

RSA SafeProxy™ Tokenization Services

Enhancing the protection of sensitive data with token-based data substitution

At a Glance

- Mitigates risk by substituting token values for the display and storage of sensitive data elements
- Provides the full cryptographic strength of an encryption-only solution
- Provides an effective compliance (PCI, PII, HIPPA) approach where clear-text storage is prohibited
- Reduces implementation impact (as compared to encryption) to applications and infrastructure
- Simplifies the operation of data protection controls within the infrastructure
- Leverages leading RSA® Key Manager technology, as part of the RSA SafeProxy™ architecture, for encryption and centralized key management across the enterprise
- Supports seamless key rotation without data loss

Organizations continue to look for ways to improve the security of their sensitive data while decreasing the impact on business operations. Encryption has been the de facto standard for data protection, but the changes required within applications can drive costs up and timelines out, jeopardizing efforts to meet regulatory deadlines and business opportunities.

An increasingly popular approach for the protection of sensitive data is the use of a token (or alias) as a substitution value for clear-text sensitive data elements. This means that instead of maintaining ciphertext and an associated key (ID) within the organization's data stores, a single token is stored and used as a pointer to the

encrypted value. A credit card number, for example, is replaced within the organization's storage environment by a token value generated in such a fashion that it cannot be cryptographically linked back to the original data element. A secure, cross reference table is established to allow authorized look-up of the original value, using the token as the index. Encryption tools and secure key management compliments this approach by protecting the original value within this environment

Effective Protection of Sensitive Data

The tokenization approach offers some significant benefits from the implementation and security perspective including:

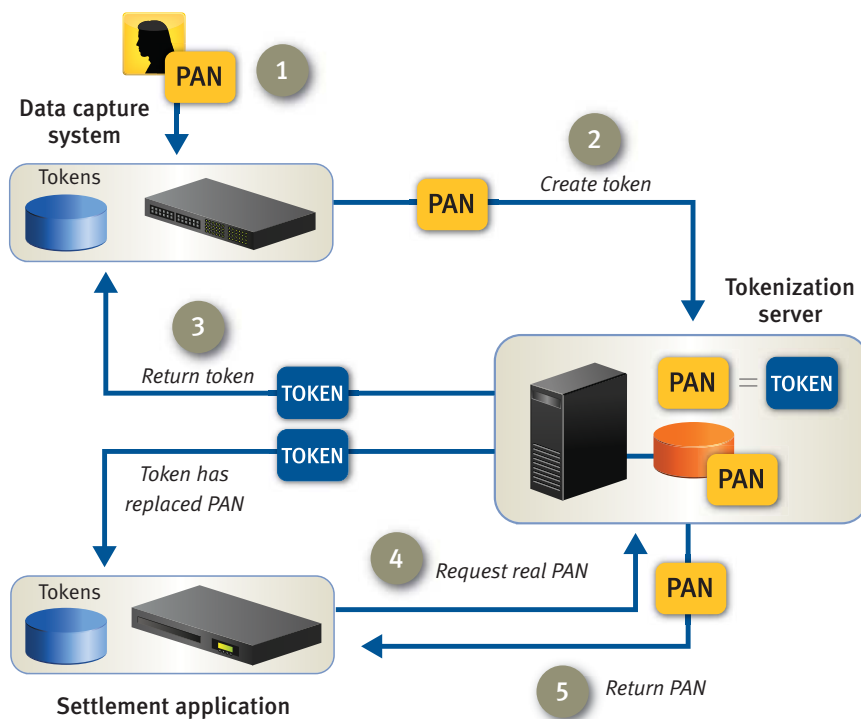
- Using a token allows applications to remain unchanged, whether it's a credit card number, Social Security number or any other sensitive data element. In addition, policy decisions regarding the extent to which the token reflects the source data (for example, mapping the final four digits of the credit card into the token) can be applied. These policy decisions can be enforced by the RSA SafeProxy tokenization server.
- Since the security of the token is based on cryptographically-strong random numbers (as opposed to encryption), policies and regulations related to encrypting sensitive data in the central repository can be managed independently of the token. For example, the key used for encrypting a credit card number can be rotated according to encryption policies specific to the card number without the risk of data loss, system downtime or needing to re-encrypt.

The RSA SafeProxy Architecture

RSA SafeProxy architecture is an innovative approach which integrates tokenization, encryption and key management to increase data security and reduce risk, simplify compliance, and reduce or eliminate system changes as well as application security or compliance audits.

As a result, the SafeProxy architecture has dramatic implications for services and solutions which address PCI, PHI and other requirements calling for increased data protection while, at the same time, delivering faster time to benefit and lower operational cost.





Tokenization Scenario

1. The full customer data, including the primary account number (PAN), is entered at the data capture system.
2. The PAN is sent in plain text to the tokenization server, where it is stored in the token database.
3. A token is returned to the data capture system and all of the customer data, with the token replacing the PAN, is sent to other systems, such as settlement applications.
4. If an authorized application needs the real PAN, it sends a request to the tokenization server.
5. The PAN is then returned to the authorized application.

The SafeProxy architecture applies RSA's leading encryption, key management and tokenization capabilities to provide the best solution for meeting complex enterprise requirements. Based upon proven RSA® Key Manager technology, RSA has designed and integrated tokenization services to offer a complete solution that:

- Accepts a piece of clear-text data
- Creates a cryptographically strong token that maps 1:1 to the data. The token has the same look and feel as the original data, maintains the same essential properties and returns consistent results across subsequent invocations.
- Securely stores the original data in a cipher-text representation
- Provides a mechanism to retrieve the clear-text value for any given token value
- Provides strong authentication, authorization, administration and audit controls for all sensitive operations
- In the event of a network disruption, enables data to be encrypted locally and, upon reconnection, tokenized using the encrypted data.

Service Benefits

RSA SafeProxy Tokenization Services with RSA Key Manager is currently deployed at several large organizations and has been proven to securely eliminate the storage and display of sensitive data in clear-text. It requires no change to existing application infrastructure and preserves database search performance. Leveraging RSA's leading key management technology helps it enable the centralized management of keys and cryptographic-quality token generation while maintaining separation of duties. The solution provides strong cross-platform support that allows organizations to leverage their current infrastructure, reduce implementation impact and simplify data protection controls.

The RSA SafeProxy architecture is supported by RSA Professional Services, offering globally recognized industry leadership and the experience gained from helping thousands of leading companies tackle their most difficult security challenges. RSA Professional Services works to identify and understand objectives and constraints for data protection, especially as it is related to near-term compliance objectives. RSA focuses on achieving a balance between strong data protection while simplifying controls to reduce the impact on users, applications and infrastructure.