

# Phylaxone Protocol Brief

**Distributed Post-Quantum Identity Infrastructure Lucid Tech LLC |  
September 2026 | Confidential**

---

## What Phylaxone Is

Phylaxone is a distributed authentication protocol built for the security environment that is already arriving: quantum-capable adversaries, AI agents acting as autonomous principals, and critical systems that cannot tolerate a single point of failure.

It is not a password manager. It is not a two-factor authentication layer bolted onto existing infrastructure. It is a ground-up rethinking of how identity is proven, how trust is delegated, and how authentication evidence is preserved.

The protocol produces cryptographic proofs, not stored secrets. No authentication credential exists as a value on any server, at any time, in any form. Compromise any collection of nodes below the threshold and you have zero information about any identity in the system.

Phylaxone is NIST FIPS 203/204/205 compliant from day one, making it certifiable for CMMC Level 2, FedRAMP, and National Security System acquisitions under NSA CNSA 2.0 as that standard takes full effect in 2027.

---

## Core Architecture

### Threshold Signing, Not Secret Storage

Traditional authentication systems store a credential somewhere, protect it, and check it when someone claims to hold it. The credential exists. It can be stolen.

Phylaxone uses FROST (Flexible Round-Optimized Schnorr Threshold Signatures, IETF RFC 9591). Each participating node holds a mathematical share of a key. No node holds the key. When an identity needs to authenticate, nodes run a two-round cryptographic ceremony that produces a valid signature, without any node ever assembling the full key. The private key that would produce the signature never exists as a complete value anywhere in the system.

This is a different class of security. The question shifts from “how well is the secret protected?” to “how many independent nodes would an adversary need to compromise simultaneously?” For a 4-of-7 threshold deployment across four geographic regions, the answer is four independent infrastructure environments at the same moment.

### Decentralized Identifiers

Every entity in a Phylaxone network, a person, an organization, an AI agent, or a device, holds a W3C Decentralized Identifier (DID). DIDs are globally unique, cryptographically provable, and stored in no central database. They cannot be revoked by a registrar. They cannot be lost in a vendor breach. Resolution requires no trusted intermediary.

Verifiable Credentials issued against a DID define what that identity is authorized to do, on which systems, for how long, and under what conditions. Expiry is enforced

cryptographically, not administratively.

## Post-Quantum Cryptography Throughout

- **ML-KEM (CRYSTALS-Kyber, NIST FIPS 203)** for all key encapsulation between nodes and clients
- **ML-DSA (CRYSTALS-Dilithium, NIST FIPS 204)** for all Verifiable Credential signatures
- **AES-256** for all symmetric encryption

All three are on the NIST approved algorithm list for new National Security System acquisitions. Phylaxone is the only distributed authentication protocol built post-quantum-first rather than retrofitting compliance onto a legacy architecture.

## Native AI Agent Authentication

AI agents are first-class entities in Phylaxone. Each agent deployment receives a DID. The Verifiable Credential issued to that DID specifies which systems the agent can access, which actions it is permitted to take, which data classifications it can touch, and when that authorization expires.

High-stakes agent actions require threshold approval from a designated human approver set before the signing ceremony completes. Every agent action is attributed to its DID with a cryptographic proof. This is the audit trail that enterprise security teams and government oversight bodies require for AI systems operating on their behalf.

## Adaptive Behavioral Intelligence

Every authentication event produces a behavioral record. The ACI intelligence layer builds a per-identity baseline from these records. Deviations from baseline trigger step-up authentication or alerts. The threshold parameter K adjusts dynamically: a low-risk request from a known identity pattern uses the baseline threshold; an anomalous request requires agreement from more nodes before the signing ceremony completes.

At scale, cross-identity pattern detection identifies coordinated attack campaigns invisible to per-identity monitoring alone.

