thalescpl.com

THALES

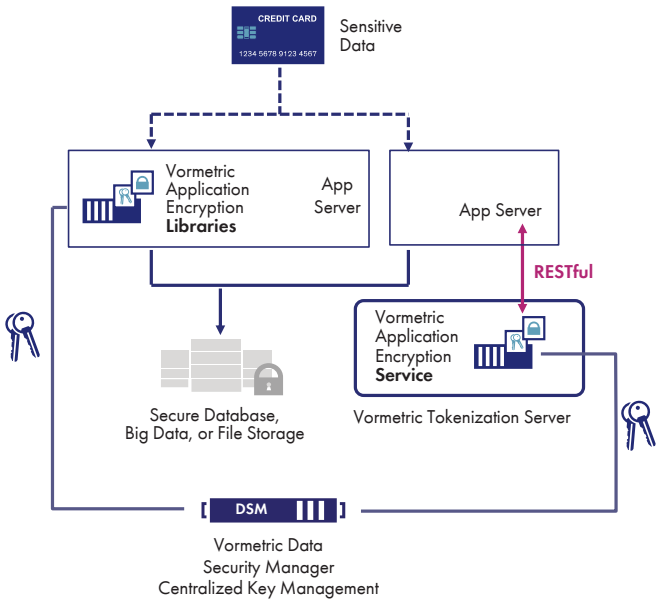
Vormetric Application Encryption from Thales

Facing the need for both IT agility and data protection, organizations often require customized security applications that include encryption for data in motion and at rest. The primary challenge for any encryption application is the safe generation, use and storage of both symmetric keys for data at rest and asymmetric key pairs for data in motion. Further, standards-based software development systems and languages are needed for development efficiency, along with secure development and runtime environments.

Vormetric Application Encryption delivers key management, signing, and encryption services enabling comprehensive protection of files, database fields and big data environments. The solution is FIPS 140-2 Level-1 certified, based on the PKCS#11 standard and includes a range of practical, use-case-based extensions to the standard. Vormetric Application Encryption eliminates the time, complexity, and risk of developing and implementing an in-house encryption and key management solution. Development options include a traditional software development kit for a wide range of languages and operating systems and a collection of RESTful APIs for the broadest platform support.

Fast creation of encryption and key management applications

- Streamline PKCS#11-standard application-level security with simple tools to add key management and encryption to application data flows
- Secure specific fields, protecting sensitive data before it is stored in database, big data or cloud environments
- Centralize key management to secure data from compromised database or cloud administrator, hackers, and subpoenas
- Software development your way: use either RESTful API's or a secure development and runtime environment with high-performing PKCS#11 libraries



Vormetric Application Encryption Customer Choice: Libraries or RESTful

Centralized key management

As a component of the Vormetric Data Security Platform, Vormetric Application Encryption utilizes the Vormetric Data Security Manager (DSM) for centralized key management, with up to FIPS 140-2 Level 3 key security. Centralized key and policy management for multiple solutions in the data security platform helps optimize IT resources with a single console and helps ensure security with comprehensive administrative role separation.

Programming architecture choices

Vormetric Application Encryption offers dual programming models, each with specific use cases and benefits.

- A software development kit (SDK) and corresponding runtime environment offers an extensive range of PKCS#11 calls. The SDK is stateful based on the PKCS#11 session model. Symmetric keys may be cached on the server running the SDK, offering high-performance encryption. The SDK and runtime environment is available for a wide range of Linux and Windows operating systems and programming language bindings
- RESTful APIs offer key management and encryption functions for multiplatform security application development and deployment

Symmetric key versioning

A symmetric key may be marked for automated key versioning. At an interval specified by either the DSM administrator or programmer, key material advances. Encrypted data is marked with the key version so that the correct key version material can be used for decryption. Key versioning enhances compliance with data protection mandates and is considered a key management best practice.

Microsoft Crypto Next Generation Support

Vormetric Application Encryption is a Key Services Provider (KSP) supporting a range of use cases for Microsoft Crypto Next Generation (CNG).

NIST key lifecycle states

Vormetric Application Encryption enables keys to be marked with NIST key states to help fulfill NIST-defined best practices for key management.

RSA Data Protection Manager compatibility

Vormetric Application Encryption offers rapid migration from the RSA Data Protection Manager (DPM) with support for three DPM data header structures and corresponding encryption algorithms.

Comprehensive security model

A clear separation of duties forms the security model base for both SDK and RESTful Vormetric Application Encryption, with multi-tenant DSM administration and key management. From there the security model differs between the SDK and RESTful API. The SDK offers up to four levels of security with two required: host registration, to enable a Vormetric Application Encryption host to communicate with the DSM, and host PIN which enables PKCS#11 operations. The RESTful API, working in concert with the Vormetric Tokenization Server, offers multiple levels of security: first, each RESTful call must be authenticated, which, on the Tokenization Server, can be based on AD/LDAP or client certificates. Then, upon login, the Tokenization server provides granular key access and usage controls. For more detailed information about the Vormetric Application Encryption security model, please see the Vormetric Application Encryption architecture white paper.

The Vormetric Data Security Platform

Vormetric Application Encryption is part of the Vormetric Data Security Platform, centered around the DSM and including a wide range of data security solutions including Vormetric Transparent Encryption, Vormetric Tokenization with Dynamic Data Masking, Vormetric Batch Data Transformation, and Vormetric Enterprise Key Management. The platform is cloud-friendly: you can deploy Vormetric Application Encryption-based applications and all other platform products on premises or in public or private cloud environments.

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.

> thalescpl.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com