

DIGITAL WALLET & MOBILE PAYMENT.

Mobile wallets keep payment credentials off the general operating system entirely — in a dedicated secure chip, or in short-lived cloud tokens that limit what's ever actually stored on the device. **A provisioned token still isn't enough to pay; a live biometric or passcode check happens at every transaction.**

- SECURE ELEMENT
- PROVISIONING VERIFICATION
- BIOMETRIC PAYMENT GATE
- REMOTE TOKEN SUSPENSION

01 THE MECHANISM



Hardware Isolation Keeps the Credential Off the OS

The strongest implementations store the payment credential in a dedicated Secure Element chip, **physically separate from the phone's general operating system**, so OS-level malware can't reach it directly.



Cloud Tokens Compensate for Weaker Isolation

Where a discrete secure chip isn't used, wallets instead limit what's stored on-device to **short-lived, limited-use tokens refreshed from the cloud**, reducing what a device compromise could expose.



Provisioning Requires Verification First

Adding a card to a wallet triggers an issuing-bank verification step **before the network token is actually provisioned** to that device, meant to catch stolen-card wallet fraud.

02 THE FLOW

The Properly Verified Provisioning CONTAINED

1

A customer adds a card to their wallet, and the issuing bank sends an **out-of-band verification** — a push to the cardholder's registered device or a call to their known number.

2

Only after that verification succeeds does the network token get **provisioned to the device's secure hardware**, bound to that specific device.

3

Every subsequent payment still requires a **live biometric or passcode check**, so a stolen but locked phone can't pay even with the token already provisioned.

The Weakly Verified Provisioning EXPOSED

1

An attacker with a stolen card's details attempts to add it to their own wallet, and the issuing bank's verification **relies only on data the attacker may already have**.

2

The verification passes, and a network token for the stolen card is **provisioned to the attacker's own device**, entirely independent of the real cardholder.

3

The attacker makes purchases before the real cardholder notices, since **no physical card was needed and no alert reached the actual customer**.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Hardware or Cloud-Based Credential Isolation	A dedicated Secure Element or a limited-use, frequently refreshed cloud token architecture, keeping persistent payment secrets away from the general OS.
Provisioning Identity Verification	Issuing-bank verification of the actual cardholder before a network token is issued to a new device, meant to catch stolen-card wallet fraud at the source.
Per-Transaction Biometric or Passcode Gate	A live authentication check at the moment of payment, independent of whether the token itself was already provisioned to the device.
Remote Device and Token Suspension	The ability to remotely deactivate a specific device's provisioned tokens without needing to cancel the underlying physical card.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Weak or Data-Only Identity Verification at Provisioning	No	Relying solely on information an attacker might already have from a breach lets a stolen card be provisioned to a fraudster's own device.
No Per-Transaction Biometric or Passcode Requirement	No	A provisioned token with no live authentication check at payment time means a stolen, unlocked phone can pay directly.
Persistent Credentials With No Hardware or Cloud-Token Isolation	No	Storing a long-lived payment secret directly in general OS-accessible storage exposes it to whatever malware can reach that storage.
No Remote Suspension Tied to the Physical Card	No	Without the ability to deactivate a specific device's token independently, a lost phone forces a full physical card cancellation just to contain the risk.
Hardware/Cloud Isolation + Verified Provisioning + Per-Transaction Auth + Remote Suspension	Yes	Covers the credential's storage, its issuance, its use, and its revocation as four distinct control points.

DIGITAL WALLET & MOBILE PAY.

ISOLATE · VERIFY · GATE

05 PROGRAM OPERATIONS

A Secure Element and a cloud-based token model solve the same isolation problem differently — one uses dedicated hardware, the other limits what's ever actually stored on the device.

Weak provisioning verification is a real, documented fraud vector. An attacker with just enough stolen card data can add someone else's card to their own wallet if the issuer's check never reaches the real cardholder.

The per-transaction biometric check is a distinct control layer from the token itself — it's what stops a stolen but locked phone from being usable, independent of the provisioned credential.

Convenience modes that skip per-transaction biometrics, like transit express-pay, are a deliberate, narrow, opt-in tradeoff of some security for speed, not a general weakening of the model.

06 CONTROL MAPPING

EMVCO TOKENISATION SPEC

The same network-tokenization standard covered for card-present transactions, extended to govern wallet-provisioned tokens domain-restricted to a device.

ISSUER ID&V REQUIREMENTS

Card network and issuer requirements for how a cardholder's identity must be verified before a network token is provisioned to a new device.

GLOBALPLATFORM SE STANDARDS

Hardware and firmware isolation standards governing how wallet providers protect credentials on-device.

FIDO ALLIANCE STANDARDS

Standards governing on-device biometric authentication and how it's communicated to relying applications like a wallet's payment flow.

07 WHAT THIS DOES NOT SOLVE

Wallet Account Takeover

Securing the payment credential doesn't protect the cloud account managing which cards are provisioned to a wallet in the first place.

Social Engineering the Cardholder

A properly verified, biometric-gated wallet still executes a payment the real cardholder was talked into authorizing themselves.

Merchant or Network-Side Fraud

Device-level wallet security protects the credential and its use; it does nothing for fraud elsewhere in the transaction chain once a payment is initiated.

Physical Coercion

A biometric or passcode gate can be defeated if an attacker physically forces the real cardholder to authenticate the transaction themselves.

08 MYTHS VS. REALITY

MYTH "A stolen phone means the attacker can use every card in the wallet."	REALITY A live biometric or passcode check is required for each transaction, independent of whether the token is already provisioned.
MYTH "All mobile wallets store payment credentials the same way."	REALITY Some use a dedicated Secure Element chip; others rely on limited-use cloud tokens with software-level protections — a meaningfully different isolation model.
MYTH "Adding a card to a wallet is as simple as typing in the number."	REALITY The issuing bank runs its own identity verification step before a network token is actually provisioned, specifically to catch stolen-card fraud.
MYTH "If my phone is lost, I have to cancel my physical card immediately."	REALITY The specific device's provisioned tokens can typically be remotely suspended independently, without touching the physical card.
MYTH "Weak provisioning verification is a hypothetical risk, not a real one."	REALITY Attackers provisioning stolen card data to their own wallets is a documented fraud pattern tied to issuers whose verification never reaches the cardholder.

09 SPEAK THE PROGRAM — KEY TERMS

SECURE ELEMENT (SE)

A dedicated, tamper-resistant hardware chip that stores payment credentials separately from a device's general operating system.

HOST CARD EMULATION (HCE)

A software-based approach using limited-use, frequently refreshed cloud tokens instead of a persistent secret in dedicated hardware.

TRUSTED EXECUTION ENVIRONMENT (TEE)

An isolated execution area within a device's main processor, offering meaningful but less rigorous separation than a discrete Secure Element.

IDENTIFICATION AND VERIFICATION (ID&V)

The issuing bank's process for confirming a cardholder's identity before provisioning a network token to a new device.

PER-TRANSACTION AUTHENTICATION

A live biometric or passcode check required at the moment of payment, independent of whether a token has already been provisioned.

REMOTE TOKEN SUSPENSION

The ability to deactivate a specific device's provisioned payment tokens without canceling the underlying physical card.