

# Dataporten

– sikker og enkel deling av data i UH-sektoren

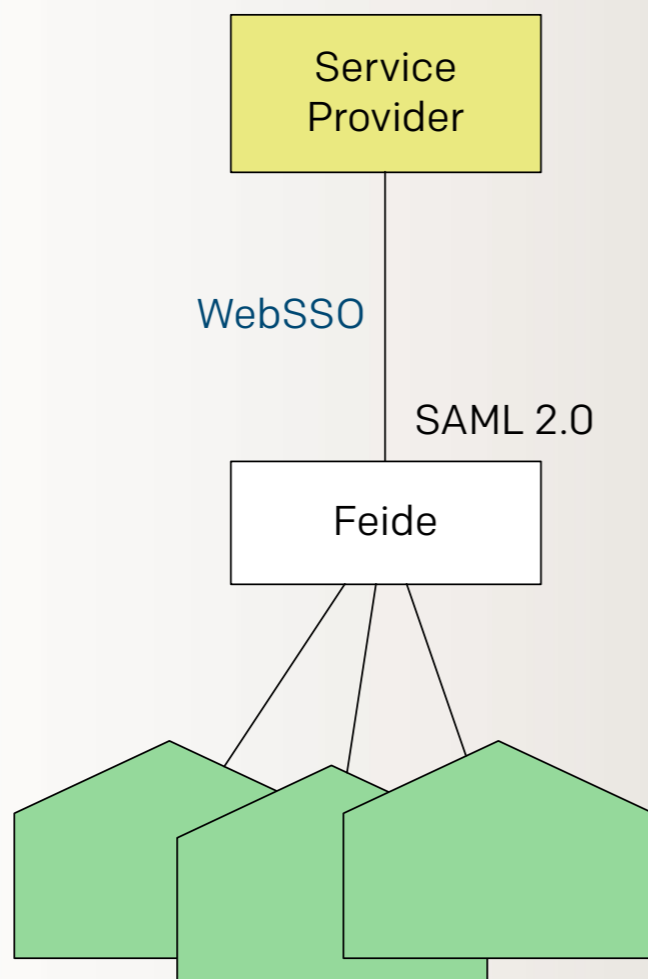
**IT-forum** Solstrand 4. mai 2016

Andreas Åkre Solberg  
[andreas.solberg@uninett.no](mailto:andreas.solberg@uninett.no)

**UNINETT**

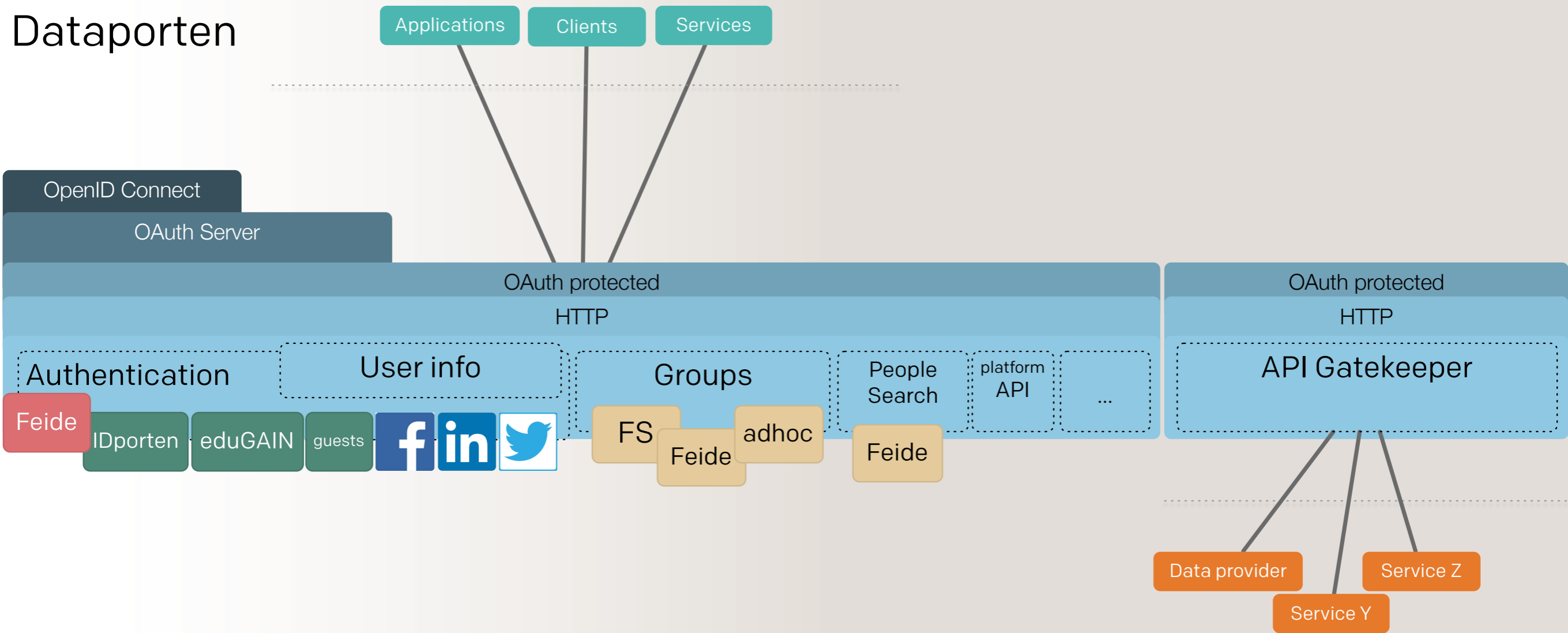


SAML 2.0 is specialized for Single Sign-On



- SAML 2.0: **KUN** autentisering + SSO
- Generelt behov for mer data. Spesielt grupper.
- Behov for tilgangsstyring til APler
- Vanskelig å tilfredstille nye behov med Feides tekniske rammer.
  
