What the JWT?

SECURING YOUR APPLICATION WITH MICROSOFT IDENTITY WEB

Agenda

- A bit about me
- A bit about JWTs
- A bit about token types
- A bit about authentication flows
- How we used to implement authentication
- Microsoft’s Identity Platform
- How Microsoft Identity Web simplifies authentication

Microsoft
Identity & Access Management
Expert
Microsoft
Identity & Access Management
Gold Contributor
Microsoft CERTIFIED
IDENTITY AND ACCESS ADMINISTRATOR
ASSOCIATE

Dee Bolt

- Graduated from Cardiff Met in 2015
- Various blended roles around software development over the years
- External Identity Consultant at Kocho in 2020

- Azure Technical Contributor Program (ATCP)
- 425 Show community

linkedin.com/in/deebolt/ dee.bolt@outlook.com

What is a JWT?

JSON Web Token

Open standard (RFC 7519)

Self-contained way of securely sending information between parties

Information is digitally signed at the sender

Verified by the receiver for trust

Typical uses

- Authorisation
- Information exchange

header.payload.signature

Header

Type of token (JWT)

Signing algorithm (RSA, SHA256, HMAC etc.)

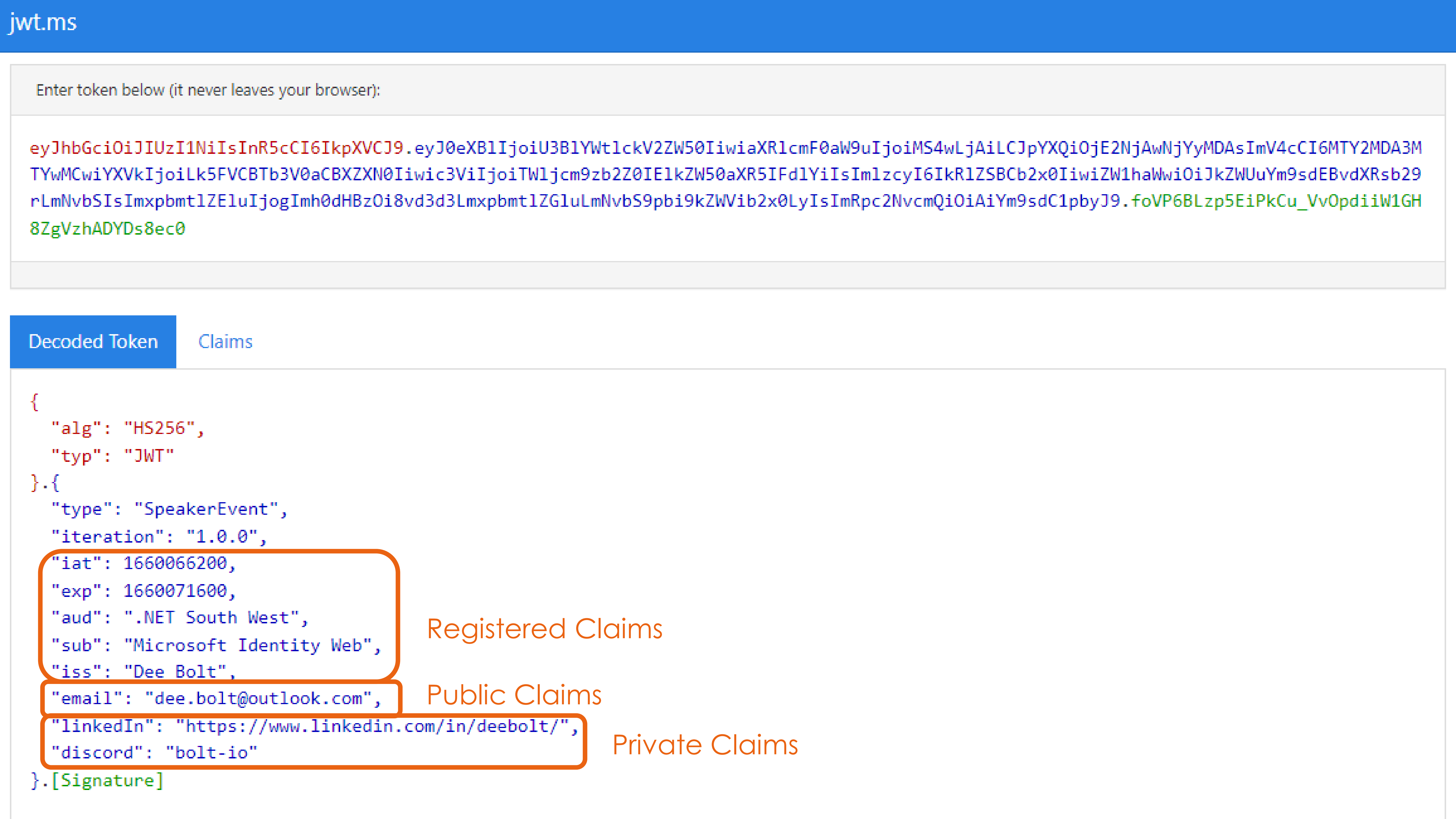
Key ID (kid) – used to match a specific public key to verify the signature

