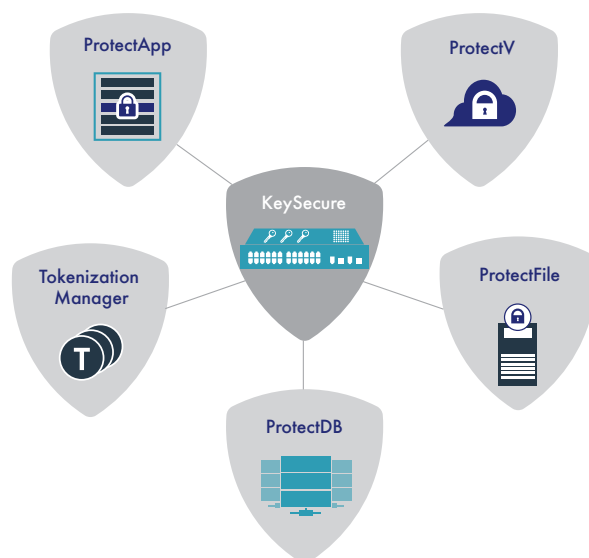**THALES**

Ensure the Right Solution for your RSA Data Protection Manager (DPM) Migration

Thales offers the following one-for-one replacements for the RSA EoL / EoPS DPM, BSAFE, and tokenization products. In addition to these proven, alternatives, we also offer a variety of solutions for both data at rest and in motion. Regardless of the environment where you store your valuable data, whether it is on-premises, in the cloud (public, private or hybrid), or virtually, Thales ensures ease of use, lower total cost of ownership, and the ability to meet compliance needs with Thales KeySecure and data protection products. Don't settle for re-packaged solutions that are not purpose built for your specific use cases.

High-Level Feature Comparison Matrix

Feature	RSA	Thales	Other
Centralized Key Management	Yes	Yes	Yes
Application-Level API Encryption	Yes	Yes	Yes
Application-Level Tokenization	Yes	Yes	Yes
File/Folder Level Encryption	No	Yes	Yes
Column-level Database Encryption	No	Yes	No
Full-Disk Virtual Machine Encryption	No	Yes	Yes

Key Management Feature Comparison

RSA DPM ----------> Thales KeySecure (Hardware or Virtual)		
Feature	**RSA DPM**	**Thales KeySecure**
Single, vendor-agnostic platform for multiple encryption types and appliances supporting Gemalto and third-party solutions	No	Yes
1.2 KMIP support for PCI-DSS compliance in 2017	No	Yes
FIPS certification	Yes	Yes
Active Directory and LDAP integration for ease of use	No	Yes
Column-level database encryption	No	Yes
Full-disk virtual machine encryption	No	Yes

In addition to offering the same functionality as RSA DPM, such as full lifecycle key support, automated operations, separation of duties, key sharing, and auditing and logging, SafeNet KeySecure also offers the following added benefits:

