Offline Mobile Payment Solution

Crunchfish's patent pending Offline Mobile Payment Solution is built on an Offline Wallet that may either use the Secure Element provided by the mobile OS or run as a Trusted Application in V-OS virtual secure element.

The Offline Wallet securely maintains an offline balance that is utilized for offline transactions. The transactions are cryptographically signed by the payer, assigned to the payee and guaranteed as they are debited against the offline balance. The payee verifies the Guaranteed Offline Payments (GOP) in an application running on a mobile, card terminal or PC. Transaction logs are settled when either party goes online.

The solution is exceptionally configurable with any type of digital payment service regardless of settlement rail, e.g. EMV, instant payment, CBDC or closed-loop wallet. It may also be integrated directly with the payment rail. The offline balance may be facilitated by sub-wallet, pre-authorization, or credit.

The offline transaction may use any type of proximity interaction, e.g. QR, NFC, BLE or ultrasound and the merchant may use any type of device to verify the Guaranteed Offline Payments in an offline mode. This provides an unprecedented flexibility to provide offline payments for any digital payment service.

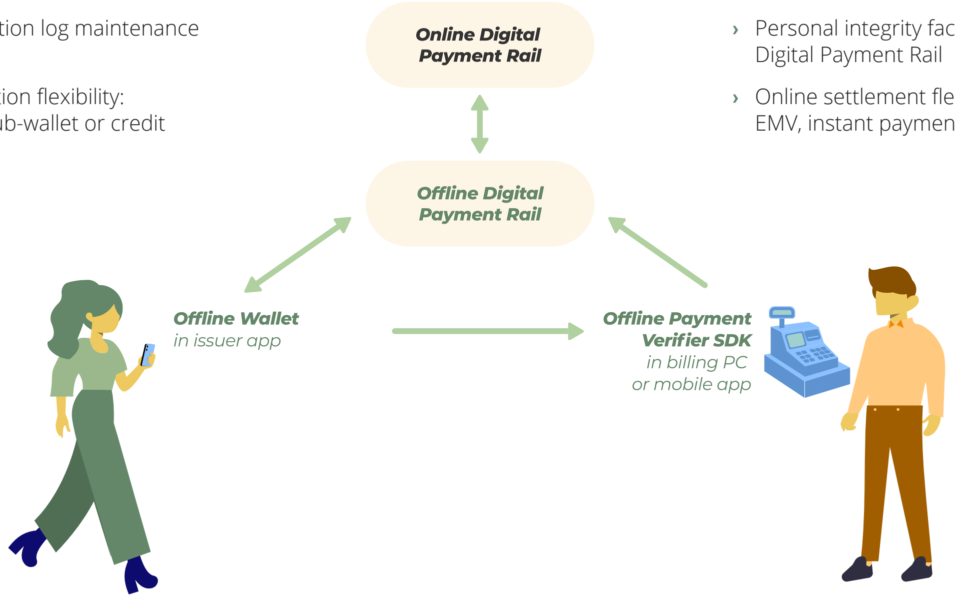
Offline Wallet using Secure Element in mobile OS

Offline Balance

- Balance exchange and auto-refill of Offline Wallet
- Configurable and signed risk parameters set by PSP or issuing bank
- Balance and transaction log maintenance in Offline Wallet
- Offline balance creation flexibility: pre-authorization, sub-wallet or credit

Online Settlement

- Independent settlement by the merchant and the customer
- Online validation and settlement of Guaranteed Offline Payments
- Personal integrity facilitated by Offline Digital Payment Rail
- Online settlement flexibility: EMV, instant payment, CBDC or wallet


Online Digital Payment Rail
Offline Digital Payment Rail
Offline Wallet
in issuer app
Offline Payment Verifier SDK
in billing PC or mobile app

Offline Transaction by Customer

- Initiation of offline transactions that debits the offline balance
- Guaranteed Offline Payments cryptographically signed by customer
- 2-factor authentication using PIN or biometrics in Offline Wallet
- Double spending protection
- Proximity interaction flexibility: QR, NFC, BLE or ultrasound

Offline Transaction to Merchant

- Merchant locked as the payment receiver in the Guaranteed Offline Payments
- Guaranteed Offline Payments cryptographically verified by merchant
- Guaranteed Offline Payments validated and collected using Crunchfish's GOP SDK
- Transaction replay protection
- Merchant terminal flexibility: mobile app, POS-terminal or PC