Payload

Contains claims

- Registered claims
- Public claims
- Private claims

Signature



Enter token below (it never leaves your browser):

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0eXBlIjoiU3BlYWtlckV2ZW50IiwiaXRlcmF0aW9uIjoiMS4wLjAiLCJpYXQiOjE2NjAwNjYyMDAsImV4cCI6MTY2MDA3M
TYwMCwiYXVkIjoiLk5FVCBTb3V0aCBXZXN0Iiwic3ViIjoiTWljcm9zb2Z0IElkZW50aXR5IFdlYiIsImlzcyI6IkRlZSBCb2x0IiwiZW1haWwiOiJkZWUuYm9sdEBvdXRsb29
rLmNvbSIsImxpbmtlZEluIjogImh0dHBzOi8vd3d3LmxpbmtlZGluLmNvbS9pbi9kZWVib2x0LyIsImRpc2NvcmQiOiAiYm9sdC1pbyJ9.foVP6BLzp5EiPkCu_VvOpdiiW1GH
8ZgVzhADYDs8ec0
```

```
{
  "alg": "HS256",
  "typ": "JWT"
}.{
  "type": "SpeakerEvent",
  "iteration": "1.0.0",
  "iat": 1660066200,
  "exp": 1660071600,
  "aud": ".NET South West",
  "sub": "Microsoft Identity Web",
  "iss": "Dee Bolt",
  "email": "dee.bolt@outlook.com",
  "linkedIn": "https://www.linkedin.com/in/deebolt/",
  "discord": "bolt-io"
}.[Signature]
```

Registered Claims

Public Claims

Private Claims

Token Types

ID tokens

Access tokens

Refresh tokens

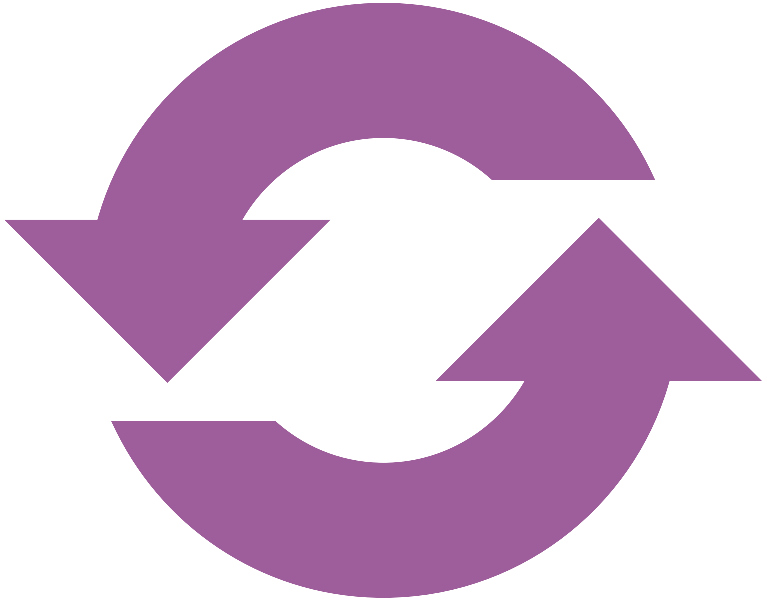
ID tokens

- OpenID Connect (OIDC) spec
- Proves the user is authenticated
- Contains user information/profile
- ONLY for the client applications use

Access tokens

- OAUTH2 spec
- Allows a client application to call a resource on behalf of the user
- Access is controlled through scopes
- Should not be inspected by the client application
- ONLY for the resource to use (e.g., an API)

Refresh tokens



- Received with an access token
- Used to obtain a new access/refresh token pair when:
  - The tokens expire
  - Requesting access to a different resource (scope)
- Can be revoked

Other types of tokens

- Simple Web Tokens (SWT)
  - Symmetrically signed by a shared secret using the HMAC algorithm

- Security Assertion Markup Language Tokens (SAML)
  - XML means SAML tokens are more verbose (larger tokens)
  - Difficult to digitally sign without introducing obscure security holes compared to signing JSON

Authentication flows

- Authorization Code (with PKCE for SPAs)
