Digdir

digdir.no

Distribuert datadeling med revidert eIDAS-forordning

Hallvard Bjørdalsbakke og Jørgen Binningsbø, ID-porten

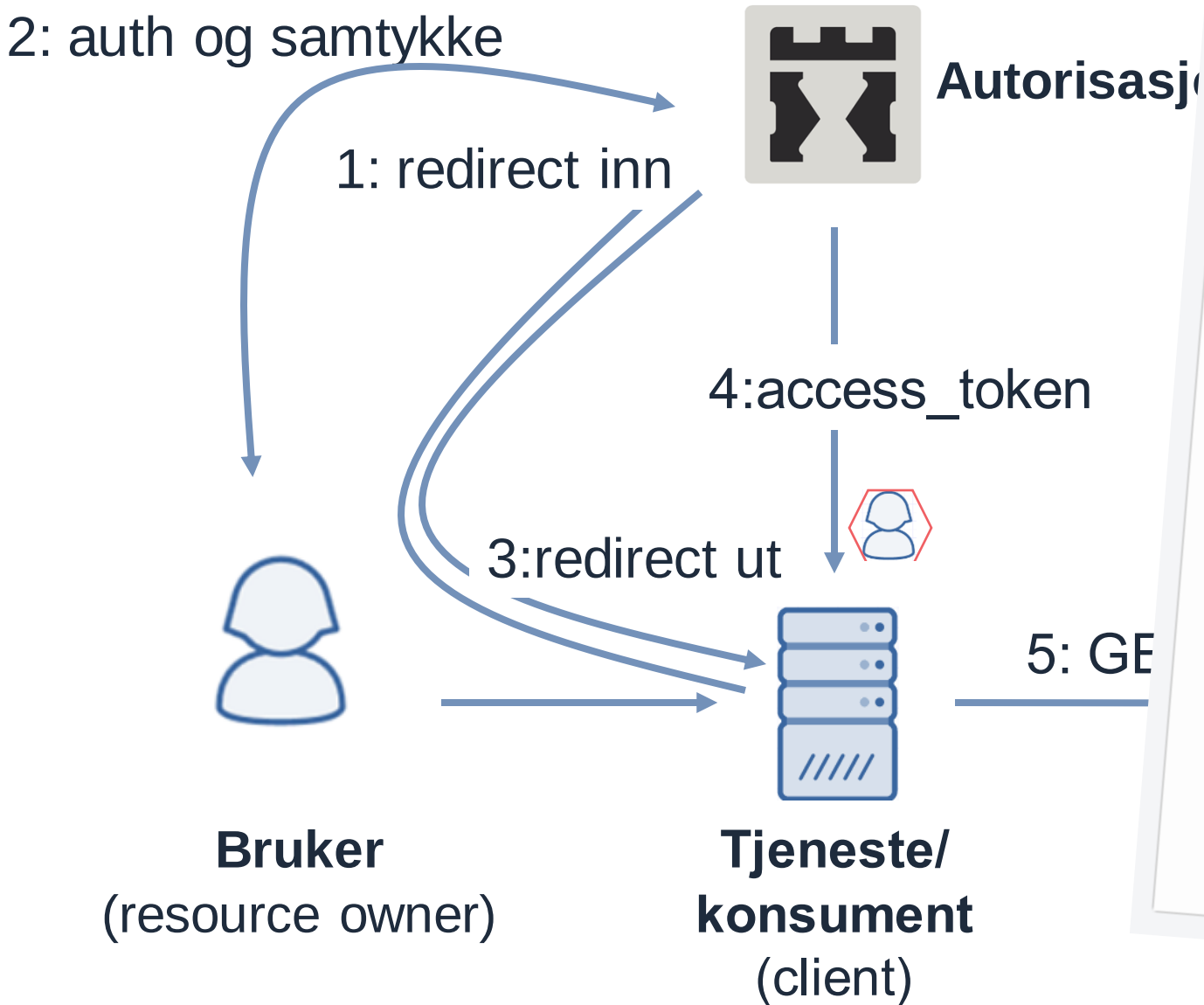
2021-10-20

