SINGLE SIGN ON EXTENSIONS V2

THIS TIME FOR REAL

Joel Rennich

NoMAD/Jamf

MacSysAdmin 2019

Single Sign On App Extensions

https://docs.macsysadmin.se

Requirements

What you need first

13

URL Session

- Apple-supplied URL loading system
- Used by Safari and most native applications
- Easy to use in your own code

Things that don’t use URLSession

SMB

SSO Extension Types

Redirect

Credential

Announced SSOEs

okta

Fast Pass

Azure

MSAL for ObjC

https://github.com/AzureAD/microsoft-authentication-library-for-objc

What’s new?

SSO Extension Tips

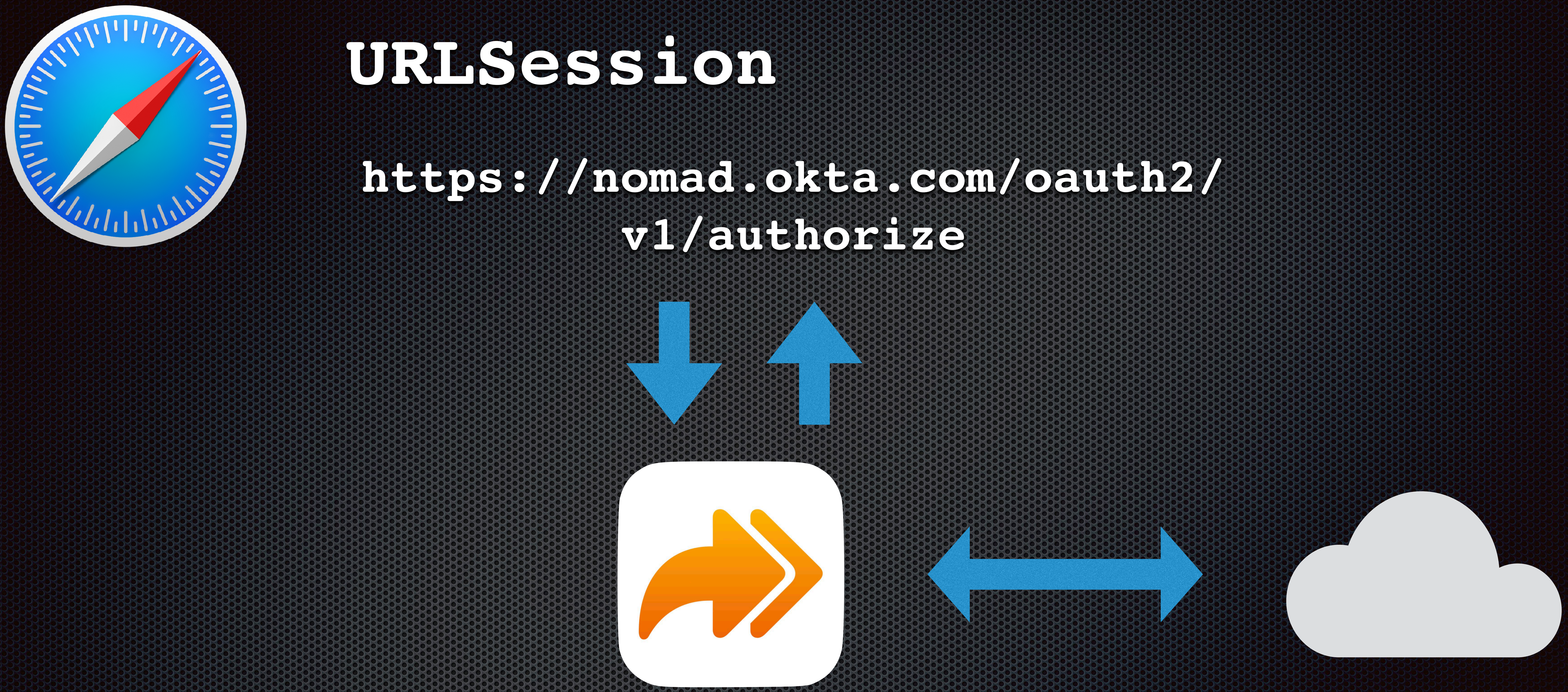
- Double Check Profile
- If iOS… reboot the device
- Can’t have multiple SSO Extensions authoritative for the same domain

