AXIOM Whitepaper
05//25//2025 | MM//DD//YYYY

AXIOM: How it works and Planned features

Phone: 520.681.8647
E-Mail: inquire@useaxiom.net
Webpage: https://useaxiom.net

Privacy & Security

AXIOM is a next-generation, privacy-first search engine designed for the modern web. From the moment a query leaves the user's browser until results are rendered on screen, AXIOM leverages zero-trust encryption, authenticated transport, and onion-routed scraping to guarantee end-to-end confidentiality and integrity. This whitepaper details AXIOM's architecture, encryption primitives, routing mechanisms, and deployment model, illustrating how we deliver fast, accurate search while preserving user sovereignty.

Traditional search services rely on large, centralized indexers that collect and store user queries in the clear, creating single points of surveillance and attack. As threats evolve—ranging from government subpoenas to large-scale data breaches—users demand a search solution built with security and privacy as foundational requirements, not afterthoughts. AXIOM meets this demand by:

- Encrypting every hop with authenticated, AEAD ciphers
- Enforcing mutual authentication between edge and compute layers
- Leveraging Tor hidden services for untrusted scraping
- Decoupling routing logic via deterministic hashing

AXIOM comprises four primary components:

1. **Client → Ingress Edge**
   - **TLS 1.3** with **AEAD** ciphers (AES-256-GCM or ChaCha20-Poly1305) provides confidentiality, integrity, and forward secrecy for all inbound queries.
2. **Edge Load Balancer**
   - **Rendezvous hashing** (HRW) determines the appropriate backend shard for each request key—ensuring minimal remapping and even load distribution.
3. **Ingress Edge → Backend Cluster**
   - **mTLS** (mutual X.509 authentication) protects the internal network and guarantees only authorized front-ends may invoke search workers.
4. **Backend → External Scraper**
   - **Tor Hidden Service** tunnels scraping traffic through an onion-routed network, preserving backend IP anonymity, while an outer layer of **TLS 1.3** secures the final hop.

All scraped results feed into a Results Parser that filters, ranks, and re-encrypts responses back to the user over TLS.

Transport Layer

- **TLS 1.3** with AEAD ensures each record is both encrypted and authenticated. ECDHE key exchange (X25519) provides forward secrecy.
- **Payload Encryption (Envelope)**
  - Sensitive query bodies (e.g. proprietary keywords or API tokens) are encrypted client-side with a Data Encryption Key (DEK) using AES-GCM. The DEK is itself wrapped by a rotating Master Key from our KMS.
- **Certificate Lifecycle**
  - Automated X.509 issuance/rotation via an internal PKI ensures no expired or compromised certs persist in production.
- **Pepper & Salts**
  - Per-request nonces (salts) and optional server-wide peppers defend against replay and rainbow-table attacks.

Routing & Load Distribution

AXIOM uses **Rendezvous (Highest-Random-Weight) Hashing** to map each request key (e.g. query ID or user fingerprint) deterministically to a backend shard. This approach delivers:

