Simplify sign in and authorization with the Microsoft identity platform

Vinodha Muthu Valli

Solution Architect

JiJi Technologies Private Limited

Vinodha Muthu Valli Gurusamyraj | LinkedIn

Agenda

· Quick demo on Microsoft Identity Platform

· What is Microsoft Identity Platform?

· Tokens

· Debug the sample WPF application
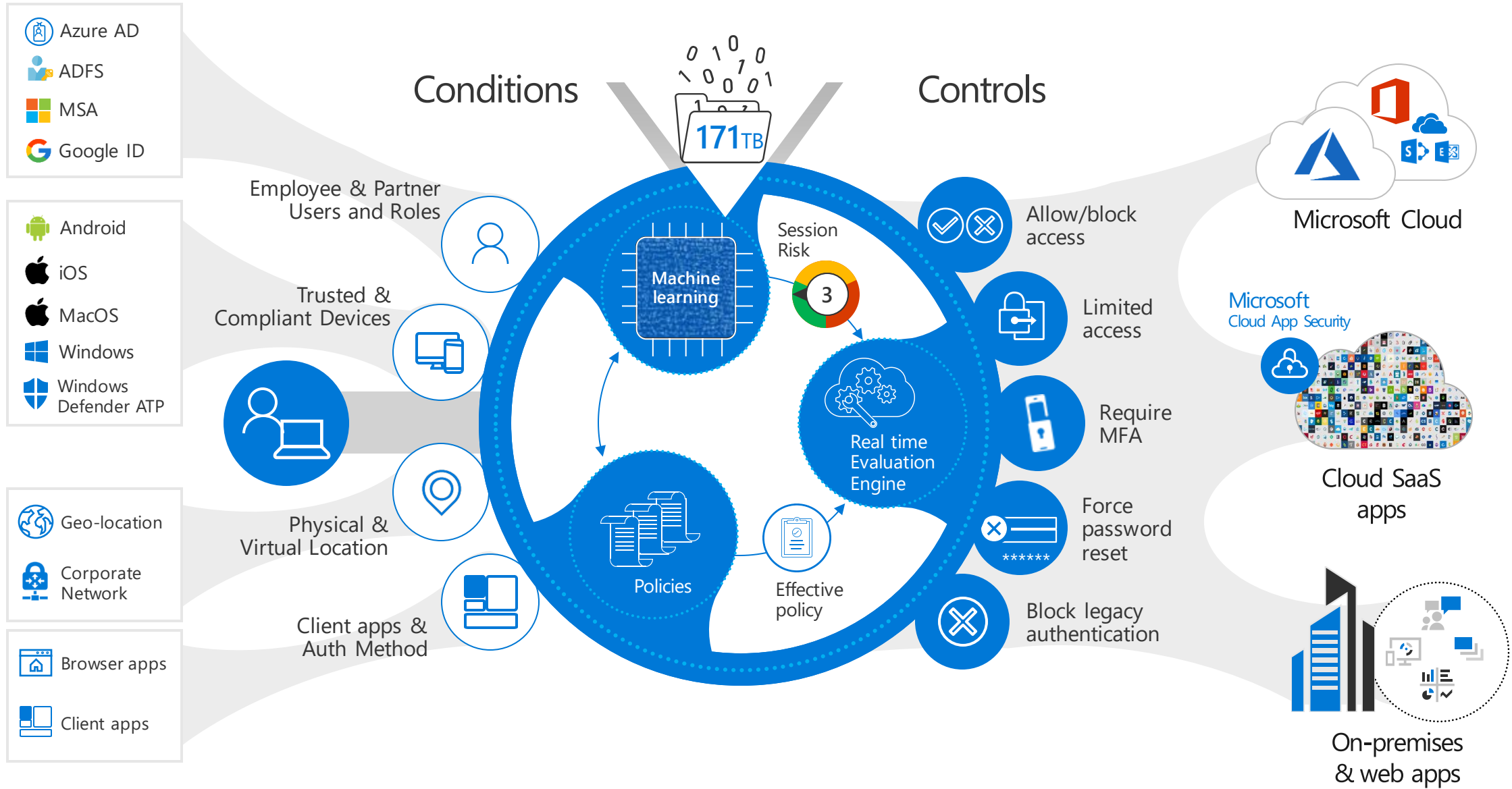
· Best Practices

Demo: Identity made simple!

What is the Microsoft identity platform?

Microsoft identity platform

Build apps that...

- Sign in **over 1 billion users** using one experience
- Securely **access user data** in any API (e.g. Microsoft Graph)
- Support ongoing innovation like **password-less**
- Comply with **IT policies** like MFA and managed devices

It's EASY and you get stuff for FREE

It's easy:

- Register your app
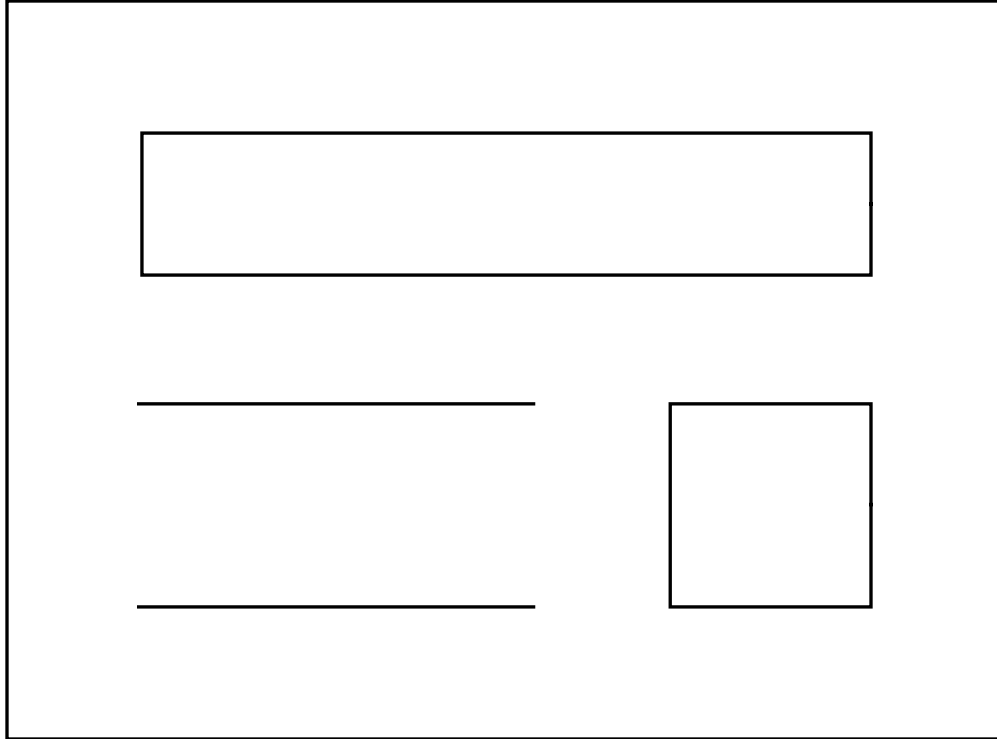- Use a QuickStart
- Request permission to data

The rest comes automatically, with no extra code:

