Helsedirektoratet

Claims based identity and access control – sikker ”tilgang på tvers”

Eirik Mangseth,
Seniorrådgiver,
Avdeling eHelse,
Helsedirektoratet

Helsedirektoratet

1. Begreper

Helsedirektoratet

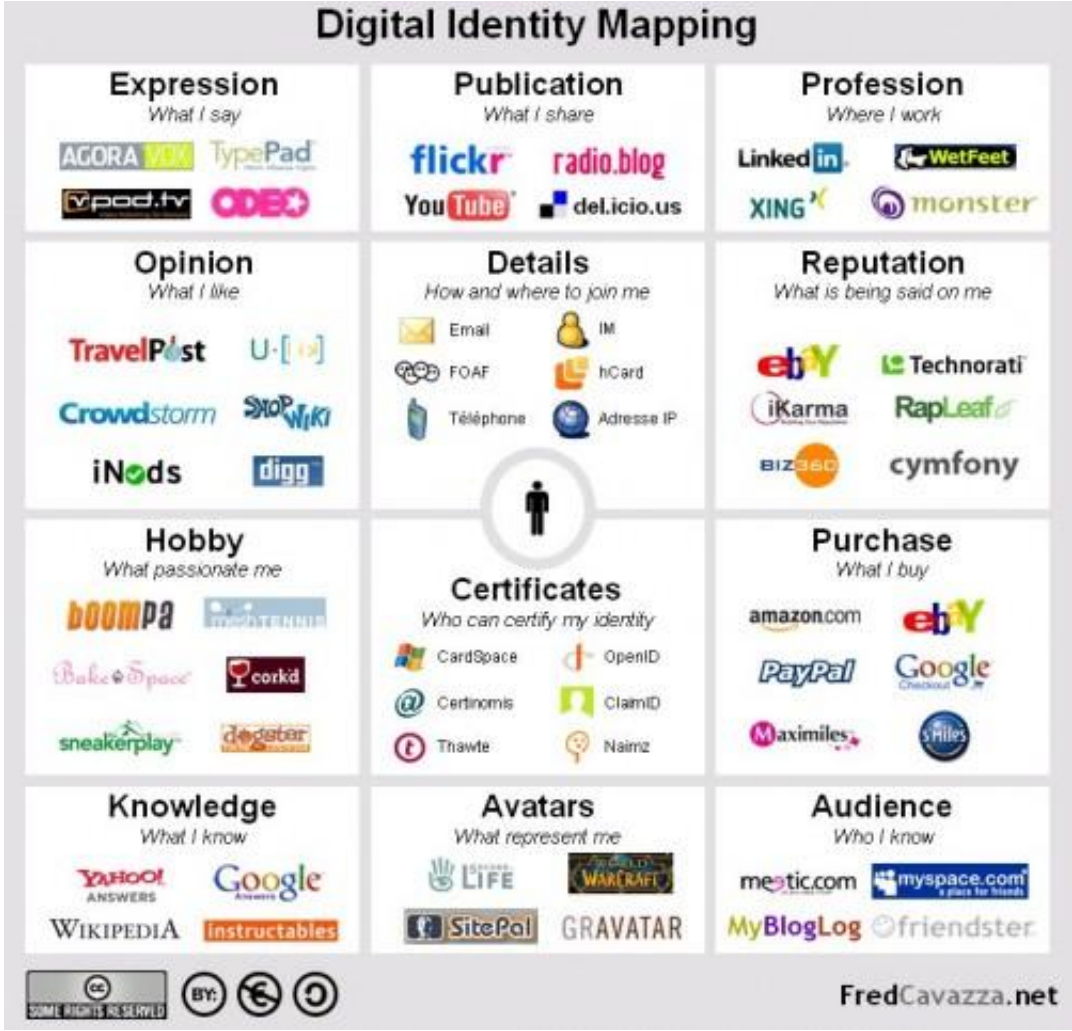
Hvem er jeg?

Hvem er du?

