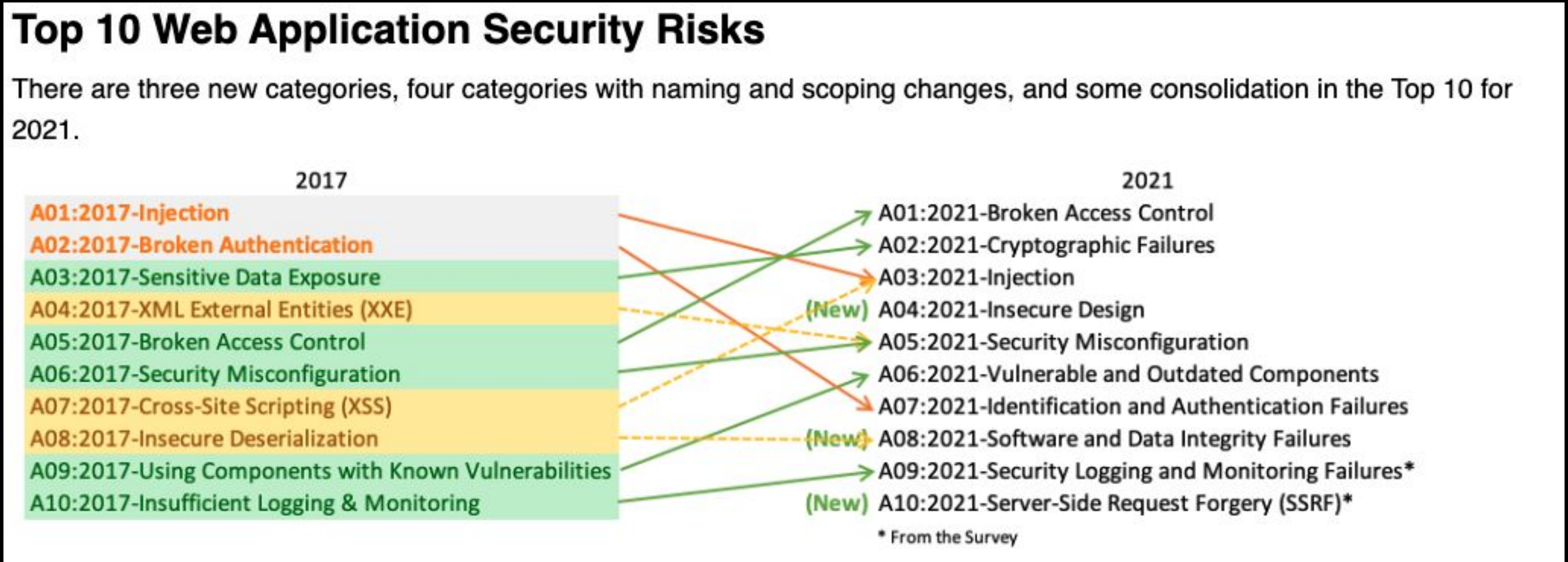
Broken authentication

Når det beste ikke er godt nok

Alexander Hatlen @ KiNS:Tech 2024



Top 10 Web Application Security Risks

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.