- Dataporten
  - Fokus på data. API-er og ikke kun WebSSO.
  - Ny teknologi.
  - Fleksibel og utvidbar.

# Dataporten



# Grensesnitt mot tjenester

Nytt, enklere grensesnitt

- Nytt teknisk grensesnitt mot Dataporten, versus Feide.
- Basert på **OAuth 2.0, OpenID Connect og HTTP API-er.**
- OpenID Connect / OAuth 2.0.
- Fra XML, XMLsig og X.509
- Til JSON, REST og JSON Web Token.
- OAuth 2.0 er en autorisasjonsprotokoll for utsteding av tokens som gir rettigheter til å benytte API-er.

# 100% selvbetjening

**UNINETT** Connect Dashboard Norsk bokmål Andreas Åkre Solberg

Personal UNINETT

### Applikasjoner

Registrer ny applikasjon

- Alumniportal2** Updated 7 days ago  
82f3684b-07f7-4da8-bd5e-9f6f8709ff8b  
blah blah
- Review LDAP group content** Updated 2 months ago  
01a2c2ea-a888-48d4-bb8f-1ed81dcde5b  
Administrative tool
- OpenID Connect Certification** Updated 2 months ago  
5ac8753f-8296-41bf-b985-59d89769005e
- Test Notebook** Updated 2 months ago  
bd4d2c74-238d-4431-b36d-3386d949db6e
- blah 1** Updated 2 months ago  
f4db0842-6611-4700-8def-dc8fb367748c  
sdf
- Studio FClient** Updated 3 months ago  
0b6f4f4c-5f4a-4249-aab6-c65c629a4846  
Andreas' testklient for eksperimentering og demo
- Public360 t**  
6ed0879a-4c79  
Andreas tester  
Dette skal kom

### API Gatekeepere


Registrer ny API Gatekeeper

- Preferanselager** Updated 7 days ago  
preferanse  
Muligheter for å lage preferanser.
- UNINETT Kalender** Updated 3 months ago  
calendar  
UNINETTs interne ansattkalender.
- Andreas sitt demo API kjører på vltord17** Updated 3 months ago  
demoapi2
- Eksamensresultater TEST (scope test)** Updated 3 months ago  
scopetestapi  
test av orgadmin scope policy

### Connect status for organization

- Ja Pilot – En eller flere kontaktpersoner har meldt seg fra institusjonen for deltagelse i piloten
- OK Databehandleravtale – signert og sendt UNINETT
- OK Autentisering – åpnet for i Feides kundeportal
- Konfigurert LDAP-oppsett – Connect settes opp for å kommunisere med organisasjonens Feide katalog  
Test results for each of the configured LDAP endpoints:
  - OK LDAP-endeppunkt ldap-tb-01.uninett.no:636
  - OK LDAP-endeppunkt ldap-bs-01.uninett.no
  - OK LDAP-endeppunkt ldap-bs-02.uninett.no[Re-run tests](#)
- OK Person søk – Connect tillates Feide katalog for brukersøk
- Ikke åpnet FS integrasjon – Connect tillates uttrekk av grupper fra institusjonens FS database.
- OK Geografisk posisjon registrert – Connect registrerer koordinater for en eller flere Campus for å gjøre det enklere å finne riktig institusjon.

**UNINETT**  
The registered realm is uninett.no.  
**Geo koordinater**  
63.415879, 10.395438



Registrert logo

**UNINETT** Connect Dashboard Norsk bokmål Andreas Åkre Solberg

Main overview [fc.org.uninett.no](#) / Client Foodle

### Basic info

Name: Foodle

Description for end-users: A simple poll and survey tool.

Redirect URI: The OAuth Redirect URI is the URL where the user is send back to after authentication and authorization.  
http://127.0.0.1:3001/   
https://beta.foodle.org/

Registered a year ago  16. Feb 2015 Updated 17 days ago  8. Jan 2016

[UNINETT Connect](#)  
For spørsmål [rapporter feil](#).



Google Search

I'm Feeling Lucky

Google.no offered in: [norsk](#)



A privacy reminder from Google

[REMIND ME LATER](#)

[REVIEW NOW](#)

Oppsett av mulige  
innloggingsmåter  
per tjeneste

Select your login provider

English

https://auth.dev.feideconnect.no/accountchooser?request=%7B"return"%3A"https%3A%5C%2F%5C%2F...

Apper UNINETT - Samskrive Groups - Feide Conn Groups - Feide Conn UNINETT Kalender Dashboard AuthNit

Bokmål Nynorsk English

# Velg hvordan du vil logge inn

For å logge inn på tjenesten **UNINETT Samskrive**, må du velge hvordan du vil logge inn.

Hvis nettleseren din får huske hvem du er får du opp en snarvei som bringer deg raskere til innloggingen neste gang.

Fjern krysset hvis du benytter en delt datamaskin.

Husk meg

Innloggingsvalg innen utdanning og forskning

Norge Søk etter navnet på din utdanningsinstitusjon...

Norway oppdater lokasjon hva er dette

- Høgskolen i Hedmark
- UNINETT
- NTNU
- Trondheim kommune
- Høgskolen i Oslo og Akershus
- Universitetet i Oslo

Innloggingsvalg for brukere utenfor utdanningssektoren.

