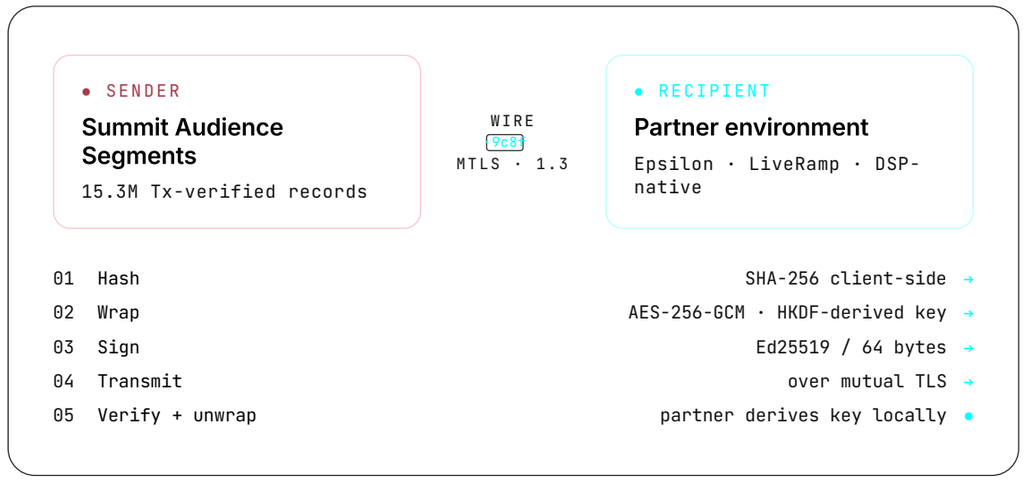
CRYPTOGRAPHIC PROTOCOL · V1.0

Bilateral cryptographic data exchange without the middleware.

Squyr is a protocol for healthcare data partnerships. Identifiers are hashed, tokens are encrypted with bilaterally-derived keys, and nothing personally identifiable ever crosses between parties.

See the demo | Read the white paper | View on docs.squyr.com ↗



PRIMER · 01

What Squyr is.

Squyr is a cryptographic protocol for exchanging healthcare patient identifiers between two parties without either side transmitting personally identifiable information.

Each party holds their own data. Identifiers are hashed client-side using **SHA-256**. The hashes are encrypted using **AES-256-GCM** with bilaterally-derived keys. The encrypted bundle is transmitted, and the recipient unwraps it using key material derived from their own infrastructure. No raw phones, emails, or other PII ever moves between systems.

Squyr was developed by **Summit Audience Segments** to enable healthcare data partnerships at production scale while staying compliant with HIPAA, BAA constraints, and state-level health privacy regulations. The primitives are standard. The architecture is what's distinctive.

Three things to know.

PII never crosses.

Identifiers hash in the partner's browser. Encrypted tokens transit. Raw data never leaves the originating environment.

PRIMITIVE — SHA-256 · AES-256-GCM

Bilateral by design.

Both parties contribute key material. Neither side can unilaterally decrypt the exchange. No third-party middleware required.

DERIVATION — HKDF-SHA256 / RFC 5869

Standard primitives.

SHA-256, HKDF-SHA256, AES-256-GCM, Ed25519. All FIPS 140-2 compliant. All published RFCs. Compatible with standard identity infrastructure.

SIGNING — ED25519 / RFC 8032

PROTOCOL · HOW IT WORKS

Eight steps from raw identifier to partner-side match.

A walk-through of the protocol — what it does, what it uses, and why the architecture matters. No vendor middleware. No PII transit.

Authored	Summit · 2026
Protocol	v1.0
Runtime	Web Crypto API · KMS
Transport	mTLS 1.3 / S3 pre-signed
Status	• PRODUCTION

FLOW · 8 STEPS

01 NORMALIZE — • SENDER

Raw identifiers are normalized — phone numbers to E.164 format, emails to lowercase + trimmed. Both parties produce identical hashes from identical underlying identifiers.

