Product Brief

THALES

CYBERSECURITY

CipherTrust Application Key Management

cpl.thalesgroup.com

THALES

CYBERSECURITY

CipherTrust Application Key Management (CAKM) is an enterprise-grade encryption key management product designed to securely handle cryptographic keys used by database encryption technologies such as Oracle Transparent Data Encryption (TDE) and Microsoft SQL Server EKM. CAKM operates with CipherTrust Manager and the CipherTrust Data Security Platform-as-a-Service (CDSPaaS) to externalize and centrally control encryption keys that would otherwise reside on database servers. It encrypts Data Encryption Keys (DEKs) with a Master Encryption Key (MEK) stored separately, ensuring that data-at-rest remains protected even if database files are compromised. CAKM supports encryption with minimal impact on application performance and requires no changes to existing applications while enforcing separation of duties among administrators.

Organizations that rely on native tools and customer scripts for the handling of encryption keys face heightened security and compliance and operational risks. Encryption keys may be inadequately protected, increasing the chance that attackers can steal or misuse them to decrypt sensitive database data, and manual or fragmented key handling makes it difficult to enforce consistent policies, audit key usage or meet regulatory requirements such as PCI-DSS, HIPAA or GDPR, potentially resulting in compliance failures and fines. Without centralized visibility, keys can proliferate unchecked across environments (key sprawl), making it harder to control access, revoke compromised keys, and respond effectively to incidents, while mismanaged or lost keys can disrupt business operations or even render critical data inaccessible.

Using **CAKM with enterprise key management (like CipherTrust Manager) and the broader CDSPaaS ecosystem** gives organizations clear security, compliance, and operational advantages. By centralizing encryption key storage and lifecycle control outside of individual database servers, CAKM **reduces key exposure risk**, enforces **separation of duties** so that DBAs cannot access master keys, and ensures consistent key policies across hybrid and multi-cloud environments. Centralized key lifecycle management — including secure key generation, rotation, revocation, and retirement — simplifies operations and minimizes human error, while robust auditing and monitoring help organizations meet regulatory requirements such as **PCI DSS, HIPAA, and GDPR** with clear, enterprise-wide visibility and reporting. Integrating with enterprise CM and CDSPaaS also delivers unified governance across platforms, improves operational efficiency, and strengthens overall data security posture, making compliance and key control reliable and scalable across complex environments.

Benefits

Stronger security & separation of duties: Keys are stored centrally outside database servers, with support for FIPS-validated HSMs, reducing exposure and preventing DBAs from accessing master keys.

Improved compliance & auditability: Centralized control and detailed logging support regulations such as PCI DSS, GDPR, and HIPAA, simplifying audits and traceability.

Unified key lifecycle management: Keys are consistently generated, rotated, revoked, and retired across environments, reducing manual effort and errors.

Independent cryptographic control: Keys can be rotated or revoked without impacting database engines, while intelligent caching balances security and performance.

Centralized monitoring & visibility: Enterprise logging provides insight into key usage and policy changes, strengthening governance, forensics, and incident response.

Scalable for large deployments: Central management reduces complexity and operational risk across large, hybrid, and multi-cloud database environments.

Performance & resilience through caching: Efficient key caching improves performance and availability while allowing tuning to security and workload requirements.

Quorum-based administrative controls: Multi-administrator approval for critical operations protects against unauthorized or high-risk changes.

CAKM with CDSPaaS

Centrally managed CAKM with CDSPaaS integrates standard key management into the CipherTrust Data Security Platform as a Service, providing a single, unified control plane for database encryption across environments. It offers a central "pane of glass" with real-time health and status visibility for all configured databases, simplifying monitoring and operations. Centralized configuration automatically synchronizes policies without service restarts, reducing manual effort and downtime. Token-based authentication and persona-based role separation further improve usability, governance, and security. Together, these capabilities simplify management at scale, strengthen compliance, and reduce operational complexity across hybrid and multi-cloud environments.

