Leveraging Fine Grained Authorization System to build a Centralized Entitlement Management Service

EXECUTIVE SUMMARY

A large insurance company (a Trevonix customer) managed a diverse ecosystem of financial products, applications, and data services spanning multiple domains and user types—internal employees, advisors, customers, and partners. Over time, the entitlement and access management model evolved organically within each system, resulting in inconsistent authorization logic, redundant configurations, and limited visibility into who can access what across applications.

The business recognized the need for a centralized, dynamic, and auditable entitlement service that can serve all applications while ensuring security, compliance, and agility. To address this challenge, the proposed solution leveraged Fine-Grained Authorization— a scalable, graph-based authorization framework that decouples authorization logic from applications and enables centralized policy control, flexibility, and transparency.

Key Features

- **Centralized Authorization Logic:** Define and manage authorization rules in one place, consumed by multiple applications.
- **Graph-Based Model:** Express complex access relationships In a scalable and high-performance system
- **Dynamic Evaluation:** Policies are enforced at runtime through real-time checks using APIs.
- **Separation of Duties:** Application developers focus on business functionality while access policies are managed centrally by the IAM team.
- **Auditability:** Every access decision and relationship change can be logged and reviewed for compliance.

BUSINESS CHALLENGE

The Insurance Company's application landscape exhibited several recurring authorization challenges:

01 **Decentralized entitlement logic:** Each application embeds its own role and permission model, making it difficult to manage access consistently.

02 **Duplication of roles and permissions:** Business roles (e.g., "Financial Advisor", "Underwriter") are defined differently across systems, causing governance and audit complexity.

03 **Limited visibility:** There is no single authoritative view of user entitlements across all systems.

04 **Compliance risk:** Proving least privilege and separation of duties during audits is manual and error-prone.

05 **Scalability constraints:** Introducing a new product or partner often requires changes to multiple application codebases.

The current model hinders operational agility and fails to meet evolving regulatory expectations for access governance and data protection.

SOLUTION OVERVIEW — FGA

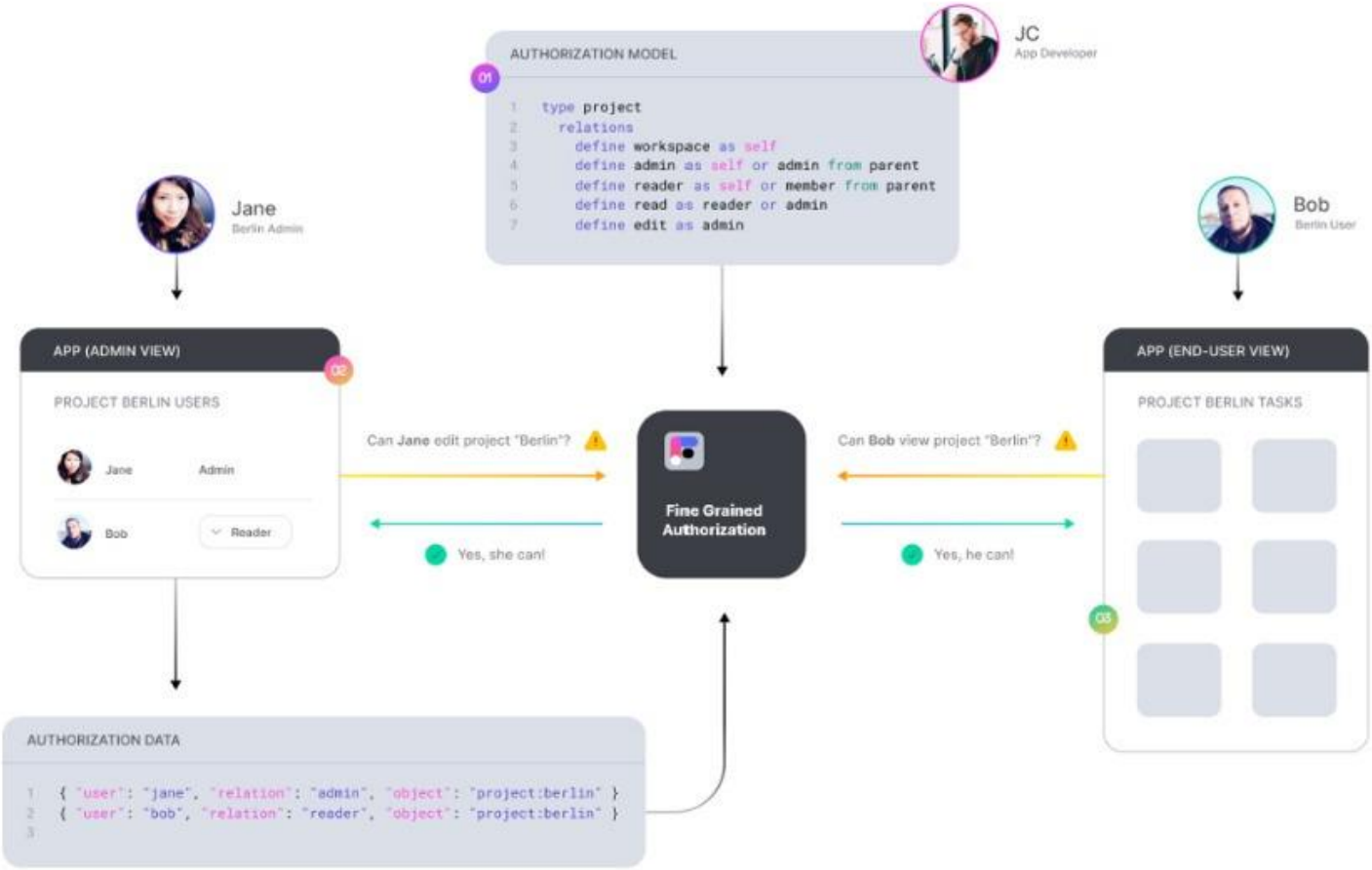
The Fine-Grained Authorization (FGA) solution provides a centralized authorization service that externalizes access control logic from applications and expresses it through a relationship-based model. Instead of hardcoding roles and permissions into applications, FGA uses relationship tuples to define "who has access to what" in a structured and scalable way.

