Fact Sheet

Cloud Token Framework

Convert any connected device into a secure channel for digital commerce

Cloud Token Framework (CTF) allows the entire payment ecosystem to minimize risks associated with managing sensitive payment data. CTF enables card-not-present (CNP) tokens to unlock new opportunities in digital commerce and accelerate payment innovation. It does this by enhancing confidence in multi-device payments, reducing friction and minimising account takeover fraud. Combining consumer identify and verification (ID&V) with device intelligence, CTF is designed to enhance security and increase approval rates for CNP transactions across multiple payment experiences and devices.

Potential benefits

Elevate payment security across devices

Use consumer ID&V and device intelligence to link the consumer, cardholder and their associated devices to better manage risk and help prevent account takeover fraud.

Trusted devices increase confidence

Enable a trusted device to minimize friction and improve authorization rates for CNP transactions, resulting in a superior consumer experience.

Futureproof payments

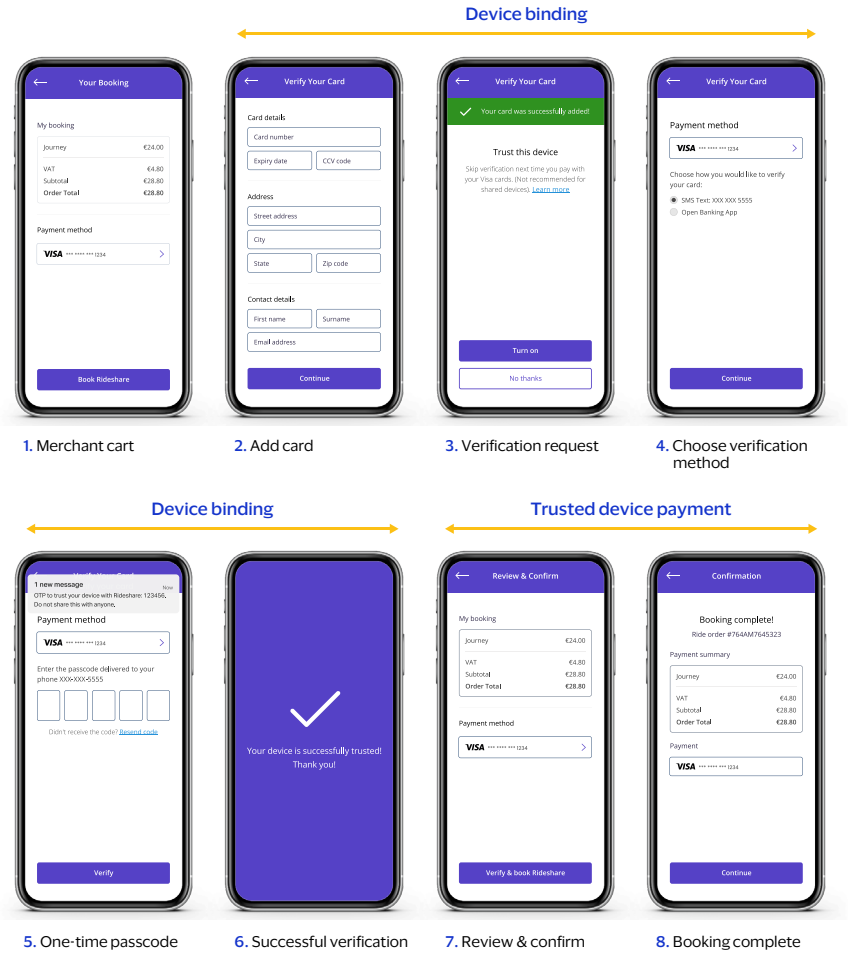
Expand digital commerce use cases with an end-to-end, secure and scalable token solution that provides a holistic approach to consumer authentication.

VISA

Customer experience

Device binding and purchase on a trusted device

The merchant or other token requestor's site or app enables the cardholder to select a connected device and mark it as trusted. This allows the cardholder to skip the verification process when they next make a payment. As an example, the below illustrates how this works when making a booking with a rideshare service.



1. The cardholder reviews the items in their booking and proceeds to checkout
2. The cardholder enters their card details and contact information
3. The app prompts the cardholder with a verification request to designate the device as trusted for future purchases
4. The merchant or other token requestor displays a list of consumer ID&V methods available from the issuer and the cardholder selects their preferred ID&V method
5. The cardholder completes verification via the ID&V method
6. Once confirmed, the cardholder receives a message to confirm that their device is trusted for subsequent transactions
7. On the trusted device, the cardholder is prompted to verify and confirm their booking
8. Once confirmed, the cardholder's transaction is complete. The issuer receives the required device information to perform further checks

Features

Issuer step-up capabilities

Use consumer ID&V to establish a clear link between the token requestor's customer and issuer's cardholder.

Unique and verifiable data

Validate the consumer's trusted device for transactions and include verified data for issuers.

Multiple trusted devices and reduced friction

Allow consumers to access their tokenized account from multiple trusted devices with minimal friction, using their trusted device as an authentication factor.

Device binding

Connect the token with multiple trusted devices via issuer ID&V and step-up authentication.

Consumer authentication

Capture and send multiple authentication factors and cardholder verification methods from multiple devices.

Token requestor-initiated cardholder verification

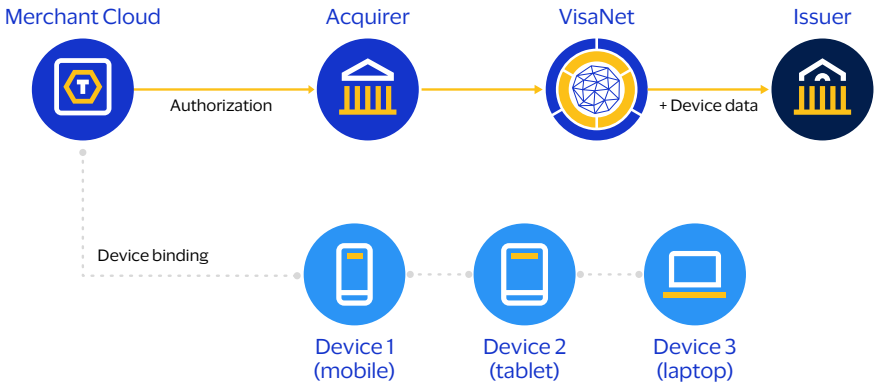
Request ID&V on a payment credential from an issuer whenever it's needed.

Please note, all device screens are presented for illustrative purposes only.

How it works

CNP tokenization with Cloud Token Framework

Cloud tokens enable a single experience across devices within an operating system.



* See footnote for figure 2 description

- Device Binding allows an eCommerce or card-on-file token, provisioned to the consumer's account, to be bound to multiple trusted devices
- Issuers will have the opportunity to perform risk-based verification of the cardholder and optionally challenge the cardholder for step-up authentication to confirm the binding of the cardholder and token to that specific device
- Subsequent card-not-present transactions from trusted devices will have device data elements and multi-factor authentication data, enabling issuers to perform strong cardholder verification, improve authorization approvals, mitigate fraud, and improve their overall token management specific

Learn more

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

Figure 2 description:

The diagram shows step-by-step process flows for card-not-present tokenization with CTF. From a device binding perspective, the diagram illustrates the ability of the VAS to enable an eCommerce or card-on-file token provisioned in the merchant cloud environment to be bound to multiple trusted devices, such as a smartphone, tablet and/or laptop. From an authorization perspective, the diagram shows the flow from the merchant cloud to the acquirer, via VisaNet and through to the issuer, enabling risk-based verification of the device binding and subsequent transactions.

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