



## Tokenization Manager

### Reducing Regulatory Scope

**SOLUTION BRIEF**

#### Benefits

- Ensure PCI compliance and strengthen security - Format-preserving tokenization enables organizations to address PCI rules by securing cardholder data
- Reduced audit costs - Save time and money by restricting the number of entities that need to be audited
- Facilitate audit process - DataSecure complies with the National Institute of Standards and Technology (NIST) and has been granted FIPS 140-2 certification

Organizations that process payment card information consider complying with PCI DSS regulations a key business initiative. This has prompted them to search for methods to minimize the skyrocketing costs associated with PCI DSS compliance including reducing the regulatory audit scope.

Tokenization enables organizations to reduce regulatory scope by significantly reducing the number of entities that are subject to auditing. SafeNet Tokenization Manager replaces cardholder data with a token. The original cardholder data is stored and encrypted in one centralized location, and entities that store, process, or transmit the token are taken out of audit scope.

#### Reduce Regulatory Scope Using Tokenization

PCI DSS specifications define the regulatory scope for any system component that stores, processes, or transmits cardholder data. As organizations evolve and grow, more and more system components are added to the PCI DSS regulatory scope.

According to the PCI Security Standards Council, any system component that is in its regulatory scope should undergo an annual audit to ensure compliance. As the regulatory scope grows, not only does the organization experience data-blooming and an increased risk of exposure of sensitive data, there is also a substantial addition to the on-going annual audit fees and the total cost of compliance.

In order to reduce regulatory scope, the PCI Security Standards Council states that system components that do not store, process, or transmit Primary Account Numbers (PANs) are not included in the scope of the regulation.

Analysis and better understanding of the business processes involving storage, processing, and transmittal of cardholder data enable reduction in the regulatory scope to which an organization should adhere to, assist in reducing costs, and allow efficient investment of resources.

Organizations are continuously looking for additional ways to reduce regulatory scope—and tokenization offers an ideal solution. Tokenization takes sensitive data, such as PAN, and replaces it with surrogate random values, while the original data is stored in a single secure location. By replacing the PAN with a different, irreversible value, organizations reduce PCI DSS regulatory scope and limit the risks associated with data-blooming.

## Technical Specifications

### Supported Sensitive Data Formats

- Numeric data:  
1234567890123456
- Dash-delimited data: 123-45-6789
- Space delimited data: 123 45 6789

### Supported Token Formats

- Random digits
- Sequential digits
- First two last four
- Fixed twenty last four
- Fixed nineteen
- First six
- Last four
- Custom token format (user specified leading or trailing mask)Luhn check support available

### Supported Web and Application Servers

- Oracle Weblogic, IBM Websphere, , Apache, , JBoss, and J2EE 1.4 Web services platforms

### Supported Databases for Token Vault

- Oracle and Microsoft SQL Server

## Example of Reducing Regulatory Scope Using Tokenization

Figure 1 illustrates a merchant system with a number of order entry systems (e.g., Web order entry application, phone order entry application, etc.), along with several order fulfillment applications and databases that store the relevant information. In the illustration, cardholder data is protected by the use of a database encryption solution, ensuring a robust and efficient process. While a database encryption solution meets PCI DSS compliance audit regulations, merchants are still looking for ways to reduce the regulatory scope.

Figure 2 illustrates how SafeNet End-to-End Tokenization reduces the regulatory scope of the same system architecture, with the order entry applications interfaced through Web APIs. The cardholder data is fed at the entry point and sent to the main order processing application, where a token is issued, replacing the cardholder data. The token is then used throughout the lifecycle of the sensitive data. The clear-text cardholder data, with its associated tokenized value, is stored in a secure Token Vault.

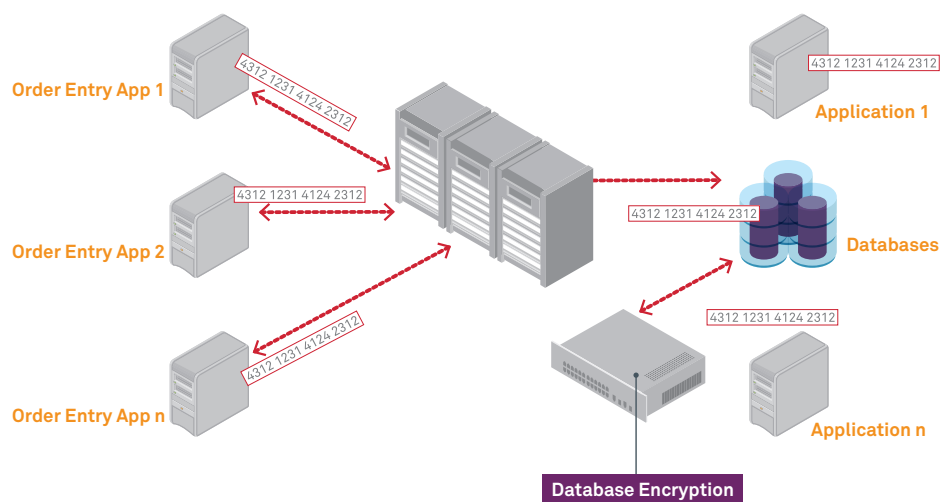


Figure 1: Merchant System Architecture. PCI DSS Compliant, with all Components in Scope

