Modern Identity for Developers

Ronny Hansen
Cloud Solution Architect OCP

Ronny.Hansen@microsoft.com

Sander van den Hoven
Cloud Solution Architect ISV OCP
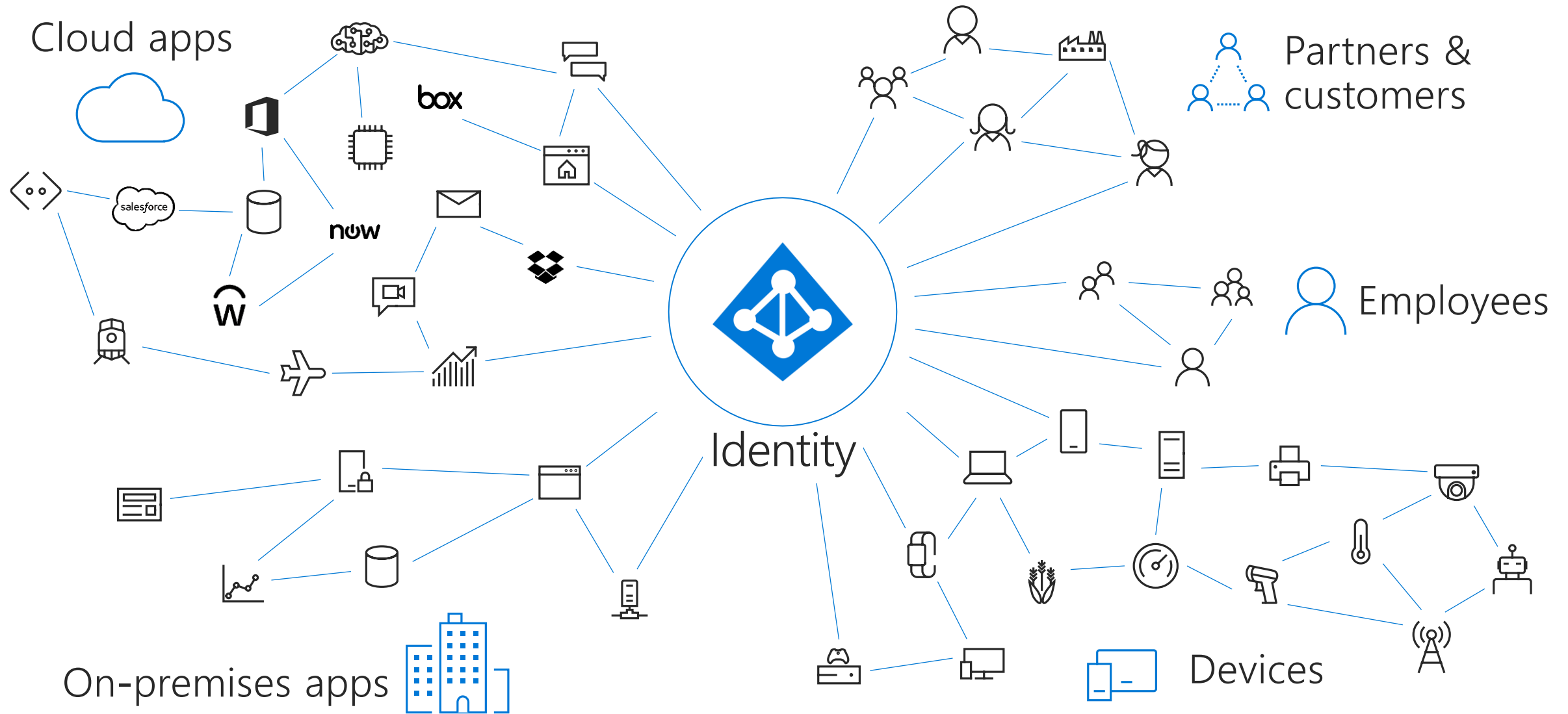
sandervd@microsoft.com

Agenda

- Why build with Microsoft Identity Platform
- B2B (Azure AD)
- B2C (Azure AD B2C)
- Integrate with Microsoft 365
- Single Tenant vs Multitenant
- What is Microsoft Identity Platform
- Demo
- Next steps
- Q&A

Let's start with some code

```
34  var graphConfig = {
35      graphMeEndpoint: "https://graph.microsoft.com/v1.0/me",
36      graphMePhotoEndpoint: "https://graph.microsoft.com/v1.0/me/photo/$value",
37  };
38
39  // create a request object for login or token request calls
40  // In scenarios with incremental consent, the request object can be further customized
41  var requestObj = {
42      scopes: ["user.read"]
43  };
44
45  var myMSALObj = new Msal.UserAgentApplication(msalConfig);
46
47  // Register Callbacks for redirect flow
48  // myMSALObj.handleRedirectCallbacks(acquireTokenRedirectCallBack, acquireTokenErrorRedirectCallBack);
49  myMSALObj.handleRedirectCallback(authRedirectCallBack);
50
51  function signIn() {
52      myMSALObj.loginPopup(requestObj).then(function (loginResponse) {
53          //Successful login
54          showWelcomeMessage();
55          //Call MS Graph using the token in the response
56          acquireTokenPopupAndCallMSGraph();
57      }).catch(function (error) {
58          //Please check the console for errors
59          console.log(error);
60      });
61  }
62
63  function signOut() {
64      myMSALObj.logout();
65  }
```