2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Før

- Gjenbruke det ene gode passordet

ELLER

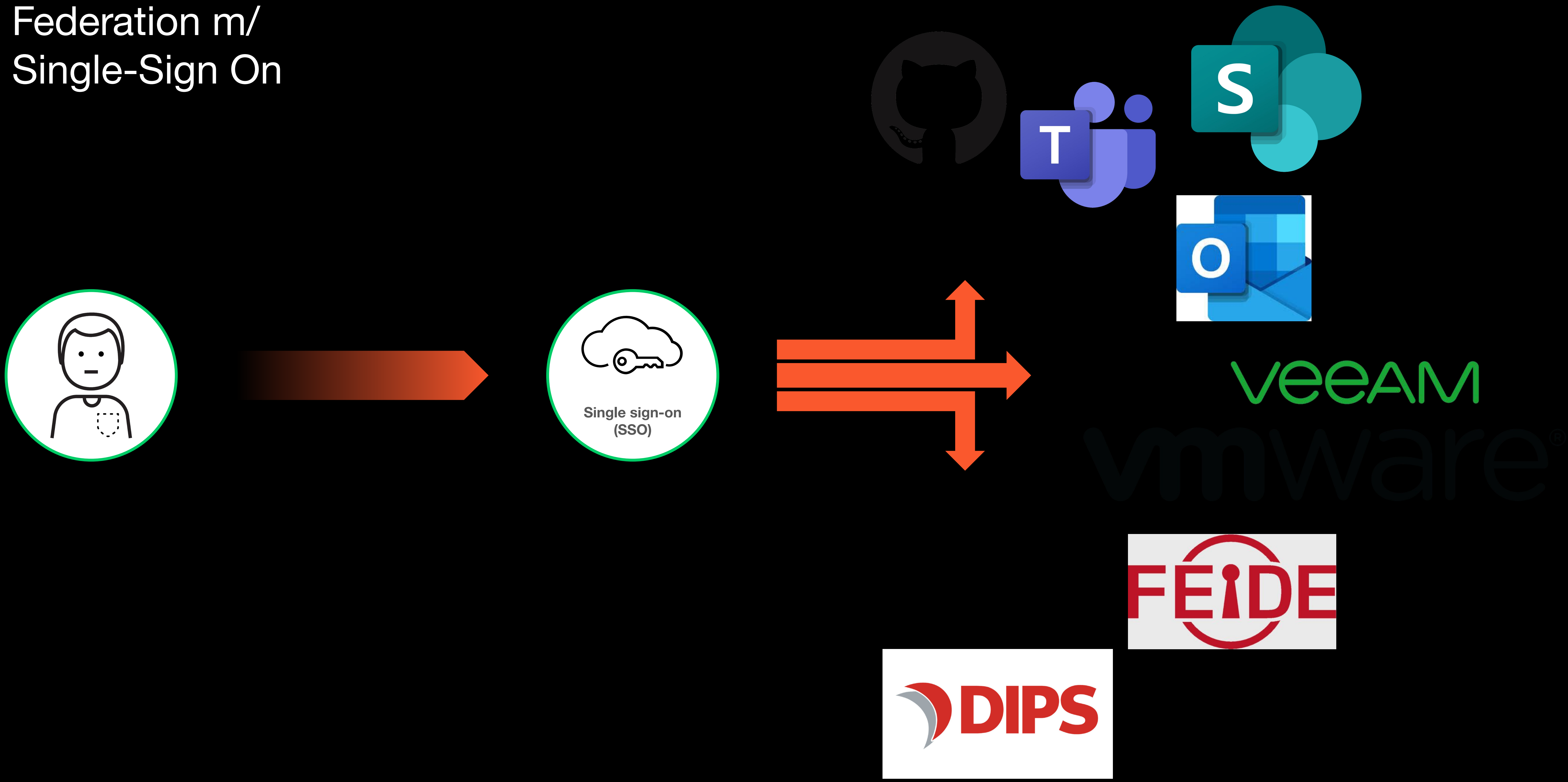
- Ha unike passord, med et mønster

For de spesielt proffe

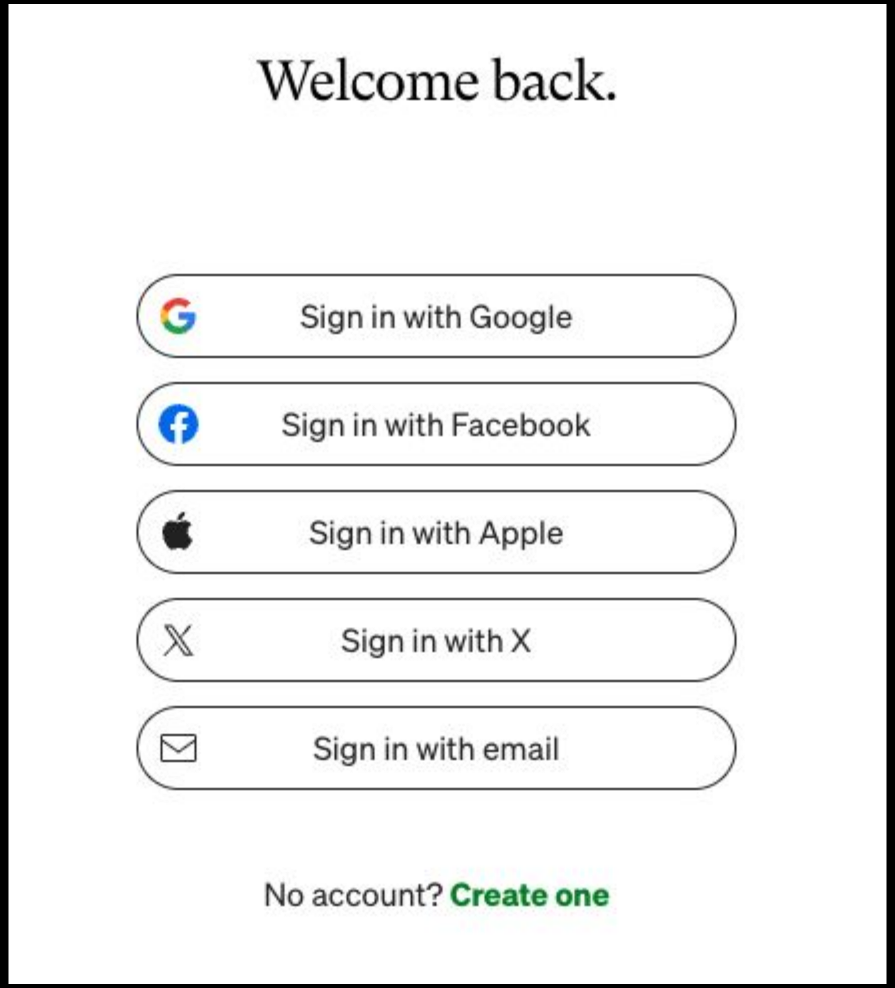
- Passordwallet

Nå

- Federation m/ Single-Sign On

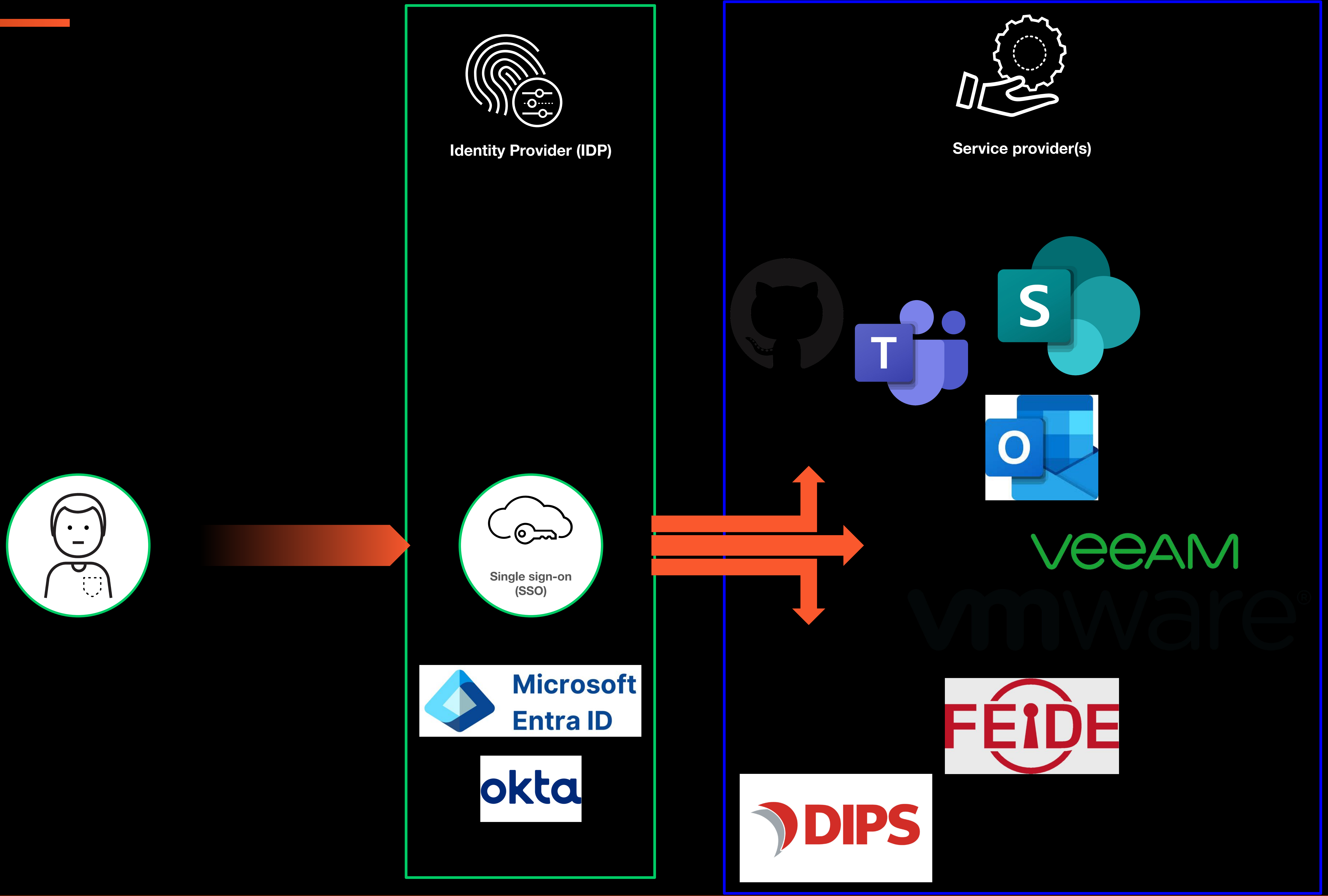


Kanskje mer kjent som



Welcome back.

No account? **Create one**



Identity Provider (IDP)

Single sign-on (SSO)

Service provider(s)

