EBOOK

Best Practices for Cryptographic Key Management

Protect the Keys That Protect Your Data

ENTRUST

SECURING A WORLD IN MOTION

INTRODUCTION

Why Key Management Matters

Cryptography helps organizations protect sensitive data at rest, in transit, and across applications, including intellectual property, customer information, and regulated workloads. That protection depends on how well the associated keys are managed.

A cryptographic key is a critical security asset that enables encryption, decryption, digital signing, and other cryptographic operations. If a key is compromised, the confidentiality, integrity, or authenticity of the data and systems it protects may also be compromised.

Poor key management can undermine even the strongest cryptographic protections. Cryptographic key management has become all the more critical as cloud adoption accelerates, digital ecosystems grow more complex, and the post-quantum era moves even closer. For security leaders, architects, and compliance teams, effective key management helps reduce risk, meet regulatory requirements, and maintain trust.

What Is Cryptographic Key Management?

Cryptographic key management refers to the policies, processes, and technologies used to control cryptographic keys throughout their entire lifecycle.

These keys enable organizations to protect data, create digital signatures, and authenticate systems and applications. Keys must be generated using approved algorithms and secure sources of randomness. Once created, they must be protected from unauthorized access or unintended exposure and made available only to approved users, systems, or applications when needed.

The Modern Threat Landscape

Today's threat environment has made cryptographic keys a primary target for attackers. As organizations adopt cloud services, containerized applications, APIs, and Zero Trust architectures, the number of encrypted assets grows rapidly, as does the volume of keys, secrets, and credentials that must be protected.

Many organizations struggle with key management in an evolving cryptographic landscape – not due to negligence but because of growth, complexity, and legacy practices.

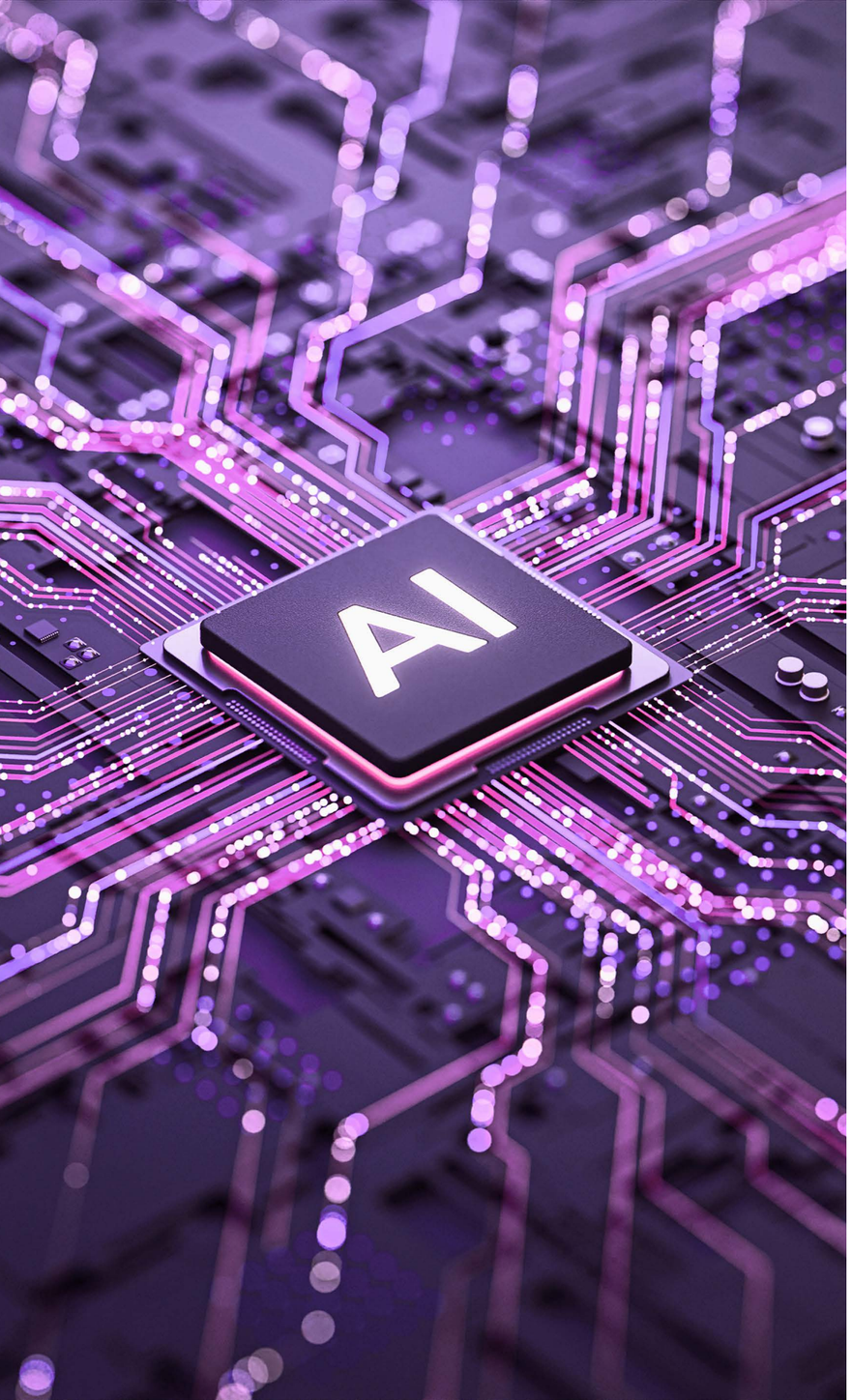
Common challenges include:

