

# CipherTrust Cloud Key Management Solutions for Amazon Web Services



External Key Store (XKS), the new Hold Your Own Key (HYOK) service from Amazon Web Services (AWS), allows customers to protect their data residing in AWS using encryption keys stored outside AWS.

Thales is collaborating with AWS to accelerate the ability of organizations to migrate sensitive data and workloads to the cloud. AWS customers can block and unblock access to encrypted data with keys stored and managed outside of AWS.

## CipherTrust Cloud Key Manager

Thales and AWS innovated to create a versatile, feature-rich implementation, providing customers with choices in managing their keys. The collaboration extends the existing key management ownership model of Bring Your Own Key (BYOK) with a Hold Your Own Key (HYOK) offer. With XKS and CipherTrust Cloud Key Manager (CCKM), customers can now choose to have data protected with keys physically located outside of AWS Cloud. The externally stored keys are only accessible via explicit customer authorization. XKS supports most AWS services already integrated with AWS KMS.



## Benefits

- Maximize choice from a single console, manage Native, BYOK, HYOK keys across clouds
- Demonstrate compliance with privacy regulations
- Improve operational sovereignty to protect against internal and external bad actors
- Reduce threat surface by centralizing control of keys outside of cloud providers
- Reduce costs by simplifying key management
- Faster time to value by speeding up migration to the cloud

## Gain Strong Key Control and Security

XKS enables customers to separate key management from AWS controlled encryption, offering a crucial layer of separation of duty and control. CCKM delivers key generation, reporting, and key lifecycle management that help fulfill internal and industry data protection mandates, with optional FIPS 140-2-certified hardware.

## Meet Organizational Needs with Flexible Deployment Options

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. Deployment environments include: public cloud, private cloud, hybrid cloud, and physical appliances. Physical appliances are available for customers who prefer an on-prem solution. Regardless of how and where CCKM is deployed, CCKM can manage keys, and access to the keys, in any reachable, supported cloud.

## Increased Efficiency

CCKM centralizes encryption key management from multiple environments, presenting all supported clouds, and even multiple cloud accounts, in a single pane of glass. Advanced cloud key management services and capabilities include automated key rotation, key expiration handling, and cloud key vault synchronization--dramatically reducing the time required for cloud key life cycle management.

In addition to HYOK and BYOK, CCKM supports full key lifecycle management of native cloud keys, including keys stored in AWS CloudHSM.

## Align with Best Practices

Deliver compliance, best security practices and control of your data by separating encryption key control from data encryption and decryption operations. Gain operational insights on encryption key usage with reports and logs provided by CCKM.

## Integrates With Your Automation Initiatives

CCKM capabilities are available programmatically using RESTful APIs, enabling DevOps and IT teams the power of centralized cloud encryption management to work with the organization's automation and self-service initiatives.

## How it Works

XKS is an option within AWS KMS. Once an externally managed key is linked to a KMS key ID using XKS, the externally managed key can be used to protect data in any of the AWS services that integrate with AWS KMS.

External key stores let you control data sovereignty. Data keys encrypted under KMS keys in your external key store can be decrypted only in the CCKM under customer control. When the customer revokes access to CCKM, by blocking the key or disconnecting the external key store, AWS loses all access to the customer's encryption keys, and data encrypted under customer keys cannot be decrypted; it is crypto-shredded.

## Thales TCT is Here to Help

Contact Thales TCT or try CCKM for free today to help you assess and define the data protection strategy that best suits your organizational requirements, and for integration guides to help accelerate your deployment.

## About Amazon Web Services

Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud offering, with more than 200 fully featured services available from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, increase security, become more agile, and innovate faster.

## 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](http://www.thalestct.com)