

Faraz Ali Zuberi

PRINCIPAL SOLUTIONS ARCHITECT

farazive@gmail.com | +61 435 733 561 | Sydney, Australia
linkedin.com/in/farazalizuberi | Australian citizen

PROFESSIONAL SUMMARY

Principal Solutions Architect with 16+ years building and modernising large-scale, multi-tenant SaaS platforms — 6+ of them at the architect level. I set current- and target-state architecture, advise C-level executives, and stay hands-on across distributed systems, event-driven architecture, identity, and AI/MCP platforms. I lead the hardest cross-domain problems: breaking up monoliths in thin slices, designing Kafka/Debezium CDC pipelines, and building secure OAuth2/PKCE and MCP authorization flows — then turn them into reusable patterns, standards, and reference architectures the whole org runs on.

CAREER HIGHLIGHTS

- 16+ years delivering cutting-edge, cloud-native solutions; 6+ years at architect level
- Sets organisational technical strategy & roadmaps for onshore/offshore teams
- Reports to and advises C-level executives
- Led ISO 27001 accreditation initiatives
- Expert in multi-tenant architectures, identity systems, integration & event-driven platforms
- Expert in domain-driven design, evolutionary architecture & test-driven development

CORE COMPETENCIES

Architecture Leadership

Current-state & target-state (strawman) architecture • Architectural governance across onshore/offshore teams • Reference architectures & architecture decision records (DACI) • C-suite technical strategy & roadmaps • Evolutionary architecture & technical-debt management • Delivery maturity models

Distributed Systems & Events

Event-driven architecture & event streaming • Kafka, Confluent, Redpanda, Debezium CDC • Avro, Schema Registry, schema evolution & compatibility • Domain-driven design, event storming, service right-sizing • Saga patterns & transactional consistency • Multi-region, GDPR-aware data pipelines

Identity & Security

OAuth2, OIDC, SAML, JWT, PKCE • Device Authorization & QR-code login flows • IAM, SCIM, IdP/SP federation • MCP authorization, consent & AI gateways • Kong, Keycloak, API Gateway authorizers • ISO 27001 accreditation; DevSecOps

Platform & Integration

Multi-tenant & single-tenant platform services • Public API, BFF & SPA foundational patterns • Two-way integration / data sync • Config, notifications & shared platform services • API standards & REST design • Reusable Terraform modules & container images

TECHNOLOGIES

Streaming & Data: Apache Kafka, Confluent, Redpanda, Debezium, Avro, Schema Registry, Kinesis, Redshift, Aurora, DynamoDB, RDS/MySQL, Elasticsearch, Redis

Languages: TypeScript, JavaScript, PHP; NestJS, Symfony, Node.js

AWS: API Gateway, Lambda, SNS, SQS, Kinesis, S3, CloudFront, ElastiCache, Cognito, Bedrock AgentCore, ECR, WAF, VPC, IAM

Identity & Gateways: Kong, Keycloak, OAuth2/OIDC/SAML, WSO2 Micro-integrator, Dell Boomi

Platform & DevSecOps: Docker, Kubernetes, Helm, ArgoCD, Jenkins, SonarQube, Artifactory, Terraform

Observability: Elastic, Kibana, Grafana, APM, RUM, JMeter, Vegeta, Temporal.io

PROFESSIONAL EXPERIENCE

ELMO Software Solutions Architect → Principal Solutions Architect

Sydney HQ

Feb 2016 – Present

Progressed from mid-level developer to principal solutions architect over 8+ years, working on the company's most critical platform, security and integration initiatives. Set strategic technical direction and roadmaps for multi-regional onshore and offshore teams, advised C-level executives, and led ISO 27001 accreditation efforts while remaining hands-on in design and delivery.

AI / MCP Authorization Platform — Secure Agent Access to Tenant Data

Principal Architect • 2024–25

- Designed a multi-phase MCP (Model Context Protocol) authorization architecture letting AI agents (Glean, Claude) securely access multi-tenant ELMO data on a user's behalf.
- Architected an AgentCore Gateway fronting N sub-MCP servers, with inbound JWT validation against the TMS identity server, semantic tool routing, and a shared-secret path-based handoff to Kong API Gateway and downstream APIs.
- Specified a hierarchical, per-tenant scope-filtering model: platform-max scopes are constrained by tenant-admin policy and enforced at the /authorize endpoint, so neither agents nor users can exceed organisational limits.
- Adopted public PKCE-only OAuth2 clients (no client secret) to align with the MCP auth standard and enable future MCP-host integrations; designed incremental-consent handling driven by WWW-Authenticate insufficient_scope challenges.
- Defined a hardcoded-consent Phase 1 to cut delivery time, with a clean migration path to the long-term flow; documented developer guidance on shared auth-code issuance and single-source-of-truth scopes.