- **Hard-coded keys embedded in application code or scripts.** Keys embedded directly into source code are difficult to rotate and can be easily exposed once committed.
- **Storing keys alongside encrypted data.** If attackers gain access to both protected data and the keys used to access it, they may be able to read that information.
- **Lack of visibility into key access and location.** Without an accurate inventory of keys and their usage, organizations struggle to enforce access controls or respond effectively to incidents.
- **Error-prone manual key rotation.** Manual rotation increases the likelihood of missed deadlines or mistakes, leaving keys active longer than intended and expanding exposure risk.
- **Over-privileged access with too many users or systems.** Granting broad access to keys increases the impact of compromised accounts, insider misuse, or accidental disclosure.
- **Fragmented tooling across systems.** Managing keys across separate tools and environments leads to inconsistent policies, making it harder to enforce standards and scale securely.
- **Knowledge gaps after employee turnover.** When employees responsible for key management leave, organizations may lose critical information about existing keys, their locations, and their uses.

Breaches involving data distributed across multiple environments, including public clouds, private clouds, and on-premises systems, accounted for 30% of all breaches studied and cost an average of

$5.05 million

Source: https://www.ibm.com/reports/data-breach



The Newest, Most Daunting Challenge – Artificial Intelligence (AI)

AI-enabled attacks: While artificial intelligence enables and accelerates workforces, it does the same for bad actors. Cyber attackers can deploy AI agents for larger scale attacks and exploit breaches to a greater effect. They accomplish this through AI and machine learning models to scan large volumes of data and code repositories to identify exposed keys, secrets, credentials, and weak security practices.

AI-enabled social engineering and phishing: IT admins, like operators overseeing key management systems, have always been high-value targets for cyber attackers. Now, AI-powered threats such as deepfake voices and adaptive attacks make theft of admin credentials more likely.

AI-enabled discovery of misconfigurations: Once a cyber attacker gains access to a key management system, their AI models can easily scan for security gaps like loose access controls, permissions, and key rotation policies.

Exposure of sensitive data to internal AI models: Internal use of AI tools, including training data or user inputs, can lead to sensitive data being exposed to AI models and an increased risk of data leakage and third-party AI models being compromised.

These challenges often take root in fast-moving development environments, where speed and convenience can outweigh long-term security considerations. Over time, what begins as a workaround can become a systemic risk.

Understanding the Key Management Lifecycle

Effective key management spans the entire lifecycle of a cryptographic key, from creation and deployment to active use and eventual retirement. Each lifecycle stage introduces unique risks and operational requirements, making it essential for organizations to apply consistent controls, visibility, and governance throughout.

The key lifecycle consists of multiple steps that can be split into three stages: creation and preparation, active use and management, and recovery and retirement.

1. Pre-Operational (Creation and Preparation)

Keys are created, associated, and securely prepared before use.

- **Key generation:** Create cryptographic keys using strong, unpredictable randomness to ensure security and prevent compromise
- **Key registration:** Associate keys with identities, systems, or policies to establish trust and enable secure use
- **Key storage (pre-operational):** Securely store keys offline or in protected environments before they are deployed

2. Operational (Active Use and Management)

Keys are actively used, distributed, and maintained in live systems.

- **Key distribution and installation:** Deliver keys securely to authorized systems or users while validating identity and preventing unauthorized access
- **Key use:** Restrict each key to a specific purpose and tightly control access to minimize exposure
- **Key storage (operational):** Protect active keys in secure hardware security modules (HSMs)
- **Key rotation:** Regularly replace keys to limit exposure, reduce risk, and align with policy and lifecycle requirements

3. Post-Operational (Recovery and Retirement)

Keys are secured, recovered if needed, or removed from use.

- **Key backup:** Create secure backups where appropriate to prevent data loss while maintaining strict controls
- **Key recovery:** Restore keys through controlled, audited processes when required for operations or compliance
- **Key revocation:** Revoke and replace compromised or suspect keys immediately to prevent misuse and protect systems

Managing keys across these stages requires more than documented policies. Organizations also need technologies that help protect keys from unauthorized access, extraction, misuse, and compromise throughout their operational life. Hardware security modules provide a secure environment for generating, protecting, and using cryptographic keys, making them an important component of a broader key management strategy.

