TECH DAYS 2015

BREAKING NEW GROUND

Microsoft

Introduction to Azure Active Directory for Developers

Jelle Druyts | Premier Field Engineer | Microsoft Services

Microsoft

Agenda

Identity in modern applications

Azure Active Directory for developers

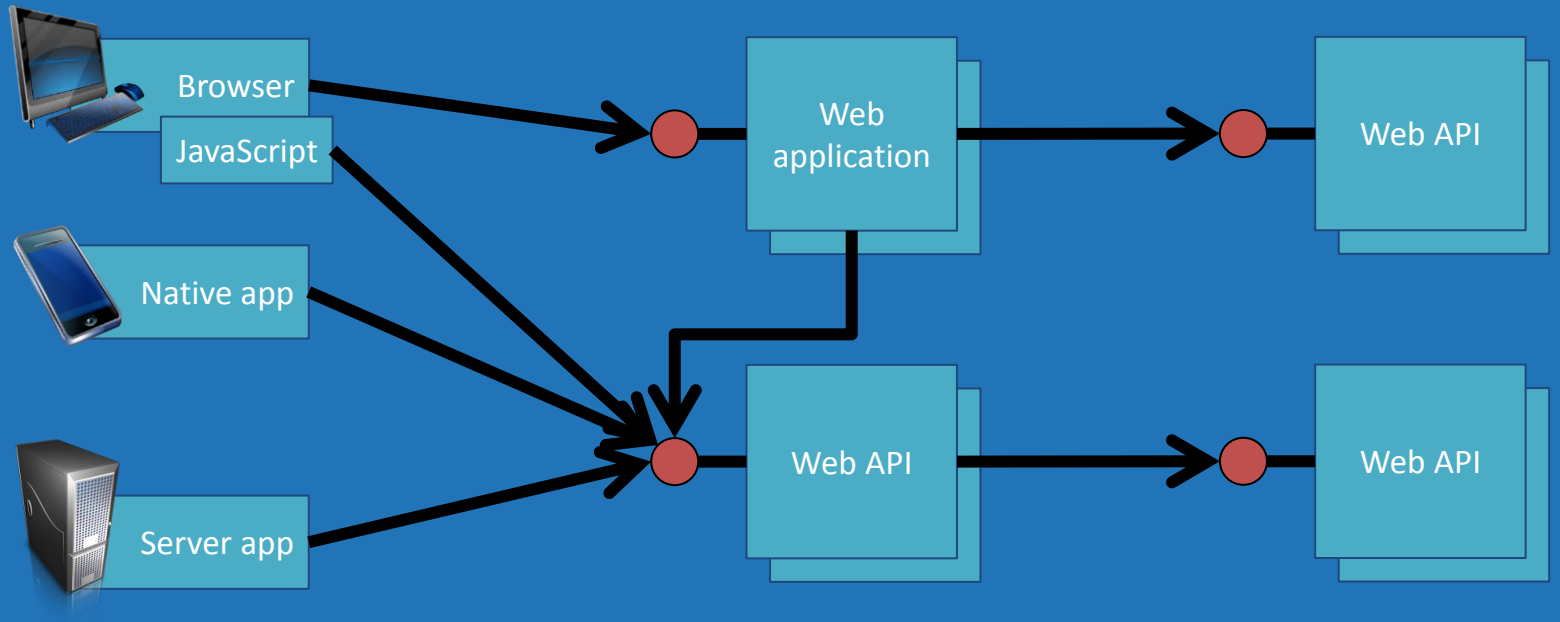
Azure Active Directory futures

Microsoft

Identity in Modern Applications

Microsoft

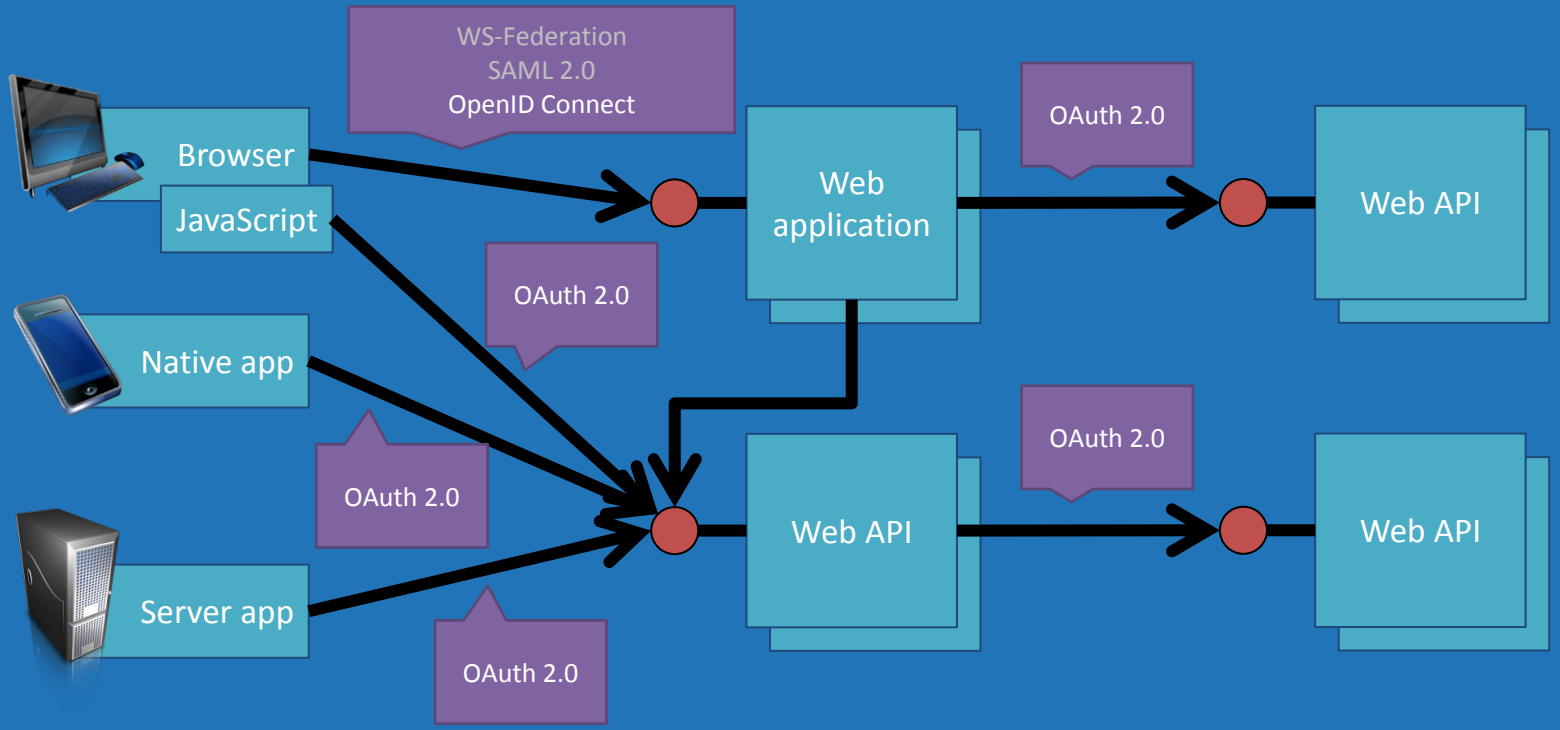
Today's Applications



Clients using wide variety of devices/languages/platforms

Server applications using wide variety of platforms/languages

Authentication Protocols



Standard-based, HTTP-based protocols for maximum platform reach

OAuth 2.0

Using authorization tokens to avoid handing out your credentials

Authorization Code Grant – Public Client	Browser-based authorization (user identity)
Authorization Code Grant – Confidential Client	Server to server authorization (user identity)
Client Credentials Grant	Server to server authorization (client identity)
Implicit Grant	JavaScript based authorization (e.g. SPA)
Resource Owner Password Credentials Grant	Sending user's actual *credentials* through highly trusted app
Refresh Token Grant	Refreshing expired tokens without prompting user
On-Behalf-Of Grant	Multi-hop server to server authorization

Tokens

What applications use to access a resource on your behalf

Tokens are packages of claims

- Usually digitally signed by the issuer
- Different formats: SAML, SWT, JWT, …

"Bearer" tokens require no additional proof that you are the intended recipient for the token

