Secure Payments and the Internet of Things

VISA

Table of Contents

Secure Payments and the Internet of Things

Introduction

The Internet of Things (IoT) is changing the way consumers interact with businesses by allowing a new channel for interacting through connected devices. Gartner forecasts that 25 billion connected things and sensors will be in use by 2021[1].

Visa offers connected device payment solutions to companies who want to offer secure payment experiences to consumers. Visa provides payments expertise, industry security standards, authentication standards and technical support to facilitate the design, implementation and consumer adoption of payments for IoT devices.

This document is intended for practitioners responsible for designing, developing and launching IoT commerce experiences. It provides an overview of how digital wallet payments work in IoT form factors, the role and benefits of payment tokens in IoT, an explanation of partner roles and common terminology, and considerations for integration models and service provider partners.

Digital Wallets in IoT

Digital wallets are a value-added service for most IoT device consumers. Enabling a tokenized payment credential in a digital wallet creates a seamless way for consumers to pay or be paid, without having to use a physical plastic card.

A digital wallet enables payments to multiple merchants and services. The consumer only has to add their payment credentials to the wallet one time (though a consumer may choose to load more than one payment credential in the digital wallet). With a merchant credential-on-file model, the consumer needs to add payment credentials separately for each merchant.

For the device OEM, enabling payment capabilities in an IoT device creates a differentiating feature and a better user experience. In a connected car, for example, it offers safety and convenience for the consumer for paying for fuel, food, parking and other transactions without pulling out a wallet and with minimal driver distraction.

For the Merchant, a Wallet app in a connected device allows additional ways for consumers to conveniently pay for Fuel, QSRs (quick-service restaurants) and other services. Merchants can process these transactions on their existing processing 'rails' and do not need to implement

1. https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

custom authentication, clearing, settlement, or exception management systems for proprietary digital wallets. Merchants can leverage digital wallets in IoT devices to deliver targeted offers and incentives, increasing brand loyalty, transaction amounts and purchase frequency.

Visa Digital Commerce Program for IoT

The Visa Digital Commerce Program for IoT is based on the EMV Secure Remote Commerce Technical Framework, and is designed to provide merchants, financial institutions, payment gateways, acquirers, and commerce platforms with the technology and tools to optimize digital payment experiences for emerging experiences like IoT and voice-activated devices. This framework will help by:

Creating simplicity – Consumers can make payments through a simple, streamlined digital experience across devices.

Decreasing fraud – The program brings advanced security methods to emerging and existing digital payments channels.

Increasing conversion – A simpler verification experience leads to higher buyer conversion.

Enabling scalable innovation – The program helps enable innovation at scale through the integration of digital platforms and IoT form factors.

Streamlining integration – The program will simplify integration and thereby lower costs by standardizing integration and enabling more scalable innovation across form factors.

Tokens and Digital Wallets

Wallet apps leverage **tokenization**, a security technology enabled by Visa Token Service (VTS). Tokenization replaces sensitive account information, such as the PAN/16-digit account number, with a unique digital identifier called a token. Visa stores the relationship between the PAN and token in its the Visa Token Vault. The token allows payments to be processed without exposing actual account details that could potentially be compromised. Key benefits of tokenization include:

Security – The sheer number of IoT devices represents a significantly high attack surface due to the number of devices, custom operating systems and other considerations. Compromises already have happened, and governments are even considering proactively hacking devices to prevent vulnerabilities. Tokenization removes high-value payment credentials from these at-risk environments.

Higher auth rates – Tokenized payments have an average of +5.75% higher auth rates[1] than traditional Ecom transactions. This allows the consumer the convenience of the digital wallet payment with higher auth success.

Decreased fraudulent transactions – Tokenized payments have a fraud rate reduction of -63%[2], decreasing merchant and issuer losses. Tokenization also enforces domain controls, ensuring that even if the token is compromised from a device OEM wallet, it can't be used in another domain.

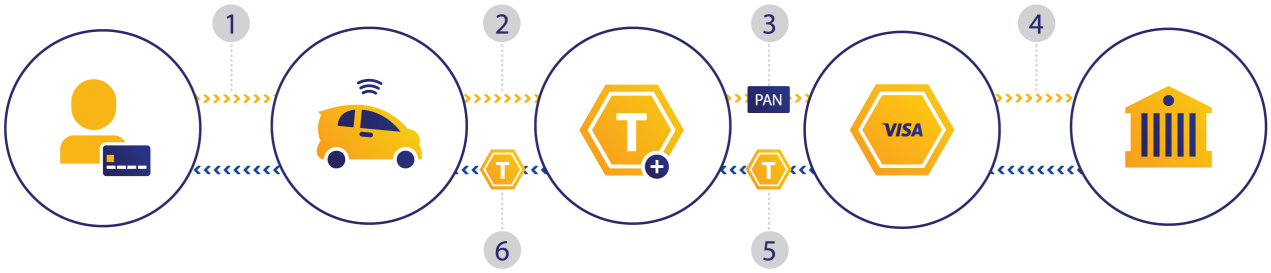
Greater scale – Proprietary tokenization doesn't provide credentials that can be used with any acquirer/gateway. Network tokenization provides this flexibility.