Best Practices for Effective Key Management

While implementations vary, strong key management programs consistently follow a set of six core principles:

1. Discover and Inventory Keys

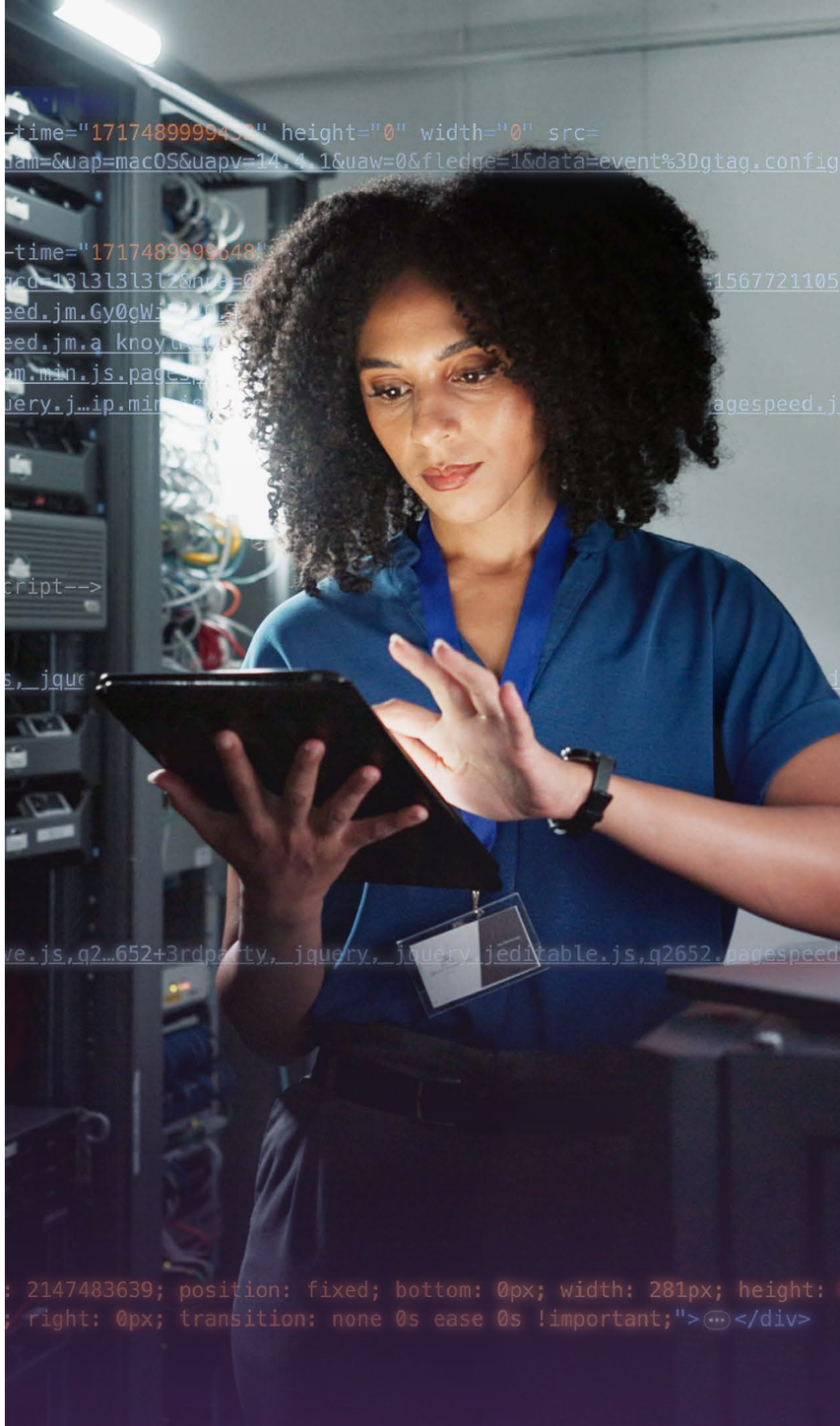
2. Centralize Visibility

3. Support Strong Key Generation and Protection

4. Establish Least Privilege and Access Controls

5. Automate Across the Key Lifecycle

6. Prioritize Auditability, Compliance, and Data Sovereignty



1. Discover and Inventory Keys

Build a clear view of where keys exist, how they are used, and where risk may be present

Effective key management starts with discovery. Before organizations can secure, govern, or automate their cryptographic environments, they must first understand what keys exist, where they are located, and how they're being used.

During discovery, organizations must consider a few important questions. Is the data the keys are protecting mission critical or of high value? How would the organization deal with a breach or loss of such data? In many enterprises, keys are distributed across siloed systems, often without a centralized record or clear ownership.

Discovery establishes the foundation for effective control. By identifying all cryptographic assets across environments, organizations can address blind spots, reduce risk, and identify keys that may be unmanaged or exposed. Without this visibility, it is difficult to enforce policies, maintain compliance, or respond effectively to threats.

As environments scale and machine identities expand, organizations need an accurate, up-to-date inventory of their keys. Automated discovery within a cryptographic security management system can help identify new keys, track changes, and surface potential risks as infrastructure evolves. It also gives organizations a clearer starting point for assessing cryptographic assets that may require migration as post-quantum requirements mature.

Comprehensive discovery enables organizations to:

- Keep a complete inventory of keys across systems, applications, and environments
- Identify unmanaged, orphaned, or duplicated keys that introduce risk
- Build a foundation for enforcing policy, automation, and lifecycle management at scale

2. Centralize Visibility

Create a single source of truth for key ownership, usage, and policy enforcement across environments

Once keys have been discovered and inventoried, organizations need ongoing visibility into how they're managed. They must be able to identify where cryptographic keys exist, how they're used, and who is responsible for them. Centralized management helps provide a single, authoritative view of keys across the organization, enabling consistent policy enforcement regardless of platform or environment. It also clarifies ownership and accountability, which are essential for both security operations and compliance.

