

ENCRYPTION SERVICES

Tokenization



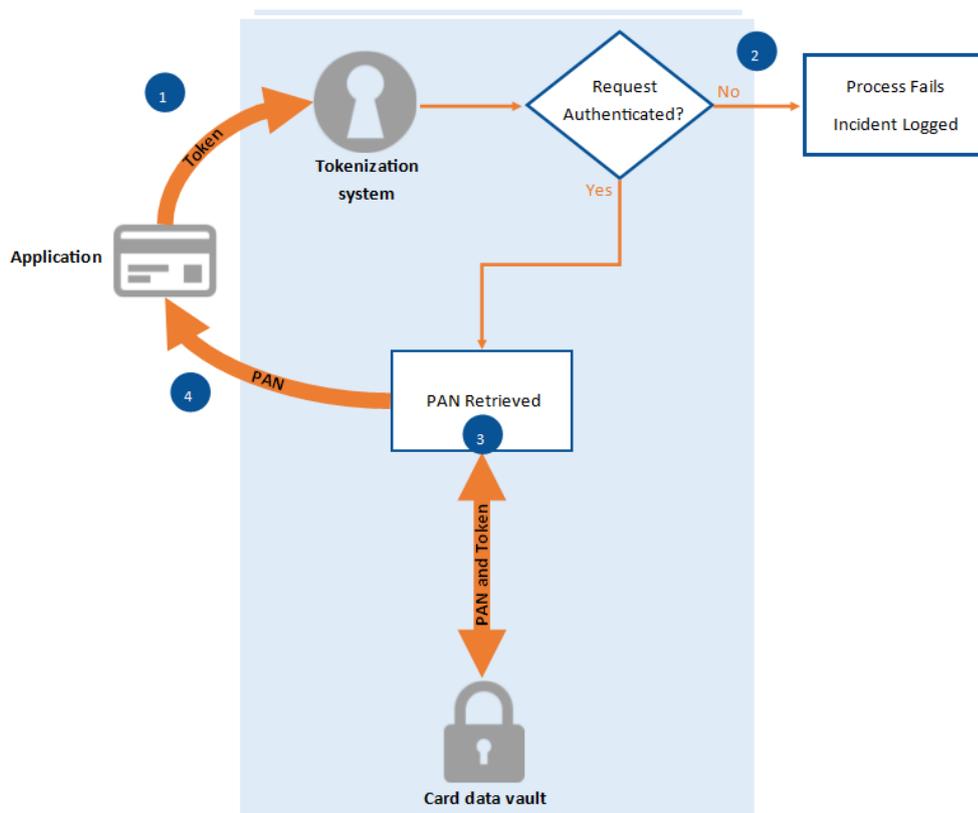
TOKENIZATION

An approach for the protection of sensitive data is the use of data substitution with a token as a replacement for a real data. In the process of tokenization, actual sensitive data is used for transactions and after that the sensitive data is sent to a centralised and highly secure server called a “vault” where it is stored securely.

This vastly reduces an organisation’s risk in the event of a data breach because the process eliminates sensitive data from an organisation’s environment after a transaction has been authorised. If token numbers are breached, they are meaningless to anyone who would attempt to use them because the tokens are simply random numbers. Additionally, using token numbers instead of real data in back-end business applications shrinks the organisation’s environment that is subject to PCI compliance requirements and audits. This reduction of PCI scope can save an organisation significant time and money.

“If token numbers are breached, they are meaningless to anyone who would attempt to use them.”

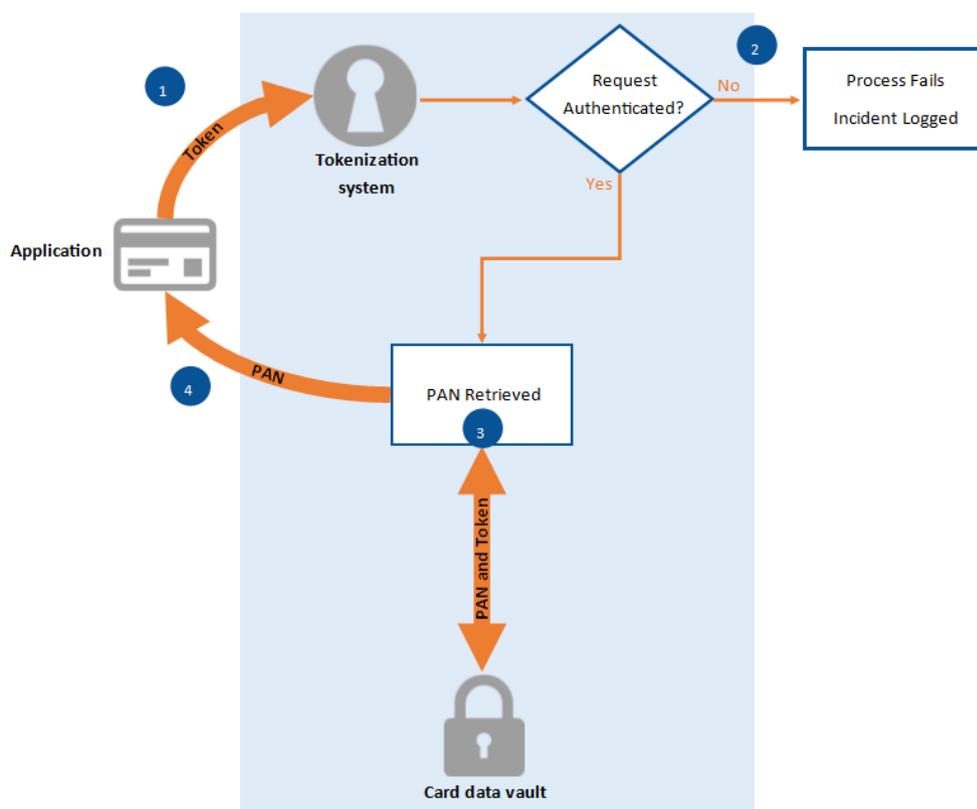
TOKENIZATION PROCESS



In the Tokenization Process in Tokenization Process figure

1. A requesting application passes a Primary Account Number (PAN), along with necessary authentication information, to a tokenization system.
2. The tokenization system verifies the authentication information presented by the requesting application. If this check fails, the tokenization process fails, and information is logged for monitoring. Otherwise, the process continues to Step 3.
3. The tokenization system generates—or retrieves if already exists—a token associated to the PAN and records both to the card data vault, following PCI DSS requirements for PAN storage.
4. The tokenization system returns the token generated or retrieved in Step 3 to the requesting application.

DE-TOKENIZATION PROCESS



In the Tokenization Process in De-tokenization process figure

1. The requesting application passes a token, along with necessary authentication information, to a tokenization system.
2. The tokenization system verifies the authentication information presented by the requesting application. If this check fails, the de-tokenization process fails, and information is logged for monitoring. Otherwise, the process continues to Step 3.
3. The tokenization system queries the card data vault for a record associated with the token, retrieves the PAN if found, and proceeds to Step 4. If no such token exists, the detokenization operation fails, and information is logged for monitoring.
4. The tokenization system returns the PAN value