- IDporten
- Twitter
- Facebook
- LinkedIn
- Feide gjestebukere
- FEIDE Feide testbrukere

UNINETT AS

Connect Dashboard Dokumentasjon Andreas Åkre Solberg

Personal UNINETT

## Mandatory applications

This organization has listed some mandatory clients, such as **UNINETT Kalenderoversikt**, **Foodle**, **Connect Groups**, **Connect Dashboard (pilot)**, and 2 more.

[Manage mandatory applications](#)

## Klienter

[Registrer ny klient](#)

- UNINETT Samskrive** Updated 2 minutes ago  
529229cc-2b41-4942-8ddb-568c37c6f8e9  
En etherpad installasjon koblet til UNINETT Connect.
- Developer Dashboard (dev)** Updated 3 days ago  
e8160a77-58f8-4006-8ee5-ab64d17a5b1e  
test2
- Min Feide Connect** Updated 3 months ago  
c148bc3f-6b15-47d7-ad23-3c36677eb8b5  
Inspiser brukerdata om deg selv, og trekk tilbake samtykke om registrerte applikasjoner.
- UNINETT Kalenderoversikt** Updated 3 months ago  
42b0c02e-0dda-4882-9da0-882a4b1abad6  
En enkel kalenderoversikt for UNINETT ansatte. Gir kun lesetilgang til kalenderene.
- Connect Groups** Updated 4 months ago  
65615472-f4af-4b9f-a966-28946c701609  
Users may review, create and manage their groups and memberships to groups.
- Connect Dashboard (pilot)** Updated 4 months ago  
a76c907f-1922-456c-a037-1b30af82c7be  
Connect Dashboard allows developers to register and manage their clients and API Gatekeepers. Site administrator may manage services for

## API Gatekeepere

[Registrer ny API Gatekeeper](#)

- Foodle** Updated 6 months ago  
A simple poll and survey tool

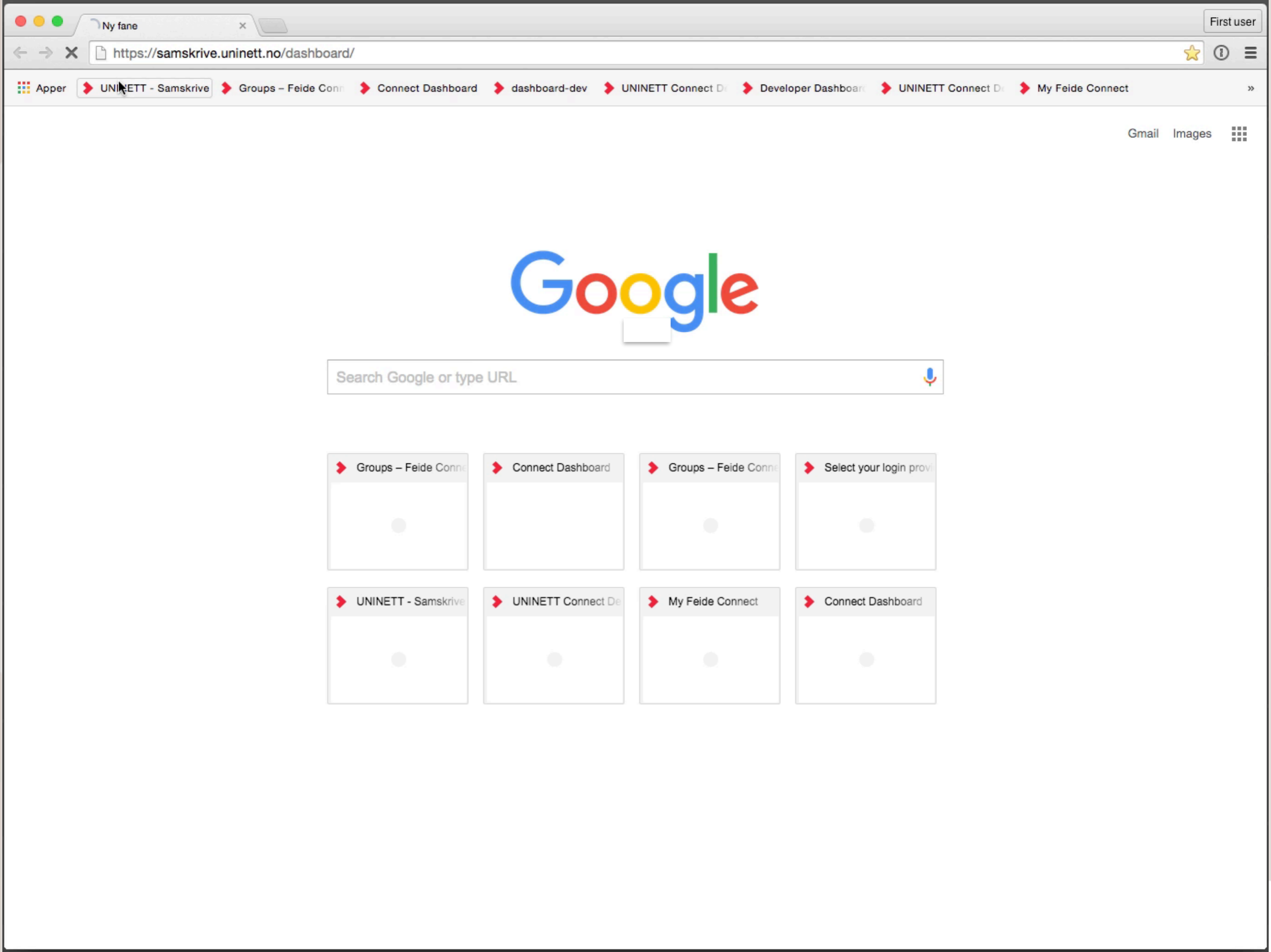


# eduGAIN

- Testet, ikke klart enda...
- Kobling til de fleste utdanningsinstitusjoner i Europa (høyere utdanning)
- Dataporten avlaster mye av kompleksiteten for tilkobling til eduGAIN.
  - SAML 2.0 metadata publisering og konsumering/aggregering
  - Attributtsemantikk
  - Åpne for nye tjenester...