How it works

Where the magic happens

Easiest definition…

MitM



URLSession

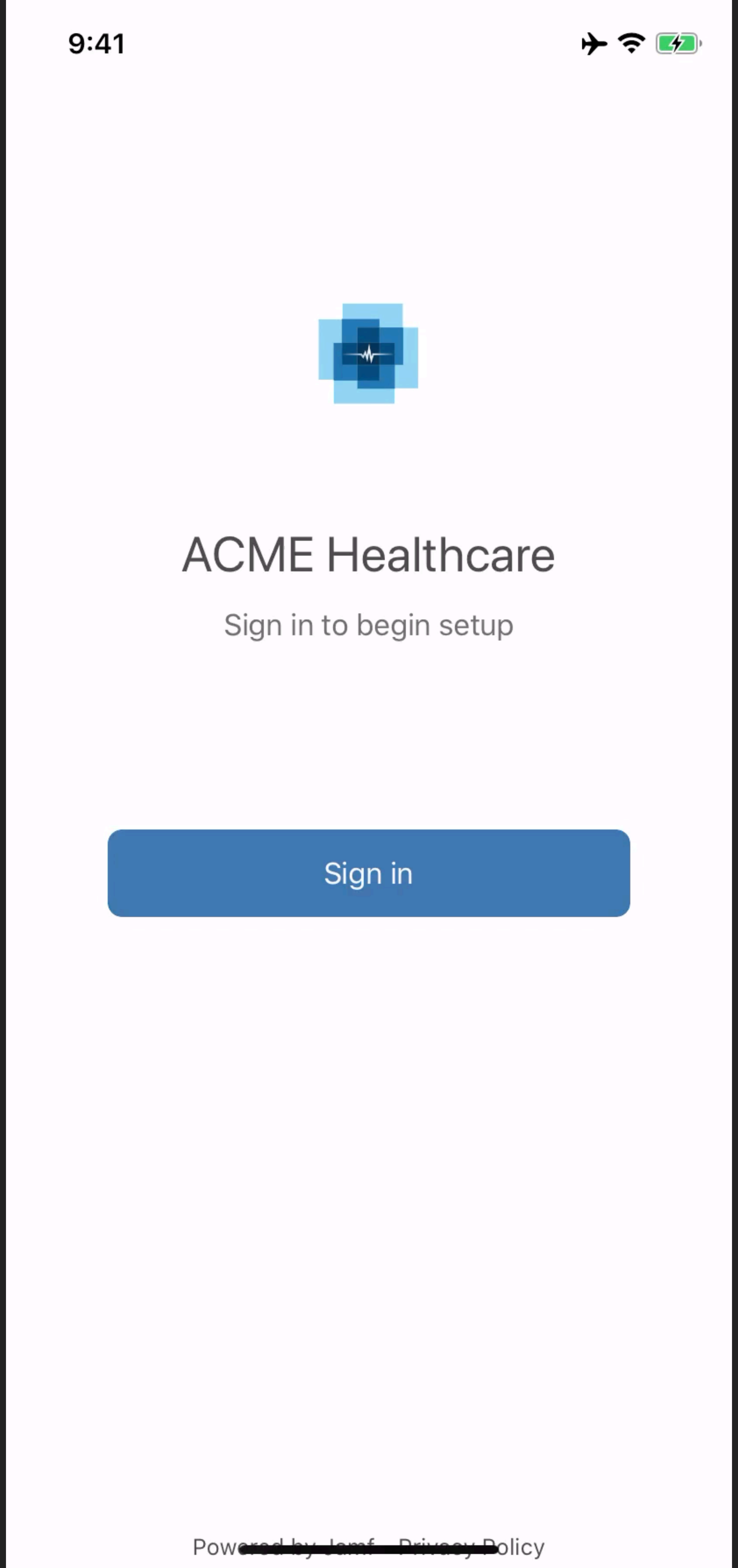
https://nomad.okta.com/oauth2/v1/authorize

(Literally anything)