- single sign on, token management, passwordless, conditional access

Tokens

- ID Token
  - -Contains identity data as claims
  - -You must validate the ID Token before you use it
- Access Token
  - -You need Access Token to access the resource
- Refresh Token
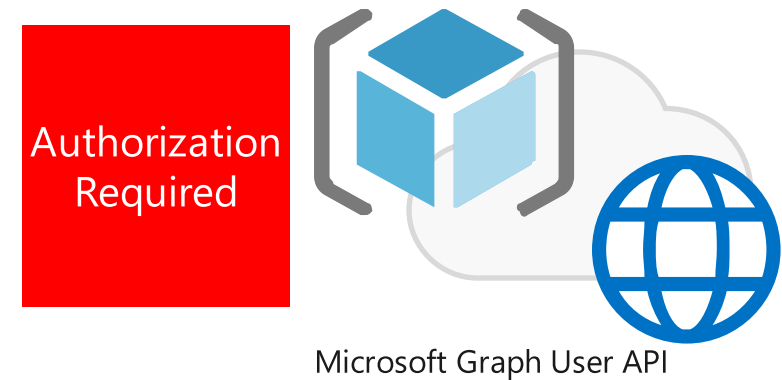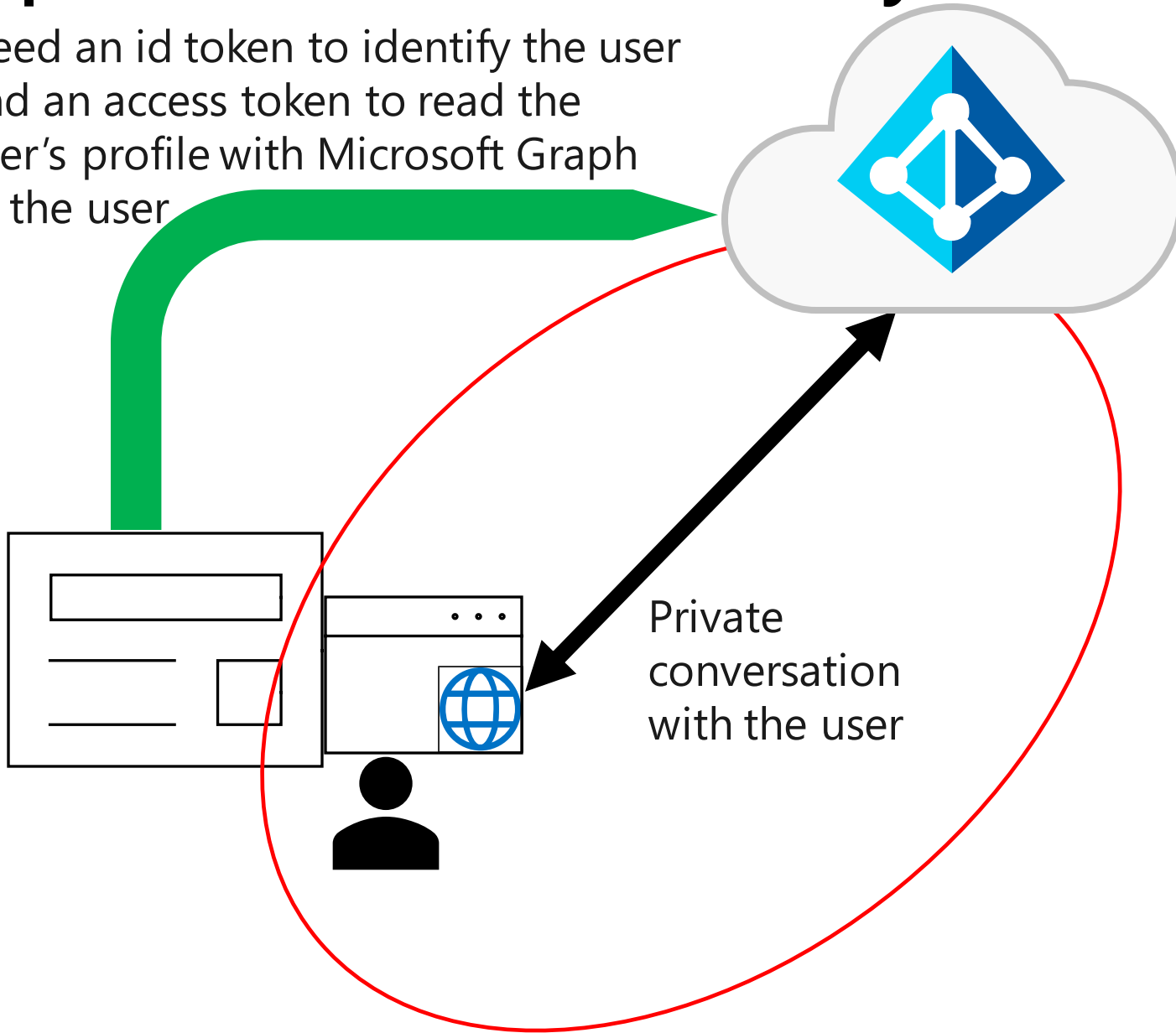
Let's start with an app
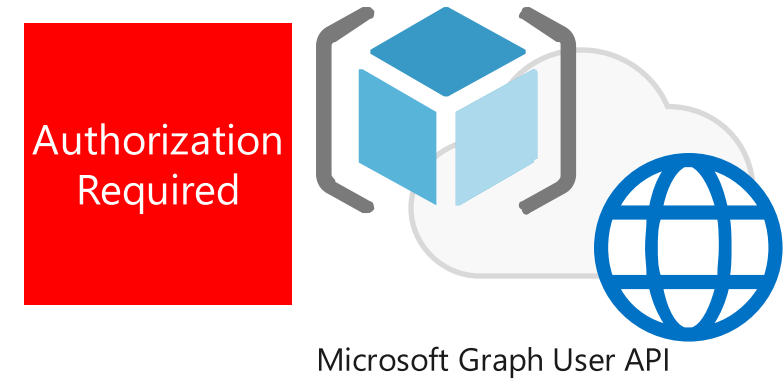
First, I need to login
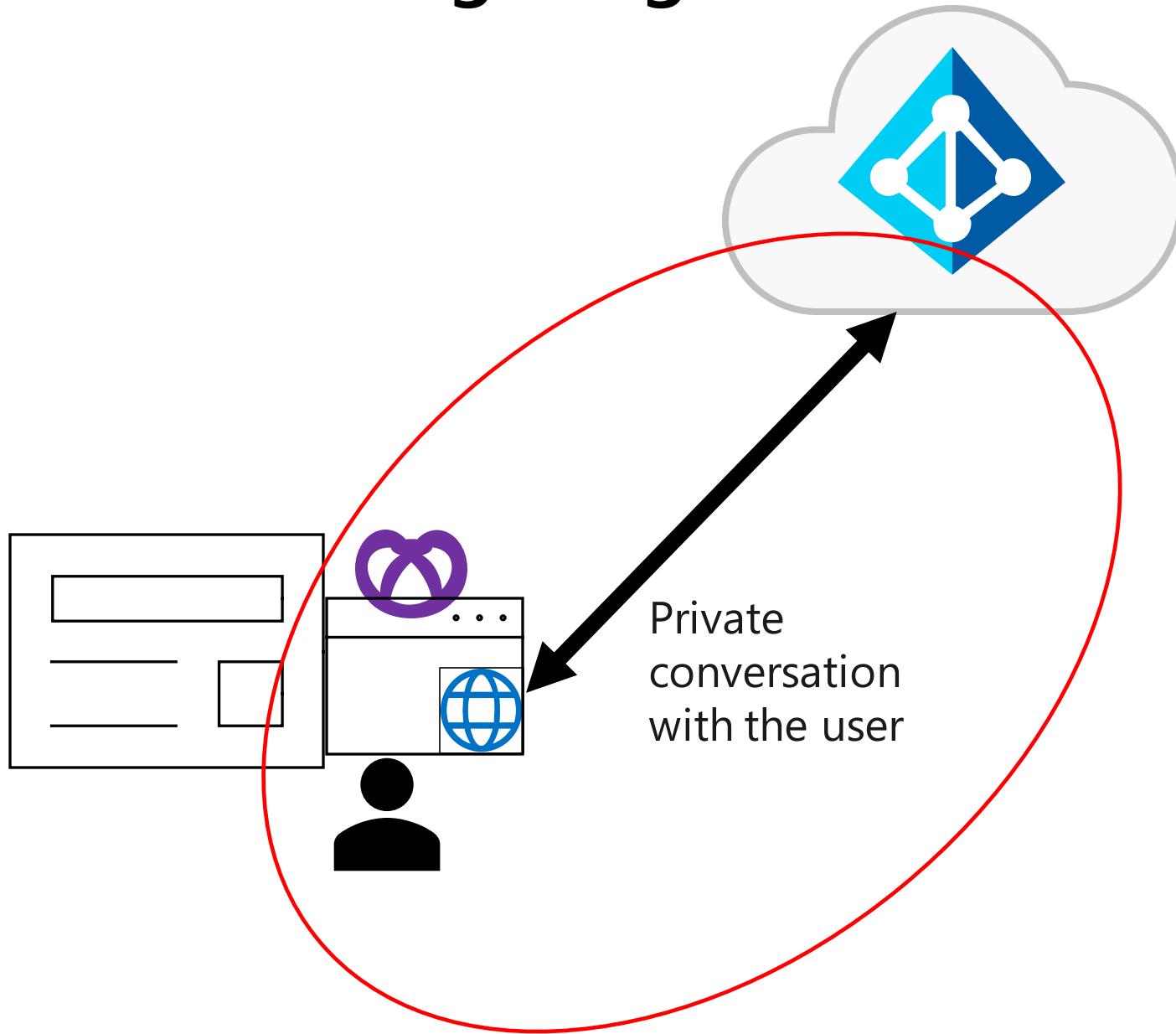Then, I need to call some APIs

