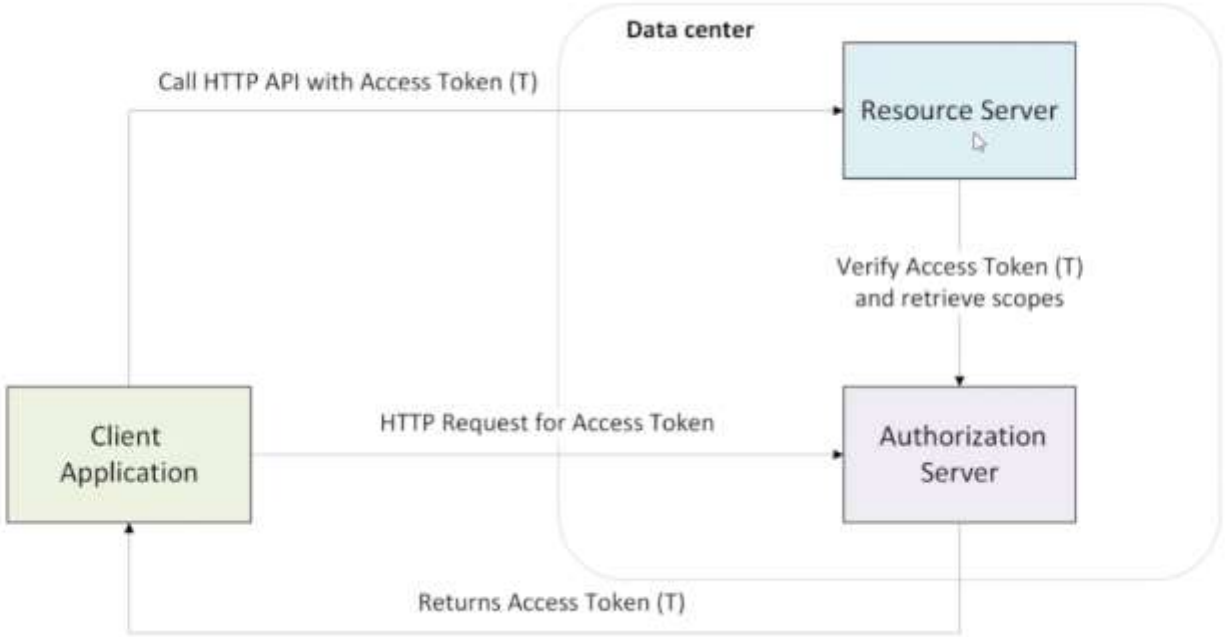
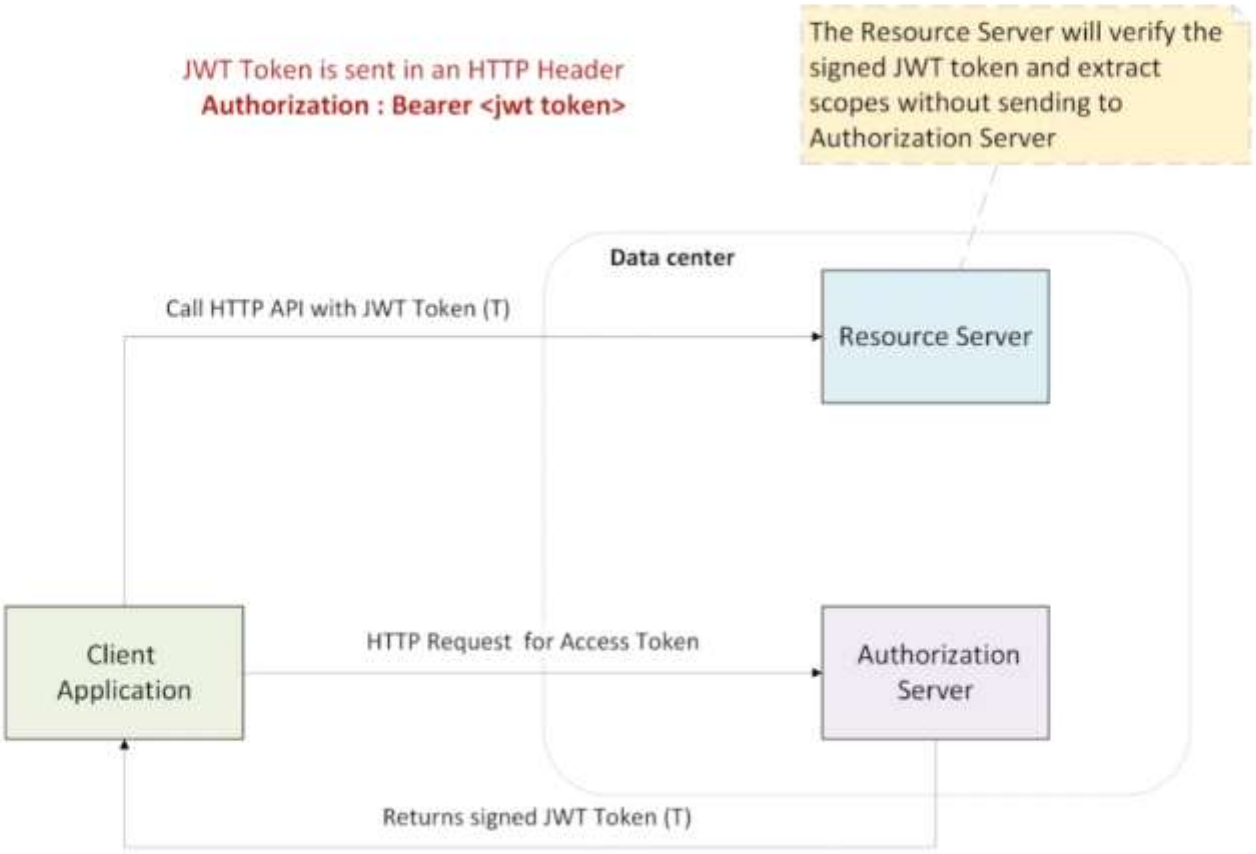
OAuth 2.0 - Opaque Token

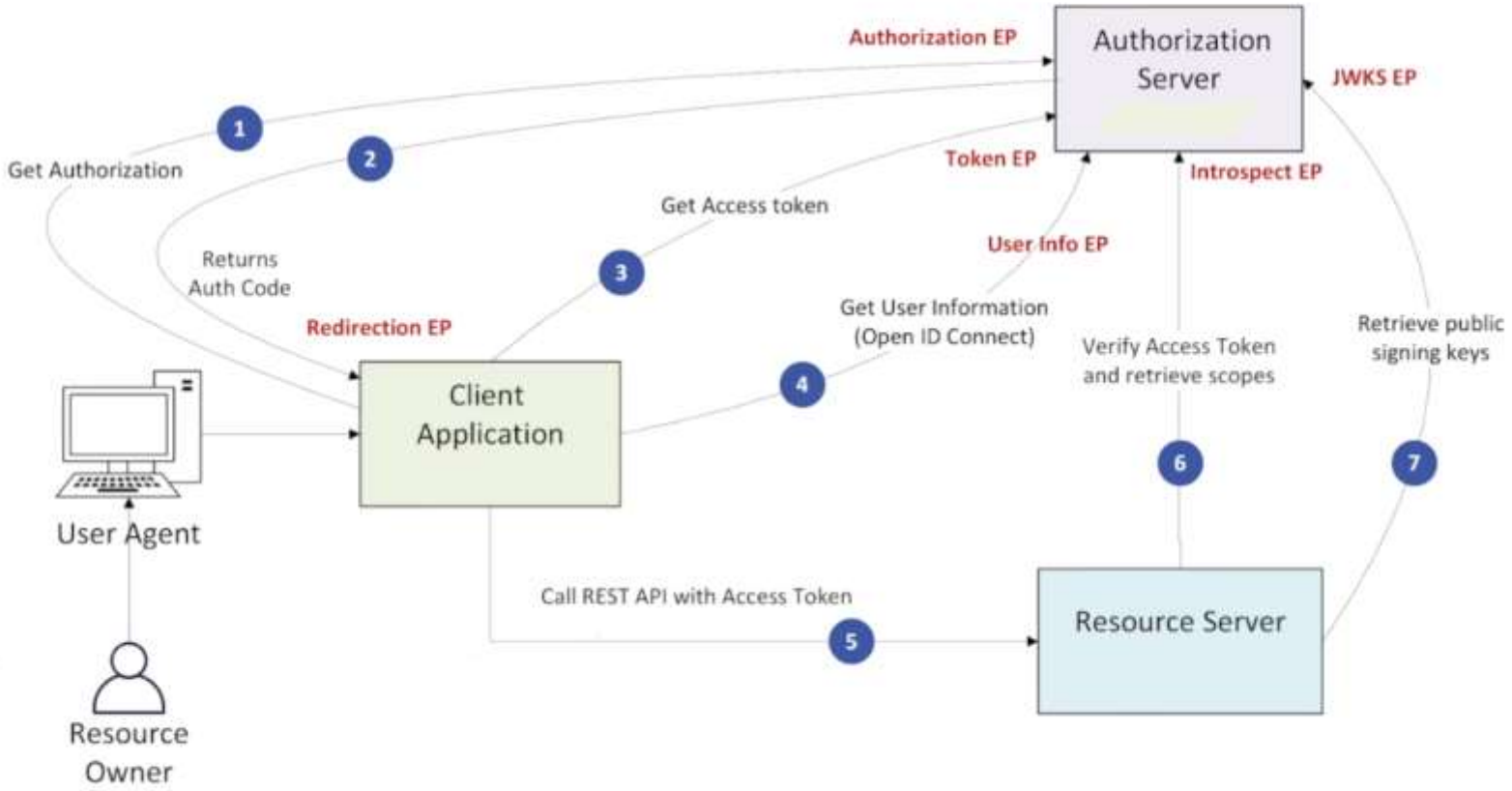
Access Token is sent in an HTTP Header
Authorization : Bearer <token>



