betabit

samen bijzonder maken;

Securing an Azure Function REST API with

Azure Active Directory

Rick
van den
Bosch

Rick van den Bosch

@rickvdbosch

rickvandenbosch.net

Agenda

Azure Active Directory

Azure Functions

Static website hosting

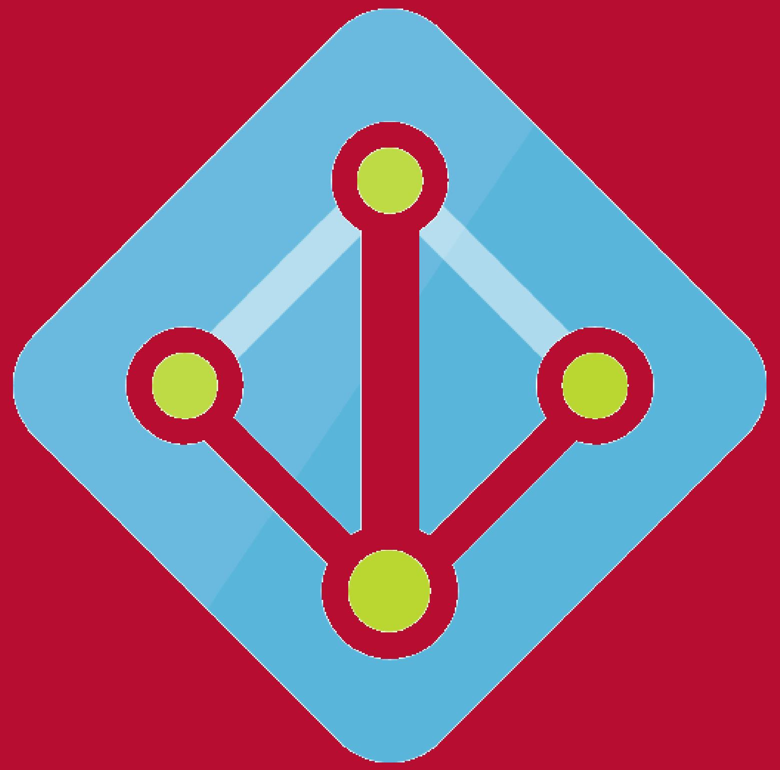
ADAL & MSAL

Putting things together

betabit

samen bijzonder maken;

Azure Active Directory



Azure Active Directory

“Azure Active Directory (Azure AD) is Microsoft’s cloud-based identity and access management service. Azure AD helps your employees sign in and access resources”