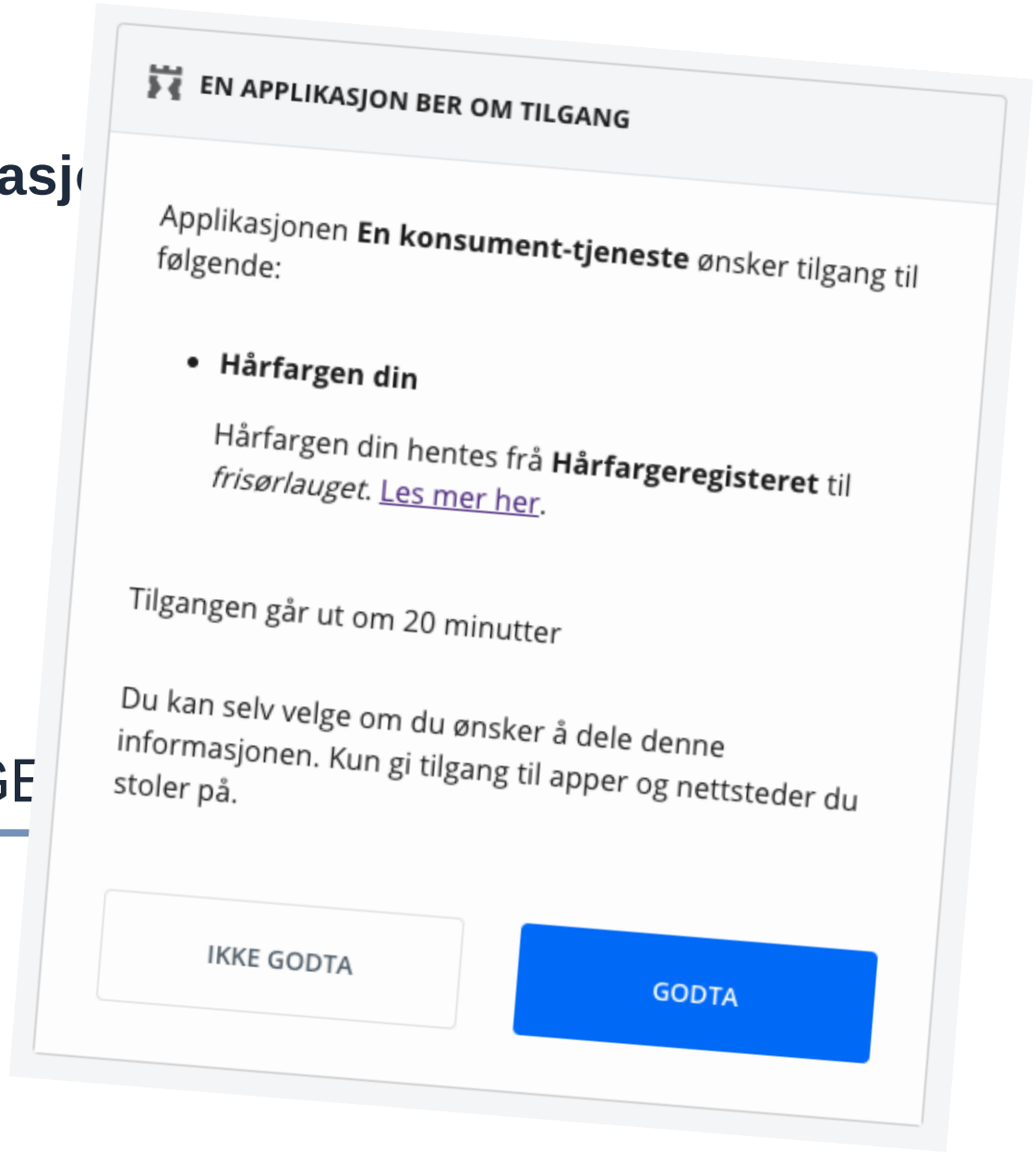
Innhald

- Lynkurs i tradisjonell datadeling med oauth2 i ID-porten
- SSI – kva er det?
- Sommarcamp 2021
- Revisjon av eIDAS-forordninga