De ~~fire~~ tre store

SAML v2.0

OAUTH 2

OpenID

“OIDC”

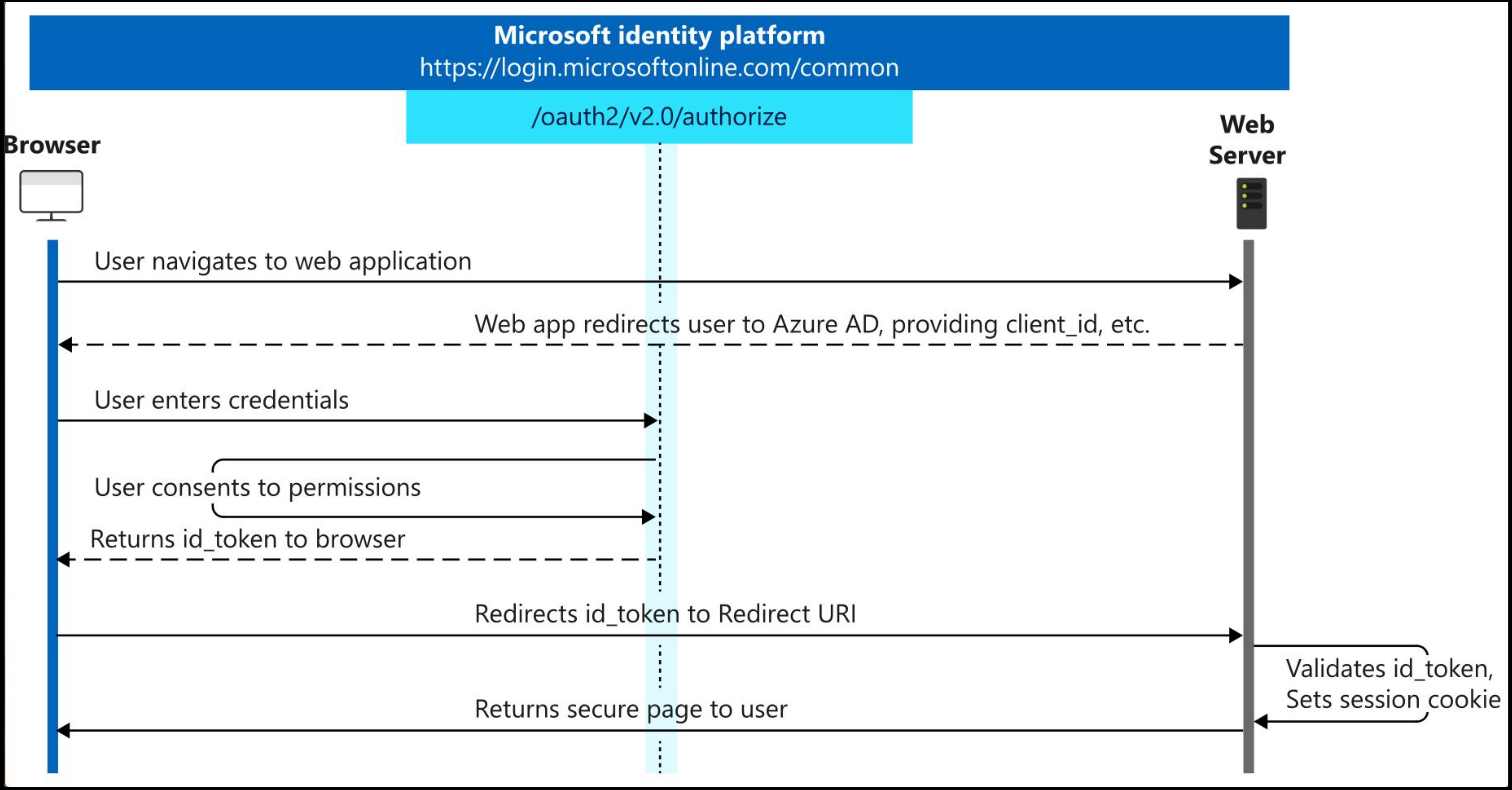
SCIM
System for Cross-domain Identity Management

WSFed

De vi snakker om i dag

“OIDC”

Hvordan fungerer Single-Sign On / federering i OpenID Connect (OIDC)?



Microsoft identity platform

https://login.microsoftonline.com/common

/oauth2/v2.0/authorize

Browser

Web Server

User navigates to web application

Web app redirects user to Azure AD, providing client_id, etc.