Azure Active Directory

Seamless, highly secure access

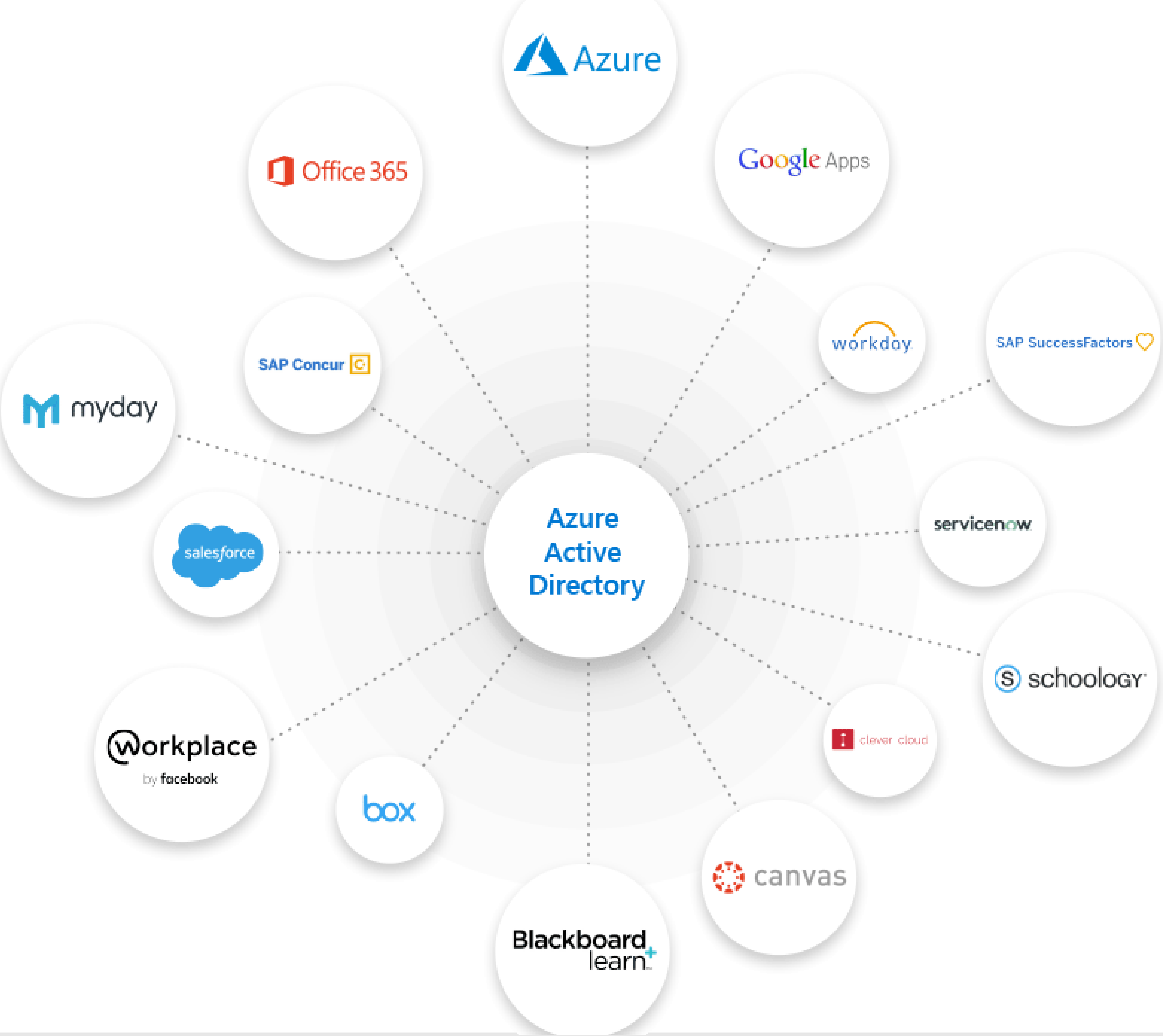
Comprehensive identity protection

Efficient management and compliance at scale

Customer and partner identities

Identity platform for developers

Identity for IaaS (infrastructure as a service)


Azure
Office 365
Google Apps
SAP Concur
workday
SAP SuccessFactors
myday
salesforce
Azure Active Directory
servicenow
schoology
clever cloud
Workplace by facebook
box
canvas
Blackboard learn

Who uses Azure AD?

