cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Protection Gateway

Transparently protect PII and sensitive data so that random people cannot see the data in the chain. CipherTrust Data Protection Gateway (DPG) protects the data at the earliest possible point, allowing the data to travel securely through the solution to its destination. Every single prying eye sees only the encrypted data. Only authorized people or applications can access the clear text.

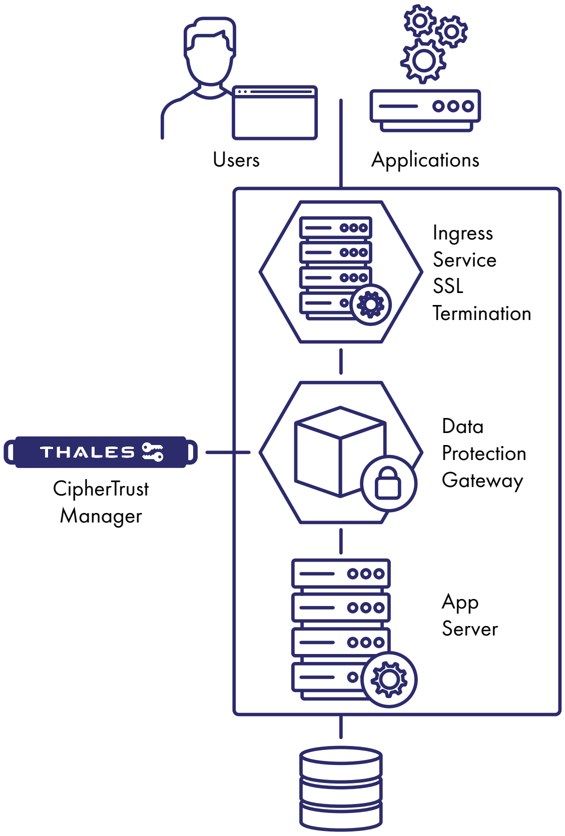
For many new and evolving applications, the DevOps team may face a challenge: protect data for web services-based applications without having access to the application and database or data store.

Deployment architectures such as containers and cloud-scalability solutions (e.g., Kubernetes, Helm) demand data protection solutions that integrate seamlessly and easily.

To meet these challenges, DPG offers transparent data protection to any RESTful web service or microservice leveraging REST APIs.

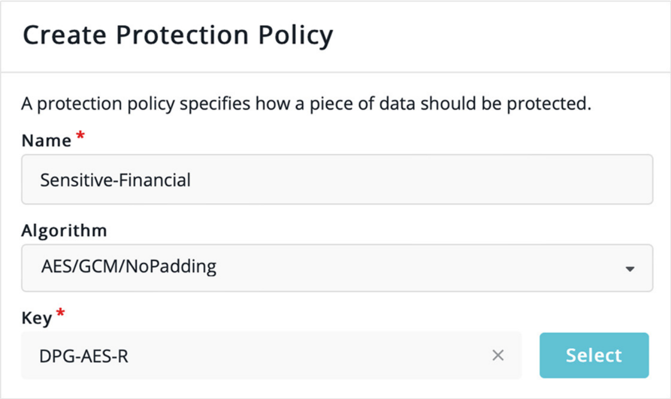
DPG is deployed inline between the client and web service and transparently protects sensitive data inline without modifying legacy or cloud native applications. DPG interprets RESTful data and performs protection operations based on policies defined centrally in the Thales CipherTrust Manager, operating seamlessly with other pod-supporting services.

Architectural Overview



Protection Methods

We enable the data security admin to define a protection policy selecting from an ever-growing list of encryption algorithms across the AES, DES and FPE families.



Create Protection Policy

A protection policy specifies how a piece of data should be protected.

Name *: Sensitive-Financial

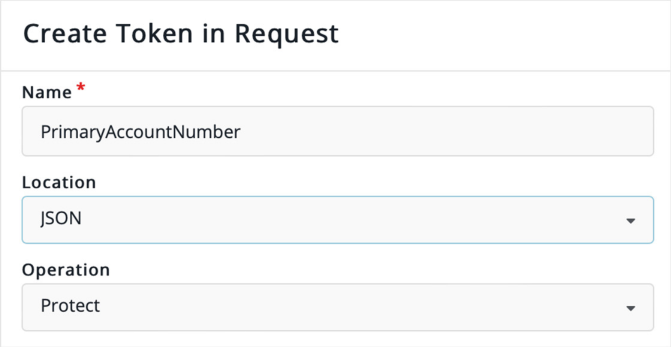
Algorithm: AES/GCM/NoPadding

Key *: DPG-AES-R

Creating a Protection Policy

Protecting Sensitive Data In REST

Selecting which fields to protect is fast and easy. Field selection, and protection and/or access policy, are configured centrally on CipherTrust Manager, delivering full separation of duties.



Create Token in Request

Name *: PrimaryAccountNumber

Location: JSON

Operation: Protect

Configuring a REST field for protection

Cloud-Ready and Cloud-Scale

CipherTrust Data Protection Gateway is deployed as a container and is fully compatible with Kubernetes orchestration systems such as Helm, Ansible and Terraform, and, of course, Kubernetes horizontal scaling. DPG can be deployed as a standalone container for legacy production deployments in addition to being used in development and testing use cases.

Thales Application-Layer Protection

DPG is one of several application-layer data protection offerings from Thales. CipherTrust Application Data Protection offers data protection from within applications with assist from developers. CipherTrust Database Protection offers transparent, column-level data protection for a wide range of databases. CipherTrust Batch Data Transformation offers high-performance encryption, tokenization and static data masking for databases and structured files.

CipherTrust Data Security Platform

DPG is part of the CipherTrust Data Security Platform, which unifies data discovery, classification, data protection, and unprecedented granular access controls, all with centralized key management. This simplifies data security operations, accelerates time to compliance, secures cloud migrations and reduces risk across your business. You can rely on the Thales CipherTrust Data Security Platform to help you discover, protect and control your organization's sensitive data, wherever the data resides.

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.