

# Suleyman Musayev

## Senior Security Engineer · IAM, PKI & Anti-Fraud

slmusayev@gmail.com · linkedin.com/in/smusayev · github.com/msuliq · msuliq.github.io  
· Remote · UTC+5

---

### SUMMARY

---

Security engineer specializing in identity, access management, and fraud defense for high-risk environments. Sole architect of the authentication platform at SSL.com (top-10 global PKI vendor), where I designed protections that cut SMS pumping fraud loss to zero and defended against state-level and advanced threat actors. Production experience with OAuth 2.0, OIDC, SAML, certificate lifecycle management, and CVE-aware defense in depth. Open to senior and staff security engineering, IAM, and application security roles.

### EXPERIENCE

---

#### Software Engineer · **SSL.com**

Aug 2023 — Present

Remote · top-10 global PKI vendor · sole architect of auth & identity platform

- **Sole architect** of the authentication and identity platform supporting tens of thousands of daily users; enabled 10× growth in TLS, code signing, and identity certificate issuance.
- Designed fraud detection and abuse prevention combining third-party services with custom analytics on **behavioral patterns, IP intelligence, device fingerprinting, user-agent analysis, and CVE-aware protections**.
- **Cut SMS pumping fraud loss to zero** through dynamic risk scoring, anomaly detection, and adaptive throttling.
- Implemented protections against **account takeover, replay attacks, session hijacking, and SMS abuse**; defended against advanced and state-level threat actors.
- Built safeguards against internal threats: credential leaks, privileged misuse, and insider abuse detection across critical workflows.
- Designed and implemented **OAuth 2.0, OpenID Connect (OIDC), SAML, and session-based** auth, including secure cross-domain flows and external identity provider integrations.
- Built MPIC (Multi-Perspective Issuance Corroboration) compliance per CA/Browser Forum Baseline Requirements; led architecture for distributed auth services, API servers, and audit-logging pipelines.

#### Software Engineer · **Midstay**

Aug 2022 — Jan 2024

Remote · early engineer, 5-person team, ~1k DAU consumer product

- Identified and mitigated **critical security vulnerabilities** across the application stack; led incident response against exploitation attempts by advanced attackers.
- Implemented safeguards to prevent recurrence and improve overall system resilience post-incident.
- Reduced backend latency by up to **5x** and improved user retention by **15%** through performance and product improvements.
- Shipped 4 major product features in 12 months, supporting multiple product pivots.
- Final 5 months were a contract wind-down with gradual transition of responsibilities to the rest of the team while ramping up at SSL.com.

## Quantitative Trading Operations · Private Trading Firm

Mar 2020 — May 2021

Risk management for leveraged portfolio across brokers, markets, and instruments

- Built automated hedging strategies; reduced hedging costs by up to **35%** through strategy optimization and execution improvements.
- Developed strong intuition for risk modeling and decision-making in high-stakes environments — a foundation I apply directly to security threat modeling.

## SKILLS

---

AUTH & IDENTITY	OAuth 2.0, OpenID Connect (OIDC), SAML, JWT, Session-based, SSO, mTLS, Cross-domain Auth, External IdP integration
SECURITY	PKI, Certificate Lifecycle Management, MPIC, Fraud Detection, Account Takeover Defense, Replay Attack Mitigation, Device Fingerprinting, Behavioral Analytics, Insider Threat Detection, CVE-aware Defense
CRYPTOGRAPHY	Memory-hard hashing (Balloon, Yescrypt), Certificate-based Encryption, X.509, TLS
LANGUAGES	Ruby, JavaScript, Python, SQL, C, C++
FRAMEWORKS	Ruby on Rails (4–8), Sinatra, Stimulus, Hotwire
DATA	PostgreSQL, Redis, Sidekiq
INFRASTRUCTURE	Docker, Linux, Nginx, AWS, GitHub Actions, CI/CD

## OPEN SOURCE

---

### **balloon\_hashing & yescrypt**

Ruby implementations of the Balloon and Yescrypt memory-hard password hashing algorithms — modern, GPU-resistant alternatives to bcrypt.

**omniauth\_oidc** — [github.com/msuliy/omniauth\\_oidc](https://github.com/msuliy/omniauth_oidc)

OmniAuth strategy for OpenID Connect with first-class support for Microsoft Entra ID and Cloudflare Access.

**ip\_geo\_lookup** — [github.com/msuliy/ip\\_geo\\_lookup](https://github.com/msuliy/ip_geo_lookup)

IP geolocation lookup for Ruby designed for fraud detection, access control, and request enrichment in security workflows.

### **Contributions**

Authlogic (Ruby authentication framework), openmpic (Multi-Perspective Issuance Corroboration reference implementation).

## WRITING

---

**"How to Stop SMS Pump Fraud From Draining Your Wallet (and Sanity)"** — Medium. Practical playbook for detecting and shutting down SMS pumping attacks, drawn from production experience.

## LANGUAGES & CERTIFICATIONS

---

**Languages:** English (Professional) · Russian (Native) · Turkmen (Native) · Turkish (Conversational)

**Certifications:** Bloomberg Market Concepts (BMC)