Payment Account Tokenization

Comprehensive software solution to protect ACH and real-time payments

Overview

Real-time payments (RTP) and direct debit (ACH) payments – where transactions are made using account credentials rather than payment cards – are seeing increasing levels of fraud. Payment Account Tokenization leverages a proven process in payment card tokenization to replace the valuable account credentials with a non-sensitive token with restricted usage. The tokens have the same format as the original numbers so that processing protocols are not changed, and the customer experience is unaffected. This process can significantly reduce the risk and impact of account-based fraud to support the development of a safe and secure instant payments framework.

Flexibility of payment account tokenization

Features

Tokenization
Reduce fraud by leveraging proven tokenization technology via non-intrusive modular installation.

Life cycle management
Link, suspend, (re)activate or unlink tokenized bank account numbers.

Domain controls
Limit token usage to a specific channel, merchant or spending limit or dates by applying a set of parameters.

ID & verification
Provide a specific token assurance level during the issuance of a token or later during its life cycle.

Cryptogram protection
Generate application cryptograms in advance of use and validate these during the transaction process.

Token vault
Manage a secure repository (secure database) that establishes, maintains and maps the payment token value to the sending/receiving account number.

Directory services
Publish or integrate directory services for account lookups using uniquely identifiable data, e.g. phone number, email, without exposing the credential.

Standard ISO 20022
Standard ISO 20022 interface used, embracing the universal financial industry message scheme, and proprietary standards can also be deployed if needed.

File-based and message-based tokenization and de-tokenization
These can be used for batch and individual transactions.

Non-disruptive integration
Implement standard member interfaces or embed tokenization transparently in the transaction flow.

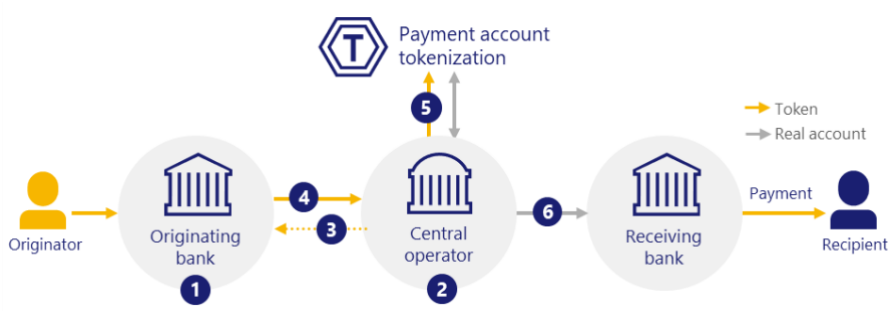
Customer service portal
Support authorized users with token life cycle management requests.

Token ID
A Visa Solution

How it works

Provisioning a token to an account

1. An originator initiates a payment and sends the transaction to the central operator as they would normally
2. The central operator identifies the transaction as non-tokenized and creates a token using Payment Account Tokenization
3. The token is sent back to the originating bank to replace the original account number with the token for future transactions



Using a token for an account-based payment

4. Once an originator initiates a payment, the originating bank sends the transaction along with the token to the central operator
5. Once received, the central operator identifies that the payment contains a token and detokenizes the transaction using Payment Account Tokenization
6. The central operator sends the account information to the receiving bank to debit the account

Direct debit (ACH) account payments contribute to a large majority of the total noncash payments value worldwide. The credentials associated with these accounts are stored in many different locations (including invoices, payrolls, ecommerce sites, mobile wallets and apps), making them potentially vulnerable for hacking. Also, as more countries adopt faster (or same-day) account-to-account payments, the timeframe for detecting and intercepting fraud is being drastically reduced, virtually eliminating the ability for financial institutions to implement manual checks on the validity of payments. Payment Account Tokenization reduces fraud while supporting a seamless integration for multiple use cases including push transactions between businesses, consumers and government.

Figure 1 description: There are two cases represented in the diagram. The first case represents the process for provisioning a token to an account. First, an originator initiates a payment with the originating bank and sends the transaction to the central operator. The central operator then identifies the transaction as non-tokenized and creates a token using Visa Payment Account Tokenization. After, the token is sent back to the originating bank to replace the original account number with the token for future transactions.

Figure 2 description: The second case represents the process for using a token for an account-based payment. Once an originator initiates a payment, the originating bank sends the transaction along with the token to the central operator. Once received, the central operator identifies that the payment contains a token and detokenizes the transaction using Payment Account Tokenization. The central operator then sends the account information to the receiving bank to debit the account.

Why tokenization?

Reduce the impact of data breaches
Sensitive account information is not stored, and stolen tokens cannot be used outside the authorized channels.

Transaction protection
Reduce risk of fraudsters using stolen account numbers to commit transactional fraud by substitution of account numbers in instructions.

No change in consumer behavior
Consumers and businesses send and accept payments without having to change their procedures.

Limit the scope of tokens with control parameters
Limit the channels, merchants, amounts or dates for use of specific tokens via domain controls.

No change in payment authorizations
Tokens route normally through the payment systems and networks.

Want to learn more?

For more information please click below to contact us

Learn more

Token ID
A Visa Solution