Read more on Tokenization.

2. Authorization rate lift from decline codes within a sample of 17 merchants. Source: VisaNet, TC05, UC01, Brand: Visa, Excludes Processing Error Declines. Declines calculated as percent of total authorizations (payment volume). Select Token participating Merchants (PAN and Token) with digital wallet TRs Issuer region US, July-Sept 2018, Potentially addressable by Token. Note: For purposes of these metrics, Super Regionals" include the top quartile of issuers by Visa PV, Regionals include the second quartile and Community banks include all remaining issuers.
3. Fraud Rate Reduction: Source: CNP & CP Average is for set of Token participating Merchants (by Merchant DBA) (PAN & Token) with digital wallet TRs April-June 2018, Issuer region: US

Provisioning Diagram

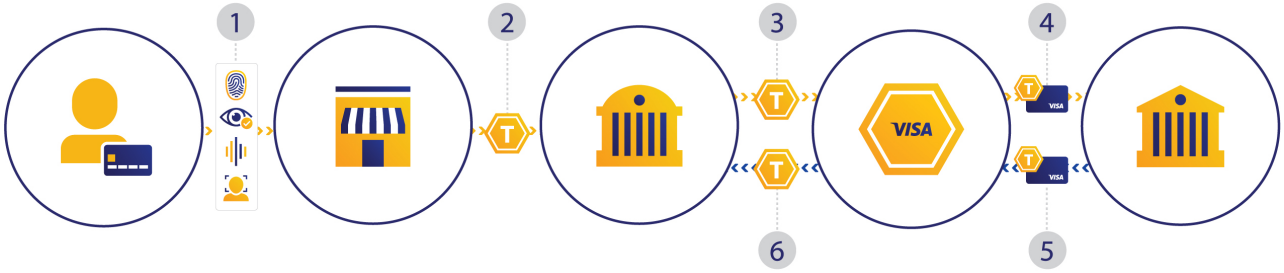
The below diagram illustrates how token provisioning and activation occurs. This is a One-Time action per payment credential.



1. Cardholder loads a Visa account to his or her connected device directly or through a companion app.
2. Device sends account load request to token requestor. Data required: PAN, CVV2, name, address verification data (from cardholder); device data and optional CDCVM (from connected device).
3. Token requestor requests payment credential from Visa Token Service
4. Visa Risk Manager makes a decision based on approval rules established by Visa account issuer. The issuer may require the cardholder to use step-up authentication in the form of a one-time issuer passcode.
5. Visa Token Service generates and delivers token to the device
6. Token requestor provisions token to the device and activates for payments

Purchase Transaction Flow

The below diagram illustrates how a digital wallet payment works in a connected IoT device. This happens with each purchase transaction.



1. Payment Initiated. The connected device app authenticates the user with PIN/Password or biometrics (voice, fingerprint, facial recognition). The consumer initiates a payment in-app.
2. Merchant sends token to acquirer. Depending on the commerce environment, the digital payment service provider (e-wallet, eCommerce merchant or app) passes the token to the acquirer as part of an authorization request.
3. Acquirer routes the token. The acquirer receives the token and routes it to Visa's network to begin processing the transaction.
4. Visa sends token to card issuer. Visa sends the token, along with the payment card details, to the issuer for authorization.
5. Issuer returns token and authorization. The issuer accepts or declines the transaction and sends its response back to Visa.
6. Transaction completed. The token and payment authorization are routed back to the merchant's bank, the acquirer.

Integration Approaches for Tokenization

The Wallet app provider may choose to integrate directly to VTS, or integrate through a Token Requestor-Token Service Provider (TR-TSP). Here are some considerations for each approach:

- **Integrate Direct to VTS**: Visa does not charge a Wallet app provider for direct integration to VTS. The Wallet app provider would have initial development effort to integrate with VTS, and would need to integrate separately to other card networks (Mastercard, American Express, etc.). There would be ongoing maintenance and testing to support changes such as enhancements or issues resolution.
- **Integrate through a TR-TSP**: The Wallet app provider may choose to integrate through a Visa Ready TR-TSP. This option provides a simplified integration with VTS, as the TR-TSP is already integrated to Visa and has gone through the Visa Ready certification process. A TR-TSP may potentially assist with integration to other card networks, depending on which card networks they support. Ongoing maintenance for enhancements or issues resolution is handled by the TR-TSP. PCI compliance is handled by the TR-TSP. There are fees for TR-TSP services.