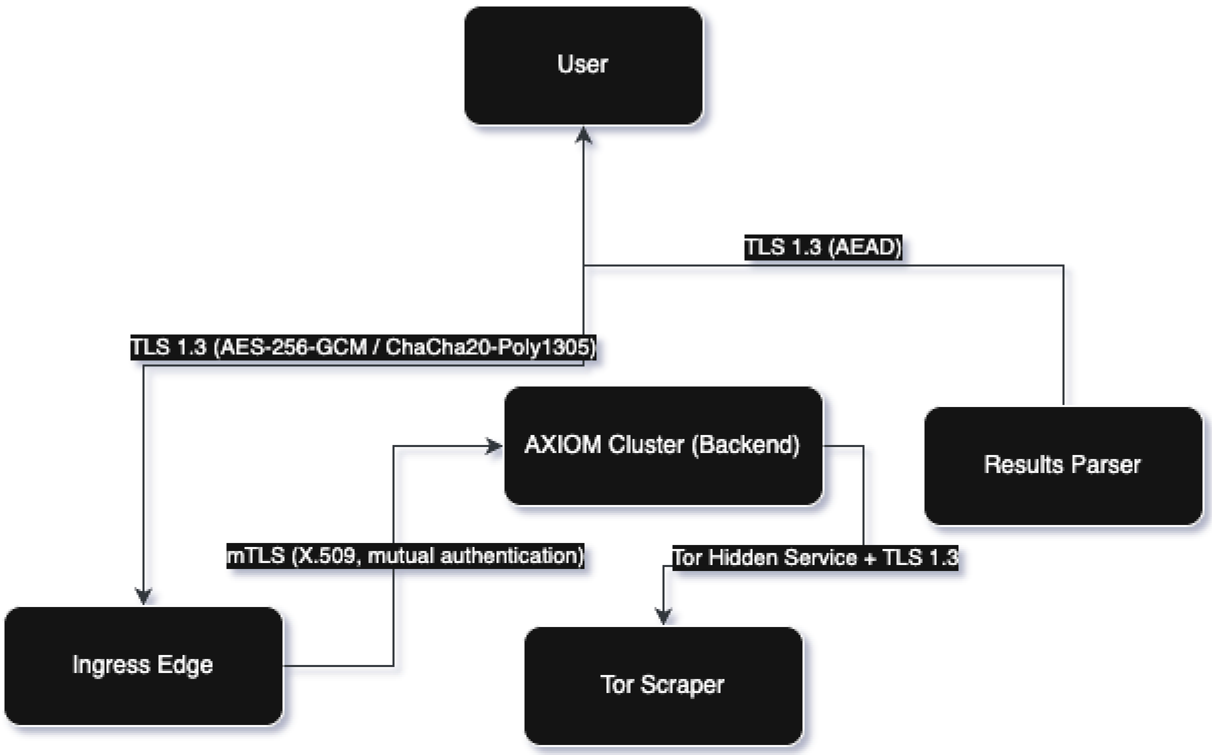
- **Minimal remapping** when nodes are added or removed
- **Uniform distribution** even under skewed key access patterns
- **Fast lookup** with a single hash per node per request

This routing logic lives inside the edge proxy. No encryption primitive maps to a server; instead, hashing guarantees the correct shard.

Security Hardening & Zero-Trust

- **Zero-Trust Network**: No implicit trust between layers — every connection is authenticated and encrypted.
- **Defense-in-Depth**: Even if the edge is compromised, scraped payloads remain encrypted and cannot be manipulated without detection.
- **Onion Routing**: Backend scrapers use Tor hidden services to prevent external observers from linking AXIOM infrastructure to scraping nodes.
- **Audit Logging**: Every TLS session and payload decryption event is logged to an immutable, append-only ledger for forensics.

