**1. Business & Project Context**

**Project Overview:**

* What is the primary business goal of this authentication system?
* What type of mobile application is this (B2C, B2B, internal employee app)?
* What's the timeline and any hard deadlines?
* What's the budget for Azure services (B2C has transaction-based pricing)?
* Are there any compliance requirements (GDPR, HIPAA, SOC 2, industry-specific)?

**User Base:**

* How many users do you expect (current and future projections)?
* What's the geographic distribution of users?
* Are users internal employees, external customers, or both?
* What's the expected authentication volume (logins per day/month)?

**2. Identity Provider Requirements**

**Supported Authentication Methods:**

* Which identity providers do you need? (You mentioned Azure AD and Google, but are there others?)
  + Social: Google, Facebook, Apple, Microsoft, LinkedIn, Twitter?
  + Enterprise: Azure AD, other SAML/OIDC providers?
  + Local accounts: Email/password, phone number?
* Do you need different providers for different user types?
* Any specific priority or preferred default provider?
* Should users be able to link multiple authentication methods to one account?

**Enterprise Integration:**

* Do you have existing Azure AD/Entra ID tenant(s)?
* Single tenant or multi-tenant Azure AD?
* Do you need to support multiple organizations/tenants?
* Any existing identity infrastructure (ADFS, Okta, Ping, etc.)?

**3. User Experience & Flows**

**Authentication Flows:**

* Sign-up and sign-in (combined or separate)?
* Self-service password reset required?
* Email verification required during sign-up?
* Phone number verification needed?
* Progressive profiling (collect info over time vs. all at once)?

**User Attributes:**

* What user information needs to be collected during registration?
  + Basic: Email, name, phone number?
  + Extended: Address, date of birth, preferences?
  + Custom attributes specific to your business?
* Which attributes are mandatory vs. optional?
* Should attributes differ by identity provider?

**Branding & UI:**

* Do you want custom branding on the authentication pages?
* Any existing brand guidelines (colors, logos, fonts)?
* Need custom HTML/CSS for sign-in pages?
* Multi-language support required? Which languages?
* Any accessibility requirements (WCAG compliance)?

**4. Mobile Application Details**

**Platform Specifics:**

* Which mobile platforms: iOS, Android, or both?
* Native apps or cross-platform (React Native, Flutter, Xamarin)?
* Minimum supported OS versions?
* Any existing authentication implementation to migrate from?

**Token Management:**

* How long should access tokens be valid?
* Refresh token requirements and expiration?
* Should tokens be automatically refreshed or require user action?
* Offline access requirements?

**Deep Linking:**

* What should the redirect URI scheme be?
* Any existing app URL schemes to accommodate?
* Universal links (iOS) or App Links (Android) needed?

**5. Security Requirements**

**Authentication Security:**

* Multi-factor authentication (MFA) required?
  + For all users or specific scenarios?
  + Which methods: SMS, authenticator app, email, hardware tokens?
* Password policy requirements?
  + Complexity, length, expiration?
* Account lockout policies after failed attempts?
* Session timeout requirements?

**Conditional Access:**

* Do you need device-based policies (managed devices only)?
* Location-based restrictions?
* Risk-based authentication (detect suspicious sign-ins)?
* Specific IP whitelisting/blacklisting?

**Data Protection:**

* Where should user data be stored (geographic requirements)?
* Data residency regulations to comply with?
* How long should user data be retained?
* GDPR "right to be forgotten" implementation needed?
* Encryption requirements beyond defaults?

**6. Authorization & Permissions**

**API Integration:**

* Will the mobile app call backend APIs?
* Are these your own APIs or third-party?
* What authorization model: OAuth 2.0 scopes, roles, claims?
* Need separate API app registrations?

**Role-Based Access Control (RBAC):**

* Do you need user roles (admin, user, premium, etc.)?
* Where should roles be managed (B2C, backend, both)?
* Custom claims needed in tokens?
* Group-based permissions?

**7. User Management**

**Administration:**

* Who will manage users and policies?
* Need admin portal for user management?
* Self-service account management features?
  + Profile editing
  + Password changes
  + Account deletion
  + Export personal data

**User Migration:**

* Existing user base to migrate?
* How many users and from which system?
* Password migration strategy (reset or seamless)?
* Bulk import requirements?

**8. Integration & APIs**

**Backend Services:**

* What backend services will authenticate against B2C?
* REST APIs, GraphQL, or both?
* Microservices architecture?
* Need token validation on backend?

**Third-Party Integrations:**

* CRM integration (Salesforce, Dynamics)?
* Analytics platforms (Google Analytics, Mixpanel)?
* Marketing automation tools?
* Customer support systems (Zendesk, Intercom)?

**Webhooks & Events:**

* Need real-time notifications for user events?
* Which events to track (sign-up, sign-in, profile changes)?
* Custom business logic during authentication (API connectors)?

**9. Monitoring & Support**

**Logging & Analytics:**

* What authentication events need to be logged?
* Audit trail requirements?
* Real-time monitoring needed?
* Integration with existing logging (Azure Monitor, Splunk, ELK)?

**Error Handling:**

* How should authentication errors be communicated to users?
* Support for troubleshooting failed sign-ins?
* Alerting for authentication failures or anomalies?

**Performance:**

* Expected response time SLAs?
* Peak usage patterns and load requirements?
* Failover and disaster recovery requirements?

**10. Testing & Deployment**

**Environments:**

* How many environments needed (dev, staging, prod)?
* Separate B2C tenants per environment?
* Testing strategy for authentication flows?

**Deployment:**

* Deployment process and approvals?
* Rollback strategy if issues occur?
* Blue-green or canary deployment?
* Maintenance windows acceptable?

**11. Cost & Licensing**

**Budget Considerations:**

* Monthly active users (MAU) estimates for B2C pricing?
* Premium P1 or P2 features needed (Identity Protection, Conditional Access)?
* Budget for additional Azure services (App Insights, Key Vault)?

**12. Future Requirements**

**Roadmap:**

* Planned features in next 6-12 months?
* Additional platforms (web app, desktop)?
* Additional identity providers?
* Passwordless authentication (FIDO2, Windows Hello)?
* Biometric authentication requirements?

**Scalability:**

* Expected growth in user base?
* International expansion plans?
* New product lines or services?

**Design Document Structure Template**

Based on the answers, your design document should include:

1. **Executive Summary**
2. **Business Requirements**
3. **Architecture Overview** (diagrams!)
4. **Identity Provider Configuration**
5. **User Flows & Journey Maps**
6. **Security & Compliance**
7. **Mobile App Integration Specifications**
8. **API & Backend Integration**
9. **User Management & Administration**
10. **Monitoring & Operations**
11. **Testing Strategy**
12. **Deployment Plan**
13. **Cost Estimates**
14. **Risk Assessment & Mitigation**
15. **Timeline & Milestones**
16. **Appendices** (config files, code samples)

Would you like me to create a design document template with these sections that you can fill in based on your client's answers?