Identity is the control plane

Cloud apps

Partners & customers

Employees

Identity

On-premises apps

Devices

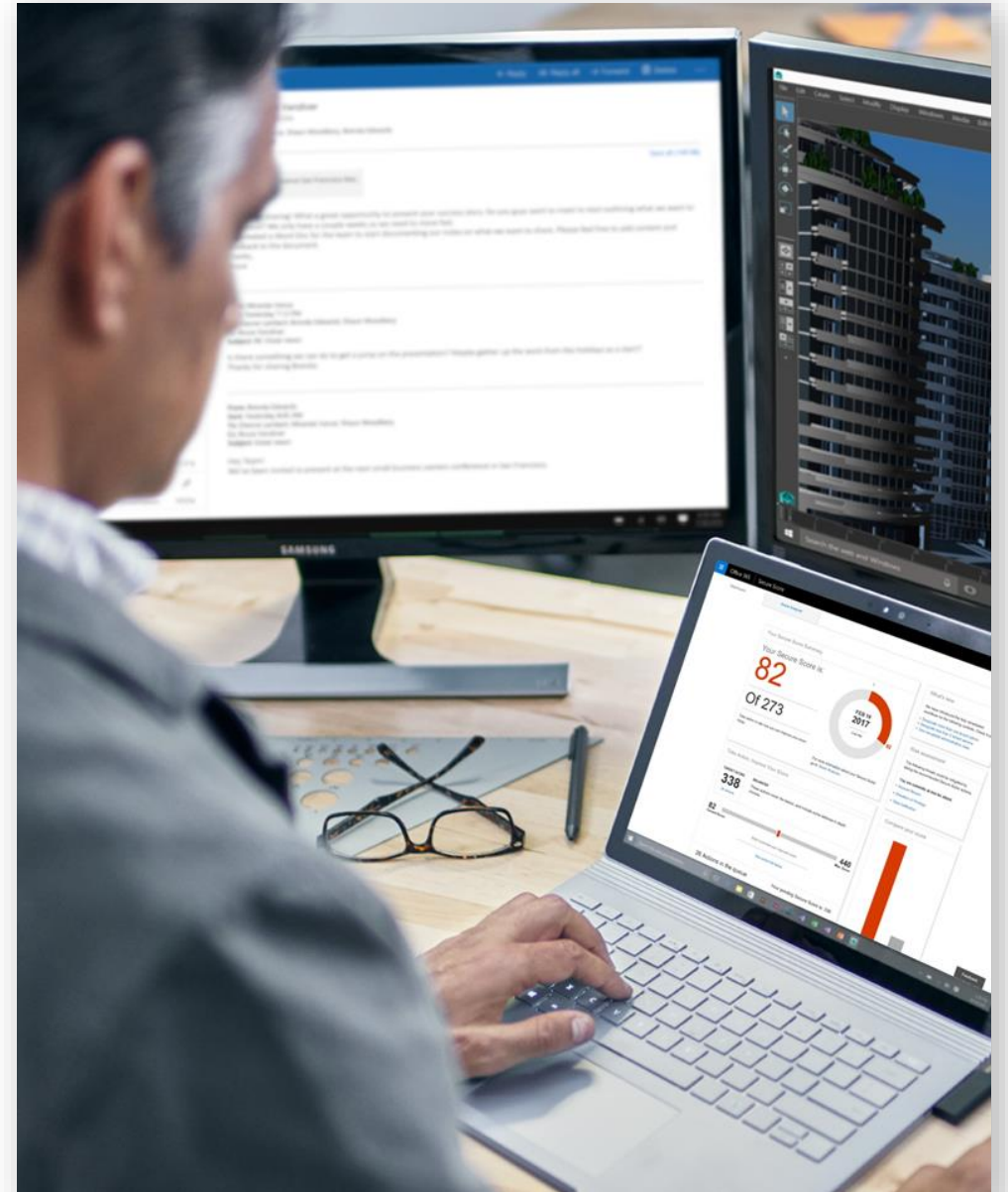# How secure and accessible is your application?

How can I accelerate adoption and usage with enterprise customers?

How can I secure my application and lower maintenance and support costs?

How do I build richer applications that can securely access user data in Microsoft 365?

Why build with the Microsoft identity platform

Unified toolkit to reach any Microsoft identity – personal Microsoft accounts to Azure AD accounts

Reach consumers and enterprises

Let your users sign in with their Microsoft personal account or work or school account provisioned by Azure AD

Protect your app and users

Comply with IT policy and extend the security benefits to your app for customers who use Azure AD

Create powerful apps

Build the next generation of apps and experiences by connecting to the Microsoft Graph

Integrate with ease

Build with confidence using our authentication libraries and open industry standards on a trusted, reliable platform

Azure Active Directory by the numbers
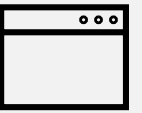The world's #1 enterprise identity service

