

# Visa Digital Wallet Enabler



## Enable and secure your mobile wallet for contactless payments with a single, end-to-end software solution

Visa Digital Wallet Enabler (VDWE) empowers payment card issuers and third-party wallets to manage their own mobile wallet, retaining control and exclusivity over customer relationships.

Enable the use of contactless mobile payment cards and in-app payment transactions while using network tokens to create safer, optimized payment experiences.

Connecting to Token ID's VDWE requires one integration and creates a unified connection towards worldwide Network Token Services such as Visa Token Service (VTS) and Mastercard Digital Enablement Service (MDES).

## Potential benefits

### **Tailor your solution**

Choose whether to integrate with global and/or private label network token services in line with business and technical requirements.

### **Simplify partner integration**

The single, unified Token Requestor API removes integration complexity with multiple token service providers (TSPs).

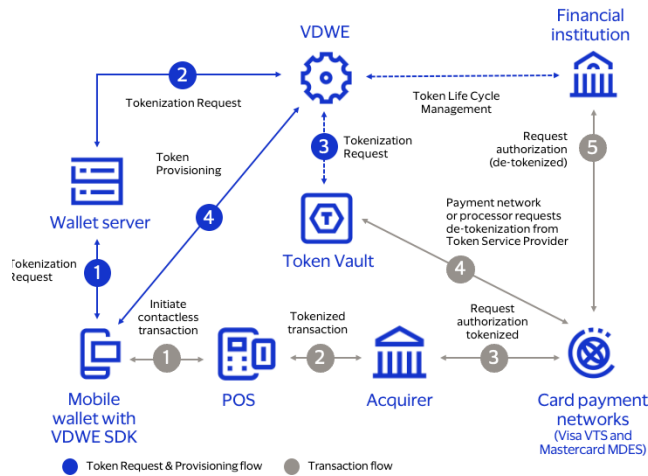
### **Plug-in to payment schemes**

Support multiple international and domestic payment schemes instantly with a scheme-agnostic and certified platform.

### **Enhance digital payments**

Protect and enrich the customer payment experience with tokenization while retaining full brand visibility and relationship control.

# How it works



## Token request & provisioning flow

1. The first step shows the initial token request from a token requestor such as an issuer mobile wallet to the wallet server.
2. The tokenization request is routed to VDWE which then requests a token from the appropriate TSP.
3. The TSP generates and issues the payment token and credentials to VDWE.
4. VDWE provisions token and credentials to VDWE SDK on mobile device.

## Transaction flow

1. As a contactless transaction is performed, a token and cryptogram are passed to the merchant point of sale.
2. The tokenized transaction is passed from the merchant to the acquirer.
3. The acquirer passes a tokenized authorization request to the payment network.
4. The payment network performs detokenization and additional checks, e.g., cryptogram validation.
5. The payment network sends an authorization request with detokenized card number and check results to the issuer for payment processing and authorization approval. The authorization is passed back along the transaction flow to the merchant and the payment is completed.

## Features

### End-to-end solution

A two-part solution: a server where virtual cards are managed, and a plug-in to provision payloads to the mobile device

### Legacy system interoperability

Support international and domestic payment schemes without upgrading existing payment acceptance infrastructure

### Offline transaction support

Provision payloads in advance to enable payments when the consumer device cannot connect to the server

### Multi-platform support

Securely connect to Apple\* or Android Near Field Communication (NFC) interface to enable contactless transactions and mobile wallet capabilities via Host Card Emulation (HCE)

\* Contact Sales Executive to see availability in your region.

## Learn more

For more information, contact your Visa Representative or [click here to fill out our online enquiry form](#)