User enters credentials

User consents to permissions

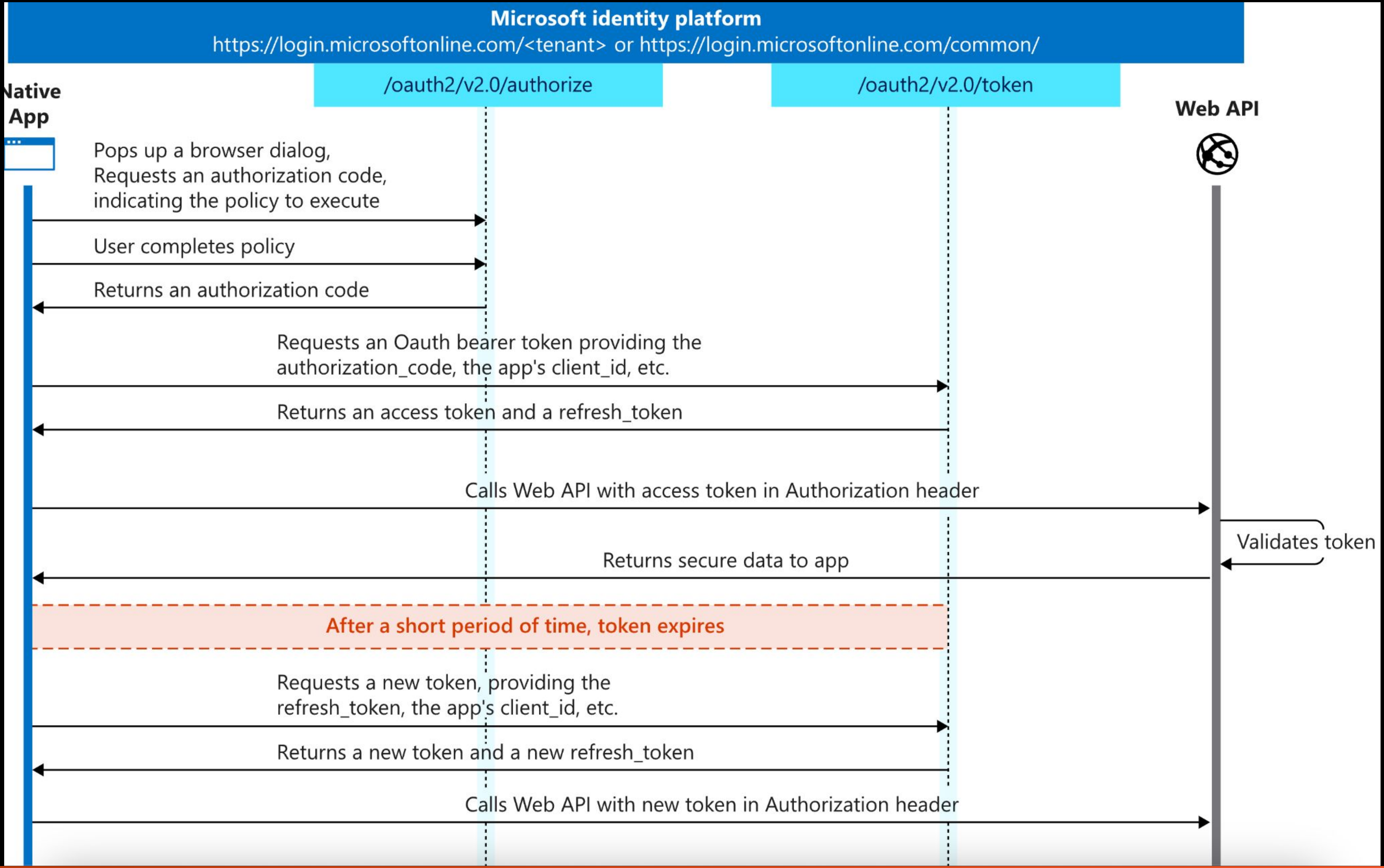
Returns id_token to browser

Redirects id_token to Redirect URI

Validates id_token, Sets session cookie

Returns secure page to user

Hvordan fungerer Single-Sign On / federering i OAUTH?



Microsoft identity platform
https://login.microsoftonline.com/<tenant> or https://login.microsoftonline.com/common/

/oauth2/v2.0/authorize

/oauth2/v2.0/token

Native App

Web API

Pops up a browser dialog, Requests an authorization code, indicating the policy to execute

User completes policy

Returns an authorization code

Requests an Oauth bearer token providing the authorization_code, the app's client_id, etc.

Returns an access token and a refresh_token

Calls Web API with access token in Authorization header

Validates token

Returns secure data to app

After a short period of time, token expires

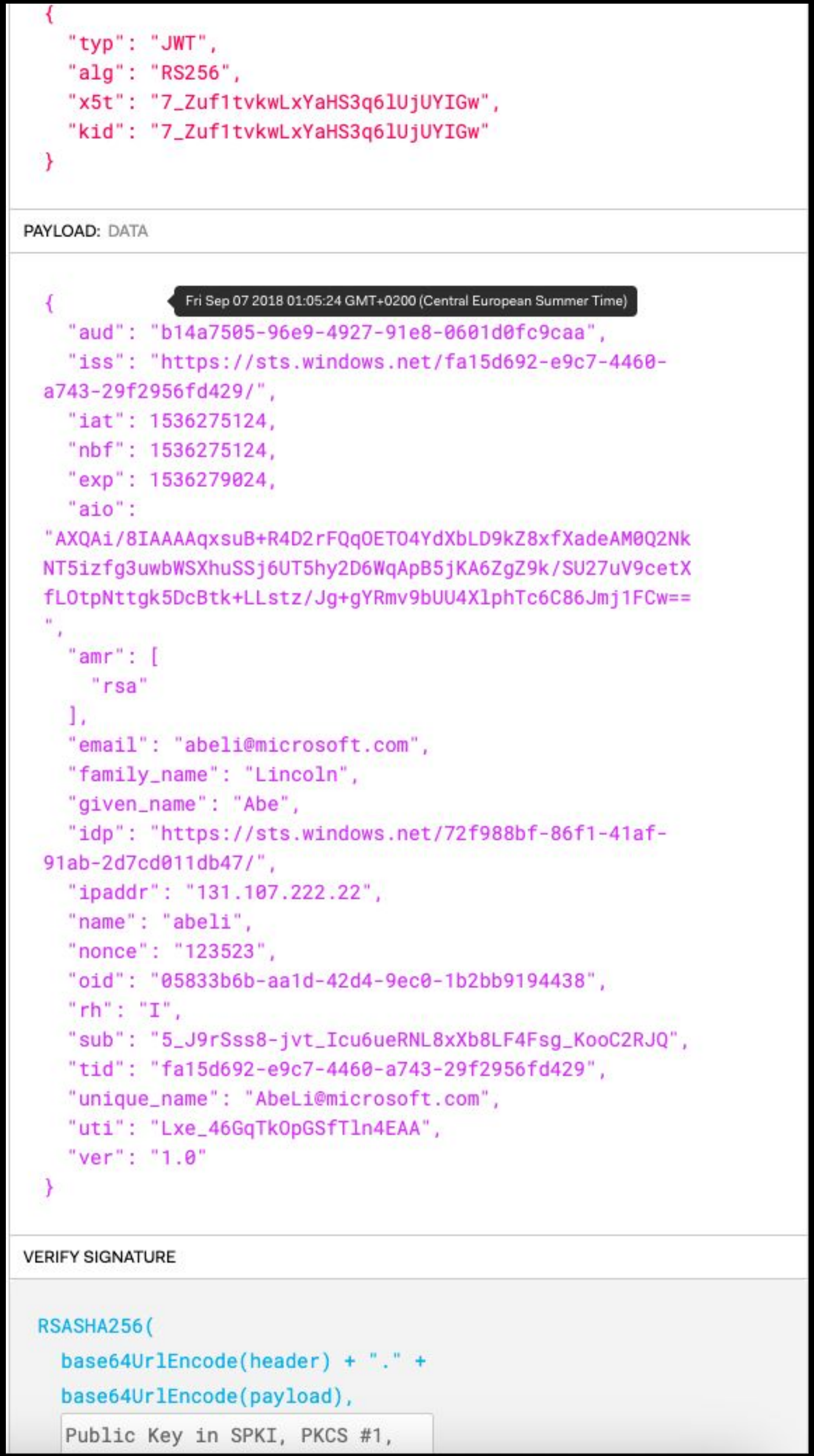
Requests a new token, providing the refresh_token, the app's client_id, etc.