Offline Wallet as a Trusted Application in V-OS

Introduction

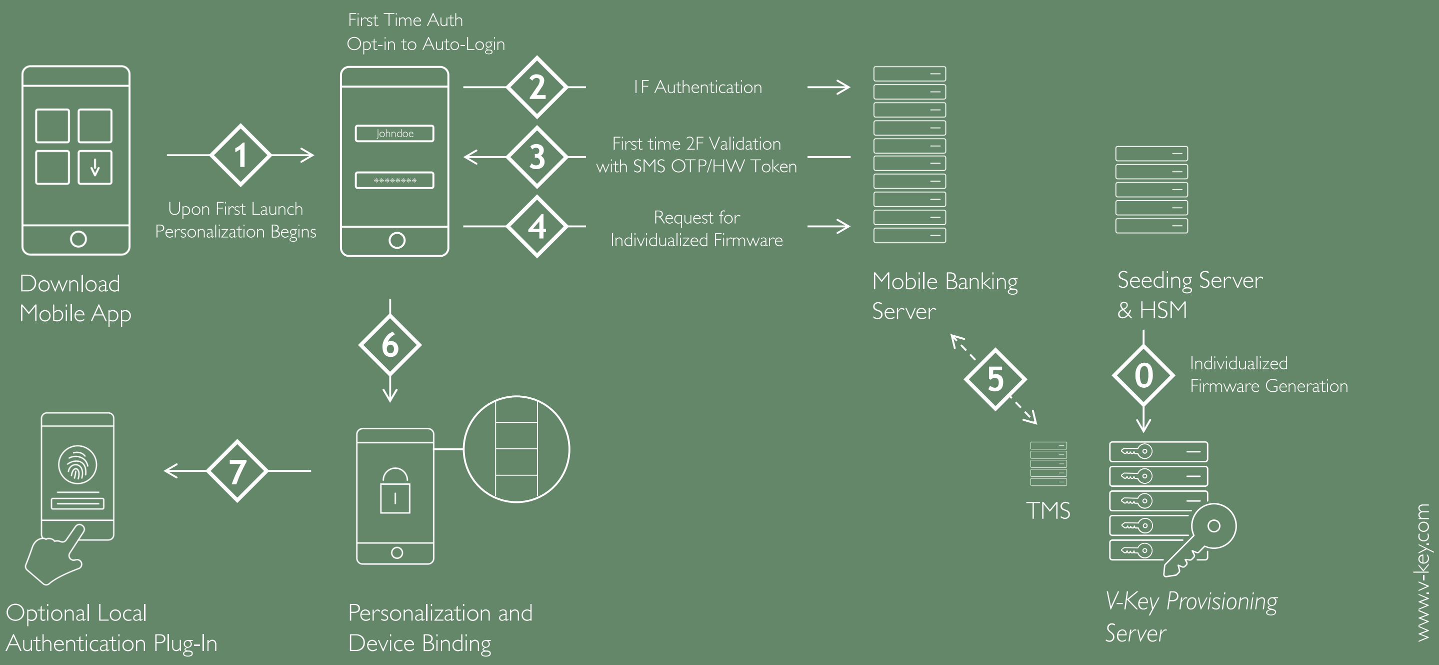
Crunchfish's Offline Wallet is a Trusted Application that runs securely on V-key's patented virtual secure element V-OS. The Offline Wallet is isolated by V-OS from the unsafe mobile application, and prevents an attacker with control of the underlying operating environment from accessing or exposing sensitive logic or data in the Offline Wallet. V-OS achieves isolation through layered tamper detection and response mechanisms such as anti-debugging, device binding, and anti-reverse engineering, to protect against hackers and malware.

V-OS Process Certified Cryptography

V-OS is a patented cryptographic virtual machine that ensures the integrity of crypto processing as well as protects encryption keys and sensitive information. It is designed to meet security requirements for FIPS 140-2 Level 3 and Common Criteria EAL3+. Sensitive cryptographic keys, data, and application codes are protected using advanced techniques in and around V-OS such as binary code morphing, memory encryption, and white-box cryptography techniques. The Offline Wallet uses efficient, state of the art elliptic-curve cryptography for balance exchange and Guaranteed Offline Payments.

V-KEY

PROVISIONING - OTA INDIVIDUALIZATION



Eradicate Costly Hardware Dependency

Without a hardware dependant secure element effortless over-the-air deployment is possible for a fraction of the costs. V-OS as a software based secure element minimizes total costs of ownership and drives faster market penetration.

Device Fingerprinting

V-OS captures hardware information that uniquely individualizes the device. This prevents malicious cloning of the mobile phone onto another device to gain access the Offline Wallet.

Cryptographic Keys Handling

The Offline Wallet handles the storage and use of cryptographic keys. Updates is handled securely by a Key management server. Personalized keys and cryptographic protections can be dynamically provisioned for the highest levels of security, and to support key rotations and tokenization requirements.

At no time are secret keys exposed to the unsafe mobile application or native operating system. The offline payments may be reconciled and monitored on the customer's offline wallet for potential fraud at the banks' servers.