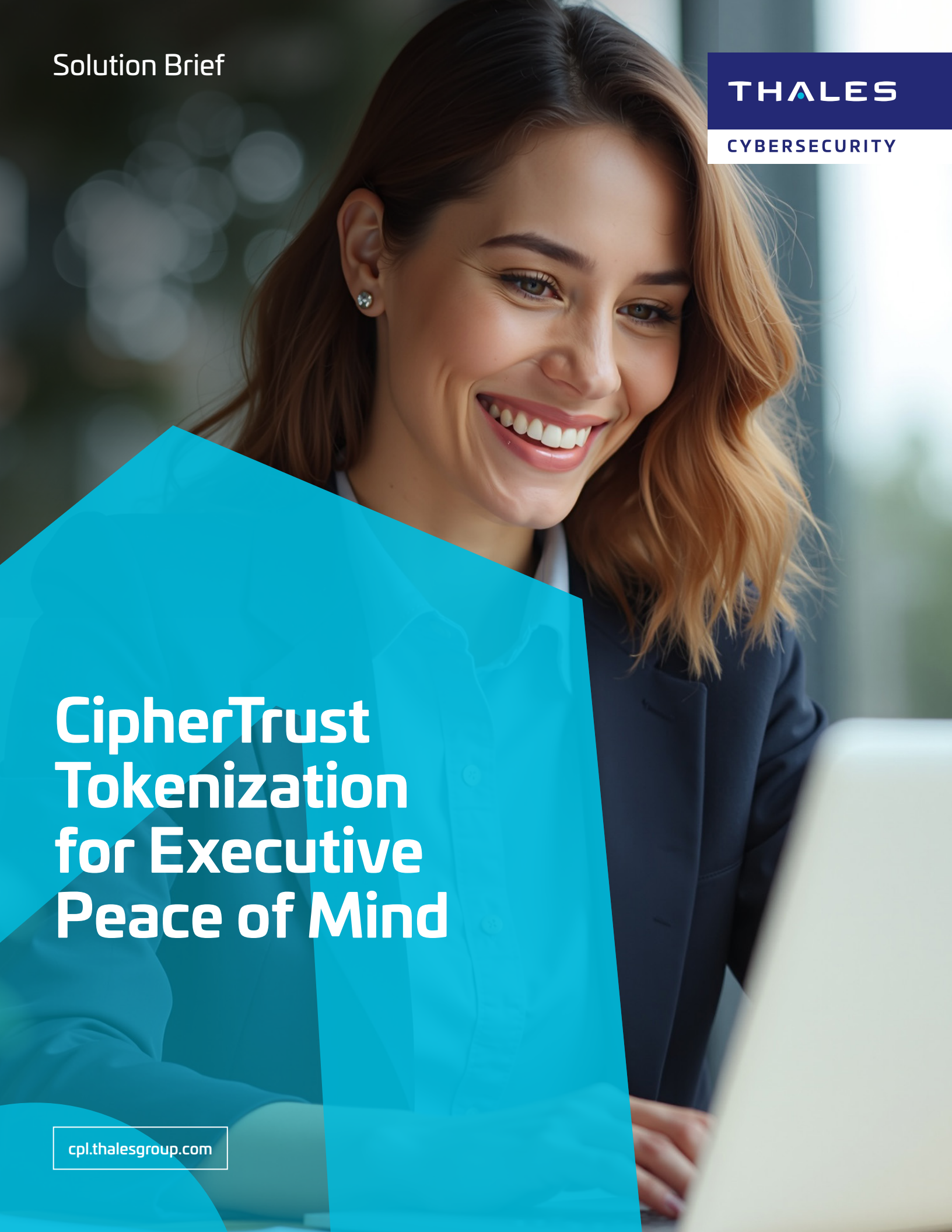
Solution Brief

THALES
CYBERSECURITY



CipherTrust Tokenization for Executive Peace of Mind

cpl.thalesgroup.com

THALES

CYBERSECURITY

When you need:

- **Compliance for security regulations such as PCI DSS 4.x**
- **Data secured before it enters AI workflows**
- **Ciphertext that looks like your data**
- **Reduced audit scope and burden, proof you have done due diligence**

The Challenge

Executives today are under increasing pressure to protect sensitive customer data. Data breaches can result in financial penalties, public disclosure, and even personal liability. Regulations like PCI DSS 4.0, HIPAA, and GDPR demand strong safeguards for personal data—but achieving compliance without hindering operations is difficult.

