Product Brief

CipherTrust Cloud Key Management

thalestct.com

THALES
Building a future we can all trust

THALES

Industry best practices as defined by the Cloud Security Alliance (CSA) require that keys be stored and managed outside of the cloud service provider and the associated encryption operations[1]. Cloud Service Providers (CSPs) can comply with best practices by offering Bring Your Own Key (BYOK) or Hold Your Own Key (HYOK) services to enable customer control of the keys used to encrypt their data. Customer control of the keys allows for the separation, creation, ownership and control, including revocation, of encryption keys or tenant secrets used to create the keys.

CipherTrust Cloud Key Management (CCKM) increases efficiency by reducing the operational burden—even when all of the cloud keys are native keys. Giving customers lifecycle control, centralized management within and among clouds, and visibility of cloud encryption keys reduces key management complexity and operational costs. Customers report that they stepped away from managing keys across a heterogeneous environment and invested in CCKM to enable them to move securely to the cloud—and their cloud use is growing exponentially, reducing management overhead and the potential for security holes.

Control Cloud Encryption Keys

- Leverage the value of BYOK and HYOK services with full-lifecycle cloud encryption key management
- Gain higher efficiency with centralized key management across hybrid, single- and multi-cloud environments, including key discovery, management of native cloud keys and automated key rotation
- Comply with the most stringent data protection mandates with secure key origination
- Amplify the benefits of native keys by using a robust multi-cloud platform with outstanding UI

Best Practices

Industry and internal data protection mandates require increasing protection for sensitive cloud data. Meanwhile, CSA and industry analysts state that cloud encryption keys should be managed by customers. Key management systems (KMSs) can grow to hundreds of master keys per KMS—requiring knowledge of how, when, and by whom encryption keys are used, in addition to backing up, monitoring, rotating, expiring, archiving, suspending, restoring, and destroying keys as needed. CCKM provides comprehensive key lifecycle management to provide visibility on a single pane of glass, and automate and fulfill requirements for safe, comprehensive key management across multiple clouds.

Improved Efficiency

CCKM offers multiple capabilities in support of increasing efficiency:

- Secure centralized key management for Native, BYOK and HYOK cloud keys from a single browser window, across multiple clouds, regions, accounts, subscriptions, projects, applications, org ids, etc.
- Automated synchronization ensuring that cloud console-specific key operations are visible in centralized key management—even if you have already created thousands of native cloud keys at your cloud provider
- Automated key rotation with support for expiring keys ensuring compliance while saving valuable time
- Metadata is collected and laid out in the same order for every cloud provider, removing the need to look for data in disparate places

Single Pane of Glass

Access to each cloud provider from a single console, across multiple accounts, regions, subscriptions and projects makes it easier for organizations to understand how their workloads across different clouds are protected. We continually increase key visibility to make it easier for administrators to manage and control access to the keys in minutes instead of days, and stop threats faster.

Strong Encryption Key Security

Customer key control requires secure key generation and storage. CCKM leverages the security of the CipherTrust Manager, Luna Network HSM, or the Vormetric Data Security Manager (DSM) to create keys with up to FIPS 140-2 Level 3 security.

Hold Your Own Key

CCKM services respond to encryption key requests from cloud providers, supporting many of the emerging HYOK offerings: AWS External Key Store (XKS); Google Cloud External Key Management (EKM), Google EKM Ubiquitous Data Encryption (UDE), and Google Workspace Client-side Encryption for Drive, Gmail, Google Calendar and Google Meet; Microsoft DKE, OCI EKMS, and Salesforce Cached Keys.

1 See CSA CCM EKM-04.

The Compliance Tools You Need

Visibility reports demonstrate compliance to the regulator for mission-critical workloads. Logs may also be directed to a syslog server or Security Information and Event Management (SIEM) tool.

Automation Tools Support Your Initiatives

CCKM capabilities are available programmatically using RESTful APIs, enabling the power of centralized cloud encryption management to work with your automation and self-service initiatives. Interactively explore the APIs with our built-in API playground.

Flexible Deployment Options

Deployment environments include: public cloud, private cloud, hybrid cloud, physical appliances and an as-a cloud-based subscription service.

Regardless of how and where CCKM is deployed, CCKM can manage keys and access to the keys, in any supported cloud.

To meet different organization's needs, CCKM is available in virtual and physical form factors: Virtual CCKM is an all-software offering easily deployed and can be run in the cloud or on premises and may be found in several cloud provider marketplaces for fast instantiation. Physical appliances are available for customers who prefer an on-prem solution. CCKM service is available on-demand through the Thales Data Protection on Demand (DPoD) marketplace and in CSP marketplaces.

Multi-cloud Data Security Solutions

CCKM simplifies the need to control and manage encryption keys for cloud services, a critical solution for fulfilling industry and organizational data protection mandates. CCKM and many additional Thales multi-cloud security products, including various Bring Your Own Advanced Encryption offerings, all with centralized key management, offer you choices on how best to protect all your cloud data. It's your data in their cloud.

Supported clouds and key management ownership models:

Increasing Customer Control

Amazon Web Services (AWS) KMS	Native	BYOK	
AWS CloudHSM	Native		
AWS XKS			HYOK
AWS GovCloud	Native	BYOK	HYOK
Google Cloud Platform CMEK	Native	BYOK	
Google Cloud Platform EKM			HYOK
Google Cloud Platform EKM UDE			HYOK -CC[1]
Google Workspace CSE			HYOK
Microsoft Azure Cloud	Native	BYOK	
Microsoft Azure GovCloud	Native	BYOK	
Microsoft Azure Managed HSMs	Native	BYOK	
Microsoft Office 365		BYOK	HYOK [2]
Oracle Cloud Infrastructure	Native	BYOK	HYOK
Oracle Cloud for Government	Native	BYOK	HYOK
Oracle US Defense Cloud	Native	BYOK	HYOK
Oracle National Security Regions	Native	BYOK	
Salesforce.com	Native	BYOK	HYOK[3]
Salesforce GovCloud Plus	Native	BYOK	HYOK[3]
Salesforce Sandbox	Native	BYOK	HYOK[3]
SAP Data Custodian	Native	BYOK	HYOK[4]

[1] HYOK-CC is HYOK for Confidential Computing
[2] Microsoft Double Key Encryption (DKE)
[3] Cache-only Key Service
[4] Coming Soon

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com