Helsedirektoratet

Et spørsmål om *identitet*

Hvem du er, avhenger av konteksten



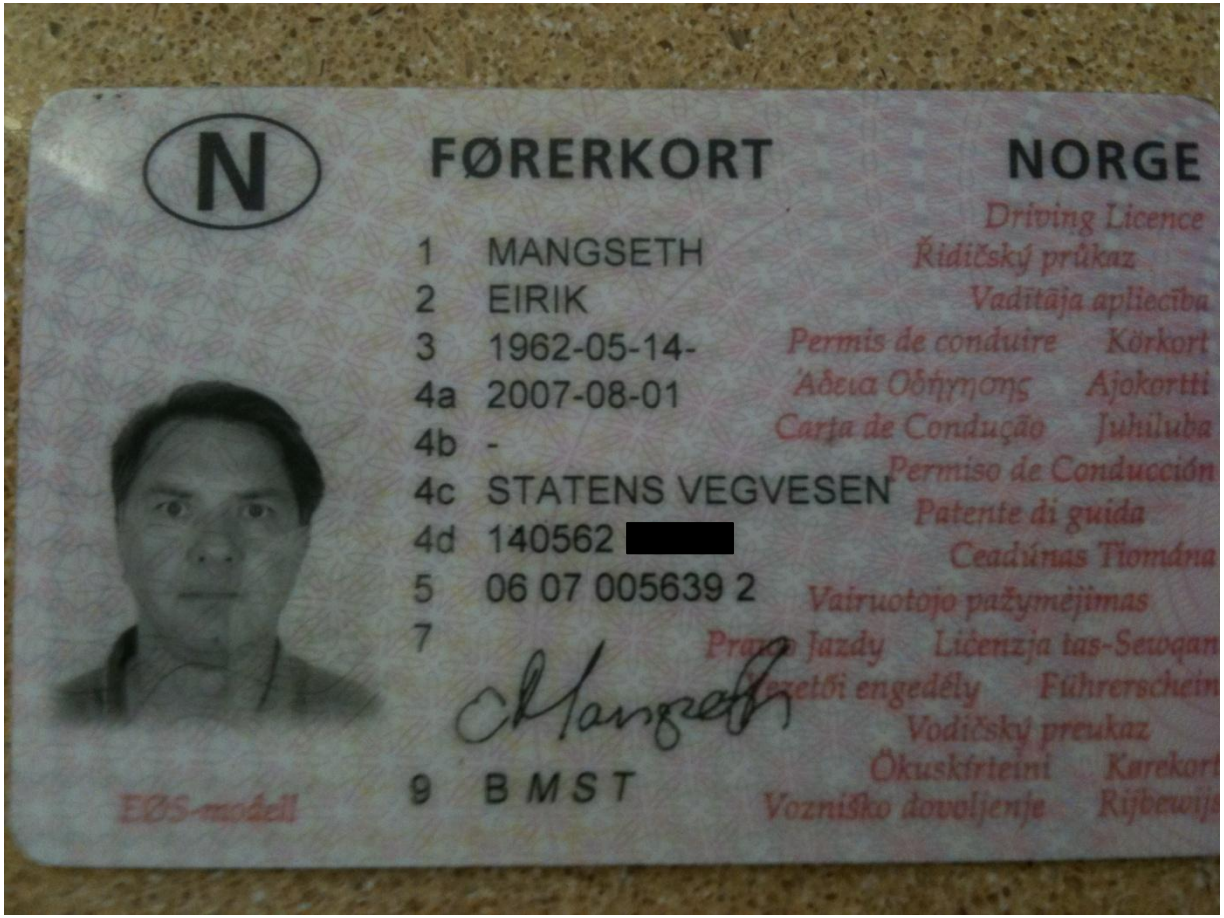
I en forretningssammenheng er identitet et *operasjonelt* konsept. Dvs., identitet er de fakta om et subjekt som er relevante i den gitte sammenhengen.

Helsedirektoratet

Faktaene og privilegiene kan vi kalle fordringer eller påstander (eng. claims).

Påstandsbasert identitet = identitet basert på et sett med fakta og privilegier

Helsedirektoratet



Helsedirektoratet

Bruk av påstandsbasert identitet fordrer et eksplisitt tillitsforhold med en såkalt *utsteder* (eng. issuer).