Importantly, centralization does not imply unrestricted access. The goal is to manage policies and accountability centrally while keeping key access tightly restricted to authorized users and systems.

Centralized management provides:

- A single, authoritative view of keys across the organization
- Consistent policies regardless of environment or platform
- Clear ownership and accountability for key usage

3. Support Strong Key Generation and Protection

Generate and protect keys using trusted controls and a hardware-backed foundation throughout their lifecycle

Keys should always be generated using approved cryptographic algorithms, appropriate key lengths, and secure sources of randomness. Weak or poorly generated keys undermine cryptographic protection from the start.

Once generated, keys must be protected throughout their lifecycle. They should be stored separately from the data they protect, shielded from unauthorized access, and protected both at rest and while in active use. For governments, regulated organizations, and other environments where keys protect high-value data, HSMs provide a hardened, hardware-backed root of trust. HSMs help isolate keys from application environments and reduce the risk of unauthorized extraction or exposure.

When building a strong key generation process consider the following:

- **Use stronger key lengths by default:** For example, AES-256 is preferred over AES-128 for sensitive data encryption due to its higher resistance to attacks. However, while algorithms like RSA-4096 traditionally offer stronger security than RSA-2048, both RSA and ECC are vulnerable to future quantum attacks, requiring organizations to plan for quantum-resistant alternatives.
- **Adopt approved algorithms and standards:** Use NIST-approved cryptographic algorithms, including AES for symmetric encryption and RSA or ECC for public-key cryptography, and generate keys in accordance with NIST guidance and industry best practices. As part of a quantum-safe strategy, plan for and progressively adopt NIST's post-quantum standards, including FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA). Additionally, use FIPS 140-3 and Common Criteria (CC) EAL 4+ validated cryptographic modules, such as Entrust nShield HSMs, to provide the highest assurance for key generation, storage, and cryptographic operations.
- **Leverage secure randomness sources:** Keys should be generated using hardware-backed random number generators (RNGs) to ensure strong entropy and unpredictability. Randomness sources should use true random number generators (TRNGs) within cryptographic modules validated to recognized standards such as FIPS 140-3 and align with guidance for entropy generation and validation, including NIST SP 800-90B and AIS 31.
- **Align with compliance and data sovereignty mandates:** In some jurisdictions and regulated industries, organizations may need to maintain cryptographic keys, HSMs, or key management operations within specific geographic boundaries to support data residency, sovereignty, or operational control requirements. Evaluate local regulations carefully and design key management architectures that align with applicable compliance obligations.

Entrust nShield HSMs

Entrust nShield® HSMs provide a tamper-resistant foundation for protecting cryptographic keys, combining enterprise-scale performance with FIPS 140-2 and FIPS 140-3 certified security to help organizations meet stringent compliance requirements, reduce risk, and enable crypto-agility.

Explore Our HSMs

4. Establish Least Privilege and Access Controls

Restrict key access to authorized users, systems, and actions based on defined roles and policies

Not every user or system requires access to cryptographic keys. Applying least privilege principles ensures that access is granted only when necessary and only for approved purposes.

This approach limits who can retrieve or use specific keys, restricts sensitive actions such as key export or deletion, and separates administrative duties to reduce insider risk. Strong identity and access controls are essential to key management, as they determine who can interact with keys and under what conditions.

Importantly, centralization does not imply unrestricted access. The goal is to manage policies and accountability centrally while keeping key access tightly restricted to authorized users and systems.

Applying least privilege principles helps organizations:

- Limit users and applications to the keys they require
- Restrict sensitive operations, such as key deletion or export
- Separate duties to reduce insider risk

5. Automate Across the Key Lifecycle

Streamline key rotation, expiration, and policy enforcement to reduce manual risk and improve scalability

Manual key management processes are difficult to maintain at scale. Automation helps reduce operational burden while improving security and consistency.

Automated lifecycle management enforces regular rotation and expiration, applies policies uniformly across environments, and reduces the likelihood of human error. By embedding automation into key management processes, security teams can better align with modern development practices and dynamic infrastructure.

The Entrust Approach: Cryptographic Security Platform

The Entrust Cryptographic Security Platform centralizes the discovery, management, and governance of keys, secrets, and certificates across environments, unifying HSMs, public key infrastructure (PKI), and lifecycle management to improve visibility, enforce consistent policies, and automate control of cryptographic assets at scale.