02 HASH — • SENDER

Each normalized identifier is hashed with SHA-256, client-side. Output is the data that will be exchanged — never the raw identifier.

▣ SHA-256 / FIPS 180-4

03 DERIVE — • BILATERAL

A derived key is computed using HKDF-SHA256 over the Sender's master, the Recipient's public commitment, and a per-segment salt. Unique to this exchange.

▣ HKDF-SHA256 / RFC 5869

04 WRAP — • SENDER

Each SHA-256 hash is encrypted with AES-256-GCM using the derived key + unique nonce + segment metadata as AAD. Output is a wrapped token with no recoverable info.

▣ AES-256-GCM / FIPS 197

05 SIGN — • SENDER

The Sender signs the bundle metadata with Ed25519. The signature proves origin and integrity. 64-byte deterministic signature.

▣ Ed25519 / RFC 8032

06 TRANSMIT — • BILATERAL

The bundle — salt, signature, wrapped tokens, metadata — is transmitted over an authenticated channel (mutual TLS or pre-signed S3 URL).

▣ mTLS 1.3

07 VERIFY — • RECIPIENT

Recipient verifies the Ed25519 signature. If invalid, the bundle is rejected and no further processing occurs. Audit log entry written either way.

▣ Ed25519 / verify

08 UNWRAP — • RECIPIENT

REF · 01 CRYPTOGRAPHIC PRIMITIVES — 4 · FIPS-COMPLIANT

SHA-256	Identifier hashing. One-way function — output cannot be reversed to recover the original. FIPS 180-4
HKDF-SHA256	Bilateral key derivation. Combines both parties' master material + per-segment salt. RFC 5869
AES-256-GCM	Authenticated symmetric encryption with AAD. Wraps hashes with the derived key. FIPS 197 · NIST SP 800-38D
Ed25519	Bundle authentication. 32-byte keys, deterministic, ~10× faster than RSA-2048. RFC 8032

REF · 02 SECURITY MODEL — 4 SCENARIOS

Summit (Sender) breached Attacker holds Sender's master + raw data	PARTNER SAFE
Partner (Recipient) breached Attacker holds Recipient's master + delivered tokens	SUMMIT SAFE
Bundle intercepted in transit Attacker holds signed wrapped tokens, no keys	NO RECOVERY
Both parties breached Attacker holds everything from both sides	SEE WHITEPAPER

REF · 03 KEY ROTATION + AUDIT

Salts rotate **per-bundle** automatically. Master material rotates on a configurable schedule — typically 90 days — with on-demand rotation supported. Old derived keys remain valid only for in-flight bundles within a 30-day grace period.

Every step is logged in a **hash-chained, cryptographically signed audit ledger** on both sides. The Recipient's and Sender's audit logs can be cross-verified at any time — providing tamper-evident records of every operation.

LIVE DEMO · V1.0 · ~90 SECONDS RUNTIME

A complete Squyr exchange, cryptographically real, in your browser.

Five cryptographic moments using Web Crypto API. Synthetic patient data — real SHA-256, AES-256-GCM, HMAC-SHA256, Ed25519 operations.

SESSION	SENDER	RECIPIENT
F8F2E82A	SUMMIT	VANTAGE HEALTH

01 CHARACTER-FLICKER HASHING · SHA-256

FIPS 180-4 256 BITS READY

SYNTHETIC PATIENT RECORD · 512 CHARS

```
NAME:        Margaret Rodriguez
DOB:         1987-06-01
PHONE:       (615) 861-6604
ADDRESS:     891 N Milwaukee Ave, Denver, CO 80202
CONDITION:   Major Depressive Disorder
RX:          Gabapentin 300mg TID
NPI:         7841507407
INSURANCE:   Humana Gold Plus
```