Apps asks Microsoft identity for tokens

Need an id token to identify the user and an access token to read the user's profile with Microsoft Graph as the user
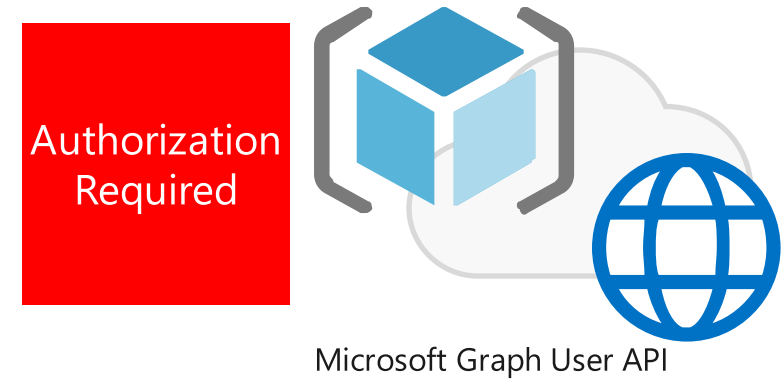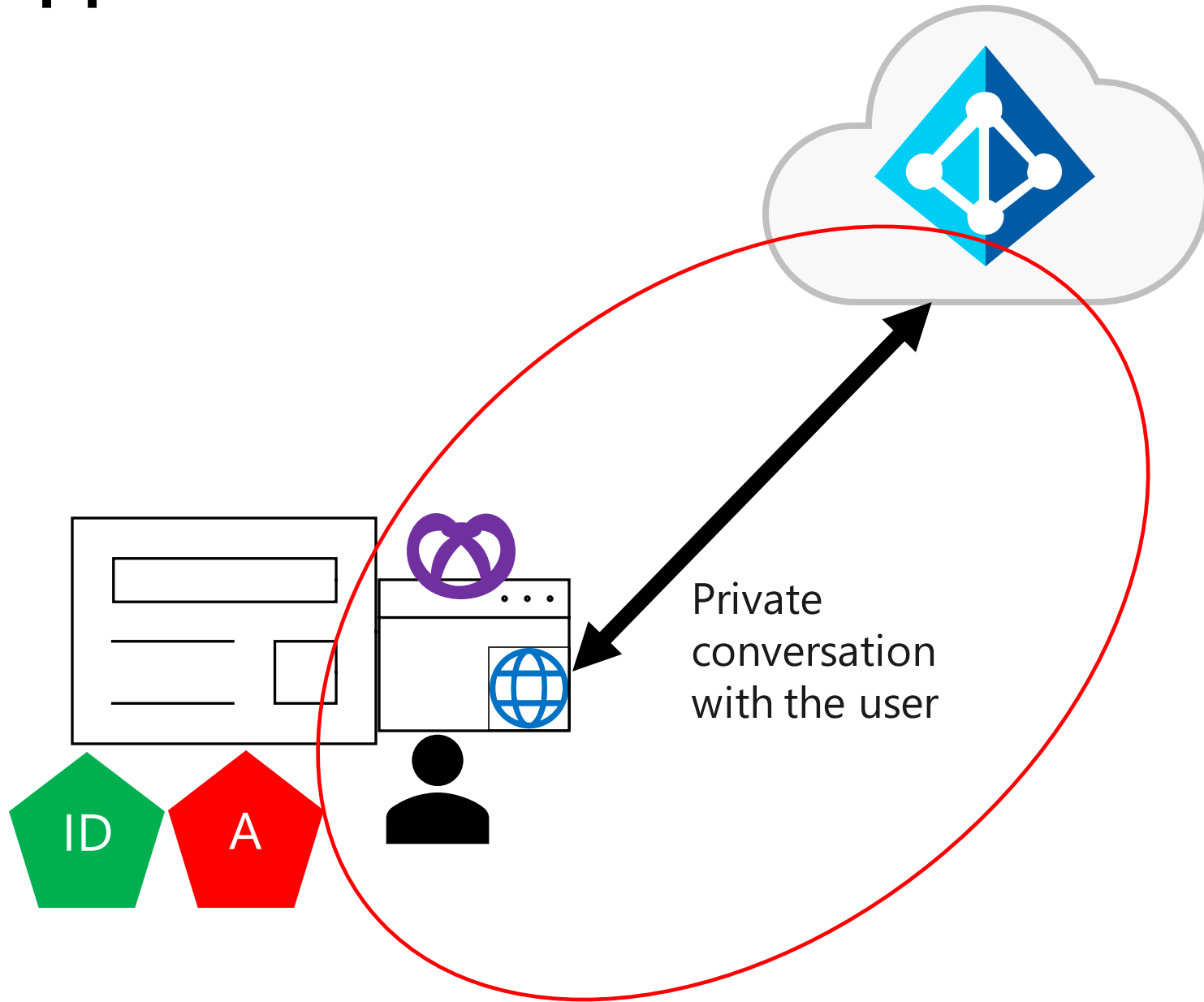
Private conversation with the user

Authorization Required

Microsoft Graph User API

The core of Single Sign On

Private conversation with the user

Authorization Required

Microsoft Graph User API

App receives an id_token

{ "typ": "JWT", "alg": "RS256", "kid": "1LTMzakihiRla_8z2BEJVXeWMqo" }.
{ "ver": "2.0",
"iss": "https://login.microsoftonline.com/9188040d-6c67-4c5b-b112-36a304b66dad/v2.0",
"aud": "6cb04018-a3f5-46a7-b995-940c78f5aef3",
"exp": 1536361411,"iat": 1536274711, "nbf": 1536274711,
"sub": "AAAAAAAAAAAAAAAAAAAAAAIkzqFVrSaSaFHy782bbtaQ",
"name": "Abe Lincoln",
"preferred_username": "AbeLi@microsoft.com",
"oid": "00000000-0000-0000-66f3-3332eca7ea81",
"tid": "3338040d-6c67-4c5b-b112-36a304b66dad",
}
.[Signature]