Returns a new token and a new refresh_token

Calls Web API with new token in Authorization header

(id_)token?

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IjFMVE16Y
WtpaGlSbGFfOHoyQkVKVlhlV01xbyJ9.eyJ2ZXIiOiIyLjAiLCJpc
3MiOiJodHRwczovL2xvZ2luLm1pY3Jvc29mdG9ubGluZS5jb2
0vOTEyMjA0MGQtNmM2Ny00YzViLWIxMTItMzZhMzA0YjY2Z
GFkL3YyLjAiLCJzdWIiOiJBQUFBQUFBQUFBQUFBQUFBQUFBQUF
BQUFJa3pxRlZyU2FTYUZIeTc4MmJidGFRIiwiYXVkIjoiNmNiM
DQwMTgtYTNmNS00NmE3LWI5OTUtOTQwYzc4ZjVhZWYzIi
wiZXhwIjoxNTM2MzYxNDExLCJpYXQiOjE1MzYyNzQ3MTEsI
m5iZiI6MTUzNjI3NDcxMSwibmFtZSI6IkFiZSBMaW5jb2xuIiwic
HJlZmVycmVkX3VzZXJuYW1lIjoiQWJlTGlAbWljcm9zb2Z0Lm
NvbSIsIm9pZCI6IjAwMDAwMDAwLTAwMDAtMDAwMC02Nm
YzLTMzMzJlY2E3ZWE4MSIsInRpZCI6IjkxMjIwNDBkLTZjNjctN
GM1Yi1iMTEyLTM2YTMwNGI2NmRhZCIsIm5vbmNlIjoiMTIzN
TIzIiwiYWlvIjoiRGYyVVZYTDFpeCFsTUNXTVNPSkJjRmF0emN
HZnZGR2hqS3Y4cTVnMHg3MzJkUjVNQjVCaXN2R1FPN1lXQ
nlqZDhpUURMcSFlR2JJRGFreXA1bW5PcmNkcUhlWVNubHR
lcFFtUnA2QUlaOGpZIn0.1AFWW-Ck5nROwSlItm7GzZvDwUk
qvhSQpm55TQsmVo9Y59cLhRXpvB8n-55HCr9Z6G_31_Ube
Ukoz612I2j_Sm9FFShSDDjoaLQr54CreGIJvjtmS3EkK9a7SJB
bcpL1MpUtIfygow39tFjY7EVNW9pIWUvRrTgVk7IYLprvfzw-CI
qw3gHC-T7IK_m_xkr08INERBtaecwhTeN4chPC4W3jdmw_IIx
zC48YoQ0dB1L9-ImX98EgypfrIbm0IBL5spFzL6JDZIRRJOu8v
ecJvj1mq-IUhGt0MacxX8jdxYLP-KUu2d9MbNKpCKJuZ7p8g
wTL5B7NIUdh_dmSviPWrw



```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "7_Zuf1tvkwLxYaHS3q6lUjUYIGw",
  "kid": "7_Zuf1tvkwLxYaHS3q6lUjUYIGw"
}
```

PAYLOAD: DATA

Fri Sep 07 2018 01:05:24 GMT+0200 (Central European Summer Time)

```
{
  "aud": "b14a7505-96e9-4927-91e8-0601d0fc9caa",
  "iss": "https://sts.windows.net/fa15d692-e9c7-4460-
a743-29f2956fd429/",
  "iat": 1536275124,
  "nbf": 1536275124,
  "exp": 1536279024,
  "aio":
"AXQAi/8IAAAAqxsuB+R4D2rFQqOETO4YdXbLD9kZ8xfXadeAM0Q2Nk
NT5izfg3uwbWSXhuSSj6UT5hy2D6WqApB5jKA6ZgZ9k/SU27uV9cetX
fLOtpNttgk5DcBtk+LLstz/Jg+gYRmv9bUU4XlphTc6C86Jmj1FCw==
",
  "amr": [
    "rsa"
  ],
  "email": "abeli@microsoft.com",
  "family_name": "Lincoln",
  "given_name": "Abe",
  "idp": "https://sts.windows.net/72f988bf-86f1-41af-
91ab-2d7cd011db47/",
  "ipaddr": "131.107.222.22",
  "name": "abeli",
  "nonce": "123523",
  "oid": "05833b6b-aa1d-42d4-9ec0-1b2bb9194438",
  "rh": "I",
  "sub": "5_J9rSss8-jvt_Icu6ueRNL8xXb8LF4Fsg_KooC2RJQ",
  "tid": "fa15d692-e9c7-4460-a743-29f2956fd429",
  "unique_name": "AbeLi@microsoft.com",
  "uti": "Lxe_46GqTkOpGSfTln4EAA",
  "ver": "1.0"
}
```