22.5M
organizations
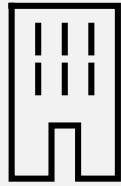
1.3B
identities

1.4M
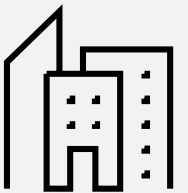third-party apps

100M
paid Azure AD/EMS seats

45B
daily Azure AD authentications

90%
of Fortune 500 companies
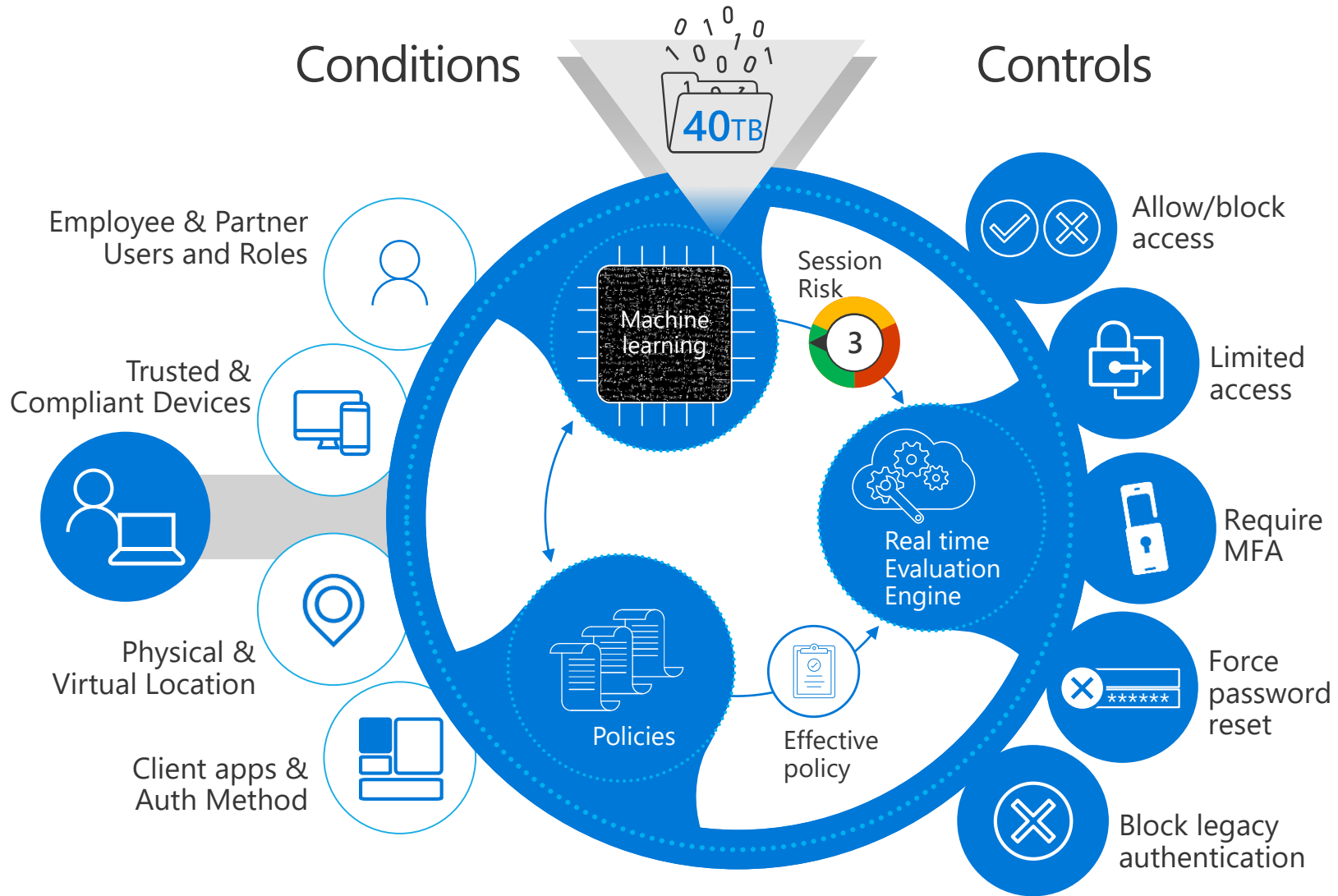
October 2019

Partners – Business to Business (B2B)

Customers – Business to Customers (B2C)
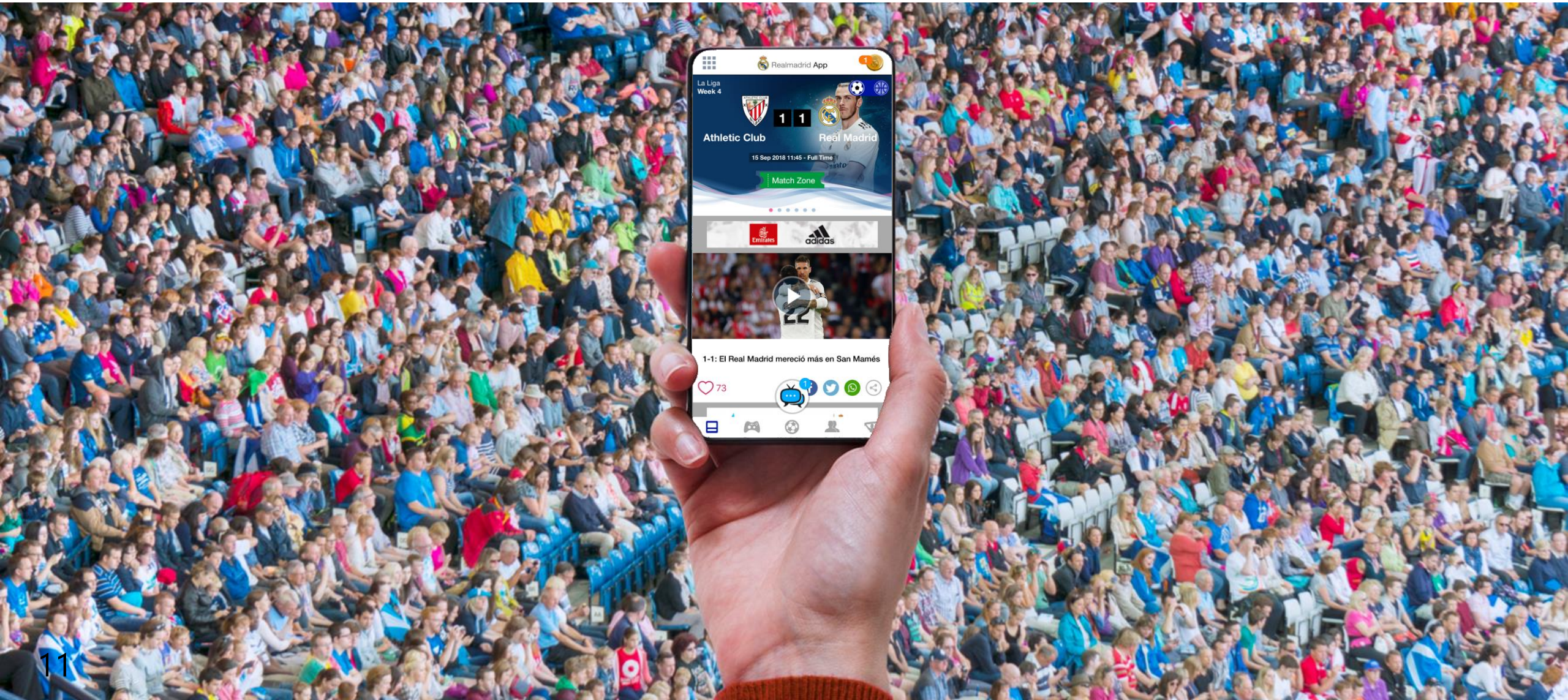
B2C provides simple, reliable and secure, SSO access to customer-facing apps with social or business IDs .