512 / 512 chars

SHA-256 OUTPUT · 32 BYTES / 64 HEX CHARS

`9c8f82ac508b2c6c454c17f12cdbe89a184bcb2f7e5b4023be7761e5d60173d6`

9	c	8	f	8	2	a	c	5	0	8	b	2	c	6	c
4	5	4	c	1	7	f	1	2	c	d	b	e	8	9	a
1	8	4	b	c	b	2	f	7	e	5	b	4	0	2	3
b	e	7	7	6	1	e	5	d	6	0	1	7	3	d	6

▣ Generate Hash ↻ Regenerate Data

02 HMAC INTEGRITY CHECK · HMAC-SHA256

RFC 2104 VERIFIED

DATA FLOW · MAC_1 → MAC_2 · 32 BYTES

MAC_1 ⟷ MAC_2 · BILATERAL DATA FLOW STATE IDLE · 32 BYTES READY

✓ Press Verify Integrity to compute and compare MAC_1 vs MAC_2

Verify Integrity

RAIL · 01 CONNECTION STATUS · LIVE

Encryption	AES-256-GCM
Token Signing	EdDSA / Ed25519
Protocol	TLS 1.3
Session ID	F8F2E82A
Key Exchange	PENDING

RAIL · 02 DATA METRICS

Record Size	512 bytes
Hash Value	9c8f82ac…73d6
Hash Valid	• VERIFIED
Bundle Size	684 bytes
Transfers	1

RAIL · 03 SECURITY EVENTS · TAILING

Session initialized	21:38:11
Hash generated 9c8f82ac…	21:38:11
HMAC integrity OK	21:38:11
Bundle signed Ed25519 · 64 bytes	21:38:12
Transmit · mTLS 1.3 684 bytes	21:38:13

RAIL · 04 PROTOCOL FACTS

All cryptographic operations run in your browser via the Web Crypto API. Data is synthetic. No network calls are made.

- NO PII ON THE WIRE

Verify integrity

03 AES-256-GCM ENCRYPTION · BILATERAL EXCHANGE

NIST SP 800-38D 256-BIT KEY KEY EXCHANGE

• SENDER · SUMMIT

NAME	DOB
M. Rodriguez	1987-06-01
PHONE	CONDITION
(615) 861…	MDD
RX	NPI
Gabapentin	7841507407

SHA-256 → AES-256-GCM wrap → bundle

WIRE

·9c8f

MTLS 1.3

• RECIPIENT · VANTAGE HEALTH

a7f3 8c41 2b9e d605 fc88 1734 ed29 b6a4
9132 5d7b ee04 a18f 23c6 7e90 4b15 d8e2
c059 7841 a30b f99d 681e 4502 c7af 1b3d

AES-GCM ciphertext · 96-bit nonce · 128-bit auth tag

▣ Encrypt + Send Inspect bundle

04 ED25519 IDENTITY TOKEN SIGNING · EDDSA

RFC 8032 32-BYTE KEYS SIGNED

Squyr uses Ed25519 (EdDSA curve) for identity token signing. 32-byte keys, deterministic signatures, ~10× faster than RSA-2048 — the modern default.

STEP 1 · KEY PAIR · GENERATED

PUBLIC KEY · JWK · X
B7vK3xQpL9mYz4nRfH8jK2sT5wG6dN8aP3eX1cM9oU4Y

PRIVATE KEY
●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

STEP 2 · MESSAGE · SHA-256 HASH FROM MOMENT 01

9c8f82ac508b2c6c454c17f12cdbe89a184bcb2f7e5b4023be7761e5d60173d6

STEP 3 · ED25519 SIGNATURE · 64 BYTES / 128 HEX CHARS

3f8a4d2b6c91e7f5028a4b6d9c3f1e8a2b5d6c4e9a7f3b1c8d5e2a4f6b9c1e3
7d5e2a4f6b9c1e3a8d4b2c6f9e1a3d5b7c4f8e2a1d6b9c3e5f7a2d4b6c8e1a

⚿ Generate Key Pair ▣ Sign Token ✓ Verify Signature

05 ZERO-KNOWLEDGE PROOF · SIMPLIFIED ZK CIRCUIT

EXPERIMENTAL READY

Proves membership in the audience without revealing the underlying data. Recipient verifies the commitment against the signed bundle.