Over 18
Er lege
Har forerkort type B

Klassisk Oauth2 – grunnflyt og aktører



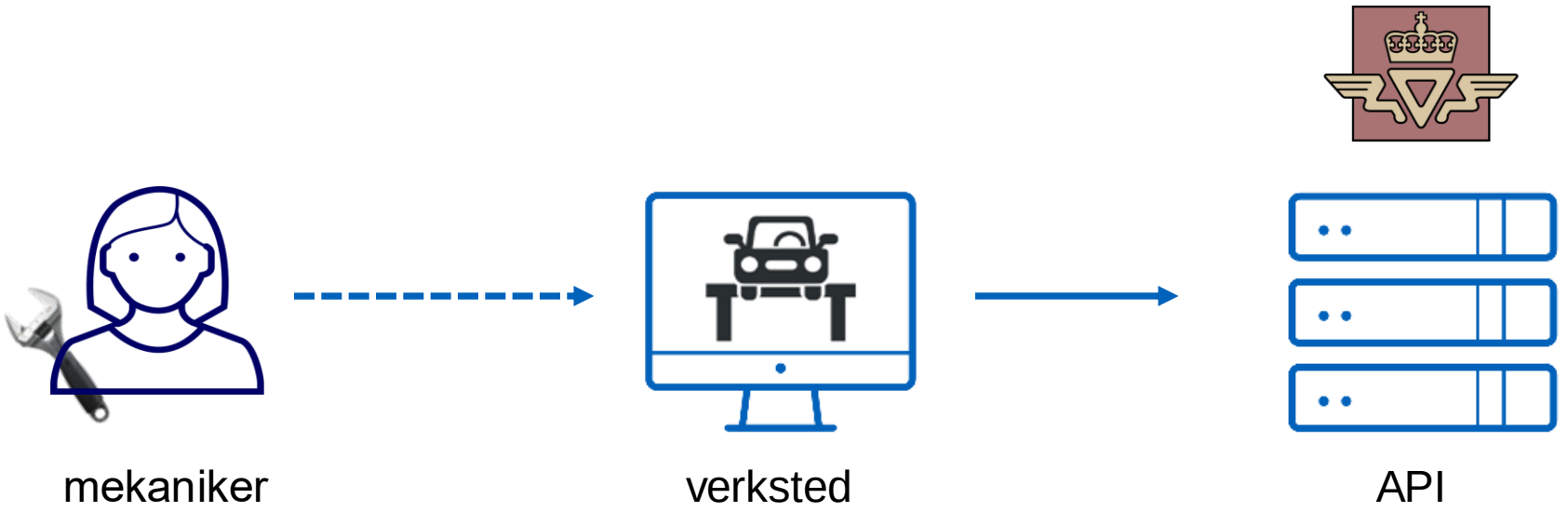


3 eksempler

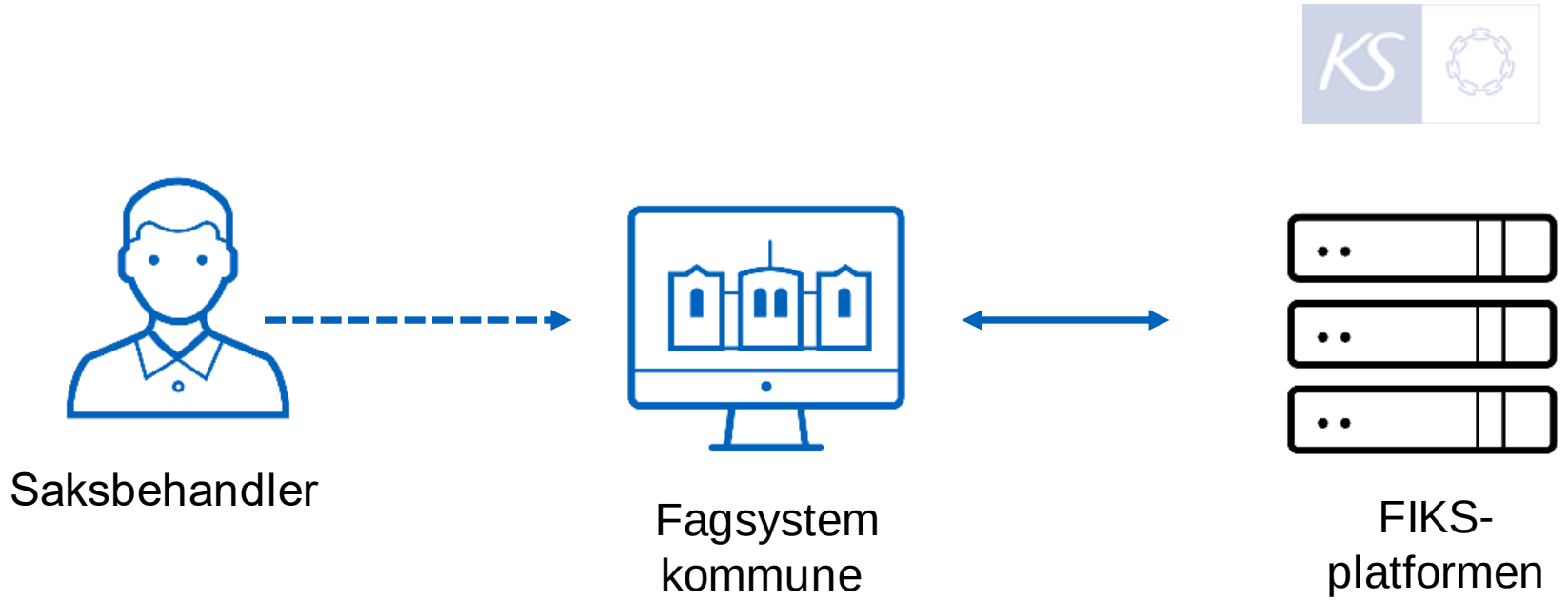
1: Søknad om sosialytelse

- bruker henter selv sine data og forhåndsutfyller

Innrapportering av periodisk kjøretøykontroll



Fagsystemer i kommunene



Fordeler med brukerstyrt datadeling

- Sluttbruker har kontroll på deling av sine data
- Datakilde slipper å eksponere hele datasettet sitt
- Andre kan integrere dine tjenester i sine løsninger

Ulemper

- Autorisasjonsserver blir eit single-point-of-failure
- Autorisasjonsserver har full oversikt over innbyggers datadeling
- Skalering/integrasjonsbehov når mange tilbyr samme API
- Fungerer ikkje offline

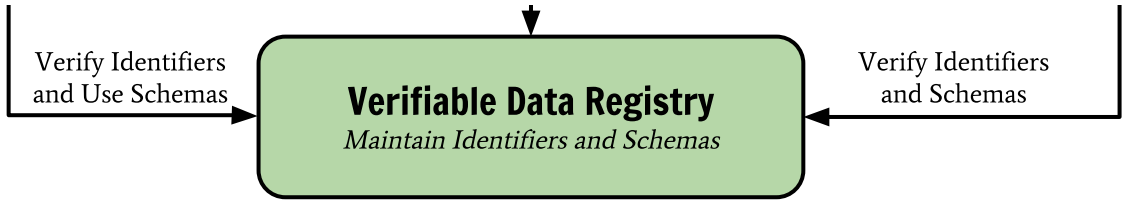
SSI –
self sovereign identity

Prinsipper for SSI

- **Existence.** *Users must have an independent existence.*
- **Control.** *Users must control their identities.*
- **Access.** *Users must have access to their own data.*
- **Transparency**. *Systems and algorithms must be transparent.*
- **Persistence.** *Identities must be long-lived.*
- **Portability.** *Information and services about identity must be transportable.*
- **Interoperability.** *Identities should be as widely usable as possible.*
- **Consent.** *Users must agree to the use of their identity.*
- **Minimalization.** *Disclosure of claims must be minimized.*
- **Protection.** *The rights of users must be protected.*

https://twitter.com/ChristopherA/status/1386715286913486857

SSI økosystemet



Aktører i SSI-økosystemet

- **En bruker (holder)** kontrollerer sin identitet gjennom en form for digital lommebok, der man oppbevarer opplysninger i form av bevis, og styrer hvem man ønsker at denne informasjonen deles med.
- **En utsteder (issuer)** oppretter bevis tilknyttet en identitet og sender denne til brukerens digitale lommebok
- **En tjeneste (verifier)** er de som mottar og verifiserer bevis fra brukere.
- **Tillitsrammeverket (verifiable data registry)** er et oppslagsverk der informasjon for å kommunisere og verifisere bevis er tilgjengelig.