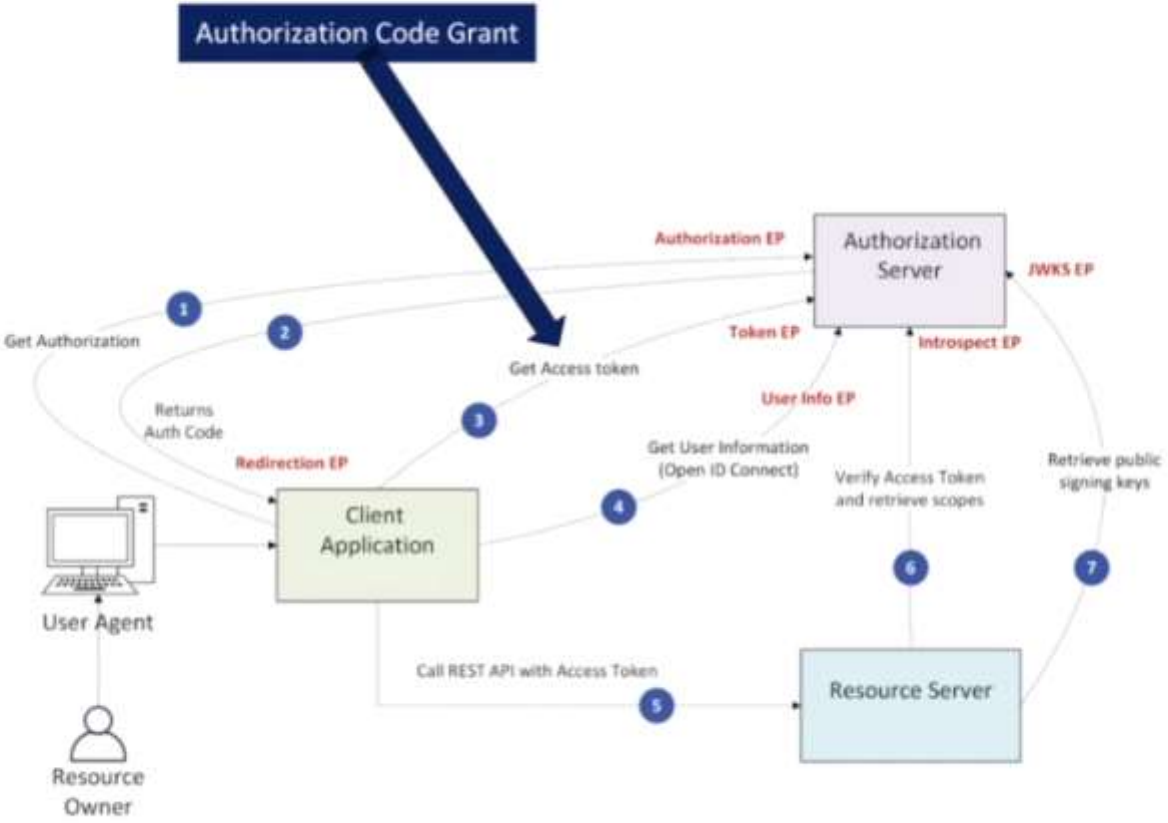
OAuth 2.0 - JWT Token



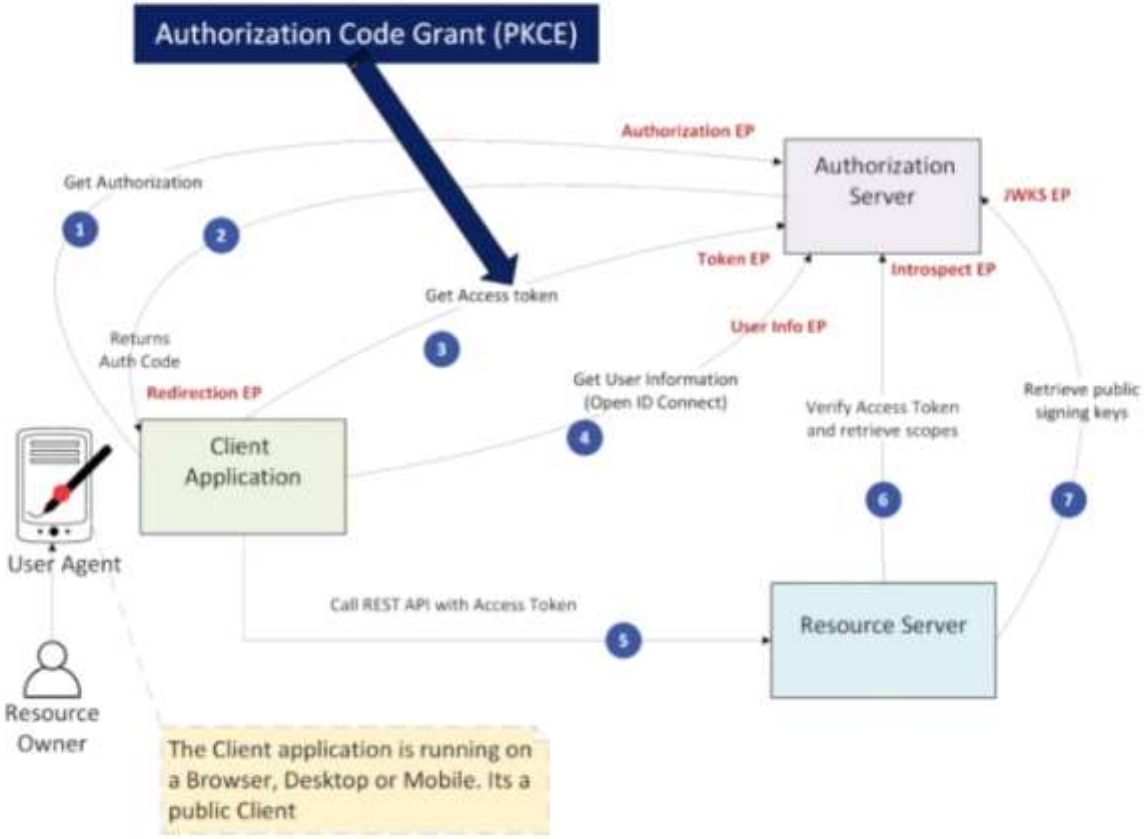
OAuth 2.0 - Endpoints (EP)



