cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Application Data Protection

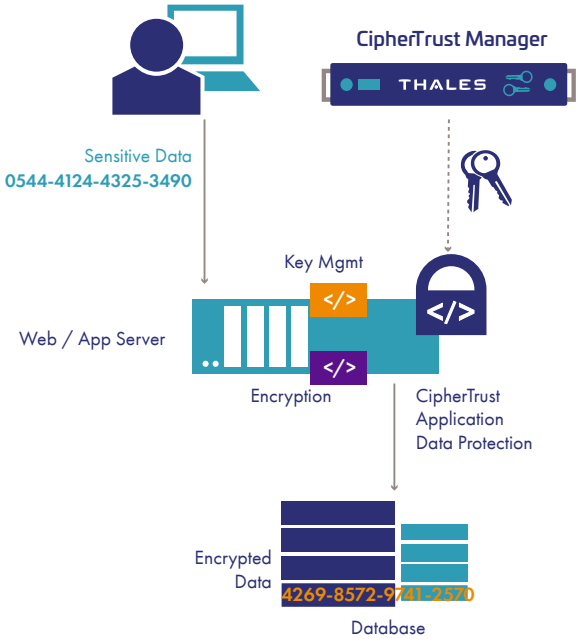
Developer-Friendly APIs for Data Protection

CipherTrust Application Data Protection offers developer-friendly software tools for encryption key management as well as application-level encryption of sensitive data. Protecting data at the application layer can provide the highest level of security, as it can take place immediately upon data creation or first processing and can remain encrypted regardless of its data life cycle state – during transfer, use, backup or copy. The solution is flexible enough to encrypt any type of data passing through an application. CipherTrust Application Data Protection can be deployed on premises or in private or public cloud infrastructure to secure data even when it is migrating from one environment to another, without any modifications to existing encryption or data processing policies.

Architectural Overview

CipherTrust Application Data Protection harmonizes interactions between developers and IT operations who share a common goal of data security. Developers enjoy language bindings appropriate to their projects. Operations can leverage choices among Crypto Service Providers that run on a wide range of operating systems. Further, the product includes many operational features that enhance performance and availability to ensure that security imposes a minimal to zero impact on business operations.

CipherTrust Application Data Protection operates with CipherTrust Manager, providing an architecture that centralizes encryption keys for applications. For enhanced separation of duties, CipherTrust Manager defines granular controls on both key users and key operational use.



One of several architectural choices for CipherTrust Application Data Protection

Developer-Friendly Data Protection APIs

Adding data protection to the software development process can be optimized by saving software engineers from having to master cryptography, deal with the challenge of finding high quality encryption keys as well as a safe store for them and mastering complex APIs without a comprehensive collection of sample code. CipherTrust Application Data Protection from Thales offers well-documented Crypto APIs with a wide range of language bindings, integrated with a range of industry-standard Crypto Service Providers that enable fast development of data protection for integration into mission-critical applications.

Development Libraries and APIs

Supported CipherTrust Application Data Protection language bindings and APIs includeinclude Java, C, and C# for .NET Core and .NET; XML Open Interface; RESTful APIs; KMIP client

Core Cryptographic Functions

Like a hardware security module (HSM) such as Thales Luna, CipherTrust Application Data Protection core cryptographic functions include, among many others including encrypt/decrypt, Sigh, Hash (SHA) and HMAC

The solution also offers support for versioned keys for encryption and decryption, signing and HMAC. Versioned keys can reduce the risk of data loss in the event of a compromised key.

Crypto Service Providers and Supported Operating Systems

In the following table, • indicates that a CipherTrust Application Data Protection crypto service provider binary is available for the operating system.

Abbreviations key:

- CAPI = C (language) API
- CSP = Crypto Service Provider (Windows)
- CNG = Crypto Next Generation [Provider]
- JCE = Java Crypto Engine

	CAPI	PKCS#11	CSP/CNG	JCE
Linux	•	•		•
Windows Server	•	•	•	•
AIX	•	•		•
HP-UX				•
Solaris		•		•
MacOS	•			

Choosing where to encrypt

Crypto operations on the application server: For many uses cases, and, in particular for the most latency-sensitive workloads CipherTrust Application Data Protection libraries on the application server include all crypto functions. Keys are cached for use on the application server. Keys are encrypted when not in use and obfuscated in memory when in use.

Crypto operations retained on CipherTrust Manager: CipherTrust Application Data Protection offers the possibility of retaining all encryption keys on CipherTrust Manager and forwarding encryption and decryption requests there. Retaining keys on CipherTrust Manager offers the highest key security. To support performance and availability for crypto operations on CipherTrust Manager, CipherTrust Application Data Protection libraries on the application server offer the following tools:

- Connection pooling
- Single- and multi-tiered load balancing

Crypto Service Aggregation Point

Applications can also choose to make RESTful API crypto requests to the CipherTrust Application Data Protection Web Services. This Web Services option can perform crypto operations locally or act as a centralized forwarder to CipherTrust Manager. Web Services option offers the same key protections for local operations as CipherTrust Application Data Protection libraries.

Rich Crypto Ecosystem

CipherTrust Application Data Protection has integrations for Microsoft SQL Server Always Encrypted, Microsoft Online Certificate Status Protocol (OCSP), Hashi Vault, HortonWorks, Apache HTTP and NGINX Servers, Lieberman ERPM, and many others.

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.

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