# NATHANAEL LEE RITZ

*Software Engineer, Cloud-native & Distributed Systems Design*

Calgary, AB  •  nathanritz@gmail.com  •  (403) 922-8199  •  nritz.com

## PROFESSIONAL SUMMARY

Passionate about building systems where security, privacy, and usability converge. Deep expertise in multi-cloud federation, zero-trust architecture, and cost-conscious system design—reduced infrastructure costs 77% while improving reliability. Architected and formally modeled a complete security protocol to address secure introduction, identity bootstrap and ongoing proof of identity continuity. Combines operational experience running mission-critical SaaS with rigorous problem-solving skills in applied cryptography. Seeking new challenges in distributed systems ownership where builder mindset meets theoretical rigor.

## CORE COMPETENCIES

**Strategy & Architecture**

( Interoperable Architectures )

( Strategic Systems Design )

**Cloud & Infrastructure**

( Hybrid Multi-Cloud )

( Cost Optimization )

**Security & DevOps**

( Zero-Trust Principles )

( CI/CD Automation )

## PROFESSIONAL EXPERIENCE

### CleanPix Corporation (Digital Asset Management SaaS)

*Owning the technical roadmap and architectural vision for a mission-critical SaaS platform. Responsible for bridging business goals with distributed systems implementation.*

#### Head of Infrastructure & Principal System Designer · 2012–Present

▷ Designed and executed a **federated multi-cloud architecture** across 5 heterogeneous providers. This strategy eliminated single-vendor dependency and drove a **77% reduction in infrastructure opex** while increasing availability.

▷ Led the architectural decomposition of legacy services, introducing an event-driven Kafka backbone that reduced P95 latencies by >1000ms and enabled asynchronous scaling.

▷ Engineered the disaster recovery protocol and cross-provider replication topology (MySQL/Storage), proven in production during a critical storage failure with **zero data loss** and sub-48h RTO.

▷ Established CI/CD and BDD methodologies, moving the engineering culture from manual release cycles to automated, zero-downtime deployments.

#### Product Champion & Integration Lead · 2009–2012

▷ Modernized legacy web application (JSP/JavaScript) to improve user experience and cross-system engagement.

▷ Facilitated alignment between business requirements and technical implementation, crafting user stories for testable integrations.

### Infrastructure Integration Specialist · 2008–2009

▷ Coordinated development, staging, and production rollouts to ensure component interoperability.

▷ Led full system rebuild after hardware transition, reintegrating data flows to maintain business continuity.

### Customer Service Representative · 2007–2008

▷ Managed customer onboarding and guided new users through initial setup.

## INDEPENDENT RESEARCH & PROTOCOL DESIGN

### Factor-based Attestation and Compliance Transport System (FACTS)

**Status:** Independent Research & Development (2025–Present)

*Designing, formally modelled, and implementing a zero-trust identity protocol suite for confidential computing environments.*

▷ **Problem Addressed:** Traditional bearer-token systems create single point of compromise. Built multi-factor attestation system where credentials are derived just-in-time rather than stored, addressing credential exfiltration in autonomous systems.

▷ **Reference Implementation:** Developed Rust toolchain (`facts-cli`) achieving under 2ms attestation ceremonies with HKDF, HPKE (RFC 9180), and Ed25519 cryptographic primitives.

▷ **IETF Engagement:** Published 2 IETF Internet-Drafts. Active participant in OAuth, RATS, and WIMSE working groups on workload identity and attestation architecture.

▷ **Formal Verification:** Applied ProVerif symbolic modeling to prove security properties including forward secrecy, replay prevention, and inert credential theorem under Dolev-Yao adversary assumptions.

▷ **Continuous Attestation:** Engineered TELS (Time-bound Ephemeral Liveness Signals) ratchet providing sub-100ms runtime integrity verification through state-bound key derivation.

## IMPLEMENTATION HIGHLIGHTS

▷ **Production Rust Toolchain:** `facts-cli` achieving <2ms authentication ceremonies with memory-safe cryptographic handling and microsecond key zeroization.

▷ **Formal Security Proofs:** 1,200+ line ProVerif model under Dolev-Yao adversary proving forward secrecy, replay prevention, and computational indistinguishability.

▷ **WebAuthn Integration:** Cross-device passkey portability demo using RFC 9180 (HPKE) and PRF extension, backward-compatible with existing WebAuthn APIs.

▷ **Multi-Transport Demonstration:** Docker orchestration proving protocol composability across TLS 1.3 extension, REST/HTTPS, and air-gapped SAE transport.

# IETF ENGAGEMENT

**draft-ritz-ephemeral-compute-attestation (ECA):** Formal protocol specification for secure machine identity bootstrapping using composable cryptographic factors. Addresses credential theft in ephemeral compute through just-in-time identity derivation.

**draft-ritz-static-artifact-exchange (SAE):** Minimal hardened transport for asynchronous cryptographic exchanges. Zero-parsing invariant eliminates vulnerability classes. Designed for IoT supply chain attestation via S3-style object storage.

**Multi-WG Engagement:** Contributing across OAuth (workload identity), RATS (attestation architecture), WIMSE (Kubernetes/SPIFFE alignment). Addressing cross-cutting concerns in identity-chaining and continuous attestation.

# TECHNICAL PROFICIENCIES

### Protocol Design & Standards

IETF I-D Authorship     FACTS Protocol Suite

OAuth/RATS/WIMSE     W3C (WebAuthn)

### Applied Cryptography

HPKE (RFC 9180)     HKDF / Ed25519

TLS 1.3 (0-RTT, PSK)     OAuth 2.0/DPoP (RFC 9449)

### Formal Methods

ProVerif     Security Property Proofs

Computational Indistinguishability

### Distributed Systems

Multi-Cloud     Kafka Event-Driven

Zero-Trust Design     Disaster Recovery

### Implementation & DevOps

Docker Orchestration     CI/CD / Infrastructure as Code

BDD (Gherkin/Cucumber)

### Languages & Tools

Rust / Python / Java     JavaScript / Bash     CLI Tooling

# EDUCATION

Diploma, Digital Graphics Communication
SAIT (Southern Alberta Institute of Technology), Calgary, AB | 2007
*Foundation in UX/design evolved into a specialization in systems architecture and integration.*