**Database Tables (15+ Tables)**

1. **User**
   * user\_id, username, email, phone, hashed\_password, status (active/inactive), created\_at, last\_login.
2. **Role**
   * role\_id, name (e.g., CUSTOMER, ADMIN, ENTERPRISE\_ADMIN).
3. **Permission**
   * permission\_id, name (e.g., TRANSACTION\_READ, ACCOUNT\_CREATE).
4. **UserRole**
   * user\_id, role\_id.
5. **RolePermission**
   * role\_id, permission\_id.
6. **Address**
   * address\_id, user\_id, street, city, country, type (e.g., billing/shipping).
7. **Enterprise**
   * enterprise\_id, name, tax\_id, registration\_number, status.
8. **UserEnterprise**
   * user\_id, enterprise\_id, enterprise\_role (e.g., owner/employee).
9. **MFA**
   * mfa\_id, user\_id, method (SMS/TOTP), secret, is\_enabled.
10. **AuditLog**
    * log\_id, user\_id, action (e.g., LOGIN, PASSWORD\_CHANGE), timestamp, ip\_address.
11. **KYCInfo**
    * kyc\_id, user\_id, document\_type (e.g., passport), document\_id, verification\_status, verified\_at.
12. **PasswordPolicy**
    * policy\_id, min\_length, require\_uppercase, expiry\_days.
13. **PasswordHistory**
    * history\_id, user\_id, hashed\_password, created\_at.
14. **Notification**
    * notification\_id, user\_id, type (email/SMS), content, status (sent/failed), sent\_at.
15. **UserPreferences**
    * preference\_id, user\_id, language, notification\_settings.
16. **EnterpriseConfig**
    * config\_id, enterprise\_id, max\_transaction\_limit, allowed\_currencies.
17. **OAuth2Client** (Optional)
    * client\_id, client\_secret, scopes, redirect\_uris.

**APIs (RESTful Endpoints)**

**1. User Management**

* POST /api/v1/users: Create a user.
* GET /api/v1/users/{id}: Get user details.
* PUT /api/v1/users/{id}: Update user info.
* DELETE /api/v1/users/{id}: Deactivate a user.
* GET /api/v1/users: List users (admin-only).

**2. Authentication & Authorization**

* POST /api/v1/auth/login: Login with credentials.
* POST /api/v1/auth/logout: Invalidate session/token.
* POST /api/v1/auth/refresh-token: Refresh JWT.
* POST /api/v1/auth/reset-password: Initiate password reset.
* POST /api/v1/auth/change-password: Update password (authenticated).

**3. Role & Permissions**

* POST /api/v1/roles: Create a role (admin).
* POST /api/v1/roles/{id}/permissions: Assign permissions to a role.
* GET /api/v1/users/{id}/roles: Get a user’s roles.

**4. Enterprise Management**

* POST /api/v1/enterprises: Create an enterprise.
* POST /api/v1/enterprises/{id}/users: Add user to enterprise.
* GET /api/v1/enterprises/{id}/users: List enterprise users.
* PUT /api/v1/enterprises/{id}/config: Update enterprise limits.

**5. MFA**

* POST /api/v1/mfa/enable: Enable MFA (e.g., TOTP/SMS).
* POST /api/v1/mfa/verify: Verify MFA code.

**6. KYC**

* POST /api/v1/kyc: Submit KYC documents.
* GET /api/v1/kyc/status: Check verification status.

**7. Audit & Compliance**

* GET /api/v1/audit-logs: Fetch logs (admin-only).

**8. Preferences**

* PUT /api/v1/preferences: Update user settings (e.g., language).

**Advanced Features**

1. **Security**
   * JWT/OAuth2 for stateless auth.
   * Rate limiting (e.g., 5 login attempts/minute).
   * Encryption for sensitive fields (e.g., KYC documents).
2. **Compliance**
   * GDPR (right to erasure), PCI-DSS (audit logs), KYC checks.
3. **Scalability**
   * Database sharding by user\_id or enterprise\_id.
   * Caching for frequent queries (e.g., user roles).
4. **Monitoring**
   * Track API latency, error rates, and security events.

**Optional Additions**

* **Webhooks**: Notify other services on user/enterprise events.
* **SSO Integration**: Support SAML/OIDC for enterprise users.
* **GraphQL**: For flexible querying of user data.