Fact Sheet

Payment Account Tokenization

Enable swift and secure automated clearing house (ACH) and real-time payments (RTP)

Payment Account Tokenization (PAT) SaaS helps financial institutions to mitigate account-based fraud for real-time and ACH payments.

With Token ID's proven tokenization technologies, central operators, clearing houses and banks can help protect sensitive account data, proactively request tokens directly and benefit from automated in-network tokenization.

Potential benefits

Limit breach impact

Deter hacking and mitigate breach impact by storing tokens rather than sensitive account data.

Protect transactions

Avert fraudsters from using stolen account credentials to make payments.

Enable innovation

Create new, secure payment services and flows, such as eCommerce, mobile payments and P2P.

Increase control

Apply domain controls to limit tokens to specific times, channels, merchants and amounts.

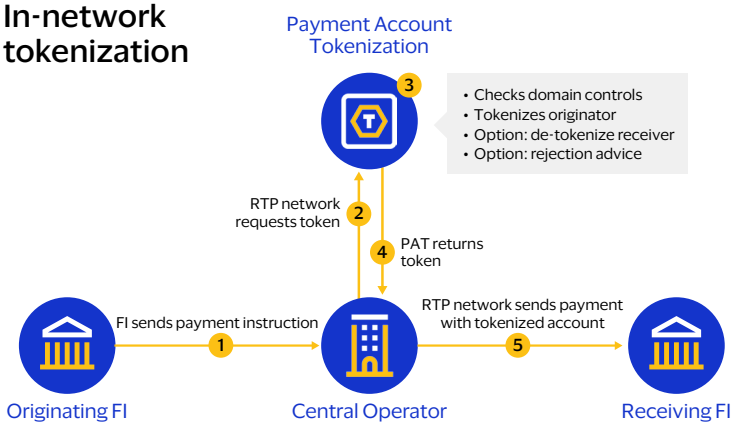
Maintain legacy flows

Route tokens through existing payment systems networks as normal.

How it works

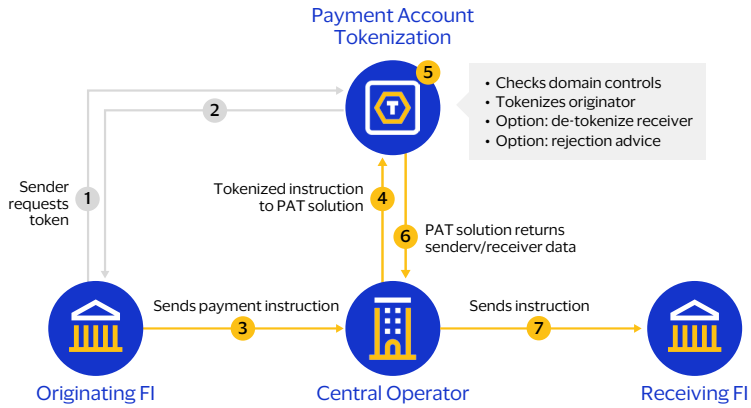
The below diagrams outline two ways that PAT can be implemented to combat fraud for real-time and ACH payments. In-network tokenization sees the central operator take ownership of tokenizing account credentials once a payment has been initiated. For direct tokenization, the originating bank tokenizes the account data and stores the token for use when a payment is initiated.

In-network tokenization



1. Originating financial institution sends payment to central operator
2. Central operator identifies sending account as 'to be tokenized' and requests token
3. PAT validates domain restrictions and optionally detokenizes the receiver
4. PAT returns payment with tokenized account
5. Central operator sends payment with tokenized account to receiving financial institution

Direct tokenization



1. Originating financial institution requests a token from PAT with additional constraints such as maximum value and counterparty restriction
2. PAT generates a token based on the request parameters and returns token to originating financial institution
3. Originating bank forwards the payment instruction, using the token receiver account
4. The central operator identifies tokenized transaction and forwards this to PAT
5. PAT validates domain restrictions and optionally detokenizes the receiver
6. PAT returns modified sender and receiver data to the central operator
7. Central operator constructs an instruction, evaluates advice and forwards message to receiving financial institution

Features

Lifecycle management

Quickly and easily suspend, (re)activate or unlink tokenized bank account numbers.

Domain controls

Enable token parameters that restrict usage to specific times, channels, merchants and spending limits.

Cryptogram protection

Generate application cryptograms in advance and validate these during the transaction process.

Seamless SaaS integration

Implement tokens without disruption of existing transaction flows.

Token vault

Manage a secure database that establishes, maintains and maps payment token value.

Learn more

For more information, contact your Visa Representative or click here to fill out our online enquiry form

Please note, all diagrams are presented for illustrative purposes only.

Token ID | A Visa Solution