# ID-porten

- Pålogging via IDporten via deres produksjonsløsning.
- Ikke enda koblet til kontaktregisteret (gir epost og mobil)
- Teknisk ganske greit. ID-porten benytter også SAML 2.0, samme som Feide.
- Må avklares rundt policy, betaling med mer..



Search Google or type URL

- Groups - Feide Connect
- Connect Dashboard
- Groups - Feide Connect
- Select your login provider
- UNINETT - Samskrive
- UNINETT Connect De
- My Feide Connect
- Connect Dashboard

# Gjestebrukere

- Facebook, LinkedIn, Twitter
- Egen løsning for selvregistrering av brukere

# Modell for juridisk grunnlag for utlevering av personlige data

- To hovedklasser:
  - Personlig samtykke og frivillig bruk. (ikke barneskole)
  - Obligatorisk bruk i undervisningen: databehandleravtale med mer.
  
- Disse to klassene bygges inn i Dataporten.

# Åpent for alle

Studenter kan også  
være tjenestetilbydere

**UNINETT Kalender**  
UNINETTs interne ansattkalender.

med følgende rettigheter

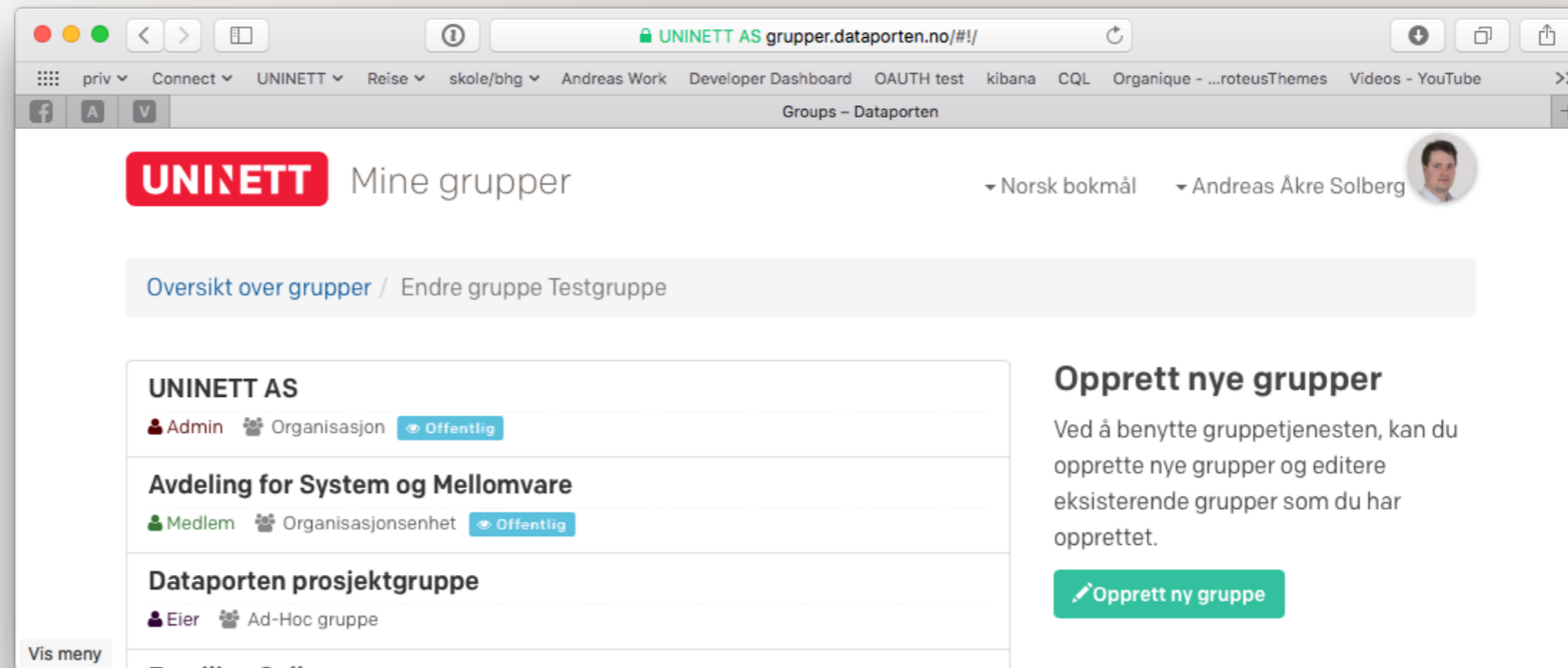
- Basic access – Basic access to this API.