IT admins

App developers

Subscribers of

- Microsoft 365
- Office 365
- Azure
- Dynamics CRM online

Pricing tiers

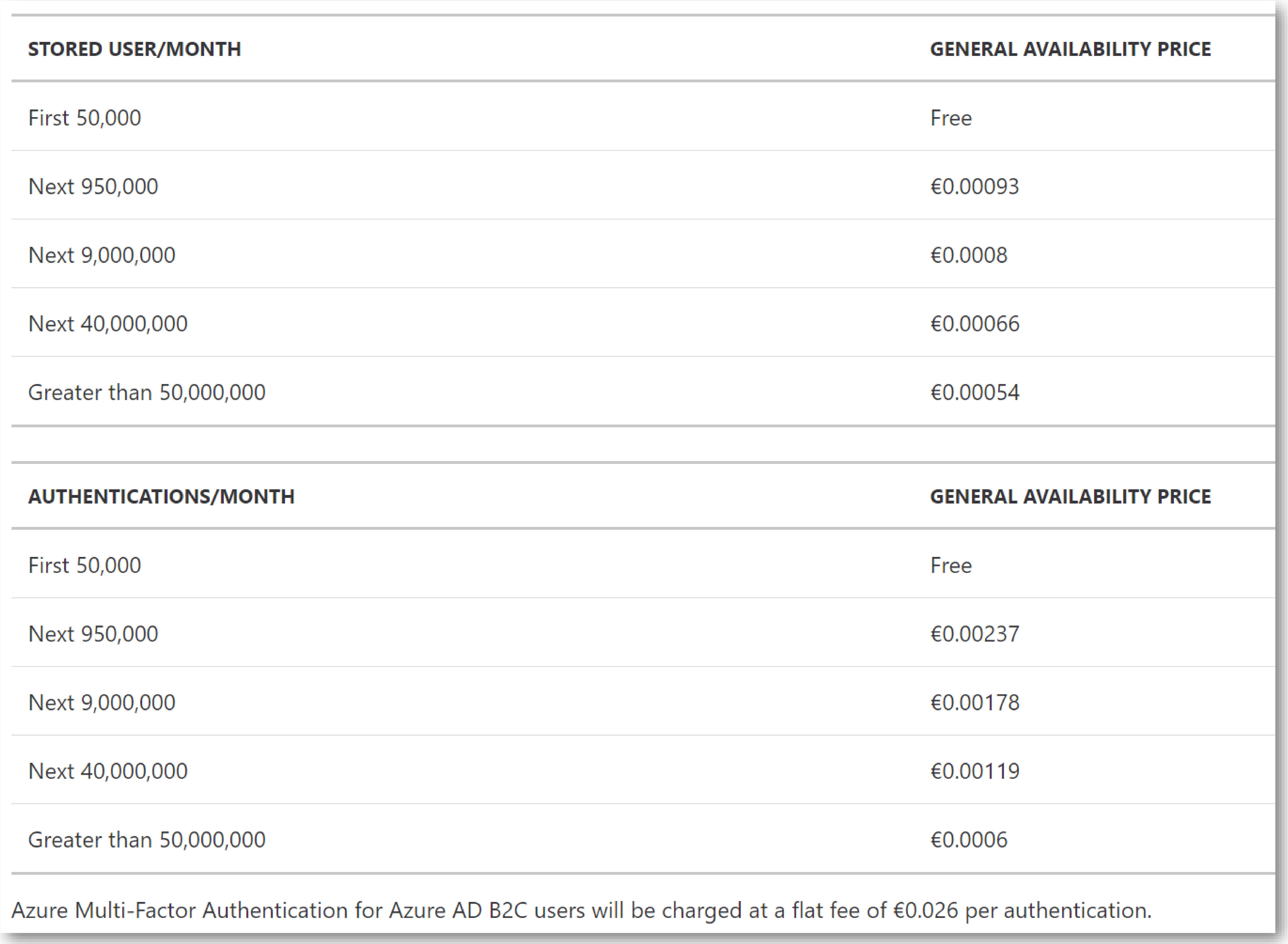
Free	FREE!
Basic	€ 0.844 user / month *
Premium P1	€ 5.06 user / month *
Premium P2	€ 7.59 user / month *

“Pay as you go” feature license.

* Annual commitment

Azure Active Directory B2C

"Azure Active Directory (Azure AD) B2C is an identity management service that enables you to customize and control how customers sign up, sign in, and manage their profiles when using your applications. This includes applications developed for iOS, Android, and .NET, among others."



STORED USER/MONTH	GENERAL AVAILABILITY PRICE
First 50,000	Free
Next 950,000	€0.00093
Next 9,000,000	€0.0008
Next 40,000,000	€0.00066
Greater than 50,000,000	€0.00054