App receives an access token

Private conversation with the user

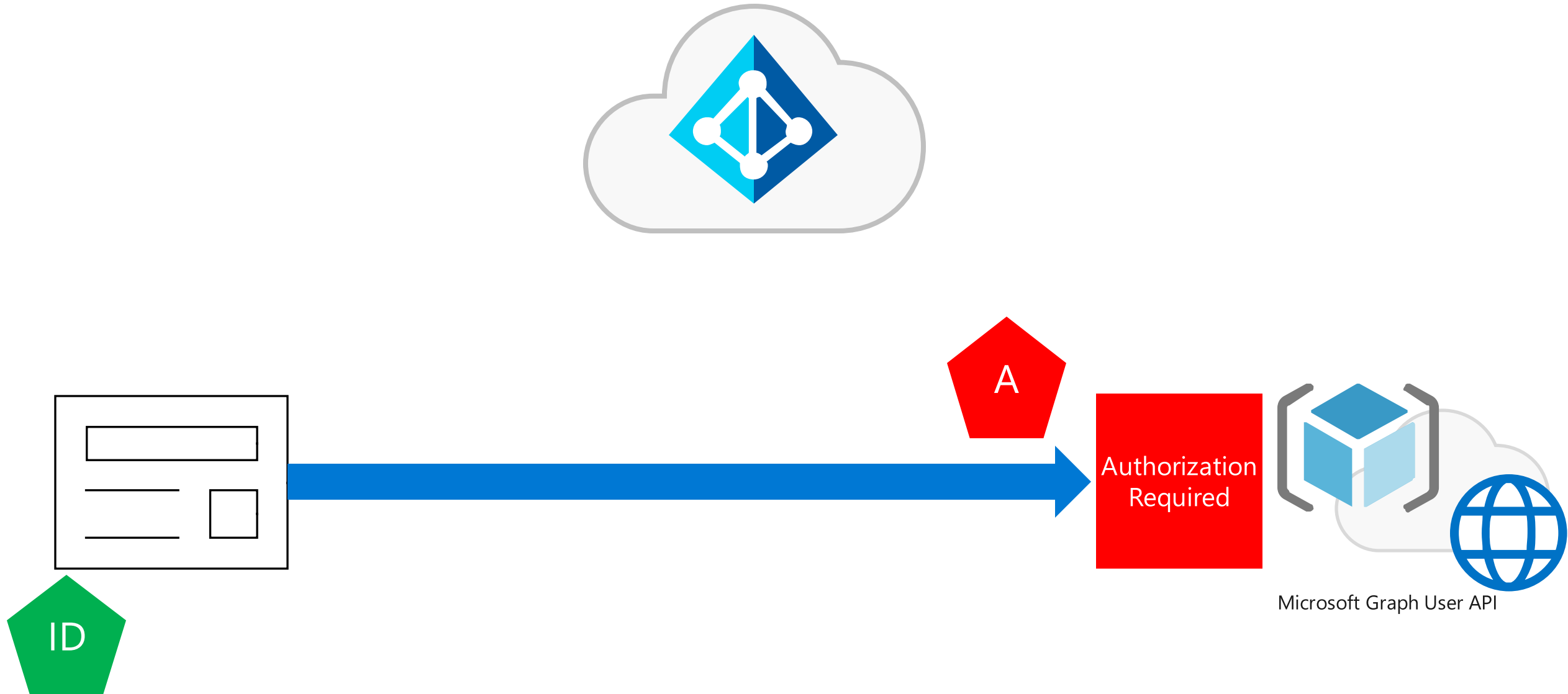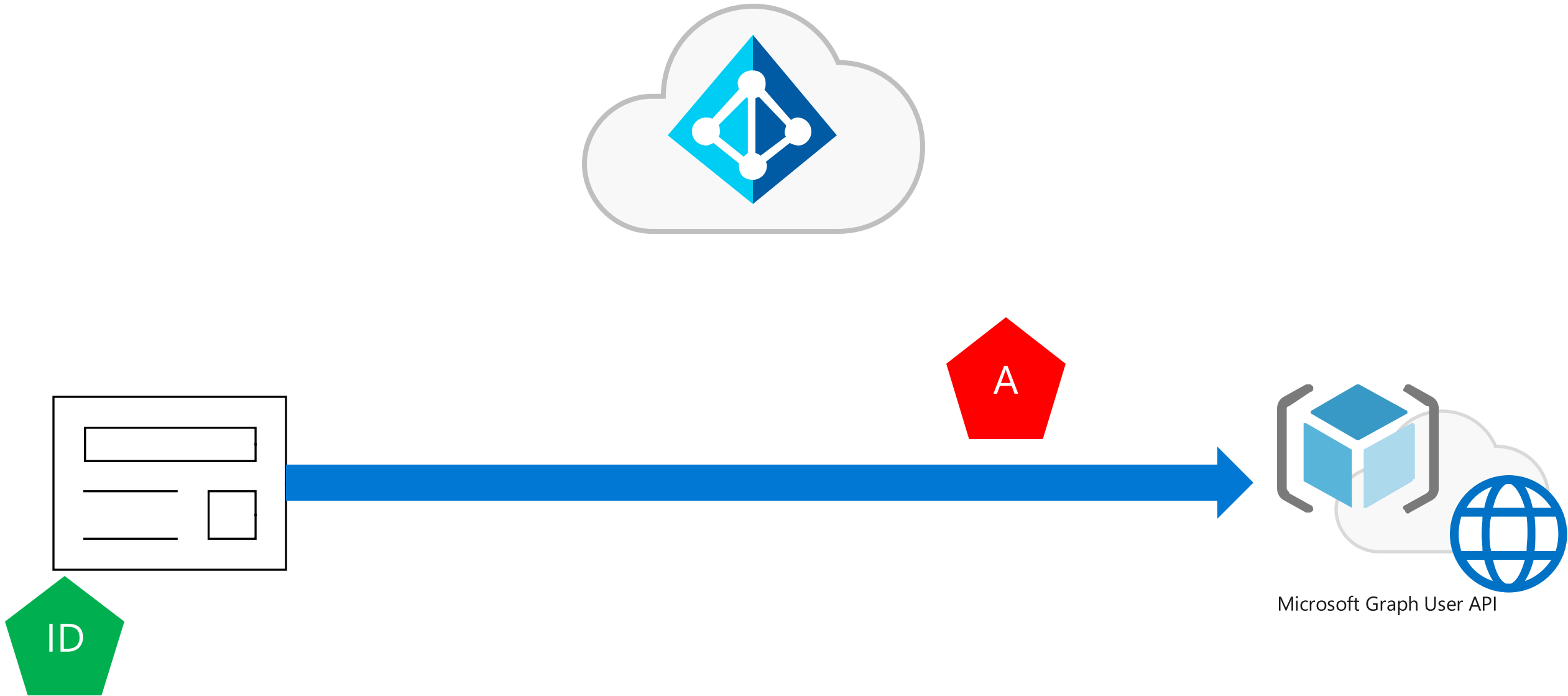ID   A

Authorization Required

Microsoft Graph User API

App receives an access token

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imk2bEdrM0ZaenhSY1ViMkMzbkVRN3
N5SEpsWSJ9.eyJhdWQiOiI2ZTc0MTcyYi1iZTU2LTQ4NDMtOWZmNC1lNjZhM2ViYjEyZTMi
LCJpc3MiOiJodHRwczovL2xvZ2luLm1pY3Jvc29mdG9ubGluZS5jb20vNzJmOTg4YmYtODZ
mMS00MWFmLTkxYWItMmQ3Y2QwMTFkYjQ3L3YyLjAiLCJpYXQiOjE1MzcyMzEwNDgsIm
5iZiI6MTUzNzIzMTA0OCwiZXhwIjoxNTM3MjM0OTQ4LCJhaW8iOiJBWFFBaS84SUFBQUF
0QWFaTG8zQ2hNaWY2S09udHRSQjdlQnE0L0RjY1F6amNKR3hQWXkvQzNqRGFOR3hYZ
DZ3TklJVkdkS2hHOUm53SjFsT0NBbk5aY2p2a295ckZ4Q3R0djMzMTQwUmlvT0ZKNGJDQ
0dWdW9DYWcxdU9UDIyMjIyZ0h3TFBBZUS91Zjc5UVgrMEtaWpkcm1wNjlSY3R6bVE9PS
IsImF6cCI6IjZlNzQxNzJiLWJlNTYtNDg0My05ZmY0LWU2NmEzOWJiMTJlMyIsImF6cGFjaUl
6IjAiLCJuYW1lIjoiQWJlIExpbmNvbG4iLCJvaWQiOiI2OTAyMjJiZS1mZjFhLTRkNTYtYWJkMS
03ZTRmN2QzOGU0NzQiLCJwcmVmZXJyZWRfdXNlcm5hbWUiOiJhYmVsaUBtaWNyb3Nv
ZnQuY29tIiwicmgiOiJJIiwic2NwIjoiYWNjZXNzX2FzX3VzZXIiLCJzdWIiOiJIS1pwZmFIeVdhZ
GVPb3VZbGl0anJJLUtmZlRtMjIyWDVyclYzeERxZktRIiwidGlkIjoiNzJmOTg4YmYtODZmMS
00MWFmLTkxYWItMmQ3Y2QwMTFkYjQ3IiwidXRpIjoiZnFpQnFYTFBqMGVRYTgyUy1JWU
ZBQSIsInZlciI6IjIuMCJ9.pj4N-w_3Us9DrBLfpCt

