

PAYMENTS SIGNAL REFERENCE ARCHITECTURE

SYNTHETIC / TRAINING ONLY

Digital wallets, network tokenisation, 3-D Secure, and cardholder-data boundaries

See how a wallet enrolls a card, uses a payment token and transaction credential, invokes authentication when required, and keeps raw card data inside controlled boundaries.

Version: Payments Signal reference architecture v1

Reviewed: 2026-07-23

REFERENCE POSTURE

This blueprint shows responsibility and trust boundaries, not a licensed token-service or wallet specification. Device attestation, issuer identity-and-verification methods, token assurance, cryptographic protocols, liability, authentication exemptions, fallback, and PCI DSS scope must be assessed against the actual providers, channels, and current rules.

COMPONENTS

01 Cardholder device and wallet [channel]

Owner: Wallet provider and device owner

Protects the user session and requests provisioning or payment with device context.

02 Wallet provisioning service [service]

Owner: Wallet provider

Coordinates card enrolment, eligibility, identity-and-verification, and token request.

03 Token service provider and token vault [security]

Owner: Network or authorised token service provider

Maps a payment token to the underlying account and manages token lifecycle and domain controls.

04 Issuer digitisation and risk service [control]

Owner: Issuer digital cards and fraud

Decides card eligibility, identity verification, token assurance, and lifecycle action.

05 Merchant wallet acceptance [gateway]

Owner: Merchant payment platform

Accepts tokenised credentials and binds them to the transaction, channel, amount, and merchant.

06 3-D Secure access and authentication domains [external-network]

Owner: Merchant, scheme directory, and issuer access-control owners

Coordinates merchant/acquirer, interoperability, and issuer authentication responsibilities for an online card payment.

07 Card authorisation and clearing rail [external-network]

Owner: Acquirer, network, and issuer

Carries the payment token and transaction credential through normal card authorisation and later clearing.

08 Token, authentication, and fraud operations [operations]

Owner: Issuer, wallet, merchant, and network operations

Investigates provisioning, token lifecycle, authentication, authorisation, and customer-reported events across organisations.

INTERFACES

01 Provisioning request

wallet-user -> wallet-provisioning | api | synchronous

- 02 Issuer eligibility and verification
 - wallet-provisioning -> wallet-issuer | message | asynchronous
- 03 Token issuance decision
 - wallet-issuer -> wallet-token-service | control | asynchronous
- 04 Device token and credential
 - wallet-token-service -> wallet-user | api | synchronous
- 05 Wallet payment
 - wallet-user -> wallet-merchant | api | synchronous
- 06 Authentication request
 - wallet-merchant -> wallet-3ds | message | synchronous
- 07 Issuer authentication
 - wallet-3ds -> wallet-issuer | message | synchronous
- 08 Tokenised authorisation
 - wallet-merchant -> wallet-card-rail | message | synchronous
- 09 Token resolution and assurance
 - wallet-card-rail -> wallet-token-service | control | synchronous
- 10 Lifecycle and fraud event
 - wallet-card-rail -> wallet-operations | event | asynchronous

TRACES AND STRESS CASES

TRACE: Provision and spend a token

1. Start enrolment - Provisioning requested
2. Ask the issuer - Eligibility under review
3. Approve token issuance - Provisioning approved
4. Issue a constrained token - Token active
5. Bind the purchase - Payment context fixed
6. Authenticate when required - Authentication outcome recorded
7. Authorise the tokenised payment - Card authorisation decided

STRESS: Provisioning outcome is lost

Settlement: No purchase settlement has occurred.

Funds: No purchase funds moved.

Owner: Issuer digital-card operations

Safe action: Query the token lifecycle by the original provisioning reference before retry.

STRESS: 3-D Secure is unavailable

Settlement: No card settlement has occurred.

Funds: No issuer authorisation hold is confirmed.

Owner: Merchant payment operations

Safe action: Apply the merchant, issuer, regulatory, and scheme fallback policy; do not label unavailable as authenticated.

STRESS: Token credential is replayed

Settlement: Settlement state of the original attempt must be checked separately.

Funds: A second hold or posting must not be assumed valid.

Owner: Issuer fraud operations

Safe action: Decline the replay, contain the token if policy requires, and correlate the original transaction.