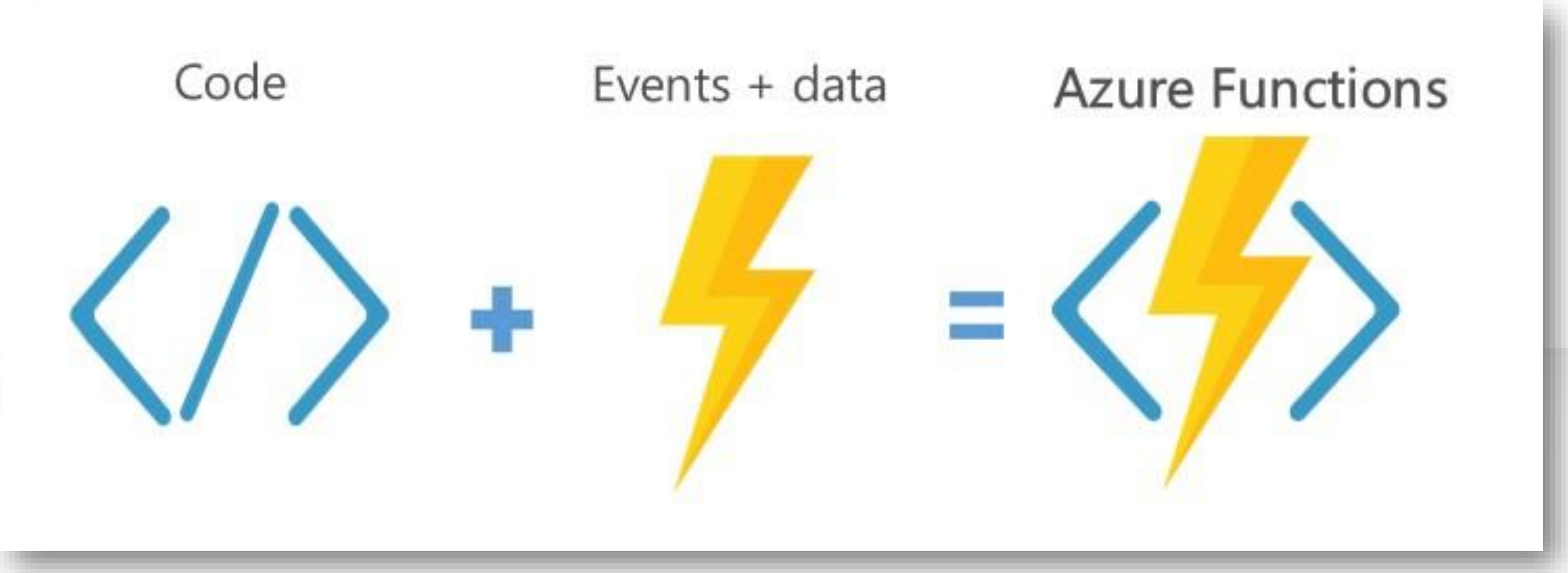
AUTHENTICATIONS/MONTH	GENERAL AVAILABILITY PRICE
First 50,000	Free
Next 950,000	€0.00237
Next 9,000,000	€0.00178
Next 40,000,000	€0.00119
Greater than 50,000,000	€0.0006

Azure Multi-Factor Authentication for Azure AD B2C users will be charged at a flat fee of €0.026 per authentication.

Azure Functions

Azure Functions

"Accelerate your development with an event-driven, serverless compute experience. Scale on demand and pay only for the resources you consume."



