

Product Brief

CipherTrust Application Data Protection

cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Application Data Protection (CADP) is a performant SDK that protects data in applications/services when the data is In Use, In Transit and At Rest.

Gain field-level encryption, tokenization, data generalization, data masking or redaction without needing to know anything about cryptography. We moved data protection details out of code to protect your data, your sanity and your product roadmap. Only insert method calls once per piece of sensitive data — no matter how many times:

- **NIST declares a cipher to be at risk**
- **Keys need to be rotated**
- **Parameters need to be updated**

You keep months of Developer time and Security gains the ability to close vulnerability gaps in less than a minute.

Just as you use different keys for different columns in your database, you use different ciphers for different types of data. Learning and applying the rules of cryptography is time-consuming and you have more exciting projects to work on.

Organizations tell us traditional encryption, tokenization, data generalization, data masking and redaction solutions require their Developers (Devs) to handle fire drills when ciphers, keys or parameters need to change—taking Devs away from roadmap and/or innovative topics for a minimum of two months each and every time an update is needed for ciphers, keys or parameters.

Their Devs get pulled into projects that are a minimum of two calendar months because the Devs have to change source code, and DBAs/Devs have to migrate current data to the new ciphers/keys/parameters. After all of the changes are submitted, all of the code must be tested and re-tested until it passes all tests. The Devs are required to become cryptographers and change source code for every individual piece of sensitive data in every database column multiplied by every service protecting data. As a result, organizations report that they typically dedicate resources to revenue generating projects and delay their data protection updates for two years, resulting in a weakened security posture, increases in failed audits and more security breaches.

To sustain your compliance and your capacity per sprint, we reduced Dev involvement and removed their need to become cryptographers. We abstracted away the cryptography with simplified APIs and centrally-managed policies, limiting a Dev's involvement to the initial coding.

Devs insert Protect and Reveal method calls (or ProtectBulk/RevealBulk for bulk transactions) that reference policies centrally-managed in CipherTrust Manager, without needing to learn or apply cryptography (encryption, tokenization, data generalization).

Data Security Admins manage the policies, entering ciphers, keys or parameters. They update data protection in real time, making a selection from a dropdown menu in the GUI or by REST API. Vulnerability gaps are reduced from months to less than a minute. Since there are no changes to code, no Dev, DBA or Test involvement is required for the updated ciphers/keys/parameters.

Benefits

Developers Focus on Development

- Devs increase their capacity by using simplified APIs to write the initial code. Inserting Protect and Reveal method calls, Devs do not have to learn, apply and test cryptography (encryption, tokenization, data generalization)
- Devs do not have to be involved in updating security within their code when ciphers, keys or parameters need to be changed
- Human error decreases due to fewer changes to source code for the initial setup, no changes to source code for updates, and subject matter experts managing the data protection

Security Experts Manage Security

- Data Security Admins can perform updates without taking Devs off of other projects
- Data Security Admins can define access policies describing how people see data, including data masking and redaction
- Vulnerability gaps for sensitive data can be closed in minutes after discovery – instead of requiring months or years of Dev and testing time
- Configured on CipherTrust Manager (CM) through REST API or GUI
- Visibility on a single pane of glass shows where protection is deployed

Continuous Compliance

- Compliance teams can easily demonstrate compliance without involving Devs – the audit will be more complete, accurate and faster. Includes tracking of all data access for easy integration with SIEM tools
- Separation of Duties aligns with compliance regulations