Demo

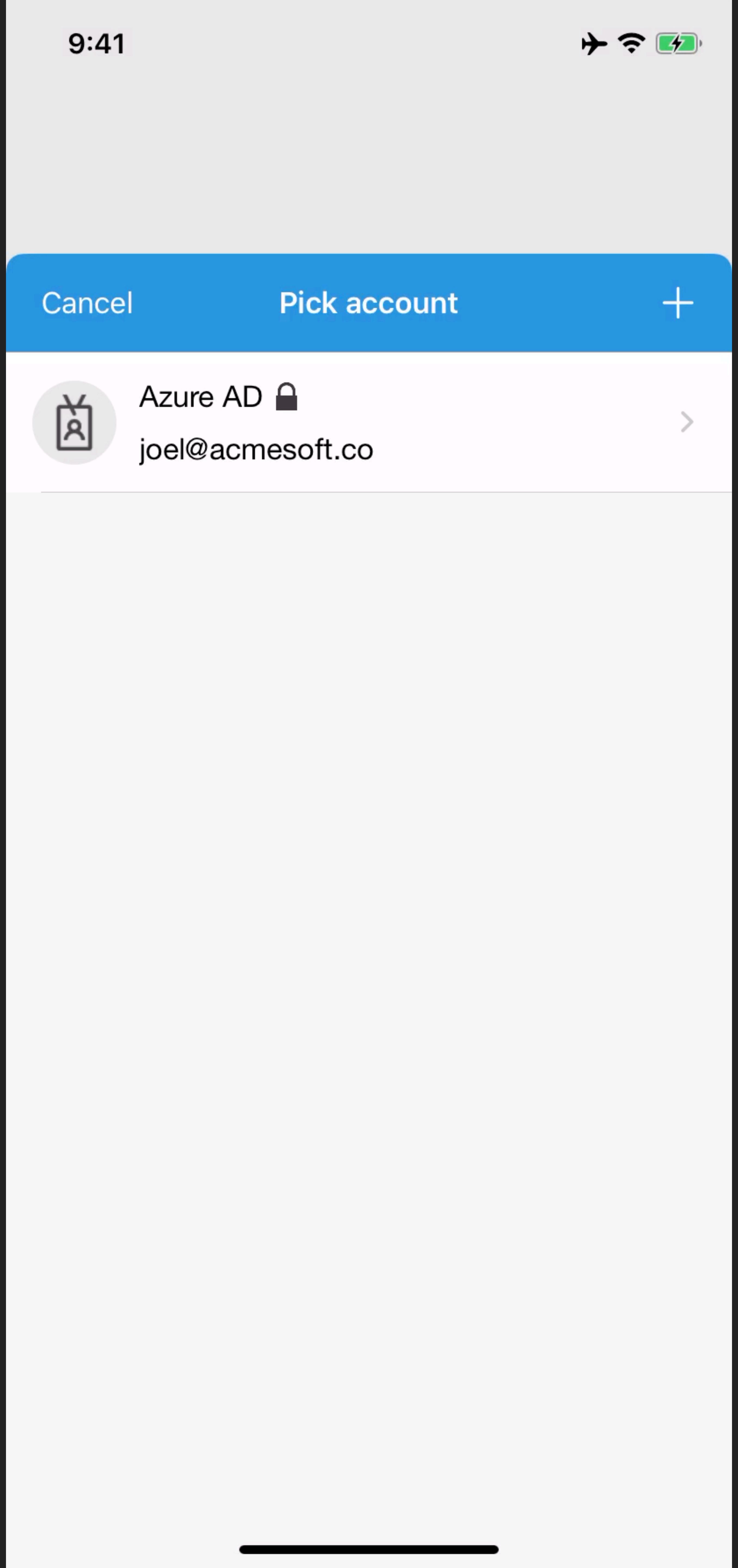
MSAL on iOS

https://docs.microsoft.com/en-us/azure/active-directory/develop/apple-sso-plugin



ACME Healthcare

Sign in to begin setup



Pick account

Azure AD 🔒
joel@acmesoft.co

Demo

Homemade SSOE for ADFS

Abuse of SSOEs

Where your own magic happens

SSOEs run in user space

- Once triggered, a user can kill the SSOE
- This effectively hands the URL back to the calling application to operate as if no SSOE was there

If you…

- Own the endpoint, and can put an AASA file on it
- Can deliver an App Extension and Profile
- Have a need that nothing else can solve

You too can MitM!

