



A ClareCorp AeroNet VPN – Secure Connectivity and Zero-Trust Framework

Prepared by A Clare, LLC (A ClareCorp)

Principal Creator: Clarence D. Hawkins, MBA

Date: October 2025

License: A ClareCorp Source Code Trust – MIT with Creator Veto

Executive Summary

A ClareCorp's AeroNet VPN is a next-generation, zero-trust connectivity platform engineered for edge, aerospace, and federal environments. It provides encrypted mesh networking, dynamic key rotation, and telemetry-integrated routing for mission-critical data flows. Built to exceed FedRAMP Moderate, FISMA, and NIST SP 800-53 compliance, AeroNet secures inter-node communications within A ClareCorp's EdgeNode and AI Utility Grid frameworks — ensuring integrity, performance, and verifiable trust.

Introduction

In the evolving landscape of distributed intelligence and digital defense, connectivity itself is now a national security vector. A ClareCorp developed AeroNet VPN to create a sovereign-grade communications layer — where encryption, compliance, and performance converge.

Architecture Overview

Core Layer: Manages certificate rotation, peer discovery, and authentication.

Edge Layer: Provides local encryption tunnels for EdgeNode and mobile systems.

Policy Layer: Implements the Digital Trust Charter™ for data integrity enforcement.

Audit Layer: Logs all connections and cryptographic events for traceable validation.

Technical Design

Protocol Base: WireGuard kernel modules with multi-peer support.

Encryption: ChaCha20-Poly1305, Argon2 key derivation.

Telemetry: Encrypted gRPC channels transmitting performance data.

Resilience: Autonomous peer fallback with adaptive rekeying.

Deployment: Terraform-based infrastructure-as-code templates for rapid provisioning.

Security and Compliance

Aligned with FISMA 2024, NIST SP 800-53 Rev. 5, FedRAMP Moderate Baseline, and CFR Title 48 – FAR 9.104-1(a)(2). Each AeroNet configuration includes immutable connection logs, zero-trust enforcement, and hardware identity verification.

Integration with AClareCorp Systems

AeroNet VPN is the communications backbone for AI EdgeNode Architecture, AI Utility Grid (AUG), Forensic Auditing Platform, and Registered Agent & Notary Systems. It enables secure, auditable cross-system communication while maintaining isolation of proprietary data and code.

Governance and IP Protections

Licensed under AClareCorp Source Code Trust – MIT. Subject to Creator Veto: No integration, resale, or API use without written authorization from Clarence D. Hawkins, MBA. Repository notarization and blockchain tracking preserve authorship and ownership.

Deployment Use Cases

Aerospace: Secure inter-drone telemetry mesh (reduces breach risk by 90%).

Energy: Grid sensor VPN isolation (enhances resilience).

Education: Remote lab access tunnels (compliant collaboration).

Finance: Encrypted ACH traceability (secure financial data transport).

Future Developments

Upcoming features include post-quantum key exchange, edge-based VPN analytics dashboard, integration with AClareCorp's Admin Dashboard observability stack, and certification under CNSSI 1253 and DoD STIG standards.

Conclusion

The AeroNet VPN is not just a networking tool — it's a compliance-anchored trust fabric connecting intelligent systems across domains. AClareCorp's engineering philosophy combines federal-grade security, ethical governance, and scalable innovation into a single, future-ready platform.

References

NIST SP 800-53 Rev. 5; FISMA 2024; FedRAMP Moderate Baseline; FAR 9.104-1; CNSSI 1253; AClareCorp Digital Trust Charter™ 2025.