Azure Functions

Take advantage of serverless compute with Functions

Manage your apps instead of infrastructure

Optimize for business logic

Develop your way

What you can do with Functions

Web application backends

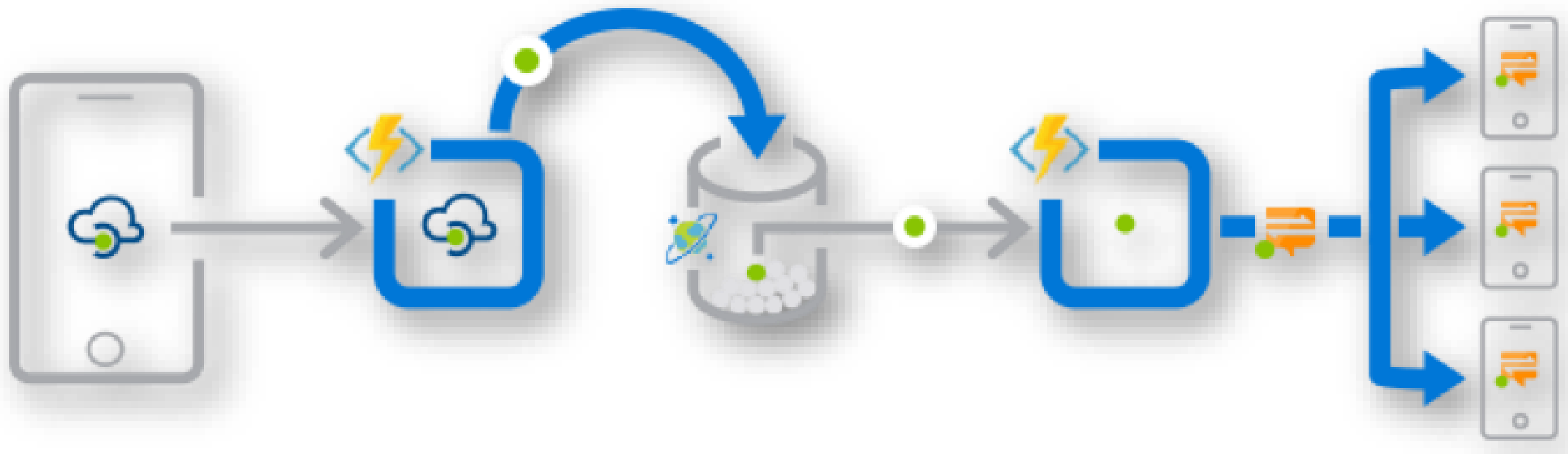
Mobile application backends

Real-time file processing

Real-time stream processing

Automation of scheduled tasks

Extending SaaS applications



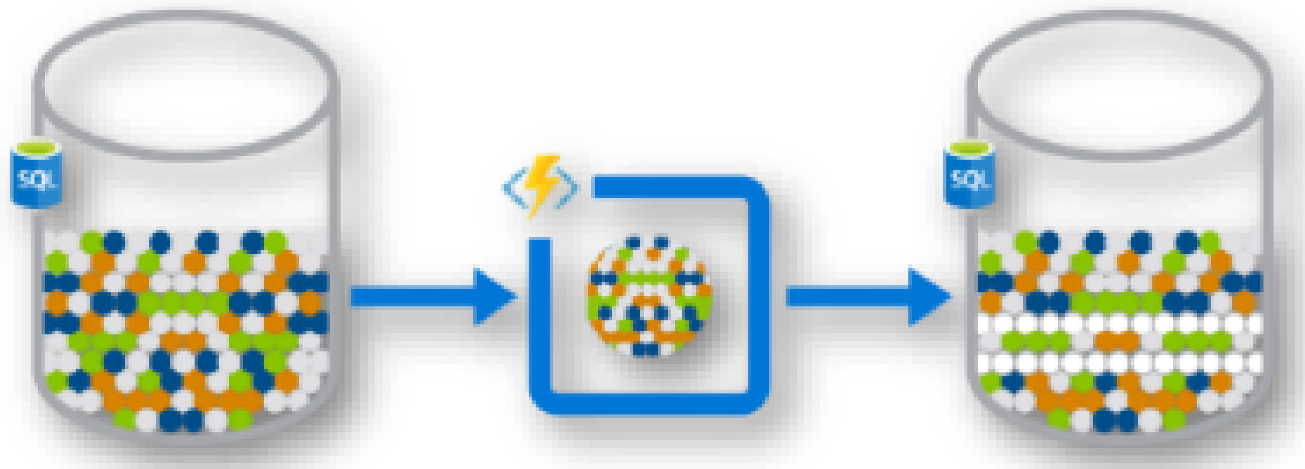
HTTP API call from a mobile app

Call processed by a function

Output data stored in Cosmos DB

Data transfer triggers second function...

...which sends notifications using Notifications Hub



A function cleans a database every 15 minutes...

...deduplicating entries based on business logic

Running Azure Functions

Consumption plan

When your function runs, Azure provides all of the necessary computational resources. You don't have to worry about resource management, and you only pay for the time that your code runs.

App Service Plan

Run your functions just like your web, mobile, and API apps. When you are already using App Service for your other applications, you can run your functions on the same plan at no additional cost.

Best Practices

Long running

- Keep the runtime short (default < 5m; max. 10m)

Stateless

- Don’t use state in the host
- Idempotent

Cold start

- Fast start up times
- Keep them small

Control

- ‘They’ control scaling
- ‘They’ control when your host is alive
- You control the code!

Static website hosting

Static website hosting

Available on General-Purpose V2

Special container: *web$*

Files in this container are:

- served through anonymous access requests
- only available through object read operations
- case-sensitive

Provided at no additional cost

ADAL & MSAL

Active Directory Authentication Library (ADAL)

Enables application developers to authenticate users to

- Cloud Active Directory
- On-premises Active Directory

- Configurable token cache that stores access tokens and refresh tokens
- Automatic token refresh when an access token expires and a refresh token is available
- Support for asynchronous method calls

