

PAYMENTS SIGNAL REFERENCE ARCHITECTURE

SYNTHETIC / TRAINING ONLY

Payment security, trust boundaries, entitlements, observability, continuity, and recovery

Treat identity, change, secrets, network boundaries, telemetry, continuity, and payment-safe recovery as one control architecture.

Version: Payments Signal reference architecture v1

Reviewed: 2026-07-23

REFERENCE POSTURE

This blueprint shows control responsibilities around payment execution and recovery. It does not define a threat model, cryptographic suite, security-zone count, cloud pattern, recovery target, privileged-access product, data-residency rule, regulatory obligation, or certification outcome for a particular institution.

COMPONENTS

01 Workforce, workload, and participant identity [security]

Owner: Identity and access management

Issues and verifies distinct identities for people, services, devices, counterparties, and network participants.

02 Entitlements and payment authority [control]

Owner: Payment control owner and access governance

Translates job, service, participant, amount, product, and context into an allowed payment action.

03 API, message, file, and network security boundary [gateway]

Owner: Platform and network security

Authenticates, authorises, validates, rate-limits, and records traffic crossing each trust boundary.

04 Cryptographic keys, secrets, and signing service [security]

Owner: Cryptographic security and key custodians

Protects key material and performs controlled signing, verification, encryption, and rotation.

05 Hardened payment runtime and data stores [infrastructure]

Owner: Platform engineering and data owners

Runs payment services with isolation, secure configuration, immutable deployment evidence, backup, and recoverable state.

06 Security and payment observability [data-store]

Owner: Security operations and payment service management

Correlates logs, metrics, traces, business events, control outcomes, and settlement checkpoints without copying secrets or full payment data unnecessarily.

07 Continuity, backup, and recovery orchestration [operations]

Owner: Operational resilience and service owner

Coordinates alternate capacity, dependency recovery, queue control, data restoration, and staged service reopening.

08 Risk, change, testing, and assurance [operations]

Owner: Payment risk, security governance, architecture, and audit

Owns threat, control, dependency, test, exception, incident, and improvement evidence.

INTERFACES

01 Authenticated identity and context

- sec-identities -> sec-entitlements | control | synchronous
- 02 Authorised payment capability
 - sec-entitlements -> sec-boundary | control | synchronous
- 03 Signing and trust service
 - sec-secrets -> sec-boundary | control | synchronous
- 04 Validated payment traffic
 - sec-boundary -> sec-platform | message | asynchronous
- 05 Technical and business telemetry
 - sec-platform -> sec-observability | event | asynchronous
- 06 Boundary security event
 - sec-boundary -> sec-observability | event | asynchronous
- 07 Incident and recovery signal
 - sec-observability -> sec-continuity | event | asynchronous
- 08 Controlled recovery action
 - sec-continuity -> sec-platform | control | operator
- 09 Access policy and review
 - sec-governance -> sec-entitlements | control | batch
- 10 Tested recovery requirement
 - sec-governance -> sec-continuity | control | operator

TRACES AND STRESS CASES

TRACE: Trusted release and recoverable evidence

1. Establish identity - Actor authenticated
2. Prove authority - Action authorised
3. Protect integrity - Trust material current
4. Validate the boundary - Traffic admitted
5. Process in a controlled runtime - Payment action recorded
6. Observe the outcome - Control evidence retained
7. Keep recovery payment-safe - Recovery boundary known

STRESS: Privileged credential is compromised

Settlement: Settlement varies by each affected payment and must be traced.

Funds: Books and external movements must be reviewed individually.

Owner: Security incident command and payment control owner

Safe action: Revoke access, contain sessions, freeze affected authority, and trace every action to payment and settlement evidence.

STRESS: Signing service is unavailable

Settlement: External settlement has not been initiated for queued messages.

Funds: Internal reservations or postings depend on product design.

Owner: Network security and payment operations

Safe action: Queue securely and invoke only the approved alternate signing or connectivity path.

STRESS: Failover restores a stale queue

Settlement: Some payments may already be settled.

Funds: Replaying the queue could duplicate value.

Owner: Incident command, ledger, and payment operations

Safe action: Stop replay and reconcile business keys across queue, ledger, network, and statements.