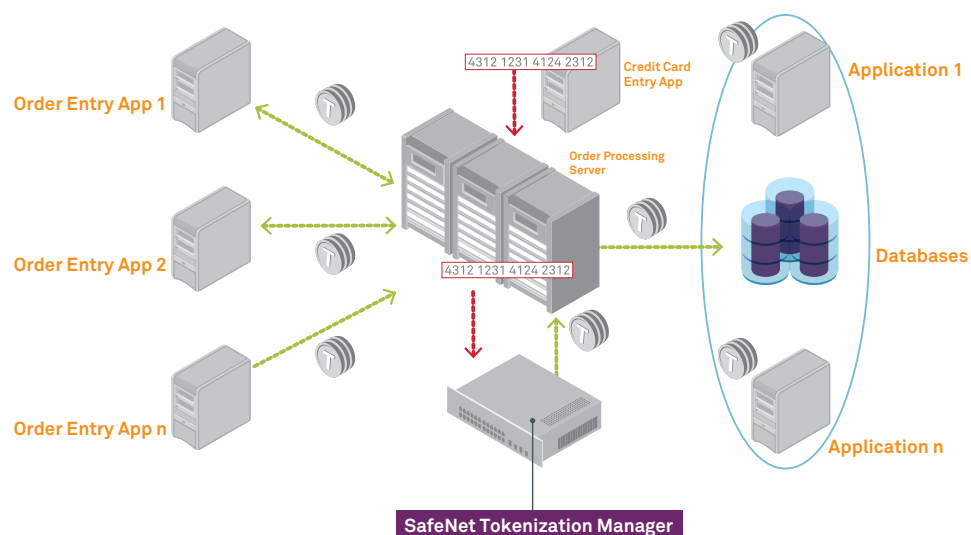


Figure 2: Same system with end-to-end tokenization

## SafeNet Solution

### End-to-End Tokenization

SafeNet Tokenization Manager receives the cardholder data right after its initial entry point, encrypts it, stores it in the Token Vault, and creates a token for it. From then on, entities that need to store, process or transmit the cardholder data, actually store, process, or transmit the token that was created for it, removing the entity from the PCI DSS audit scope.

SafeNet Tokenization Manager is an application running on top of the SafeNet DataSecure appliance. The solution provides a single, centralized interface for logging, auditing, and reporting access to protected data, keys, and tokens.

Once cardholder data is received by the Tokenization Manager, it is encrypted and a token is created for it. From entry point through applications to databases, the token is stored, processed, or transmitted throughout the organization, while the cardholder data is encrypted and its key is securely stored in the DataSecure appliance.

Although the Tokenization Manager and DataSecure eliminate the need to audit multiple systems within the organization, these two systems will always remain in the scope. However, the auditing process of DataSecure is significantly eased since it complies with the National Institute of Standards and Technology (NIST) and has been FIPS 140-2 validated.

### Clearing Entry Points out of Scope

The entry point of cardholder data will always remain in scope when using tokenization. A new feature of SafeNet Tokenization Manager enables organizations to remove the entry point systems from regulatory scope.

SafeNet Tokenization Manager adds an additional layer to the entry point that acts as a hub database between the entry point and the Tokenization Manager. When cardholder data is provided, it goes straight into the hub database and the entry point does not store, process, or transmit it.

For example, if there are multiple points of sale (PoS) and the cardholder data goes straight into the hub database, all of the PoS sites are taken out of scope and only a single system, the database hub, remains in scope. This enables organizations to even further reduce regulatory scope, helping to continuously minimize costs.

### Format Preserving Tokenization

The tokens are created using Format Preserving Tokenization (FPT), maintaining the length and format of the original data, yet masking the actual information, or some of it. SafeNet Tokenization Manager offers multiple options for FPT, all of them in accordance with PCI DSS requirements.

Format preserving tokenization minimizes the changes and adaptations that applications undergo when implementing a tokenization solution.

Every token that is issued, represents the cardholder data of a single, unique card. A hash key is issued and stored in the DataSecure appliance to ensure that each card receives the same token, no matter how often it is used, and that a specific token is issued only one time.

### De-Tokenization

Be it for forensic needs or others, in some cases, entities in the organization have to access the actual cardholder data. In order to de-tokenize a token, the system that stores the token will be connected to the Tokenization Manager and will be brought back into scope. These instances are quite rare yet they do occur. It is recommended that tokenization not be the only security measure and that additional security layers, such as authentication, be implemented when de-tokenizing cardholder data.

### Tokenization as a Service (TaaS)

Tokenization as a Service enables payment processors to offer tokenization services to their customers, helping them reduce regulatory scope. With Tokenization Manager and DataSecure, a payment processor can provide its customers with full encryption and tokenization services, taking all or most of the customers' systems out of scope.

Once cardholder data is received, it is transmitted to the Tokenization Manager, leaving only the entry point in scope. The entry point may remain in the customers' regulatory scope or may become the payment processor's regulatory responsibility.

### About SafeNet

Founded in 1983, SafeNet is a global leader in information security. SafeNet protects its customers' most valuable assets, including identities, transactions, communications, data, and software licensing, throughout the data lifecycle. More than 25,000 customers across both commercial enterprises and government agencies, and in over 100 countries, trust their information security needs to SafeNet.

**Contact Us:** For all office locations and contact information, please visit [www.safenet-inc.com](http://www.safenet-inc.com)

**Follow Us:** [www.safenet-inc.com/connected](http://www.safenet-inc.com/connected)

©2011 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. SB (EN)-07.13.11