Aktuelle standarder

- **Verifiable Credentials Data Model (VC),**
  a standard way to express credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable.
  https://www.w3.org/TR/vc-data-model/

- **Decentralized identifiers (DID),**
  DIDs are a new type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) https://www.w3.org/TR/did-core/

  ```
  did:example:123456789abcdefghi
  ```

Døme på VC for studiebevis

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": {
    "id": "did:example:76e12ec712ebc6f1c221ebfeb1f",
    "name": "Example University"
  },
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "proof": { ... }
}
```

Behov for mye informasjonsforvaltning....

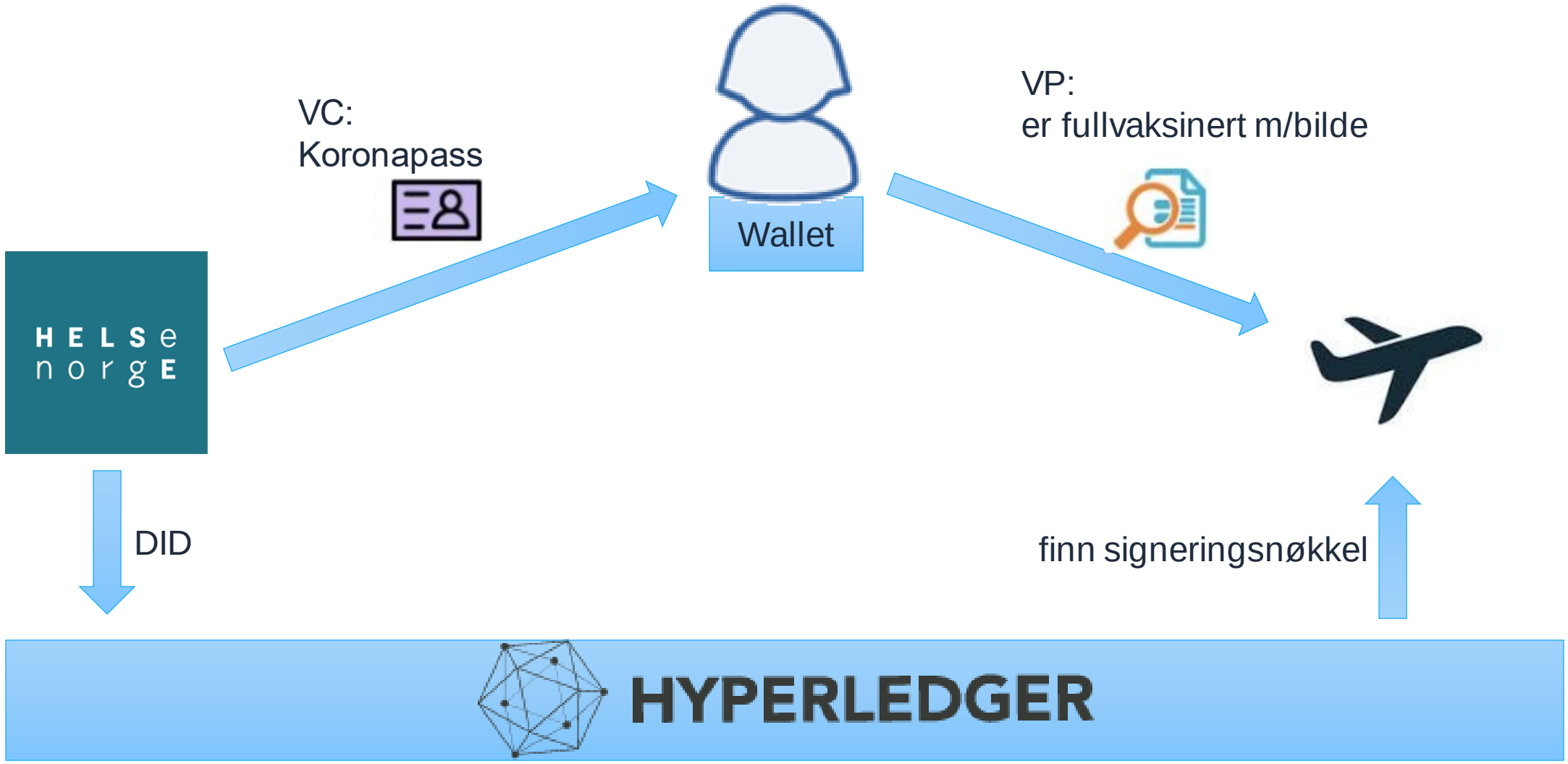
- Hvordan ser et gyldig bevis av gitt type ut ?
- Hvordan vet tjenesten hvem utsteder er ?
- Hvordan vet tjenesten at en utsteder faktisk har lov til å utstede slike bevis?

VC er berre ein datamodell – korleis overføre bevisa?

- Scanne QR-koder med lommeboka
- Lommeboka kan blir ein mini-OIDC-server
- W3C arbeider med "DIDcomm"
- Traversere lenka data dersom VC er i JSON-LD representasjon
- Brukers DID vil peike på ein DID-metode som kanskje hjelper med transport

https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf

Mulig døme: koronopass



Digdircamp 2021

Dette er DigdirCamp

Rekruttering

- Korleis konkurrere mot dei store konsulenthusa om dei kloke utviklarhovuda?

Omdømme

- Korleis synleggjera at det eksisterer kompetansearbeidsplassar i distriktet?

Innovasjon

- Kva skjer om vi lar våre eigne utviklarar få frie tøylar til å løyse ei utfordring?

Årets oppgåve til DigdirCamp

- Formål
  - Utforske SSI og dele erfaringar med Digdir
  - Finne ut kva Digdir si rolle i SSI-økosystemet kan vere

Anbefalingar

- **Lommebok**
  - Studentane anbefalar at istadenfor at Digdir skal utvikle ei lommebok sjølv, burde vi la private aktøra i marknaden gjere det.