Explore CSP

Automation key management reduces operational burden while improving security by:

- Enforcing regular key rotation and expiration
- Applying consistent policies across environments
- Reducing human error and configuration drift

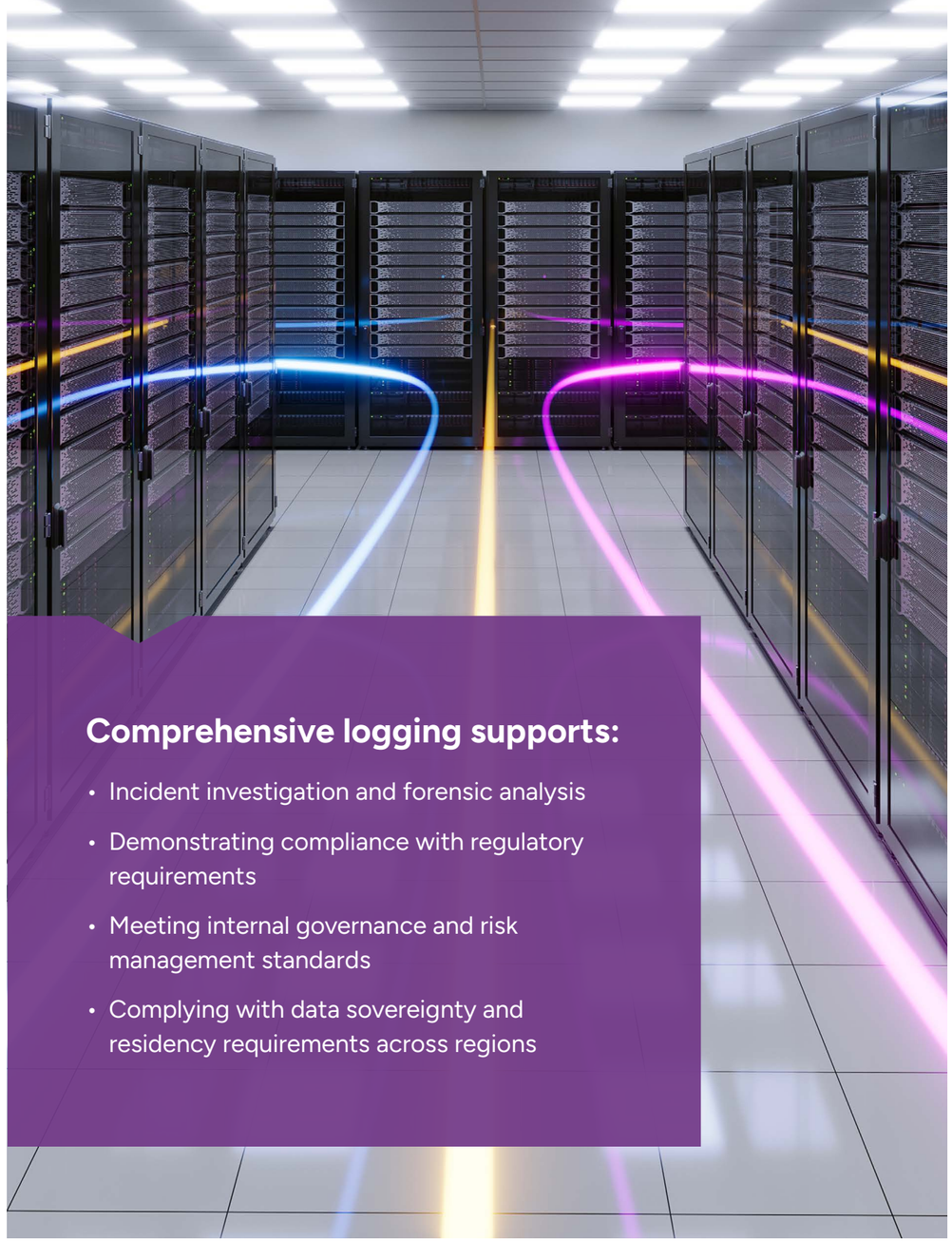
6. Prioritize Auditability, Compliance, and Data Sovereignty

Maintain comprehensive logging and reporting to support regulatory requirements and security oversight

Every interaction with a cryptographic key should be logged and auditable. Comprehensive audit trails support incident investigation and analysis while making it easier to comply with regulatory requirements.

Beyond compliance, organizations must also address data sovereignty requirements that govern where cryptographic keys and sensitive data are stored, processed, or accessed. Meeting these requirements adds a layer of complexity, requiring visibility into where keys reside and how they are managed across geographies.

Clear visibility into how keys are accessed, used, and governed builds confidence for auditors, leadership, customers, and business partners that rely on the organization to protect sensitive information and meet regional requirements.