Data protection solutions often exist in silos. Developers are burdened with crypto implementation. Policy enforcement is inconsistent and the audit trail is fragmented.

How Thales Can Help

Thales provides Tokenization as part of a unified Data Security Platform that supports Tokenization, Encryption, Data Masking and Redaction so that you have the right data protection for every type of data you have—regardless of where it resides; in an application or a database, on premises or in the cloud.

CipherTrust Tokenization provides both Vaulted and Vaultless Tokenization solutions enabling you to:

- Protect customer data whether it is in applications or databases
- Replace sensitive values with format-preserving tokens
- Choose vaulted or vaultless models to fit your systems
- Centralize control of policies, keys and audit trails

Both Vaulted and Vaultless options integrate with CipherTrust Manager and a FIPS 140-3 Level 3 HSM, helping you prove due diligence and reduce scope.

CipherTrust Tokenization Solutions

CipherTrust Vaulted Tokenization is available with:

- CipherTrust Vaulted Tokenization (CT-V) - offers tokenization where the token is not mathematically related to the actual data to protect data via RESTful services, SOAP web services, Java SDKs and .Net SDKs within a customer's environment. Supports Oracle, Microsoft SQL Server, MySQL and Informix databases as its vault.

In contrast to vaulted tokenization, CipherTrust Vaultless Tokenization, does not store any sensitive user data, thereby reducing your potential attack surface and risk.

CipherTrust Vaultless Tokenization solutions include:

- CipherTrust Batch Data Transformation (BDT) - offers high-performance tokenization and encryption for databases and structured files [File to File, File to DB, DB to File, DB to DB]
- CipherTrust Application Data Protection Software Development Kit (CADP SDK) - offers tokenization and encryption for field-level data protection as a simple-to-integrate library for developers [Java SDK]
- CipherTrust RESTful Data Protection RESTful API (CRDP RESTful API) - offers tokenization and encryption for field-level data protection as a RESTful service [RESTful WebService]
- CipherTrust Data Protection Gateway (DPG) - offers tokenization and encryption for transparent field-level data protection to any RESTful web service or microservice leveraging REST APIs [REST API]

BDT, CADP SDK, CRDP RESTful API and DPG support Static Data Masking and Redaction. CADP SDK, CRDP RESTful API and DPG additionally support Dynamic Data Masking.

Thales helps you secure sensitive data across any system without operational complexity. And it gives you the ability to demonstrate accountability when it matters most.

