PAYMENTS SIGNAL REFERENCE ARCHITECTURE
SYNTHETIC / TRAINING ONLY

Swift connectivity, FIN, FINplus, RMA, security-zone, and MT-to-MX coexistence architecture

Shows the business, relationship, identity, interface, network, and operations boundaries that sit between a payment engine and FIN or FINplus.

Version: Payments Signal reference architecture v1
Reviewed: 2026-07-23

REFERENCE POSTURE

This is a logical Swift architecture, not a diagram of one connectivity vendor, interface product, or Customer Security Controls Framework attestation. Exact zone boundaries, products, message support, and contingency options must be checked against the institution's deployment and current Swift documentation.

COMPONENTS

01 Payment core and message preparation [application]
Owner: Payments technology
Creates the approved MT or MX instruction and keeps its lifecycle reference.

02 Relationship Management Application policy [control]
Owner: Swift security administration
Controls whether the institution permits a counterparty to send within the governed Swift relationship and scope.

03 Swift messaging interface [gateway]
Owner: Swift platform operations
Applies queueing, signing, service selection, acknowledgements, and local message controls.

04 Swift secure zone and identity services [security]
Owner: Cybersecurity and Swift security officers
Protects credentials, signing authority, administrative access, and the controlled Swift footprint.

05 Resilient Swift connectivity [infrastructure]
Owner: Network and Swift infrastructure operations
Carries FIN and FINplus traffic through independently recoverable network paths.

06 FIN service [external-network]
Owner: Swift
Transports supported MT messages and returns network validation and delivery evidence.

07 FINplus service [external-network]
Owner: Swift
Transports ISO 20022 messages under the applicable Swift service and usage guideline.

08 Swift operations and security monitoring [operations]
Owner: Swift operations and payment operations
Reconciles local queues, network evidence, security alerts, and business outcomes.

INTERFACES

01 Counterparty authorisation
swift-payment-core -> swift-rma | control | synchronous

02 Authorised release
swift-rma -> swift-interface | control | synchronous

03 Identity and signing authority

swift-security-zone -> swift-interface | control | synchronous

04 Encrypted service traffic

swift-interface -> swift-connectivity | message | asynchronous

05 FIN MT traffic

swift-connectivity -> swift-fin | message | asynchronous

06 FINplus MX traffic

swift-connectivity -> swift-finplus | message | asynchronous

07 Queue and acknowledgement telemetry

swift-interface -> swift-ops | operator | asynchronous

08 Reconciled network outcome

swift-ops -> swift-payment-core | event | operator

TRACES AND STRESS CASES

TRACE: Release one CBPR+ pacs.008 through FINplus

1. Prepare the profiled message - Ready for release
2. Check the relationship - Counterparty authorised
3. Queue and sign - Locally released
4. Carry the service traffic - Network submitted
5. FINplus accepts the message - Network accepted
6. Correlate the acknowledgement - Technical outcome reconciled
7. Update the lifecycle - Submitted to counterparty

STRESS: RMA relationship blocks release

Settlement: No network or settlement submission has occurred.

Funds: Any internal reservation remains under the bank’s unreleased-payment policy.

Owner: Swift security administration and payment operations

Safe action: Keep the message on hold and correct the relationship only through the authorised RMA process.

STRESS: Connectivity fails after local release

Settlement: Unknown; technical uncertainty is not settlement evidence.

Funds: Do not reverse or resend solely because connectivity is down.

Owner: Swift platform operations with payment operations

Safe action: Reconcile the interface queue, delivery state, and network evidence before failover or replay.

STRESS: Unsupported MT after migration milestone

Settlement: No settlement submission has occurred.

Funds: The payment remains unreleased and must not be treated as sent.

Owner: Migration programme and payment product

Safe action: Use the supported native MX path or an explicitly authorised contingency service; do not invent a conversion.