Tredjepartstjenesten vil da få tilgang til

- Tilgang til informasjon om hvem du er
  - Bruker ID
  - Feide bruker-ID

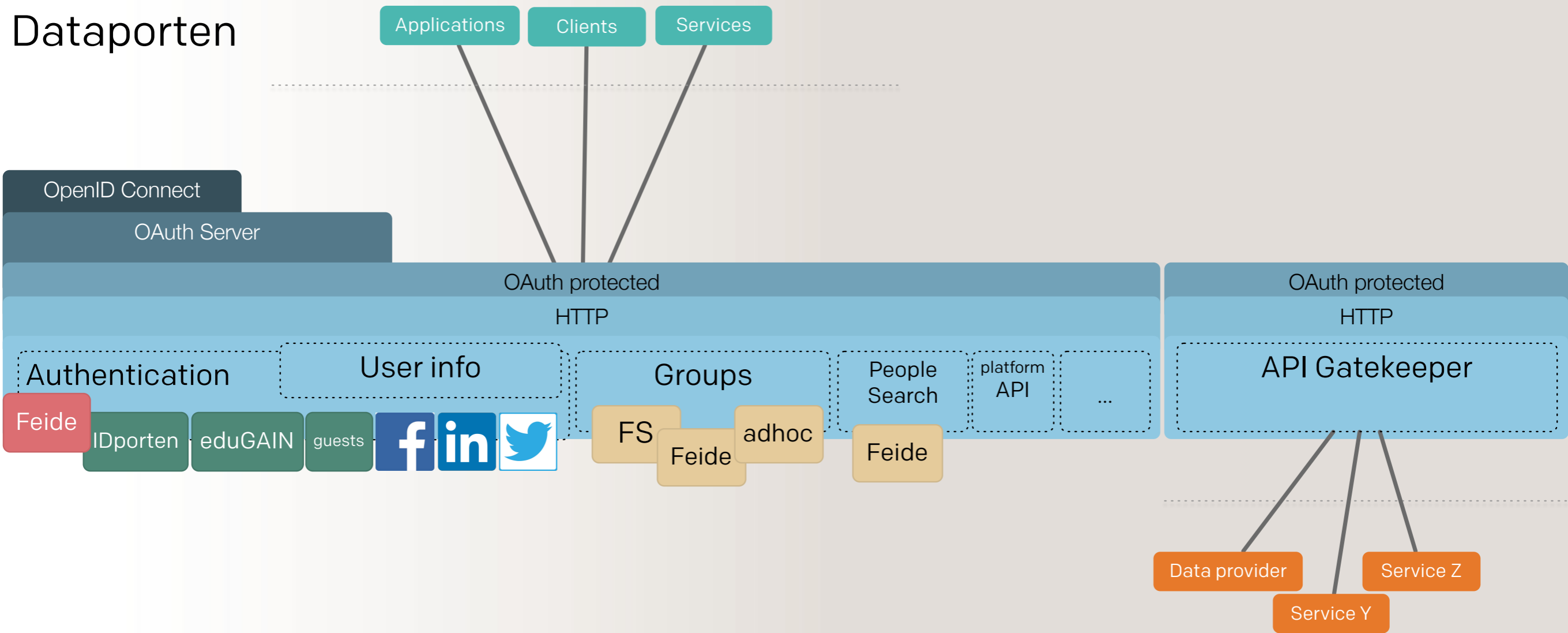
Denne tredjepartstjenesten leveres av  
**Andreas Åkre Solberg**  
andreas.solberg@uninett.no

# Grupper



- Gruppe API for tjenester.
- Enkel gruppemodell, abstraksjon.
- Organisatoriske grupper fra Feide (org og orgUnit)
- FS: kull, klasse studieprogram, studieretning og emne.
- Ad-hoc grupper
- Mulighet for kobling mot flere kilder i fremtiden.

# Dataporten





# Litt om API Gatekeeper

# OAuth 2.0 Access Token

- Når man får en access token, så kan denne benyttes mot både Connects interne APIer, men også mot tredjeparts APIer via API Gatekeeperen.
- En access token er knyttet til et sett av **scopes**. En liste av scopes kan for eksempel være: `userinfo, feide, email, gk_mediasite, gk_mediasite_admin`

# Klient

OAuth protected API requests that are sent to in example

<https://calendar.gk.feideconnect.no/foo/bar> , like this:

```
GET /foo/bar HTTP/1.1
Host: calendar.gk.feideconnect.no
Authorization: Bearer a005656a-8510-4d34-8897-f10638bb7b05
```

# API Gatekeeper

is forwarded to your API, <https://cal.uninett.no/foo/bar> , like this:

```
GET /foo/bar HTTP/1.1
Authorization: Basic XXXXXXXX
X_FEIDECONNECT_CLIENTID: 42b0c02e-0dda-4882-9da0-882a4b1abad6
X_FEIDECONNECT_USERID: 76a7a061-3c55-430d-8ee0-6f82ec42501f
X_FEIDECONNECT_USERID_SEC: feide:xxxx@uninett.no
```

# API Library



Langsiktig mål om et bredt tilbud av API-er som bidrar til å minimere integrasjonskostnadene ved oppbygging av nye tjenester  
– både sektorens egne tjenester og eventuelle kommersielle tredjeparts tjenester.

The screenshot shows the 'API Library' interface. At the top, there's a breadcrumb 'Main overview personal / Client OpenID Connect Certification'. Below that, there are tabs for 'Basic info', 'Accepted APIs', 'Requested APIs', 'My APIs', and '3rd party available APIs'. The '3rd party available APIs' tab is selected. A search bar is present with the placeholder text 'Search for an API'. To the right, there's a 'Filter APIs by provider' section with a 'Show all' button and buttons for 'UNINETT' and 'FSAT'. The main content area displays a list of APIs:

- Foodle Core API**: A simple poll and survey tool. Provider: UNINETT.
- UNINETT Kalender**: UNINETTs interne ansattkalender. Provider: Andreas Åkre Solberg.
- Det beste fra Simon's vitsekolleksjon!**: Tilbyr deg og dine en kolleksjon med over snitt morsomme vitser. Du kommer til å le helt til du stopper! Scopes kategoriserer og tilgangsstyrer iht. aldersgrense. Aldersgrenser for vitser er lånt fra medietilsynets aldersgrenser for kino: <http://www.medietilsynet.no/barn-og-medier/aldersgrenser/>. Provider: Simon Skrødal.
- Test-grensesnitt for FS Alumni**: Bruk GET <url>/data for å hente ut alumnidata. Dersom du logger på med ID-porten må du i tillegg sende med institusjonsnr som et Query-parameter. Institusjonsnr er et kjent tall ved institusjonen som har alumnisystemet. Provider: Richard Edvin Borge.
- Accesspoint til preferanselager for foresatte.** Provider: Aleksander Hougen.