Customers

Social IDs, email, or local accounts

Any SAML provider

Business & Government IDs

Any OIDC provider

Azure Active Directory B2C

OAuth2

OIDC

Business

API

Web App

Mobile App

Azure AD integration	Connect with existing systems
SSO to customer apps	Social accounts
Use your own branding	Open standards
Native sign-in experience	Enrich user journeys
Self-service capabilities	Compliance

Azure AD versus Azure B2C for ISV

Azure AD
Directories
+ MSA

federate

Azure AD

App registered   redirect

App

Any OpenId
Or SAML RDP

federate

Azure B2C

App registered   redirect

App
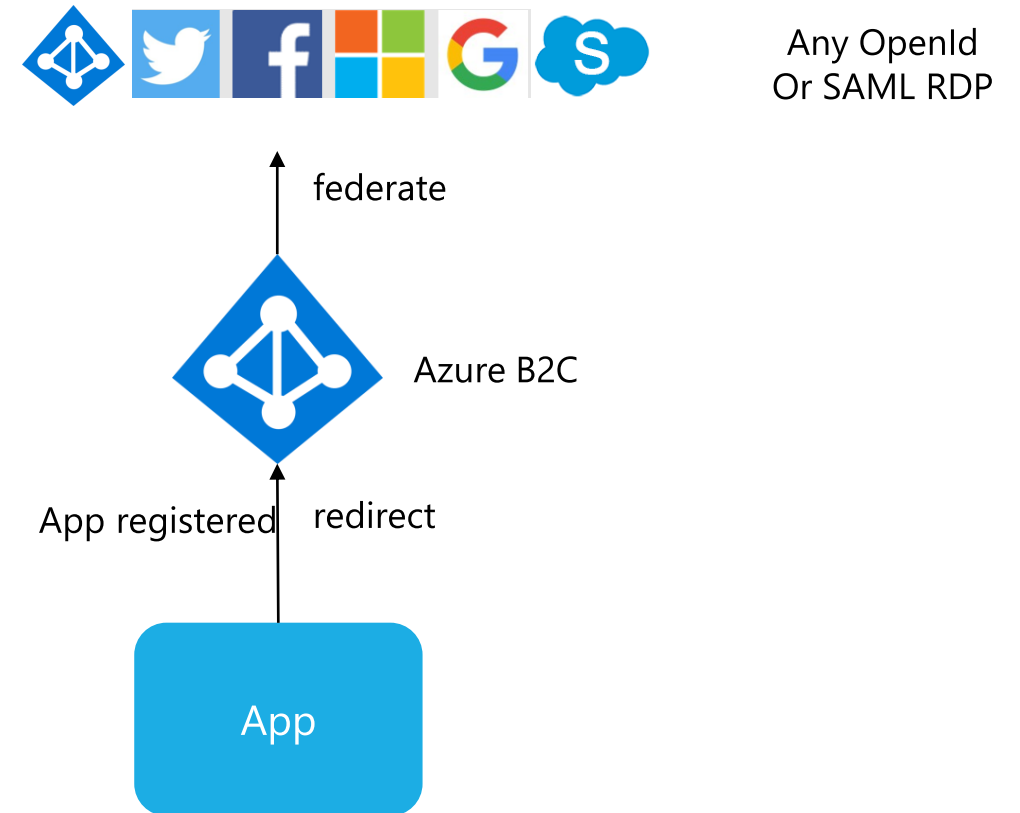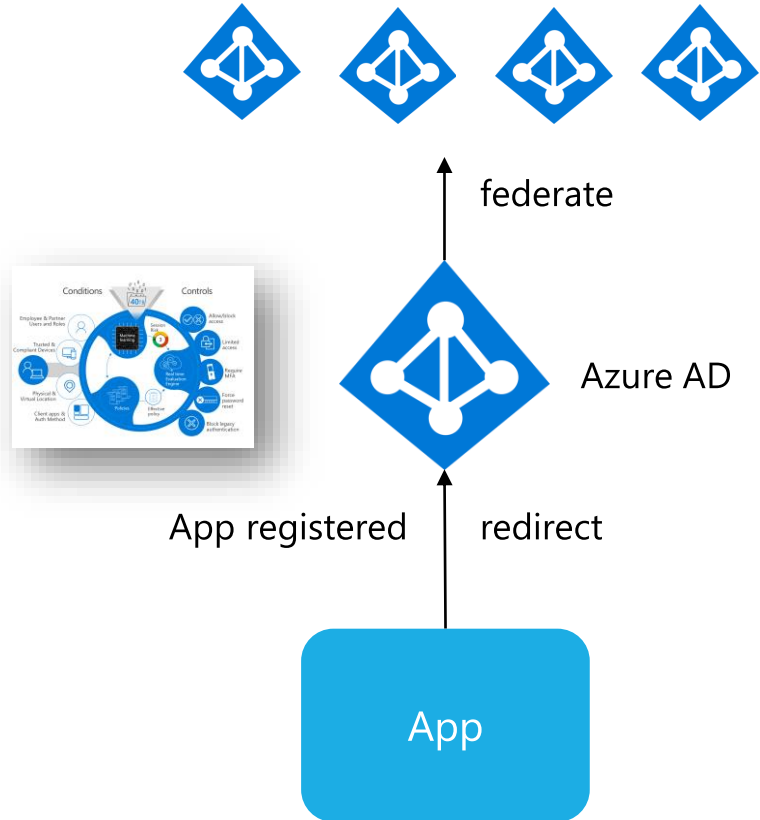
Integrate with Microsoft 365