- *So… don't lose them (rely on transport security and store safely)*

Microsoft

Claims

What the application sees about you

Claim Type	Example Value	Purpose
Object ID	3b62dcc4-2213-40ef-924b-9387019d2b22	Immutable and reliable user ID
Name	John Doe	Displayable user name
Audience	http://api.contoso.com/	Target application ID
Issuer	https://sts.windows.net/6272ea46-5ba0-4854-b99e-cd76a754ef1b/	Security Token Service ID
Groups	Marketing, Sales	Groups the user is member of
Roles	Reader, Contributor	Roles the user was assigned
...	...	...

OpenID Connect

Using OAuth 2.0 for user authentication

OAuth 2.0 is purely for *authorization*, not *authentication*

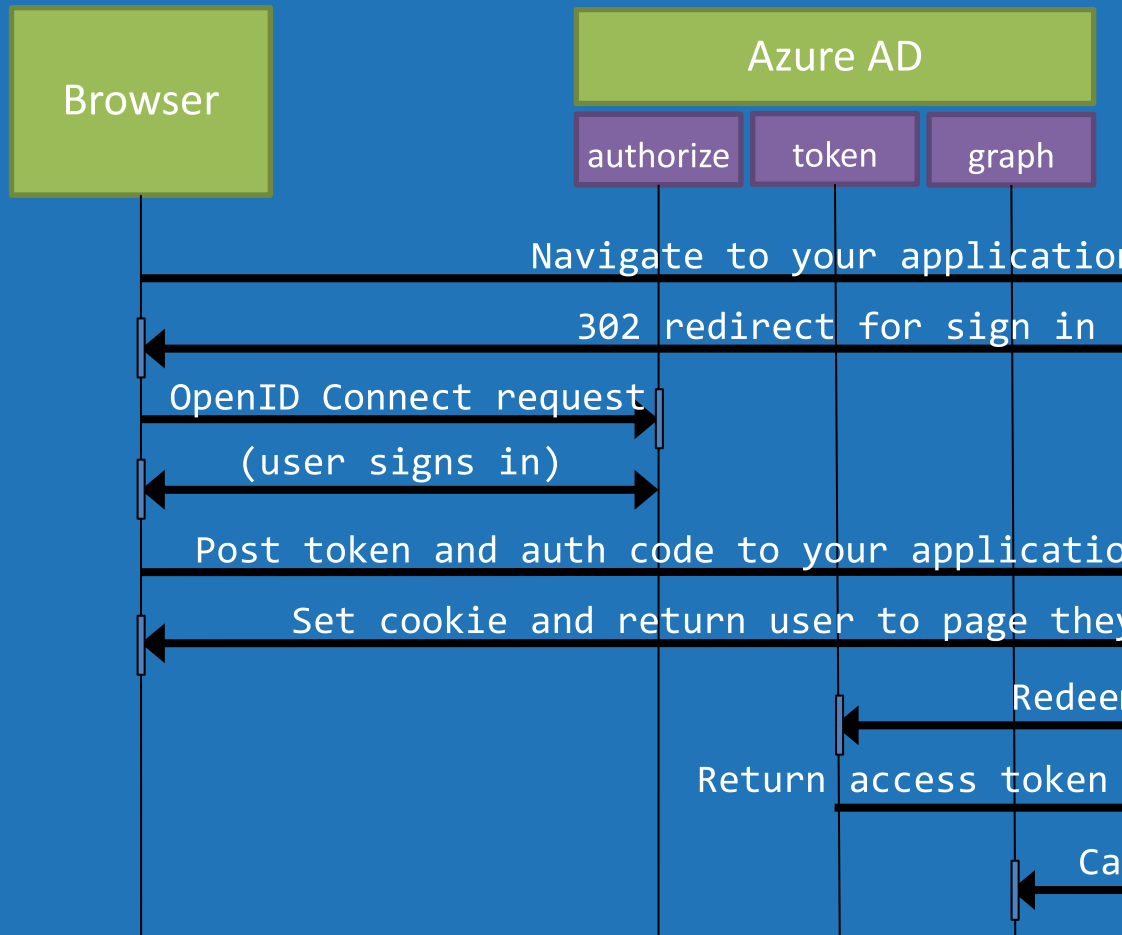
- Access Token
- Refresh Token

OpenID Connect builds on OAuth 2.0 and adds authentication information

- ID Token: JWT with at least a “sub” claim to identify the end user (“subject”)
- UserInfo Endpoint: returns more claims about the end user (JSON/JWT)

```
{
  "sub": "248289761001",
  "name": "Jane Doe",
  "given_name": "Jane",
  "family_name": "Doe",
  "email": "janedoe@example.com",
  "picture": "http://example.com/janedoe/me.jpg"
}
```

Sign-In + Web API Call



No session, send authN request

Verify token signature

Demo: Identity in Modern Applications

Microsoft

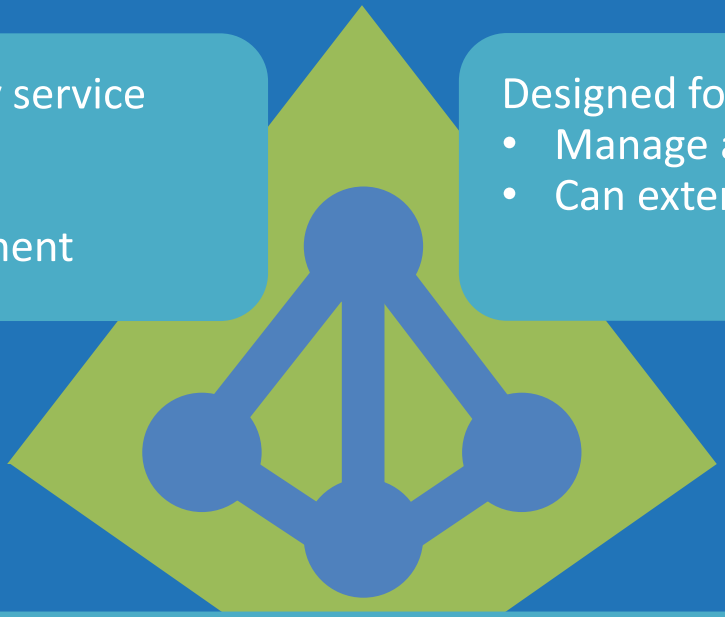
Azure Active Directory for Developers

Microsoft

What Is Azure Active Directory?

Cloud-based identity service
- Authentication
- Directory
- Identity Management

Designed for organizations
- Manage access to cloud apps
- Can extend on-premises AD



- Designed for cloud and mobile
- HTTP/REST & industry standard protocols

