

Microsoft identity platform

Developer community call

Authentication in collaborative apps with Microsoft Teams and Microsoft Identity



Kyle Marsh

Principal Program Manager
Microsoft Entra
App Dev Architecture

June 16, 2022 | 9:00AM PT / 6:00PM CET

Introduction

- First things first
 - Please note: **We are recording this call** so those unable to attend can benefit from the recording.
 - This call is designed for developers who implement or are interested in implementing Microsoft identity platform solutions.
- What kind of topics will we discuss?
 - We will address development related topics submitted to us by the community for discussion.
 - We build a pipeline of topics for the next few weeks, please submit your feedback and topic suggestions - <https://aka.ms/IDDevCommunityCallSurvey>
 - View recordings on the Microsoft 365 Developer YouTube channel - <https://aka.ms/M365PnP/videos>
 - Follow us on Twitter **@Microsoft365Dev** and **@azuread**
 - This is NOT a support channel. Please use Stack Overflow to ask your immediate support related questions.
- When is the next session?
 - Community Calls: Monthly – 3rd Thursday of every month
 - Next Identity Developer Community Call: July 21st

AGENDA

Microsoft Identity dev community call 16th of June

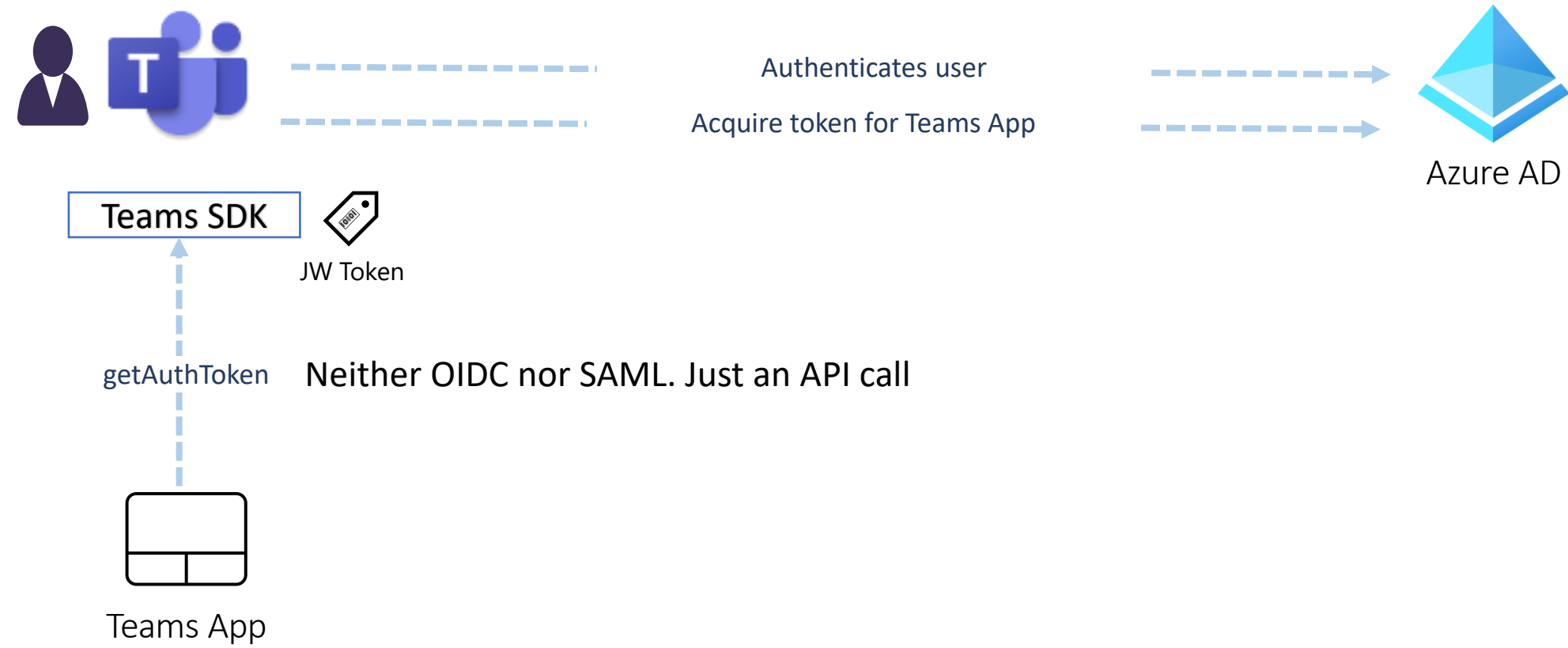
Download recurrent invite from
<https://aka.ms/IDDevCommunityCalendar>