Microsoft 365 Platform

Extend Microsoft 365 experiences

Documents

Conversations

Portals

Timeline

Search

Build your experience

Web apps

Bots & agents

Device & native

Daemon apps

Workflow automation

Analytics apps
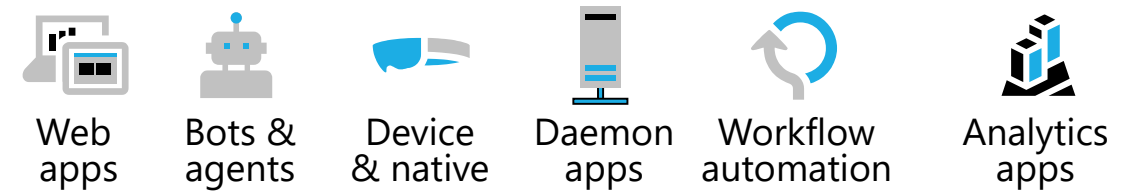
Microsoft Graph API

Microsoft 365

People

Chats

Files

Devices

Mail

Alerts

Lists

Security

Search

Events

• • •

Single tenant vs multi tenant (for Azure AD)

Single Enterprise App – Users come from only one enterprise

App registered for a specific Azure AD directory

Single-tenant

Registered with Azure Portal, script, automation provided by developer

Admins decide who can register apps in their tenant

App
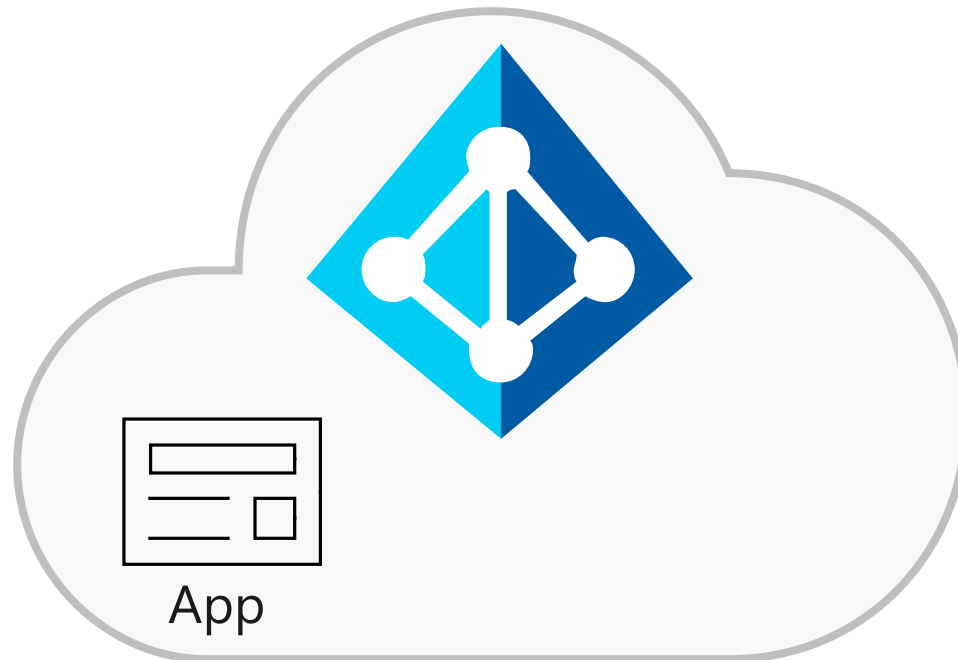
Making getting your app easier

App registered for use in any Azure Directory or any Azure AD and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

Multi-tenant

Registered in its "Home" directory (same process as single-tenant)