Semi-Practical Example

“Take Over” an IdP

Discovery Metadata

- Typically found at /.well-known/openid-configuration
- Lists the endpoints for authorization, tokens, etc.
- Most apps that support OpenID Connect start here

Discovery Metadata

{"TOKEN_ENDPOINT":"HTTPS://LOGIN.MICROSOFTONLINE.COM/COMMON/OAUTH2/
TOKEN","TOKEN_ENDPOINT_AUTH_METHODS_SUPPORTED":
["CLIENT_SECRET_POST","PRIVATE_KEY_JWT","CLIENT_SECRET_BASIC"],"JWKS_URI":"HTTPS://LOGIN.MICROSOFTONLINE.COM/
COMMON/DISCOVERY/KEYS","RESPONSE_MODES_SUPPORTED":["QUERY","FRAGMENT","FORM_POST"],"SUBJECT_TYPES_SUPPORTED":
["PAIRWISE"],"ID_TOKEN_SIGNING_ALG_VALUES_SUPPORTED":["RS256"],"RESPONSE_TYPES_SUPPORTED":
["CODE","ID_TOKEN","CODE ID_TOKEN","TOKEN ID_TOKEN","TOKEN"],"SCOPES_SUPPORTED":["OPENID"],"ISSUER":"HTTPS://
STS.WINDOWS.NET/{TENANTID}/","MICROSOFT_MULTI_REFRESH_TOKEN":TRUE,"AUTHORIZATION_ENDPOINT":"HTTPS://
LOGIN.MICROSOFTONLINE.COM/COMMON/OAUTH2/
AUTHORIZE","HTTP_LOGOUT_SUPPORTED":TRUE,"FRONTCHANNEL_LOGOUT_SUPPORTED":TRUE,"END_SESSION_ENDPOINT":"HTTPS://
LOGIN.MICROSOFTONLINE.COM/COMMON/OAUTH2/LOGOUT","CLAIMS_SUPPORTED":
["SUB","ISS","CLOUD_INSTANCE_NAME","CLOUD_INSTANCE_HOST_NAME","CLOUD_GRAPH_HOST_NAME","MSGRAPH_HOST","AUD","E
XP","IAT","AUTH_TIME","ACR","AMR","NONCE","EMAIL","GIVEN_NAME","FAMILY_NAME","NICKNAME"],"CHECK_SESSION_IFRAME":"HTTP
S://LOGIN.MICROSOFTONLINE.COM/COMMON/OAUTH2/CHECKSESSION","USERINFO_ENDPOINT":"HTTPS://LOGIN.MICROSOFTONLINE.COM/
COMMON/OPENID/
USERINFO","TENANT_REGION_SCOPE":NULL,"CLOUD_INSTANCE_NAME":"MICROSOFTONLINE.COM","CLOUD_GRAPH_HOST_NAME":"GR
APH.WINDOWS.NET","MSGRAPH_HOST":"GRAPH.MICROSOFT.COM","RBAC_URL":"HTTPS://PAS.WINDOWS.NET"}

Discovery Metadata

{"TOKEN_ENDPOINT":"HTTPS://LOGIN.MICROSOFTONLINE.COM/COMMON/OAUTH2/
TOKEN","TOKEN_ENDPOINT_AUTH_METHODS_SUPPORTED":
["CLIENT_SECRET_POST","PRIVATE_KEY_JWT","CLIENT_SECRET_BASIC"],"JWKS_URI":"HTTPS://LOGIN.MICROSOFTONLINE.COM/
COMMON/DISCOVERY/KEYS","RESPONSE_MODES_SUPPORTED":["QUERY","FRAGMENT","FORM_POST"],"SUBJECT_TYPES_SUPPORTED":
["PAIRWISE"],"ID_TOKEN_SIGNING_ALG_VALUES_SUPPORTED":["RS256"],"RESPONSE_TYPES_SUPPORTED":
["CODE","ID_TOKEN","CODE ID_TOKEN","TOKEN ID_TOKEN","TOKEN"],"SCOPES_SUPPORTED":["OPENID"],"ISSUER":"HTTPS://
STS.WINDOWS.NET/{TENANTID}/","MICROSOFT_MULTI_REFRESH_TOKEN":TRUE,"AUTHORIZATION_ENDPOINT":"HTTPS://
LOGIN.MICROSOFTONLINE.COM/COMMON/OAUTH2/
AUTHORIZE","HTTP_LOGOUT_SUPPORTED":TRUE,"FRONTCHANNEL_LOGOUT_SUPPORTED":TRUE,"END_SESSION_ENDPOINT":"HTTPS://
LOGIN.MICROSOFTONLINE.COM/COMMON/OAUTH2/LOGOUT","CLAIMS_SUPPORTED":
["SUB","ISS","CLOUD_INSTANCE_NAME","CLOUD_INSTANCE_HOST_NAME","CLOUD_GRAPH_HOST_NAME","MSGRAPH_HOST","AUD","E
XP","IAT","AUTH_TIME","ACR","AMR","NONCE","EMAIL","GIVEN_NAME","FAMILY_NAME","NICKNAME"],"CHECK_SESSION_IFRAME":"HTTP
S://LOGIN.MICROSOFTONLINE.COM/COMMON/OAUTH2/CHECKSESSION","USERINFO_ENDPOINT":"HTTPS://LOGIN.MICROSOFTONLINE.COM/
COMMON/OPENID/
USERINFO","TENANT_REGION_SCOPE":NULL,"CLOUD_INSTANCE_NAME":"MICROSOFTONLINE.COM","CLOUD_GRAPH_HOST_NAME":"GR
APH.WINDOWS.NET","MSGRAPH_HOST":"GRAPH.MICROSOFT.COM","RBAC_URL":"HTTPS://PAS.WINDOWS.NET"}

