Digital Cash Wallet xoxo.cash

Crunchfish Digital Cash Wallet is an extremely flexible and interoperable solution that compliments any payment service, on any payment scheme, with capabilities that replicate paying with cash. A two-step hierarchical architecture makes Digital Cash payments independent from the net, offering instant payment offline, followed by settlement online to move money between accounts. On request by the payer, payments may be private in relation to banks, within the limits of money laundering regulations.

The Digital Cash Wallet has a mirrored Digital Cash Account which is used for settlement online, when either the payer or the receiver connects online, independently of each other. The Digital Cash Account may only be debited from the Digital Cash Wallet protecting against double spending and overdrafts. It registers all activity in the Digital Cash Wallet.

Digital Cash payments are debited against a balance maintained by the Digital Cash Wallet, which may be implemented using signed risk parameters or as a trusted application running on a smart card or a digital wallet, on either a smartphone or a feature phone. It functions like a tollgate securing that sufficient balance is available and that issuer rules are fulfilled, before a cryptographically signed Digital Cash payment is generated. The payments are assigned and transferred to the receiver using proximity interaction, who may verify them on an electronic device in offline mode.

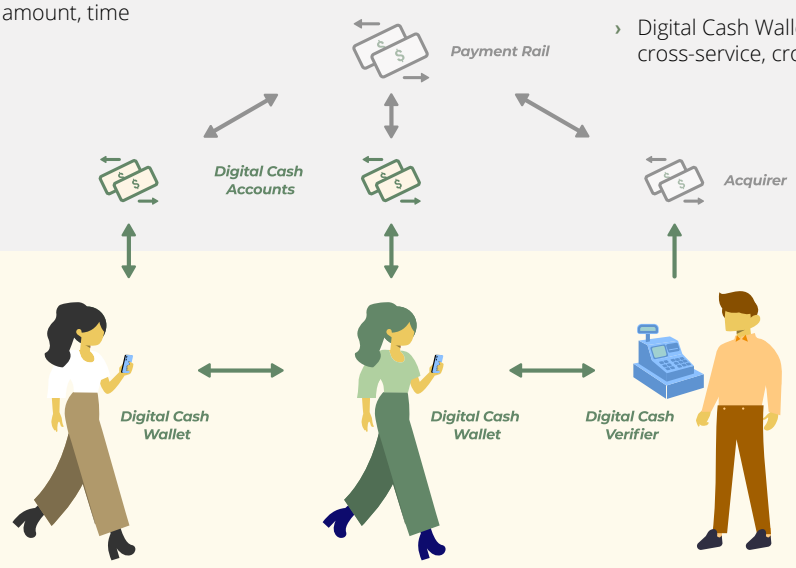
Crunchfish is global Certificate Authority for the Digital Cash Wallet. It is globally interoperable cross-service and cross-scheme by the use of signed user and Digital Cash certificates. It is also cross-border by the use of a foreign exchange table in the payment app.

Digital Cash Balance

- Balance exchange and auto-refill of Digital Cash Wallet
- Balance and transaction log maintenance in Digital Cash Wallet
- Digital Cash Wallet is synchronized with an online Digital Cash Account
- Issuer risk limit flexibility: maximum amount, accumulated amount, time
- Network connectivity flexibility: https, cellular, sms, e-mail, post

Online Settlement

- Independent settlement by the receiver and the payer
- Online validation and settlement of Digital Cash payments
- Personal integrity may be protected
- Payment scheme flexibility: EMV, RTP, CBDC, crypto, eWallet or mobile money
- Digital Cash Wallet interoperability: cross-service, cross-scheme and cross-border



Digital Cash payment by Payer

- Initiation of Digital Cash payments that debit the Digital Cash Wallet
- Guaranteed Digital Cash payments cryptographically signed by payer
- 2-factor authentication using PIN or biometrics in Digital Cash Wallet
- Protection against overspending
- Bearer device flexibility: smartphone, feature phone or cards
- Security implementation flexibility: SE, SIM or signed risk parameters