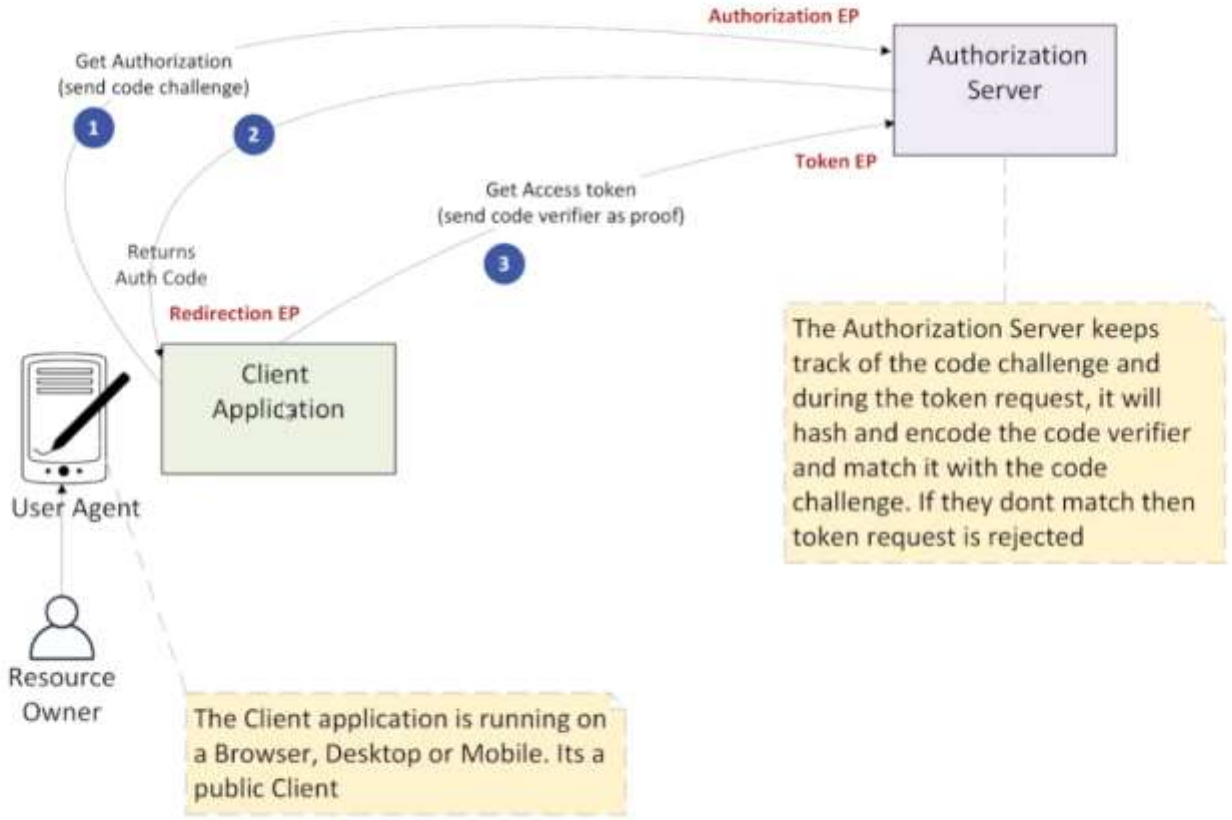
OAuth 2.0 - Authorization Code



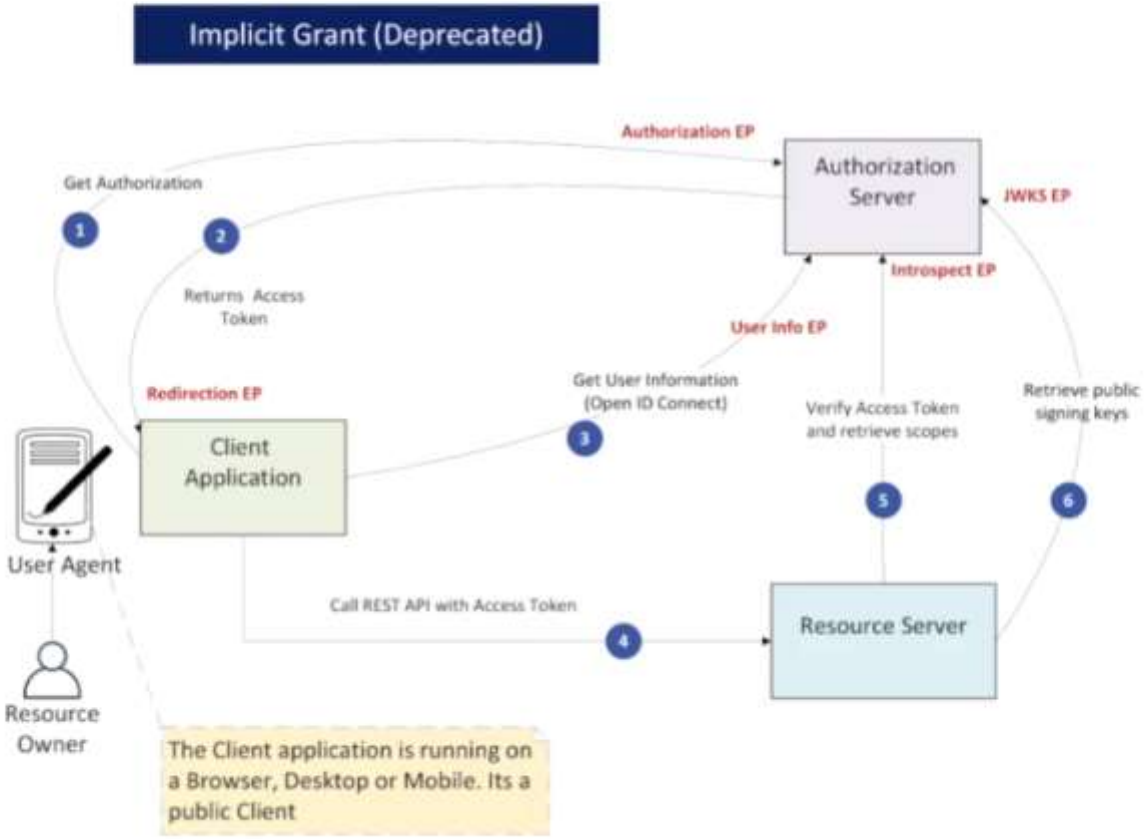
OAuth 2.0 - Authorization Code (PKCE)



