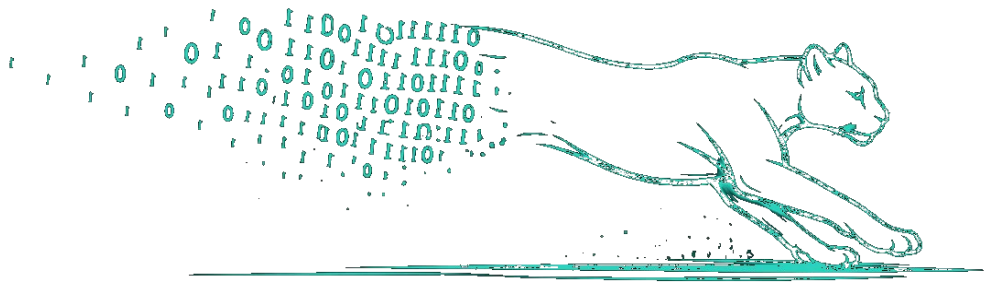
PumaMesh Shield



Post-Quantum Encryption & Key Management

Every byte in transit is encrypted with hybrid post-quantum cryptography and authenticated with TLS 1.3 — node-to-node, relay-to-relay, end-to-end. **FIPS 140-3 validated. CNSA 2.0 compliant. Quantum-safe today.**

FIPS 140-3	ML-KEM	AES-256	TLS 1.3
NIST Certificate #4282	Post-quantum key exchange	GCM authenticated encryption	Every connection, always

The Harvest-Now-Decrypt-Later Threat

Nation-state adversaries are intercepting and storing encrypted traffic today, waiting for quantum computers to break classical key exchange. RSA-2048 and ECDH-P256 — the algorithms protecting most enterprise data in transit — will fall to Shor's algorithm. Data intercepted today with a 10-year sensitivity window is already at risk.

The CNSA 2.0 timeline is clear: all national security systems must transition to post-quantum cryptography by 2030, with software/firmware implementations required by 2025. PumaMesh Shield is compliant today.

Cryptographic Stack

Layer	Algorithm	Details
Key Exchange	**X25519MLKEM768**	Hybrid classical + post-quantum. X25519 for immediate security, ML-KEM-768 for quantum resistance. Always enabled on every connection.
Authentication	**ECDSA / RSA (classical)**	Mutual TLS (mTLS) with node certificates. RSA-4096 or ECDSA-P521 key sizes.
PQ Authentication	**ML-DSA-87 (optional)**	CNSA 2.0 post-quantum digital signatures. Full quantum resistance for node identity.
Payload Encryption	**AES-256-GCM**	Authenticated encryption on every shard. Integrated into QUIC TLS 1.3 record layer.
Cipher Suite	**TLS_AES_256_GCM_SHA384**	The only permitted cipher suite. No fallback to weaker algorithms.
Content Hashing	**BLAKE3**	Per-shard and per-file cryptographic integrity verification. Tamper detection independent of transport.
Gossip Auth	**HMAC-SHA256**	Every gossip message authenticated. Master key with version tracking and auto-rotation.
OpenSSL	**3.5.5 LTS (static)**	FIPS 140-3 validated module, NIST Certificate #4282. Statically linked — no system library dependency.

Node-Level Key Architecture

PumaMesh Shield establishes encryption at the node level. Every QUIC connection between any two nodes — agent-to-hub, agent-to-relay, relay-to-hub — negotiates a unique session via hybrid post-quantum key exchange. The key hierarchy:

✓ **Node Identity Keys** — Each node holds an X.509 certificate (RSA-4096 or ECDSA-P521) for mTLS authentication. Optional ML-DSA-87 certificate for full PQ identity. Certificates are provisioned at install and validated on every connection.

✓ **Session Keys** — Every QUIC connection negotiates ephemeral session keys via X25519MLKEM768 key exchange. New keys per connection — no session reuse. Forward secrecy guaranteed: compromising one session reveals nothing about past or future sessions.

✓ **Master Gossip Key** — A symmetric HMAC key protects all gossip protocol messages. Distributed via gossip with version tracking. Rotated cluster-wide within 30 seconds. Auto-recovery after 5 consecutive HMAC failures.

✓ **Key Escrow** — Hub nodes provide key escrow for disaster recovery. Escrowed keys are encrypted at rest with AES-256-GCM and require explicit administrative action to access.

Encryption in the Data Pipeline

In Transit • TLS 1.3 on every QUIC connection (mandatory, not optional) • AES-256-GCM in the QUIC record layer • Hybrid PQ key exchange on session establishment • Relay nodes forward encrypted bytes — never decrypt • Zero-knowledge relays: no access to plaintext at any hop	**At Rest — Transparent Agent Encryption** • Linux: FUSE virtual filesystem encrypts/decrypts on read/write • Windows: ProjFS projected filesystem with inline encryption • AES-256-GCM with node-level keys • Files appear plaintext to authorized users, encrypted on disk • No application changes — transparent to all file operations
Integrity Verification • BLAKE3 hash per shard on send, verified on receive • BLAKE3 hash per whole file after reassembly • HMAC-SHA256 chain-of-custody in audit trail • Tamper detection independent of TLS • Wire bytes = file bytes confirmed on every transfer	**Key Lifecycle** • Ephemeral session keys — new per QUIC connection • Forward secrecy on every session • Master key rotation cluster-wide in 30 seconds • Key escrow on Hub for disaster recovery • Per-tenant isolation — compromised node contained

Compliance

✓ **FIPS 140-3** — NIST Certificate #4282
✓ **CNSA 2.0** — ML-KEM + ML-DSA compliant
✓ **NIST 800-207** — Zero Trust Architecture
✓ **CMMC 2.0** — Cryptographic control coverage
✓ **ITAR / EAR** — Export-controlled data protection

Crypto Discovery (Puma Pulse)

✓ **11 artifact types** — X.509, private keys, CSRs, keystores
✓ **Weak cipher detection** — RC4, DES, 3DES, deprecated TLS
✓ **Key size validation** — RSA <2048 flagged automatically
✓ **Insecure PRNG** — Weak random number generator detection
✓ **Crypto inventory API** — Full posture assessment endpoint

Quantum-Safe Encryption. On Every Connection. Today.

sales@pumamesh.com | **pumamesh.com**

PumaMesh Inc. | April 2026 | Written in Rust. Built on Open Standards.