Functional Specification: EJBCA-Based PKI System

Project Name: SecureCorp PKI Infrastructure

Version: 1.0

Document Date: 2025-07-23

Author: [Your Name or Team]

Stakeholders: Security Team, IT Infrastructure, Development Team

# 1. Purpose

This document defines the functional specifications for the implementation of a Public Key Infrastructure (PKI) using EJBCA. The PKI will provide digital certificate management, enabling secure communication and identity verification for internal and external systems.

# 2. Scope

The system will provide the following key services:  
- Certificate Authority (CA) and Subordinate CA provisioning  
- Certificate enrollment and lifecycle management  
- Revocation through CRL and OCSP  
- End-entity (user/system) management via web UI and REST API  
- Integration with LDAP/Active Directory for user lookup  
- Automation of certificate renewal and revocation  
- Auditing and logging

# 3. Stakeholder Requirements

|  |  |
| --- | --- |
| Stakeholder | Requirement |
| Security Officer | Enforce certificate policy and CRL validity |
| DevOps Team | API integration for automated certificate requests |
| SysAdmin | Manage users and certificates via EJBCA GUI |
| End Users | Receive personal or system certificates securely |

# 4. Functional Requirements

4.1 Certificate Authority Setup

- Support creation of a Root CA and at least one Subordinate CA  
- Support ECDSA and RSA key pair algorithms  
- Configure X.509 certificate profiles and issuance policies

4.2 Certificate Lifecycle Management

- Enrollment via Web UI, SCEP, CMP, EST, REST API  
- Server-side key generation  
- Track expiration, renewal  
- Email alerts for expiring certs

4.3 Revocation

- Manual revocation via UI  
- Publish CRLs regularly  
- Real-time OCSP validation

4.4 Authentication and Access Control

- Role-based admin access  
- LDAP/2FA for user auth

4.5 API Access

- Expose endpoints for enrollment, revocation, entity management  
- Require token or mTLS authentication

4.6 Logging and Auditing

- Record issuance, revocation actions  
- Export logs for security audits

# 5. Non-Functional Requirements

- High availability (HAProxy/Kubernetes)  
- Daily DB/keystore backups  
- 100 certs/min performance  
- 10,000+ end-entity scalability  
- NIST, GDPR compliance

# 6. User Interfaces

- Admin Web UI  
- User Portal  
- API for CI/CD automation

# 7. Assumptions and Dependencies

- PostgreSQL or MySQL backend  
- LDAP available  
- Ubuntu 22.04 host  
- HAProxy/NGINX for routing

# 8. Out of Scope

- Code signing certs  
- Smart card automation  
- Governance docs