TREVONIX
IDENTITY SIMPLIFIED

TREVONIX
IDENTITY SIMPLIFIED

ARCHITECTURAL APPROACH

- **Single Source of Truth for Entitlements —** All access relationships are stored in FGA system.
- **Decoupled Authorization —** Applications delegate access decisions to the central FGA service through APIs.
- **Attribute-Driven Context —** Access policies are driven by user, resource, and contextual attributes.
- **Composable and Extensible Model —** New entities, roles, and policies can be added without refactoring existing applications.
- **Zero Trust Alignment —** "Never trust, always verify" enforced through real-time entitlement validation.



Each application queries the FGA API at runtime to evaluate permissions such as:

"Can user X approve claim Y?"
"Can advisor A access financial report Z?"

London, UK (HQ) 124 City Road, London, England,EC1V 2NX

New York, USA 803, 447 Broadway, 2n Floor, New York, NY, New York, US,10013

H1-2222 RIICO Industrial Area Sitapura, Jaipur 302905 India

www.trevonix.com +44 (0) 208 660 4918
contact@trevonix.com

IMPLEMENTATION STRATEGY

The deployment at customer was structured into phases to reduce risk and enable incremental adoption.

Phase 1 — Foundational Setup

- Define a common authorization model across departments.
- Map existing roles and permissions from legacy systems.
- Build the initial relationship schema (e.g., user, group, policy, resource).
- Integrate FGA with existing identity systems.

Phase 2 — API Enablement

- Deploy APIs to expose real-time entitlement checks to consuming applications.
- Enable application teams to query entitlements dynamically instead of storing roles locally.
- Introduce policy versioning and testing environments.

Phase 3 — Full Integration & Audit Enablement

- Extend FGA integration to all core finance applications.
- Enable centralized reporting and audit dashboards.

BUSINESS BENEFITS

Centralized Governance:

All entitlements stored and managed in one system for consistent policy enforcement.

Enhanced Security Posture:

Enforces least-privilege and separation of duties dynamically.

Improved Compliance & Auditability:

Enables traceable, real-time reporting on access rights and policy changes.

Agility & Scalability:

Simplifies onboarding of new products or business lines without changing core app code.

Reduced Operational Overhead:

Eliminates redundant authorization logic across applications.

CONCLUSION

By adopting Centralized Fine-Grained Authorization, our customer achieved a centralized, auditable, and scalable entitlement service that significantly improves both security and operational efficiency.

This approach allows the business to modernize its IAM foundation, reduce technical debt across legacy systems, and ensure a consistent, policy-driven authorization experience across all applications.

Phased approach of FGA deployment offers the flexibility to start small — focusing on high-impact use cases, while providing a robust foundation for future enterprise-wide access governance.

London, UK (HQ) 124 City Road, London, England,EC1V 2NX

New York, USA 803, 447 Broadway, 2n Floor, New York, NY, New York, US,10013

H1-2222 RIICO Industrial Area Sitapura, Jaipur 302905 India

www.trevonix.com +44 (0) 208 660 4918
contact@trevonix.com