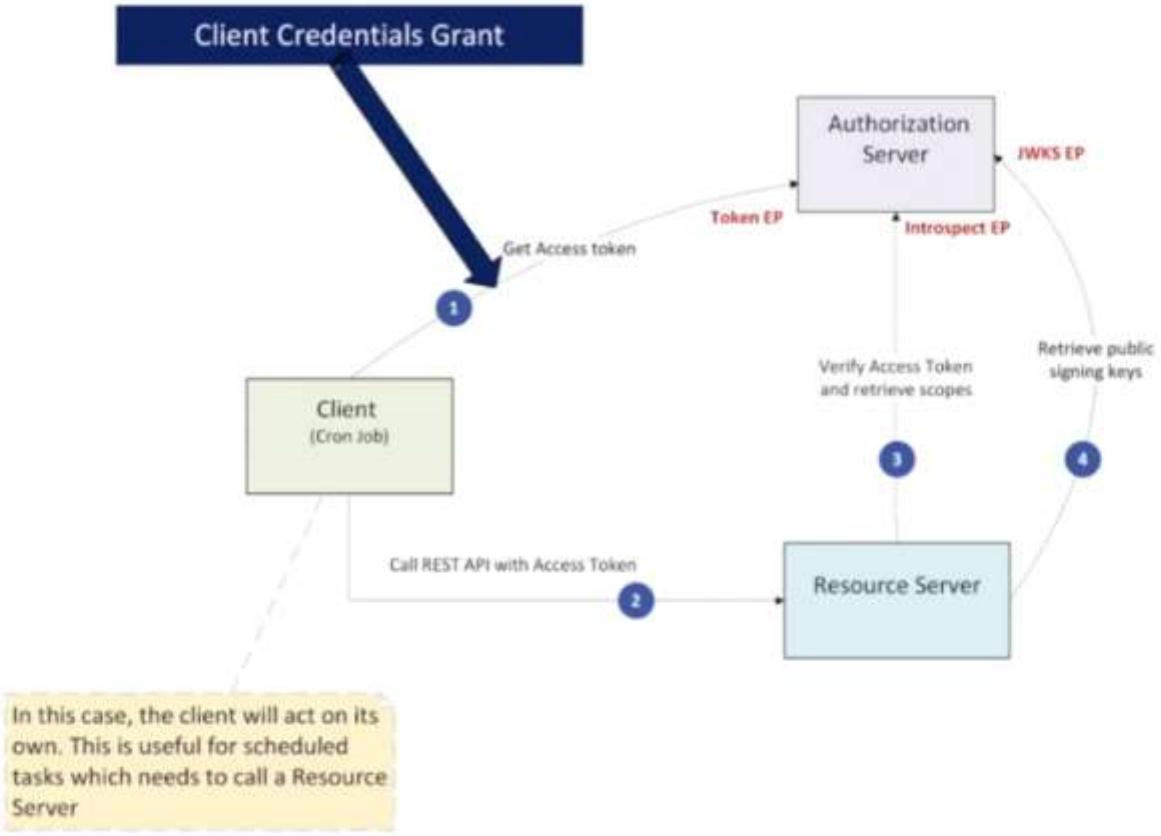
OAuth 2.0 - PKCE Extension



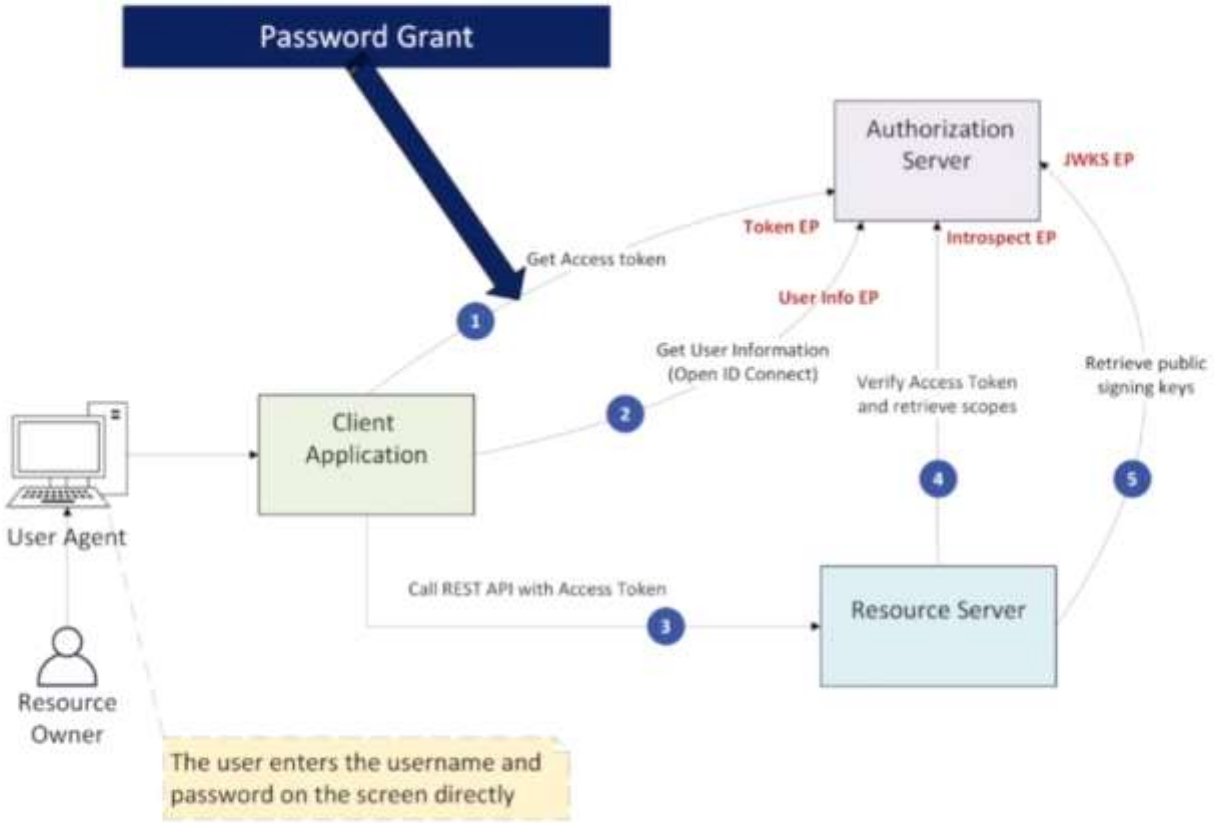
OAuth 2.0 - Implicit



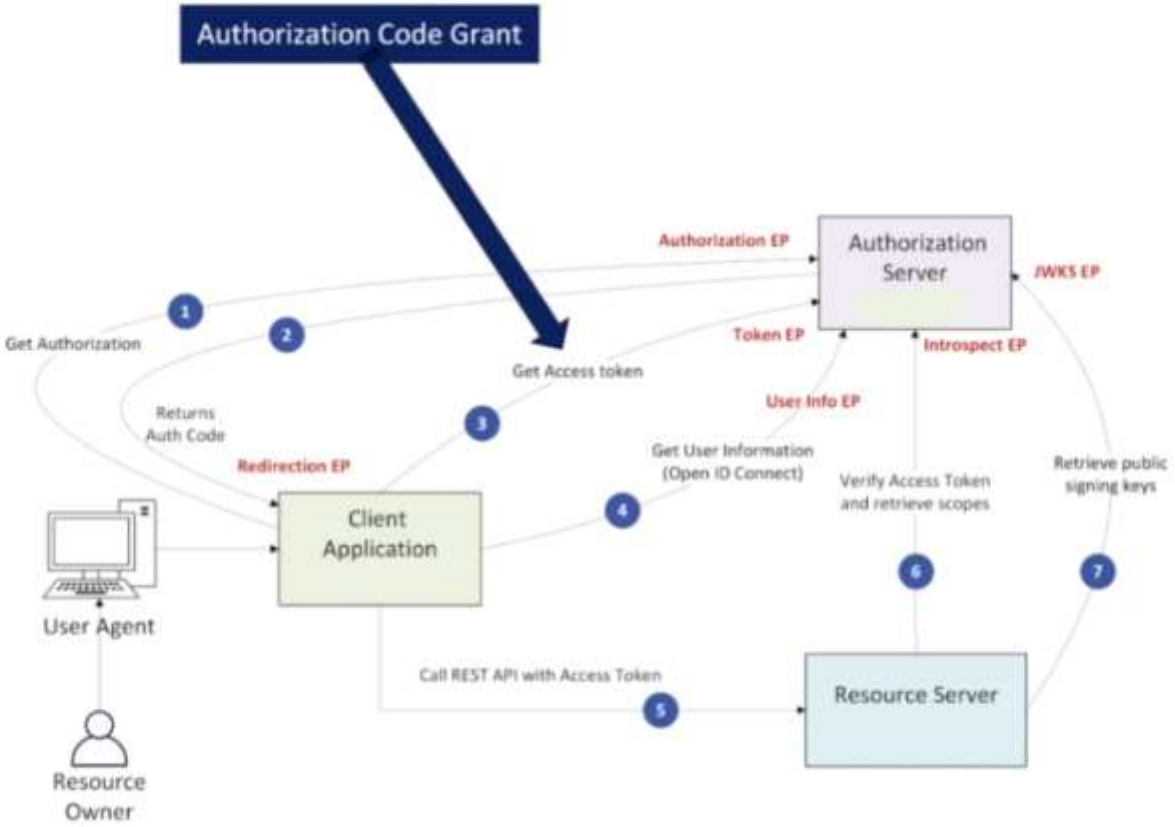
OAuth 2.0 - Client Credentials



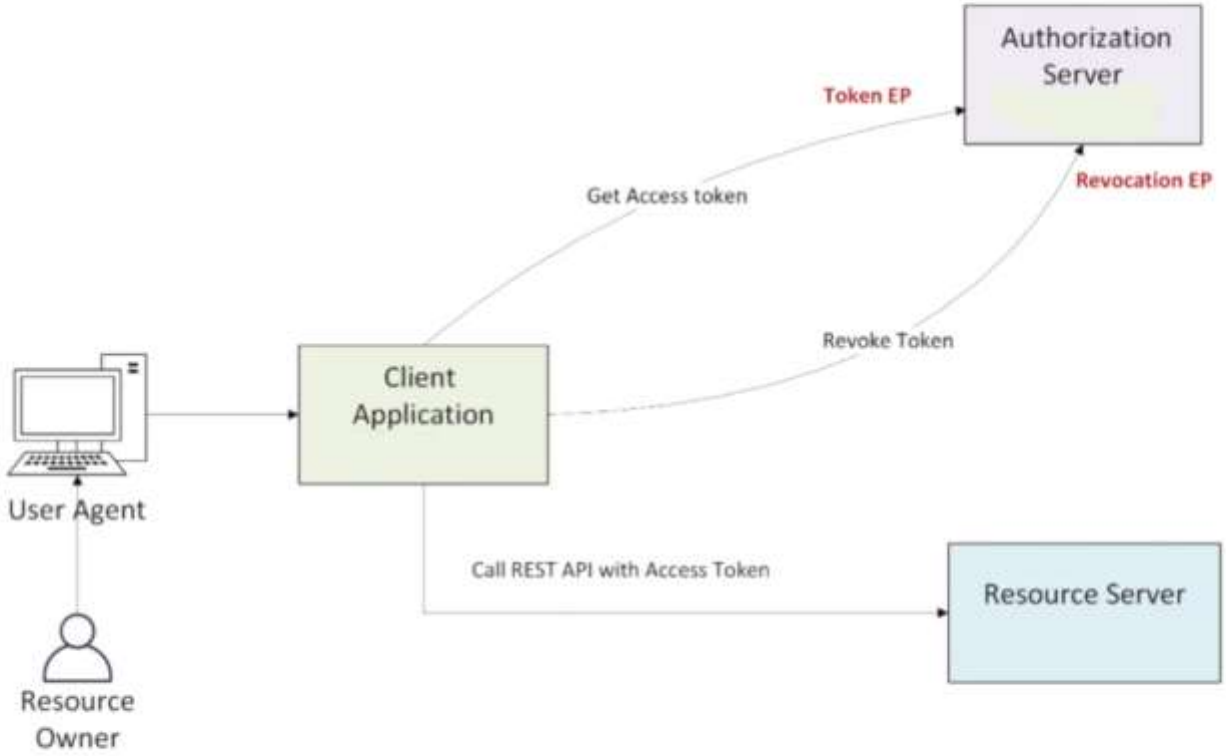
OAuth 2.0 - Resource Owner Password Credentials



