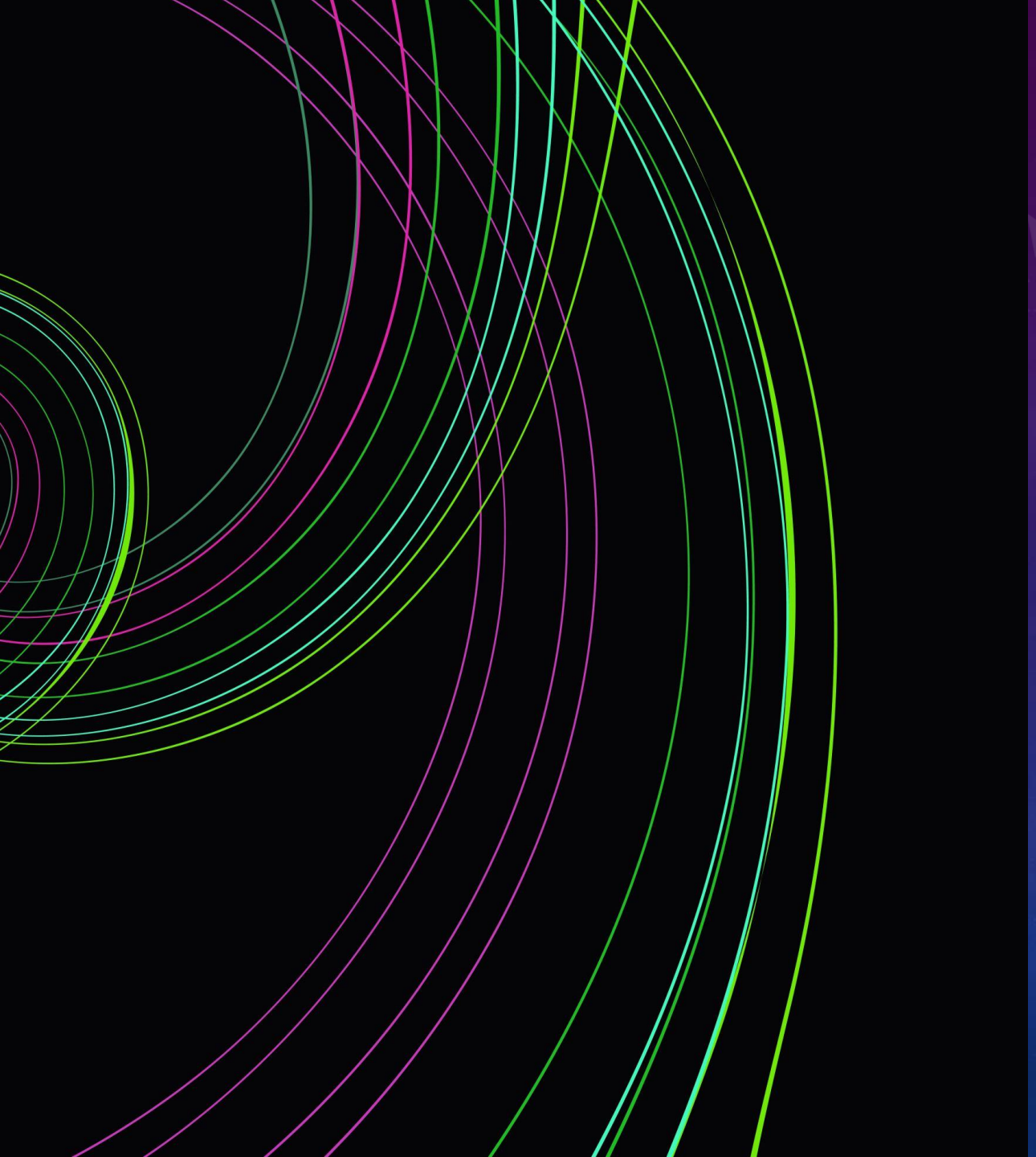


# DEMYSTIFYING AZURE AD, JWTS & OIDC


- Graeme Foster
- Apps & Innovation Technical Specialist
- @ Microsoft

# AIMS FOR THIS SESSION

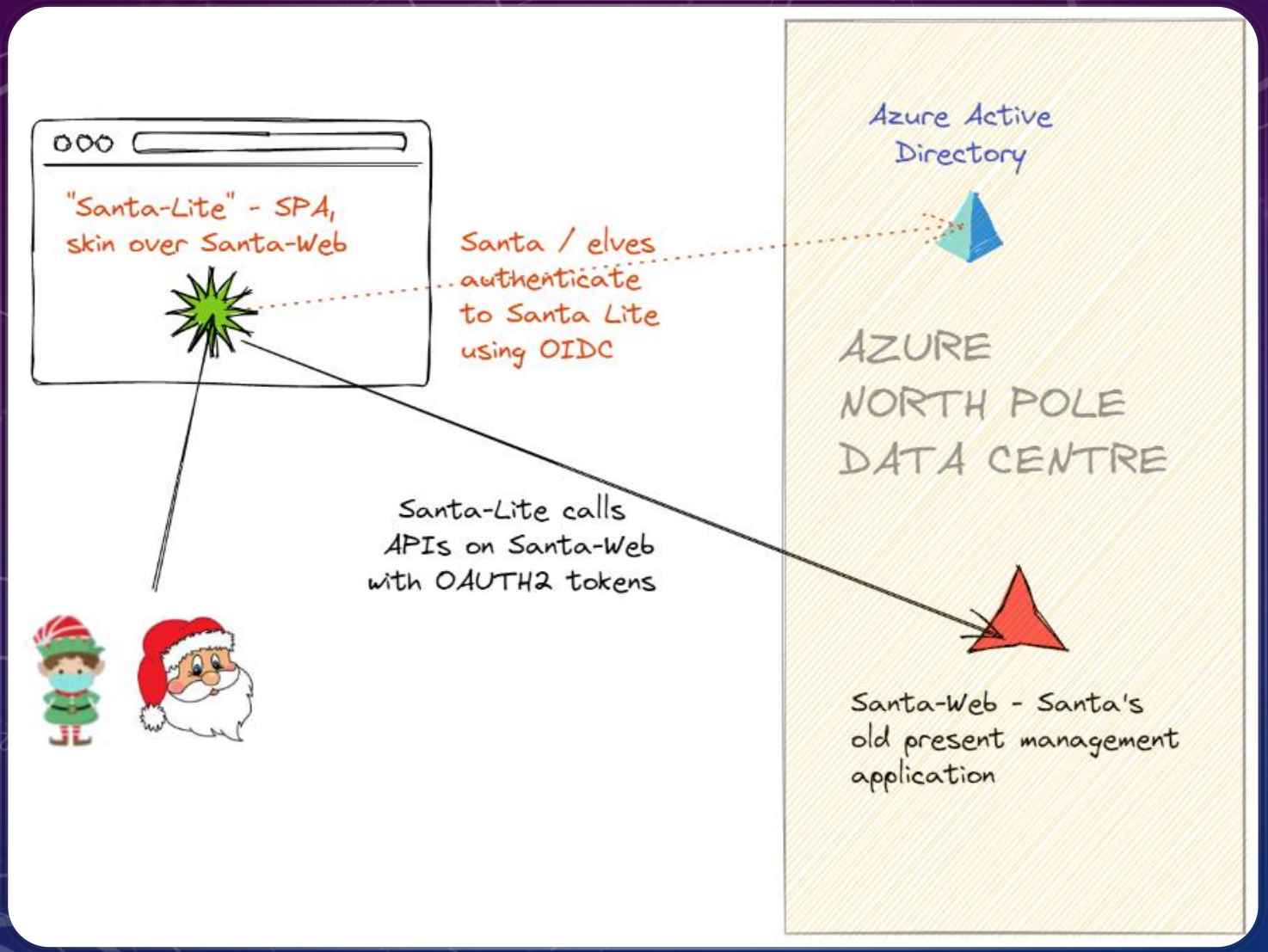
Show tools and techniques to diagnose common problems with OIDC, AAD and MSAL

Show the moving parts involved in the PKCE flow

Break down JWT's and relate their components to real world authentication and authorisation

