Watch integration

The Watch Payment product allows payments using Watch connected to Android and iOS smartphones. Payments are based on the MDES Token Requestor solution from Mastercard. Contactless payments are possible without a constant internet connection—both on the smartphone and the smartwatch.

The core payment and token provisioning process is based on the Token Requestor product and requires an active project with Mastercard. VCPSDK is a certified and secure product, approved by EMVCo and Mastercard, and has been launched in multiple banking and partner applications.

Introduction

Basic information

The Wearables SDK is an SDK designed to integrate with **Watch as Payment Instrument**. Wearables SDK enabling direct communication between smartwatches and payment systems. It allows to create applications that support contactless payments directly from the Watch, eliminating the need for a paired smartphone during transactions. This streamlined integration offers a secure and efficient way for users to make payments simply by wearing their smartwatch.

> **Note:** Product is based on Verestro Cloud Payment solutions for NFC Issuer Wallet with Mobile MasterCard MCBP 2.1 SDK.

See Verestro Product description here Token Requestor.

Requirements

Issuer Wallet integration

Verestro Cloud Payment solutions for NFC Issuer Wallet integration as described Token Requestor

Wearables SDK

Verestro Wearables SDK for Android or iOS

Watch Manufacturer

Integration with Watch Manufacturer

Components

- **Mobile Payment Application (MPA)** - application for integrating Verestro Cloud Payments for safe device&user authentication, card management and tokenization
- **User management MDC SDK (Mobile DC SDK)** - Verestro SDK for device, user and cards management
- **Token Requestor SDK (VCP SDK)** - Verestro SDK for tokenization, token management and payment
- **Wearengine SDK (Wearables SDK)** - Verestro SDK for enabling VCP SDK tokenization on Watch SDK
- **Watch payment SDK** - Verestro SDK for token management and payment on Watch
- **Watch communication SDK** - SDK on the watch for communication with watch.
- **Watch Application** - Verestro integration layer integrated directly to Client's watch application for communication with Wearables SDK and Watch SDK

Architecture

architecture_watch.png

Use Cases

Watch integration

Connection to Watch is usually realized by Watch's manufacturer application which allow to create connection and pair Watch device with Android/iOS Phone.
Development requires additional configuration on Watch manufacturer store. In order to start integrate Watch in client Mobile Payment Application (MPA) client need to:

- create account on Watch manufacturer Store
- add MPA packageId or bundleId
- configure MPA trusted certificates for signing

MPA to Watch Connection

Connection from MPA to Watch is realized by Watch's manufacturer Library.
Wearables SDK allows to simply use Watch library along Verestro UCP SDK.

Watch connection

MPA to Watch Pairing

Once Watch is connected with MPA it can be used with Watch application for communication with Wearables SDK.
In order to create secure channel to WatchSDK bundled with Watch application UCP SDK must exchange pairing data with WatchSDK.

Watch pairing

Secure channel for data sending

During this process Wearables SDK create secure connection between UCP SDK and Watch SDK to send card profile and transaction credentials.

- Every data synchronization requires to create new secure channel.
- Both sender and receiver is verified during connection.
- Process is transparent for MPA.

Secure channel

Token creation

During this process new Token is created for usage on dedicated Watch device.
Verestro SDK allow to create multiple Device along one SDK instance and tokenize same Card for each device.

Read more about Verestro SDK integration in order to tokenization.

Add Token to Watch

During this process new created token for unique device (Watch) is transferred from certified UCP SDK to to Watch SDK using a secure channel.
Transferred Token contains token data to show on Watch UI like last four digits, expiration date and card visual.

Add Token to Watch

Add Token Credentials to Watch

During this process encrypted transaction credentials are transferred to Watch SDK and assigned to Token making it ready for contactless payments.
These credentials are stored on the device, enabling payments even without a constant internet connection or a direct link to the phone.
Process is used both for credentials add after sending token and for data synchronization between

UCP SDK and Watch SDK.

Add Token Credentials to Watch

Token data synchronization

This process ensures that all token and payment-related data on the watch remains up to date.
During synchronization, both the MPA and the Watch application update the token status (active, suspended, or deleted) and the status of transaction credentials within the Watch SDK.
The Wearables SDK is responsible for maintaining the maximum number of transaction credentials on the Watch SDK to enable standalone payments directly from the watch.
Token and transaction credentials synchronization can be initiated by either the MPA or Watch application and should be performed every time the application is launched.

Additional Token synchronization use cases

- token managed by MPA or Client's Admin Panel
- token updated by MasterCard with re-digitization
- application and related tokens ares removed on Phone or Watch

Additional transaction credentials synchronization use cases

- sending new transaction credentials along with associated Token
- transaction is performed on Terminal and Watch request synchronization
- finished replenish credentials process on MPA

Synchronization

Token data - synchronization

Standard communication between MPA and Watch in order to keep both up to date.

Token status update

Invoked on MPA or remote (Admin Panel) action related to Token.

Token data - status update

Watch Payment

Process describes Payment flow on Watch.

- User must unlock Watch to process payment and open Payment application.
- Once the Payment Token is selected, the user can Tap & Pay on a terminal.
- After the payment, the watch should attempt to communicate with the MPA to synchronize the credential state.

Payment

Payment authentication

Transactions must be authenticated, but this does not mean that every transaction requires separate confirmation.

The application uses **Consumer Device Cardholder Verification Method (CDCVM)** to authenticate the user. Depending on specific circumstances, the app may request biometric authentication or a PIN.

Since the service uses on-device authentication, no additional security mechanisms need to be implemented by the integrator.

Disabling Payments

The table below summarizes how different unpairing or blocking scenarios affect smartwatch payment availability.

Situation	Result	Payment availability
Watch is unpaired from the phone via the Wearable Provider's app or the payment app	It is no longer able to process payments.	**Not available**
Watch was connected to the phone at the time of unpairing	Stored payment data is automatically deleted from the watch	**Not available**

User switches to a new phone or another watch	Payment data cannot be transferred between devices or retained on the watch	**Requires new setup**
Payments are blocked through the Admin Panel	Payments are blocked on both the phone and watch	**Not available**
User removes the watch pairing from the mobile application	Smartwatch payments are disabled	**Not available**

Revision #13
Created 4 May 2026 11:56:39 by Beata Rzemieniak
Updated 12 May 2026 12:04:09 by Beata Rzemieniak