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key in SPKI, PKCS #1,
```

base64(header).base64(payload).base64(signature)

Issue #1: aud(ience)

Issue #2: Iss(uer)

Issue #3(0?): Email

Issue #4: Complicated signature verification

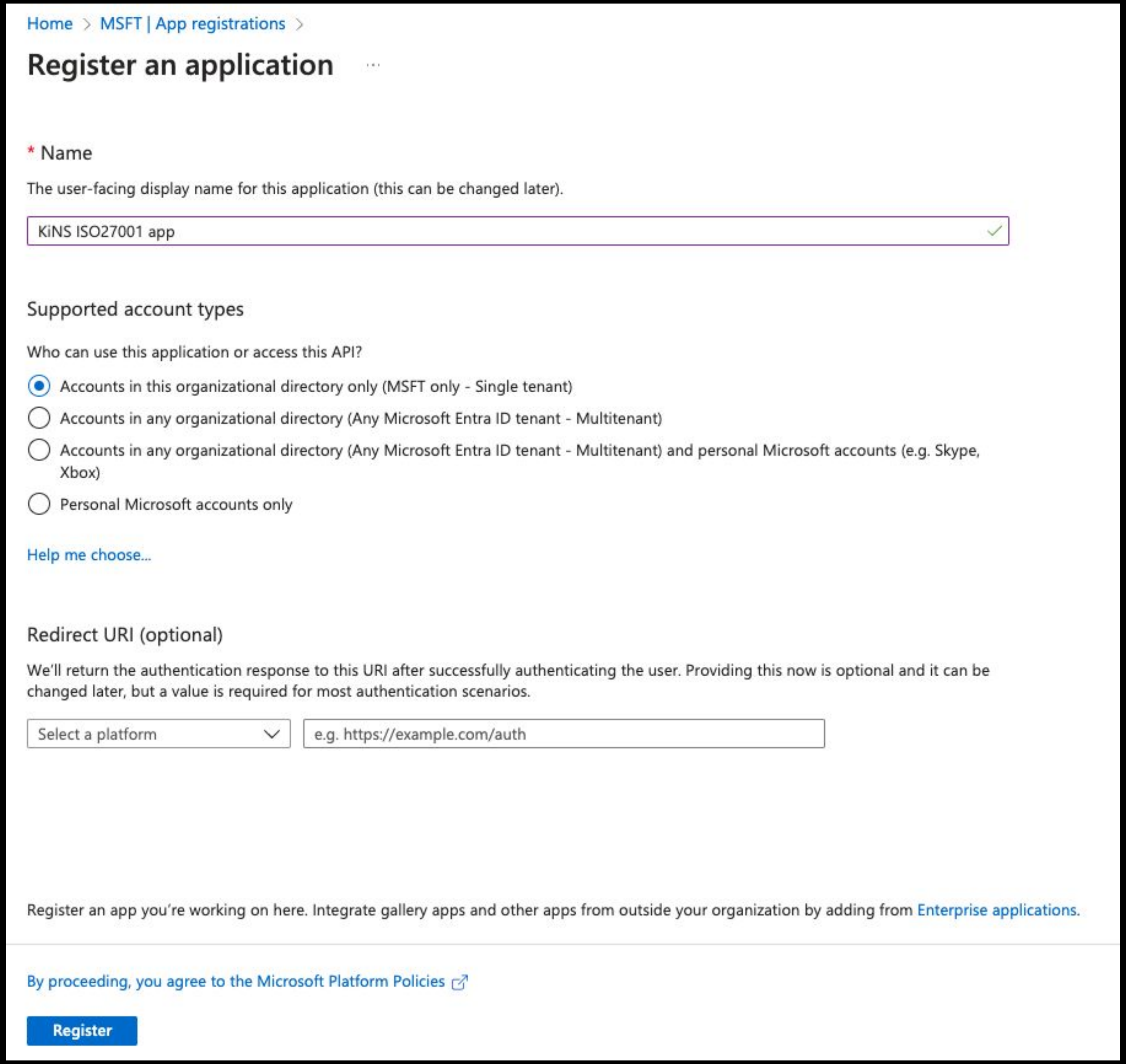
Issue #5: Mangel på Step-Up funksjonalitet

Issue #6: Multi-tenancy

In-App tenancy
Multi-tenancy funksjonalitet inni app.
Tenancy tilhørigheter.

Public vs private oauth/cloud apps

Hvem har lov til å benytte en “app” for pålogging?



Home > MSFT | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

KiNS ISO27001 app ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (MSFT only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

> The results surprised us: 25% of all the multi-tenant apps we scanned were vulnerable to authentication bypass.
> - Wiz.io

Issue #7: Lack of implementation guidelines

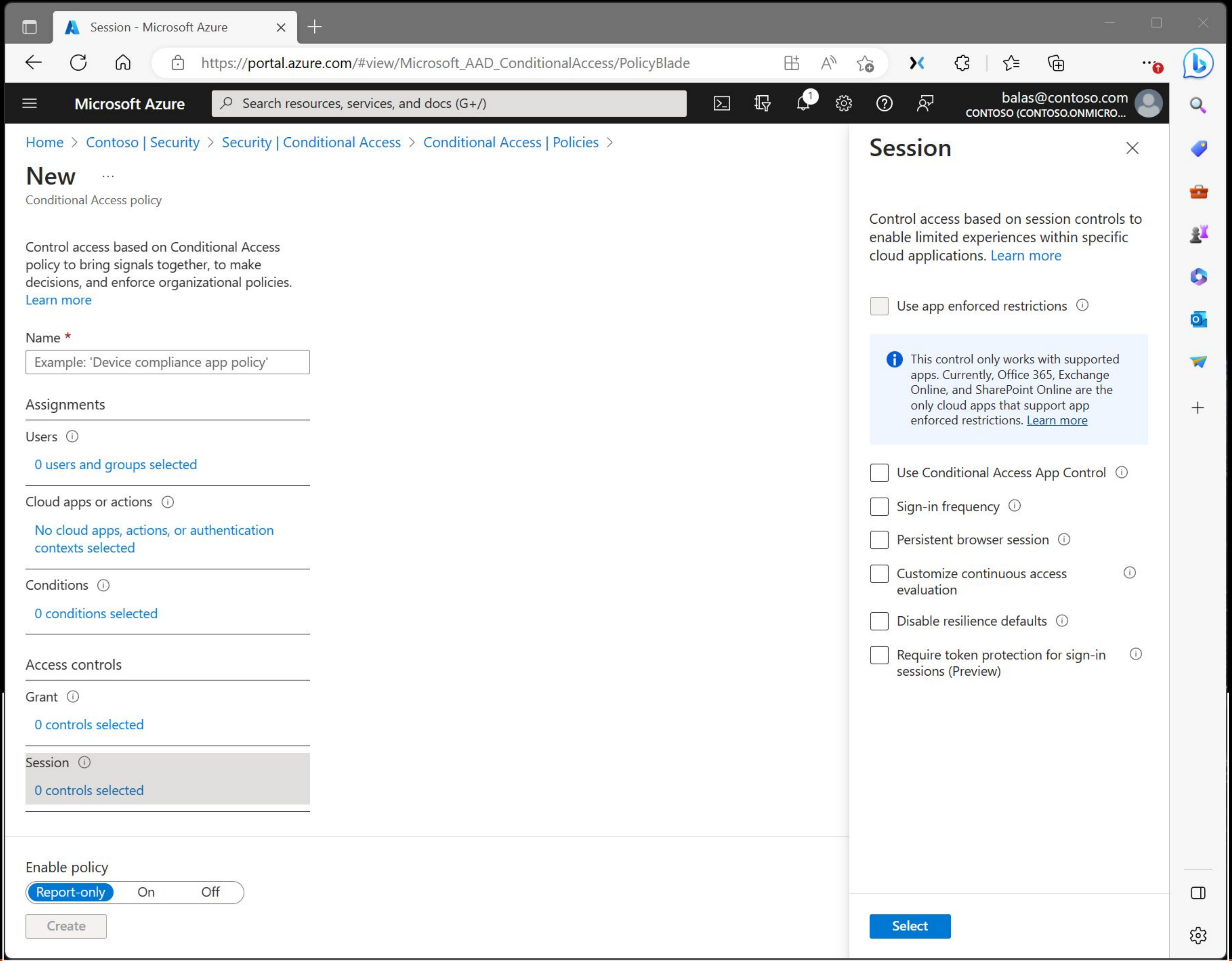
Makes stuff like using email typical, or ending up with Single Sign-Up…

Multi-tenancy issues.

AuthZ is a bit limited, easier to implement on app-side than IdP.

Very few default/required claims, big differences in IdPs.

Issue #8: Microsoft Conditional Access fallacity



Session - Microsoft Azure
https://portal.azure.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade
Microsoft Azure