  Token Service Providers (TSPs) are approved third-party partners connected to Visa Token Service and other networks who help token requestors enable tokenized payments. There are two TSP types:

  - An Issuer TSP (I-TSP) provides solutions for financial institutions in participating token requestors payment services.
  - A Token Requestor TSP (TR-TSP) allows token requestors to develop digital payment solutions powered by VTS).

A **Mobile Payment Processing Application (MPPA)** can play a valuable role in enabling digital wallets for IoT form factors. The MPPA offers the ability to coordinate between the front-end application (in-vehicle or mobile) and the gas station or convenience store. This allows IoT device OEMs to originate payment transactions in what has traditionally been a card-present segment. Some MPPAs also connect to other services such as parking, electric charging, vehicle maintenance and QSR for order-ahead.

For the OEM, in-vehicle wallets can be a differentiating feature by providing a safe, convenient way to pay for in-vehicle purchases and services. Partnering with an MPPA can simplify the process of integrating with merchants by building the app on the OEM's behalf to enable in-vehicle ordering. MPPAs can provide valuable purchase and vehicle maintenance data specific to the in-vehicle experience, which can lead to additional revenue opportunities for the OEM.

For the consumer, MPPAs can contribute to a better user experience by providing targeted digital offers for discounts and incentives on items and services the consumer is likely to buy. Connectivity to the consumer's merchant loyalty account provides the incentive of rewards and discounts, and the convenience of not having to provide loyalty account information separately.

For the merchant, the ability to provide targeted digital offers encourages more frequent and higher-volume purchases. Connection to the consumer's loyalty account also contributes to brand loyalty and repeat business.

Merchant Acceptance of Tokenized Payments

For IoT transactions, the merchant's payment processor will need to be able to process a payment with token and cryptogram. IoT transactions are very similar to Apple Pay, Visa Checkout and other in-app transactions. The merchant does not need to integrate with Visa; they just need to be able to accept tokenized payments. There are field-level changes required to support token and cryptogram for payments vs. 16-digit PAN and CVV. The merchant's payment processor will provide technical specifications with those details.

APIs to enable IoT Experiences

Visa offers several APIs that enable payment experiences for IoT form factors, including:

- **Visa Token Service** – replaces sensitive account information – such as the 16-digit primary account number - with a unique digital identifier called a token. This allows payments to be processed without exposing actual account details.
- **Visa Direct** – enables secure, real-time, push payment capabilities.
- **Visa Commerce Network** – allows merchants to retrieve active promotions, locate best-matched offers, enroll eligible Visa cards and be notified when consumers complete qualifying requirements.
- **Merchant locator** – enables the consumer to find a merchant by name or category.
- **Visa Sensory Branding** – provides sensory cues when a customer pays with their Visa card.

Steps for Enabling a Digital Wallet

The IoT device OEM defines the user experience interface for their device, and can ensure a consistent and safe experience across merchants. This is especially useful for avoiding driver distraction in a connected car, and for interacting with IoT form factors that do not have a visible UX, such as a voice-controlled speaker.

These are the high-level steps for designing and building a digital wallet for IoT, whether integrating directly with VTS or through a TR-TSP partner. Visa will work with the partner's project leads to compile a detailed schedule for each project.

Legal agreements with Visa are required to proceed, as noted.

Integration with other card networks would have their own steps and timelines, to be discussed with those networks directly.

Design:

- Visa will facilitate a co-creation workshop with the Wallet app provider and other partners (merchant, TR-TSP, etc.).
- The parties will identify the relevant use cases, target merchants and processing partners and set the project schedule.
- The Wallet app provider will design solution wireframes. Visa will provide design support and solution architecture approval.
- Note - A Collaborative Framework Agreement (CFA) between the Wallet app provider and Visa is required before Design can begin. The Visa Digital Enablement Program (VDEP) agreement is required before VTS specifications will be shared, though VTS specifications are only required by the Wallet app provider if a direct integration to Visa is planned. Integration to Visa through a Visa-certified TR-TSP will not require access to the VTS specifications.

Development:

- Development includes the front-end and back-end development for the Wallet app, integration with the merchant(s), and integration with the TR-TSP (if applicable).
- Note - The VDEP agreement and possibly additional legal agreements such as a Project Addendum are required before development can begin.