Setup

- Create new Discovery Metadata document for “Pseudo” IdP (PIdP)
- Use AWS API Gateway to forward from PIdP to real IdP, or not
- Snag `URLSessions` to PIdP, do what you need in the SSOE

OpenID Configuration

https://login.microsoftonline.com/common/v2.0/.well-known/openid-configuration

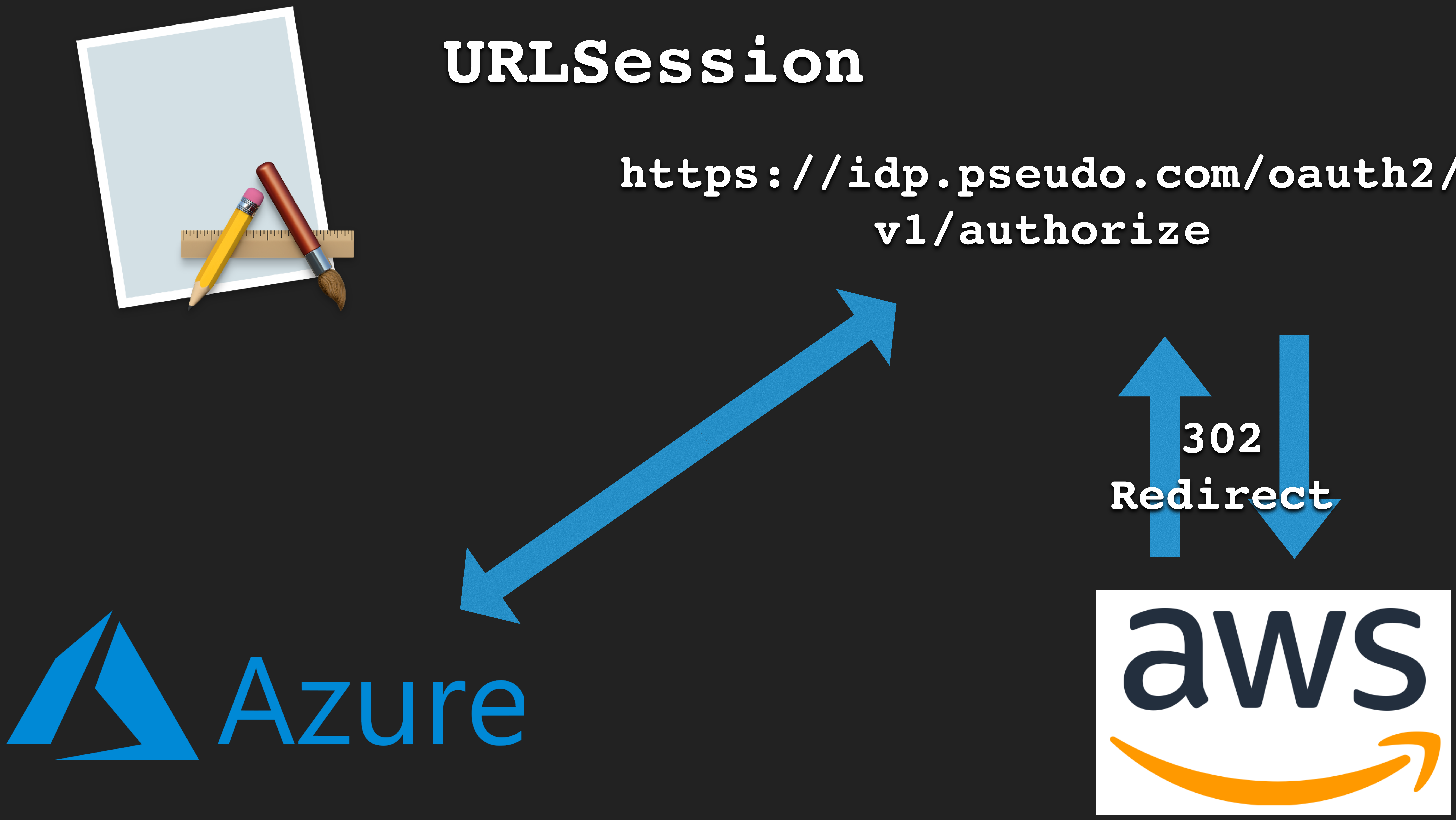
Azure

OpenID Configuration

https://idp.pseudo.com/.well-known/openid-configuration

API Gateway

1. Swap authorize endpoint
2. Setup 302 redirect



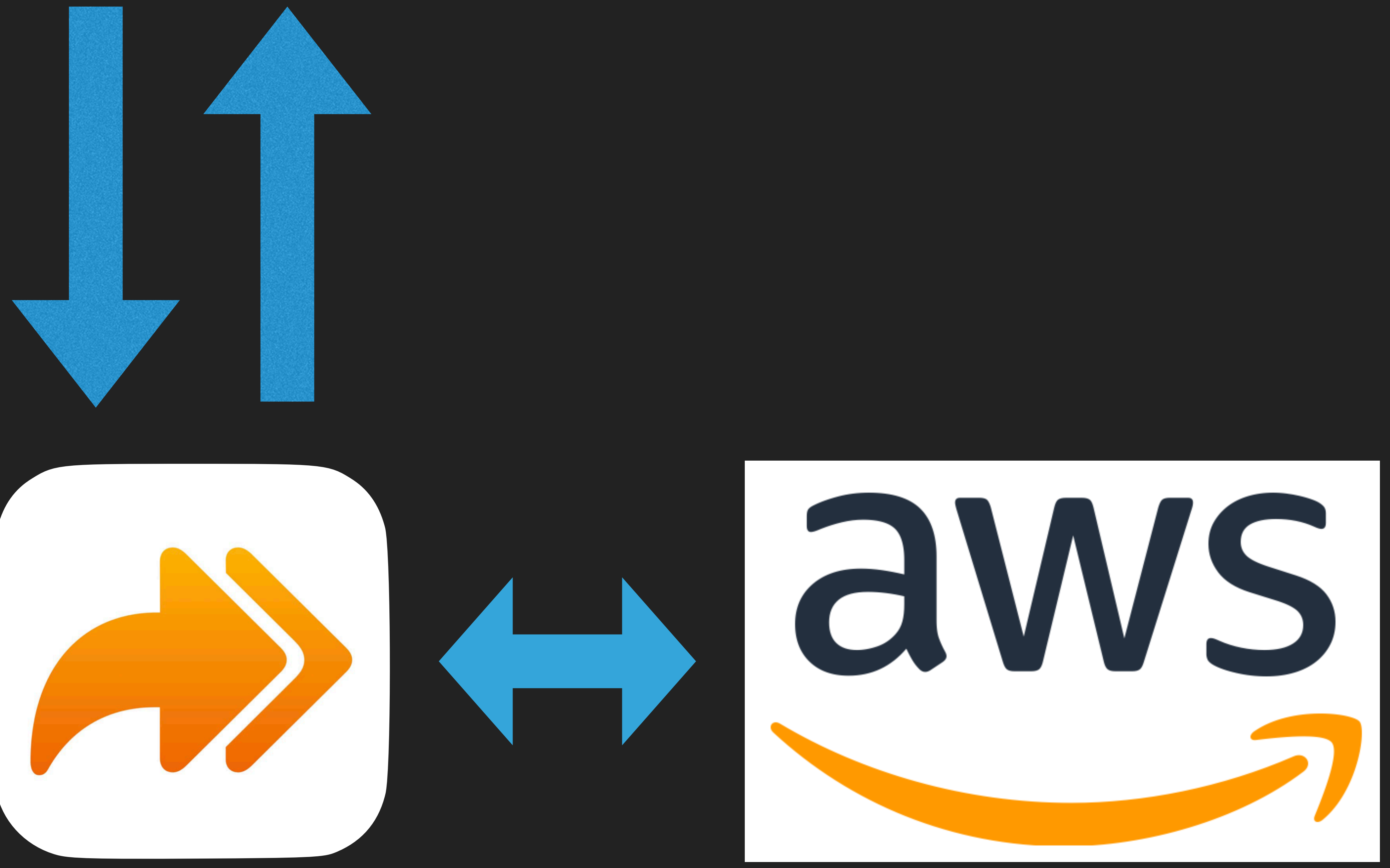
URLSession

https://idp.pseudo.com/oauth2/v1/authorize

302 Redirect

