PaymentsEd Forum

Common methods and types of tokenization

In-House Tokenization (Merchant Tokens)

Merchant tokens are created and managed by merchants themselves, replacing the cardholder data with a proprietary token, with the PAN data stored securely in an encrypted data vault, managed by the merchant.

Benefits: Provides the most control.

Drawbacks: Requires high security and compliance with standards like the PCI DSS.

Token Service Providers (TSPs)

Merchants can outsource tokenization to Third-Party Token Service Providers (TSPs) to create merchant tokens, support acquirer tokens, or assist with network tokens.

Benefits: Offers flexibility and uses the provider's security infrastructure.

Drawbacks: Invokes dependency on the TSP.

Acquirer-Based Tokenization (Acquirer Tokens)

Acquirer tokens are provided by the merchant's acquirer. Acquirers can offer their own unique tokens or enable network tokenization.

Benefits: Acquirers' robust infrastructure ensures smooth payment processing and reduced security requirements for storing PAN on-premise.

Drawbacks: Tokens are acquirer-specific and may be unusable if the merchant changes acquirers. Acquirers also may charge per transaction fees for token usage.

Network-Based Tokenization (Network Tokens)

Network tokens are created and managed by card networks (Visa, Mastercard, Discover, American Express, etc.), usable across different merchants.

Benefits: Widespread acceptance across different acquirers, improved authorization rates, reduced interchange, reduced security requirements, and added fraud protection.

Drawbacks: Relies on card network infrastructure and is not fully supported yet.

Hybrid Tokenization Approach

Combines multiple methods for optimal security, control, and operational efficiency. For example, a merchant may use in-house tokenization while also using network tokenization with the assistance of a TSP.

Benefits: Flexibility and the ability to leverage different methods' strengths.

Drawbacks: Implementation can be complex and managing multiple tokens could be challenging

Glossary of terms

Primary Account Number (PAN): Identifies a specific payment card, often referred to as a card number.
Card Holder Data (CHD): All information printed, processed, transmitted, or stored on a payment card in any form.
Tokenization: The process of replacing sensitive data, like the PAN, with a non-sensitive equivalent, called a token.
Token: A secure substitute for sensitive data, such as a PAN.
Single-Use Tokens: Tokens created for a single transaction. They lose their value once used.
Multi-Use Tokens: Tokens linked to a customer's payment information and reusable for multiple transactions.
Format Preserving Token: A method where the output, the token, retains the same format as the input, the PAN.
Non-Format Preserving Token: A method where the output data, the token, does not retain the same format as the input, the PAN.
Token Vault: A secure data repository for storing tokens and their associated original data values (like PAN, customer data, etc.).
Token Service Provider (TSP): An entity offering tokenization services to merchants or other service providers.
Device Primary Account Number (DPAN): Device-specific tokens created within digital wallets (ie. Apple Pay)
Merchant Primary Account Number (MPAN): Merchant-specific tokens created within digital wallets (replacing DPANs)
Customer-Initiated Transactions (CIT): These are purchases made directly by the customer. In the context of tokenization, a token is created during this transaction to secure the customer's card information. This token can later be used for Merchant-Initiated or Card on File (COF) Transactions.
Merchant-Initiated Transactions (MIT): These are COF transactions started by the merchant, such as recurring payments or subscription fees. In tokenization, a previously created token from a CIT is used to process the transaction safely, which requires a prior agreement between the customer and merchant.
Card Lifecycle Management: The process of managing a card's life from issuance to updates, expiry, or cancellation.
Payment Card Industry Data Security Standard (PCI DSS): Security standards ensuring all companies dealing with credit card information maintain a secure environment.