Search resources, services, and docs (G+/)
balas@contoso.com
CONTOSO (CONTOSO.ONMICRO...

Home > Contoso | Security > Security | Conditional Access > Conditional Access | Policies >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Example: 'Device compliance app policy'

Assignments

Users

0 users and groups selected

Cloud apps or actions

No cloud apps, actions, or authentication contexts selected

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Enable policy

[✓ Report-only] On Off

Create

Session

Control access based on session controls to enable limited experiences within specific cloud applications. Learn more

□ Use app enforced restrictions

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Learn more

□ Use Conditional Access App Control

□ Sign-in frequency

□ Persistent browser session

□ Customize continuous access evaluation

□ Disable resilience defaults

□ Require token protection for sign-in sessions (Preview)

Select

Issue #9-99: Alle de andre angrepene mot oauth

Token replay

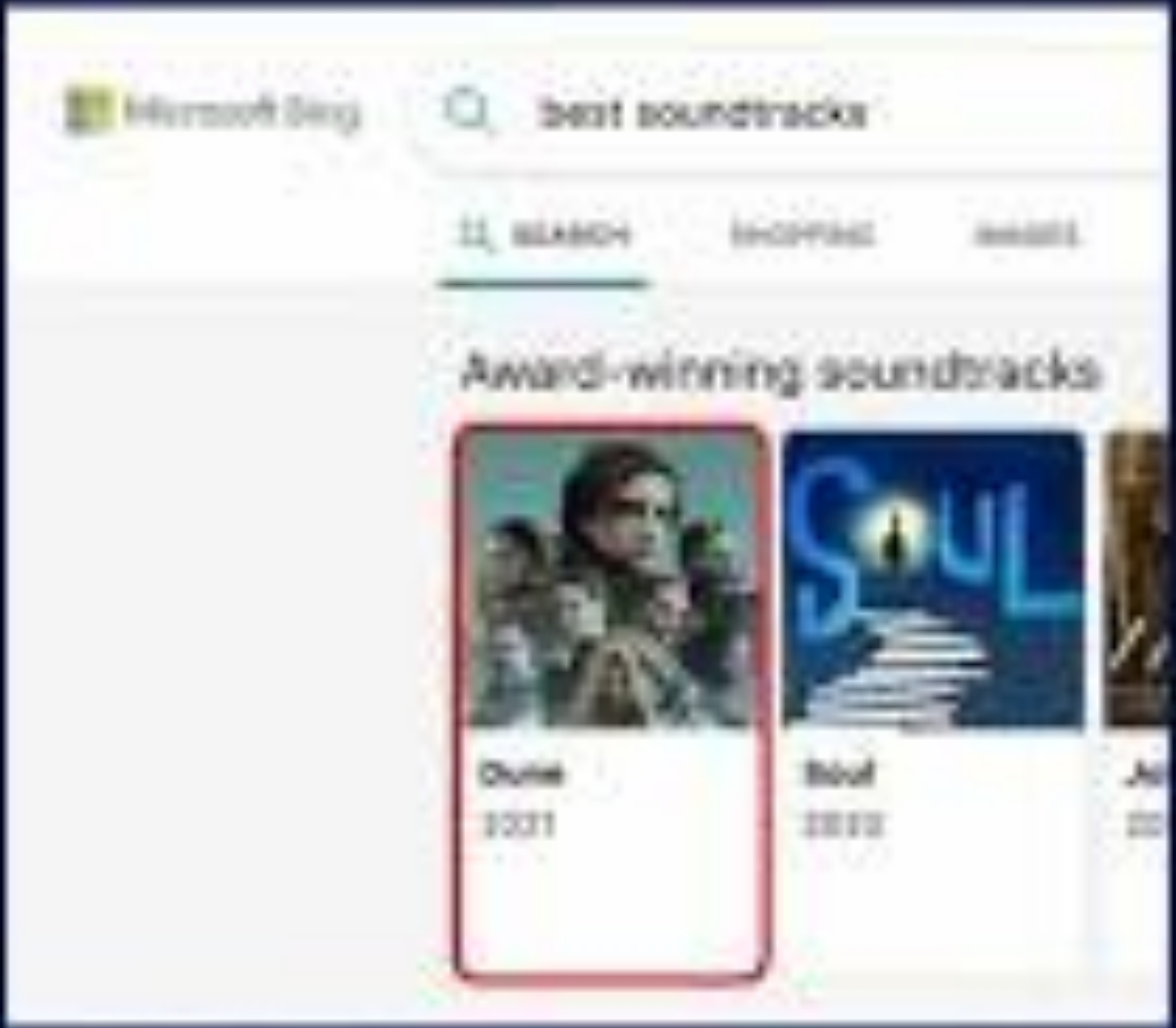
Device code phishing

Javascript-stealable tokens (and refresh tokens..)

Access tokens kan ikke revokeres

Mange diverse ting i utdaterte OAUTH flows før versjon 2.1. Gjenstår noen få problemer på protokoll-nivå, men det aller meste av trøbbel skjer ved implementasjon.