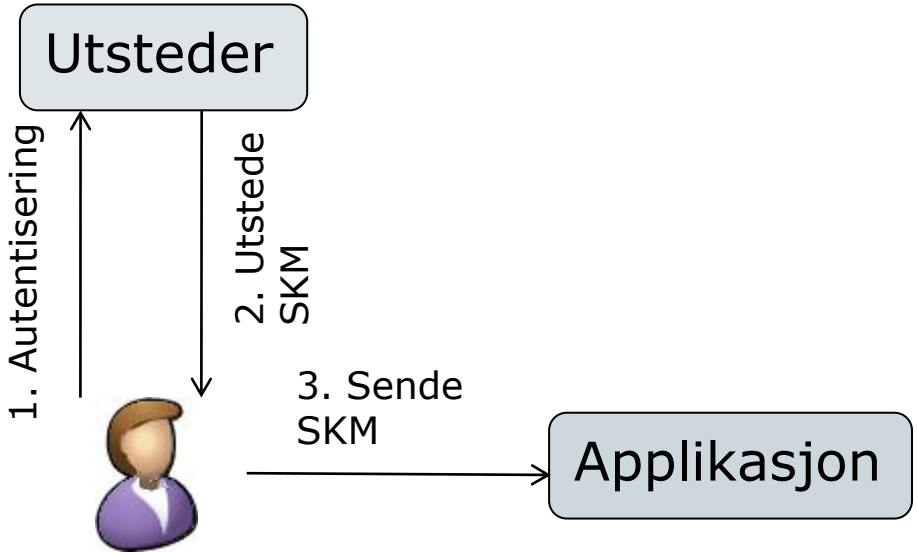
En applikasjon tror på en eller flere påstander om en bruker, kun hvis applikasjonen stoler på den som utstedte påstandssettet.

”You have to decide who you trust, before you decide what to believe”

Et sett med påstander kalles et sikkerhetskjennemerke (SKM) (eng. security token).

Hvert sikkerhetskjennemerke signeres digitalt av den som har utstedt kjennemerket.

En påstandsbasert applikasjon aksepterer at brukerne er autentisert hvis de kan fremvise et gyldig, signert sikkerhetskjennemerke fra en utsteder man har et tillitsforhold til.



Helsedirektoratet

Standardbasert

- Dagens løsninger er basert på åpne standarder, eks,
  - WS-Trust
  - WS-Federation
  - SAML
  - o.a.

Oppsummering så langt

- Påstand (eng. claim): et faktum
- Sikkerhetskjennemerke (eng. security token): Et (signert) sett med påstander
- Påstandsbasert identitet (eng. claims based identity): identitet basert på et sett med fakta og privilegier
- Påstandsbasert sikkerhet (eng. claims based security): Autentisering og autorisering basert på påstander.
- Utsteder (eng. Issuer or Identity provider): den som utsteder gyldige og signerte sikkerhetskjennemerker

Helsedirektoratet

Oppsummering så langt

- Påstandsbasert sikkerhet
  - Frakopling av autentiseringsmekanismen fra applikasjoner og tjenester
  - Erstatter roller med påstander/påstandssett som en mer finkornet autentiserings- og autoriseringsmekanisme
  - Støtter scenarioer basert på føderert sikkerhet

Helsedirektoratet

Oppsummering så langt

- Føderert sikkerhet
  - Samme fordeler som for påstandsbasert sikkerhet
  - Autentisering delegeres til en annen tjeneste, påstander pakkes inn i et såkalt sikkerhetskjennemerke
  - Kan gi brukere i domener man stoler på tilgang til applikasjoner og funksjonalitet i eget domene, les ”tilgang på tvers”
  - Støtter ”Single Sign-On”