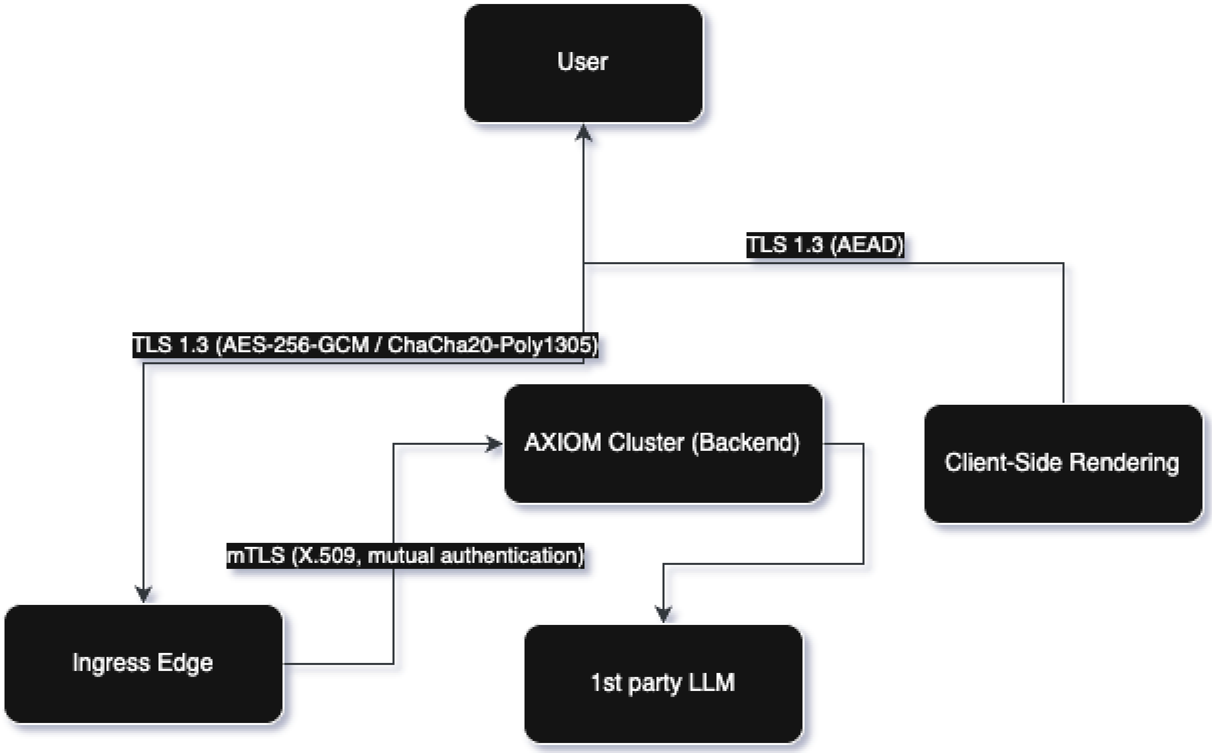
(Diagram: "AXIOM Encryption & Routing Flow" — see page bottom)


User
TLS 1.3 (AEAD)
TLS 1.3 (AES-256-GCM / ChaCha20-Poly1305)
AXIOM Cluster (Backend)
Results Parser
mTLS (X.509, mutual authentication)
Tor Hidden Service + TLS 1.3
Ingress Edge
Tor Scraper

Artificial Intelligence (AI) and Large Language Model (LLM)

AXIOM will have an “AI Overview” feature and use Meta’s Llama 3 8b (8 Billion parameters) that will be run on the AXIOM Cluster/Backend. It may also feature an AI Chatbot/Assistant in future updates. Instead of using an 3rd party Application Programming Interface (API) AXIOM uses a 1st party locally run (locally meaning run on AXIOM owned and operated servers) Large Language Model, with similar encryption to search encryption in and out of the server.

(Diagram: “AXIOM LLM Encryption and Routing Flow” — see page bottom)



Chat Rooms and Communication

AXIOM could possibly (depending on development time and internal/external factors) feature encrypted chat rooms, both user-to-user (Direct Messaging or DMs) and/or small <50 user “rooms”, where multiple users could collaborate or talk to each other. This is so far hypothetical and has not been designed yet.

Browser & Mobile App Considerations (Launch)

AXIOM could feature a Chromium (For Mac/Windows/Linux/Android) based browser, as well as a WebKit (For iOS) based browser, that would feature AXIOM as the default search engine, and have similar features to AXIOM, with privacy and security in mind. AXIOM Launch, as the program would be called, would be a way for users to enhance their browsing experience, in addition to the search experience. This is not a promised feature upon release of the main product, as it would take a lot of development time that may be focused elsewhere.

Advertising & Company Profit

AXIOM will turn a profit using advertisements, however, unlike typical advertisements, the ads will be either

- A. Completely random

or

- B. Based on the search query, not linked to the user in any way.

This will be determined later in development, and any questions/concerns/suggestions should be sent to inquire@useaxiom.net