Authentication in collaborative apps with Microsoft Teams and Microsoft Identity
– Kyle Marsh (Microsoft)

Environment

- Teams or Outlook or Office.com authenticate the user with Microsoft Entra
 - Azure AD native user, Guest Business to Business user, Microsoft Account
- Teams apps can authenticate the user to their system by asking Teams who the user is
- On-premise apps used to ask Windows, the OS, who the current user is.
- Teams apps (Outlook, Office.com) can ask Teams who the user is.

Teams SSO



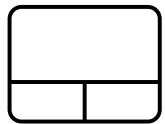
Teams SSO



Teams SDK



Azure AD



Teams App



JW Token

Really an access token for Teams to access your app.

Teams (Outlook, Office.com) is the client app

Your app is the resource

[Home](#) > [KylesDev](#) >

TeamsAuthSSO



Delete



Endpoints



Preview features



Overview



Quickstart



Integration assistant

Manage



Branding & properties



Authentication



Certificates & secrets



Token configuration



API permissions



Expose an API



App roles

^ Essentials

Display name : [TeamsAuthSSO](#) Client ID

Application (client) ID : 38666c8c-2066-4f19-9fa4-a1e5cc0a44fc Redirect URI

Object ID : 2c741923-ce52-40cf-a3d1-37556e50f381 Application ID

Directory (tenant) ID : cccc930d-c57e-4948-8d61-cd86afc7be46 Managed by

Supported account types : [All Microsoft account users](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL).




Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant applications.


[Get Started](#)[Documentation](#)

Application ID URI

api://teamsauthsso.kylemar.dev/38666c8c-2066-4f19-9fa4-a1e5cc0a44fc

 Add a scope

Scopes

	Who can cons...	Admin conse...	User co...	State
api://teamsauthsso.kylemar.dev/38666c8c-2066-4f19-9fa4-a1e5cc0a44f1/access_as_user	 Admins and users	My Teams App		Enabled

Authorized client applications

[+ Add a client application](#)

Client Id	Scopes
5e3ce6c0-2b1f-4285-8d4b-75ee78787346	1
1fec8e78-bce4-4aaf-ab1b-5451cc387264	1

More authorized client applications

+ Add a client application

Client Id	Scopes
4345a7b9-9a63-4910-a426-35363201d503	1
4765445b-32c6-49b0-83e6-1d93765276ca	1
0ec893e0-5785-4de6-99da-4ed124e5296c	1
bc59ab01-8403-45c6-8796-ac3ef710b3e3	1
00000002-0000-0ff1-ce00-000000000000	1
d3590ed6-52b3-4102-aeff-aad2292ab01c	1
5e3ce6c0-2b1f-4285-8d4b-75ee78787346	1
1fec8e78-bce4-4aaf-ab1b-5451cc387264	1

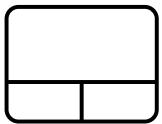
Teams SSO



Teams SDK



Azure AD



Teams App



JW Token

Locate user with tid+oid
If found, Consider the user authenticated and proceed

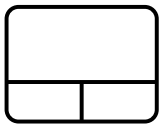
Teams SSO



Teams SDK



Azure AD



Teams App



JW Token

If the user (tid+oid) is not found have the user **authenticate existing IDP**.
Add tid+oid to user object in app system

Don't match on values that changed or can be spoofed

Where do your users come from?