Bottom line: sign-in users from organizations without being responsible for their accounts

TECH DAYS 2015
BREAKING NEW GROUND

Microsoft

Azure AD By The Numbers

86%
of Fortune 500 companies on Microsoft Cloud (Azure, O365, CRM Online and PowerBI)

Azure AD manages identity data for
>5 M
organizations

More than
500 M
objects hosted on Azure Active Directory

1 Trillion
Azure AD authentications since the release of the service

50 M
Office 365 users active every month

>1 Billion
authentications every day on Azure AD

Every Office 365 and Microsoft Azure customer uses Azure Active directory

TECH DAYS 2015
BREAKING NEW GROUND

Microsoft

Developer Features

#1: You never need to store another password again

Identity management
- Manage users & groups
- Manage applications & permissions

Authentication
- Signing in to applications

Authorization
- Getting tokens to access resources
- Group membership
- Application Roles (“RBAC”)

Microsoft

Security Features

Imagine you had to build this yourself

Reporting and security alerts for suspicious activity

- Possible successful brute force attack
- Signing in from an anonymizer network
- Unlikely travel
- Anomalous activity across tenants
- Signing in from a known infected device

Microsoft

Azure AD Basic & Premium

*Note that all base features are completely **free***

Basic

- Organization branding
- Group-based application access
- Self-service password reset
- Application Proxy
- 99,9% SLA

Premium

- Self-service group management
- Self-service password reset with write-back to on-premise AD
- Advanced reporting
- Multi-Factor Authentication
- Microsoft Identity Manager

