Business Requirements Document (BRD)

Project Name: GoCloak

Prepared by: Sajib Jahan

Date: March 10, 2025

# Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Prepared by | Checked by |
| 10/03/2025 | 1.0.0 | Sajib Jahan | Masihur Maruf |

# 1. Project Overview

GoCloak is an open-source, lightweight, high-performance alternative to Keycloak, written in Go. It is designed to provide core Identity and Access Management (IAM) features such as authentication, authorization, and user management for modern applications and services.  
  
**Why GoCloak?**  
Keycloak is powerful but Java-based, which can be heavyweight for many modern DevOps environments. GoCloak offers a more minimal, modular, and easily deployable option in the Go ecosystem. It targets developers looking for Go-native tools, faster performance, simpler deployments, and extensibility via a microservice-friendly approach.  
  
**GoCloak Core Components**  
- REST API for managing realms, users, clients, and roles  
- Admin Panel for internal configuration and management  
- Token service for OAuth2/OIDC-based login  
- Optional UI for user registration and login  
- Modular architecture for extending features like MFA, identity federation, and audit logging

# 2. Business Objectives

- Provide a Go-native, modular IAM system supporting multi-tenancy (realms)  
- Deliver RESTful APIs for integration and automation  
- Build an internal Admin Panel for visual management of IAM resources  
- Enable SSO and centralized session/logout control per realm  
- Focus on performance, scalability, and low-maintenance deployments  
- Promote extensibility through a pluggable design for future add-ons (e.g. MFA, social login, audit logs)

# 3. Scope

In Scope:  
- REST APIs for managing: Realms, Users, Clients, Roles, Groups, Auth Flows  
- Internal Admin Panel: Manage realms, users, roles, logs  
- OAuth2/OIDC token issuance  
- Secure password hashing (e.g., bcrypt)  
- Basic brute-force protection mechanisms  
- User/Admin login UIs  
  
Out of Scope (Initial Release):  
- SAML support  
- Social login (Google, GitHub, etc.)  
- External IdP federation  
- Advanced customizable authentication flows

# 4. Non-Functional Requirements

- Performance: Handle 100k concurrent sessions per realm in cluster mode  
- Security: Enforce HTTPS, CSRF/XSS protection in Admin Panel, secure storage, brute-force protection  
- Portability: Docker-based deployment and container orchestration readiness  
- Scalability: Stateless design supporting horizontal scaling  
- Extensibility: Pluggable provider interface for future modules (e.g., MFA, LDAP, external IdPs)

# 5. Minimum Viable Product (MVP)

- Realm/User/Client/Role CRUD APIs  
- Admin Panel for basic IAM management  
- OAuth2 password grant + refresh token flow  
- JWT issuance and validation  
- Secure password storage with bcrypt  
- Internal audit logging

# 6. Stakeholders

Product Owner: Intimationinc Team  
Backend Engineering: IAM API Team  
Frontend Engineering: Admin Panel UI Team  
DevOps: Infrastructure Team  
QA: Quality Assurance Team

# 7. Milestones

|  |  |
| --- | --- |
| Milestone | Dateline |
| BRD Approval | April 15, 2025 |
| API Design Finalization | April 25, 2025 |
| MVP Development Start | May 1, 2025 |
| MVP Complete | July 10, 2025 |
| Internal Alpha Testing | August 15, 2025 |
| Beta Release | September 5, 2025 |
| Production Release | October 1, 2025 |

# 8. Risks & Mitigation

- High development complexity → Limit MVP scope, prioritize essentials  
- Over-complex Admin Panel → Use modular UI components and keep UX simple  
- Security vulnerabilities → Penetration testing and code audits  
- Scalability challenges → Stateless microservice architecture and load testing  
- Legal/compliance requirements → Include spec-driven tests and security validations

# 9. Success Metrics

- 90%+ test coverage on API and UI  
- API average response < 200ms under load (target: 1k RPS)  
- 3+ realms and 1,000+ users per realm tested in staging  
- Zero critical vulnerabilities in penetration testing  
- Positive user feedback from internal and beta testers