

Tokenization Server with RSA® Key Manager

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

At a Glance

- Substitutes token values for the display and storage of sensitive data elements
- Provides the full cryptographic strength of an encryption-only solution
- Effective compliance (PCI, PII, HIPAA) approach where clear-text storage is prohibited
- Reduced implementation impact (as compared to encryption) to applications and infrastructure
- Simplifies the operation of data protection controls within the infrastructure
- Leverages RSA's leading Key Manager technology for encryption and centralized key management across the enterprise
- Supports key rotation without loss of data

Organizations continue to look for ways to improve the security of their sensitive data while decreasing the impact on their 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 plaintext sensitive data elements. This means that instead of maintaining cipher-text and an associated key (ID) within the organization's data stores, a single token is stored and used as a pointer to the

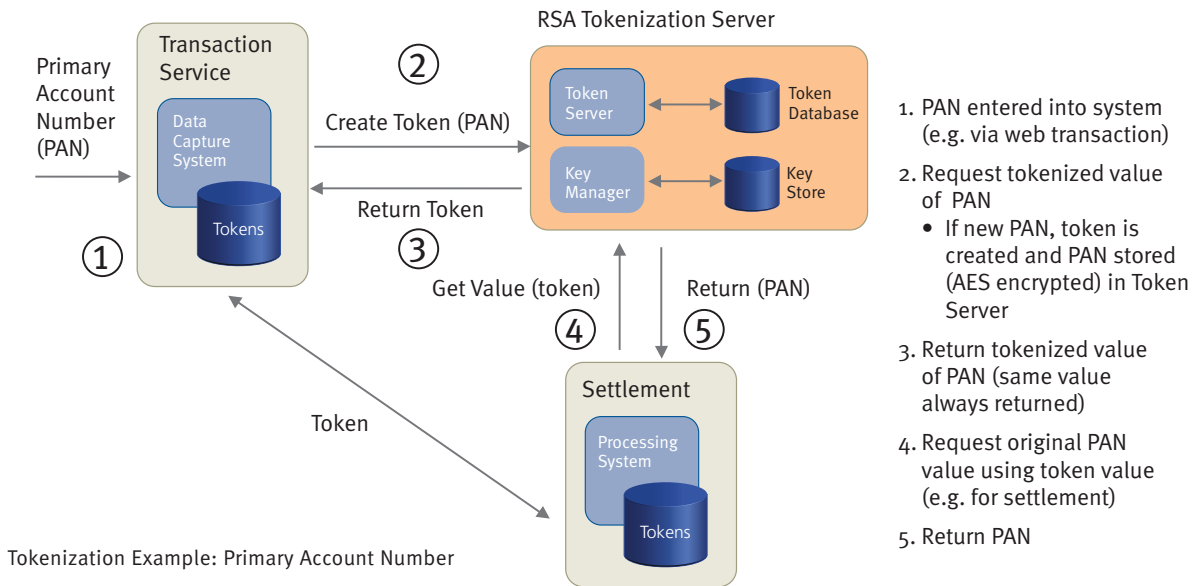
encrypted value. A credit card number, for example, is replaced within the organization's storage environment by a token value generated in such a way that it cannot be linked back to the original data element. A secure, cross-reference table is established to allow authorized look-up of the original value, using the token as the index. Encryption tools and secure key management complements 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 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 credit card number without the risk of data loss or need to re-encrypt.





Tokenization Example: Primary Account Number

Integrated Tokenization and Key Management

RSA Professional Services has significant depth and breadth of experience working with the majority of Fortune 100 companies and other large enterprise customers. RSA Professional Services works to identify and understand an organization’s objectives and constraints for data protection, especially as it is related to near-term compliance. RSA focuses on achieving a balance between strong data protection while simplifying controls to reduce the impact on users, applications and infrastructure.

RSA employs an architectural strategy which applies both encryption and token approaches to providing the best solution for meeting complex enterprise requirements. Based upon RSA’s proven Key Manager technology, RSA Professional Services has designed and integrated the tokenization server 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
- Enables data to be encrypted locally in the event of a network disruption and tokenized using the encrypted data upon reconnection

Service Benefits

RSA Professional Services offers recognized industry leadership and experience to help thousands of leading companies tackle their most difficult security challenges. The tokenization server 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. In leveraging RSA’s leading Key Management technology, it enables 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.