Admins decide who can consent to apps in their tenant
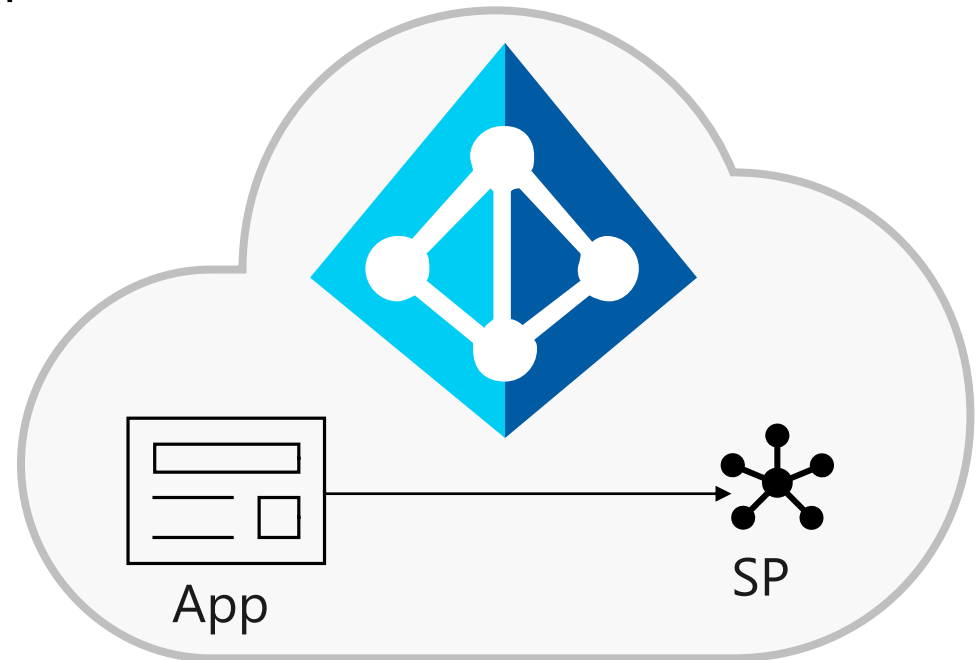
Microsoft

Microsoft Identity Platform (evolution of Azure AD for Developers)

Microsoft identity platform

http://aka.ms/IdentityPlatform

What type of app are you building?

Single-page app (SPA)

- Register app + complete quickstart (Sign-in users & call API pattern)
- Configure permissions & call API of choice

