THALES
Building a future we can all trust

CipherTrust Tokenization for SAP ERP Solutions
Integrating Data Protection to Facilitate Data Privacy Compliance

Key Benefits

- Secure SAP ERP data without changing your architecture or source code
- Field-level security protects private data before it is written to databases
- Data is protected before it is written to the database, simplifying database access controls
- Protect your sensitive data (PII, PCI, etc) in the cloud from privileged user risk
- Secure development environments and remain compliant by using tokenized production data
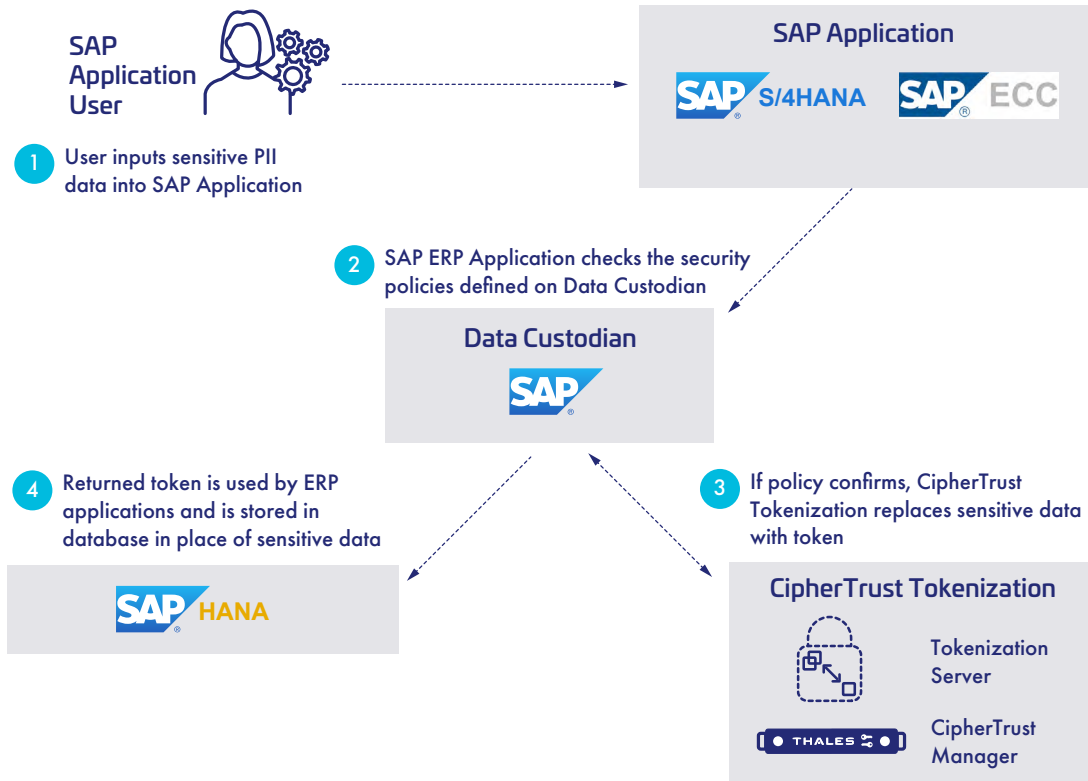
The Business Challenge

Modern enterprises today are defined by applications. Every aspect of a business's identity is defined by how its many different applications access, analyze, utilize, and share data. From HR to Finance to Engineering, the typical business day comprises hundreds of different applications operating together with SAP's ERP offerings portfolio often at the heart. SAP's goal of turning business connections into a worldwide community will only further intertwine the way applications will work together both within an organization and across corporate and geographic boundaries. The trending migration toward S/4HANA in the public cloud means that the perimeter of where sensitive data comes from and goes to has greatly expanded beyond the walls of the main corporate data center.

This reality poses new challenges to data management, protection, and sovereignty. How can you enable the flow of this data, within a company and to and from the public cloud, while still maintaining control? How do you migrate HR functions to the cloud while still protecting employee privacy? Can you enable a developer's access to a database without exposing PII? Is it possible to orchestrate sensitive data across a growing array of disparate functions and still meet regulatory and compliance requirements?

In addition, data breaches are an ever-increasing threat to data security.

Arguably, the ultimate strength of an organization's security protections is preventing breaches. Respondents reported breaches at a relatively high rate, with 56% globally identifying a security breach at some point. Out of these, 41% said they experienced a breach in the last 12 months

SAP Data Custodian & Thales CipherTrust Portfolio

SAP Application User

SAP Application

SAP S/4HANA   SAP ECC

1 User inputs sensitive PII data into SAP Application

2 SAP ERP Application checks the security policies defined on Data Custodian

Data Custodian

SAP

4 Returned token is used by ERP applications and is stored in database in place of sensitive data

SAP HANA

3 If policy confirms, CipherTrust Tokenization replaces sensitive data with token

CipherTrust Tokenization

Tokenization Server

THALES

CipherTrust Manager

The Solution

Thales and SAP have established a co-innovation partnership to provide an integrated data protection solution for SAP's ERP applications. Thales CipherTrust Tokenization now secures SAP S/4HANA and ECC 6.0 data via the SAP Data Custodian.

The sooner an organization can secure its data, the better. Tokenizing data at the application level replaces sensitive data with randomized values – optionally also of the same length and format – as soon as it is created. In place of sensitive data, databases will store tokens. Since these tokens have no inherent value, databases aren't storing sensitive information which makes them less of a data security risk and outside of the scope of many regulatory mandates.

Via the SAP Data Custodian, SAP customers can choose to tokenize specific fields and assign access policies that determine which users have access to sensitive data. Specific functions such as HR, Finance, and Legal may all have access to the same application, but have permissions to see different application fields. Any field that isn't authorized will show token values in place of real data.

Key Features and Benefits

- Schrems II alignment by masking protected data from CSPs, outsourced contractors, developers, and internal privileged access users
- Go live with sensitive data in production deployments within days rather than in months

- Access controls ensure only authorized users or applications can view tokenized data
- Thales Luna HSMs available to provide root-of-trust key protection to help attain FIPS 140-2 regulatory requirements

In Summary

SAP ERP solutions provide the heartbeat of today's enterprise across many corporate functions. The sensitive information these applications hold frequently requires protection. Given the criticality of SAP deployments, the optimal solution to secure SAP data needs to overcome the challenges of privacy and compliance, without stifling new software development. CipherTrust Tokenization delivers on the need.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com