2. Utfordringsbildet

Helsedirektoratet

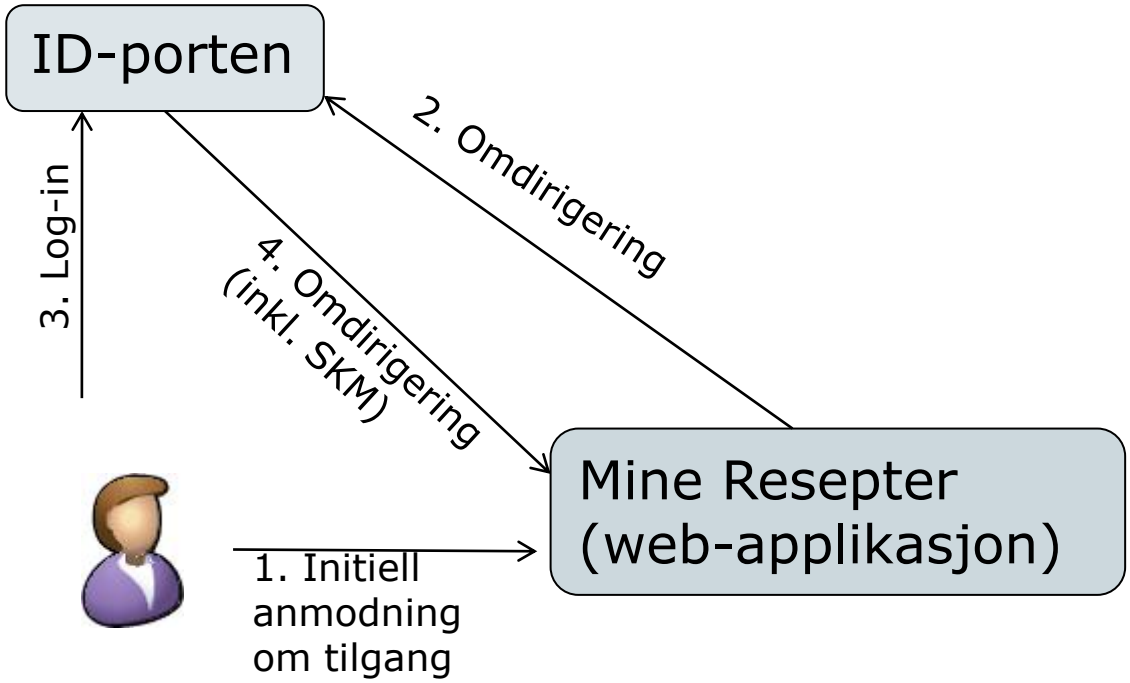
Utfordringsbildet

- Kunne støtte forskjellige akkreditiver (eng. credentials)
- Manglende fleksibilitet i rollebasert sikkerhet
- Opprettelse og sletting av eksterne brukere
- Synkronisering på tvers av domener
- Etablere tillitsforhold mellom forskjellige sikkerhetsdomener
- Single sign-on
- Sikkker ”tilgang på tvers”