Microsoft Authentication Library (MSAL) Preview for JS

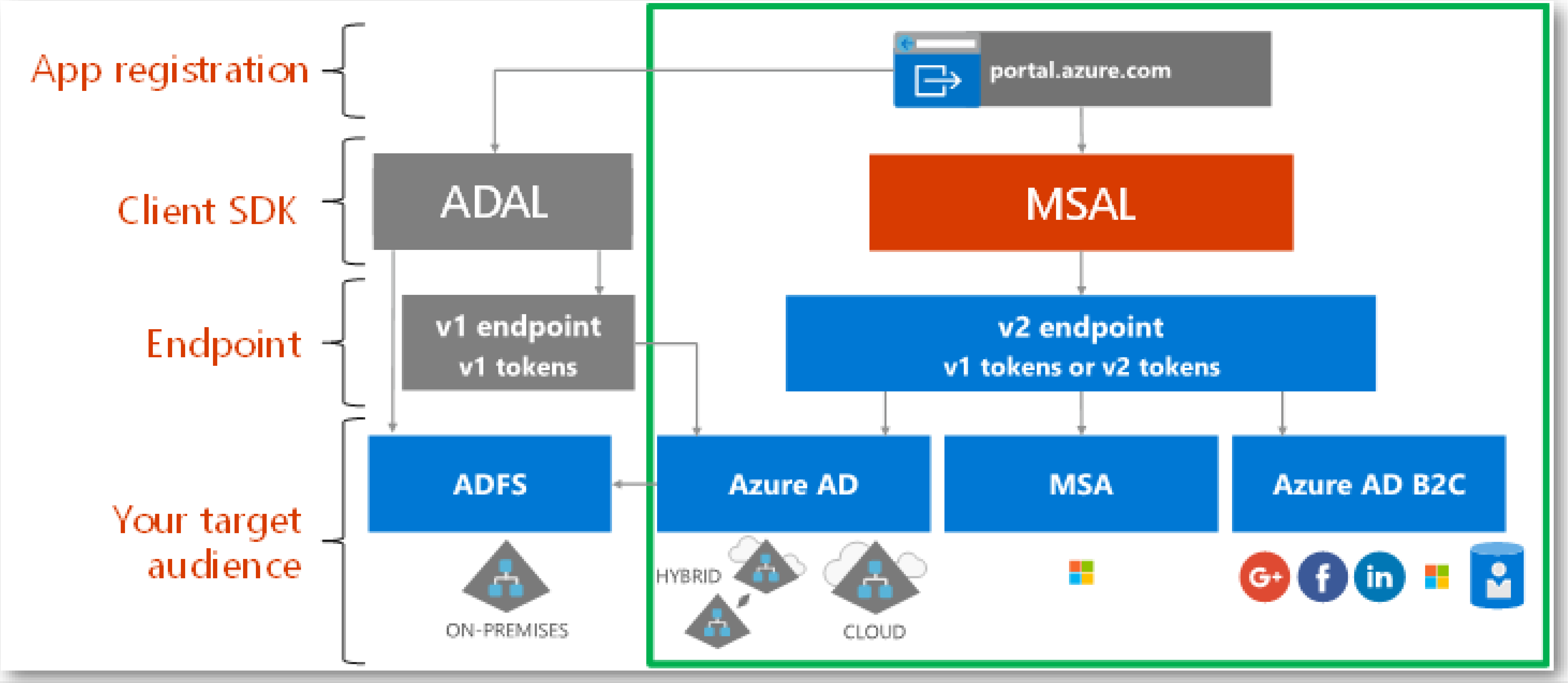
Enables Single Page Applications to authenticate users with

- Microsoft Azure Active Directory accounts
- Microsoft accounts
- Accounts in social identity providers like Facebook, Google, LinkedIn etc.