## Fault Tolerance by Design

If a node is offline, corrupted, or under attack, the signing ceremony continues with the remaining nodes. No manual intervention. No service interruption. The compromised node is excluded automatically. A 4-of-7 deployment continues operating through the simultaneous failure of any three nodes.

---

## Product Suite Built on Phylaxone

**Phylaxone Verify** - Distributed digital authenticity verification network. Submit any document, email, image, or digital artifact; K-of-N independent nodes analyze it for AI generation probability, tamper detection, provenance dating, and process integrity; threshold-agreed results are issued as a hash-bound W3C Verifiable Credential. The credential is publicly verifiable by any party, with no dependency on Phylaxone Verify as a vendor. Built for DFIR evidence chain of custody, regulatory submissions, contract authentication, and compliance report verification.

**AXIOsecurity Enterprise** - Enterprise compliance and AI governance platform. Provides CMMC evidence management, AI agent policy enforcement, identity audit

logging, and the AXIOsecurity certification mark. All certifications are backed by Phylaxone Verify credentials. The AXIOsecurity certification standard is updated continuously from real adversarial behavioral data rather than committee publication cycles.

**ACI Shield** – Consumer-facing AI threat analysis and identity protection. Preemptive detection of AI-generated social engineering, breach monitoring, and conversational security advising. Powered by the Phylaxone identity layer for breach correlation and threat attribution.

---

## Patent Portfolio

Seven provisional patents filed under Lucid Tech LLC / CogniSet LLC (US Application 19/680,696 and related filings):

- **Patent A:** FROST distributed authentication protocol with DID integration
- **Patent B:** AI Agent DID delegation with threshold human approval chains
- **Patent C:** Dynamic K-of-N threshold adjustment by ACI behavioral risk score
- **Patent D:** Consumer AI threat analysis pipeline with identity-threat cross-correlation (ACI Shield)
- **Patent E:** Preemptive attack surface modeling and adaptive threat communication
- **Patent F:** Behavioral VPN and endpoint AI threat detection (ACI Shield consumer layer)
- **Patent G:** Distributed multi-node threshold agreement for digital content authenticity verification with hash-bound Verifiable Credential issuance (Phylaxone Verify)

Patent separation from US 10,650,375 B2 (Worthington, 2020) is documented in detail. Phylaxone uses FROST threshold signing (no stored certificate, no pass/fail vote, no credential rotation) applied to identity authentication (not currency exchange). These are structurally and taxonomically distinct.

---

## Compliance Posture

| Standard                       | Status                           |
|--------------------------------|----------------------------------|
| NIST FIPS 203 (ML-KEM)         | Compliant by design              |
| NIST FIPS 204 (ML-DSA)         | Compliant by design              |
| NIST FIPS 205 (SLH-DSA)        | Roadmap Phase 3                  |
| NSA CNSA 2.0                   | Certifiable for NSS acquisitions |
| CMMC Level 2                   | Certifiable from day one         |
| FedRAMP                        | Certifiable from day one         |
| W3C Verifiable Credentials 2.0 | Native                           |
| IETF RFC 9591 (FROST)          | Native                           |

---

## Build Timeline

Twenty weeks from team formation to full protocol production-ready.

- Weeks 1-6: FROST authentication core, 7-node network
- Weeks 4-10: DID registry, Verifiable Credential system, AI agent authentication
- Weeks 6-12: Post-quantum cryptographic layer (ML-KEM, ML-DSA)
- Weeks 8-16: ACI behavioral intelligence, adaptive threshold, anomaly detection
- Weeks 12-18: Client SDK (JavaScript, Python, Go), node packaging, developer

- portal
- Weeks 14-20: Distributed encrypted storage layer

Estimated build cost: \$166,000 to \$250,000 including engineering team, infrastructure, tooling, and independent security audit.

---

## Contact

Corey Strange, Lucid Tech LLC [phylaxone.com](http://phylaxone.com)

*This document is confidential. Distribution outside the recipient organization requires written authorization from Lucid Tech LLC.*