Solution Brief

Customer Controlled Hold Your Own Key with Thales CipherTrust Cloud Key Management and SAP Data Custodian Key Management Service

Enabling secure and controlled access to SAP encryption keys

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Key Benefits

- Address PCI DSS, GDPR, DORA, LGPD, and CCPA compliance mandates
- Streamline encryption key and policy management for SAP HANA based applications and services
- Separate duties to provide customers full control over their SAP data
- Simplify management and reduce administration costs
- Optional 140-3 Level 3 hardware security

The Challenge

In the world of cloud applications and data deployments, maintaining the security of sensitive data is paramount. Security is a major concern for customers who place SAP's applications and database at the core of their operations. For organizations using SAP's native encryption to secure their critical data, it is essential that they separate duties between their encryption key administrators and their cloud-based SAP services. By keeping these elements distinct, organizations can significantly enhance their data protection and directly address their compliance obligations.

Encryption is the digital lock that safeguards data, ensuring only authorized individuals can access sensitive data. If encryption keys are compromised, the entire dataset becomes vulnerable. Therefore, storing encryption keys within the same environment as the cloud data creates a single point of failure. A breach of these systems could potentially expose the data and the keys, leading to catastrophic consequences. To mitigate this risk, it is essential to hold encryption keys separately from the cloud-based service where data is stored.

The Solution

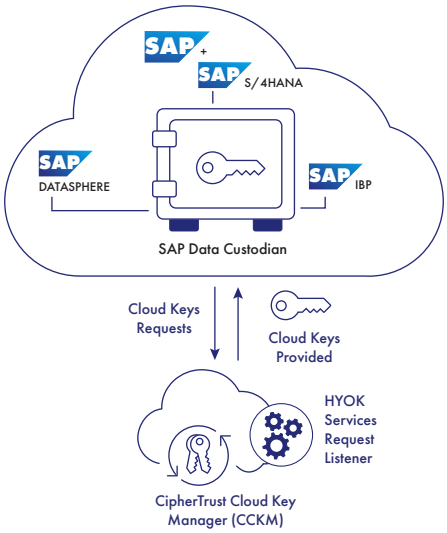
Thales CipherTrust Cloud Key Management (CCKM) integrates with SAP Data Custodian Key Management Service (SAP Data Custodian KMS) to provide full Hold Your Own Key (HYOK) external key storage and management. Organizations can implement a more robust security environment for their applications and services that are backed by SAP HANA by holding encryption keys outside of SAP's cloud-based services. They can choose to store keys on premises or in a dedicated Thales key management service that can even include a hardware security module (HSM). This separation allows for greater flexibility and control over key management processes, including key generation, rotation, and revocation. Additionally, organizations can implement stringent access controls to provide extra protection for the keys.

Furthermore, separating data and encryption keys is often required to achieve security compliance standards such as HIPAA, PCI DSS, DORA, and GDPR. These regulations mandate specific measures to protect sensitive information, and holding encryption keys independently is a key component of meeting these compliance obligations. By implementing this configuration, organizations can demonstrate their commitment to data security and avoid costly penalties or compliance failures.

CCKM supports keys being stored on CipherTrust Manager. Administrators must explicitly authorize sharing keys before the externally stored keys are available for use by SAP HANA based applications and services. Customers remain firmly in control of their encryption keys and, by extension, their data.

Features and Benefits

- Securely store encryption keys outside of the cloud to enforce separation of duties between your organization and your cloud service provider
- Simplify demonstrating compliance with security and privacy regulations such as GDPR, SCHREMS II, PCI-DSS, and CCPA by incorporating best practices and maintaining digital sovereignty
- Mitigate risk through key management controls and workload protection based on applicable compliance mandates
- Generate and store encryption keys with up to FIPS 140-3 validated HSM-based entropy and bring them to your SAP applications
- Gain higher IT efficiency with centralized key lifecycle management across multiple cloud environments
- Comply with the most stringent data protection and sovereignty mandates with encryption and key management
- Simplified compliance reporting with detailed audit logs and prepackaged reports
- Root keys in up to FIPS 140-2 Level 3/FIPS 140-3 Level 3 security by leveraging CipherTrust Manager or Thales Luna HSMs



SAP Data Custodian Key Management Service HYOK as Part of Your Broader Key Management Strategy

CipherTrust Cloud Key Management allows you to manage your SAP Data Custodian KMS alongside all your other keys for any combination of public clouds and private or on premises data infrastructure. This cloud management strategy can be applied to native keys, bring your own keys (BYOK), and hold your own keys (HYOK) leveraging CipherTrust Manager.

SAP Products Supported by Thales Cloud Key Manager

Thales supports HYOK for SAP HANA, SAP products or services backed by SAP HANA (both on-premises and SAP Cloud products), and SAP S/4HANA Cloud Private Cloud Edition. Thales supports a broader list of SAP applications for centralized BYOK management.

SAP APPLICATIONS	BYOK	HYOK
SAP Cloud Products based on SAP HANA	√	√
SAP S/4HANA Private Cloud Edition (RISE and non-RISE)	√	√
SAP S/4HANA Cloud (Grow) IBP	√	√
SAP On-premises product using SAP HANA Platform	√	√
SAP BTP*	√	√
SAP HANA Enterprise Cloud	√	√
SAP Integrated Business Planning for Supply Chain	√	√
SAP Successfactors Incentive Management	√	√
SAP Successfactors HCM**	√	√
SAP Analysis Cloud – Private Edition	√	√
SAP Datasphere	√	√
SAP HANA Cloud, data lake	√	√
SAP Cloud Identity Services	√	
SAP Commissions	√	
SAP Fieldglass Vendor Management System	√	
Backup/Wrapping Keys	√	
General/IaaS Applications (General)	√	

*The integration with SAP Data Custodian is not currently supported across all BTP applications.
**SAP SuccessFactors HCM is supported with HYOK, customers need to purchase the advanced encryption feature from the SuccessFactors product line. SuccessFactors advanced encryption allows the customer to manage their keys through SAP Data Custodian KMS.

Summary

CipherTrust Cloud Key Management with SAP Data Custodian Key Management Service HYOK allows encryption keys to be stored outside the organization's cloud-based service. This powerful Hold Your Own Key option protects the organization's time and data with a single pane of glass view enabling customers to move securely to the cloud.

About SAP

As a global leader in enterprise applications and business AI, SAP (NYSE: SAP) stands at the nexus of business and technology. For over 50 years, organizations have trusted SAP to bring out their best by uniting business-critical operations spanning finance, procurement, HR, supply chain, and customer experience. For more information, visit www.sap.com.

About Thales

Thales is a global leader in cybersecurity, helping the most trusted companies and organizations around the world protect critical applications, sensitive data, and identities anywhere at scale. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.