OAuth 2.0 - Refresh Token

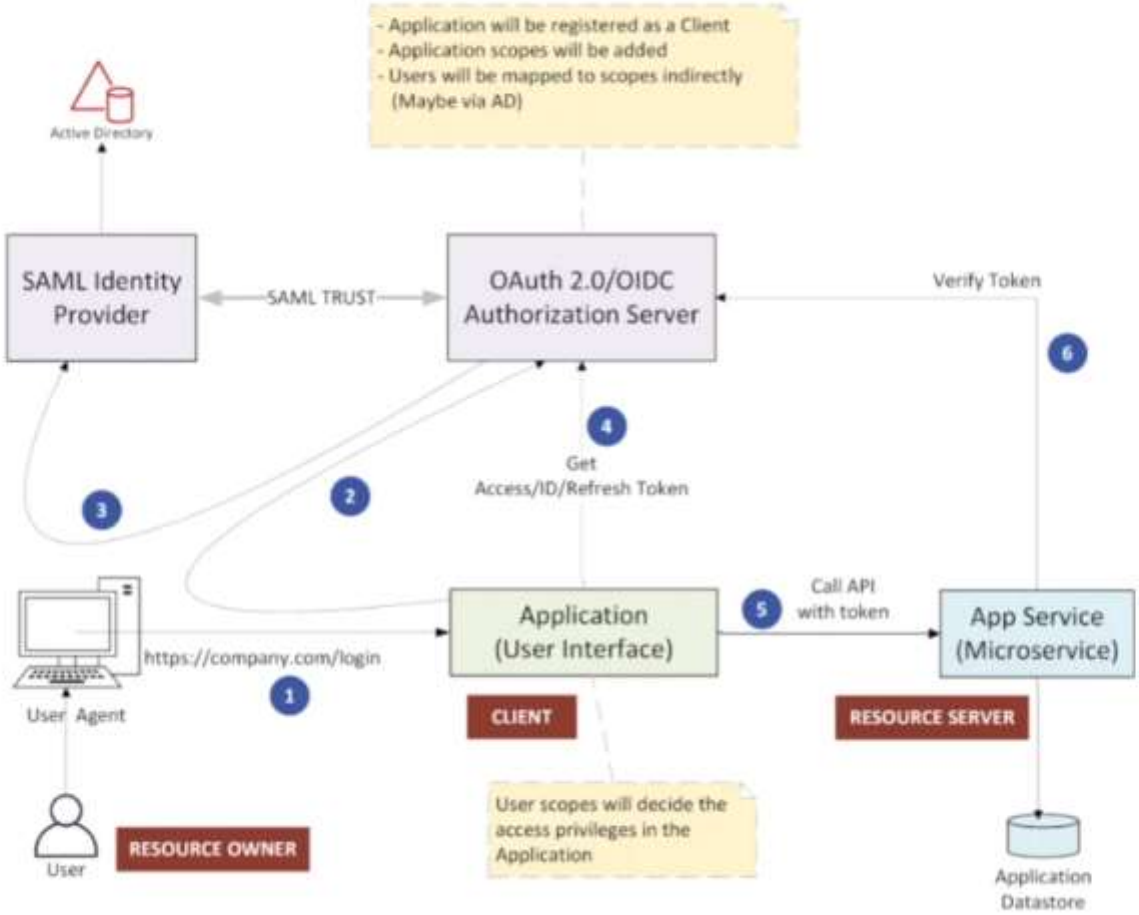


OAuth 2.0 - Token Revocation

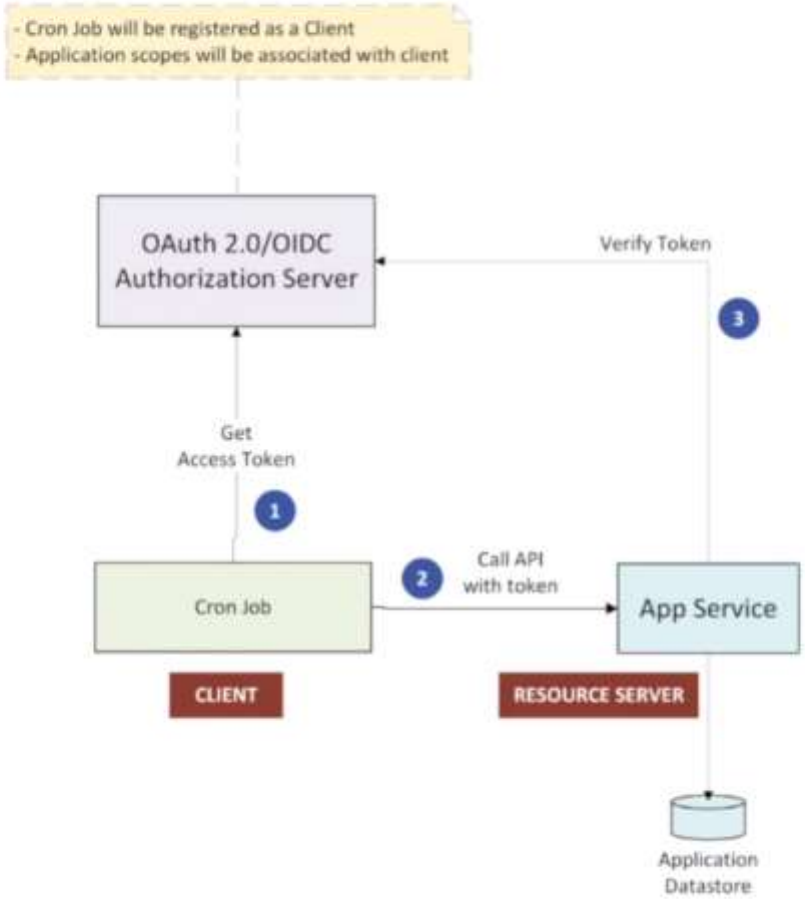


Authorization Code	• Server side web applications • Needs User Agent • Can use Refresh tokens • Very Safe	Confidential Client 
Implicit	• Single Page applications • Needs User Agent • Cannot use Refresh tokens • Danger of Access token exposure • Not recommended (Deprecated)	Public Client 
Authorization Code (PKCE extension)	• Recommended for public clients • Needs User Agent • Can use Refresh tokens	Public Client Confidential Client 
Client Credential	• Use for Cron Jobs on the server • No User Agent needed • Cannot use Refresh tokens	Confidential Client 
Resource Owner Password Credentials	• Resource Server and Client must be from same Organization • No User Agent needed • Can use Refresh tokens • Not Recommended (Deprecated)	Public Client Confidential Client 

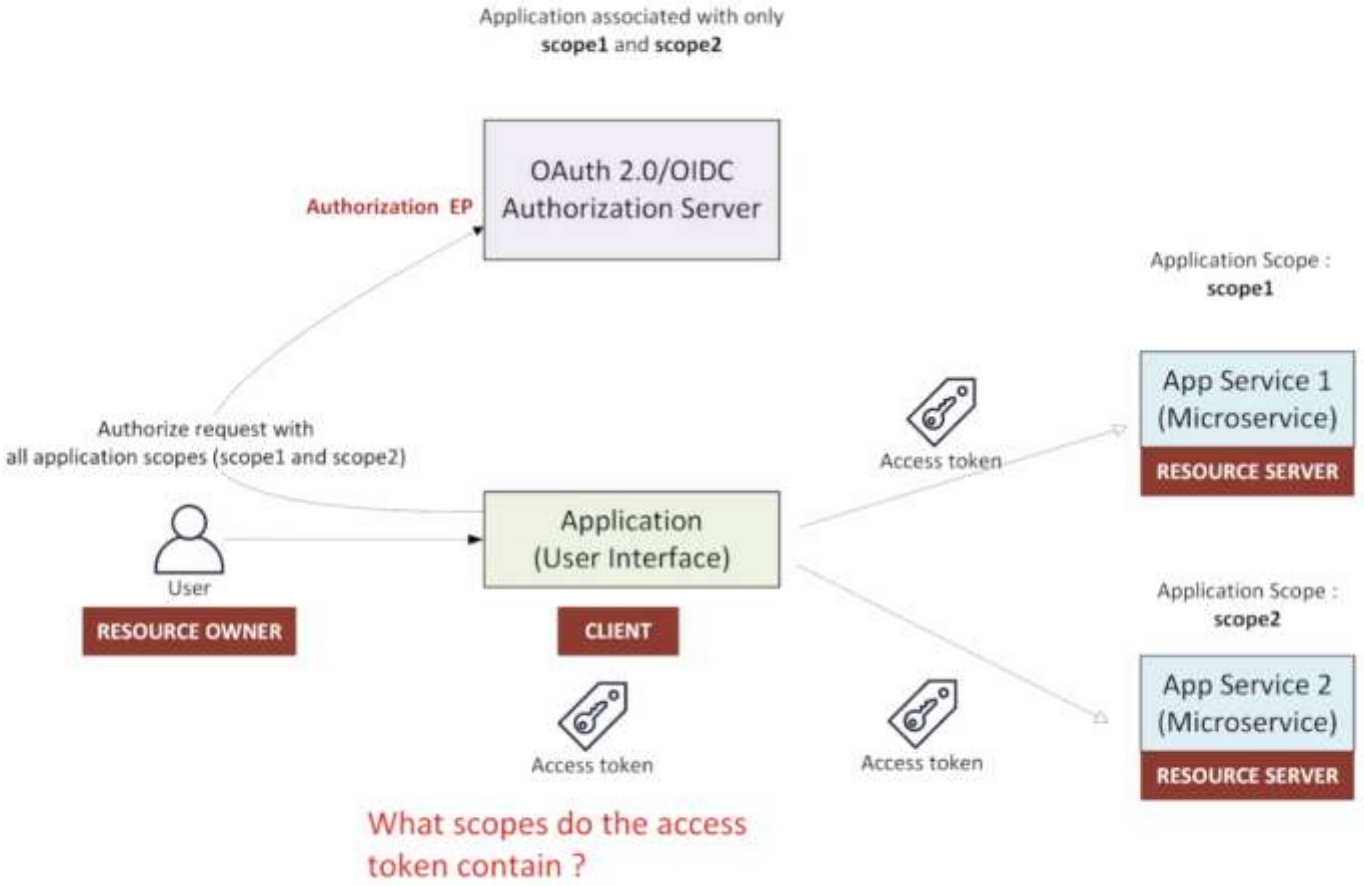
OAuth 2.0 - Typical Enterprise Microservices Application