- **Over 45 field-tested and documented KMIP product integrations** spanning backup, storage, archive, applications (commercial-off-the-shelf or in-house), database, and cloud encryption gateway solutions
- Manage cryptographic modules and storage devices from different vendors within a **single solution**
- **Certified KMS for NetApp and Dell Storage**, plus, expand your storage integrations with EMC, Nutanix, HPE, IBM, HDS, and more
- **FIPS 140-2 Levels 1 and 3 certifications**
- **Infield Software Updates:** ensure easy installation of new features, core software updates, and security patches, or run older appliances in cluster with new appliances
- **Virtual key manager interoperability with Hardware Security Modules (HSM):** Thales is the only company to offer added security through Thales Luna Network HSMs, or Amazon CloudHSM
- **Remote encryption:** offload cryptographic services to a token
- **Easy use case expansion:** through the Thales Data Protection portolio of products for encrypting databases, files, virtual machines, and applications, as well as the largest ecosystem of KMIP and 3rd party product integrations, including storage
- **Virtual appliance support** for VMware and Amazon Web Services Marketplace including Bring your Own License (BYOL)
- **Truly own your keys and data** when stored in a hosted cloud service provider environment
- **Manage and store your keys** in the deployment model that best fits your architecture:
  - Flexible key management on-premises or in the cloud
  - Strengthen key management in the cloud with a hardware root of trust
  - Leverage one or multiple cloud service providers, and your cloud management company of choice, such as Rackspace or AWS
- Cluster between **multiple cloud vendors**
- **Scalability** through clustering of 10 or more appliances
- **Cloud-agnostic** encryption portfolio allows securely moving sensitive data to the cloud
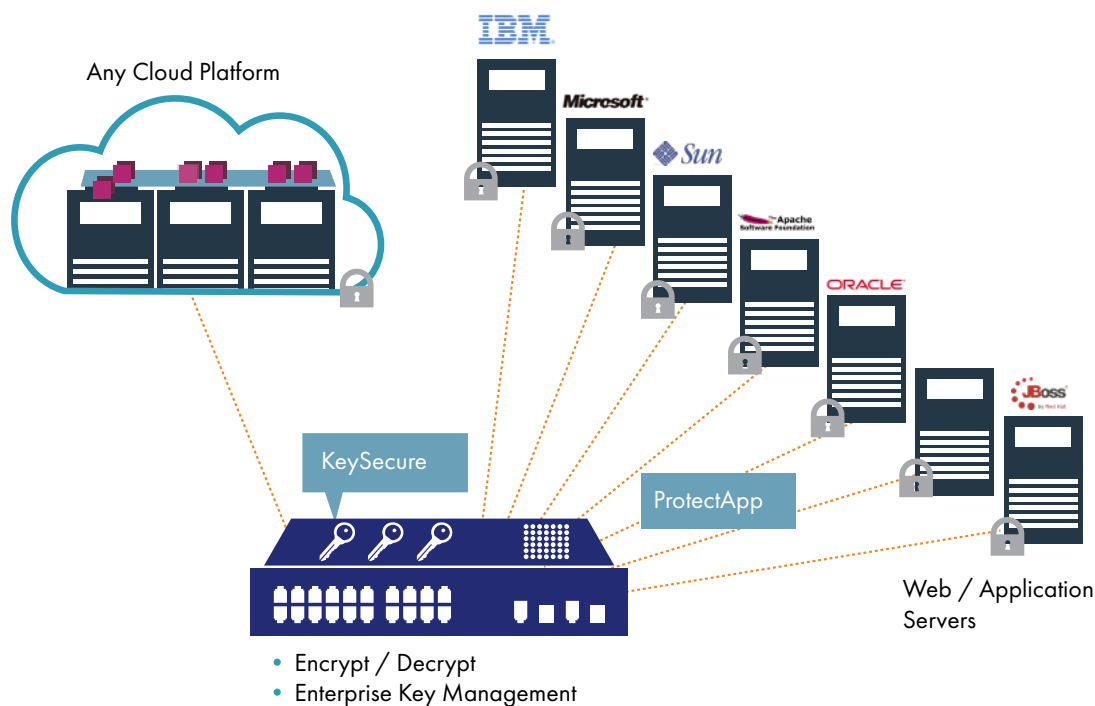
Application-level API Encryption Feature Comparison

RSA BSAFE ----------> Thales ProtectApp

Feature	RSA DPM	Thales KeySecure
Batching APIs	Yes	Yes
Certificate interfaces	Yes	Yes
Key management interfaces	Yes	Yes
Transparent key rotation	Yes	Yes
Transparent data re-keying	Yes	Yes
Local key caching	Yes	Yes
Mainframe integration	Yes	Yes
Application-Level encryption	Yes	Yes
Format Preserving Encryption (FPE)	No	Yes
Broad standard and interface support including web services (REST and SOAP)	No	Yes
Transparent database encryption	No	Yes
C/C++, C#, Java, .Net for key management	Yes	Yes
Secure key management	Yes	Yes

Encrypt application data and keep it secure across its entire lifecycle – no matter where it is transferred, backed up, or copied with ProtectApp. Apply transparent and efficient encryption to all types of sensitive application-level data across on-premises, virtual, public cloud, and hybrid environments.

ProtectApp benefits include:

- **Transparent encryption for data at rest,** meeting compliance mandates, and ensuring granular access controls through:
  - Protecting data residing in files, databases (file- and column-level granularity), and the full disk, with encryption
  - Transparent native database encryption (TDE)
  - Group permissions for encryption, decryption, export
  - Time controls that restrict encryption operations to a specified time period (e.g. 8am-5pm Mon-Fri)
  - Rate restrictions to perform a specified number of operations per hour or per day
- **Broad standard and interface support,** including web services (REST and SOAP)
- **Easy deployment and management** with customizable sample applications, including built-in key rotation and data re-keying
- Built-in **health checking** and **multi-tier load balancing**
- Comprehensive **auditing and logging capabilities** tracking access to encrypted data and keys
- **Bulk encryption and Format Preserving Encryption** (FPE)
- **Large ecosystem of 3rd party integrations** including AWS, Azure, IBM SoftLayer, Google, IBM, NetApp, Dell, EMC, Chef, Ciphercloud, and SkyHigh