Web app

- Register app + complete quickstart (Sign-in users & call API pattern)
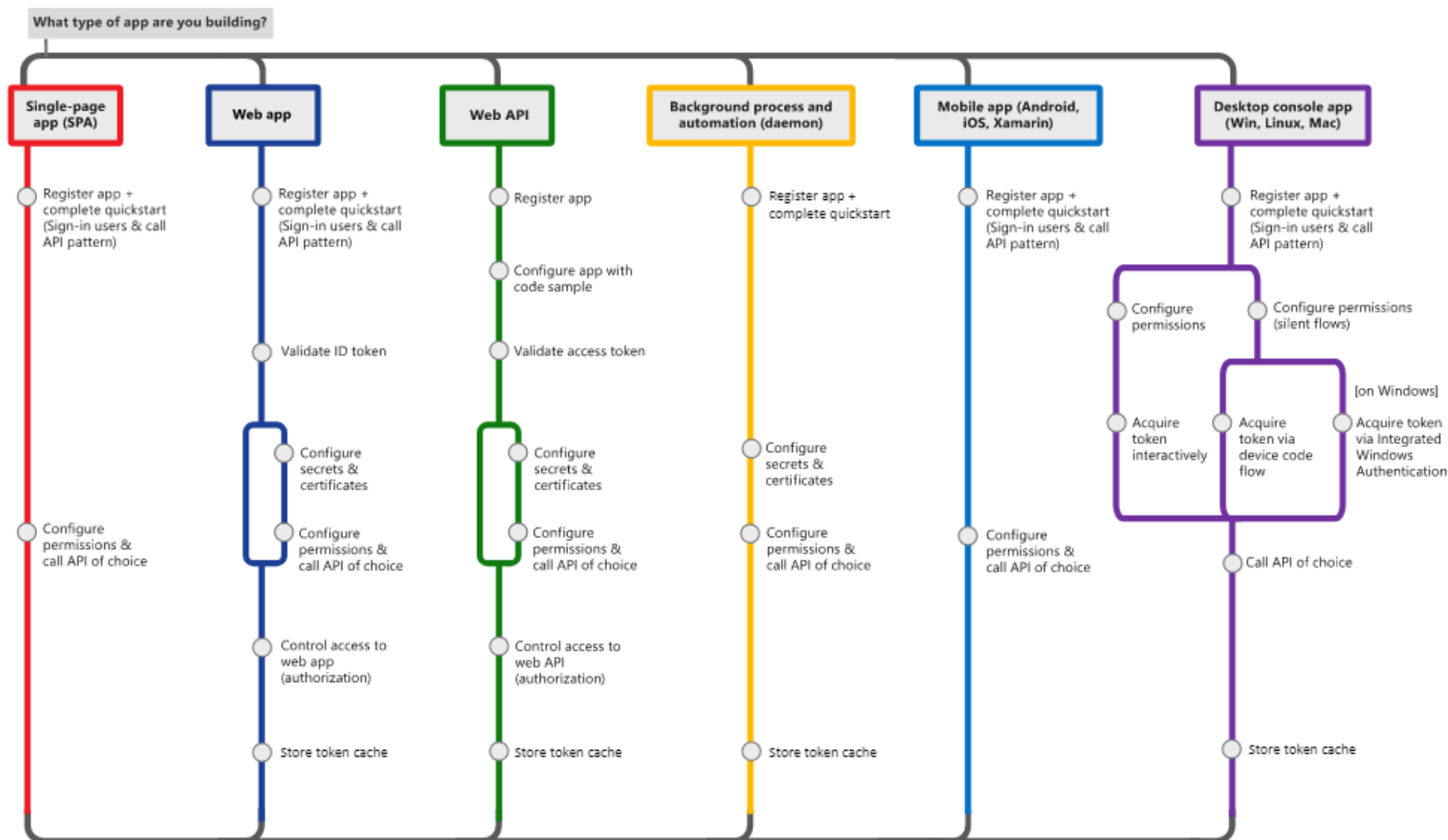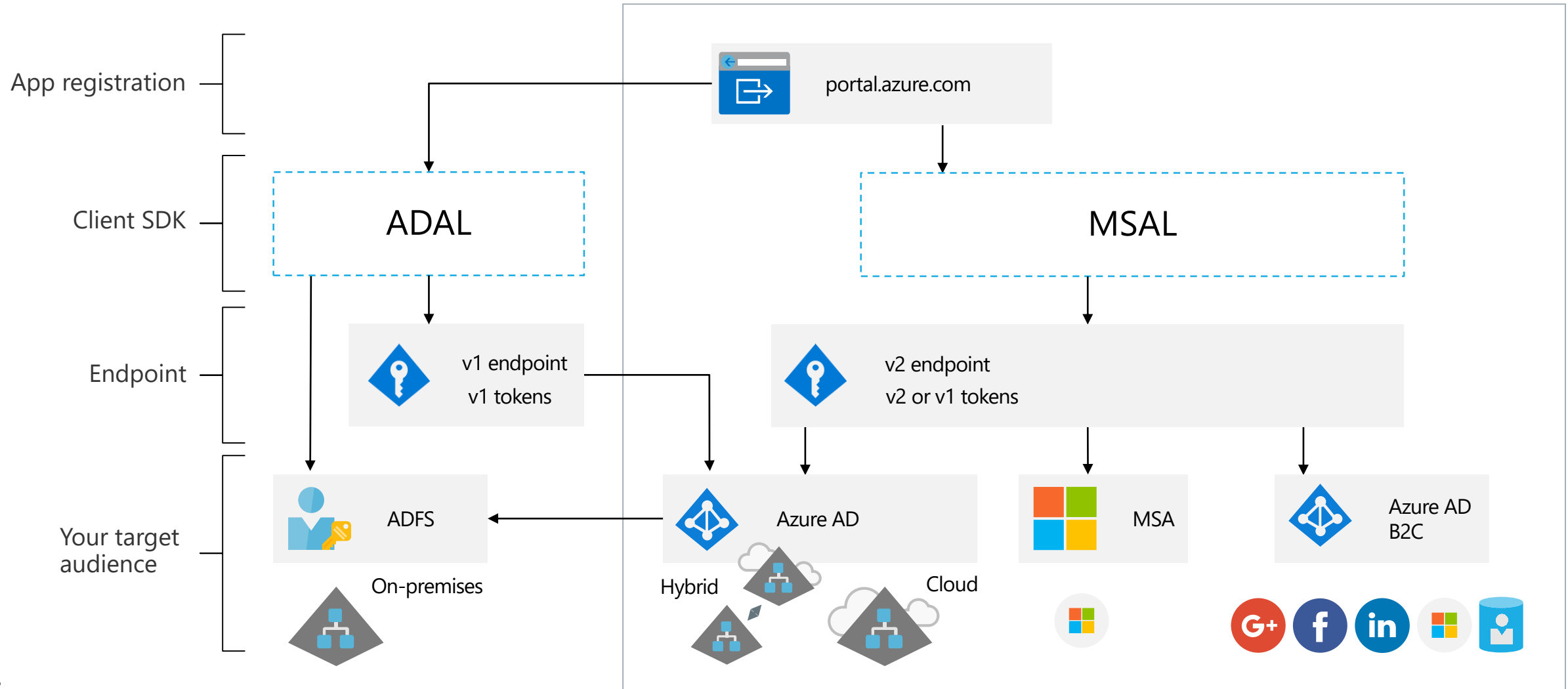- Validate ID token
- Configure secrets & certificates
- Configure permissions & call API of choice
- Control access to web app (authorization)
- Store token cache

Web API

- Register app
- Configure app with code sample
- Validate access token
- Configure secrets & certificates
- Configure permissions & call API of choice
- Control access to web API (authorization)
- Store token cache

Background process and automation (daemon)

- Register app + complete quickstart
- Configure secrets & certificates
- Configure permissions & call API of choice
- Store token cache

Mobile app (Android, iOS, Xamarin)

- Register app + complete quickstart (Sign-in users & call API pattern)
- Configure permissions & call API of choice

Desktop console app (Win, Linux, Mac)

- Register app + complete quickstart (Sign-in users & call API pattern)
- Configure permissions
- Configure permissions (silent flows)
- Acquire token interactively
- Acquire token via device code flow
- Acquire token via Integrated Windows Authentication [on Windows]
- Call API of choice
- Store token cache

Microsoft Identity Platform

Unified toolkit for building identity-connected applications

Fast and simple integration
Authentication libraries

- Secure access to users and data made simple
    - Microsoft's world (Microsoft Graph, other APIs)
    - Your own APIs

- MSAL - best in class auth libs
    - Built for v2 endpoint, reach any audience
    - Follows Microsoft Security Development Lifecycle

- Update at your own pace
    - ADAL based apps continue to work
    - Portfolio of ADAL and MSAL apps get Single Sign On

MOBILE APP   CLIENT SDK

Microsoft Authentication Libraries (MSAL)