App has an authenticated user and a token to call API

Authorization Required

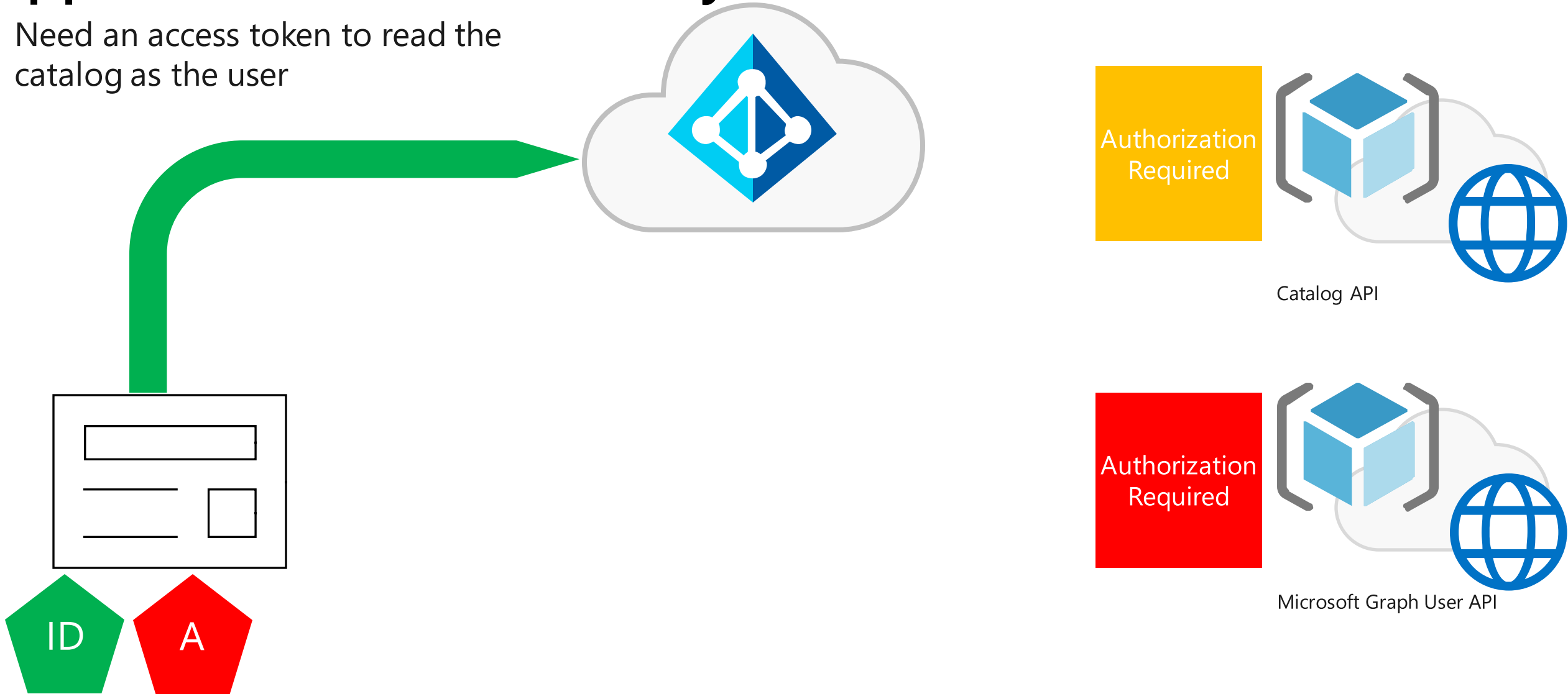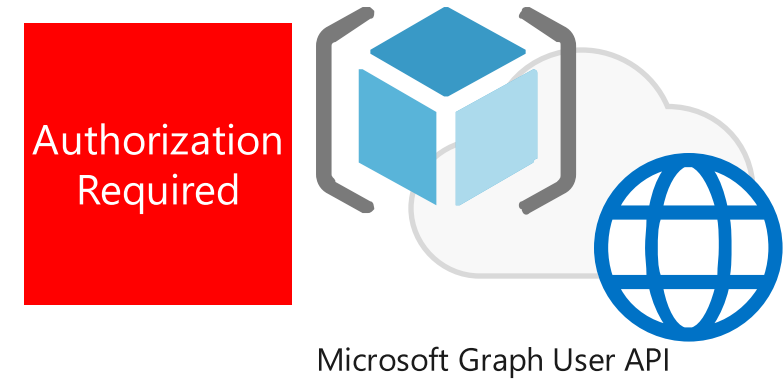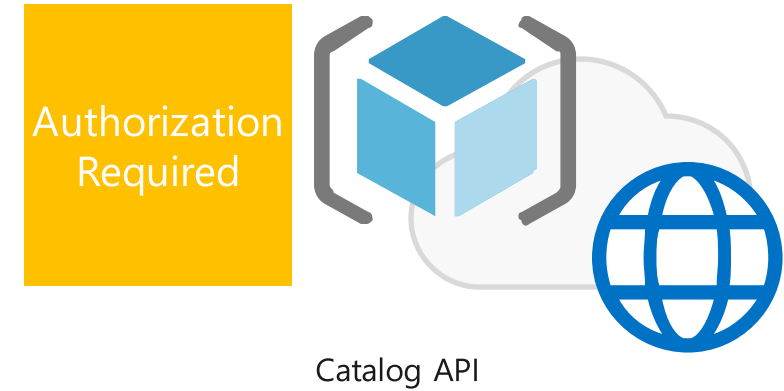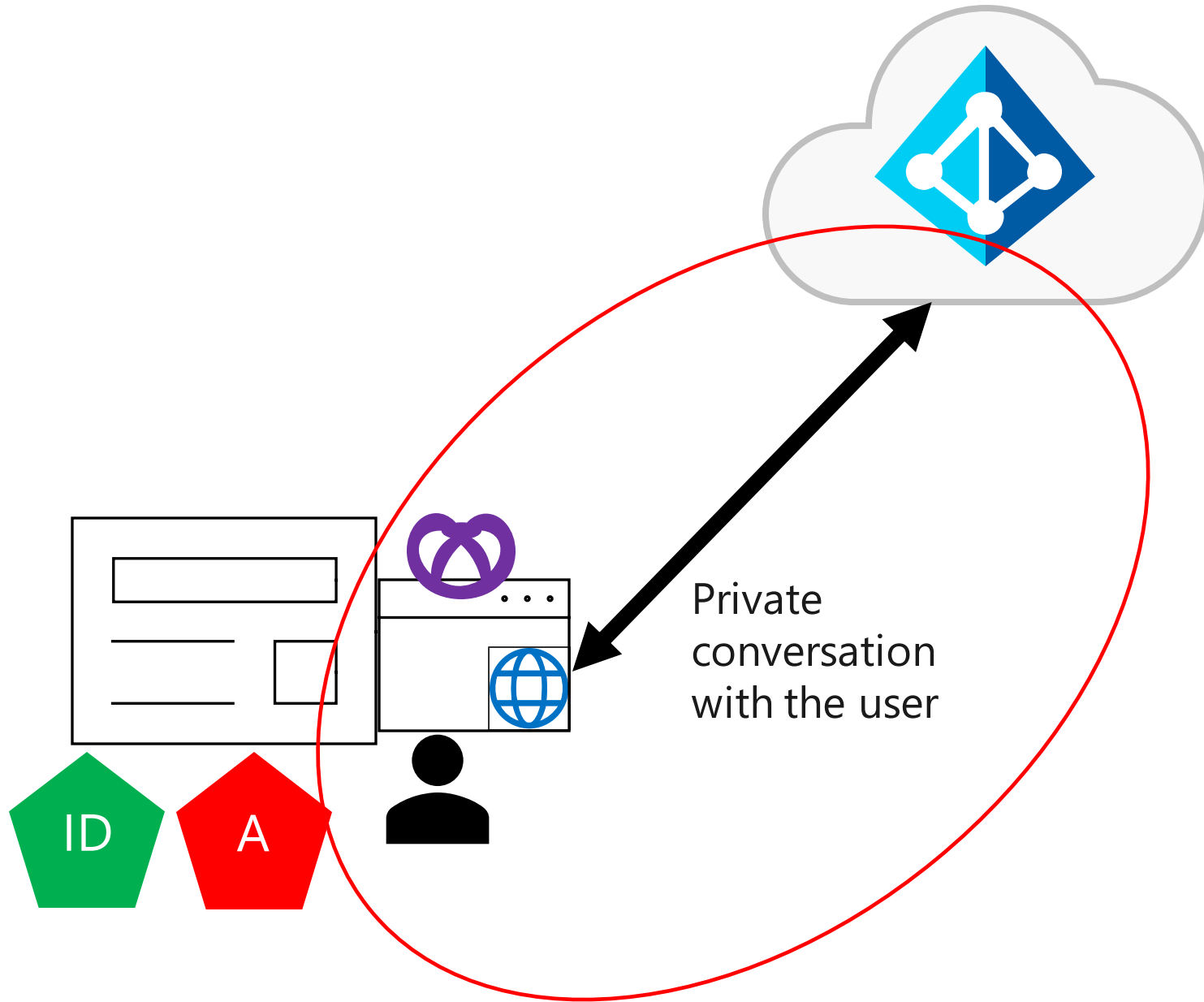Microsoft Graph User API