Demo



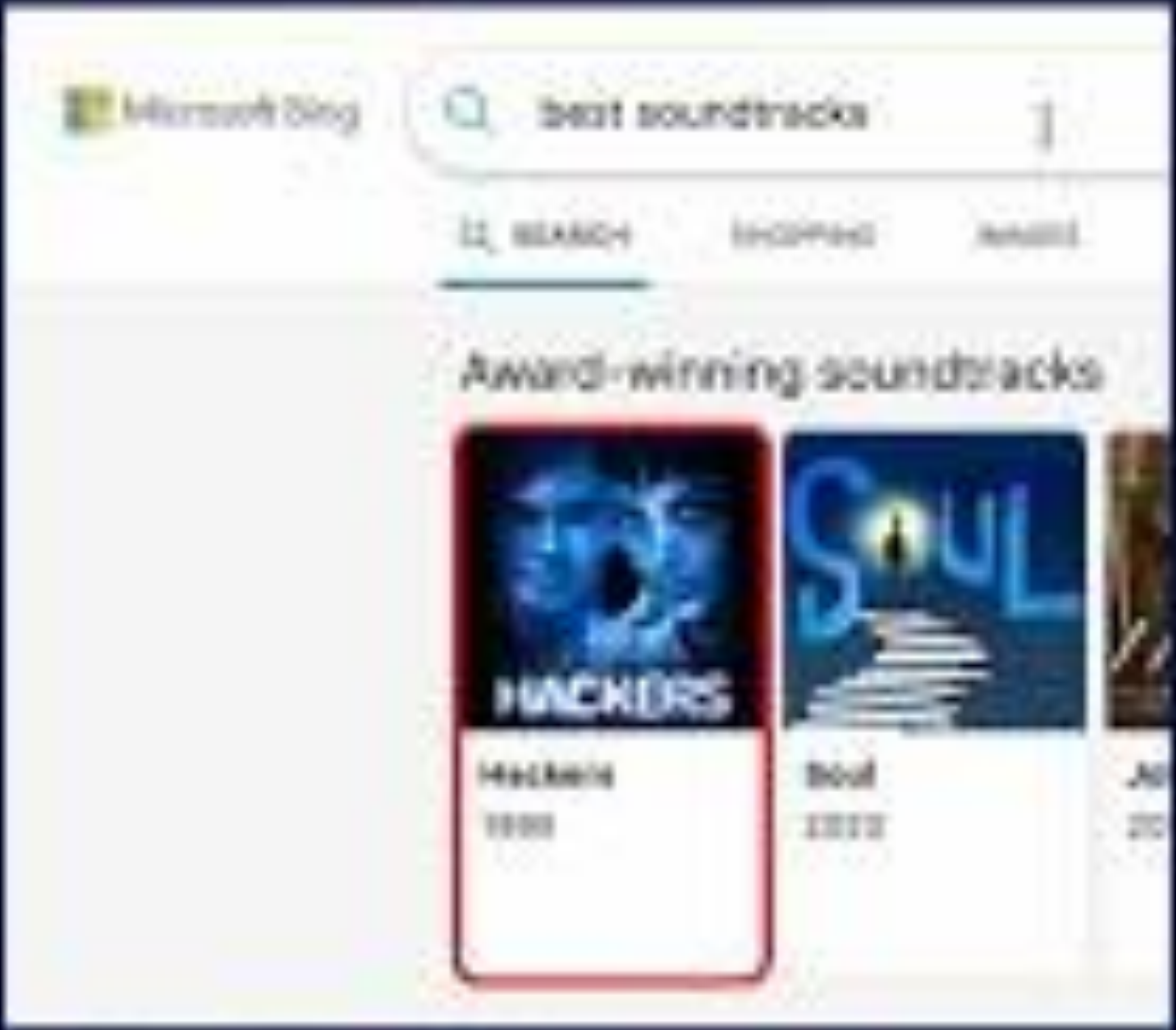
best soundtracks

Award-winning soundtracks

Dune
2021

Soul
2020

Original bing.com results



best soundtracks

Award-winning soundtracks

Hackers
1995

Soul
2020

Modified bing.com results

Konklusjon

Positivt

- En veldig god og sikker protokoll
- Sikker som banken!
- Forenkler hverdagen for brukerne
- Raskere å jobbe, ingen passord-gjenbruk, ingen behov for passordwallet, sømløs brukeropplevelse
- Gir kontroll på SaaS gjennom identitets-federering
- Gir logging for pålogginger i eksterne applikasjoner
- Lar deg sentralt håndtere lifecycle av brukere i fagapplikasjoner
- Perfekt å bruke sammen med passordløs autentisering for å fjerne phishing-risikoer

Negativt/obs

- Implementasjon på tjenestetilbyder-siden er alfa omega
- Mangler MYE implementasjons-guiding
- De som lager OAUTH app må ha kontroll på tenant-scope og aksesstilganger
- Apper bør allow-listes i enhver business tenant for å hindre phishing og persistens fra angripere
- "Identitet er den nye perimeteren" hindrer ikke tilgang til å utnytte sårbarheter i tjenesten slik nettverksperimeter gjør
  (husk at exploiting har skutt i været forbi phishing i 2023)

Thank You

paloaltonetworks.com

Alexander Hatlen
Løsningsspesialist
@ Palo Alto Networks
ahatlen@paloaltonetworks.com