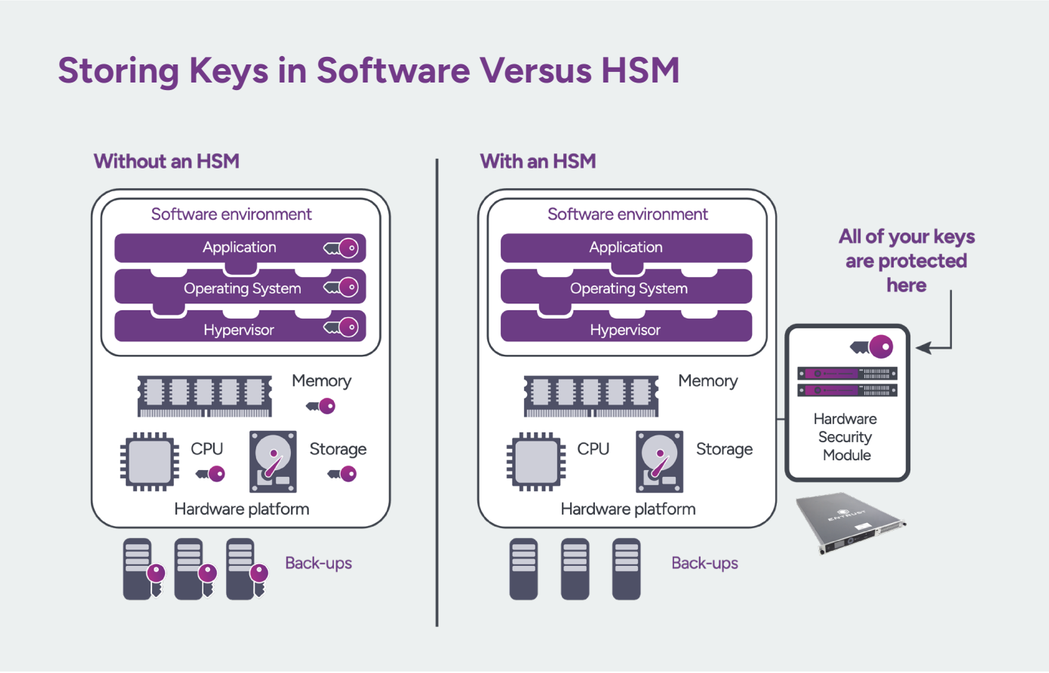
Comprehensive logging supports:

- Incident investigation and forensic analysis
- Demonstrating compliance with regulatory requirements
- Meeting internal governance and risk management standards
- Complying with data sovereignty and residency requirements across regions

Why Cryptographic Keys Require Hardware-Based Protection

Protect keys with hardware-backed security to reduce exposure and prevent compromise

Storing cryptographic keys in software environments – such as application memory, configuration files, or standard servers – introduces significant risk. When keys are stored alongside the systems or applications they protect, an attacker who gains access to that environment may also be able to locate and extract the keys. Keys in software may also be exposed to malware, unauthorized access, or misuse by users with elevated privileges.



For example, if the same administrator or privileged account can access an encrypted database and the keys used to access that data, the separation between protected information and its keys is weakened. Keeping high-value keys in a separate, hardware-backed environment helps reduce this risk.

This risk is amplified in modern environments where workloads are dynamic, distributed, and frequently accessed. As machine identities scale and systems become more interconnected, software-based key storage creates a larger attack surface. This makes it more difficult to maintain consistent control, enforce policies, and prevent unauthorized use.

Hardware-backed key protections help address these challenges by isolating cryptographic keys from the systems and applications that use them. In dedicated hardware environments, like HSMs, keys are generated, stored, and used within a secure boundary that is resistant to tampering, extraction, and unauthorized access. Even if an application or server is compromised, the keys remain protected.

Hardware-backed protection provides:

- Strong isolation of keys from applications, memory, and operating systems
- Resistance to extraction attempts, including malware and memory scraping
- Controlled access to keys based on defined policies and authorization
- Secure execution of cryptographic operations within a protected environment

By moving key storage and operations out of software and into secure hardware, organizations can significantly reduce the risk of key compromise. This approach strengthens the overall security posture and ensures that cryptographic controls remain effective even in the face of evolving post-quantum threats.

Key Management Across Environments

Few organizations operate in a single environment, and cryptographic keys often span multiple platforms, teams, and technologies. Each environment introduces different risks, but fragmented or inconsistent controls create security gaps. A unified approach to key management helps organizations maintain consistent security policies, HSM-backed protection, and visibility.

On-Premises Infrastructure

On-premises environments often rely on legacy systems and sometimes long-established manual processes, making it difficult to modernize key management practices. Keys may be tightly connected to hardware, applications, or manual workflows, increasing the risk of inconsistent controls and limited visibility.

Public and Private Cloud Platforms

Cloud platforms introduce scale and speed but also rely heavily on cryptographic keys, service accounts, and identity-based access. Without effective key management, misconfigurations or broad permissions can quickly expose keys across cloud systems. Cloud-delivered HSM solutions such as Entrust nShield® as a Service extend hardware-backed protection into cloud environments without requiring organizations to deploy and manage physical infrastructure.

Bring/Hold Your Own Key

Organizations may use Bring Your Own Key (BYOK) to generate or control keys used with cloud services, or Hold Your Own Key (HYOK) when they require greater control over key possession and use. The appropriate approach depends on security, compliance, data sovereignty, and operational requirements. In either model, HSM-backed protection can help establish trust in the keys involved

Hybrid and Multi-Cloud Deployments

Hybrid and multi-cloud deployments increase complexity by spreading keys across providers with different native tools and policies. Inconsistent key handling across platforms makes it harder to enforce standards and respond to incidents effectively.

DevOps and CI/CD Pipelines

Build and deployment pipelines frequently require access to signing keys, API keys, and secrets to automate application delivery. When these keys are embedded in scripts or pipelines without strong controls, they become attractive targets for attackers.

