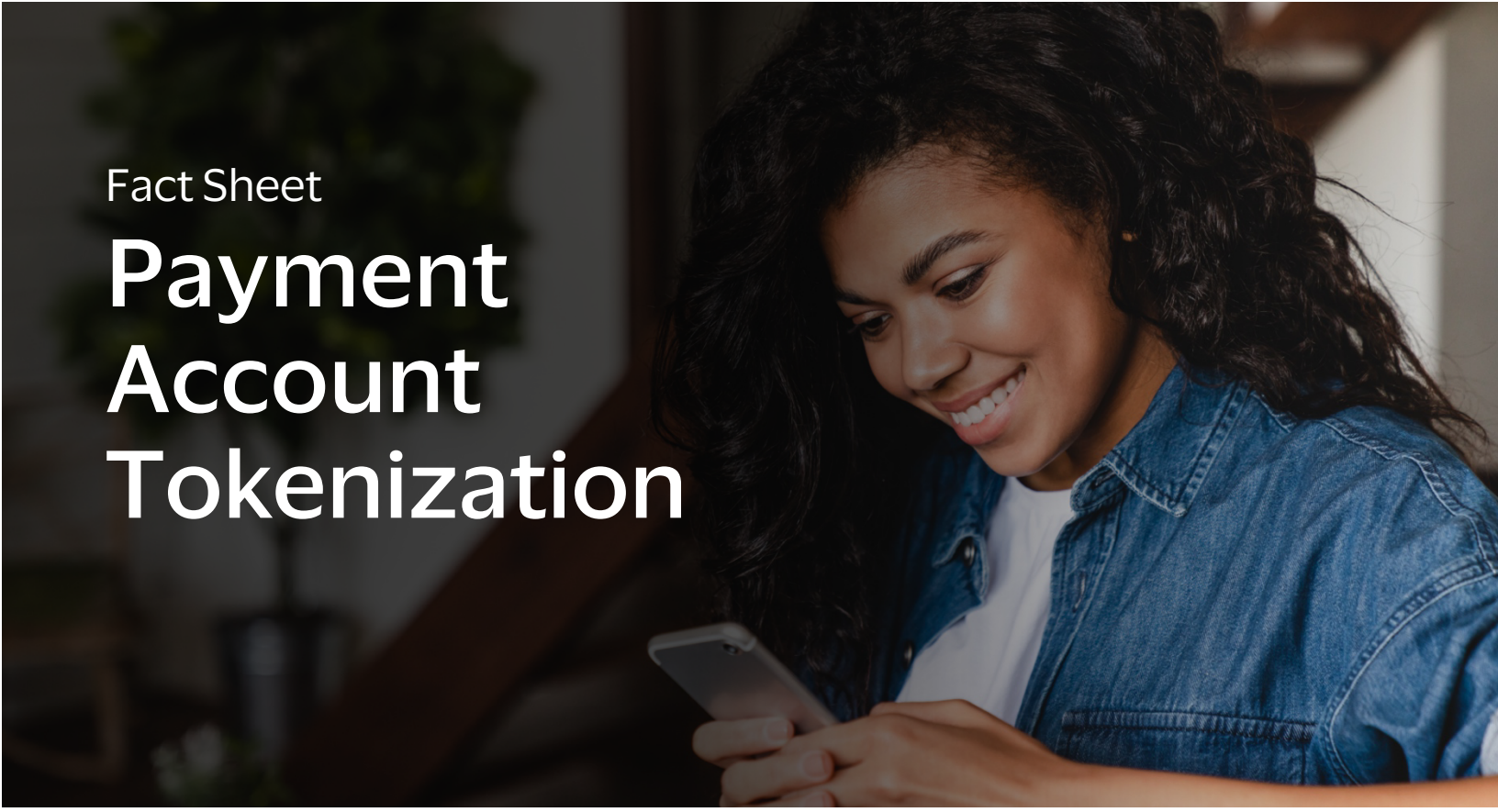


Fact Sheet

# Payment Account Tokenization

## Scale account-to-account payments with tokens designed to enhance security and control for seamless payment experiences

The rapid growth and evolution of fraud on faster payment networks is driving the need for new innovative solutions to keep the payments industry ahead of fraudsters' use of scams and artificial intelligence (AI).

With Token ID's proven Payment Account Tokenization (PAT), banks add token-level payment controls, manage risk exposure with token rules,and share account insights between banks to make more informed payment decisions.

## Potential benefits

### Make payments more resilient to fraud

Token rule validation and account attributes provide banks with the insights on counterparty accounts to manage risk exposure for each payment use case, fintech, digital wallet, or specific payee.

### Share account insights while protecting account data

Banks reduce account data exposure with the option to share only token rule validation results with other banks for sensitive account attributes.

### Secure and scale A2A use cases

Token-level payment controls enable banks to suspend a token for a specific payment use case when no longer authorized, set token-use counters (single-use, monthly, etc.) and apply use-case specific token rules.

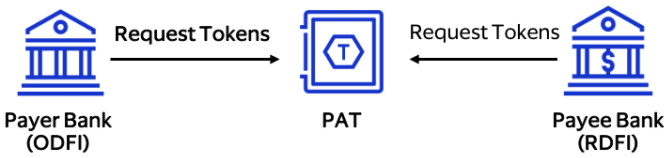
### Address regulation compliance

'Commercially reasonable' fraud mitigation, fraud data sharing, validate account is in good standing, full account name check, protect account data.

# How it works

PAT is available as a service or cloud native deployment. Banks connect directly or through a central network operator and integration requires only 3 APIs: Tokenize, detokenize and lifecycle management. Additional deployment models are available.

## Banks tokenize accounts

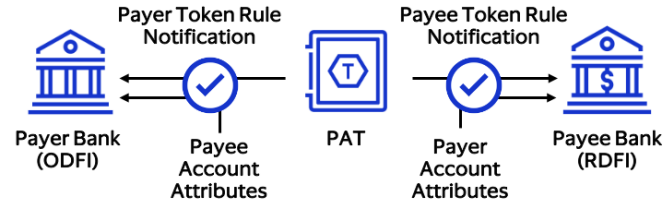



Banks tokenize their accounts, requesting a unique token from PAT for each payment use case (e.g., C2B, P2P, request-to-pay, open banking, specific payer/payee) and setting token rules to control risk exposure and make sure each token is used in payments only as intended.

During tokenization, banks also assign account attributes to be shared with the counterparty bank at time of payment.
Lifecycle management keeps the attributes up-to-date.

PAT generates and returns the tokens to the banks while storing account attributes and token rules.

## Banks detokenize at time-of-payment




When an account holder initiates a payment, their bank sends a detokenize message to PAT.

PAT applies token rules to counterparty bank account attributes and returns notifications along with account attributes, enabling banks to make a more informed payment decision before payer bank submits payment to the network or payee bank releases funds.

# Features

### Account token attributes

Banks share account insights to improve fraud detection and payment decisions.

### Token rules

Banks enable token-level controls that flag risks when payment velocity, channel, account type, amount, currency, etc. are outside set token rule limits for each use case (C2B, P2P, request-to-pay, specific payee, etc.).

### Lifecycle management

Quickly and easily update token status and account token attributes.

### Cryptogram protection

Generate account cryptograms in advance for validation during the payment process.

### Payment rail agnostic

Account tokens are configurable to work on instant payment rails such as The Clearing House (TCH) RTP, as well as other account-to-account payments rails, e.g., ACH, wire, etc.

### Seamless SaaS integration

Implement account tokens without disrupting existing transaction flows.

## Learn more

For more information, contact your Visa Representative or fill out an inquiry form.