.NET, JS GA at Build

Updates frequently

Adding new features to MSAL only, security updates for ADAL

JavaScript

Angular

.NET

UWP

Java

Android

iOS

Xamarin

Python

Open Standards

Demo

Next steps

Modern Identity – Deep Dive Webinar Serie

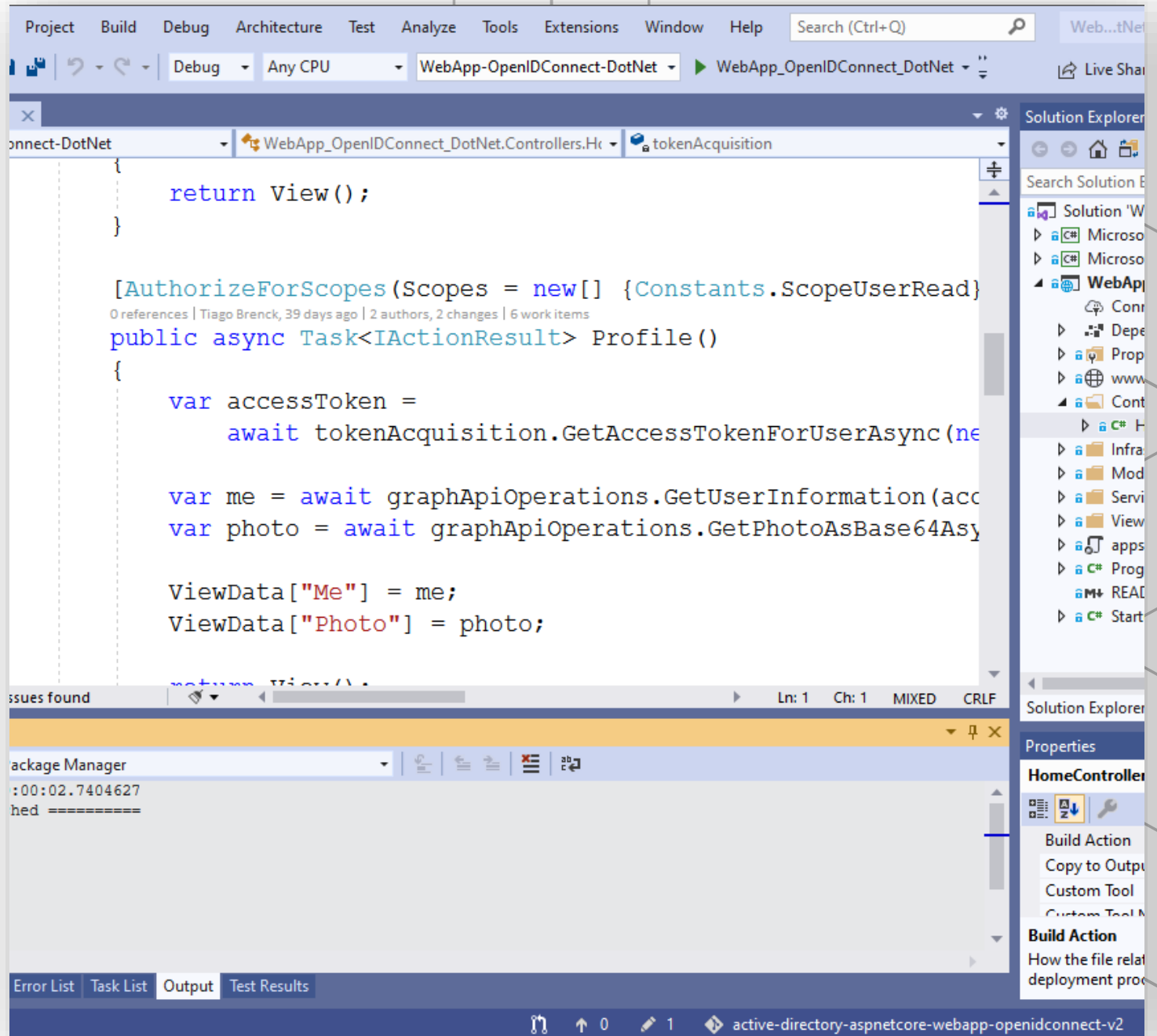Repeat topic Monday and Thursday – One topic pr week

Format: 45 minutes presentation. Intro to homework, Q&A. Listeners get a coding excercise as homework.

1. Adding Authentication   Week 18
2. Permission and Consent framework   Week 19
3. Accessing and protecting API's   Week 20
4. Authorization   Week 21
5. Azure Active Directorey B2C   Week 22
6. Best practices for securing your services Week 23

1:1 Hands on Modern Identity Enablement for select ISV's

Accelerate partner competence and help them integrate their products with Azure Active Directory for managing their identity through a 4-step virtual engagement

1. Architecture Design Session (ADS)

2. Make the ISV Application multitenant (Guidance on how to architect and implement the solution to be multi-tenant)

3. Enable ISV application to integrate with Azure AD (Hands on training and guidance to do the integration through our toolkits)

4. Register the application in Azure Active Directory App Gallery

This offer is only valid to managed partners that has a multitenant app or that want to make their application multitenant.

Resources

Accelerate adoption and protect your application

SERVICE & SUPPORT
[Stack Overflow](#) | [Support](#)

DOCS
[Azure Active Directory](#) | [Microsoft Identity Platform](#) | [Microsoft Graph](#)

TOOLS
[Quick Starts](#) | [Graph Explorer](#) | [MSAL Libraries](#)

PRODUCT INFLUENCE
[UserVoice](#) | [MSAL Survey](#)

Bookmark or subscribe

developer.microsoft.com/identity/blogs/

azure.microsoft.com/services/active-directory

[github.com/AzureAD](#)

[aka.ms/MsIdStackOverflow](#)

[@AzureAD](#), [@msiddev](#)

Get your completed integrations listed into our app gallery by submitting it to [aka.ms/AzureADAppGallery](#)

Microsoft

Ronny.Hansen@Microsoft.com