ID   A
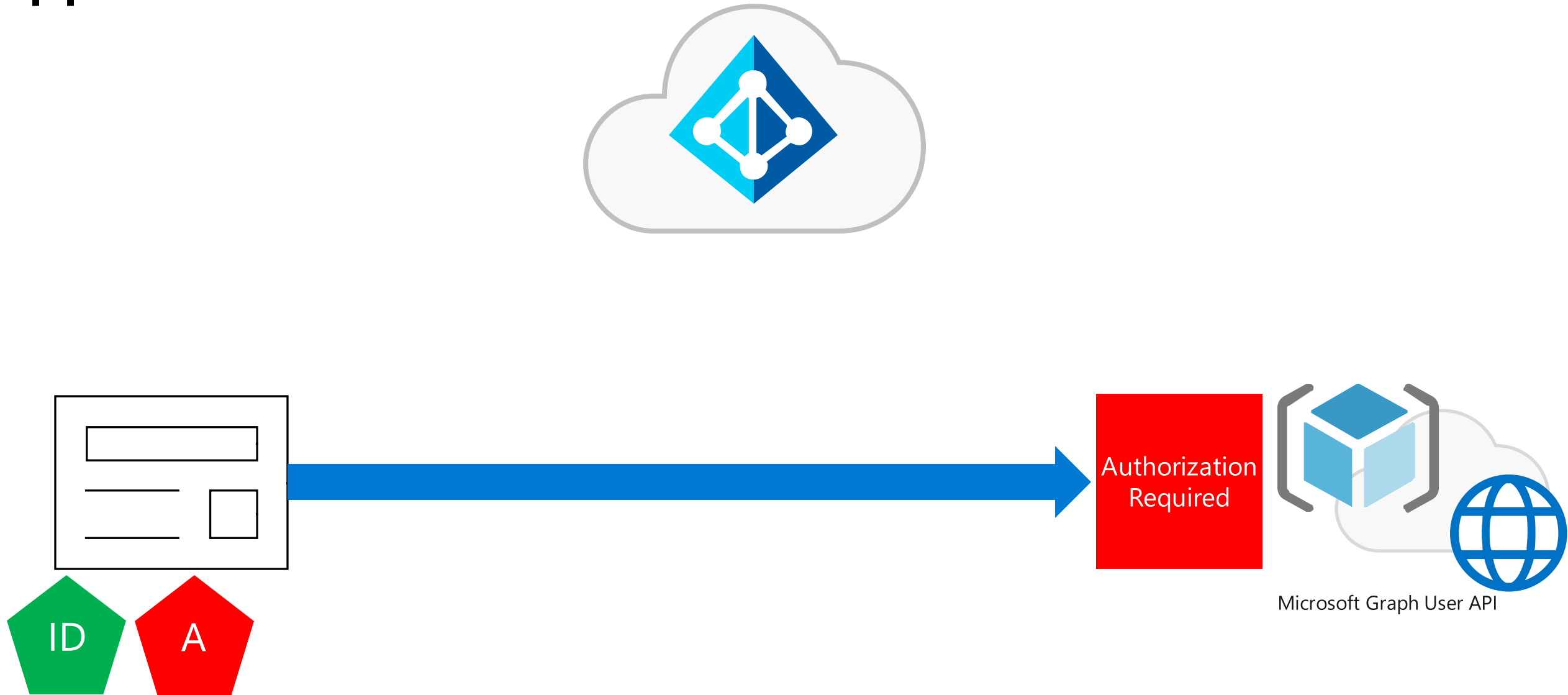
Call the API

Call the API

But what if I need to call another API?
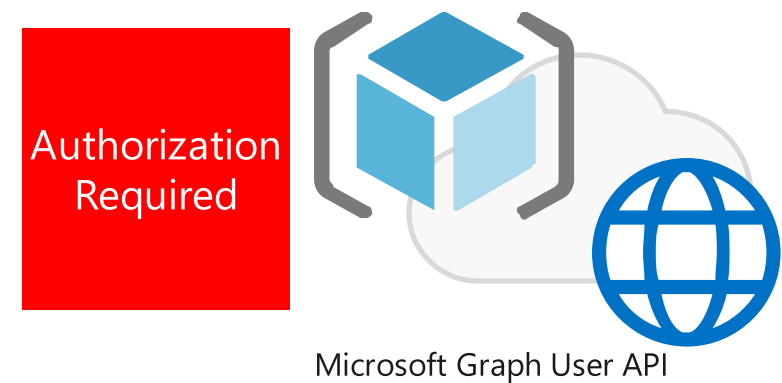
Apps asks Microsoft identity for another access token
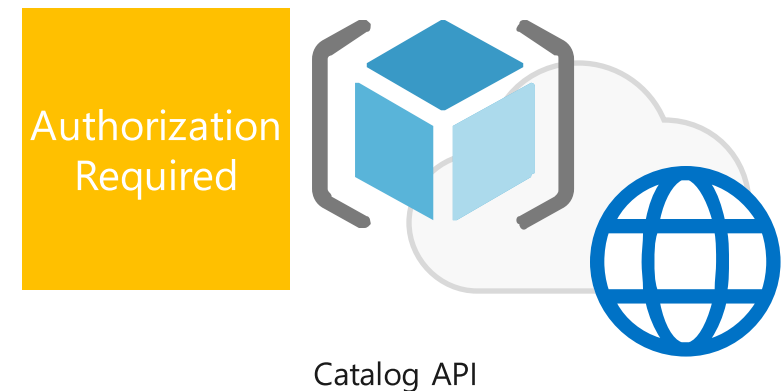
Need an access token to read the
catalog as the user