# Åpne data

- Data hos utdanningsinstitusjoner bør deles by default.
- Viktig for fremtidig verdiskaping.
- Ikke vent på forespørsler eller konkrete behov!
- Kan også brukes internt!
- Mye enklere å håndtere datasett som ikke behøver aksesskontroll.

The screenshot shows the DATA.NORGE.NO website. The header includes the 'difi' logo and the text 'DATA.NORGE.NO Åpne offentlige data i Norge'. A search bar is located in the top right corner. The main navigation menu contains links for 'Datasett', 'Apper og tjenester', 'Veiledning', 'Lisens', 'Datahotellet', and 'API'. The current page is titled 'Hjem » Veileder i tilgjengeliggjøring av offentlige data » Hvorfor åpne data'. The content is divided into two columns. The left column is titled 'Veileder i tilgjengeliggjøring av offentlige data' and contains a numbered list of topics: 1. Hva er åpne data? (with sub-points 1.1 Norsk lisens for offentlige data (NLOD), 1.2 Hvilke data kan jeg åpne?, 1.3 Hvilke data skal jeg ikke åpne?, 1.4 Trafikklyssystemet, 1.5 Usikkerhet rundt åpning av data), and 2. Hvorfor skal man dele data? (with sub-points 2.1 Næringsutvikling og verdiskaping, 2.2 Effektivisering og innovasjon i offentlig sektor). The right column is titled 'Veileder i tilgjengeliggjøring av offentlige data' and contains the text 'Hvorfor skal man dele data?' followed by a paragraph explaining that many public organizations collect a wide range of data to perform their tasks, and that this information is a valuable resource. It also mentions that it is difficult to predict exactly how and where value will be created. At the bottom of the right column, there is a button labeled '< Forrige'.