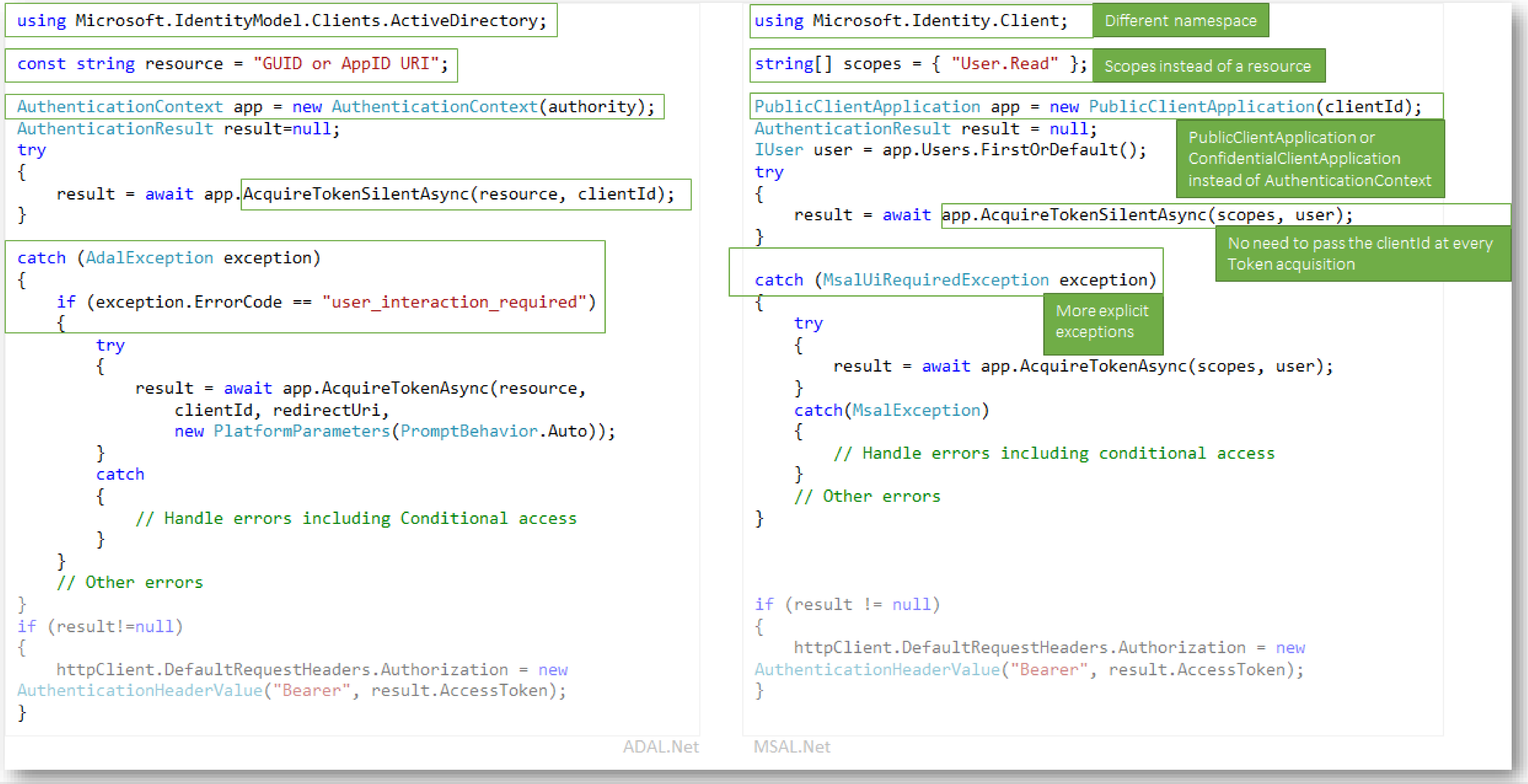
Interacts with

- Microsoft Azure Active Directory
- Microsoft Azure AD B2C
- Microsoft accounts

Differences (process)



Differences (implementation)



```
using Microsoft.IdentityModel.Clients.ActiveDirectory;

const string resource = "GUID or AppID URI";

AuthenticationContext app = new AuthenticationContext(authority);
AuthenticationResult result=null;
try
{
    result = await app.AcquireTokenSilentAsync(resource, clientId);
}

catch (AdalException exception)
{
    if (exception.ErrorCode == "user_interaction_required")
    {
        try
        {
            result = await app.AcquireTokenAsync(resource,
                clientId, redirectUri,
                new PlatformParameters(PromptBehavior.Auto));
        }
        catch
        {
            // Handle errors including Conditional access
        }
    }
    // Other errors
}
if (result!=null)
{
    httpClient.DefaultRequestHeaders.Authorization = new
AuthenticationHeaderValue("Bearer", result.AccessToken);
}
```

ADAL.Net

```
using Microsoft.Identity.Client;

string[] scopes = { "User.Read" };

PublicClientApplication app = new PublicClientApplication(clientId);
AuthenticationResult result = null;
IUser user = app.Users.FirstOrDefault();
try
{
    result = await app.AcquireTokenSilentAsync(scopes, user);
}

catch (MsalUiRequiredException exception)
{
    try
    {
        result = await app.AcquireTokenAsync(scopes, user);
    }
    catch(MsalException)
    {
        // Handle errors including conditional access
    }
    // Other errors
}


if (result != null)
{
    httpClient.DefaultRequestHeaders.Authorization = new
AuthenticationHeaderValue("Bearer", result.AccessToken);
}
```

