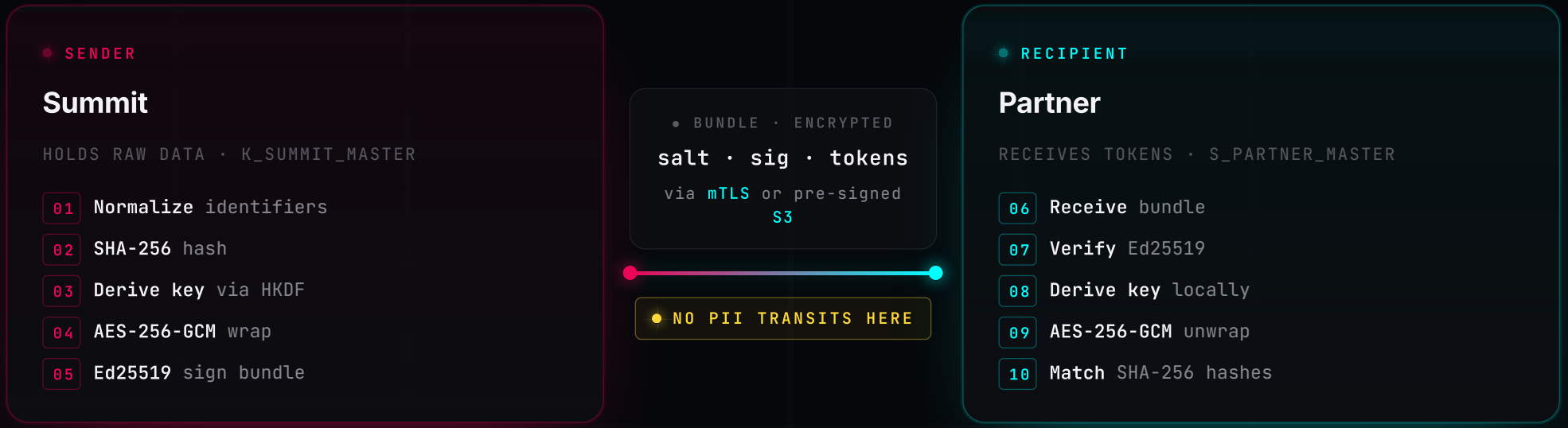
Squyr.

PROTOCOL LIVE
ARCHITECTURE · V1.0 · MAY 2026

SQUYR ARCHITECTURE

Bilateral cryptographic data exchange.

Squyr ships SHA-256 tokens between two parties — sender and recipient — without either party sharing PII, depending on a shared infrastructure vendor, or trusting the other unilaterally. No personally identifiable information ever traverses the wire.



HOW IT WORKS

One protocol. Two environments. Zero PII transit.

Both parties hold their own master cryptographic material in their own KMS infrastructure. Neither party shares raw key material. A **derived key is computed bilaterally** using HKDF-SHA256 over both parties' public commitments and a per-bundle salt.

Identifiers are normalized and hashed with SHA-256 at the Sender. The hashes are encrypted with AES-256-GCM using the derived key. The Sender signs the bundle with Ed25519. The bundle transits over mutual TLS or a pre-signed S3 URL. The Recipient verifies the signature, derives the same key locally, and unwraps the tokens.

Only SHA-256 hashes — wrapped in authenticated encryption — flow between parties.

CRYPTOGRAPHIC PRIMITIVES

SHA-256	FIPS 180-4	Identifier hashing
HKDF-SHA256	RFC 5869	Bilateral key derivation
AES-256-GCM	FIPS 197 · 800-38D	Token encryption
Ed25519	RFC 8032	Bundle authentication

PROPERTIES

- ✓ **No PII transits.** Only encrypted SHA-256 hashes flow between parties.
- ✓ **Bilateral key derivation.** Neither party alone can decrypt the bundle.
- ✓ **FIPS 140-2 compliant primitives.** All algorithms are publicly specified RFCs.
- ✓ **Tamper-evident audit ledger.** Hash-chained, cryptographically signed on both sides.

COMPLIANCE POSTURE

HIPAA SAFE HARBOR · BAA COMPATIBLE · CALIFORNIA CMIA · WASHINGTON MHMDA · FIPS 140-2

Developed by **Summit Audience Segments**
summitaudiencesegments.com

DETAILED PROTOCOL SPEC · SQUYR.COM/DOWNLOADS
CONTACT · INFO@SUMMITAUDIENCESEGMENTS.COM