DATASHEET

# Entrust Cryptographic Security Platform Key Management Vault for Application Security

## Protect Sensitive Data With Format-Preserving Encryption and Data Masking

### Overview

Ensuring data security is a critical necessity for modern-day businesses. Organizations can, and should, leverage various technologies to safeguard their sensitive information. Tokenization, first implemented in the early 2000s, is among the most widely adopted security techniques used today. It minimizes the amount of sensitive information that merchants and payment processors need to store and reduces the risk of data breaches.

Tokenization substitutes sensitive data like personally identifiable information (PII) and other confidential data elements with surrogate values, known as tokens. Tokens retain certain features of the original data, including character set and length.

Vaultless tokenization, provided by Entrust, doesn't require the use of a centralized vault or database to store the mapping between original data and its corresponding tokens. Offering a more secure approach, it removes a single point of failure while reducing the risk of a data breach. This method offers enhanced scalability and flexibility.

By leveraging the Entrust Cryptographic Security Platform Key Management Vault for Application Security, you can implement vaultless tokenization with dynamic data masking to safeguard your sensitive data.

### Key Features

- Pseudonymizes and masks sensitive data while maintaining data format
- RESTful API enables integration of multiple programming language environments and reduces development effort and lead
- Supports multiple character sets, including alphanumeric, numeric, numeric-Luhn, Chinese, Japanese, Korean, Thai, Vietnamese, and more
- Highly available, scalable, and stateless solution
- Supports separation of duties, least privilege, dual control, and multitenancy
- (Optional) Hardware key protection using FIPS 140 Level 3 certified HSMs
- (Optional) Automated compliance engine for PCI DSS, DISA STIG, NIST 800-130, HIPAA, and other standards

## Benefits

### Facilitates Compliance With PCI DSS and Other Standards

Tokenization can help organizations minimize the expenditure and resources necessary to adhere to internal security policies and regulatory requirements such as the Payment Card Industry Data Security Standard (PCI DSS) and the European Union's General Data Protection Regulation (GDPR). In the case of PCI DSS, tokenization simplifies compliance efforts by reducing the number of system components for which PCI DSS requirements apply.

### Highly Scalable and Flexible Solution for Safeguarding Structured Data

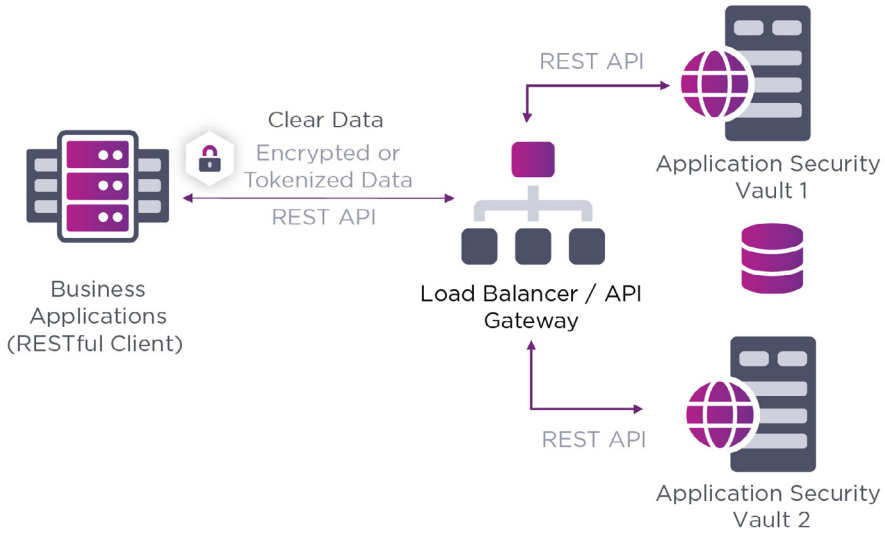
Traditional, vault-based tokenization methods are costly to scale and have capacity limitations, while vaultless tokenization, by eliminating the need for a centralized vault, provides a highly scalable, flexible, and powerful method for protecting both structured and semi-structured data. Vaultless tokenization generates tokens that retain important data attributes such as type, format, value, and length that can be processed by applications in their tokenized form but easily reversed when required for authorized users.

Minimize the impact on existing applications. Format-preserving tokenization makes it easier to integrate into existing applications since it does not require changes to the application's data storage, transmission, or processing logic.

Furthermore, Entrust Cryptographic Security Platform Key Management Vault for Application Security provides user-friendly REST APIs that allow seamless integration with existing applications, making it easy and straightforward for application developers to implement tokenization and dynamic data masking. With this approach, developers can avoid the need to manually establish identity management or implement access control policies, reducing the burden of implementation and enabling more efficient development processes.

