

Global Energy Leader Secures High-Value Secret Data with Thales CipherTrust Cloud Key Manager and SAP

The Business Challenge

An industry-leading global energy company needed to protect “Tier 1” highly classified internal data as they migrated their SAP HANA and SAP applications to the public cloud. To adhere to their internal data protection mandates, they needed a solution that provided control over the protection of secret data by keeping encryption key generation and storage on-premises. This Bring Your Own Keys (BYOK) approach added the sovereignty they required while still enabling the efficiencies of cloud migration.

The Solution

To meet their mandate of local key generation and storage, the energy company implemented Thales CipherTrust Cloud Key Manager integrated with SAP Data Custodian. Thales leveraged their close working relationship with SAP to jointly expand and improve the external key management capabilities of Data Custodian. This combined solution offers the benefits of both SAP’s standard cloud-based key vault with the external key lifecycle management sovereignty of a Thales Bring Your Own Key (BYOK) solution.

CipherTrust Cloud Key Manager

CipherTrust Cloud Key Manager provides the global energy company with simplified management and control over Bring Your Own Keys managed on-premises with up to FIPS 140-2 Level 3 certified Hardware Security Modules (HSMs) guaranteeing high entropy key generation and secure key storage.

Specially designed for managing cryptographic keys in multi-cloud environments, CipherTrust Cloud Key Manager enables single pane of glass key management and gives users complete control of their encryption keys in the public cloud.

Offering seamless support for SAP’s Data Custodian, CipherTrust Cloud Key Manager automates key lifecycle management, enables key generation, usage logging, reporting, and facilitates ‘keys decoupling’ by securely storing the keys separately from the encrypted data. Once the encryption keys are generated locally by Thales CipherTrust Cloud Key Manager they are imported to Data Custodian’s key vault, where they replace and behave the same as native keys and can be used across the SAP’s portfolio of cloud applications.



CipherTrust Cloud Key Manager, together with SAP Data Custodian, provided the global energy provider a secure path to cloud migration while meeting internal data protection mandates.



The Results

With on-premises hosting of CipherTrust Cloud Key Manager, the energy company maintained full ownership of its encryption key lifecycle resulting in complete visibility into how its encryption keys were created, used, and managed in their SAP application ecosystem.

Benefits included:

- Generate encryption keys on-premises to align with internal data protection mandates
- Achieved complete visibility and control over key lifecycle management
- Rooted keys in up to FIPS 140-2 Level 3 security by leveraging CipherTrust Manager and Thales Luna HSMs
- Automated key lifecycle management that simplifies generation, rotation, backup, and revocation of millions of keys
- Encryption key material backup and restoration prevents the possibility of losing access to high-value secret data
- Ability to revoke an encryption key as needed, instantly locking down the protected secret data if and when it was found to be at risk
- Simplifying key management across cloud providers reduced IT costs and training

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.