- Personal account
 - kylemar@outlook.com
- Corporate License
 - Kyle.marsh@microsoft.com
- Personal account that used corporate email
 - Kyle.marsh@microsoft.com
- User in their home tenant
- User as a guest in a different tenant using corporate ID
- User as a guest in a different tenant using their personal account

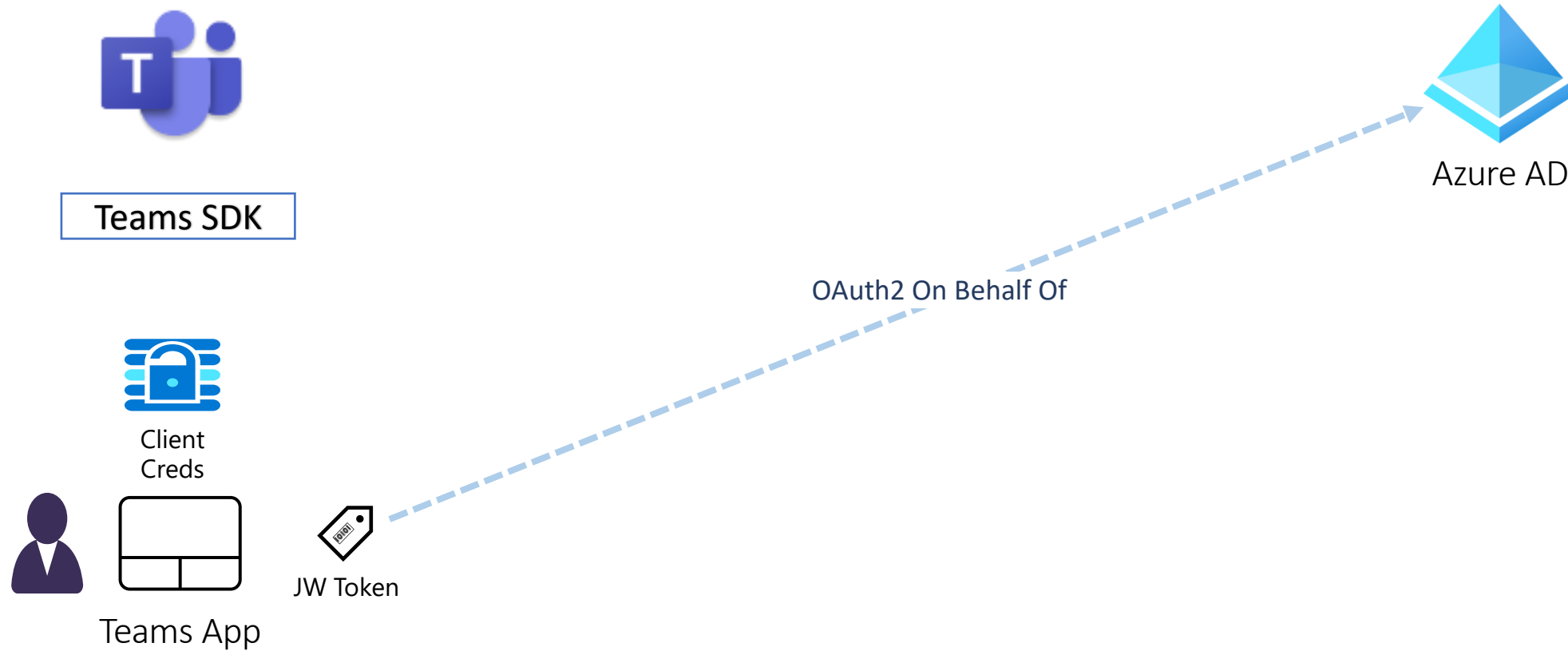
Be prepared for a many to many relationship for account linking

Just need to authenticate the user?