Authorization
Required

Catalog API

Authorization
Required

Microsoft Graph User API

ID

A

The core of SSO

Private conversation with the user

Authorization Required

Catalog API

Authorization Required

Microsoft Graph User API

App receives another access token

Private conversation with the user

Authorization Required
Catalog API

Authorization Required
Microsoft Graph User API
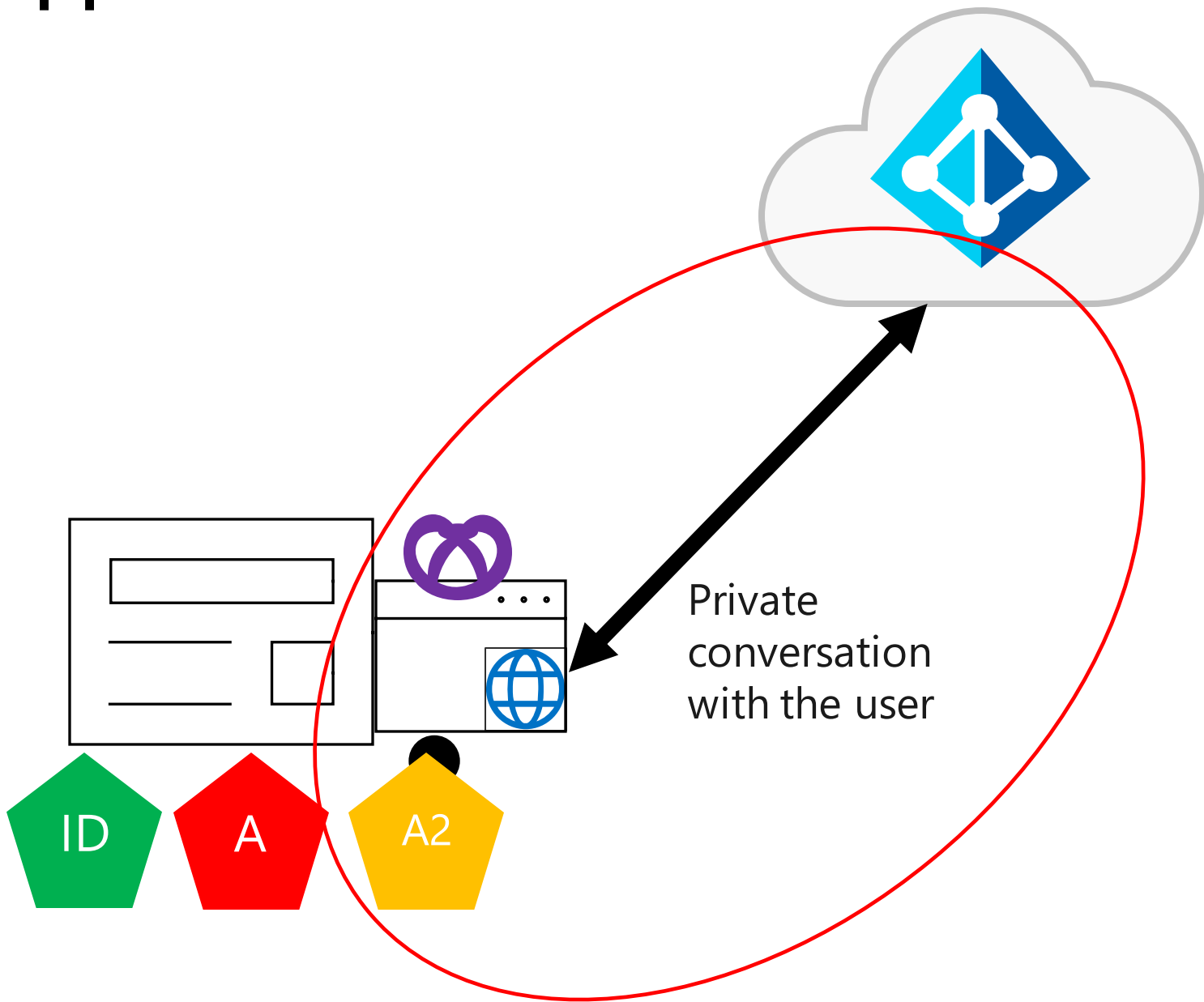
App has a token to call API

