Case Study

IIFL Group Differentiates Itself with Early Adoption of Mandatory Security Regulations

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

How Thales helped a leading financial conglomerate become one of the first Regulated Entities to initiate compliance with a new government security regulation — reinforcing the conglomerate's position as a market leader.

Challenge

IIFL Group is a conglomerate with a portfolio of companies. IIFL Securities caters to high-end investors as one of the largest independent full-service retail and institutional brokerage houses in India. 5Paisa Capital caters to retail investors as a discount stockbrokerage with a self-service stock trading application.

Urgent projects took precedence for over a year as Shanker Ramrakhiani, CISO of IIFL Group, looked for an opportunity to gain complete ownership of the encryption keys. As CISO of one of the top financial conglomerates in India, Ramrakhiani wanted to future-proof their infrastructure with an external key manager that had a platform approach with support for Bring Your Own Key (BYOK), Bring Your Own Encryption (BYOE) and other use cases as their business grew (e.g., multi-cloud, secrets management, data discovery and classification). Like other financial organizations in India who were moving sensitive data to the cloud to increase scale and reduces CAPX, IIFL Group was dealing with increased cyber attacks so Ramrakhiani had to balance strategic investments with urgent needs.

BYOK rose in priority as a strategic investment in March 2023 when the Securities and Exchange Board of India (SEBI) introduced the Framework for the Adoption of Cloud Services by Regulated Entities (REs). SEBI set baseline standards for security and regulatory compliance to help REs implement secure and compliant cloud adoption policies. The framework includes implementation of strong controls for data protection and cryptographic key management in the cloud, including adoption of "Bring Your Own Key" (BYOK) or "Bring Your Own Encryption" (BYOE) where applicable, and use of Hardware Security Modules (HSMs) for secure generation and storage of keys.

Shanker Ramrakhiani, CISO of IIFL Group

Ramrakhiani recognized that trust is crucial for both ends of the investor spectrum and IIFL Group is committed to publicly demonstrating their trustworthiness to all of their investors. So, for both IIFL Securities and 5Paisa Capital, Ramrakhiani committed to being one of the first REs to be SEBI-compliant. By complying with the new security regulation early, IIFL Group reinforces their position as a market leader and demonstrates a strong commitment to protecting their customers' data and finances which will attract more new investments and new customers. IIFL Group is establishing themselves as a market leader across the spectrum of investors.

All finance organizations need to comply with government regulations, regulated authority guidelines and internal governance policies. Ramrakhiani saw that if they implemented BYOK early, they could comply with SEBI and reinforce not only their security estate but their position as a market leader – leveraging their security investment to achieve a win at both the security team and business levels.

IIFL

Solution

An external key manager with a platform approach, a cloud key manager and a hardware security module (HSM).

To help with SEBI compliance and to future-proof their infrastructure for both IIFL Securities and 5Paisa Capital, IIFL Group chose Thales CipherTrust Data Security Platform (CDSP), CipherTrust Cloud Key Management (CCKM), and Luna Network HSMs.

External key manager with a platform approach:

CipherTrust Data Security Platform/ CipherTrust Manager

CipherTrust Data Security Platform was selected for the platform, featuring CipherTrust Manager as the external key management system (KMS). Initially, the customer implemented one of the platform's integrated solutions with a plan to add more integrated solutions in the near future.

> " We are proud to be an early adopter of the SEBI Framework for the adoption of cloud services by REs. It enables us to bring more security and confidence to our customers."
>
> **– Shanker Ramrakhiani, CISO of IIFL Group**

Using the CipherTrust Data Security Platform enables quick integration with multiple proven use cases including CipherTrust Cloud Key Management, Transparent Encryption and Secrets Management.

Using the CipherTrust KMS simplifies data security administration and accelerates time to compliance.

Cloud Key Manager:

CipherTrust Cloud Key Management

CipherTrust Cloud Key Management (CCKM) was selected to centralize and automate key lifecycle management across the enterprise's Microsoft Azure environment with a plan to expand with Amazon AWS. Within five months, IIFL Group expanded to use AWS in addition to Azure, secure in the knowledge that they can add more supported clouds seamlessly and always find the metadata in the same location.

CCKM can discover and manage thousands of Azure and AWS native keys. The solution provides the conglomerate with a single user interface for simplified management and control over their cloud native and bring-your-own-key (BYOK) keys managed on premises with HSMs guaranteeing high entropy key generation and secure key storage.

CipherTrust Cloud Key Management enables key generation, usage logging and reporting, and facilitates 'key decoupling' by securely storing the keys separately from the encrypted data. These features provide customers with control over the encryption keys used to encrypt their data in the cloud and are considered industry best practices. When organizations choose an external key manager, the majority choose CCKM. With every release we help to de-risk the customer's security estate and increase the customer's control.

Using CCKM, customers can support BYOK keys to help them comply with SEBI, reclaim control of regulated workloads, highly sensitive data and cloud keys. Customers can reclaim time previously lost to repetitive or non-productive tasks, looking for keys and their metadata, recovering from data loss, and managing KMS systems across clouds. Additional power comes with remaining in control across multiple clouds or KMS systems, and ensuring they adhere to compliance mandates.

Hardware security module:

Luna HSM

Thales Luna HSMs are a proven product entrusted by banks around the world to ensure protection of the most sensitive data. Adding Luna HSMs to the existing infrastructure was smooth and seamless thanks to its efficient setup and administration. The overall security architecture, including tamper-resistant hardware, multi-factor authentication and secure delivery protect cryptographic keys and sensitive data. It is scalable, flexible and crypto agile to handle multiple applications with different crypto requirements. Luna HSMs are available in multiple models and form factors to meet customer needs, which can be used on-premises, in the cloud, or across hybrid environments making it the ideal choice to support digital transformations.

> " Security doesn't have to be limited to being a cost center. Choose your solution wisely and your security becomes a competitive edge."
>
> **– Shanker Ramrakhiani, CISO of IIFL Group**

Benefits

The combination of CDSP, CCKM and Luna HSM:

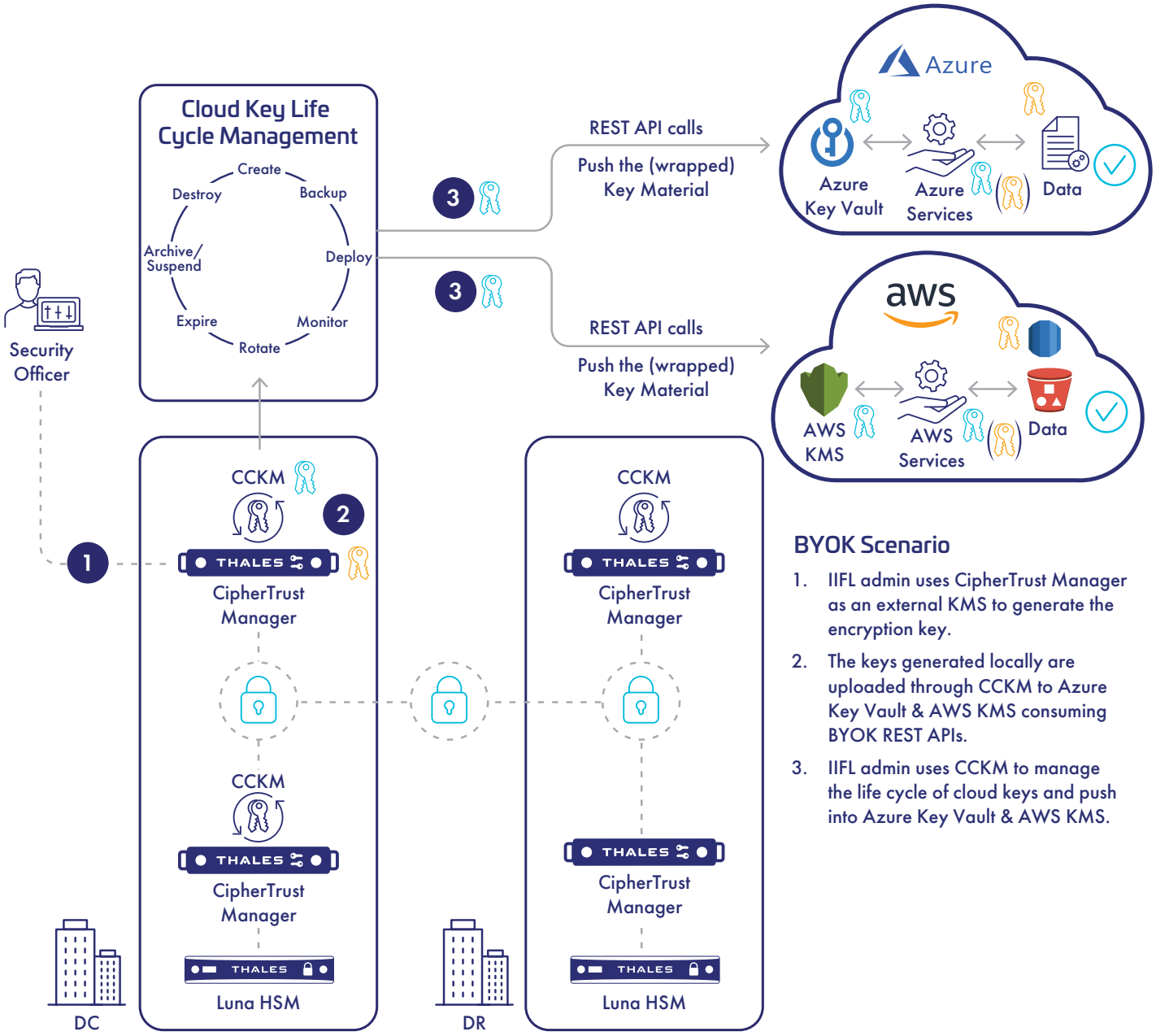
- Helps IIFL Group to be SEBI-compliant
- Gives IIFL Group full control of its encryption keys
- Improves ease-of-use, reduces complexity
- Supports multi-cloud
- Enables quick integration with multiple proven use cases including Transparent Encryption and Secrets Management
- Gives access to an unparalleled partner ecosystem
- Helps IIFL Group to reclaim time and control that had been yielded to the CSP

With the implementation of BYOK, IIFL Group CISOs and security teams are now more efficient and are retaining control over their encryption keys so they can better protect customers' PII and their financial data. Despite hackers targeting India's financial industry, CISOs can relax a little on the subject of penalties from regulatory organizations, and the ever-present questions from board members asking if the company is secured.

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.

BYOK for Azure & AWS



BYOK Scenario

1. IIFL admin uses CipherTrust Manager as an external KMS to generate the encryption key.
2. The keys generated locally are uploaded through CCKM to Azure Key Vault & AWS KMS consuming BYOK REST APIs.
3. IIFL admin uses CCKM to manage the life cycle of cloud keys and push into Azure Key Vault & AWS KMS.

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