Authentication Flow:

1. User clicks "Sign In" → Redirected to Microsoft Entra ID login page

2. User enters credentials → Microsoft validates identity

3. OAuth 2.0 Authorization Code → Sent back to your app

4. Token Exchange → App exchanges code for access/ID tokens

5. Session Creation → User logged in with secure cookies

Technologies Used:

| Component | Purpose |

|-----------------------|----------------------------------------------------------|

| Microsoft Entra ID | Identity Provider (IdP) - manages users & authentication |

| OAuth 2.0 | Authorization protocol - handles permissions |

| OpenID Connect (OIDC) | Authentication layer on top of OAuth 2.0 |

| PKCE | Security enhancement for OAuth flow |

| JWT Tokens | ID tokens containing user information |

What Entra ID Provides:

- ✅ User Authentication - Corporate/Microsoft accounts

- ✅ Single Sign-On (SSO) - One login for multiple apps

- ✅ User Profile Data - Name, email, department, etc.

- ✅ Role Management - Admin, User, Manager roles

- ✅ Multi-Factor Authentication - If configured

- ✅ Conditional Access - Location/device policies

Application Components:

Your Next.js App Microsoft Entra ID

│ │

├─[Sign In]──────────────────────────►│ Login Page

│ │

│◄─────────[Authorization Code]────────│

│ │

├─[Exchange Code for Tokens]─────────►│

│ │

│◄─────────[Access & ID Tokens]────────│

│ │

└─[Create Session with User Info]

Key Integration Points:

1. Redirect URI - Where Microsoft sends users after login

- Must be registered in Entra ID

- Example: http://localhost:3000/api/auth/callback

2. Client ID & Secret - App credentials from Entra ID

- Identifies your application

- Authenticates token requests

3. Tenant ID - Your organization's ID in Microsoft cloud

- Single-tenant: Only your org's users

- Multi-tenant: Any Microsoft account

Security Features:

- HttpOnly Cookies - Prevents JavaScript access to sessions

- CSRF Protection - Prevents cross-site attacks

- Token Validation - Verifies tokens are from Microsoft

- Secure Sessions - Encrypted JWT session data