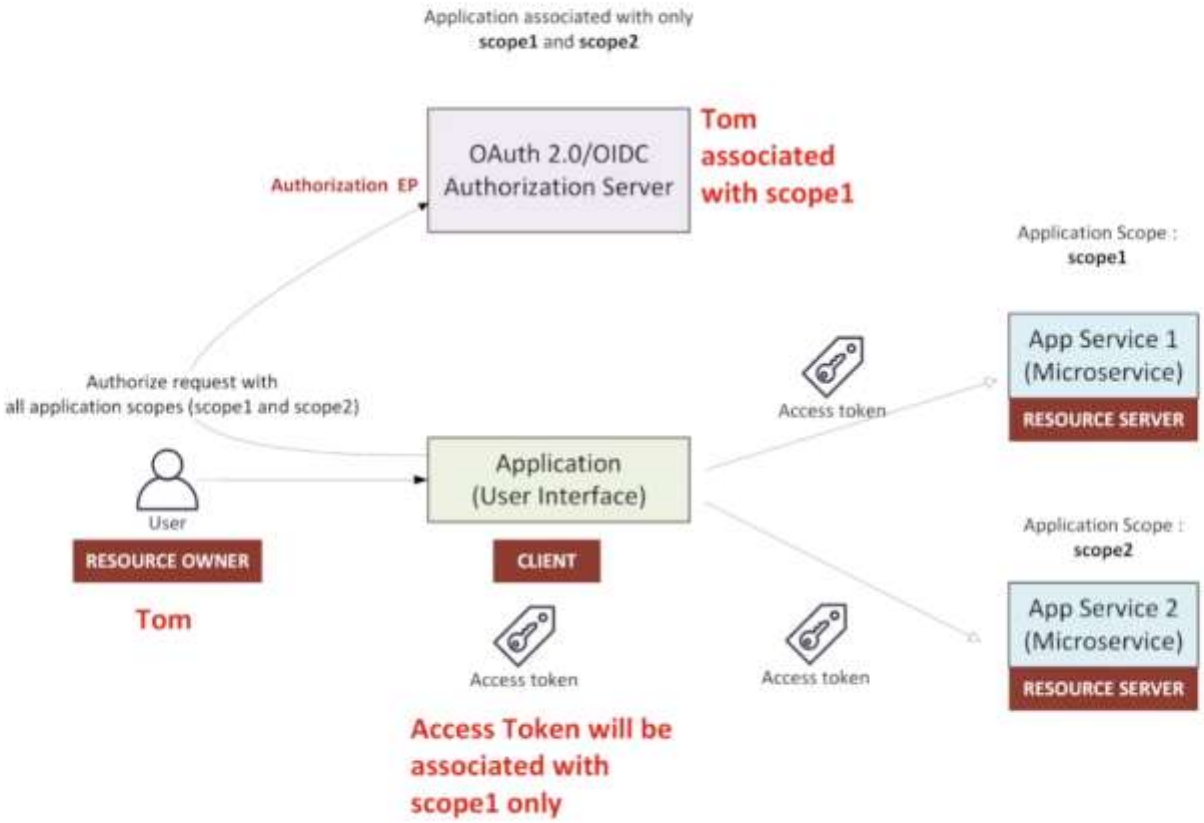
OAuth 2.0 - Typical Enterprise Cron Job



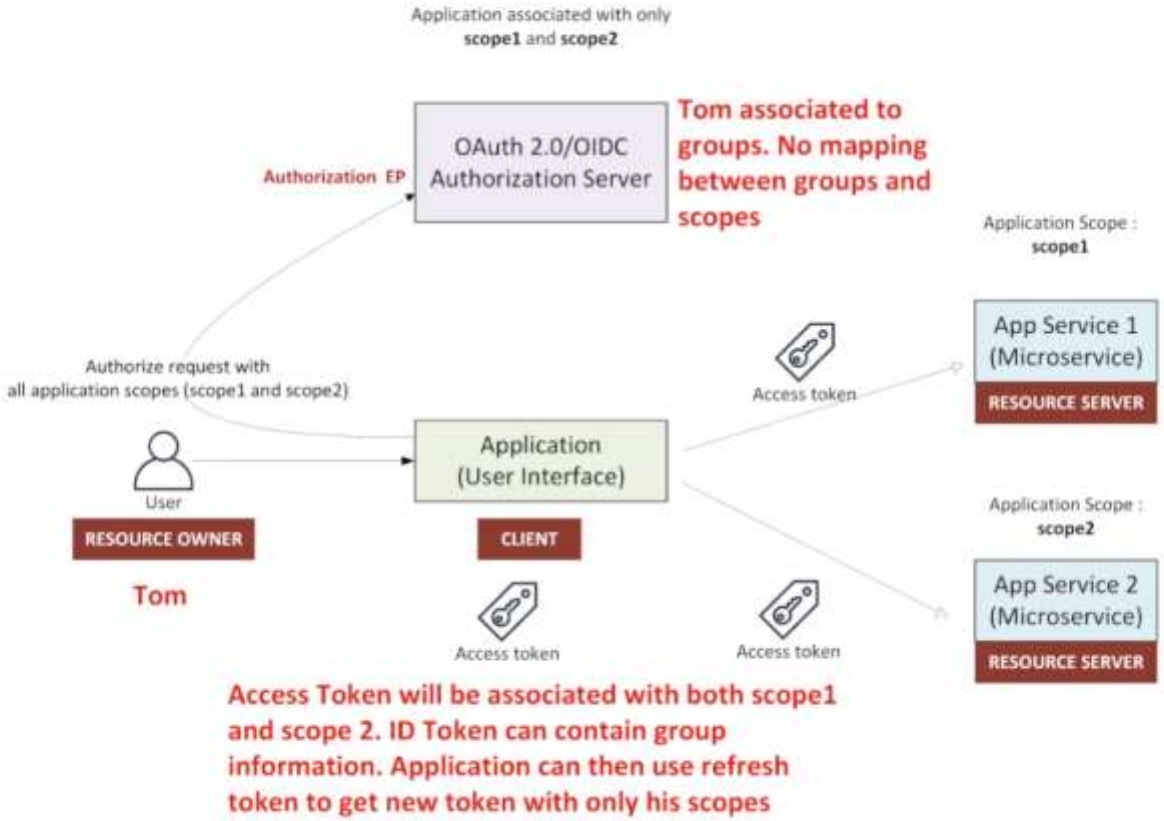
OAuth 2.0 - User association to scopes



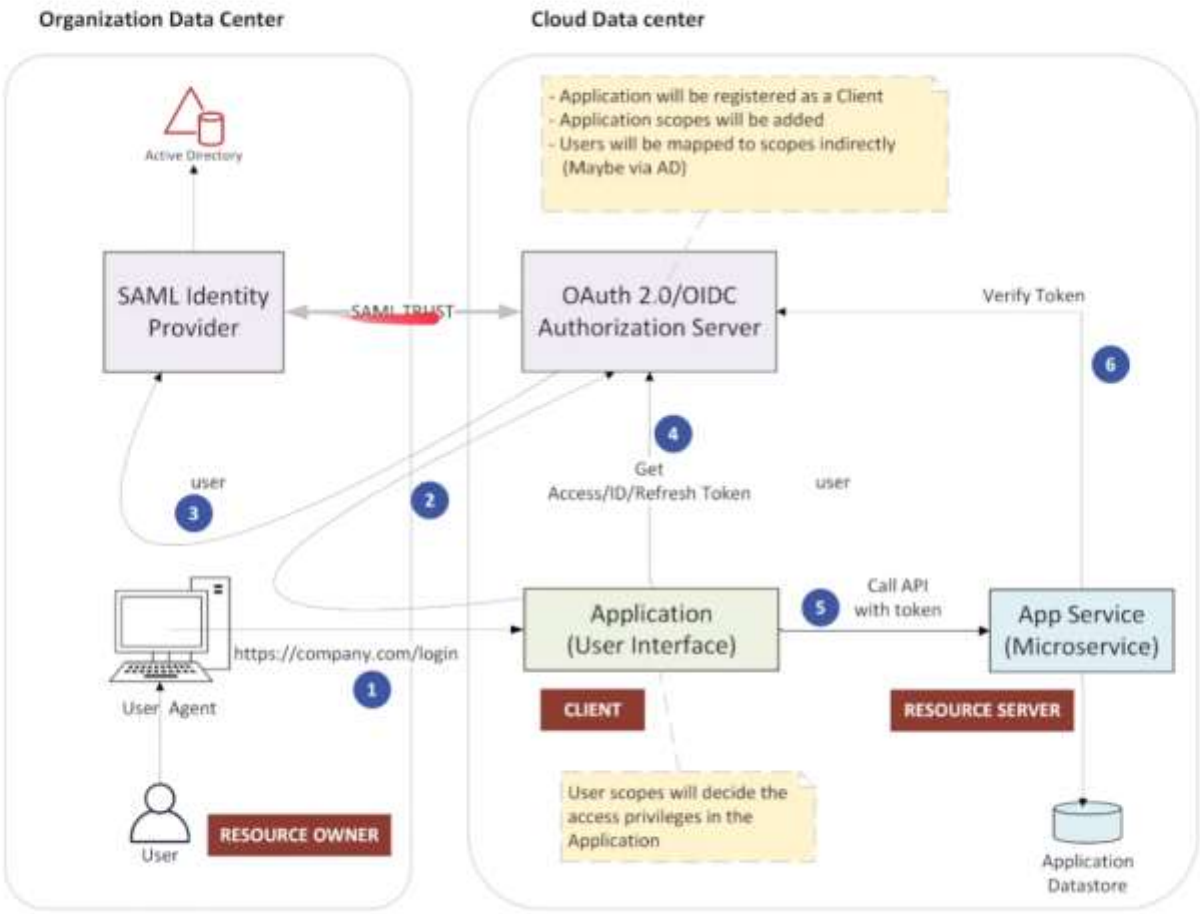
OAuth 2.0 - Downscoping



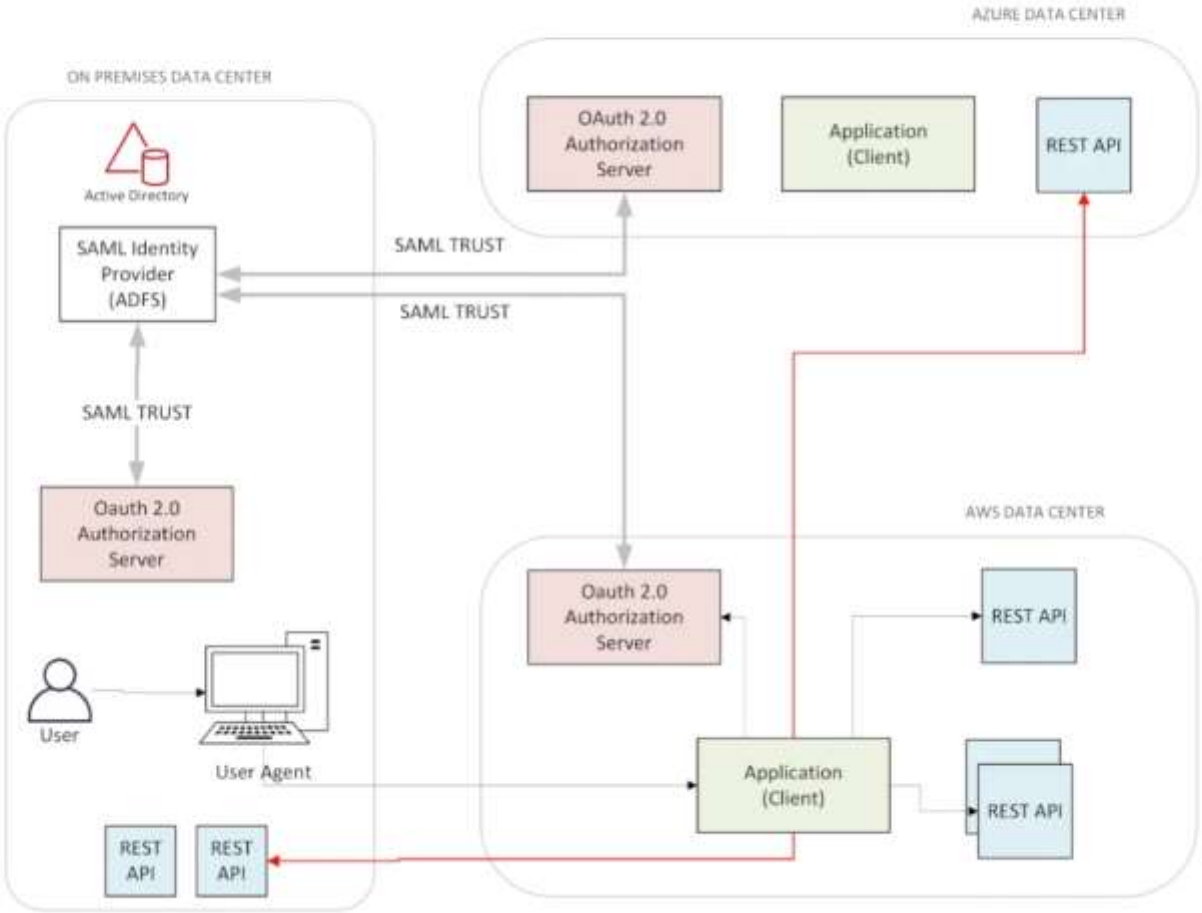