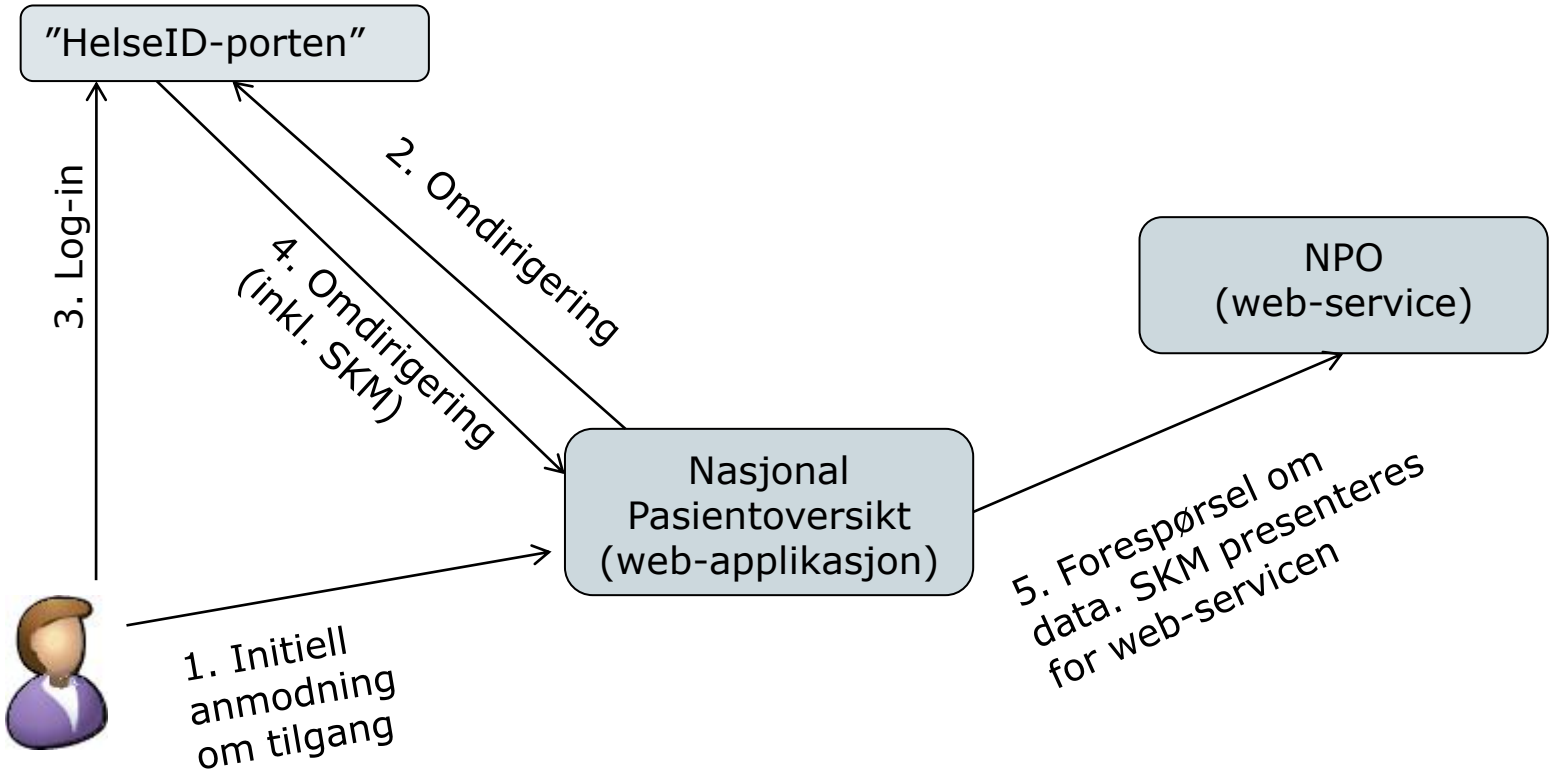
Helsedirektoratet

3. Scenarioer

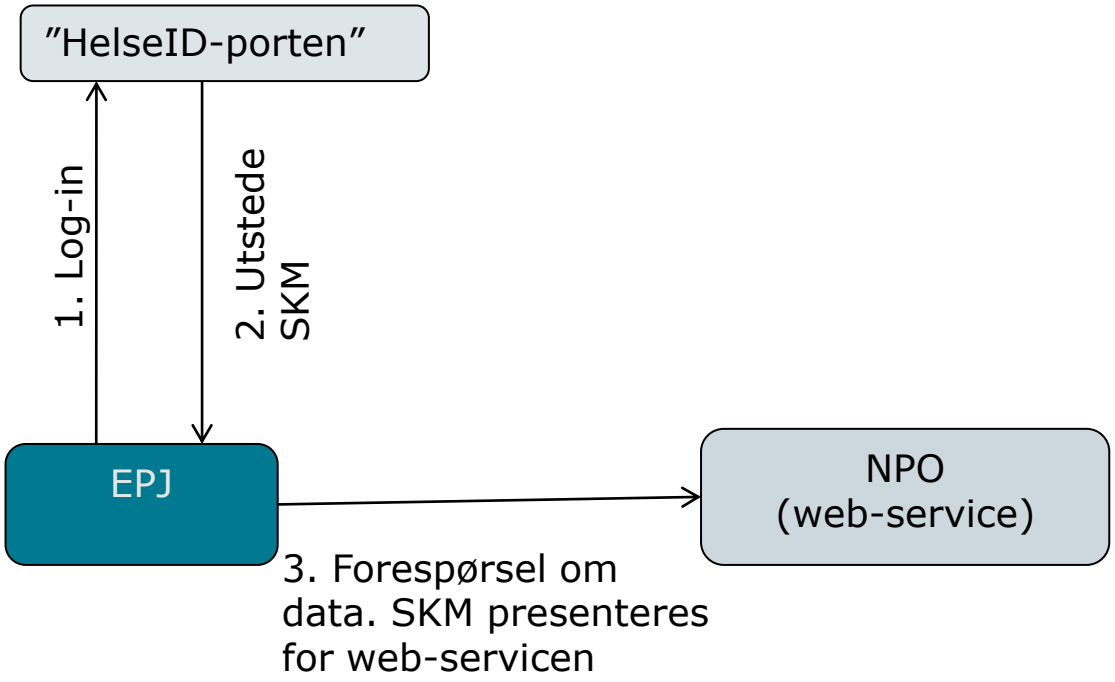
Mine Resepter, en borgertjeneste



NPO (kun et konsept)