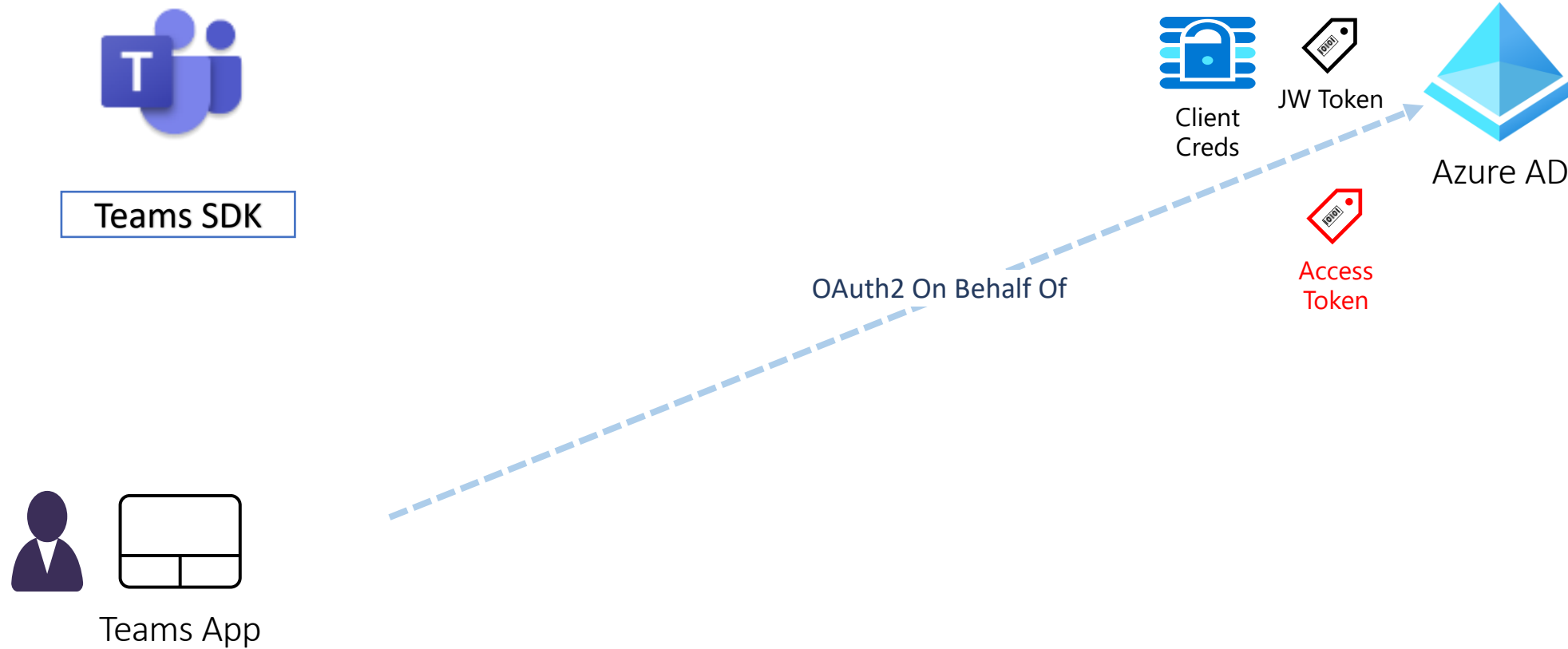
- Stop now.
- To call an API, any API, protected with Microsoft Entra you need a different token
- 2 choices
 - On behalf Of from a secure back end - preferred
 - Regular OAuth2 request from client