APIs, Containers, and Microservices

Modern applications rely on machine-to-machine communication, requiring secure access to cryptographic material. The dynamic nature of containers and microservices makes manual key management inefficient and increases the need for centralized governance and automation.

Learn more about Entrust nShield® as a Service.

Aligning Key Management With Business Goals

Strong key management directly supports both security priorities and business outcomes. When implemented effectively, it helps reduce the likelihood and impact of data breaches, supports controlled adoption of cloud and digital services, and helps organizations meet compliance requirements without unnecessary friction. Hardware-backed solutions like Entrust nShield® HSMs help organizations achieve these outcomes while balancing security, flexibility, and operational efficiency.

Well-managed keys also improve resilience and operational stability while reinforcing trust with customers, partners, and regulators. As cryptographic standards evolve, organizations need key management practices that can support post-quantum migration without unnecessary disruption. Treating key management as a strategic capability helps organizations align security controls with business objectives and prepare for changing cryptographic requirements.

Evaluating a Key Management Strategy

Organizations assessing current risk and future readiness should ask these key strategic questions:

- Do we have visibility into all cryptographic keys and secrets?
- Are key policies consistent across environments?
- How automated is key rotation and lifecycle management?
- Are access controls aligned with least privilege principles?
- Can we easily support audits and compliance reviews?
- Are we prepared to transition to quantum-resistant cryptographic algorithms?
- Can our key management approach support crypto-agility without disrupting systems?
- Do we have clear ownership and accountability for cryptographic keys across teams and systems?
- Can we quickly identify and revoke keys if a compromise is suspected?
- How well does key management integrate with existing identity, access, and security tooling?
- Are development teams provided safe, approved ways to access keys without workarounds?
- How resilient is our key management approach during outages or incidents?
- Are policies enforced consistently across internal systems, partners, and third-party services?
- Can our strategy scale as data volumes, applications, and automation increase?

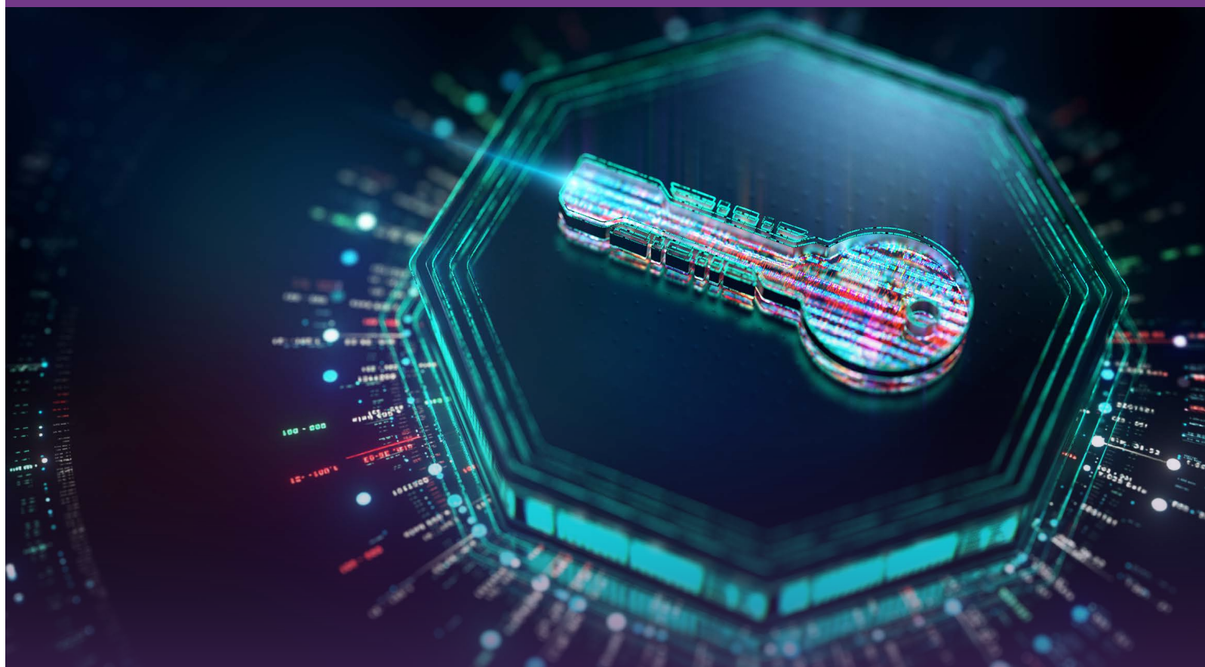
These questions help identify gaps and guide future investments without locking organizations into specific technologies too early.