Any Cloud Platform

IBM
Microsoft
Sun
Apache Software Foundation
ORACLE
JBoss by Red Hat

KeySecure

ProtectApp

Web / Application Servers

- Encrypt / Decrypt
- Enterprise Key Management

Integrates with KeySecure to:

- Improve protection through centralized administration of application encryption policies and keys
- Offload cryptographic processing to SafeNet KeySecure for improved performance

Tokenization Feature Comparison

RSA DPM and Token Client ---> Tokenization		
Feature	**RSA DPM and Token Client**	**Thales Tokenization**
Numeric and alphanumeric data	Yes	Yes
Built-in and custom token formats	Yes	Yes
LUHN check support	No	Yes
Horizontal and vertical scalability	Yes	Yes
.NET and Java support	No	Yes
Web Service REST / SOAP API	Yes	Yes

Apply transparent and secure application-level tokenization to structured sensitive data across onpremises, virtual, public cloud, and hybrid cloud environments with SafeNet Tokenization:

- **Protect high value information in databases** by replacing it with a surrogate value, a "token," that preserves the length and format of the data
- **No changes necessary** to database tables, file layouts or application changes for systems that don't require the original data
- Take systems leveraging tokenization **out of scope for compliance audits**, such as PCI DSS
- **Granular access controls** to ensure only authorized users or applications can view protected tokens and data
- **Unlimited data type support** enables tokenization of primary account numbers (PAN), as well as other data types (PCI, PII, PHI, etc.) in any environment including payment systems and big data
- **Fast and easy deployment** with web services (SOAP and REST/JSON), as well as the ability to leverage bulk tokenization and batch APIs
- Built-in, automated **key rotation and data re-keying**
- **Track user access** to tokens and protected data with comprehensive logging and auditing capabilities

Integrates with Thales KeySecure to provide:

- Single, centralized interface for logging, auditing, and reporting access to protected data, keys, and tokens
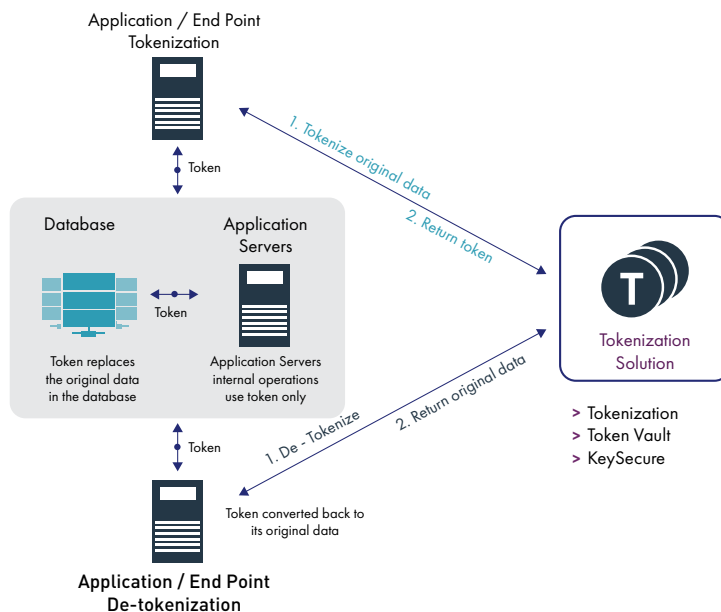
Let us help

Thales helps enterprises of all sizes to define an RSA DPM migration strategy and helping to implement the solution that best suits their needs.

Alleviate your migration frustrations with Thales KeySecure, which will manage your existing keys from third-party solutions, while offering a full portfolio of flexible encryption options for applications, tokenization, databases, virtual machines, and files that work onpremises, in traditional data centers, and virtualized public or private-clouds.

We understand that key management is not easy – but we make it simple for you. Our Professional Services and 24/7 Support teams are here to help with your specific use case, plan next steps, and define your migration strategy. KeySecure, together with the Thales data protection portfolio and ecosystem of partners, offers a proven solution to hundreds of customers worldwide. Count on us to protect your highvalue data and encryption keys, manage risk, and ensure compliance regardless of your environment.

Visit our website Thalesgroup.com for more information. Let us help – you won't be disappointed.

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.

> thalesgroup.com <