## How It Works

The Entrust platform Key Management Vault for Application Security provides a RESTful web service to tokenize and detokenize data. The solution is simple to deploy, manage, and maintain, and provides performance and scalability to support an unlimited number of servers.






ENTRUST
SECURING A WORLD IN MOTION

Data masking policies allow you to set up how tokenized data is presented to different users based on their roles, allowing you to limit access to only authorized personnel while ensuring that necessary data remains visible for operational purposes.

## Technical Specifications

**Supported Tokenization Methods:**

- Format Preserving Encryption
- Partial tokenization
- Dynamic data masking

**Application Integration:**

- RESTful APIs

**Management and Monitoring:**

- Centralized management with Web UI and Rest API
- Syslog and Splunk integration

**Supported Hypervisors for Platform Key Management Vault**

- VMware ESXi 7.0 (HW version 17) and above
- Red Hat KVM 7.8 and above
- AWS, Azure, and GCP (latest Entrust version available in the marketplace)

**Deployment Media:**

- ISO, OVA (Open Virtual Appliance), AMI (Amazon Web Services Marketplace), or VHD (Microsoft Azure Marketplace)

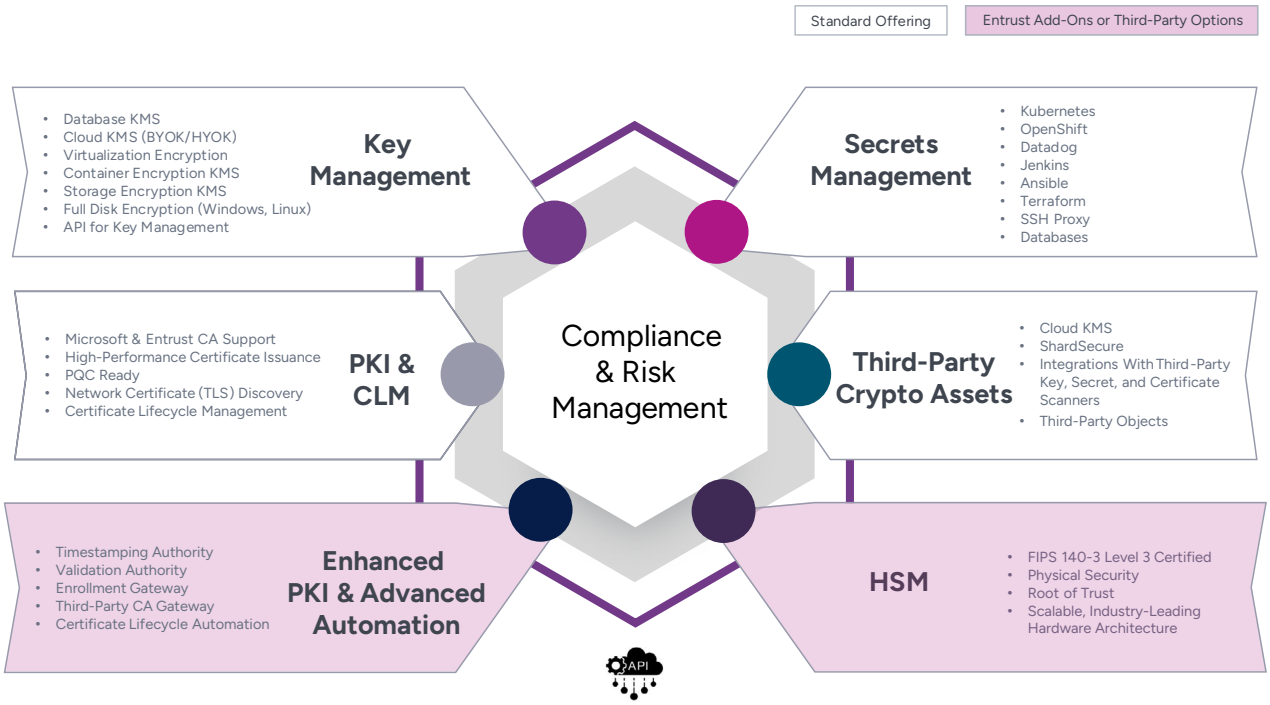
**Certification**

- FIPS 140 Level 3 compliance via Entrust nShield HSM on-premises or as a service

# Entrust Cryptographic Security Platform

The Entrust Cryptographic Security Platform provides a comprehensive solution for discovering and managing the lifecycles of certificates, cryptographic keys, secrets, tokens, libraries, protocols, and configurations.

By centralizing cryptographic asset management, it enhances security, helps ensure compliance, and streamlines operations, enabling seamless integration across both on-premises and cloud environments.






entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION