folkehelseinstituttet

The need and value of a centralized credential-service

Peter Holmes
Project Leader, Folkehelseinstituttet

folkehelseinstituttet

Agenda / overview

- purpose
- abbreviations, terminology (with examples)
- background
- business cases / service offers
- example with PANVAK
  - quick assessment
  - making authorization more elegant

folkehelseinstituttet

Agenda / overview (ii)

- important types of claims in health sector
- division of responsibilities
- maturity of claims-based authorization
- some key architectural considerations
- ongoing work and FHIs vision
- summary / consequences of introducing claims-based ID management

folkehelseinstituttet

Purpose

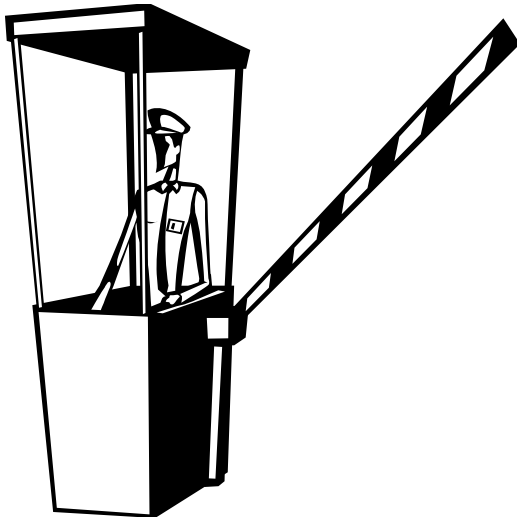
- originally…
  - to exemplify and lobby for the need to prioritize this area
- today...
  - to exemplify the value and positive consequences of developing and deploying this kind of service

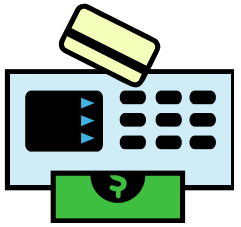
folkehelseinstituttet

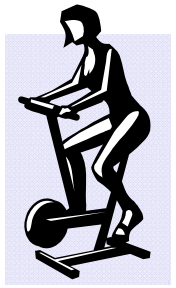
Abbreviations and terminology

- NHN
  - Norsk Helsenett
  - Norwegian Health Net
- Hdir
  - Helsedirektoratet
  - The Norwegian Directorate of Health
- HOD
  - Helse- og omsorgsdepartementet
  - The Ministry of Health and Care Services
- DIFI
  - Direktoratet for forvaltning og IKT
  - Agency for Public Management and eGovernment
- FHI
  - Nasjonalt folkehelseinstitutt
  - The Norwegian Institute of Public Health
- credentials

When you need credentials…







Examples of credentials and their attributes

- driver's license
- passport
- credit card
- boarding card
- membership cards

- personal ID data
- serial number
- issuing agency
- date of issue
- date of expiry
- privileges
- …

Credentials are claims

- e.g., a passport is a security document (”token”)
  - issued by a trusted provider
  - each attribute inside is a claim about its owner
  - collection of attributes = set of claims
- any controller may question whether the claims inside are true
  - underlying question: ”Do I trust the issuer?

What's meant by "credential-service" ?

- a service which facilitates
  - access to secured resources
  - across security domains mananged by different organizations
  - "tilgang på tvers"
- in the literature, this area is known as
  - **claims-based identity management**
- in Dagens Helsetall (FHI), called
  - "sentral akkrediteringstjeneste"

folkehelseinstituttet

Background

- Feb 2008:
  - FHI discussed its projected needs with NHN and Hdir
  - HDir v/ KITH: ongoing standardization activities
  - FHI in dialogue with the Norwegian Data Inspectorate (Datatilsynet)
- certain service offers would require
  - real-time response
    - asynchronous (message-based) service offerings inadequate in some contexts
  - specialized authorization for access

folkehelseinstituttet

Sample business cases / service offers

- review of FHIs service types
- relations amongst service types

folkehelseinstituttet

Review of FHIs service types

- for citizens
  - fhi.no
  - norgeshelse.no
  - reseptregistret.no
  - msis.no
  - reservation register (reservasjonsregisteret)
  - ”my register data” (mineRegisterdata)

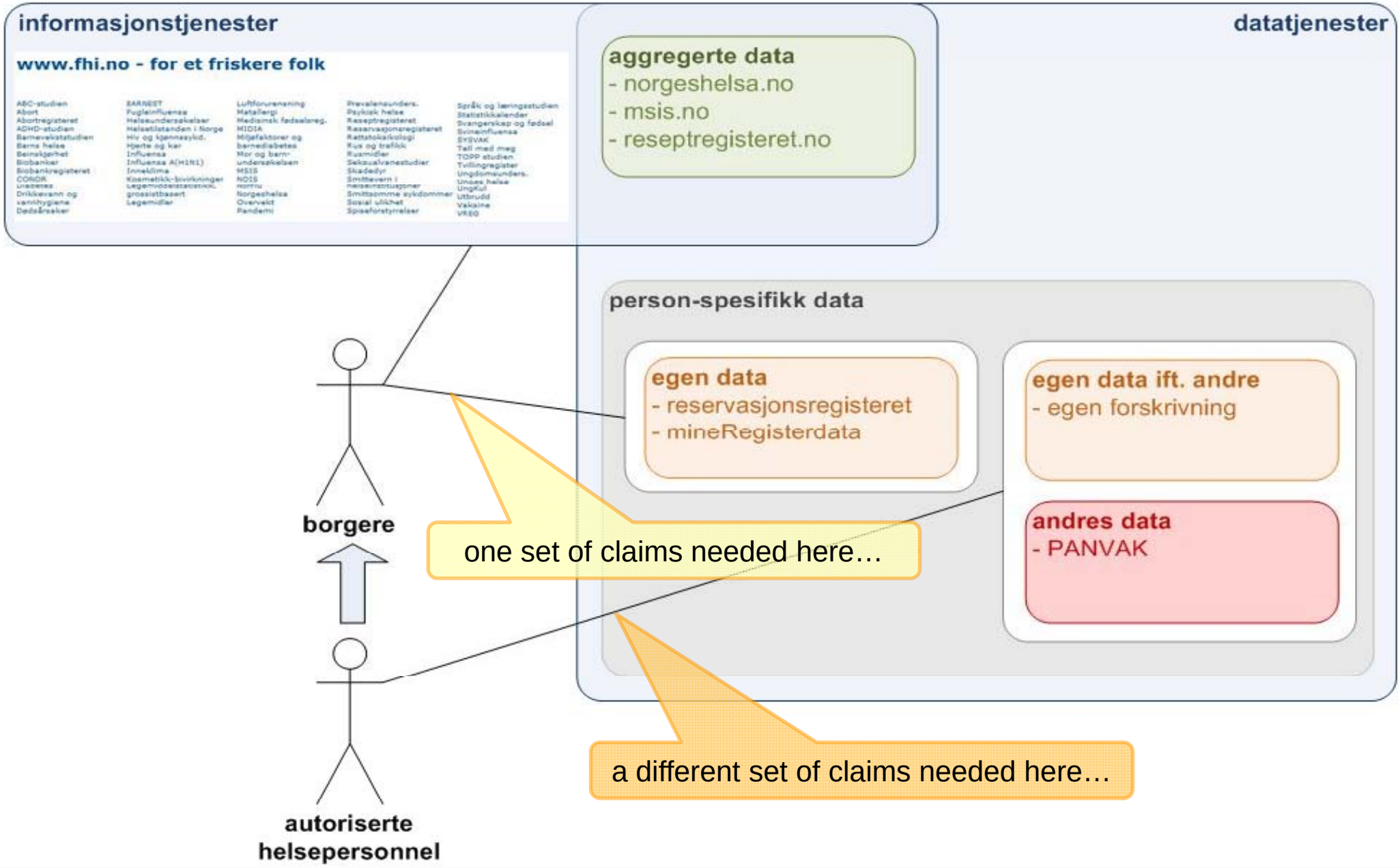
folkehelseinstituttet

Review of FHIs service types (ii)

- for health professionals…
  - PANVAK
  - ”my presciption pattern” (egen forskrivning)
  - reporting to MSIS

folkehelseinstituttet

Relations amongst service types


informasjonstjenester
www.fhi.no - for et friskere folk
datatjenester
aggregerte data
- norgeshelsa.no
- msis.no
- reseptregisteret.no
person-spesifikk data
egen data
- reservasjonsregisteret
- mineRegisterdata
egen data ift. andre
- egen forskrivning
andres data
- PANVAK
borgere
autoriserte
helsepersonnel
one set of claims needed here…
a different set of claims needed here…

folkehelseinstituttet

Business case: PANVAK

- summer 2009: pandemic influenza
- need to provide facility for registration of vaccinations into SYSVAK
  (Norway's National Vaccination Register)
- characteristics / requirements
  - wide-scale registration
  - evt. high volume
  - rapid, lightweight deployment
- web-based registration application built: PANVAK

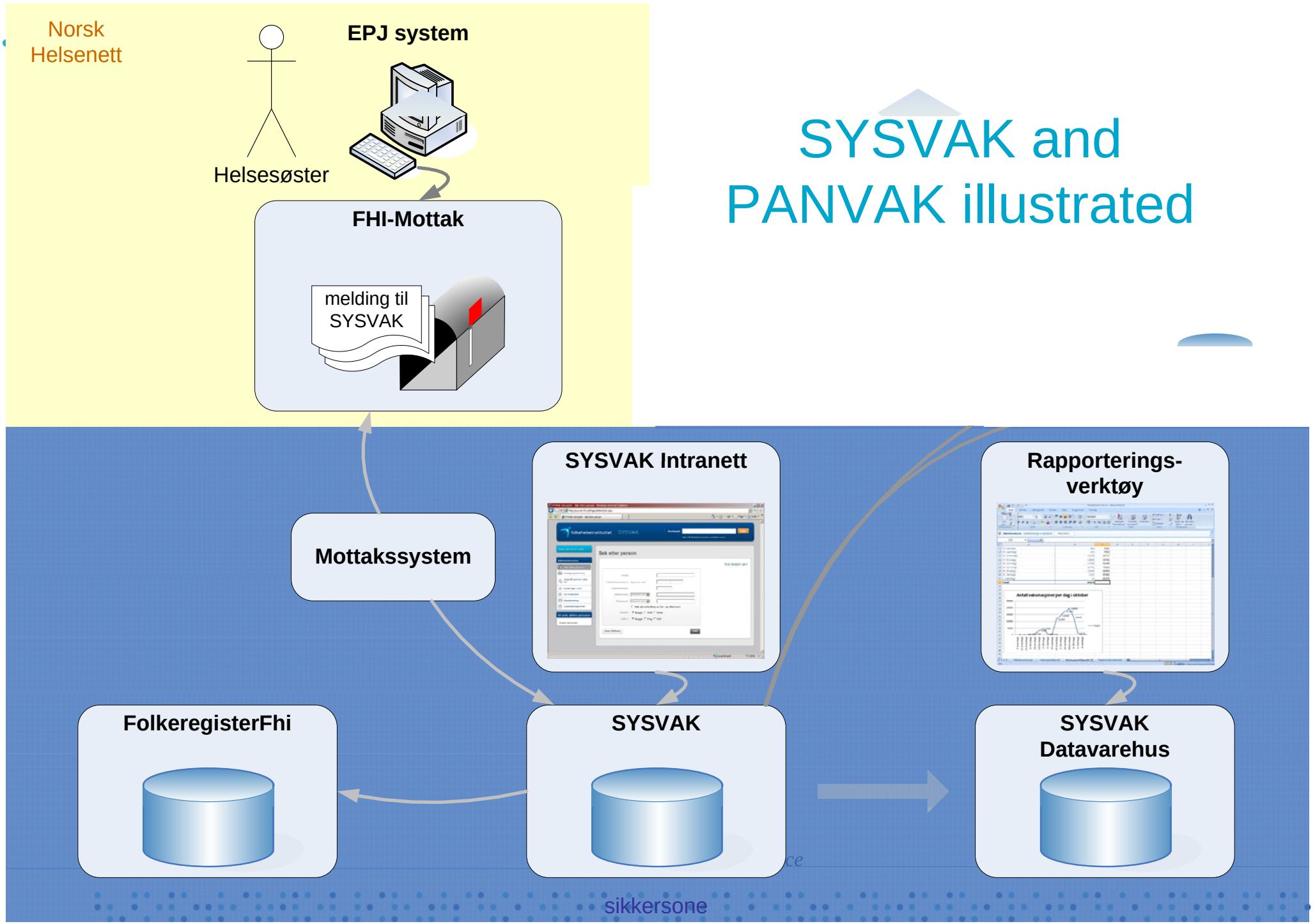
Who should be allowed to register data ?

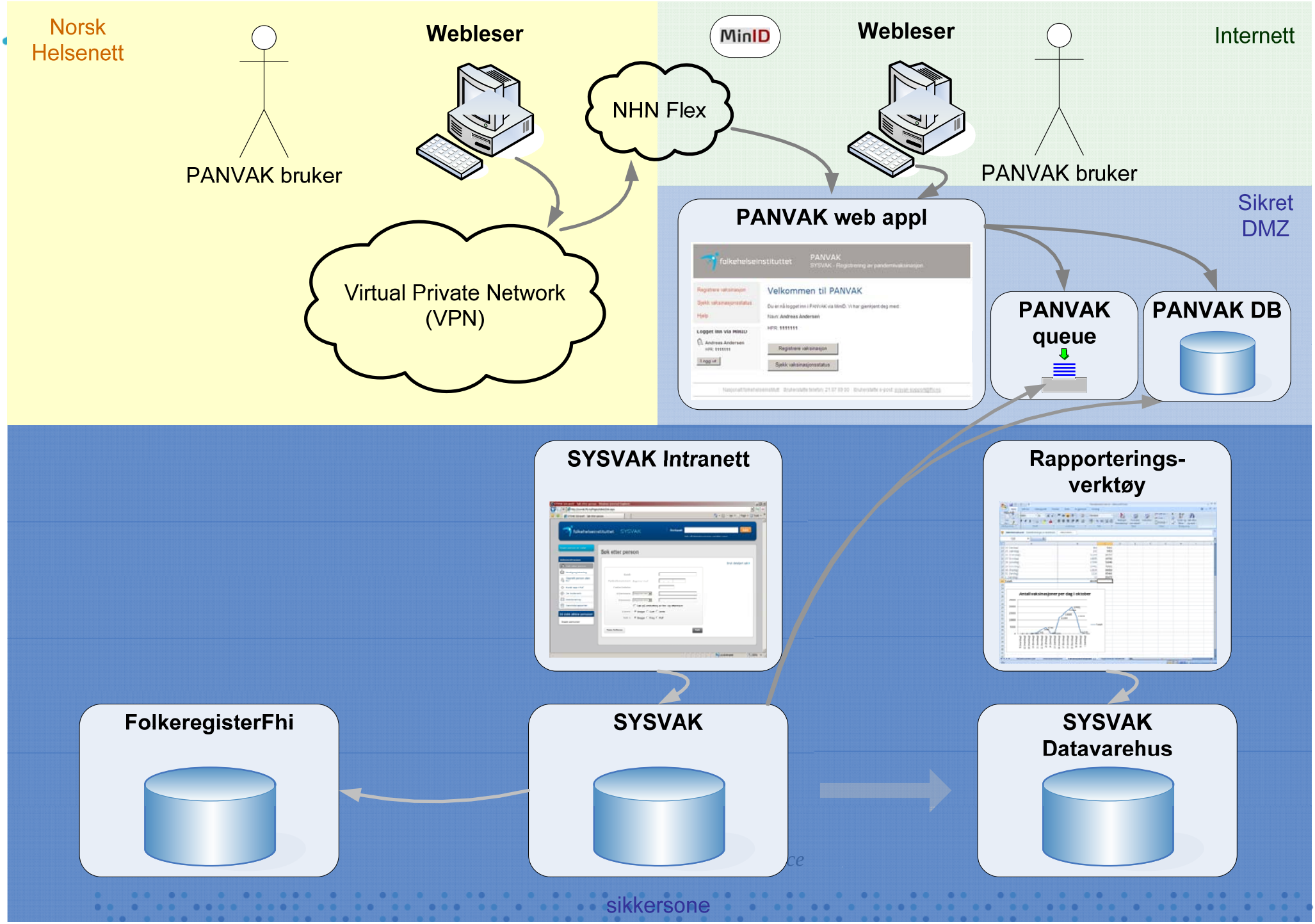
- pre-approved access for
  - doctors (leger)
  - nurses (sykepleiere)
  - ”health workers” (helsefagarbeidere)
  - bioengineers (bioingeniører)
  - ”reserve health workers” (vernepleiere)
  - health secretaries (helsesekretærer)
- access could be requested for others…

How was pre-approved access enabled ?

- weekly update of HPR sent to FHI
  (National Health Personnel Register)
- HPR attributes included
  - person ID number (fødselsnummer)
  - HPR number
  - category of profession
- used MinID to authenticate person ID number
- checked against local copy of HPR DB to authorize access

SYSVAK and PANVAK illustrated




Norsk Helsenett
PANVAK bruker
Webleser
MinID
NHN Flex
Virtual Private Network (VPN)
Webleser
Internett
PANVAK bruker
Sikret DMZ
PANVAK web appl
Velkommen til PANVAK
PANVAK queue
PANVAK DB
SYSVAK Intranett
Rapporterings-verktøy
FolkeregisterFhi
SYSVAK
SYSVAK Datavarehus
sikkersone

What's wrong with PANVAK's authorization approach ?

- HPR data updated weekly at FHI
  - HPR data potentially incomplete or expired
- manual operations to "fetch in" these updates
- special purpose SW was written to
  - process, store and manage these updates
  - check for authorization against this data source

folkehelseinstituttet

What would be more elegant ?

- when a user requests access, PANVAK could ask a local claims provider to help support decision about granting access
- the local claims provider could interoperate with trusted external claim providers to collect claims about the user
- based on these claims and local policies, the local claims provider can provide authorization support to PANVAK
- most importantly, the local claims provider could be used by any local application

folkehelseinstituttet

What kinds of claims are useful for authorization in the health sector ?

- category of profession
- place(s) of work
- role(s) at each work-place
- HPR number
  - ➢ HER and HPR registers can be used to obtain many of these attributes
  - ➢ HPR and HER are **attribute stores** (”credential repositories”)

folkehelseinstituttet

HPR: The Health Personnel Register

attribute classes	***# attributes (ca)***
– personalia	15
– education	5
– authorization	4
– prescription rights	4
– speciality	4
– ”legeturnus” (clinical training)	12

HER: Health Entity Register

Fornavn
Etternavn
Fødselsnr
HPR-nummer
HER-id
Tittel
EDI-adresse
Faxnummer
Telefonnummer

Tilhørende enhet
Organisasjonsnr
Forelders HER-id
Forelders RESH-id
Enhets ID

Kode	Yrke
LE	Lege

Kode	Spesialitet
1	Allmennmedisin

folkehelseinstituttet

Authorization: division of responsibilities

- relying party (e.g., PANVAK)
  - relies upon claims provider for authorization support
  - ultimately responsible for decision to grant access
- claims provider
  - delivers claims from attribute stores, in response to requests
  - can cooperate with trusted, external claim providers
  - can transform sets of claims
- data quality within the attribute stores
  - in HER, data quality is the responsibility of each legal organization
  - for HPR, SAFH* is responsible
    (* Norwegian Registration Authority for Health Personnel)

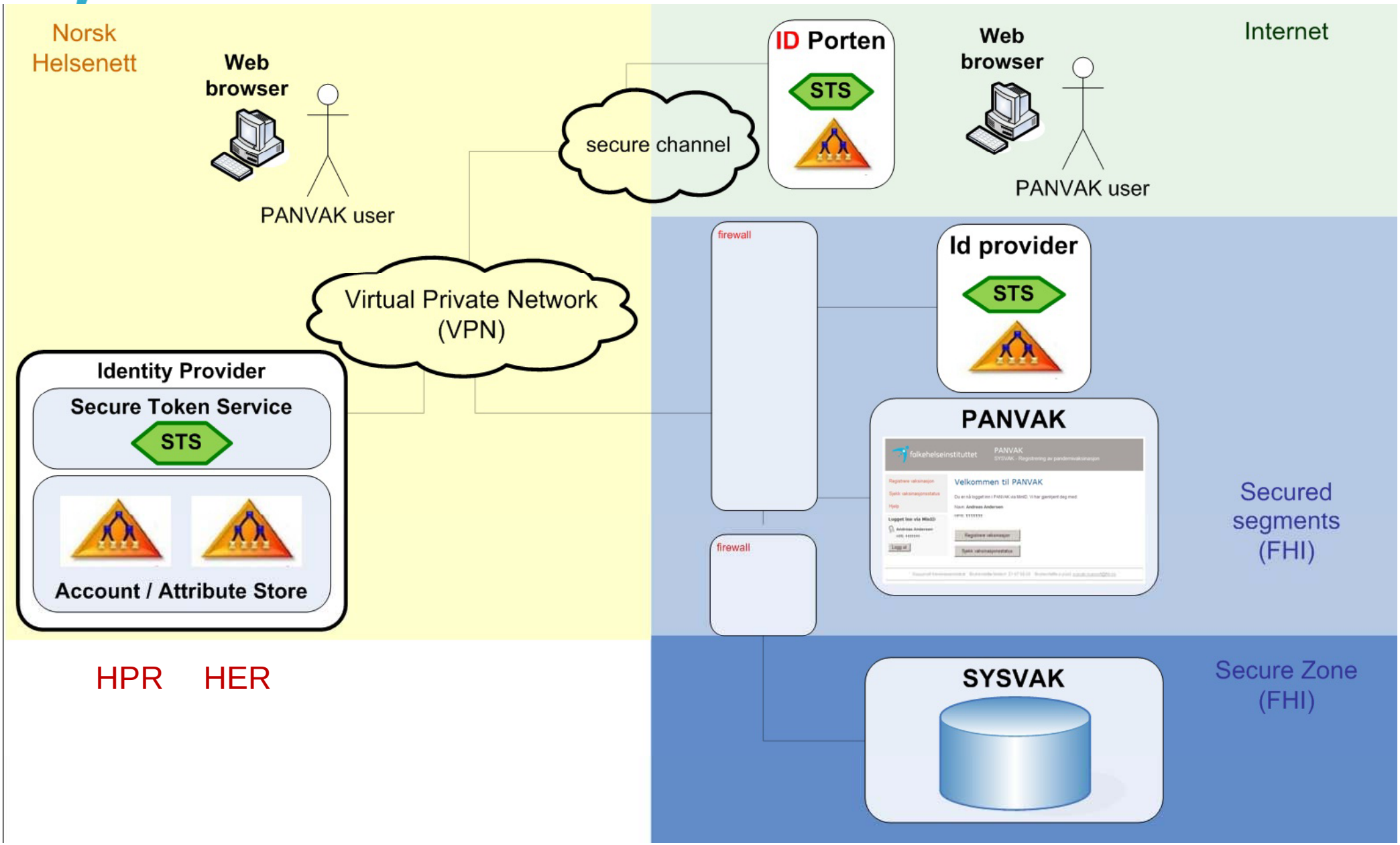
folkehelseinstituttet

Maturity of claims-based authorization

- key international standards exist
  - WS-Trust
  - WS-Federation
  - SAML 2.0 (Security Assertion Markup Language)
- products implemented by several vendors
  - OpenSSO (SUN/Oracle)
  - ADFS 2.0 (Microsoft)
- DIFI: demonstrated product interoperability

folkehelseinstituttet

a more elegant PANVAK…



folkehelseinstituttet

Some key architectural choices

- should a relying party use *externally* provided claims directly, or should it only trust claims from its local provider ?
- should a claims provider be protected by a proxy ?
- should access policies be centralized or distributed ?
  - ref. claims transformation…

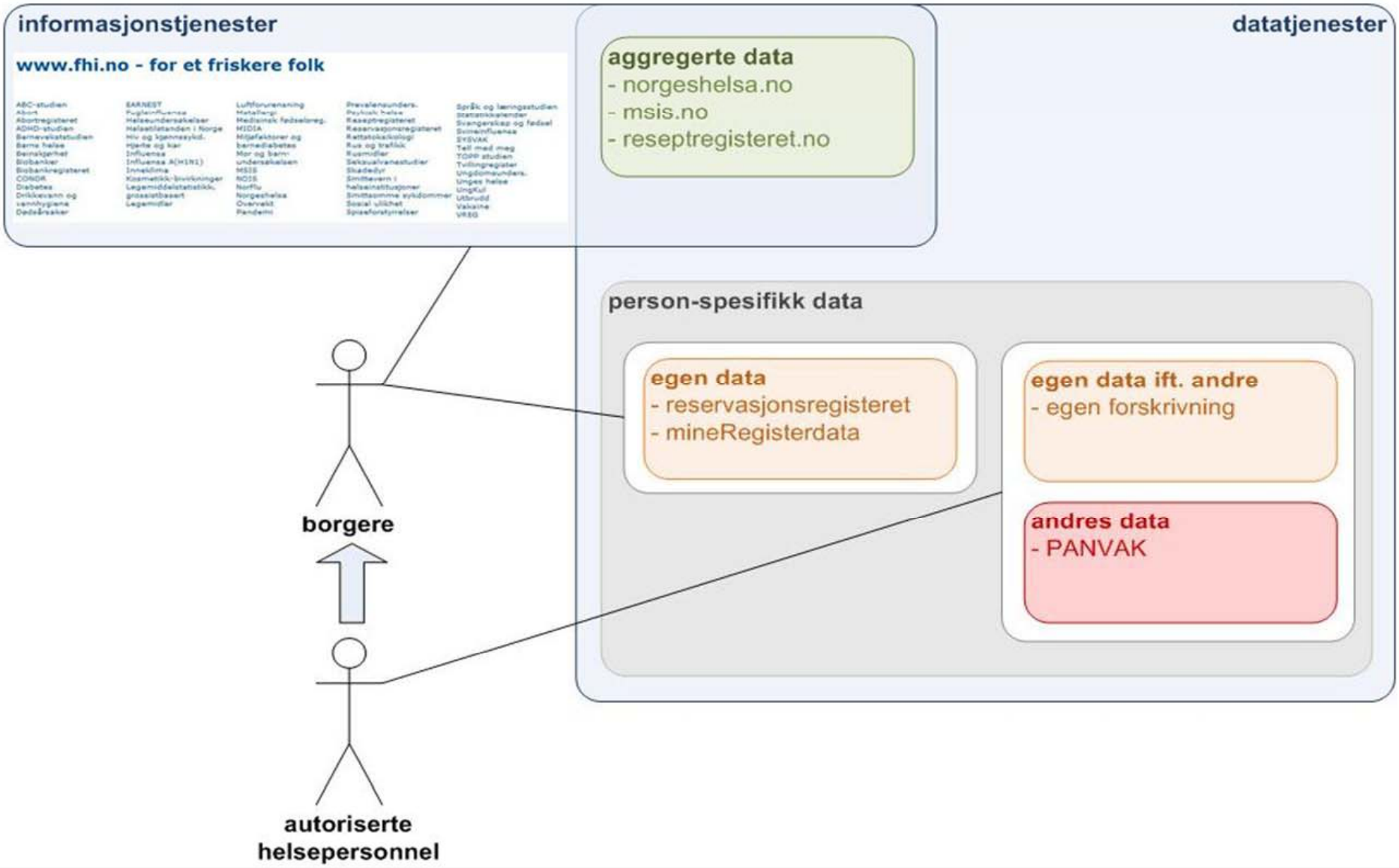
folkehelseinstituttet

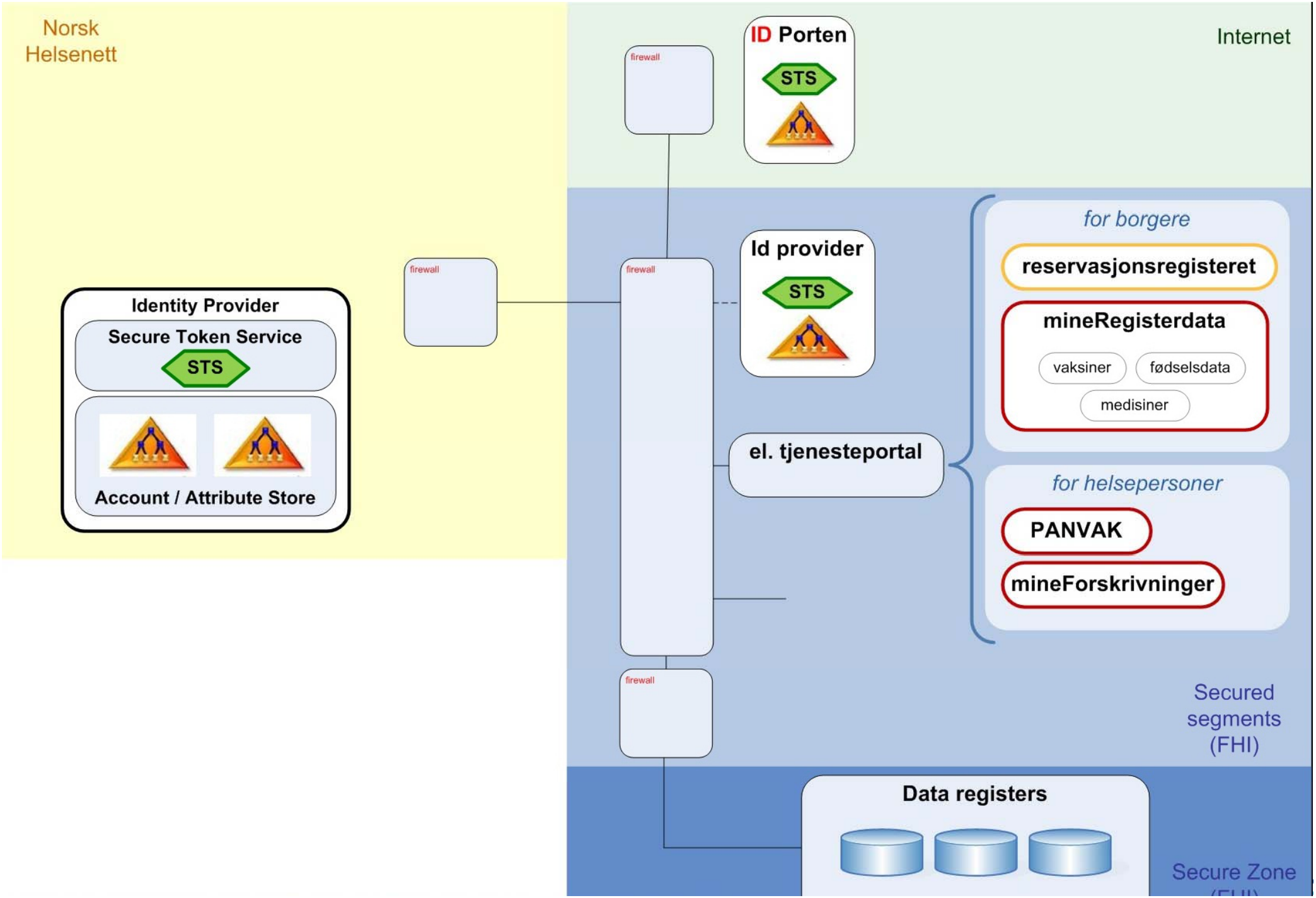
Ongoing work

- POC effort initiated
  - NHN, FHI, DIFI, HDir
- Upcoming tasks
  - Definition of POC environment
  - Definition of initial claim set
    - should later be circulated for review and evt. standardized

folkehelseinstituttet

FHIs vision…




Norsk Helsenett
Internet
ID Porten
STS
firewall
Identity Provider
Secure Token Service
STS
Account / Attribute Store
firewall
firewall
Id provider
STS
el. tjenesteportal
for borgere
reservasjonsregisteret
mineRegisterdata
vaksiner
fødselsdata
medisiner
for helsepersoner
PANVAK
mineForskrivninger
firewall
Secured segments (FHI)
Data registers
Secure Zone

folkehelseinstituttet

Summary / consequences of introducing claims-based ID management

- can help faciltitate secure access across organizational boundaries (”tilgang på tvers”)
- for HPR / HER, can:
  - increase degree of register population
  - sharpen requirements upon data quality

folkehelseinstituttet

Summary / consequences of introducing claims-based ID management (ii)

- other attribute stores could be leveraged where relevant, e.g.,
  - legal parent and guardian information could be supplied by Tax Authorities via DIFIs ID Porten…

- existing security infrastructures not threatened
  - technology can be introduced when organization is ready