Institusjoner



Data



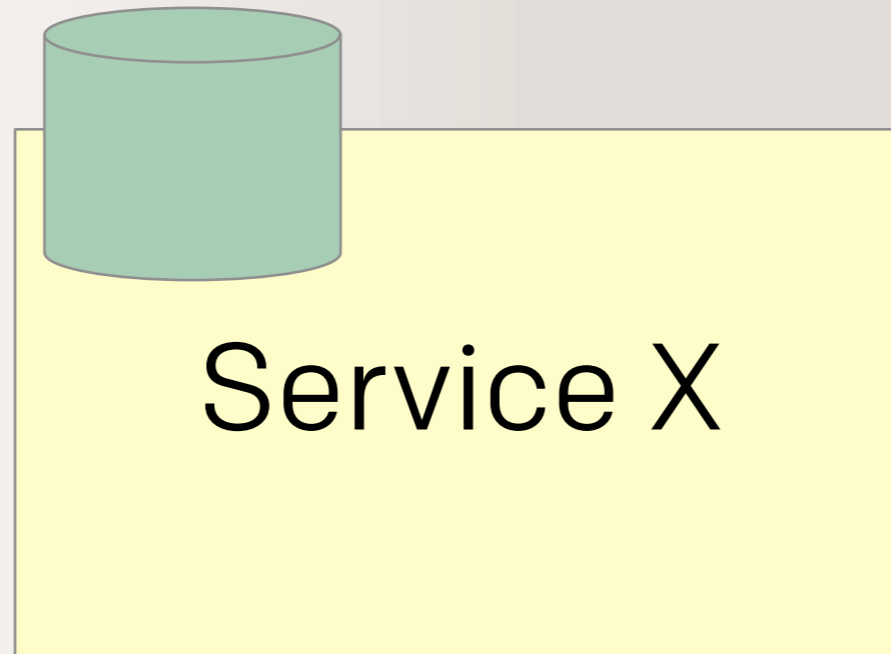
Datatilgang

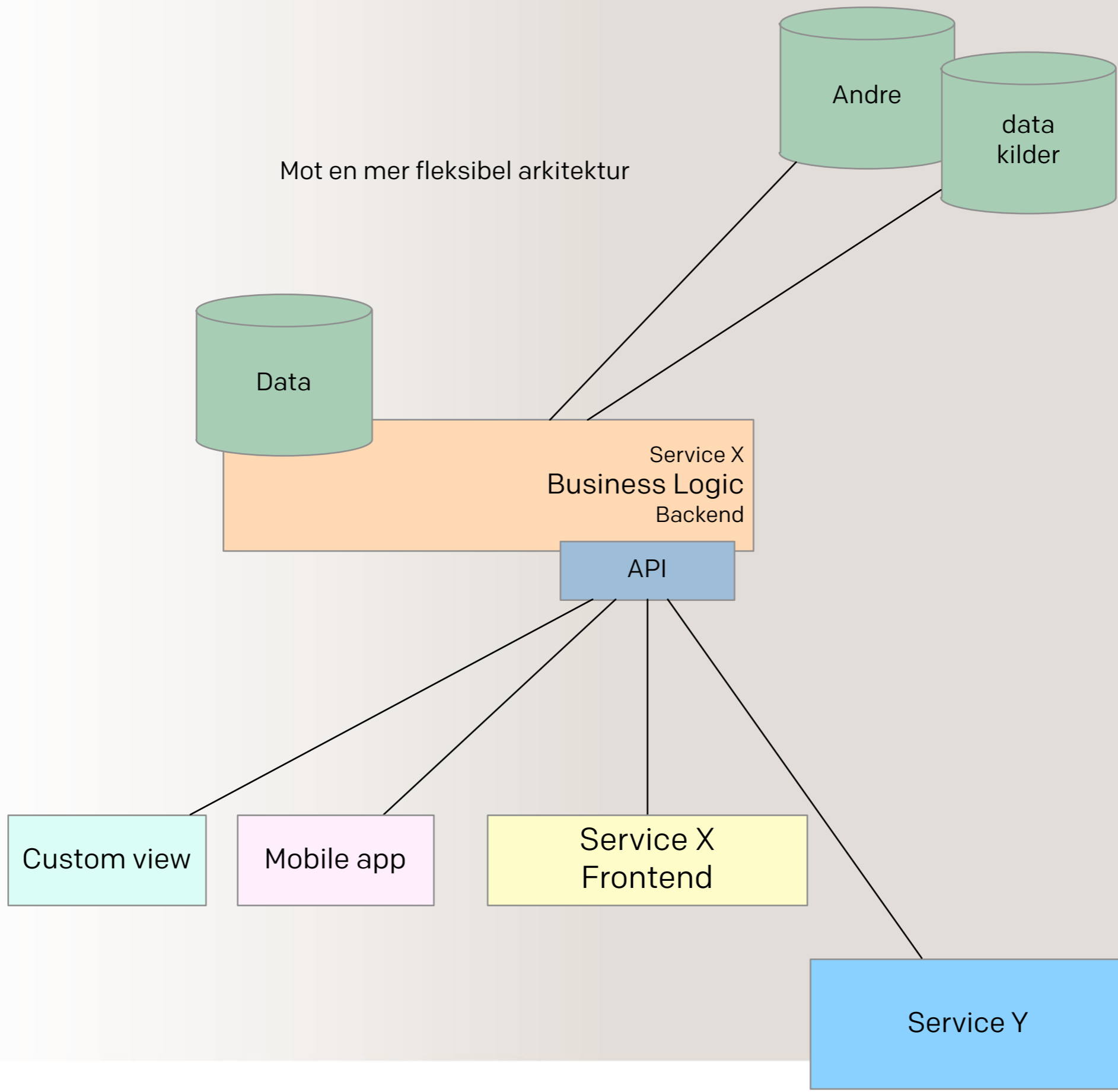


- › Harmonisering av datamodeller
- › Fremstå enhetlig
- › Samme fremgangsmåte for alle både for teknisk og administrativ tilgang
- › 100% Selvbetjening

