Solution Brief

Thales CipherTrust Cloud Key Management for Salesforce

Providing customers with encryption key options

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

salesforce PARTNER

Due to a growing number of requirements, including security and sovereignty mandates, organizations need to control their date. This is particularly challenging for enterprises using SaaS-based solutions since they do not directly manage, host, or even own the cloud-based platform containing their data.

Managing encryption keys and storing them securely is the cornerstone to meeting data security and sovereignty requirements. This is because encryption keys (also called cryptographic keys) are the strings of bits generated to encode and decode data. Whoever owns and manages the keys, therefore also ultimately owns the data. This is why organizations must prove they manage and control their encryption keys to be compliant with many digital sovereignty and data protection requirements.

Additionally, ensuring control over encryption keys can bolster security for SaaS-based applications in the event of a cyber-attack since the keys are stored and managed separately from the data.

The Solution

Thales and Salesforce have partnered to provide enterprise customers with choices in managing their data encryption keys for Salesforce data.

External Key Management

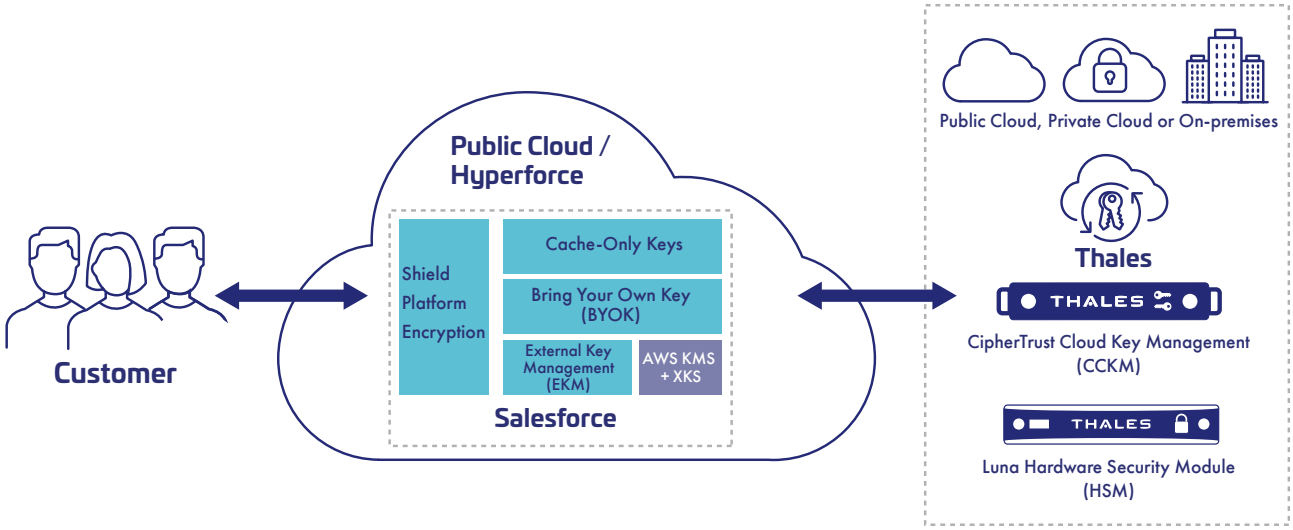
Thales can enable digital sovereignty for organizations using Salesforce by ensuring they retain more control and management over their encryption keys with our CipherTrust Cloud Key Management (CCKM) offering. By using Thales CCKM, organizations can safely store, manage, and maintain the tenant secrets used to derive the encryption keys that protect data within the Salesforce environment.

Thales CCKM delivers key generation, reporting, and key lifecycle management that helps fulfill internal and industry data protection mandates. To securely store encryption keys, customers can leverage Thales CipherTrust Manager with optional FIPS 140-2 Level 3 certified HSM card or Luna Network Hardware Security Modules (HSMs) that securely protect cryptographic keys in a high-assurance, tamper-resistant, network-attached appliance that is FIPS 140-2 Level 3 certified.

By using Thales CCKM, Salesforce customers can implement Cache-Only Keys, Bring-Your-Own-Key (BYOK) and Hold-Your-Own-Key (HYOK) capabilities. By leveraging these options, customers retain more control of their encryption keys - and therefore also their encrypted data. This helps organizations meet compliance and best practice requirements for encryption key management, data security, and digital sovereignty.

Additionally, Thales supports Salesforce External Key Management (EKM) service for Salesforce Shield Platform Encryption, allowing users to provide and manage their own encryption keys that protect their Salesforce content. The combined Salesforce and Thales solution leverages the AWS External Key Store (XKS) service so customers can protect their Salesforce data using encryption keys stored physically outside the cloud.

Thales Encryption Key Management Solutions with Salesforce



Salesforce and Thales - Solution Overview

Flexible Deployment Options

Both Thales CCKM and Luna HSMs are available in both 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 including AWS and Salesforce Hyperforce. Deployment environments include public cloud, private cloud, hybrid cloud, and physical appliances. Physical appliances are available for customers who prefer an on premises solution.

Increased Efficiency

Thales CCKM centralizes encryption key management across all supported clouds, and multiple cloud accounts, regions, subscriptions, org IDs and projects, from a single pane of glass. Advanced cloud key management services and capabilities include automated key rotation, key expiration handling, and cloud key inventory--dramatically reducing the time required for cloud key life cycle management.

Best Practices

Together, Thales and Salesforce offer security best practices (such as CSA CCM EKM-04), control of customer data by separating key control from data encryption/decryption operations, and help gain operational insights on encryption key usage with reports and logs provided by Thales CCKM.

About Salesforce

Salesforce empowers companies of every size and industry to connect with their customers through the power of CRM + AI + Data + Trust. For more information about Salesforce, visit: www.salesforce.com.

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.