Stack: AWS Bedrock AgentCore, Kong, TMS Identity Server, OAuth2/PKCE, OIDC, JWT/JWKS, MCP

Event Streaming Platform & CDC Pipeline — Kafka, Debezium & Schema Registry

Architect / DACI Driver • 2024–25

- Drove the event-streaming platform decision (DACI) comparing AWS Kinesis vs Kafka/MSK and DMS vs Debezium+Kafka Connect for CDC; landed on Apache Kafka for both CDC and domain events, with Confluent in evaluation.
- Designed the CDC topology to make domains eventually consistent — moving the platform off shared-database coupling and ad-hoc HTTP/SNS calls toward ordered, retained, replayable event streams.
- Architected the ELMO Kafka Consumer Library (EKCL) for Node.js: multi-topic subscription, schema-registry integration, deserialization, tenancy resolution, Debezium-to-native translation, and idempotent, ACL-scoped, DLQ-backed consumers writing only to sink tables.
- Defined time-based CDC SLOs (binlog → Debezium, Debezium → Kafka, consumer time-lag per partition) targeting p95 < 500ms, replacing brittle offset-based lag with intuitive time-based measurement.
- Established the schema-registry strategy for 400+ source tables across 5+ teams: Avro + Confluent/Glue, FULL_TRANSITIVE compatibility reasoning, auto-registration trade-offs, and a defined process for breaking changes.
- Authored partition/throughput planning guidelines and the org guide on when Kafka is NOT the right choice — preventing premature standardisation on a single broker.

Stack: Apache Kafka, MSK, Confluent, Debezium, Kafka Connect, Avro, Schema Registry, Node.js, MySQL/RDS

Identity Platform — OAuth2 Device Authorization & QR-Code Login

Principal Security Architect & Team Lead • 2023–24

- Led the upgrade of ELMO's identity server to implement the OAuth2 Device Authorization flow, enabling mobile-app login via QR code.
- Implemented IETF specifications and hardened the flow beyond the baseline spec to make authorization more secure.
- Built CI/CD with automated security scanning into the identity delivery pipeline.

Stack: OAuth2 Device Flow, OIDC, PKCE, JWT, CI/CD, automated security scanning

Two-Way Data Sync Platform — Payroll Integration

Principal Architect • 2023–24

- Principal architect for a two-way sync keeping payroll data consistent between two independent systems, partnering with Thoughtworks Australia.

- Designed an event-ledger state machine and a worker/conflict-management service with timestamp-based conflict resolution.
- Delivered on a serverless + container stack with full observability and C4/UML documentation.

Stack: AWS SNS/SQS/API Gateway/Lambda/S3/CloudFront/CloudWatch, DynamoDB, Elasticsearch, Kubernetes/Helm, Redis, WSO2 Micro-integrator, Node.js, PHP

Public API, BFF & SPA Foundational Pattern + Integrations Platform

Principal Architect • 2022–23

- Authored and ratified the Public API / BFF / SPA foundational pattern: per-service-area edge routing (CloudFront), S3-hosted SPAs, BFFs that keep auth secrets server-side in an ElastiCache/Redis session cache, and distributed public API gateways unified under one apex domain.
- Designed the external-party access model (OAuth2 auth-code and client-credentials flows, API-key usage plans, throttling) and standard URL naming across environments and regions.
- Built reusable Terraform modules (elmo-cloudfront-strict, elmo-elasticache, elmo-apigw-public) and a shared configurable BFF container image to raise the baseline and speed up new service areas.
- Built ELMO's reusable, scalable integrations platform between ELMO and third-party vendors, plus the public API architecture and infrastructure.

Stack: AWS CloudFront, API Gateway, Lambda, S3, ElastiCache/Redis, Terraform, OAuth2

IAM Platform & Architectural Governance

Principal Architect • 2021–22

- Principal architect on ELMO's Identity & Access Management system — ELMO acting as both Identity Provider and Service Provider.
- Implemented OpenID Connect, OAuth 2.0, SAML and JWT authorization frameworks, plus SCIM for cross-domain identity management.
- Established the architectural governance framework used to govern onshore and offshore teams.

Stack: OIDC, OAuth2, SAML, JWT, SCIM

Monolith Modernisation — Thin-Slice Refactoring

Architect • Ongoing

- Defined the org's strategy for re-architecting the TMS monolith toward target state using the Strangler Fig and Interceptor patterns — replacing functionality in small, low-risk slices rather than a big-bang rewrite.
- Specified a parallel-run (shadow) approach for high-risk extractions (e.g. payroll tax calculation, permissions engine): run new and old logic side by side, compare results, then cut over once verified.
- Tied modernisation to event interception/streaming so new services develop rapidly without explicit coupling to the legacy emitter.

Stack: Strangler Fig, Interceptor pattern, event interception, DDD

Mariah Solutions Senior Developer → Head of Programming

Jeddah

May 2010 – Jan 2016

Rose to Head of Programming, leading a team that built critical infrastructure and platform systems.

NDC Technologies Temenos T24 Consultant

Aug 2008 – Apr 2010

Core-banking consultant on the Temenos T24 platform.

PUBLISHED STANDARDS & THOUGHT LEADERSHIP

- API Standards (org-wide, 100+ readers) — REST design, versioning, resource modelling, bulk/idempotency, error responses
- Right-Sizing Your Service Areas — a microservice guide on coupling metrics, cohesion & decomposition (Ratified)
- Load Testing & Planning for Goodput — SLOs, peak/average load, replica & goodput calculations
- Authored large parts of ELMO's Architecture Handbook: Architectural Vision & North Star, Architecture Principles, Strawman stack, Reference Architectures (monolith/microservice/serverless), database-tenancy & naming-convention guides, Refactoring the Monolith, Public API/BFF/SPA, Authentication & Token Auth, Event Streaming (Kafka), ELMO MCP

EDUCATION

Bachelor of Computer Sciences — FAST-NU, Pakistan (*Aug 2004 – Jun 2008*)