Tjenesteleverandør

Fra en enkel og fastlåst  
tjenestearkitektur





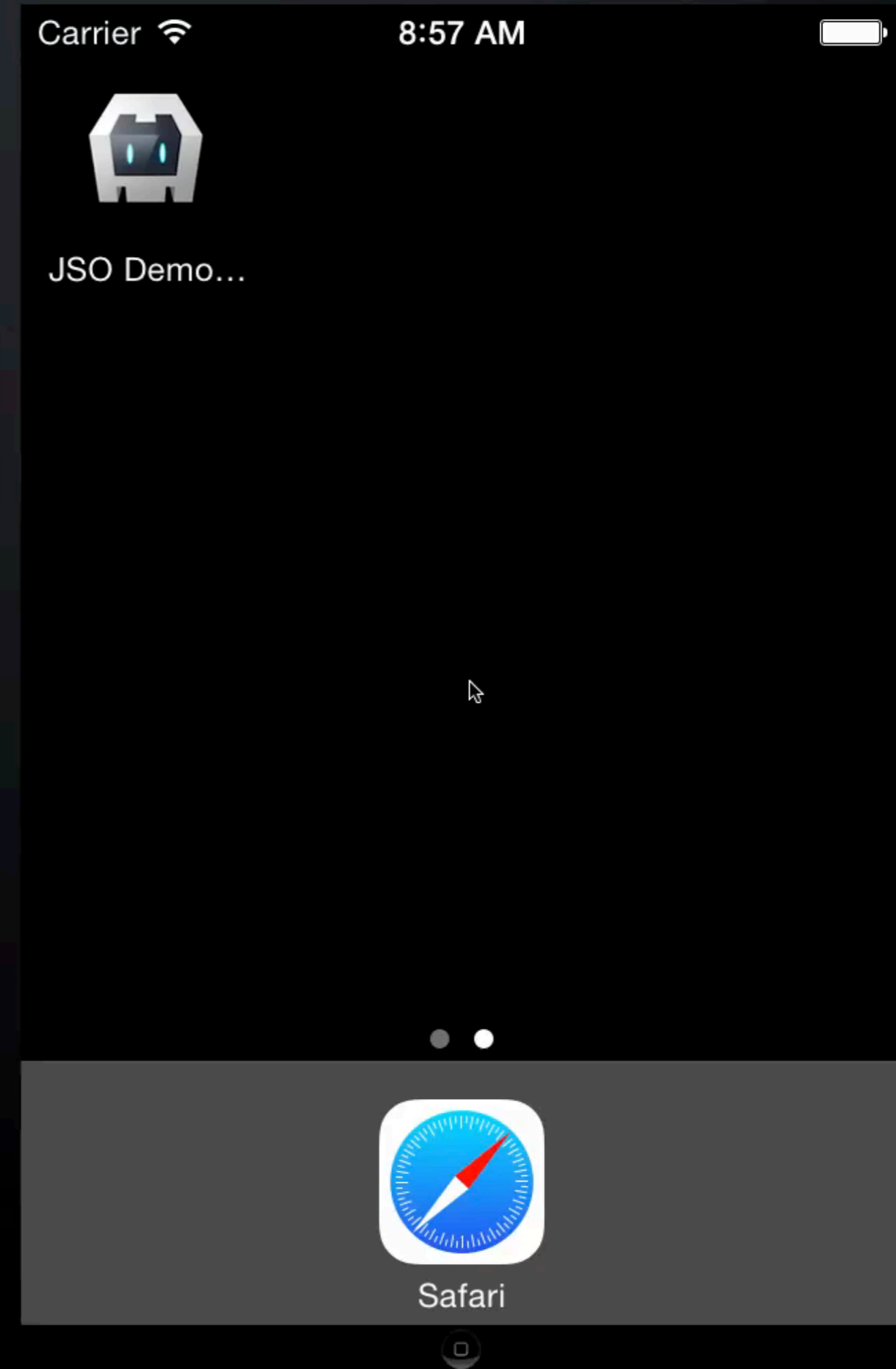


Sesjonsvarighet  
8 timer eller 2 år

## OAuth gir mulighet for innlogging via mobil.

- › In-app browser vs.
- › System browser +  
custom url scheme

**UNINETT**



for sluttbrukeren

## ➤ Valg av organisasjon

➤ erstatter Feides valg av org.

➤ inkrementell søk

➤ sortering etter avstand. logoer og koordinater.

➤ Legger også til alternative påloggingsvalg: sosiale nett og IDporten.

➤ Introduserer internasjonal pålogging med selektor for land.

➤ Vises **veldig skjelden**. Kun første gang per bruker per maskin/nettleser

## Velg hvordan du vil logge inn



For å logge inn på tjenesten **UNINETT Kalenderoversikt**, må du velge hvordan du vil logge inn.

Innloggingsvalg innen utdanning og forskning

Norge

📍 63.425, 10.449

	NTNU
	Trondheim kommune
	UNINETT
	Høgskolen i Hedmark
	Akershus fylkeskommune
	Høgskolen i Oslo og Akershus
	Universitetet i Oslo
	Fjellhaug Internasjonale Høgskole
	Senter for IKT i utdanningen

Hvis nettleseren din får huske hvem du er får du opp en snarvei som bringer deg raskere til innloggingen neste gang.

Fjern kryssset hvis du benytter en delt datamaskin.

Husk meg

Innloggingsvalg for brukere utenfor utdanningssektoren.

IDporten

Twitter

Facebook

LinkedIn

Feide gjestebukere

Feide testbrukere

## ➤ Kontovelger


➤ *innfører click-through for SSO*



➤ *oppmerksomhet rundt hvilken rolle man logger inn på tjenesten som.*

➤ *I fremtiden kan dette representere rollevalg.*

➤ *En variant av det å huske hvilken institusjon man valgte å logge inn med forrige gang, og samtidig holder åpent muligheten for å velge annerledes denne gangen.*

### Velg hvilken brukerkonto du vil logge inn med

 For å logge inn på tjenesten **UNINETT Kalenderoversikt**, må du velge hvordan du vil logge inn.


	<b>Andreas Åkre Solberg</b> UNINETT feide.andreas@uninett.no	<input checked="" type="radio"/> ➤
	<b>Andreas Åkre Solberg</b> Twitter twitter:6405972	➤

[✕ fjern snarveier](#)


eller velg en annen brukerkonto

➤ Samtykke


➤ Erstatte Feides info om overføring av attributter.

 **Andreas Åkre Solberg** Mine tjenester <  
Logg ut <

Tjenesten


 **UNINETT Kalenderoversikt** ▼  
En enkel kalenderoversikt for UNINETT ansatte. Gir kun lesetilgang til kalenderene.





Denne tjenesten leveres av


**UNINETT** 

cal.uninett.no


etterspør følgende rettigheter på vegne av deg:

 Tilgang til informasjon om hvem du er ▼




 Bruker ID  Navn  Feide bruker-ID  Profilbilde

 Langvarig tilgang ◀

I tillegg etterspør tjenesten følgende rettigheter til tredjeparts tjenester på vegne av deg:

 **UNINETT Kalender** ◀

✓ Basic access

 Tilgang til informasjon om hvem du er  Bruker ID  Feide bruker-ID

**?** Din organisasjon har ingen avtale med tjenestertilbyderen, og har ikke akseptert bruken av tjenesten på vegne av sine brukere. Du kan fortsatt velge å benytte tjenesten på eget initiativ.

Godtar du dette?

# Personlige brukeridentifikatorer for utdanningssektoren







status.dataporten.no

**UNINETT** Dataporten Docs Status Om Dataporten

## Status

Dataporten er tilgjengelig for tjenesteleverandører allerede nå. Feide vertsjansjoner kan ta kontakt for å koble seg til. Her følger en status for tilkobling av vertsjansjoner

### Tilsluttede vertsjansjoner

	UNINETT	Avtale	Feide	LDAP	Personsök	FS	Geo
	Det teologiske Menighetsfakultet	Avtale	Feide	LDAP	Personsök	FS	Geo
	Høgskolen i Østfold	Avtale	Feide	LDAP	Personsök	FS	Geo
	Universitetet i Oslo	Avtale	Feide	LDAP	Personsök	FS	Geo
	Dronning Mauds Minne Høgskole	Avtale	Feide	LDAP	Personsök	FS	Geo
	Universitetet i Bergen	Avtale	Feide	LDAP	Personsök	FS	Geo

# behind the scene

- CI - jenkins
- Absolutt all funksjonalitet eksponert via APIer, også interne
- Auth engine, core apis, group engine.
- Frontends SPA/javascript web apps som benytter APIene direkte.
- Docker
- Cassandra database cluster
- Logging, logstash elasticsearch kibana



# Dataporten