COMMITMENT	WITNESS	PROOF
0x4b1e9a7c2d8f3...	●●●●●●●● HIDDEN	π = { a, b, c }

— Generate Proof Verify

CRYPTOGRAPHIC REFERENCE

4 PRIMITIVES

</>	HASHING PROTOCOL — SHA-256	FIPS 180-4 ▾
</>	ZK CIRCUIT — SIMPLIFIED PROOF	EXPERIMENTAL ▾
</>	ENCRYPTION SPEC — AES-256-GCM	NIST SP 800-38D ▾

</> IDENTITY TOKEN —	EdDSA / Ed25519	RFC 8032 ▾

AUDIT LOG · HASH-CHAINED LEDGER — • TAILING 5 EVENTS

TIMESTAMP (UTC)	ACTION	DATA HASH	IP ADDRESS	RESULT
2026-05-19 21:38:11	SHA-256 HASH	9c8f82ac508b2c6c…	138.62.115.164	• SUCCESS
2026-05-19 21:38:11	HMAC INTEGRITY	74a49678804e4231…	99.63.161.188	• SUCCESS
2026-05-19 21:38:12	AES-GCM WRAP	3f8a4d2b6c91e7f5…	138.62.115.164	• SUCCESS
2026-05-19 21:38:12	ED25519 SIGN	0b5e21cf94d72a18…	138.62.115.164	• SUCCESS
2026-05-19 21:38:13	BUNDLE TRANSMIT	a7f3 8c41 2b9e…	99.63.161.188	• SUCCESS

REFERENCE DOCUMENTATION

Downloads.

Reference documentation for Squyr. All documents are non-proprietary and may be shared freely with security, legal, and engineering teams during partner evaluation.

Library	3 documents
License	Non-proprietary
Version	v1.0 · 2026
Updated	2026-05-15

PDF · 6 PAGES

Squyr Protocol Whitepaper

Detailed protocol specification. Cryptographic primitives, key derivation, attack scenarios, compliance posture.

2026-05-15 v1.0

Download whitepaper

PDF · 1 PAGE

Architecture One-Pager

Single-page visual overview of the bilateral exchange architecture. Suitable for executive briefings.

2026-05-15 v1.0

Download one-pager

PDF · 2 PAGES

Compliance Posture

HIPAA Safe Harbor framing, BAA compatibility, state-level health privacy considerations, FIPS 140-2 primitives.

2026-05-15 v1.0

Download summary

PARTNERS · GATED

For authorized partners.

Documents below the public line are non-proprietary and reflect the protocol as publicly described. **Implementation details, reference client code, and integration documentation** are distributed separately to authorized partners through docs.squyr.com.

To request partner access, contact your Summit account manager or sign in to the partner portal. SOC 2 Type II report and the external cryptographic audit are available under NDA prior to first paid deployment.

Visit docs.squyr.com ↗ Request partner access

Visit docs.squyr.com ↗ Request partner access

All documents are **cryptographically signed**. Verify signatures via the public key on docs.squyr.com before sharing externally.

View signing key

ABOUT SQUYR

The only company in healthcare with exclusive access to a decade of patient acquisition data.

Operationally generated. First-party. Condition-confirmed. Licensed exclusively for 20 years.

T3 RECORDS

condition-confirmed cohort

EXCLUSIVE LICENSE

2026 through 2046

OPERATING ENTITIES

licensors of the data layer

COMPANY ORIGIN · 01

Built operationally. Licensed exclusively.