- Client Credentials
- Device Code
- Implicit grant
- On-behalf-of
- Resource Owner Password Credentials (ROPC)
- Integrated Windows Authentication (IWA)

Before Microsoft Identity Platform

- Complicated implementations
- Easy to leave vulnerabilities
- Often required rolling your own middleware, cookie managers, token validators
- Write your own sign-in / sign-out endpoints

#identityCrisis

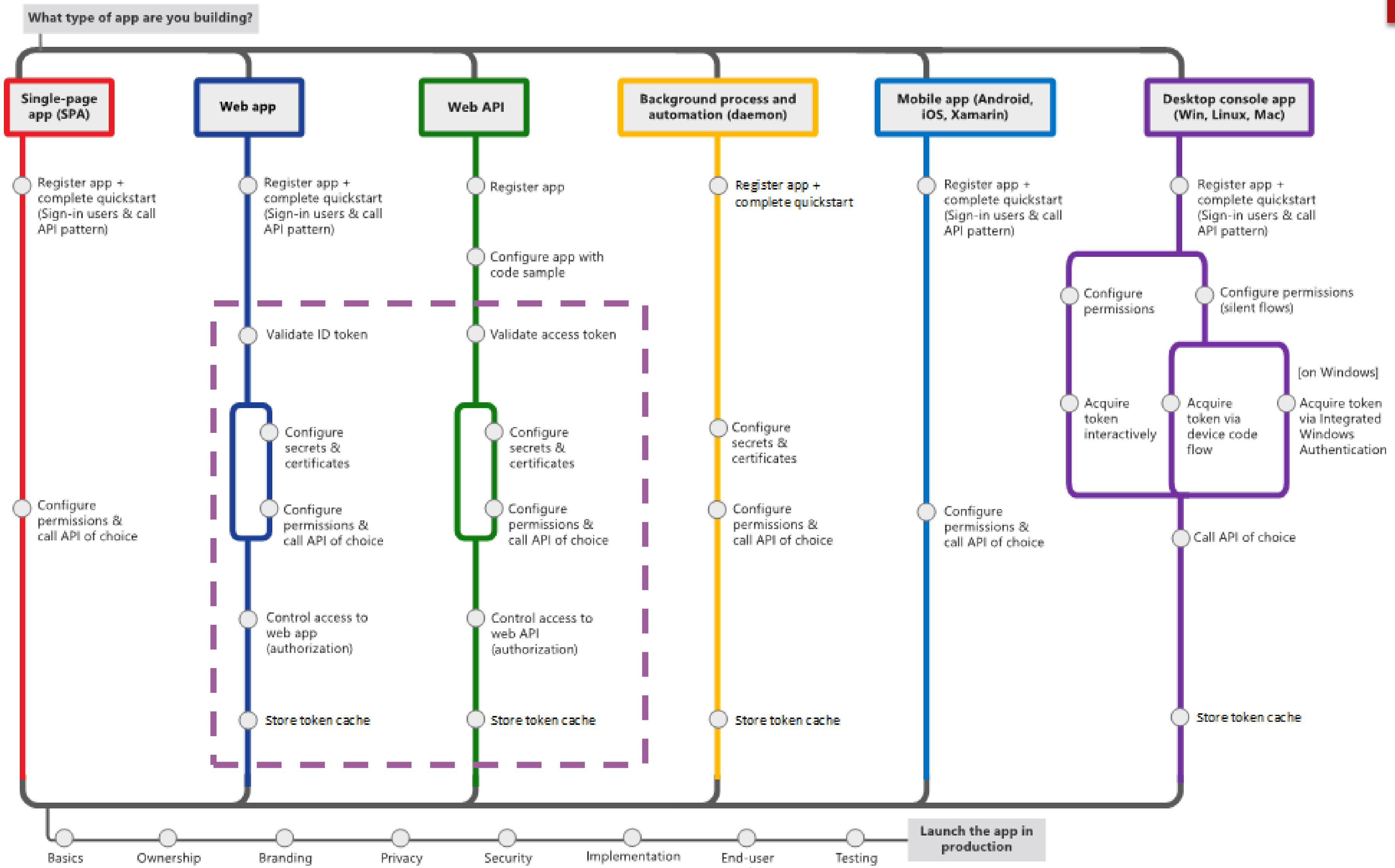
Let’s dig around!

Microsoft Identity Platform

- **OAuth 2.0 and OpenID Connect standard-compliant authentication service** enabling developers to authenticate several identity types, including:
  - Work or school accounts, provisioned through Azure AD
  - Personal Microsoft account, like Skype, Xbox, and Outlook.com
  - Social or local accounts, by using Azure AD B2C
- **Open-source libraries**: Microsoft Authentication Libraries (MSAL) and support for other standards-compliant libraries

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
- Acquire token interactively
- Configure permissions (silent flows)
- Acquire token via device code flow
- [on Windows] Acquire token via Integrated Windows Authentication
- Call API of choice
- Store token cache

Basics · Ownership · Branding · Privacy · Security · Implementation · End-user experience · Testing · **Launch the app in production**

https://aka.ms/IdentityPlatformChecklist

Microsoft

Microsoft Identity Web

- Microsoft.Identity.Web
- Microsoft.Identity.Web.UI (optional)

- A wrapper over MSAL

- Minimal frontend additions (only buttons to sign-in, sign-out)
- Easy to add a downstream APIs
- Don’t need to be an identity expert!

Talk is cheap. Show me the code.

Linus Torvalds

Demo

Recap

We seen what JSON Web Tokens are

The different types of tokens

How painful identity implementations were

How Microsoft's Identity Platform simplifies implementations

Questions?

- aka.ms/425show/discord/join
- Linkedin.com/in/deebolt
- dee.bolt@outlook.com
- github.com/bolt-io

- More info:
  - aka.ms/Microsoft-identity-web
  - aka.ms/msal