Dig into Scopes, Groups and Roles

# CHRISTMAS IN JULY IS COMING…

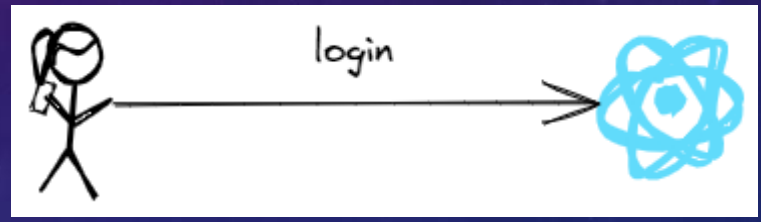



# SANTAWEB

# "CHRISTMAS DONE RIGHT"

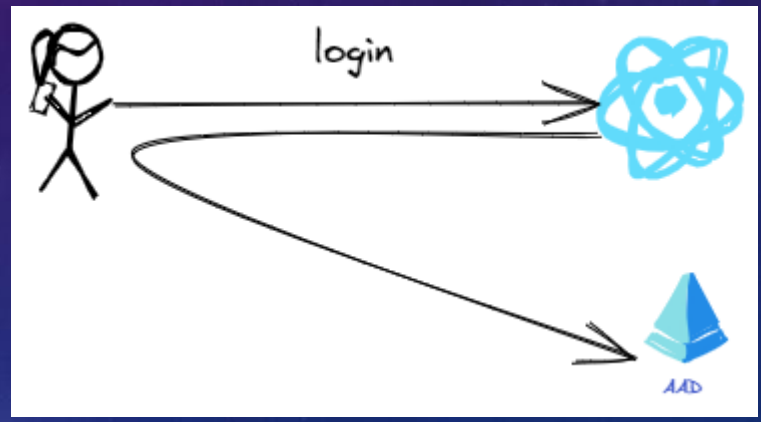
# SIGN IN FLOWS

`https://santalite.localtest.me`



# SIGN IN FLOWS

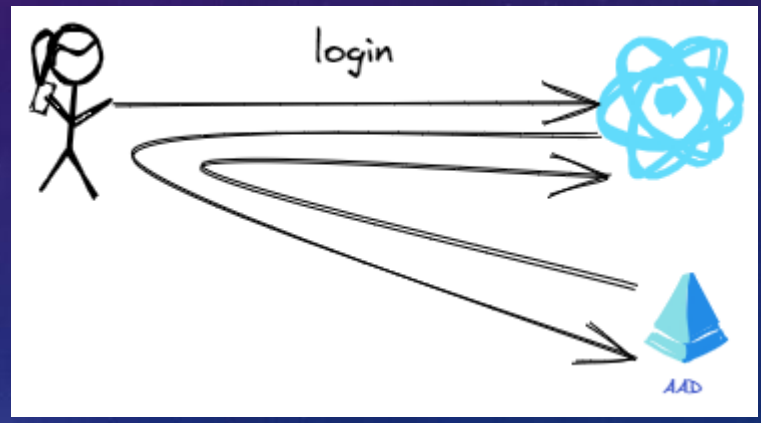
302
https://login.microsoftonline.com/.../authorize?
- 'which application this is'
- 'what the application wants to do'
- 'where to redirect to after the sign-in flow'
- 'security information'



# SIGN IN FLOWS (IMPLICIT)

200 / 302

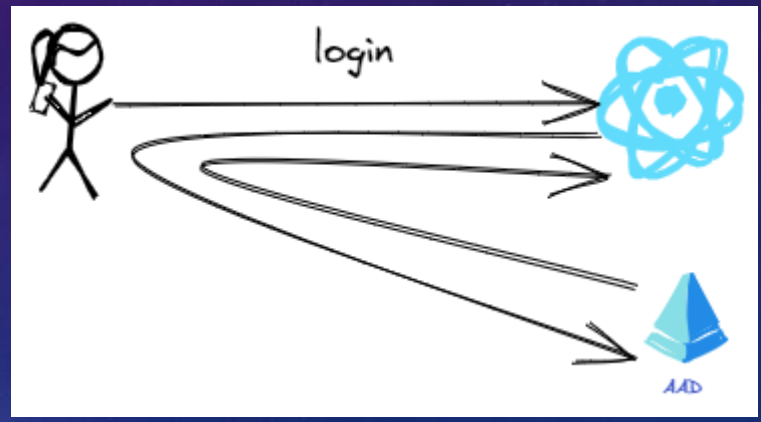
https://santalite.localtest.me/#id_token=ey.....



