KT Session – Microsoft Entra ID OAuth Flows

1. Identity Basics and Tokens

- Microsoft Entra ID is an Identity Provider that authenticates users and applications.
- OAuth 2.0 allows secure API access using access tokens instead of passwords.
- ID Token is used for authentication (who the user is).
- Access Token is used for authorization (what can be accessed).

2. Delegated vs Application Permissions

- Delegated Permissions (Scopes) are used when a user is signed in.
- Permissions are granted on behalf of the user.
- Token contains 'scp' claim.
- Application Permissions (App Roles) are used when no user is involved.
- App runs as itself and token contains 'roles' claim.

3. Authorization Code Flow with PKCE

- Used for web apps, SPAs, and mobile apps with user login.
- PKCE secures the authorization code exchange.
- User logs in, app gets auth code, exchanges for access token.
- Uses Delegated Permissions (Scopes).

4. Client Credentials Flow

- Used for background services and daemon applications.
- No user login involved.
- App authenticates using client ID and secret or certificate.
- Uses Application Permissions (App Roles).

5. On-Behalf-Of (OBO) Flow

- Used when one API calls another API on behalf of a user.
- Frontend gets user token and calls API A.
- API A exchanges token to get a new token for API B.
- Maintains user context across services.
- Uses Delegated Permissions (Scopes).

6. Flow Comparison

Flow	User Involved?	Permission Type	Token Claim	Best For
Auth Code + PKCE	Yes	Delegated (Scopes)	scp	Web, SPA, Mobile apps

Client Credentials	No	Application (Roles)	roles	Background services
OBO Flow	Yes	Delegated (Scopes)	scp	API to API with user context

End of KT Session Guide