- **Informasjonstilbyder**
  - Anbefalinga er at Digdir bør ta oppgåva som informasjonstilbyder. Vi sit på ein del informasjon om brukaren, og er dei som har moglegheit til å utstede grunnidentitet gjennom ID-porten.

Demo

Revisjon av eIDAS-fordningen

Om eIDAS

- Påbegynt 2006-ish, beslutta 2014, tatt inn i norsk rett 2018 som *Lov om elektroniske tillitstjenester* , består av 2 deler:
  - Tillitstjenester (sertifikater mm..)
  - Gjensidig anerkjennelse av eID på tvers av landegrenser

- Evaluering 2021: minimal bruk av tverrgående eID

=> Behov for revisjon av forordningen

DIGITAL LOMMEBOK

EU planlegger felles digital lommebok for ID, betaling og passord

Avhenger av samordning på tvers av medlemslandene.

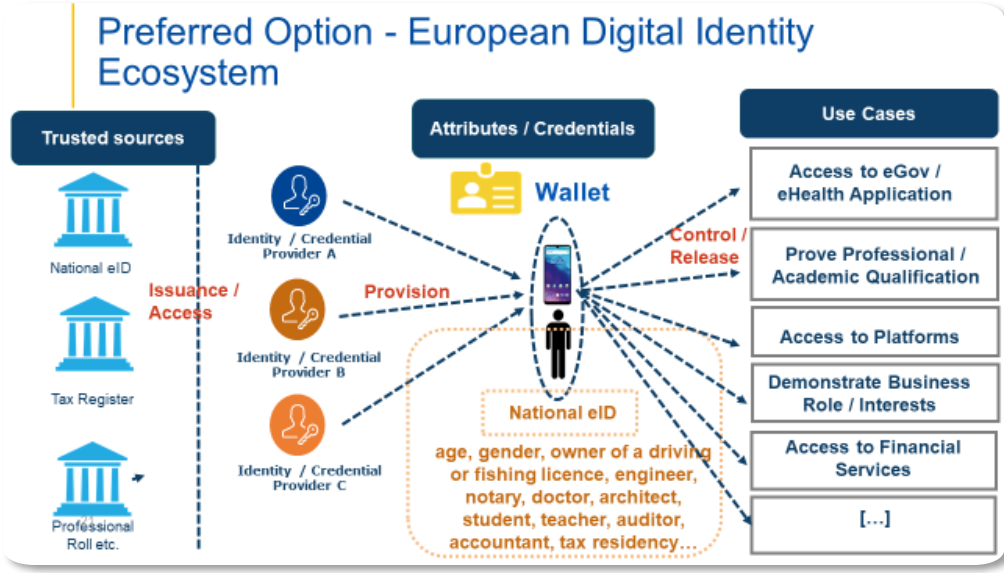
HARALD BROMBACH DIGITAL LOMMEBOK 1. JUNI 2021 - 17:00

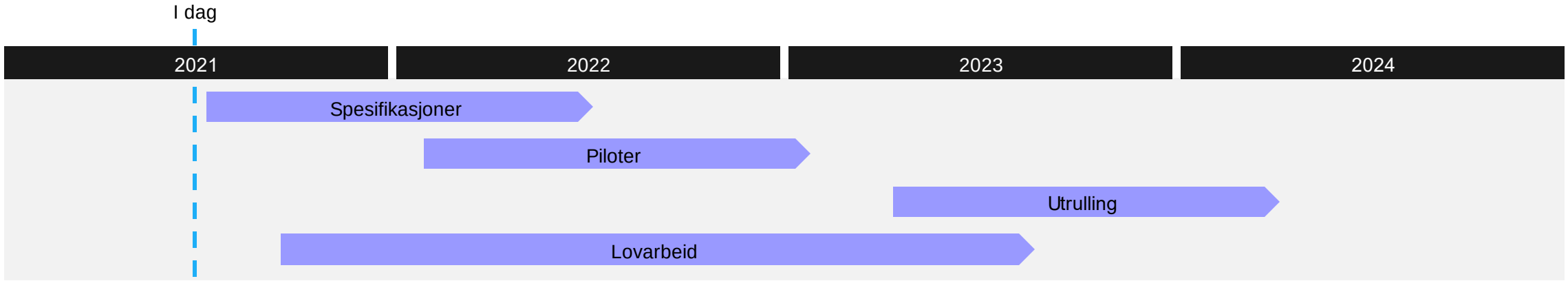
EU skal onsdag denne uken legge fram planer om en digital lommebok for som skal gi innbyggerne i EU-landene, og trolig også EØS-land som Norge, enklere tilgang til både offentlige og private tjenester som tilbys i landene.

Dette forteller ikke navngitte personer med kjennskap til planene til Financial Times (for abonnenter), som siteres av blant annet

Nye rammebetingelser – eIDAS 2.0

- Harmonisert løsning i alle land
- Harmonisert forretningsmodell
- En digital lommebok-app på telefonen
- Inneholder attesterte attributter
- Tvungen aksept i de fleste sektorer, også bank-finans
- Store plattformer som Amazon, Google, Facebook må akseptere





Mogelege attesterte atributt

- Førerkort
- Pass
- Nasjonalt ID-kort
- Styringsmiddel for IoT
- Adgangskort til jobb eller skole
- Bibliotekkort
- Digitale sentralbankpenger

Er eIDAS 2.0 = SSI ?

- Tvilsomt
- Trolig gjenbruk av mye SSI-prinsipper og standarder
- EU vil kreve sertifisering/fagfellevurdering av løsninger
  - får ikke komme med “din egen lommebok”
