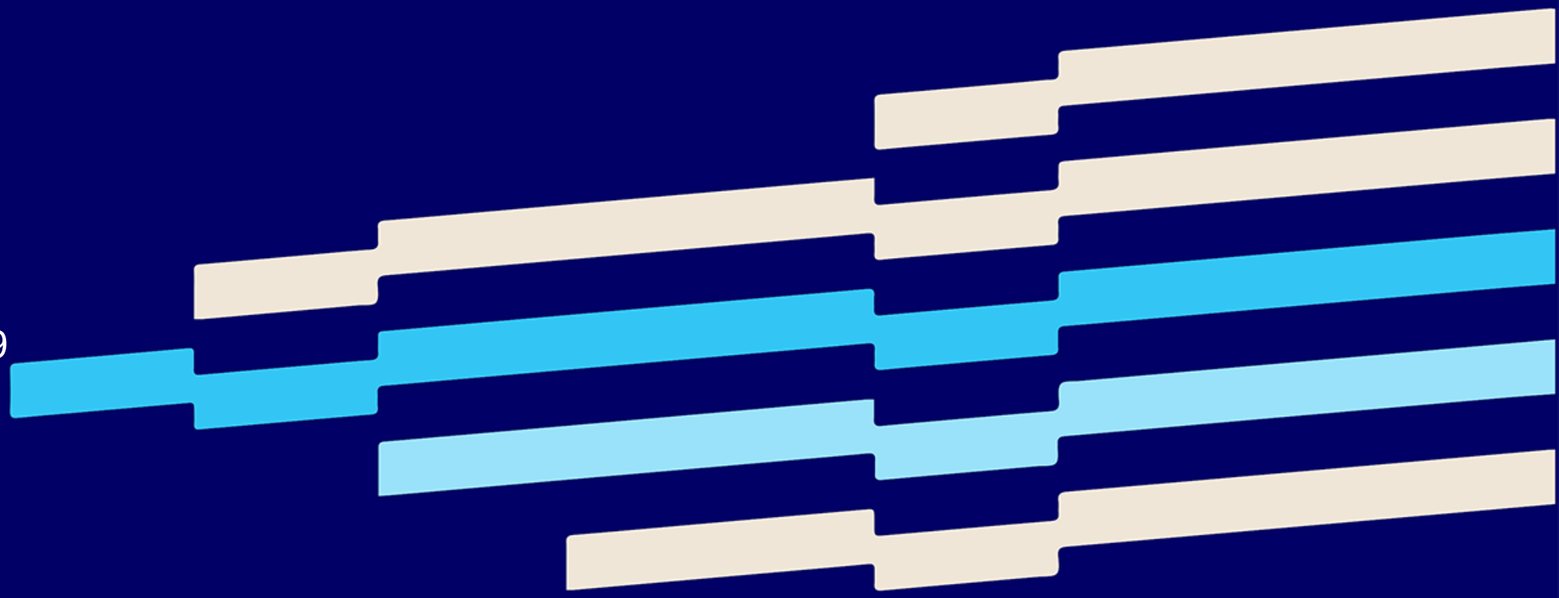
Difi
Direktoratet for
forvaltning og ikt

Korleis bruke eit API sikra med ID-porten i din SPA

Randi Øyri

19.11.2019

Integrasjons- og sikkerhetsforum 2019



Plan

- SPA
- SPA -> API
- Demo
- Demo
- Demo
- Demo
- Demo
- Demo
- ….

Difi

Difi

SPA – Single Page Application

- Javascript-applikasjon som lever i nettlesaren til sluttbrukar på ei side.
- Laster inn dei delene av sida den treng, ikkje heile sida på nytt som tradisjonelle web-applikasjoner
- Betre brukaropplevelse og ytelse

Difi

SPA vs serverside applikasjon: utfordringar

- Ikkje kontroll på hemmelegheiter (client secret)
- Hente data frå 3-parts API med brukar-id (Cross-Origin)

Difi

“SPA may turn out to be impossible to completely secure.

However that wont stop people from creating them.”