On Behalf Of

Teams Authorization



Teams Authorization



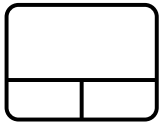
Teams Authorization



Teams SDK



Azure AD



Teams App Access
Token



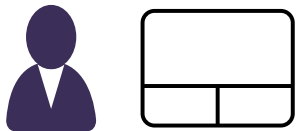
Teams Authorization



Teams SDK



Azure AD



Teams App



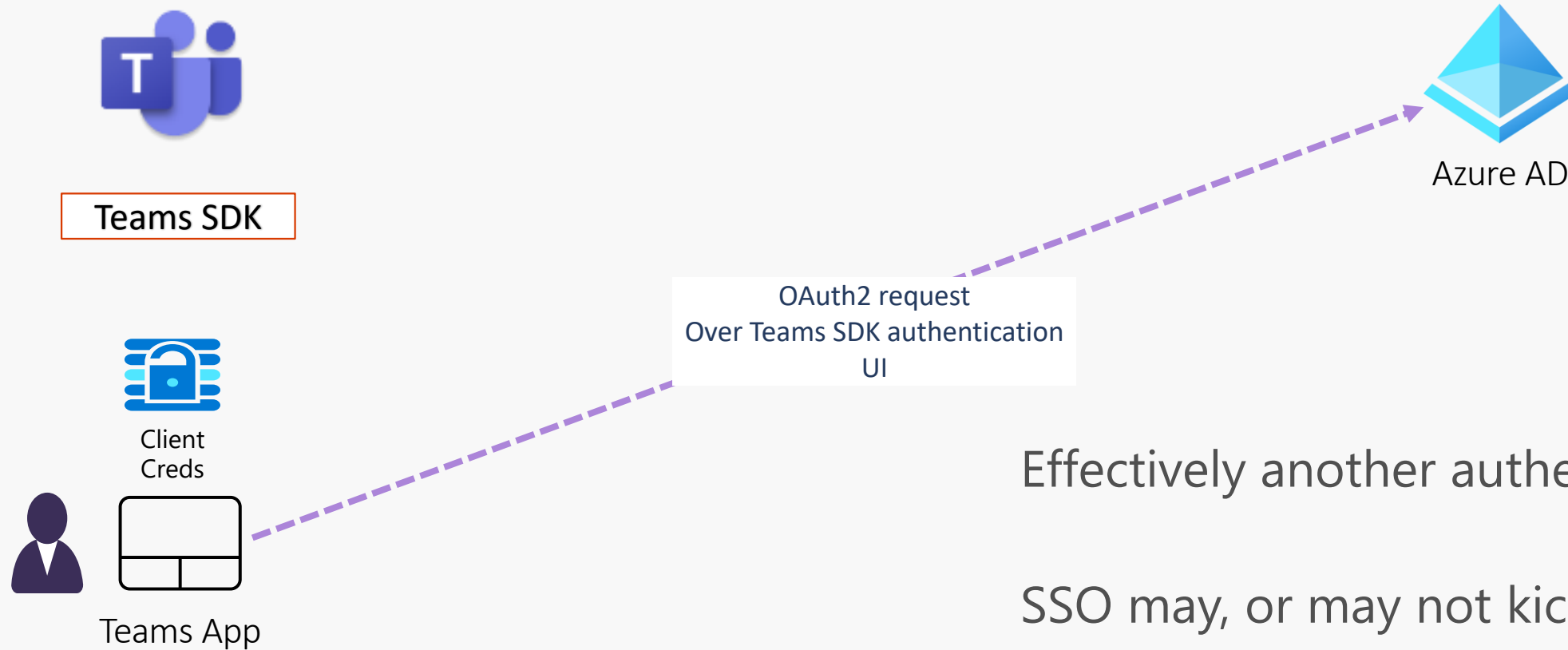
Access
Token



Microsoft
Graph

On Behalf Of

Teams Authorization



Effectively another authentication

SSO may, or may not kick in

Only option for SPA

Questions

Thank you

Recording will be available soon on the
Microsoft 365 Community (PnP) YouTube channel

<https://aka.ms/M365PnP/videos>

(subscribe today)

Follow us on Twitter

[@Microsoft365Dev](#) and [@azuread](#)

Next call: **July 21st at 9:00am PST**

<https://aka.ms/IDDevCommunityCalendar>