# SIGN IN FLOWS (PKCE)

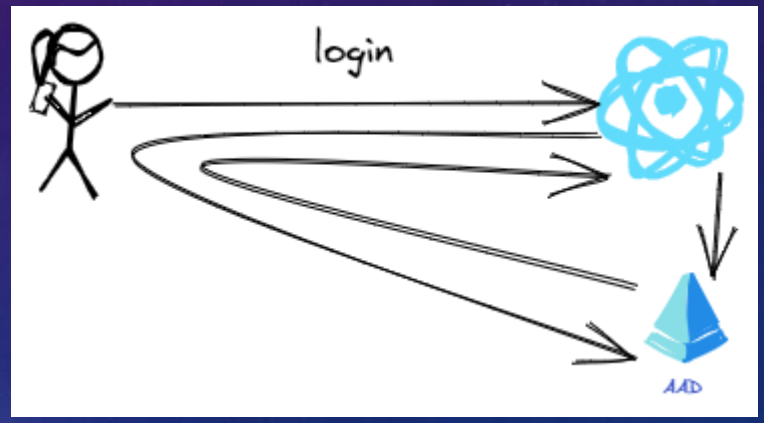
200 / 302

https://santalite.localtest.me/#code=sdkjfhkjsdf



# SIGN IN FLOWS (PKCE)

```
POST https://login.microsoftonline.com/.../token
```




Request includes
plaintext and
Code to get secret

# JWTS (JSON WEB TOKENS)

- Base 64 encoded self-contained security tokens
- Consist of three parts
  - Information about the signing key
  - A signature
  - The payload – assertions about the subject of the token.
- Clients fetch the Authorisation server's public keys ahead of time
- If the audience isn't 'you' then the token is for someone else
  - Microsoft Graph tokens are a good example as they don't validate using normal methods

# OIDC / PKCE

- Use MSAL over ADAL unless you have no option
- OIDC redirect URI must match between Client and IdP
  - Open redirects caused a security issue
- PKCE is recommended for traditional web servers as-well as mobile / SPA clients
  - The Implicit flow revealed tokens in front-channel flows (# tags, query-strings)
  - PKCE binds the token request to the token retrieval using a 1-time passcode

# REDIRECT MISMATCH

Redirect must be the same in 2 places, Client Application and AAD (IdP)

Self explanatory error when it’s wrong.

Fiddler / Browser Network trace will show redirect passed to AAD

AAD Configuration page shows expected redirects

# AUDIENCE MISMATCH

- Must be the same in 3 places, SPA, AAD and API
- Microsoft.Identity.Web assumes an Audience based on version of token, unless given one
- Diagnosed through fiddler trace / or diagnostics of Web App
- Confirmed by looking at tokens in JWT.ms

# MICROSOFT.WEB.IDENTITY

```
// handle v2.0 access token or Azure AD B2C tokens (even if v1.0)
if (IsB2C || token.Claims.Any(c :Claim => c.Type == Constants.Version && c.Value == Constants.V2))
{
    validationParameters.ValidAudience = $"{ClientId}";
}

// handle v1.0 access token
else if (token.Claims.Any(c :Claim => c.Type == Constants.Version && c.Value == Constants.V1))
{
    validationParameters.ValidAudience = $"api://{ClientId}";
}
```

https://github.com/AzureAD/microsoft-identity-web/blob/bb1b65fb4e3cc40080e2a61ed6554bef31767983/src/Microsoft.Identity.Web/Resource/RegisterValidAudience.cs#L70

# SCOPES

- Scopes are fully qualified with the Application's Uri
- A token can only contain scopes from 1 API - the aud claim
- In AAD a client can ask the end user to consent to any Scope defined on your API
- Scopes are permissions for your client applications. Not your users

# GROUPS AND ROLES

- Groups are tenant wide. Azure AD limits the number returned in a token
- Roles are bound to Applications.
- They only appear in tokens whose Audience is that Application
- Roles don’t work with users in nested groups.
- Roles are not a replacement for fine grained business authorisation

# ENTERPRISE APPLICATIONS / SERVICE PRINCIPALS / MANAGED APPLICATIONS

- An AAD “Application” describes your application
- A Service Principal is a manifestation of an application in a tenant
- User / group assignment and conditional access are defined against the Service Principal
- In a directory a single service principal represents an application
- A multi-tenant application can have service principals in many tenants (e.g. SaaS)

# RESOURCES

- https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow
- https://nicolgit.github.io/AzureAD-Endopoint-V1-vs-V2-comparison/
- https://brockallen.com/2019/01/03/the-state-of-the-implicit-flow-in-oauth2/
- https://docs.microsoft.com/en-us/azure/active-directory/develop/msal-migration
- https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-add-app-roles-in-azure-ad-apps