Digital Cash payment to Receiver

- Receiver assigned in the Digital Cash payment cryptogram
- Digital Cash payments verified by receiver in an offline mode
- Digital Cash payments stored and forwarded by Digital Cash Verifier or payment terminal
- Transaction replay protection
- Proximity interaction flexibility: Chip, QR, NFC, BLE or ultrasound
- Receiver device flexibility: mobile, cash register or payment terminal

Digital Cash Wallet running as an Offline Wallet as a Trusted Application in V-OS

Introduction

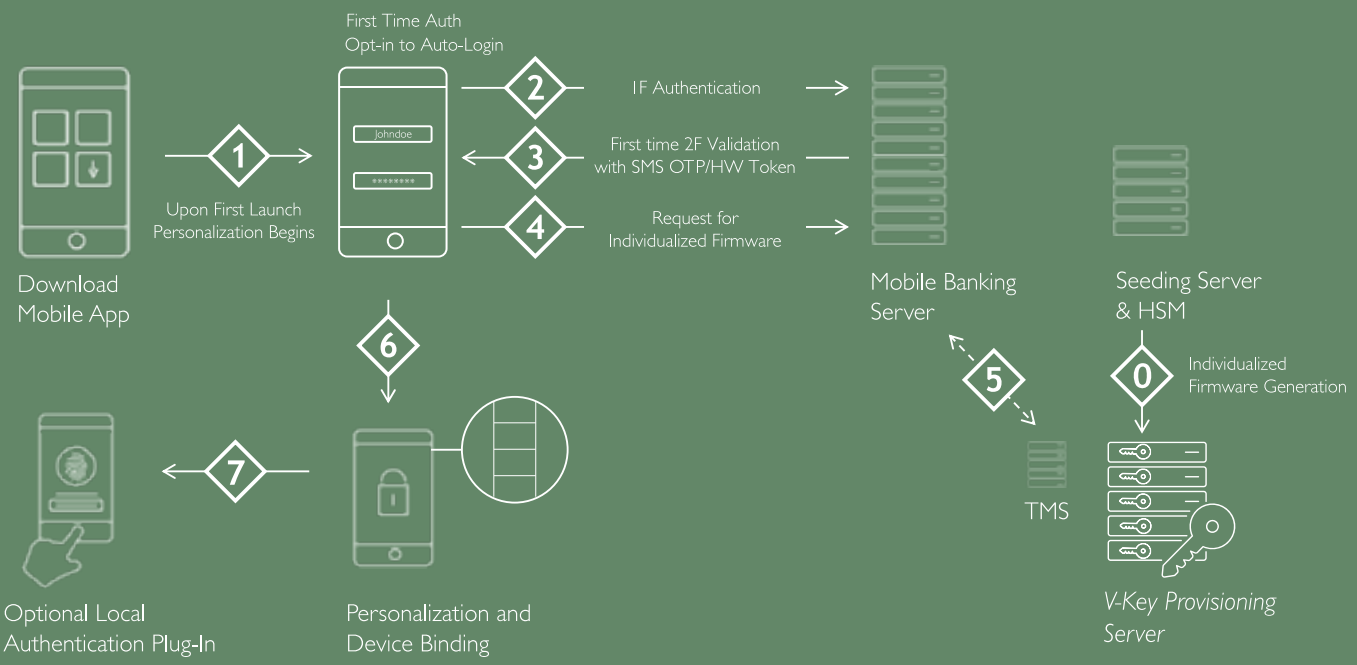
Crunchfish's Digital Cash Wallet is a Trusted Application that runs securely on V-key's patented virtual secure element V-OS. The Digital Cash Wallet is isolated by V-OS from the unsafe mobile application, and prevents an attacker with control of the underlying operating environment from accessing or exposing sensitive logic or data in the Digital Cash 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 Digital Cash Wallet uses efficient, state of the art elliptic-curve cryptography for balance exchange and Guaranteed Digital Cash 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 to the Digital Cash Wallet.

Cryptographic Keys Handling

The Digital Cash 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 Digital Cash payments may be reconciled and monitored on the customer's Digital Cash Wallet for potential fraud at the banks' servers.