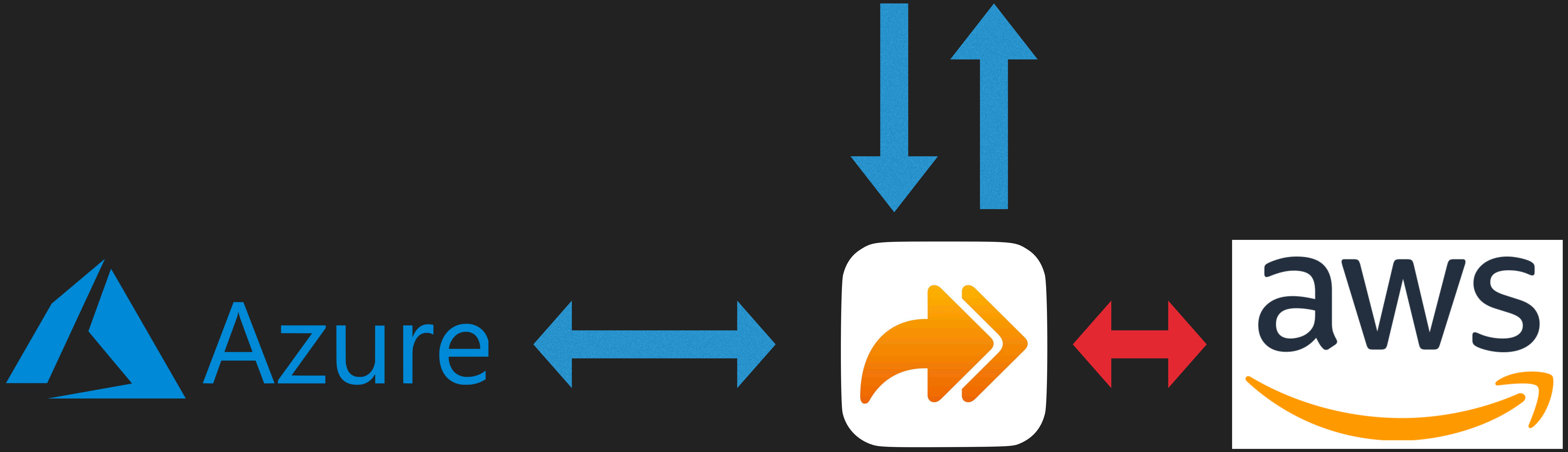
URLSession

https://idp.pseudo.com/oauth2/v1/authorize



URLSession

`https://idp.pseudo.com/oauth2/v1/authorize`



Working Example

https://gitlab.com/Mactroll/ssoeexample

Note: you'll need a few things to make this work…

1. Apple Dev Account
2. An endpoint you can use and host an AASA file
3. MDM

Troubleshooting

Figuring out what’s gone wrong

Troubleshooting Redirects

- `swcutil`
- `pluginkit`
- `curl`
- `com.apple.AppSSO` subsystem

swcutil

- `/System/Library/PrivateFrameworks/SharedWebCredentials.framework/Support/swcutil`
- Used to troubleshoot Shared Web Credentials, but also covers associated domains for this

pluginkit

- `pluginkit -m -i menu.nomad.sso`
- Used to determine which app extension is registered for which uses and domains

curl

- Curl https://login.micorosftonline.com/.well-known/apple-app-site-association
- Validate AASA file

Logs

- Console or your favorite log viewer
- Search on `AppSSO`

In Summary

Some parting thoughts…

There are a lot of moving pieces to a SSOE

If you control your IdP you can make an SSOE

If you don’t control your IdP you may still be able to do some things

Thanks!

👋