Microsoft

Developing For Azure AD

Three steps to get your applications ready

1/ Register your application in Azure AD
- Retrieve Client ID & (optional) Secret
- Configure Redirect URL
- Configure API permissions

2/ Add code to your client for sign in and authorization
- Web: WS-Federation, SAML 2.0, OpenID Connect
- Other (native, desktop, server): OAuth 2.0

3/ Add code to your Web API
- Web API: OAuth 2.0 Bearer Token authorization

Microsoft

Protocol Support

So... everything discussed here also applies to Windows Server 2016

Category	Protocol	ADFS	Azure AD
Native client	OAuth 2.0 auth code grant, public client	WS 2012	Now
Web sign-in	WS-Federation	WS 2008	Now
	SAML 2.0	WS 2008	Now
	OpenID Connect	WS 2016	Now
Web to Web API	OAuth 2.0 auth code grant, confidential client	WS 2016	Now
	OAuth 2.0 client credential grant	WS 2016	Now
Server to Web API	OAuth 2.0 on behalf of	WS 2016	Now

Open Source Libraries

http://github.com/azuread

Client: Active Directory Authentication Library (ADAL)

- .NET, Windows Store, Windows Phone
- JavaScript
- iOS
- Android

Server

- .NET: ASP.NET OWIN middleware for OpenID Connect and OAuth 2.0
- Node.js

In use today by Office apps, Visual Studio and more
Even more languages to come

Microsoft

Graph API

Cloud- and mobile-friendly counterpart to LDAP

REST API for accessing the directory

- Authorization using OAuth 2.0
- POST, GET, PATCH, DELETE to create, read, update, delete
- OData compatible
- Client libraries available for .NET, Cordova, iOS, Android

Available information

- Objects: users, groups, roles, devices, applications, …
- Relationships: member/memberOf, manager/directReport

```
https://graph.windows.net/contoso.com/users?
api-version=1.5&$filter=country eq 'USA'
```

Demo: Azure Active Directory for Developers

Microsoft

Azure Active Directory Futures

Microsoft

Azure AD B2C

Identity Management as a Service for Applications

Azure AD security, availability, and scalability for non Azure AD accounts

- Support for social identity providers and “application local accounts”
- Self-service sign up, password reset, profile management
- Customizable sign in and sign up UI
- Same protocols, libraries, and programming model

Consumption based pricing

- Based on # users and # authentications

Microsoft

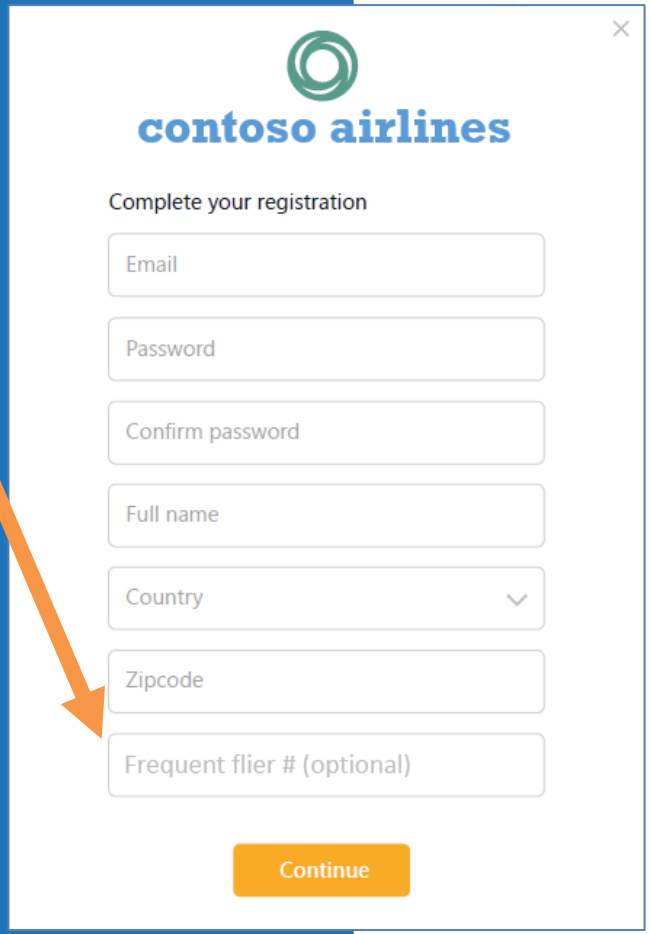
Azure AD B2C

Customize UI

Social and local accounts

Handles sign up, password reset

Define attributes to gather during sign up



Microsoft

MSA + AAD

Unified experience for Microsoft Account and Azure AD

- Sign in to an application using either MSA or AAD account
- Single developer service for developers
- Single sign in experience for end users

