashing architecture ensures high performance for all cryptographic operations, including code signing, SSH, TLS, document signing, application-level encryption, S/MIME, secure backup, and more. Visit us at https://www.garantir.io/ to learn more.

sales@garantir.io **(858) 751-4865** **www.garantir.io**