- John Bradley

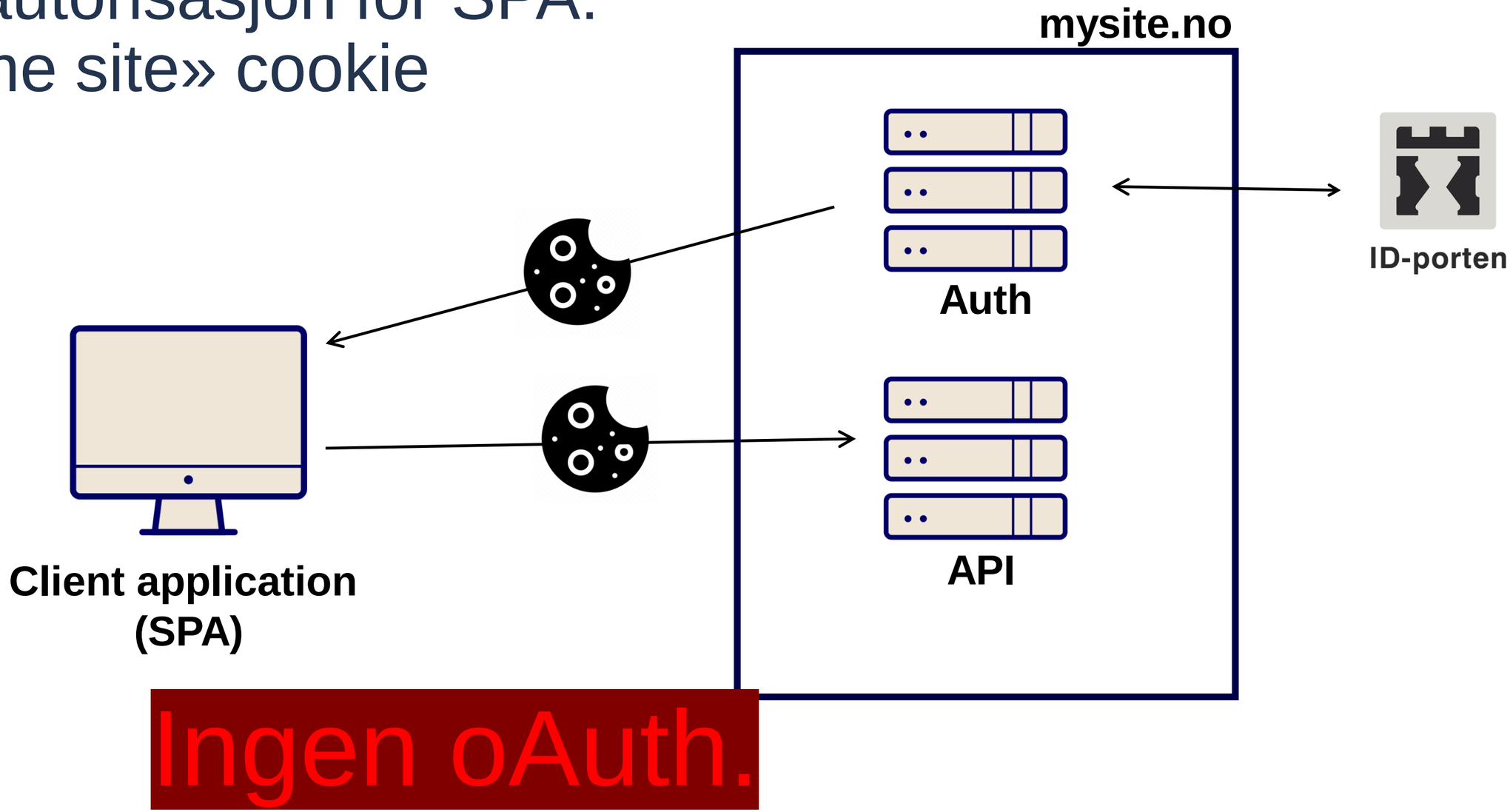
Difi

Korleis lage ein SPA for å hente ut data frå eit API?

…som er er trygg nok?