- Utstedelse av grunnidentitet tilsvarende nivå “høyt”
  - så du kan ikke være anonym, men du kan trolig hvelge hvor mye identitetsinformajon du vil dele
- Uavklart hva som skal være tillitsrammeverk

Konsekvenser for ID-porten

- Antatt sentral rolle for utstedelse
  - Utstede **grunn-identitet** (≈ eid)
  - **Bistå** andre etater med å utstede bevis
  - MinID kan få en rolle som offentlig basis-lommebok
- «Proxy»-funksjonalitet for gradvis innføring
  - Kunne bruke lommebøker som innloggingsmekanisme til eksisterende tjenester
- Slipper å være en single-point-of-failure (på lang sikt)

Konsekvenser for data-tilbydere

- Trolig ikke SÅ stor forskjell på å utlevere data som et VC-bevis som å tilby samme dataene over et API.
- Arbeid med datamodeller/skjema blir (minst) like viktig som før
  - vanskeligere å deprecate et bevis-skjema enn å versjonere et API ?
  - uklart om tilbyder må bestemme Verifiable Presentations forhånd – zero-knowledge proof er “tungt”
- Blir tvinga til å ta stilling til levetid på bevis
- Vet ikke hvem som mottar data (utover brukeren)

Konsekvenser for data-konsumenter

- Slipper å etablere integrasjoner for datadeling mellom virksomheter
- Kan bruke data uten at det blir spora
  - t.d. lommebok til oppfølging av psykisk sykdom
- Risikerer å måtte håndtere (mange?) nye tillitsrammeverk for å vite om en kan stole på et bevis;
- Måtte håndtere flere versjoner/skjema av samme bevis?

Konsekvenser for brukeren

- Betre personvern: får meir kontroll med deling av sine data
- Blir «postbud» for offentlig sektor
- Må innstallere ein app
- Mer komplekst for svake brukere ?

Vegen vidare...

Ingen revolusjon på kort sikt...

- Veldig spennande, kan vere “rett verktøy” for ein del use case !
  - Tradisjonell datadeling vil leve lenge

- ID-porten vil følge “EU-sporet”
  - Plan om lansering 2024 er ambisiøst
  - Interessert i dialog om samarbeidsprosjekt for pilotering gode use case