Use Cases

Security Administrator

- Gains centralized control and visibility over all encryption keys and policies.
- Enforces consistent access controls and separation of duties, reducing risk of unauthorized access.
- Simplifies compliance with standards like PCI DSS, GDPR, and HIPAA through centralized auditing and detailed logs.
- Improves governance, incident investigation, and audit readiness.

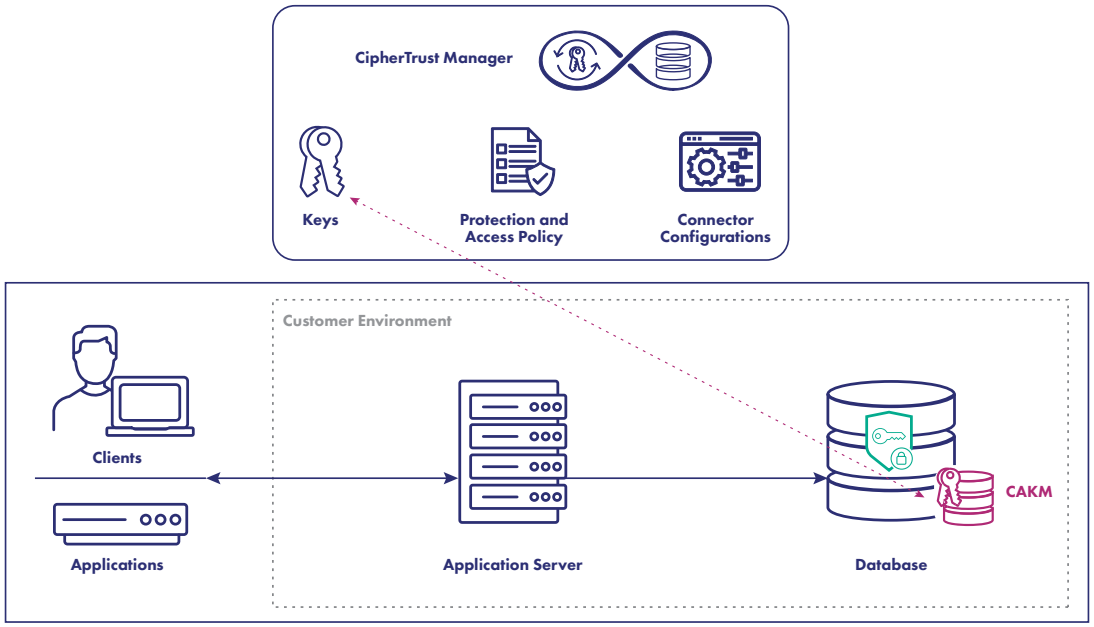
Database Administrator (DBA)

- Manages database functions without dealing directly with cryptographic key storage or lifecycle.
- Configures database encryption (e.g., Oracle TDE, SQL Server EKM) through CAKM, ensuring keys are stored externally and securely.
- Avoids manual key handling and potential mistakes, while maintaining database performance.
- Separation of duties reduces exposure to key misuse and insider risk.

DevOps Administrator

- Integrates key management into CI/CD pipelines and infrastructure automation without custom cryptographic coding.
- Ensures consistent application of security policies and automated key lifecycle tasks across environments.
- Reduces fragmentation in key handling across development and operational environments.

CAKM Database Protection Flow



CipherTrust Data Security Platform

CipherTrust Data Security Platform delivers unified data protection by integrating data discovery, monitoring, protection, and control into a scalable solution. It identifies sensitive data across cloud, on-premises, and hybrid systems, continuously monitors usage and risk, applies strong encryption, tokenization, and key management, and enforces granular access controls. This holistic methodology helps organizations reduce exposure, strengthen compliance, and maintain consistent security policies while simplifying administration and safeguarding critical information throughout its lifecycle.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted organizations protect critical applications, data, identities, and software anywhere, at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us