

Central Permission Engine

Client EPAM
Role Enterprise Architect
Period 2022-03 — 2022-10

CONTEXT

Numerous internal and external systems were used by a mixed population — employees, students, subcontractors — and access was managed separately in each system and process. The decentralization raised cost and the risk of inconsistent or excessive access.

APPROACH

Framed permissions as a shared enterprise capability with a clear contract: consistent identity inputs, central policy evaluation, and governance over rule changes. Designed the target state with the solution architect and formalized requirements for build.

OUTCOME

Defined a centralized permission-engine concept that assigns access by both role-based and resource-based models, replacing decentralized per-system access control with one governed, auditable capability.

- Single permission engine with flexible role- and resource-based configuration.
- Potential to save the organization millions of dollars annually in access-management effort.
- Reduced risk of unauthorized access; stronger position as a reliable partner.

KEY RESULT

Defined a centralized permission engine supporting role- and resource-based access for a mixed user population, replacing scattered per-system access logic with one auditable, governed capability.