Summit Audience Segments is the licensee of a 20-year exclusive dataset built operationally by three healthcare patient acquisition businesses. **The team behind the data is the team running the company.**

For a decade, three operating entities ran condition-specific patient acquisition campaigns across diabetes, sleep apnea, obesity, cardiac, and adjacent conditions. The data they generated was the operational byproduct of running those campaigns. Each entity held its own piece of the funnel.

In 2026, those operating entities collectively granted Summit Audience Segments an **exclusive license to the de-identified data layer** across all three businesses. Summit holds the commercial relationship; the source entities continue operating. The license runs from 2026 through 2046.

The result is the only company in healthcare with exclusive access to a decade of operationally-generated, first-party, condition-confirmed patient acquisition data. Combined with **the Squyr protocol** and the Summit Exchange platform, Summit operates as a vertically integrated patient acquisition company.

PHILOSOPHY · 02

How Squyr was designed.

Squyr is the bilateral cryptographic data exchange protocol that powers Summit's commercial partnerships. Three design principles drove every decision:

01 **No PII should cross between parties in a data partnership.** The architecture enforces this — not just the policy.

02 **No third-party vendor should sit between two parties exchanging data they both legitimately own.** Middleware introduces dependency, cost, and a third point of failure.

03 **The cryptographic primitives should be the most boring possible.** Public RFCs, FIPS-

compliant, broadly implemented. Architectural novelty is acceptable. Cryptographic novelty is not.

TEAM · 03

The team behind the data is the team running the company.

JA

COMMERCIAL STRATEGY & PARTNERSHIPS

Jake Arnold

20 years building patient acquisition infrastructure in healthcare media. Led sales during the rise of one of the largest healthcare-vertical ad networks online, then ran sales at a category leader in pharma DTC media buying. Founded his company in 2015 to operate at the intersection of healthcare consumer acquisition and direct-response strategy — work that produced the partnerships and operating relationships that became Summit's underlying data foundation. At Summit, Jake leads commercial strategy, partnerships, and the platform architecture that turns a decade of operationally-generated patient records into an addressable audience layer. He also owns Provocateur Gallery in Park City, where he lives with his three sons.

G

COMPANY LEAD

Greg

A **two-time founder, two-time exited operator, and eight-time investor** across seed and venture stages. Started his career as a G-10 spot currency trader and credit derivatives broker during the post-2008 derivatives market reconstruction. Shifted to operating roles, running supply chain through growth from $700K to $80M+ in annual revenue. Later co-founded companies (first-to-market ready-to-eat overnight oats, sold to Cedar's Mediterranean Foods in 2019). Has invested across consumer products, biomaterials, fitness, and financial technology — including Newlight Technologies, Betterment, Lume Cube, Zeno Gym, and Barry's. At Summit, Greg leads the company.

J

DATA OPERATIONS & INFRASTRUCTURE

Jordan

The operator behind the data. **18+ years building and running healthcare patient acquisition businesses.** Built the digital acquisition platform that enrolled 25,000+ sleep apnea patients in 18 months. Today Managing Partner & COO of one of the largest national mail-order providers of diabetic testing supplies, serving 50,000+ patients. Founded the direct-response marketing engine specializing in diabetes and sleep health verticals. Both companies are operating entities whose decade of patient acquisition data Summit licenses exclusively. Also co-founded a medical device manufacturer where he holds two issued patents.

GET IN TOUCH · 04

Three paths to a conversation.

BRANDS

Scope a license.

The fastest path is a focused conversation about your condition.

AGENCIES

Multi-brand relationships.

Summit operates as the unbranded sponsor entity for unbranded

PARTNERS

Open to structures.

Summit's data is exclusive. The platform is operational. The protocol

We'll scope a license structure and walk through match rates and cohort sizing.

campaign work that brand clients cannot run directly. Multi-brand relationships across the full data layer are available.

is proprietary. We're open to partnership structures depending on what you're building.

For partnership inquiries or technical questions, contact **Summit Audience Segments** at info@summitaudiencesegments.com.

Get in touch ↗

See the demo →