Solution Brief

Enterprise Key Management: Securing Data Across Complex Environments

Achieve seamless, scalable, and compliant encryption key management for your enterprise.

cpl.thalesgroup.com

THALES
Building a future we can all trust

Enterprise Key Management (EKM) is the backbone of robust data security strategies. In a digital landscape dominated by multi-cloud environments and stringent regulatory requirements, your organisation must manage cryptographic keys with precision. This includes generating, storing, distributing, rotating, and securely retiring keys to ensure only authorised users can access your data. With EKM, you control critical practices like key rotation, revocation, and auditing, helping you maintain security and compliance.

The Barriers to Effective Data Protection

Managing cryptographic keys is no easy task, especially in a complex enterprise IT setting. Common challenges include:

Achieving scalability across multi-cloud systems: Enterprises must manage thousands of cryptographic keys across cloud service providers (CSPs) and on-premises systems. Inconsistent protocols and siloed tools create inefficiencies and vulnerabilities.

Maintaining compliance: Regulatory mandates such as GDPR, HIPAA, and PCI DSS require robust encryption practices. Non-compliance can result in fines ranging from 4% of global turnover to millions in direct penalties.

Integration across hybrid environments: Ensuring consistent security across on-premises, cloud, and hybrid systems is challenging. CSPs operate under the Shared Responsibility Model, which means they secure the infrastructure, but you are responsible for safeguarding your data, including encryption and key management. Poor integration can create security gaps, such as inconsistent access controls, increasing the risk of data breaches.

Rising cybersecurity threats: Advanced attacks, such as side-channel breaches, specifically target encryption keys. Enterprises without strong defences face significant risks of data loss and reputational damage.

For example, according to 2024 global research by Thales, 49% of enterprises have already encountered a data breach, with 44% of those breaches originating within cloud services.

Cloud Providers vs Dedicated Solutions

When managing encryption keys, organisations often choose between the key management services provided by cloud service providers (CSPs) and dedicated solutions from independent vendors.

Under the Shared Responsibility Model, CSPs provide tools for basic key management, but these are often limited in scope, tied to specific platforms, and can increase vendor lock-in risks.

CSP vs Thales

Feature	CSP	Thales
Integration	Cloud-native	Hybrid support
Scalability	High	Depends on the environment
Security	High but cloud-dependent	Very high, fully compliant
Deployment	Cloud-only	On-prem, cloud, hybrid
Cost	Usage-based	Initial investment and licensing fees
Customization	Limited	Highly customizable

Safeguarding Cryptographic Keys

Effective EKM solutions are designed to address these challenges through comprehensive tools and technologies:

Centralised key management: A unified platform simplifies the management of encryption keys across environments, eliminating silos and enabling consistent policies.

Advanced encryption and supportive tools: Encryption technologies ensure persistent security, while supporting tools like Hardware Security Modules (HSMs), APIs, and access controls enable secure operations. Automation of key lifecycle activities—such as rotation and revocation—further enhances efficiency.

Compliance enablement: EKM systems provide built-in audit trails, reporting capabilities, and policy enforcement mechanisms to ensure alignment with global regulations.

Orchestration and integration: Seamless integration with databases, cloud platforms, and applications ensures consistent key usage and secure workflows, from DevOps to analytics.

Scalability and flexibility: Modern EKM solutions are designed to grow alongside enterprises, adapting to new environments and technologies without compromising performance.

Making Key Management Simpler and Smarter

EKM doesn't have to be complex. Streamlining key management is possible through unified, automated solutions that prioritise usability and scalability.

Unified platforms: Centralised systems offer a single interface for managing keys across hybrid and multi-cloud environments, reducing administrative overhead and ensuring consistent governance.

Automation: Key rotation, policy updates, and access controls can be automated, reducing manual intervention and minimising errors.

Scalability: Flexible solutions adapt to enterprise growth, whether expanding cloud adoption or integrating new technologies.

Through these measures, enterprises can achieve robust key management while reducing operational burdens.

Adapting to Tomorrow's Data Security Needs

Looking ahead, EKM solutions must evolve to address emerging challenges and technologies:

Quantum-resistant encryption: As quantum computing becomes a reality, encryption standards must adapt to maintain data security. EKM systems must incorporate quantum-resistant algorithms to remain future-ready.

Confidential computing: Platforms designed for secure processing environments are becoming essential for sensitive data operations.

DevOps and cloud integration: Seamless integration with DevOps workflows ensures that key management aligns with agile software development practices.

Regulatory evolution: As regulations continue to tighten, EKM systems must enable real-time policy updates and continuous compliance monitoring.

Effective EKM requires advanced technologies, specialised expertise, and clear, enforceable policies. Partnering with a flexible vendor like Thales ensures a scalable, secure strategy that evolves with your organisation's needs and supports long-term growth.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.