[Technical Assessment] Auth Services

Status	Draft
Tags	Auth Auth0 Backend
Position	Sr. Authentications Engineer
Created by	JC Navarrete

Introduction

Welcome to our technical assessment for the Authentications Engineer position. This challenge will evaluate your skills in building a secure authentication system that handles user identity and access management for customers.

🌎 Context

🔍 The Challenge

Design and implement a robust authentication system that showcases your expertise in security, scalability, and modern authentication standards. Your solution must demonstrate industry best practices in secure software development—including proper token management, encryption, and thorough security testing. Additionally, show proficiency in software fundamentals like clean code, design patterns, and SOLID principles, as well as cloud architecture concepts like high availability, fault tolerance, and infrastructure as code. Your implementation should reflect strong system design principles including modularity, loose coupling, and separation of concerns.

🎯 Objectives

- Create a secure and scalable authentication and authorization system
- Demonstrate expertise in OAuth 2.0 and JWT implementations
- Implement industry-standard security measures and best practices
- Show understanding of authentication architectures and security patterns
- Provide clear documentation and security testing strategies

📋 Requirements Levels

1️⃣ Basic Level Requirements (1-2 days)

- Implement Core Authentication Flow:
  - Create signup endpoint with email/password validation
  - Build login endpoint with JWT token generation
  - Implement logout mechanism and token invalidation
- Set up Security Fundamentals:
  - Implement password hashing using bcrypt or similar
  - Add basic password validation (min length, complexity)
  - Create rate limiting for authentication endpoints
- Build Protected Routes:
  - Create JWT verification middleware
  - Implement basic error handling
  - Add request validation

2️⃣ Intermediate Level Requirements (2-3 days)

- Add Role-Based Access Control:
  - Implement role and permission system

    - Create middleware for role verification
    - Add endpoint-specific permission checks
- Implement Password Recovery:
    - Create password reset token generation
    - Set up email service integration

3️⃣ Advanced Level Requirements (4-5 days, Nice to Have)

- Implement Two-Factor Authentication:
    - Add TOTP-based 2FA
    - Implement backup codes generation
    - Create 2FA enablement/disablement flow
- Add Security Enhancements:
    - Implement comprehensive audit logging
    - Add automated security headers
    - Create basic monitoring alerts
- Enhance Token Management:
    - Implement refresh token mechanism
    - Add token rotation strategy
    - Create secure session handling
- Implement WebAuthn and Passkeys:
    - Add WebAuthn registration flow
    - Implement passwordless authentication with passkeys
    - Create fallback authentication methods
    - Add device management capabilities

🛠️ Technical Specifications

🔧 Required Technologies

- Backend: Node.js with TypeScript
- Authentication: JWT, OAuth 2.0, OpenID Connect, Webauthn (nice to have)
- Cloud: AWS
- Database: Amazon RDS or DynamoDB

📝 Submission Guidelines

- Create a public GitHub/GitLab repository
- Include comprehensive README.md with:
  - Project setup instructions
  - API documentation
  - Architecture diagrams
  - Testing instructions
- Use feature branches and pull requests
- Commit messages should follow conventional commits format
- You can choose to implement requirements from different levels based on your expertise and time availability - quality is more important than quantity
- Submit your solution by email and we will schedule a review session with the hiring manager to discuss your implementation

🎖️ Evaluation Criteria

- Code quality and organization
- Architecture design
- Documentation quality

- CI/CD Setup
- Security considerations

⏰ Time Expectations

- Basic Level: 1-2 days
- Intermediate Level: Additional 2-3 days
- Advanced Level: Additional 4-5 days

> 💡 Note: While we appreciate thorough implementations, we value quality over speed. Focus on demonstrating your best practices and engineering principles.

Please submit your solution by sharing your GitHub repository link when completed. Good luck!