Thales Solution Benefits

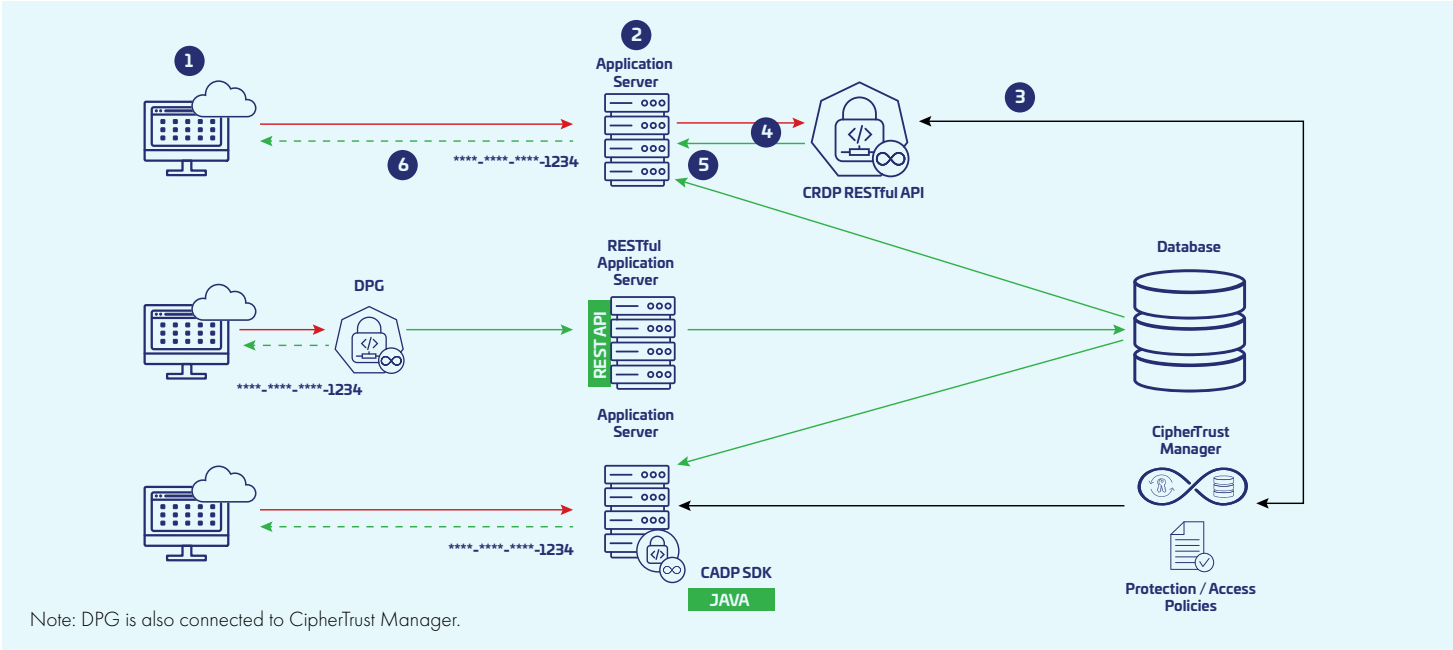
- Reduce PCI DSS compliance scope and associated audit burden
- Protect PII, PHI, and PCI data even if systems are breached
- Avoid liability by proving data was protected and access was controlled
- Combine Tokenization with Data Masking and Redaction to deliver end-to-end control
- Simplify deployment and enable innovation in cloud and analytics environments without increasing risk
- Tokenize data at rest, in motion, and in use

Core Use Cases

- Format-preserving Tokenization for applications and databases
- Vaulted or Vaultless protection for data in cloud, hybrid, or on-prem environments
- Tokenization, Encryption, Data Masking and Redaction on one platform

Tokenizing incoming data at the Application Layer

To provide consistent security and compliance across an organization without disrupting existing systems, CipherTrust Tokenization solutions enable an organization to tokenize with a solution that aligns with their deployment requirements (RESTful API/ API Gateway/ Java SDK) and detokenize with a solution that aligns with downstream applications (RESTful API/ API Gateway/ Java SDK).



Note: DPG is also connected to CipherTrust Manager.

Steps 1 - 6 illustrate the flow of data coming into an organization at the application layer, being tokenized, processed, and returned to the user with the first 12 numbers masked.

1. Using local or cloud-native applications, data enters organization using TLS.
2. The app server identifies which data is sensitive and calls the Connector associated with the application (RESTful API or Java SDK).
3. The Connector communicates with CipherTrust Manager to access the Protection and Access policies applicable to the customer.
4. The Connector protects the data according to the Protection Policy and returns the token to the App Server.
5. The app ingests the tokenized data and can use it to access related data in the database regardless of which app collected the data.
6. If the application needs to return data to the client, the app server will send sensitive data to the tokenization Connector to be revealed as plaintext, masked, tokenized or redacted based on their Access Policy. This diagram shows the sensitive data returned to the user with the first 12 numbers masked.

Conclusion

Thales Tokenization solutions reduce executive exposure by removing sensitive customer data from high-risk systems. It simplifies compliance and deployment, lowers audit costs, and strengthens your ability to respond confidently to regulators, customers, and the board.

About The CipherTrust Data Security Platform

The award-winning CipherTrust Data Security Platform is an integrated set of data-centric solutions that remove complexity from data security, accelerate time to compliance, and secure cloud migrations. Thales is proud to have been recognized as an Overall Leader in the KuppingerCole Leadership Compass on Data Security Platforms as well as a Strong Performer in the Forrester Wave and to be featured in Gartner's Market Guide to Data Security Platforms.

The CipherTrust Platform unifies data discovery, classification, data protection, and centralized management for keys and secrets into a single platform. This results in fewer resources dedicated to security operations, ubiquitous compliance controls, and significantly reduced risk across your business.

About Thales

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

cpl.thalesgroup.com

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us