MSAL.Net

Different namespace

Scopes instead of a resource

PublicClientApplication or ConfidentialClientApplication instead of AuthenticationContext

No need to pass the clientId at every Token acquisition

More explicit exceptions

Adal-angular4

Angular 4/5/6/7 ADAL Wrapper

Can be used to authenticate Angular applications against Azure Active Directory v1 endpoint.

@azure/msal-angular

Wrapper of the core MSAL.js library

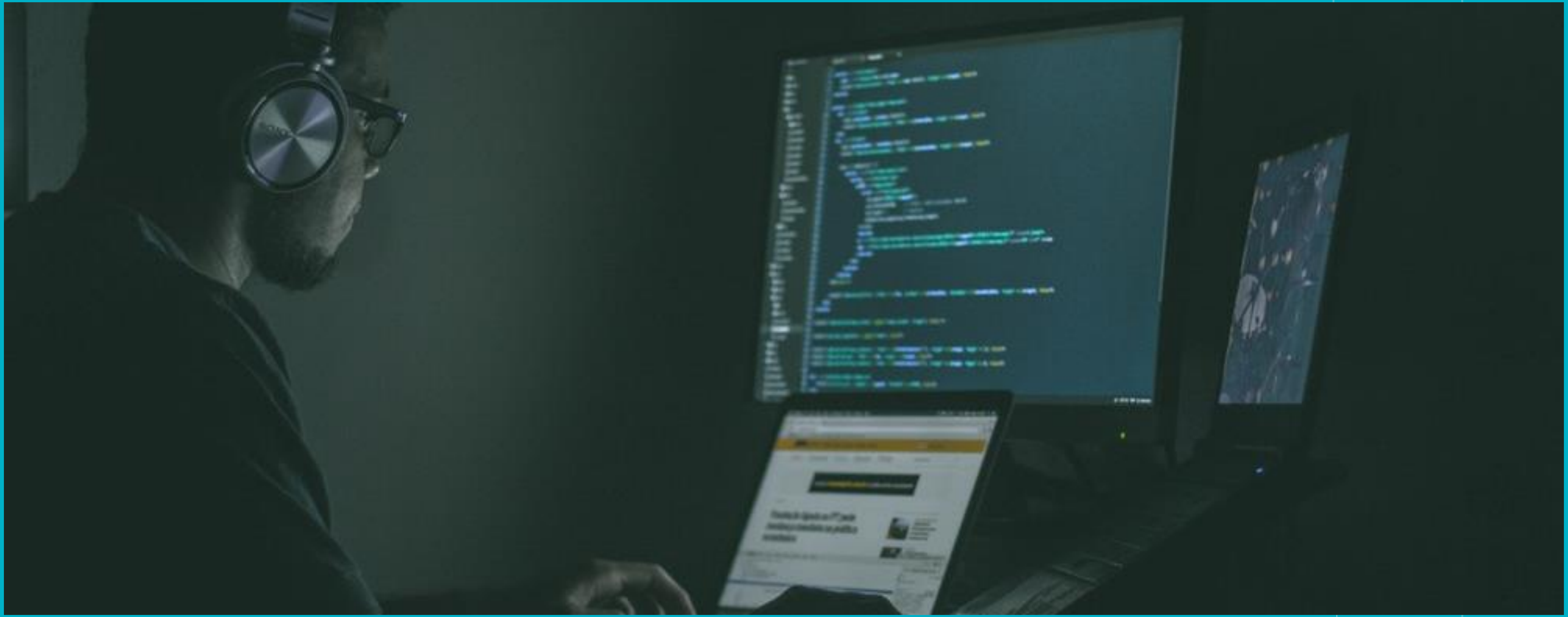
Suitable for use in a production environment

The same production level support as current libraries

Changes may impact your application

When GA: update within six months

Putting things together



Resources

Build a Serverless web app in Azure

About Microsoft identity platform

adal-angular4

@azure/msal-angular

rickvdbos.ch/safwad

betabit {...}

samen bijzonder maken;

Thank you for your attention