OAuth 2.0 - Non Downscoping



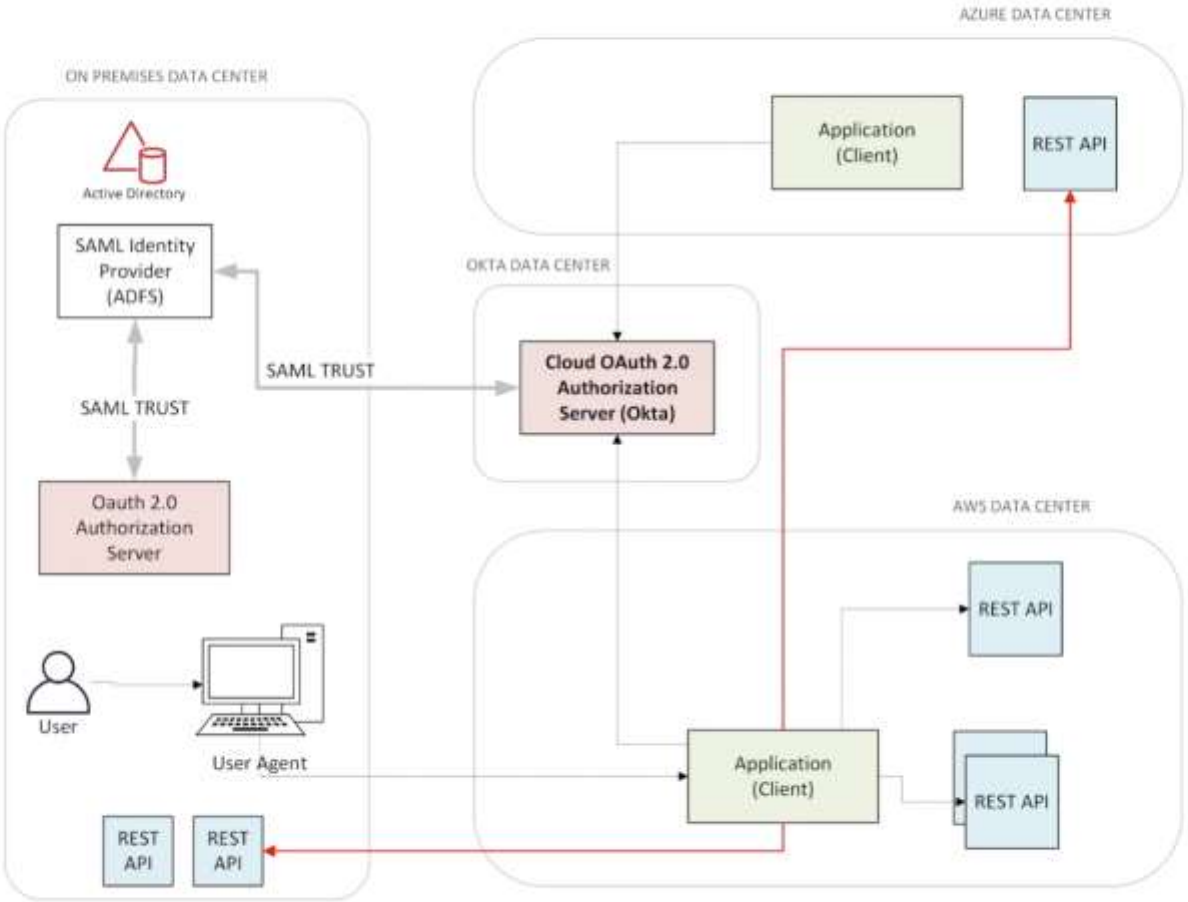
OAuth 2.0 - Cloud Deployment

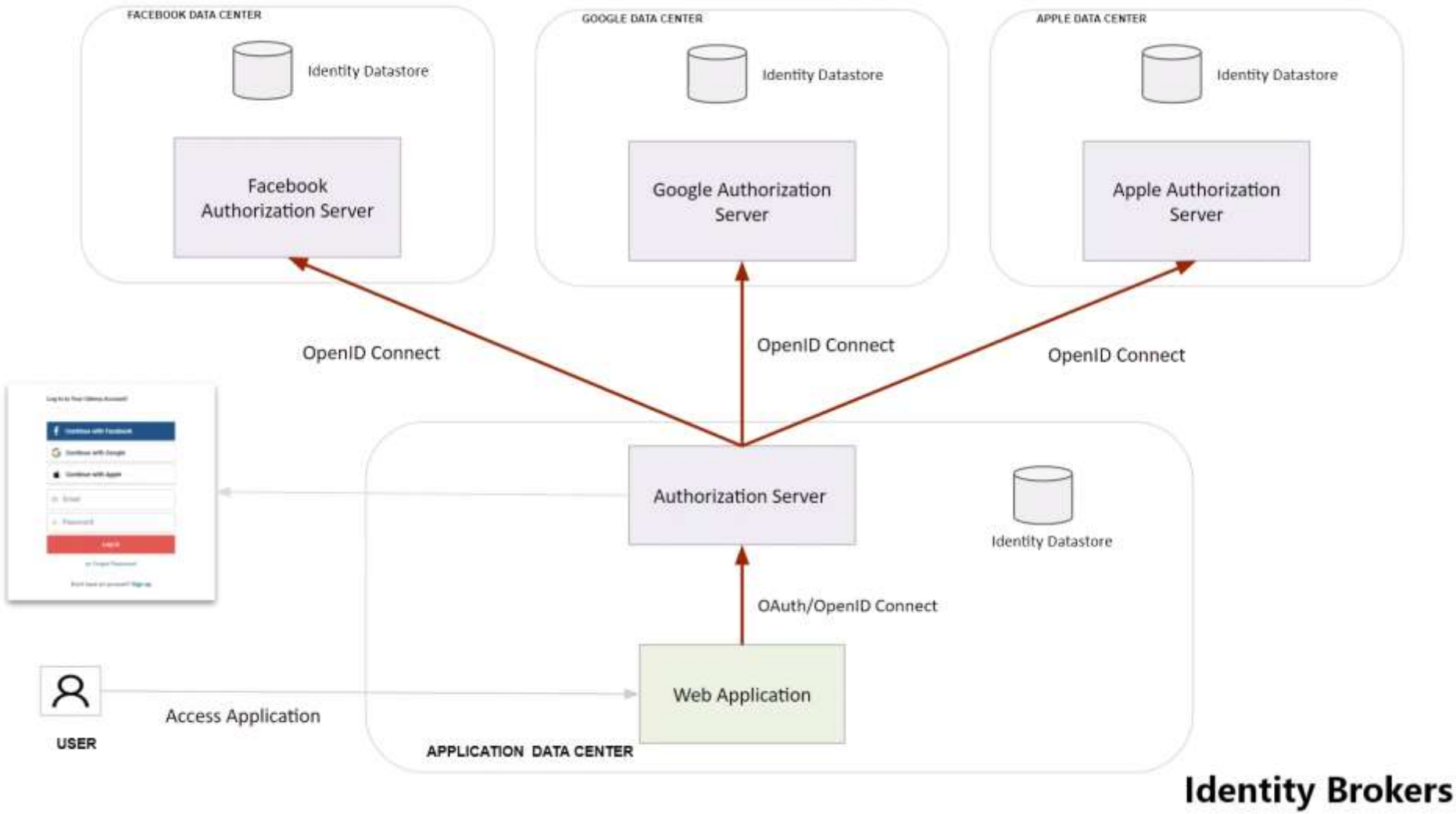


OAuth 2.0 - Multi Cloud Deployment



OAuth 2.0 - Multi Cloud Deployment (OAuth As a Service)