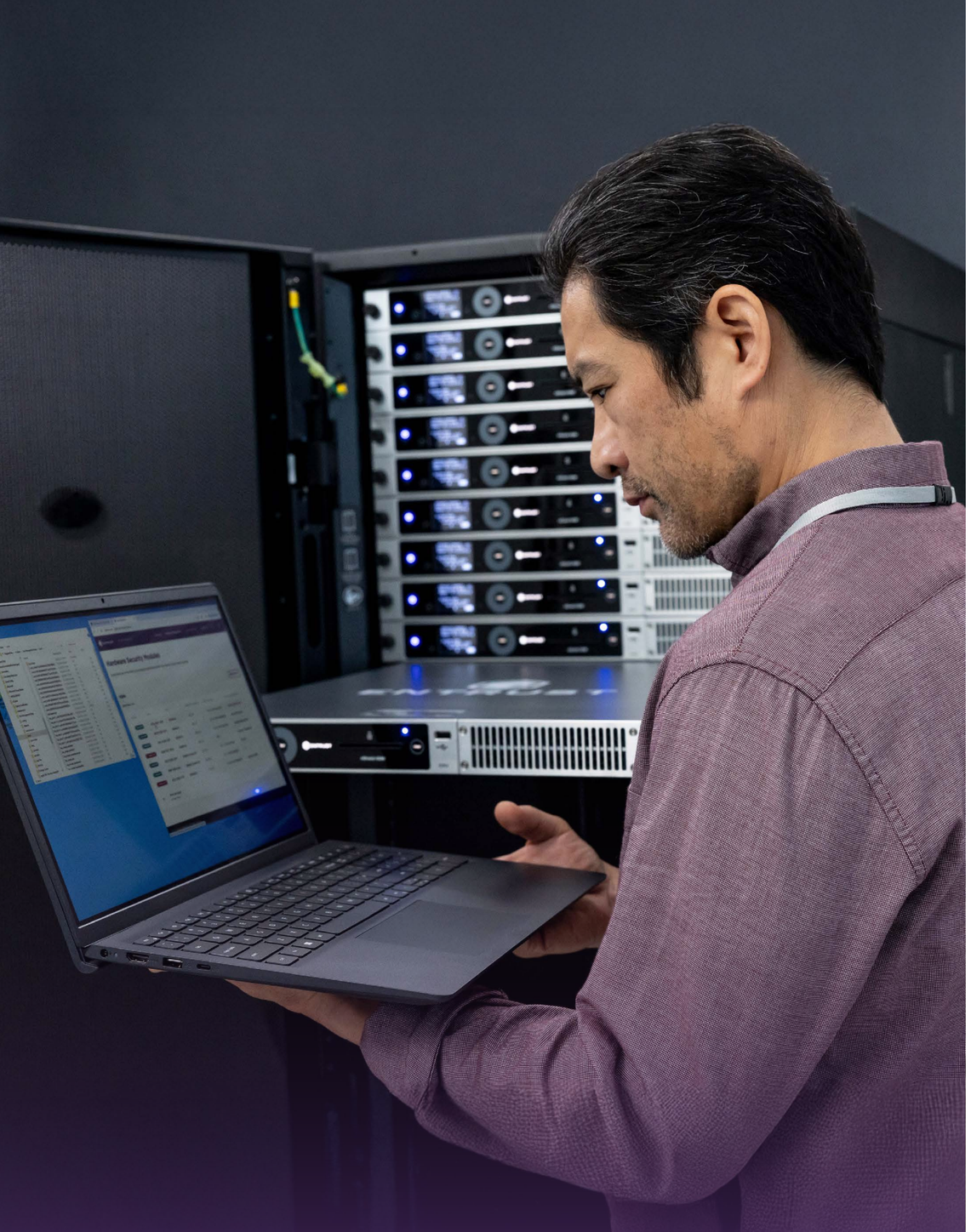
The Future of Key Management

Key management will continue to evolve as organizations rely on cryptography across more systems, applications, and environments. To get ahead, organizations are focused on:

- **Cryptographic agility to adapt to new threats and standards.** Organizations must be able to quickly change algorithms, key sizes, and policies without disrupting operations as threats, regulations, and post-quantum standards evolve.
- **Policy-driven controls tied to identity and context.** Key access is moving toward policy-based enforcement that considers identity, role, environment, and context, rather than relying on static permissions.
- **Greater integration with developer workflows.** Key management must align with modern development tools and processes, providing secure, automated access to keys without impacting delivery.
- **Shifting to secure keys earlier in the application lifecycle.** Addressing key handling, access controls, and rotation during design and build phases reduces risk and prevents insecure practices from reaching production.
- **Preparation for post-quantum cryptography.** Organizations are beginning to adopt hybrid approaches and assess readiness for quantum-resistant algorithms, requiring visibility and control across all cryptographic assets.

Organizations that invest early in adaptable, policy-driven approaches will be better positioned to manage risk, support innovation, and transition smoothly to post-quantum cryptography. Unified platforms like the Entrust Cryptographic Security Platform help organizations centralize visibility, enforce consistent policies, and transition to quantum-ready cryptography with confidence.





Make Key Management a Priority

Cryptographic protection is only as effective as the security and management of the keys behind it. Organizations that treat key management as a foundational security capability are better positioned to protect sensitive data, meet regulatory expectations, and support modern, cloud-based architectures.

It starts with hardware-based protection. HSMs should be used for key generation, storage, and cryptographic operations.

Entrust nShield HSMs provide high-assurance, FIPS-certified key protection, available in on-prem, cloud-based, and hybrid deployments to help organizations build a resilient, future-ready cryptographic foundation.

Learn more about Entrust nShield HSMs

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST

SECURING A WORLD IN MOTION