Solution Approval:

- Visa will review the developed solution for adherence to Visa Brand and User Experience standards and Security requirements.
- There will be functional testing for use cases and payload format.

Launch: production launch and support activities and marketing promotional content.

Common Payments and IoT Terminology:

Biometrics, such as a fingerprint or facial scan, provides a secure form of authentication that is easier for users than memorizing a password.

Credential-on-File (COF) - Credential on File (sometimes referred to as Card on File) payments refer to payments made using a funding method that the customer has stored for current and repeat transactions online (as opposed to "Form Fill payments" which refers to consumers actively selecting the payment method and entering their payment and address details on every transaction).

CAVV is the Cardholder Authentication Verification Value. It allows VisaNet to validate the integrity of the Verified by Visa (VbV) transaction data. These values are passed back from the issuer to the merchant after the VbV authentication has taken place.

CDCVM is the Consumer Device Cardholder Verification Method, a type of consumer verification method (CVM) supported by the card networks when assessing transactions originating from IoT and mobile devices.

A **Cryptogram** is a dynamic, one-time use code for each transaction that accompanies the token. The TAVV cryptogram is a 20-byte Base64-encoded binary value required by VisaNet Field 126.9. It is the cryptogram type that Visa is requesting merchants use with tokens long term and is already used today, for example, by the major mobile wallets.

CVV2 is Card Verification Value, an authentication system to reduce fraud for internet transactions. The card holder is required to enter the CVV2 number, 3 digits on the back of the card, at the time of card provisioning to verify that the card is on hand.

A **Digital Wallet** is a way for a user to carry credit and debit card information in a secure digital form on an IoT or mobile device. Instead of using a physical, plastic card to make purchases, a mobile wallet on a smartphone, wearable or connected car can be used to make purchases.

EMVCo is a joint effort between payment networks including Visa, American Express, Discover, JCB, Mastercard and UnionPay to ensure security and global acceptance. It is the global standard for chip-based Debit and Credit Card transactions and Secure Remote Commerce specifications.

The **Internet of Things (IoT)** is a network of devices such as vehicles, wearables and home appliances that contain electronics and software which allows these things to connect, interact and exchange data.

A **credit card Issuer** is a bank or credit union that offers credit cards. When consumers make credit card purchases, the credit card issuer is responsible for sending payments to merchants for purchases made with credit cards from that bank.

Original Equipment Manufacturer (OEM) is the maker of the IoT device, such as a connected car, voice-enabled device or wearable.

A **Payment Processor** is a company selected by a merchant to handle transactions from various channels such as credit cards and debit cards for merchant acquiring banks.

Primary Account Number (PAN) is the 16-digit number on a payment instrument.

The **Payload** contains the Token, Cryptogram, optional CDCVM and device details, and the order summary attributes.

PCI Compliance – The Payment Card Industry Data Security Standard (PCI DSS) applies to any company that accepts credit card payments, or stores, processes and transmits cardholder data. Working with a PCI compliant provider reduces the responsibilities of the Wallet app provider. Read more on PCI Compliance.

QSR – Quick service (fast food) restaurant.

Step-Up Authentication is the process by which a user is prompted to produce an additional form of authentication. This provides a higher level of assurance that the user is who they claim to be. For example, a user may be prompted to provide a one-time passcode while entering payment credentials to a Wallet.

A **Token** is a security technology Visa provides through the Visa Token Service. It replaces sensitive account information, such as the 16-digit account number, with a unique digital identifier. Visa stores the relationship between the PAN and token in its secure Token Vault. The token allows payments to be processed without exposing actual account details that could potentially be compromised. The key benefits of tokenization are improved security within the financial ecosystem and improved authorization rates. Read more on Tokenization.

Token Service Providers (TSPs) are approved third-party partners - connected to Visa and other networks - who help token requestors enable tokenized payments. There are two TSP types:

- An Issuer TSP (I-TSP) provides solutions for financial institutions in participating token requestors payment services.
- A Token Requestor TSP (TR-TSP) allows token requestors to develop digital payment solutions powered by VTS.

A **Token Requestor (TR)** is an entity that requests payment tokens for end-users. Some examples of TRs include digital wallet providers, payment enablers, merchants and IoT manufacturers.

Voice Commerce has a powerful influence on User behavior with the growing popularity of smart home speakers. The ability to control IoT devices with voice commands is especially important, as many devices do not have a visual user interface. Also, the ability to interact with a mobile wallet using voice commands provides a safety feature for users in a connected car by removing visual distractions.