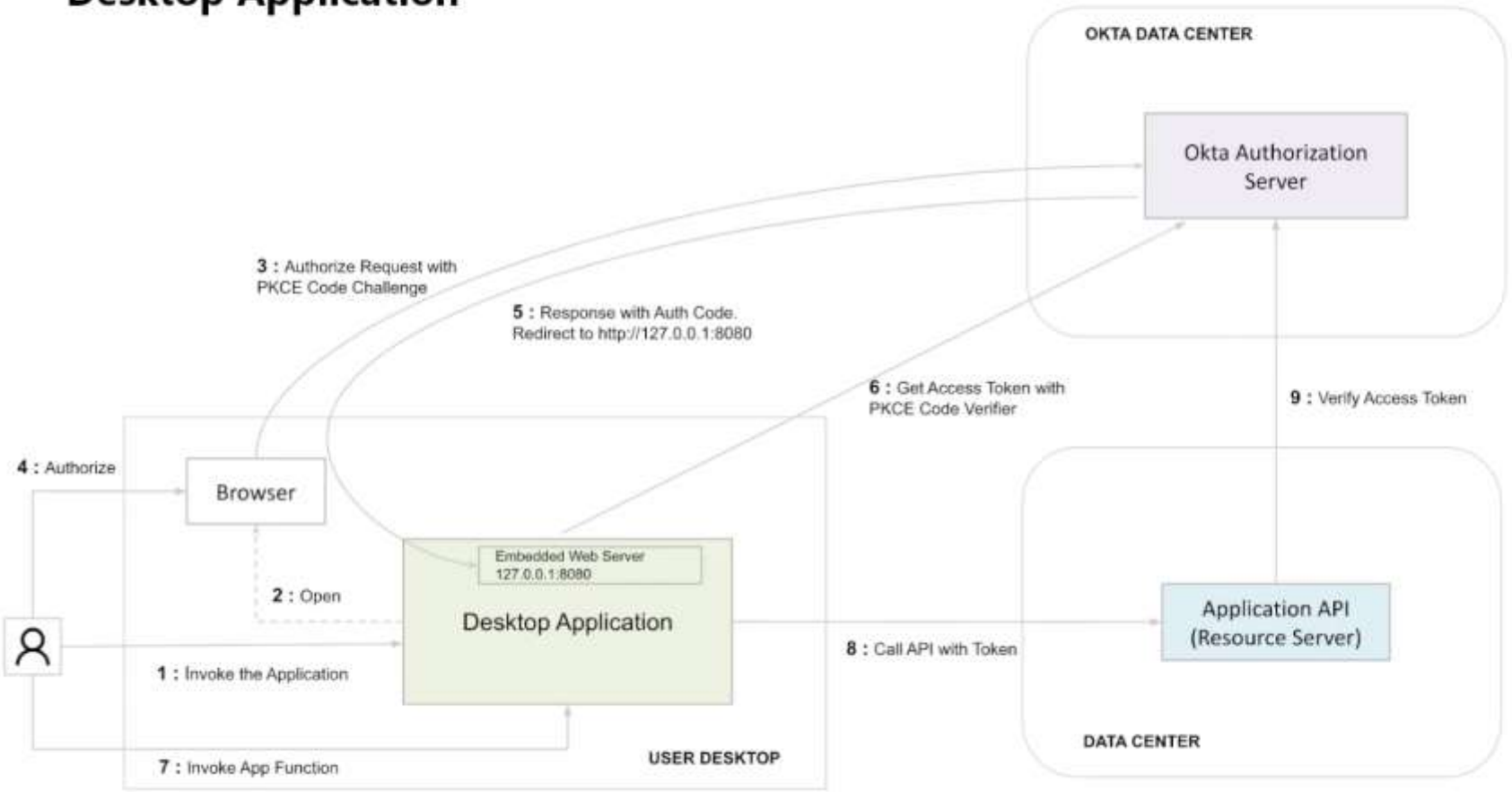


Identity Brokers

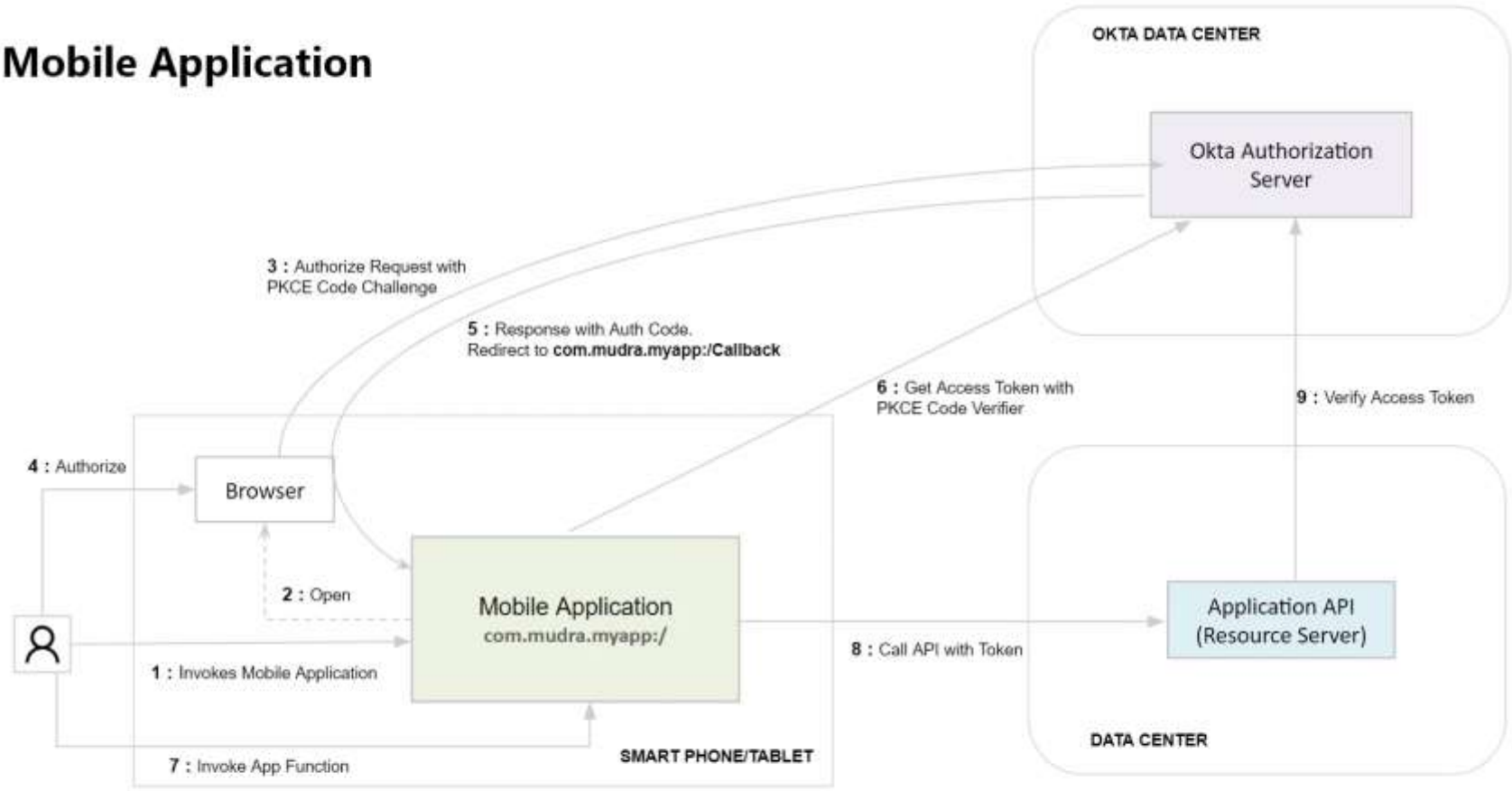
OAuth 2.0 Best Practices

- Prefer Authorization Code Grant with PKCE
- Prefer Client Credentials Grant for Cron Jobs
- Avoid using Implicit Grant
- Avoid using Resource Owner Password Grant
- Store the secrets in a Safe place
- Rotate the secrets regularly
- Keep Access tokens short (5 min)
- Avoid using local users of the Authorization Server
- Do not associate users with more scopes than needed
- Use the enterprise logout (all sessions)
- Do not store tokens or secrets in the browser or Mobile devices

Desktop Application



Mobile Application



Device Application