Solution Brief

Thales CipherTrust Cloud Key Management for Oracle Cloud Infrastructure

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Benefits

- Meet compliance mandates such as PCI DSS, GDPR, Schrems II and CCPA
- Streamline data encryption management with seamless key rotation
- Enable separation of duties to provide customers more control over their own data
- Reduce administration costs with centralized key and policy management
- Optional FIPS 140-2 Level 3 hardware security

The Problem

The adoption of Oracle Cloud Infrastructure (OCI) continues to grow exponentially. A successful migration to OCI from legacy on-prem implementations requires that organizations must first address the security of their sensitive data. While OCI's native encryption allows organizations to securely move sensitive data to OCI, it also has new administrative and compliance implications. To extract the full value of OCI, organizations need to find a way to maintain control of their sensitive data and streamline their security administration. Fortunately, Thales together with Oracle ease the challenges of managing data protection of sensitive data when migrated to OCI.

The Solution

Thales' CipherTrust Cloud Key Management (CCKM) provides visibility and streamlined security administration. The integration of OCI External Key Management Service (EKMS) with CCKM gives organizations the ability to physically store their keys outside of OCI and use a single pane of glass to seamlessly manage the encryption key lifecycle for OCI Services and other cloud encryption solutions. OCI offers key management with integrated visibility and security to secure data in the cloud. OCI encryption combined with CCKM gives organizations seamless end-to-end security. To enable customer control of encryption keys, Thales solutions include Oracle Native Key Management, Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) Services.

Native Keys

Native Keys are available through OCI's Vaults. CCKM automates key inventory and rotation to simplify compliance and ensure that OCI key operations are visible from the Thales centralized key manager - even if you already created thousands of native cloud keys.

Bring Your Own Key (BYOK)

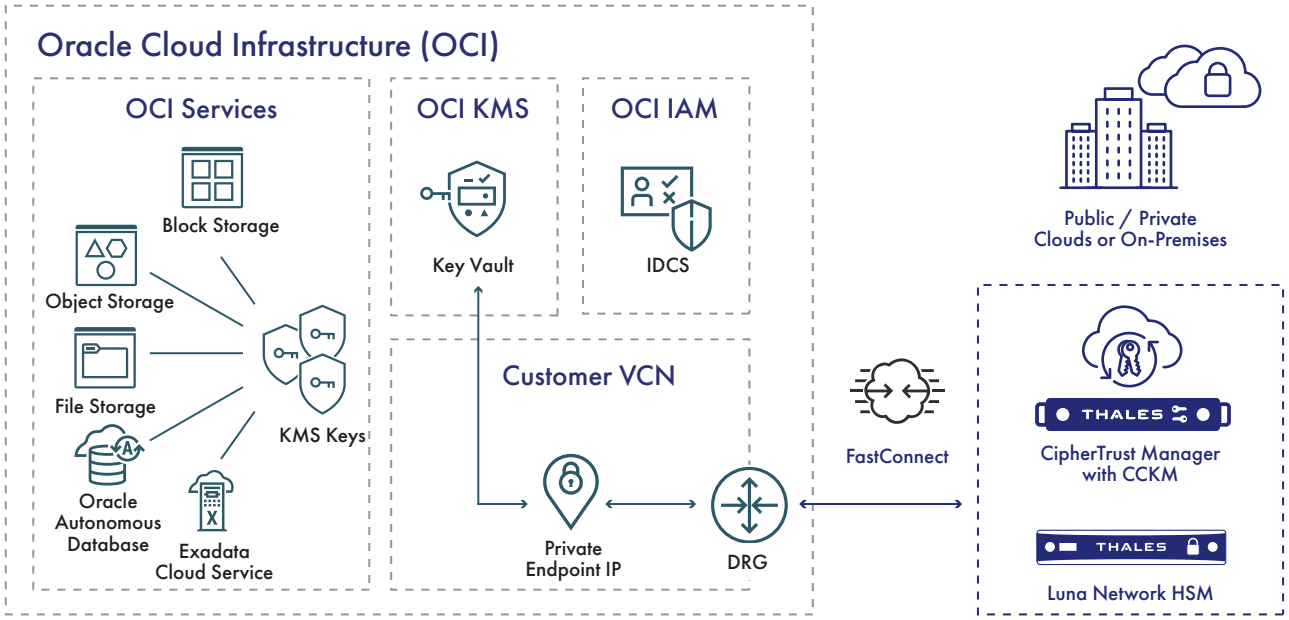
Customer key control allows for the separation, creation, ownership and control, including revocation, of encryption keys. Leveraging cloud provider BYOK APIs, CCKM reduces key management complexity and operational costs by giving customers lifecycle control of cloud encryption keys with centralized management and visibility.