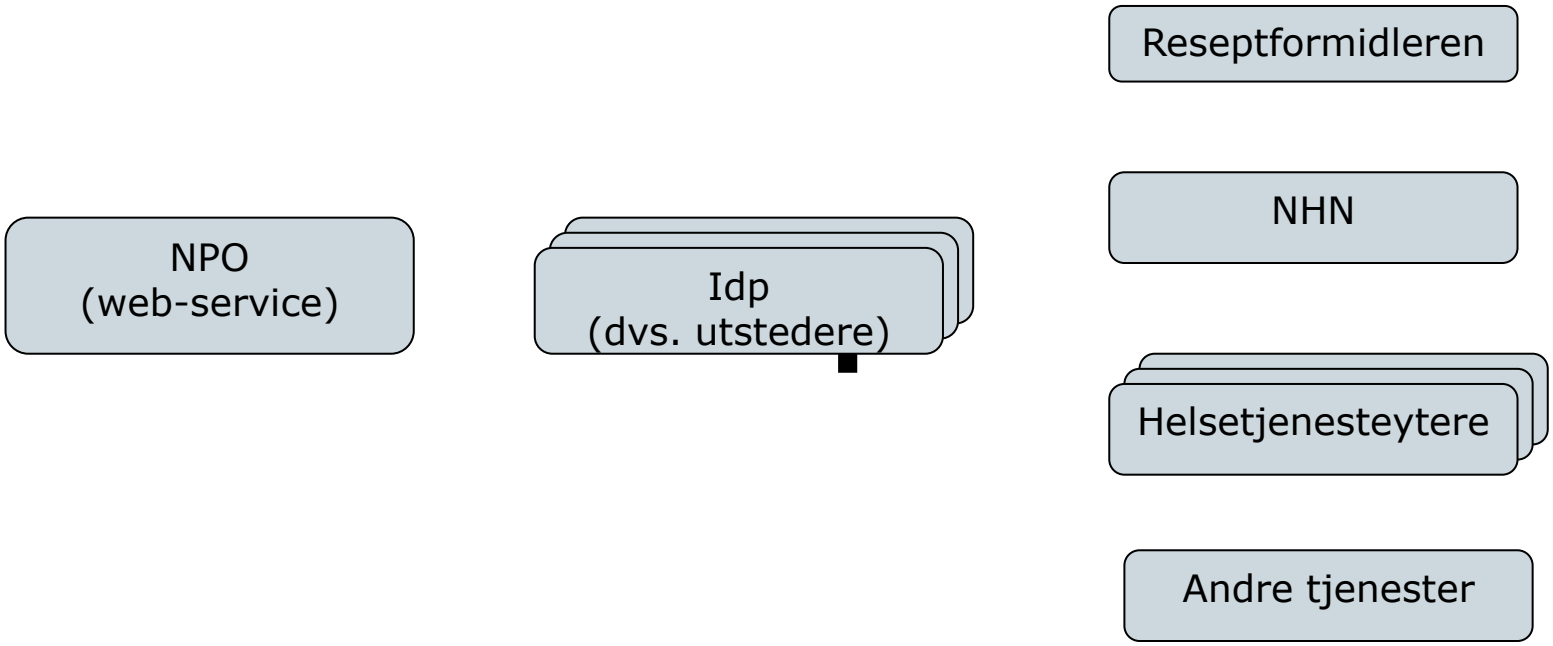


NPO (fremdeles kun et konsept)



En ”smart-client”, for eksempel et EPJ-system, vil på forhånd vite hvilke utstedere den skal benytte, mens en nettleser må omdirigeres til den eller de utstederne som nettstedet har et tillitsforhold med.

NPO (fremdeles kun et konsept)



Utstederne ovenfor kan spille rollen som påstandsomformere, dvs. de tar et sett med påstander som input og omformer disse slik at de blir tilpasset mottaker før de oversendes mottaker.

Påstand

Påstandsbasert identitet
og
føderert sikkerhet
danner det tekniske grunnlaget
for
sikker ”tilgang på tvers”

Helsedirektoratet

Tillit ☺

Helsedirektoratet

Takk for oppmerksomheten