Microsoft

Windows 10

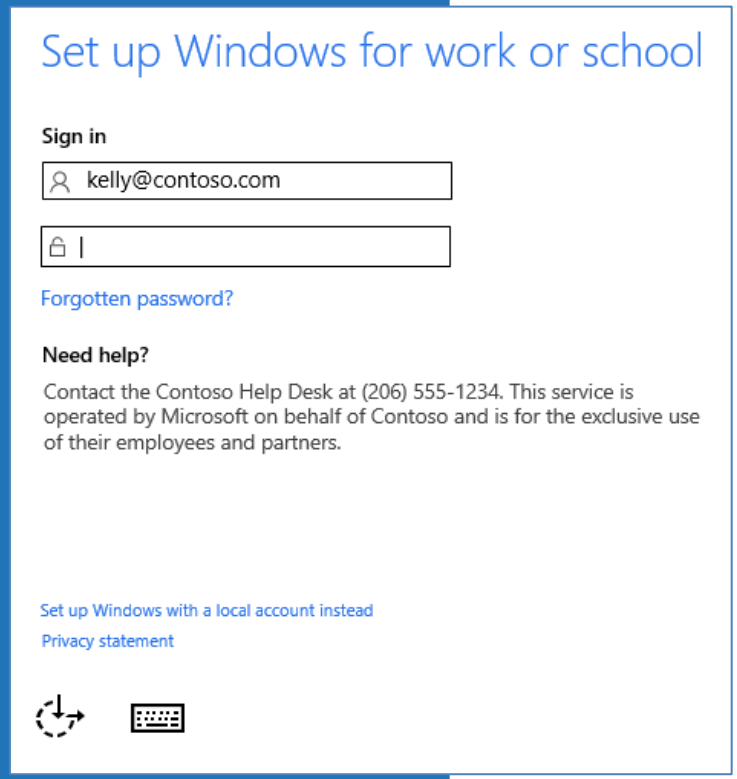
Built-in support for Azure AD identities

Windows 10 Azure AD Join

- Sign-in to desktop with Azure AD account

Single sign on to

- Kerberos-based on-premises applications
- Native applications that use WebAccountManager
- Web apps that support Azure AD sign-in



Microsoft

Wrapping Up...

Microsoft

Summary

Azure Active Directory – what's in it for developers?

Azure Active Directory

- Cloud-scale identity service
- Supports modern authorization & authentication scenarios
- REST-based Graph API

Reduces or removes custom security implementation

- Authenticating users
- Detecting suspicious activity
- Authorizing users via Groups or Roles (RBAC)
- B2C will allow social and "application local" accounts

Microsoft

Resources

What's next?

Documentation & News

- http://aka.ms/aaddev
- http://aka.ms/aadauthprotocols
- http://blogs.technet.com/b/ad/

Open Source Tools & Samples

- https://github.com/azuread
- https://github.com/azureadsamples
- https://github.com/jelledruyts/identitysamples

Microsoft

Your feedback is important!
Scan the QR Code and let us know via the TechDays App.

Laat ons weten wat u van de sessie vindt via de TechDays App!
Scan de QR Code.

MVA

Microsoft Virtual Academy

Bent u al lid van de Microsot Virtual Academy?! Op MVA kunt u altijd iets nieuws leren over de laatste technologie van Microsoft. Meld u vandaag aan op de MVA Stand. MVA biedt 7/24 gratis online training on-demand voor IT-Professionals en Ontwikkelaars.

Microsoft

TECH DAYS 2015

BREAKING NEW GROUND

Microsoft