Authorization Required

Catalog API

Authorization Required

Microsoft Graph User API

ID   A   A2

Call the API

Call the API

A2

Catalog API

Authorization Required

Microsoft Graph User API

ID   A
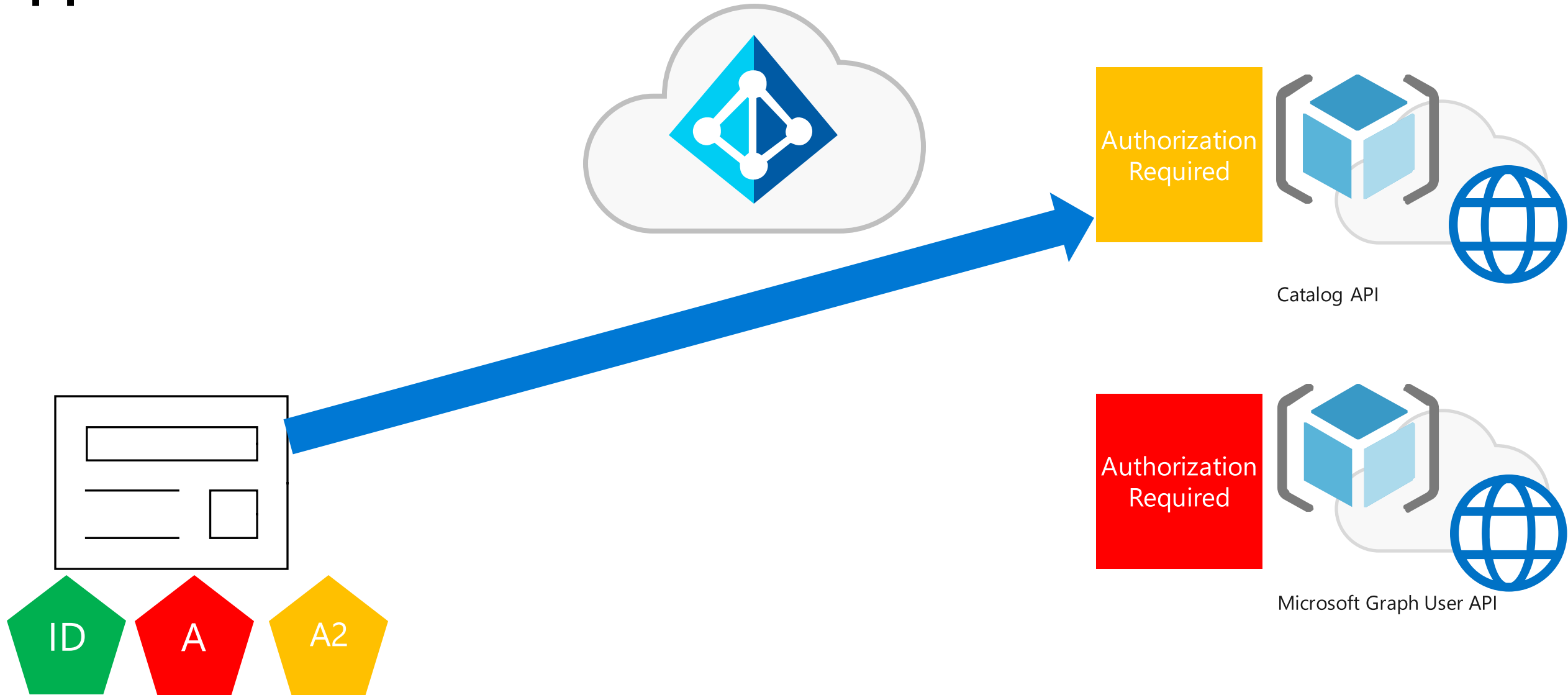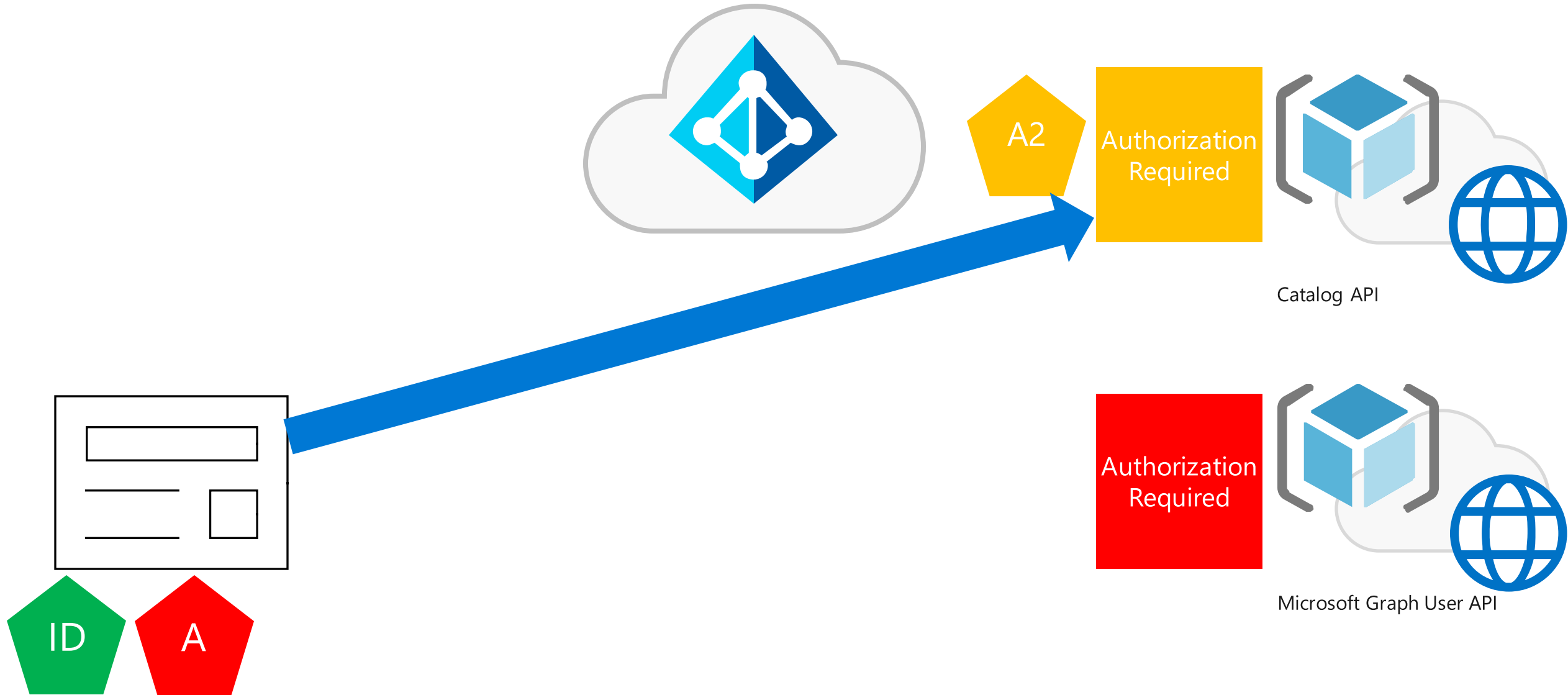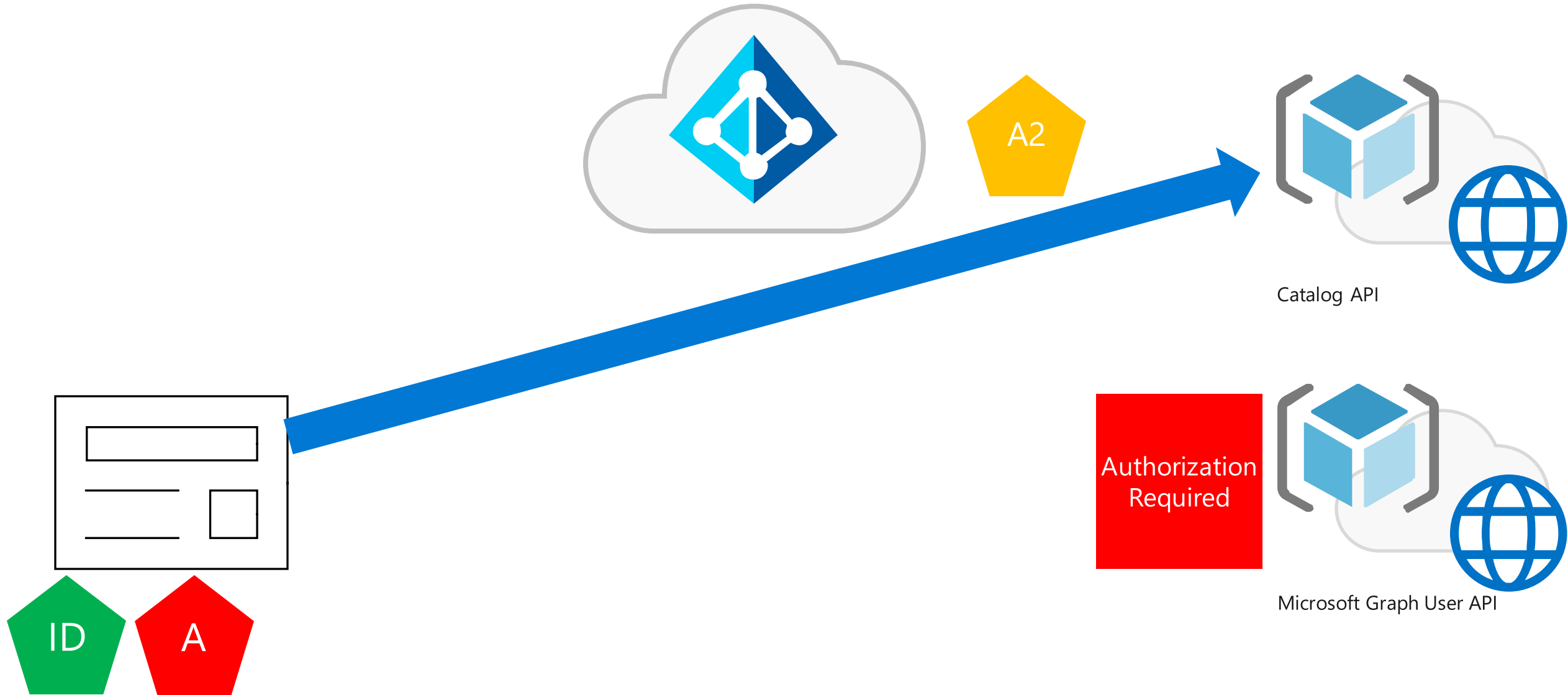
Best practices

Golden Rules for Tokens

Use tokens only for their intended function

      ID Tokens identify the user to the application

      Access tokens authorize the app for a range of operation for an API

Never mess with someone else's tokens

      Apps do not look at access tokens

      APIs never use ID Tokens for authorization

      APIs never accept Access Tokens for other APIs

Cache the tokens appropriately

      MSAL handles this automatically

Demo Debug Info

https://github.com/kylemar/BestPracticesDemo

Best practice for single sign on

Always try the silent token acquisition before attempting interactive token acquisition!

```
try
{
    result = await app.AcquireTokenSilent(scopes, account).ExecuteAsync();
}
catch(MsalUiRequiredException ex)
{
    result = await app.AcquireToken(scopes, account).ExecuteAsync();
}
```

This simple pattern enables SSO and handling IT policy.

Best practices for secure authentication

- Build your solutions by using libraries (MSAL, .NET middleware)
- Don't store login names and passwords. Use MSAL/B2C
- Apps shouldn't handle raw passwords (avoid ROPC)
- Confidential clients (daemon, web services) should use certs
- RedirectURI hygine

Best practices: aka.ms/msidbestpractice

Best practices for updating to MSAL

- Write your new apps using MSAL
- Update your ADAL apps to MSAL to get the latest innovation

Guides:

aka.ms/UpdateToMSALjs

aka.ms/UpdateToMSALNet

aka.ms/UpdateToMSALAndroid

aka.ms/UpdateToMSALiOSmacOS

THANK YOU