Hold Your Own Key (HYOK)

OCI EKMS allows OCI customers to physically store their encryption keys outside of the cloud in an HYOK model, enabling separation of duties, and giving customers more control of their own data protection. Thales co-innovated with OCI to develop the EKMS offering resulting, in the first HYOK solution available to OCI customers. With CCKM, organizations consolidate OCI encryption key storage and lifecycle management in the same centralized key manager they use for their non-OCI encryption.

CCKM supports keys being stored on CipherTrust Manager or Luna Network HSM. Administrators must explicitly authorize sharing before the externally stored keys become available for use by OCI. Though they may use OCI encryption services with CCKM, customers remain firmly in control of their encryption keys, and by extension, their data.

Figure 1. Deployment architecture example - CCKM hosted external to OCI



Supported Oracle Cloud Services

External Key Management design is transparent to OCI services or customer applications.

So, if your services (examples: Object Storage, Block Volume, Database) are already integrated to OCI Key Management, then you can leverage the External Key Management capabilities.

Centrally Define and Manage Policies to Separate Duties

Administrators can use CCKM to set authentication and authorization policies that define which users and processes are allowed to access the encrypted data in clear text. Organizations tighten governance of their sensitive data through these controls. Properly tuned policy-based access controls provide an important security layer for organizations subject to mandates that require clear separation of duties between IT and security administrators.

Detailed Logging Functionality for Auditing and Reporting Requirements

CCKM records detailed data concerning key status and access in centralized logs that simplify reporting to auditors and regulators. Centralized tracking of key usage and access requests reduces blind spots and improves data security. CCKM's reports help to streamline the compliance reporting process while strengthening security around OCI's native encryption keys.

Streamlined, Simplified Encryption Administration

Vendor-provided encryption can easily turn into a collection of security silos if not managed well. CCKM consolidates OCI's encryption keys into an easy-to-use platform where organizations can manage OCI keys alongside keys from a wide variety of encryption solutions including: transparent encryption, application data protection, database protection and an ever growing list of vendors supporting the OASIS Key Management Interoperability Protocol (KMIP) standard.

Flexible Deployment Options to Meet Any Need

CCKM is available as a virtual machine, a physical appliance and as a service. Virtual CCKM is an all-software offering that deploys and runs easily in OCI, on premises, and in a range of third-party public clouds, private clouds, hybrid and multi-clouds, physical appliances and an as-a cloud-based subscription service. Organizations that prefer to keep their encryption keys stored or managed from an on-premises location have a physical appliance option to satisfy the most stringent requirements.

In Summary

OCI's native encryption functionality provides the security that customers need to move their sensitive data to the cloud. With Thales' encryption key management, additional control is offered to customers to protect their data, providing the tools organizations need to demonstrate that they alone, are in control of their own data – even as it resides outside the walls of their own data center. When Thales and Oracle are combined, customers have a powerful solution to the security, compliance and sovereignty challenges associated with widespread cloud adoption.

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.

About Oracle Cloud Infrastructure

Oracle Cloud Infrastructure (OCI) is a deep and broad platform of cloud infrastructure services that enables customers to build and run a wide range of applications in a scalable, secure, highly available, and high-performance environment. From application development and business analytics to data management, integration, security, AI, and infrastructure services including Kubernetes and VMware, OCI delivers unmatched security, performance, and cost savings. In addition, with multicloud, hybrid cloud, public cloud, and dedicated cloud options, OCI's distributed cloud offers customers the benefits of cloud with greater control over data residency, locality, and authority, even across multiple clouds. As a result, customers can bring enterprise workloads to the cloud quickly and efficiently while meeting the strictest regulatory compliance requirements.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us