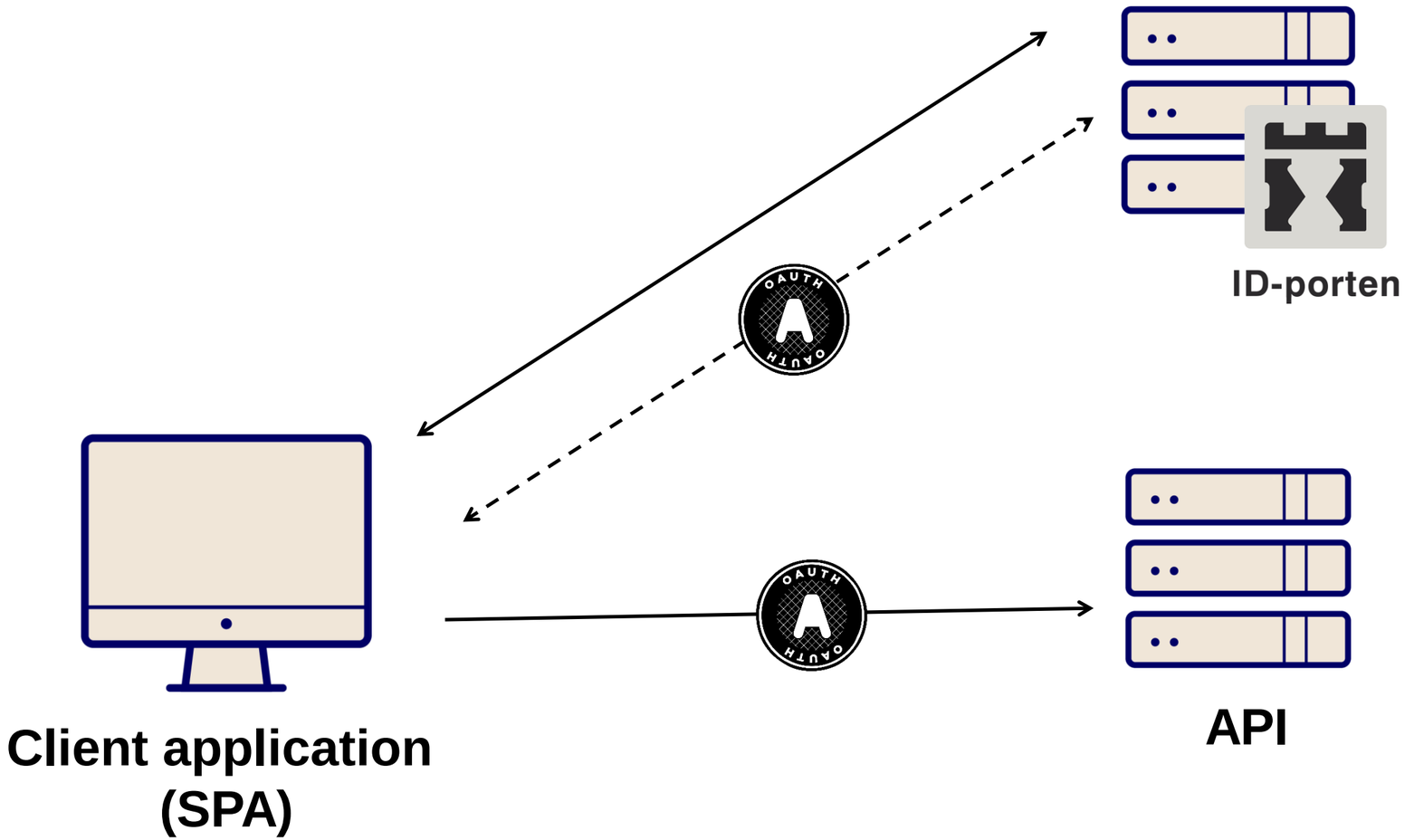
Difi

API-autorisasjon for SPA: «Same site» cookie



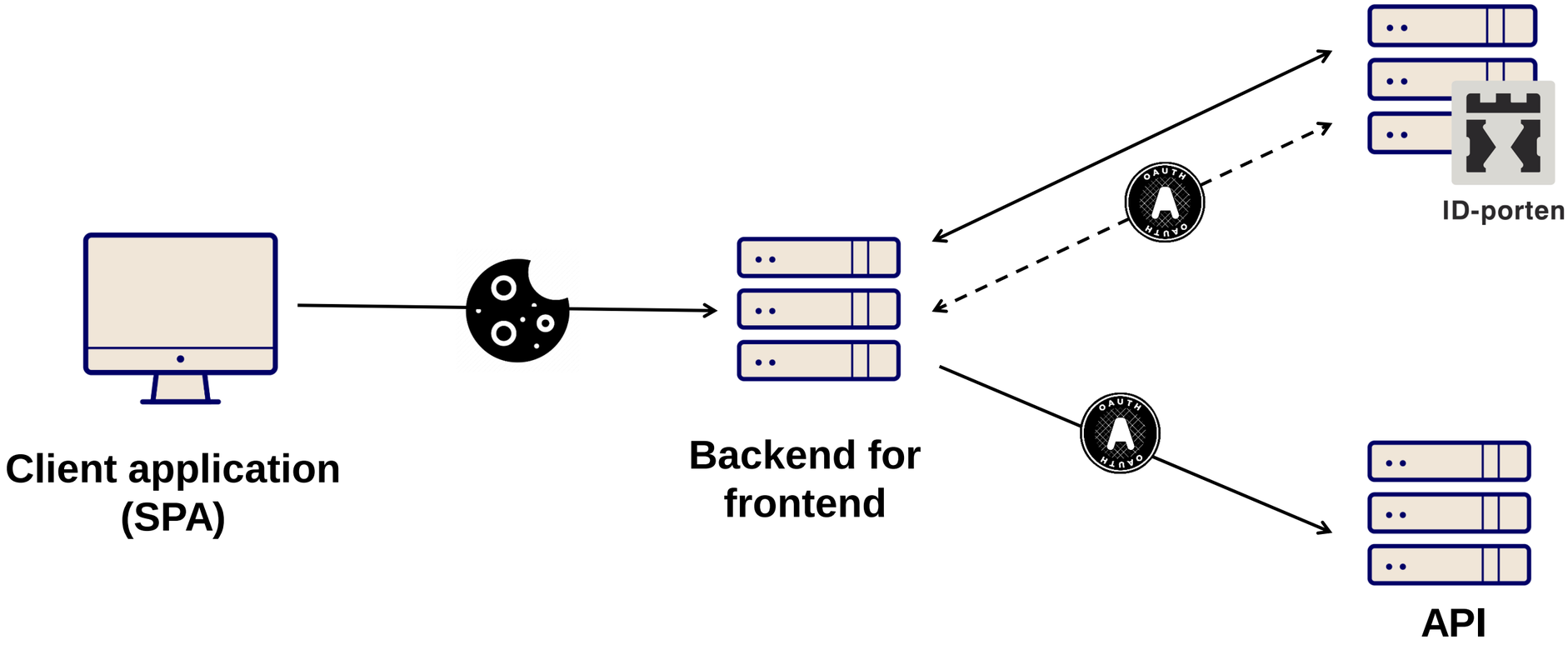
Difi

API-autorisasjon for SPA:
OAuth2 Authorization Code + PKCE



Difi

API-autorisasjon for SPA: «Backend-for-frontend» pattern



Difi


LIVE DEMO ?
VIA 9GAG.COM
I LIKE IT BECAUSE IT ALWAYS FAILS.
quickmeme.com

Difi

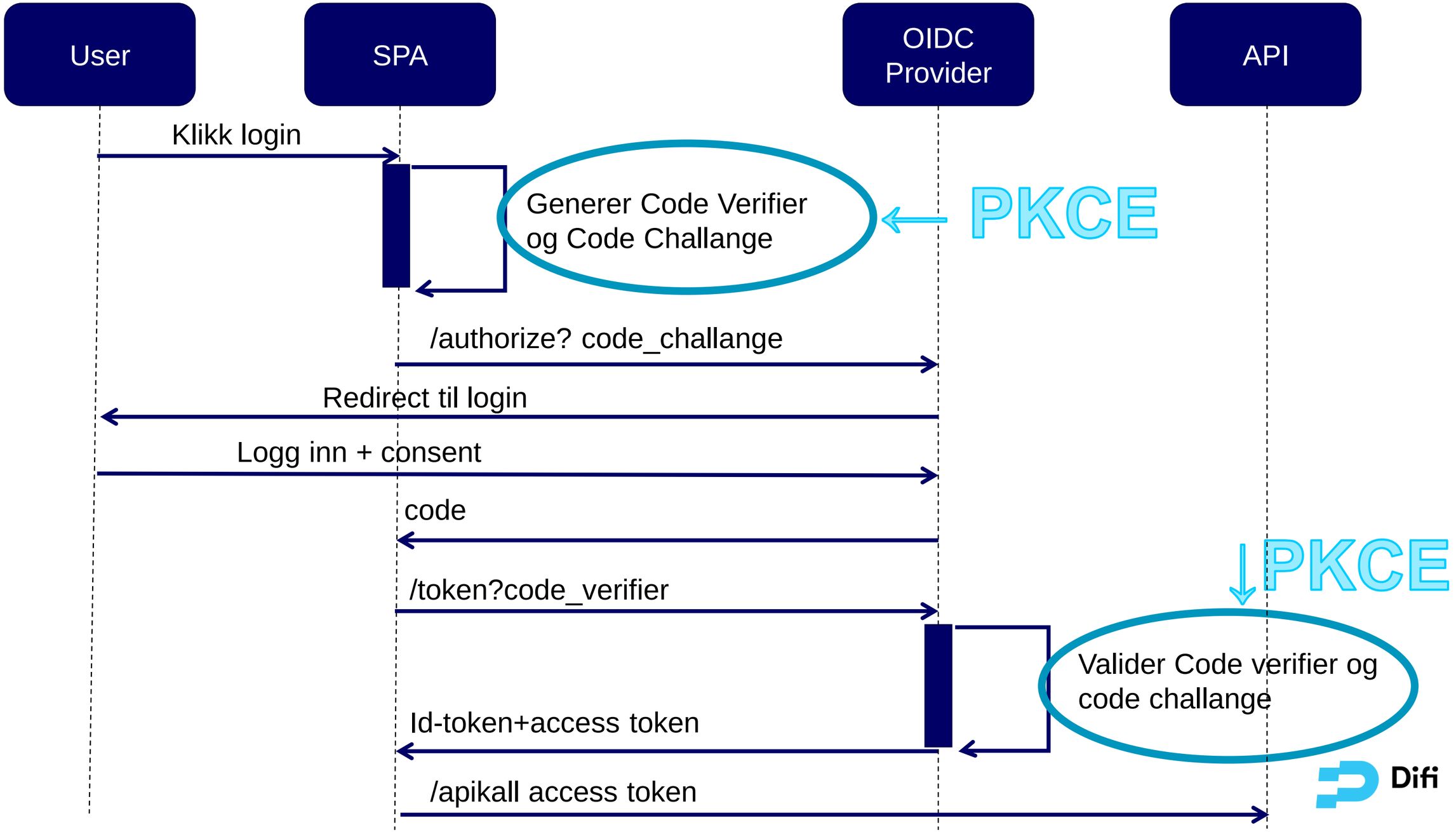
Demo: spek

1. Innlogging over ID-porten OIDC
2. Utlogging
3. Hente data frå API

https://github.com/difi/oidc-spa-example

Difi

Difi


User
SPA
OIDC Provider
API
Klikk login
Generer Code Verifier og Code Challange
PKCE
/authorize? code_challange
Redirect til login
Logg inn + consent
code
PKCE
/token?code_verifier
Valider Code verifier og code challange
Id-token+access token
/apikall access token
