# Systemdesign

## Entwurf der Architektur der Anwendung, einschließlich Backend- und Frontend-Komponenten

Die Anwendung basiert auf einer 3-Schichten-Architektur. Die Schichten sind ein Frontend, ein Backend und eine Datenbankschicht.

Das Frontend beinhaltet die Präsentation und die Benutzerinteraktion.

Das Backend enthält die Geschäftslogik (Finanzmanagement) und Sicherheitsüberprüfungen (inklusive JWT- und MFA-Management und dynamisches Zugriffskontrollsystem.

In der Datenbank-Schicht wird die Speicherung von Benutzer- und Kontextdaten implementiert.

**Frontend:**

* Technologien: HTML und CSS
* Funktionalitäten:
  + Login-Formualar
  + MFA-Dialog (OTP, Push-Benarichtigung, etc.)
  + Benutzer-Dashboard
  + API-Kommunikation mit dem Backend
  + Finanzverwaltung

**Backend:**

* Technologien: Java Spring Boot
* Services:
  + Authentication Service
    - Verarbeitung von Login-Anfragen
    - Validierung von Benutzernamen und Passwörtern
    - Generierung von JWTs
  + MFA Evaluation Service
    - Analyse von Kontextdaten
    - Entscheidet über Verwendung von MFA
  + JWT Service
    - Erstellt und validiert Tokens
  + Context Service
    - Erfasst und analysiert Kontextdaten (IP-Adresse, Gerät, Standort, etc.)
  + Logging Service
    - Speichert sicherheitsrelevante Ereignisse (z.B verdächtige Logins)

**Datenbank-Schicht:**

* Technologien: MySQL
* Datenmodelle
  + Users: Enthält Benutzerinformationen (Hash des Passworts, MFA-Einstellungen)
  + Context Logs: Speichert Kontextdaten vergangener Logins
  + MFA Configurations: MFA-Status und Regeln für jeden Benutzer

**Systemarchitektur**:

Ein Bild, das Text, Screenshot, Diagramm, Plan enthält.

Automatisch generierte Beschreibung

## Definition der JWT-Strategie für die Authentifizierung, einschließlich Token-Generierung und -Verwaltung

Eine gut durchdachte Strategie für die Verwendung von JSON Web Tokens (JWT) in der Authentifizierung sorgt für eine sichere, skalierbare und leicht wartbare Lösung. Diese Punkt beschreibt die wesentlichen Aspekte der verwendeten JWT-Strategie.

1. Grundlagen von JWT
   1. Aufbau eines Tokens: Ein JWT besteht aus drei Teilen, die durch Punkte getrennt sind
      1. **Header**: Enthält den Algorithmus und Token-Typ (z.B HS256 für HMAC-SHA256
      2. **Payload**: Beinhaltet die Ansprüche (Claims), z.B Benutzer-ID und Berechtigungen
      3. **Signatur**: Gewährleistet die Integrität, basierend auf einem geheimen Schlüssel (bei HMAC) oder einem privaten Schlüssel (bei RSA)
2. Token Generierung
   1. Benutzer-Authentifizierung: Der Benutzer sendet Anmeldeinformationen (z.B Benutzername und Passwort an den Authentifizierungsdienst)
   2. Der Authentifizierungsdienst überprüft die Anmeldeinformationen gegen die Datenbank
   3. Ein JWT wird generiert mit
      1. Header: { „alg“: „HS256“, „typ“: JWT }
      2. Payload: Benutzer-ID, Benutzername, Zeitpunkt der Tokenerstellung, Ablaufdatum und Benutzerrollen
      3. Signature: HMAC-SHA256
   4. Rückgabe an den Benutzer (wenn Kontextanalysen etc. passen)
3. Token-Verwaltung
   1. Der Benutzer sendet das Token bei jeder Anfrage im Authorization-Header
   2. Der Authentifizierungsdienst überprüft
      1. **Signatur**: Das Token wird mit dem geheimen Schlüssel oder dem öffentlichen Schlüssel (bei asymmetrischer Signierung) validiert
      2. Ablaufzeit (exp): Tokens mit abgelaufener Zeit werden abgelehnt
      3. Ansprüche: Überprüfung, ob der Benutzer die notwendigen Berechtigungen hat (z.B. Zugriff auf eine Ressource)
4. Sicherheitsmaßnahmen
   1. Geheimhaltung der Schlüssel
      1. Verwendung eines sicheren, gut geschützten Geheimschlüssels für die Token Signierung
      2. Für asymmetrische Algorithmen (z.B RSA) schützen des privaten Schlüssels
   2. Gültigkeitsdauer
      1. Lebensdauer des Tokens beschränken
   3. Verwendung von HTTPS: Tokens werden ausschließlich über verschlüsselte Verbindungen gesendet.
5. Payload-Prüfung
   1. Tokens mit manipulierten oder unerwarteten Payload Daten werden nicht akzeptiert
6. Token Löschung
   1. Nach Abmeldung wird Token gelöscht

## Planung des dynamischen Zugriffskontrollsystems

## Planung der Multi-Faktor-Authentifizierung (MFA) mit Auswahl geeigneter Methoden (SMS-OTP, biometrische Authentifizierung)