Crypto Agility

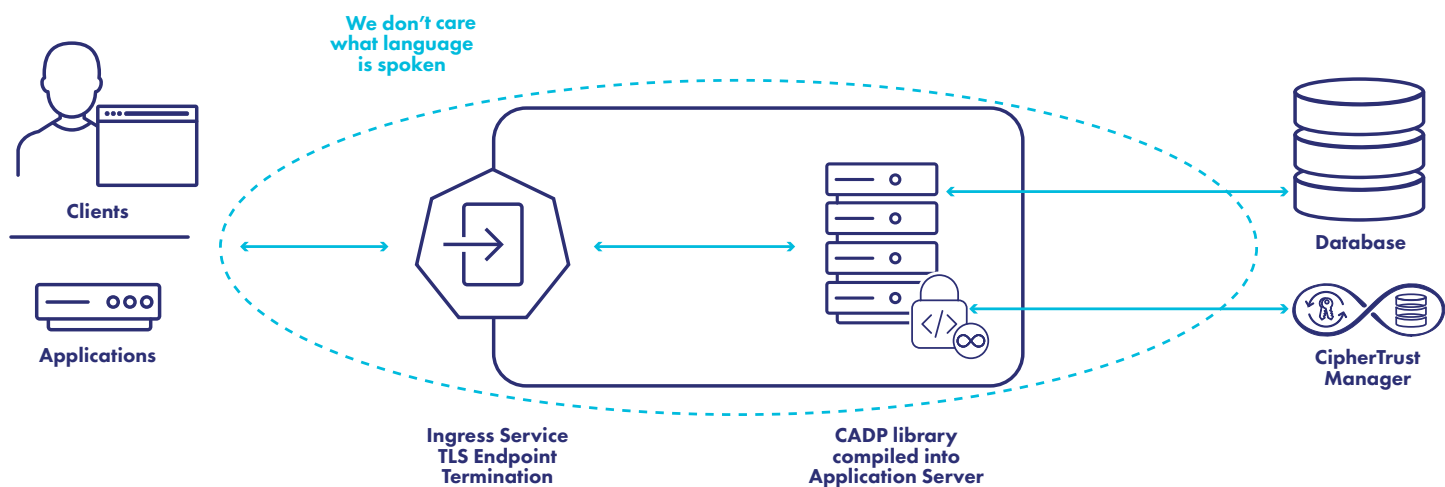
CADP supports crypto agility for data protection due to the convergence of three design elements:

- Centrally-managed Protection and Access Policies
- Developer-friendly APIs (Protect/Reveal)
- Separation of duties

Crypto agility enables Data Security Admins to change ciphers, keys and parameters in real time.


Architectural Overview

CADP is a library compiled into your application/service and can be scaled up to provide high availability and performance.



Protection Methods

We enable the Data Security Admin to define a protection policy by selecting from an ever-growing list of NIST-sanctioned algorithms.

 EDIT PROTECTION POLICY (VERSION 1)

Name*

alpha-external

Algorithm*

FPE/FF3

Key*

AES-256

×

Select

Character Set*

Alphanumeric

×

Select

Access Policy*

plaintext-and-masked

×

Select

Masking Format

Select a Masking Format

×

Select

Tweak Algorithm ⓘ

SHA256

Tweak*

tweakvalueforapplicationhr

The Access Policies can be automated for onboarding/offboarding.

Cloud-Ready and Cloud-Scale

CADP enables efficient resource management across multiple instances. CADP is offered as a library in language-native forms for: Java, C/C++ and .NET Core.

Thales Field-Level Data Protection

CADP is one of several centrally-managed Thales data protection offerings. CipherTrust RESTful Data Protection (CRDP) is a RESTful service that offers field-level data protection. CipherTrust Data Protection Gateway (DPG) offers transparent field-level data protection to any RESTful web service or microservice leveraging REST APIs.

CipherTrust Database Protection (CDP) offers transparent, column-level data protection for a wide range of databases. CipherTrust Batch Data Transformation (BDT) offers high-performance encryption and tokenization for databases and structured files.

All centrally-managed Connectors support Static Data Masking, Dynamic Data Masking and Redaction.

CipherTrust Data Security Platform

CADP is part of the CipherTrust Data Security Platform (CDSP), which unifies data discovery, classification and data protection with unprecedented granular access controls and centralized key management. Protecting your sensitive data with CDSP decreases time to compliance, simplifies data security operations, 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.

ESG Statement

The Thales CipherTrust Application Data Protection (CADP) software development kit equips the application with information to know when to scale up or down, in alignment with Thales' ESG (environmental, social, and governance) commitment to a greener, safer world.

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.