Difi

Bonus

Difi

Begrensninger i ID-porten på Logout

- Id-porten støttar berre front-channel-logout spek-en (impliserer redirect og må laste SPA på ny)
- Session managment spec beskrive 2 andre tilnærmingar til å håndtere logout
  - Regelmessig polling mot OIDC-provider med prompt=none (slient reauth)
  - Iframe
- Begge desse baserer på å synke brukar sin session mellom klient og OIDC Provider
- Dette støttes ikkje i ID-porten

Difi

Fragment i redirect URI

- Ugyldig ihht oAuth2 spek

http://somedomain.com/page#routing-strategies

Difi

Redirect tilbake til side inni din applikasjon

- For path type lenker:
  - bruke state-uri
  - ELLER
  - legge inn fleire redirectURIs i oidc client config
- Ditt val

Oppslagstjenesten over REST

- Tillet ikkje cross-orgin kall i dag

- Cross-Origin Read Blocking (CORB) blocked cross-origin response https://oidc-ver2.difi.no/kontaktinfo-oauth2-server/rest/v1/person with MIME type application/json. See https://www.chromestatus.com/feature/5629709824032768 for more details.

Lenker SPA og OIDC

- React SPA
  - https://github.com/facebook/create-react-app
  - https://github.com/IdentityModel/oidc-client-js/wiki

Difi

Kilder

- https://www.scottbrady91.com/OAuth/Cheat-Sheet-OAuth-for-Browser-Based-Applications
- https://blog.angular-university.io/why-a-single-page-application-what-are-the-benefits-what-is-a-spa/
- https://developer.okta.com/blog/2019/08/22/okta-authjs-pkce
- https://twitter.com/vibronet/status/1194553237556252672?s=09
- https://tools.ietf.org/html/draft-ietf-oauth-browser-based-apps-04

Difi