Behov for en nasjonal sikkerhetsinfrastruktur for helse- og omsorgssektoren - hvorfor?

HelsIT/esikkerhetsdagen
19. September 2013

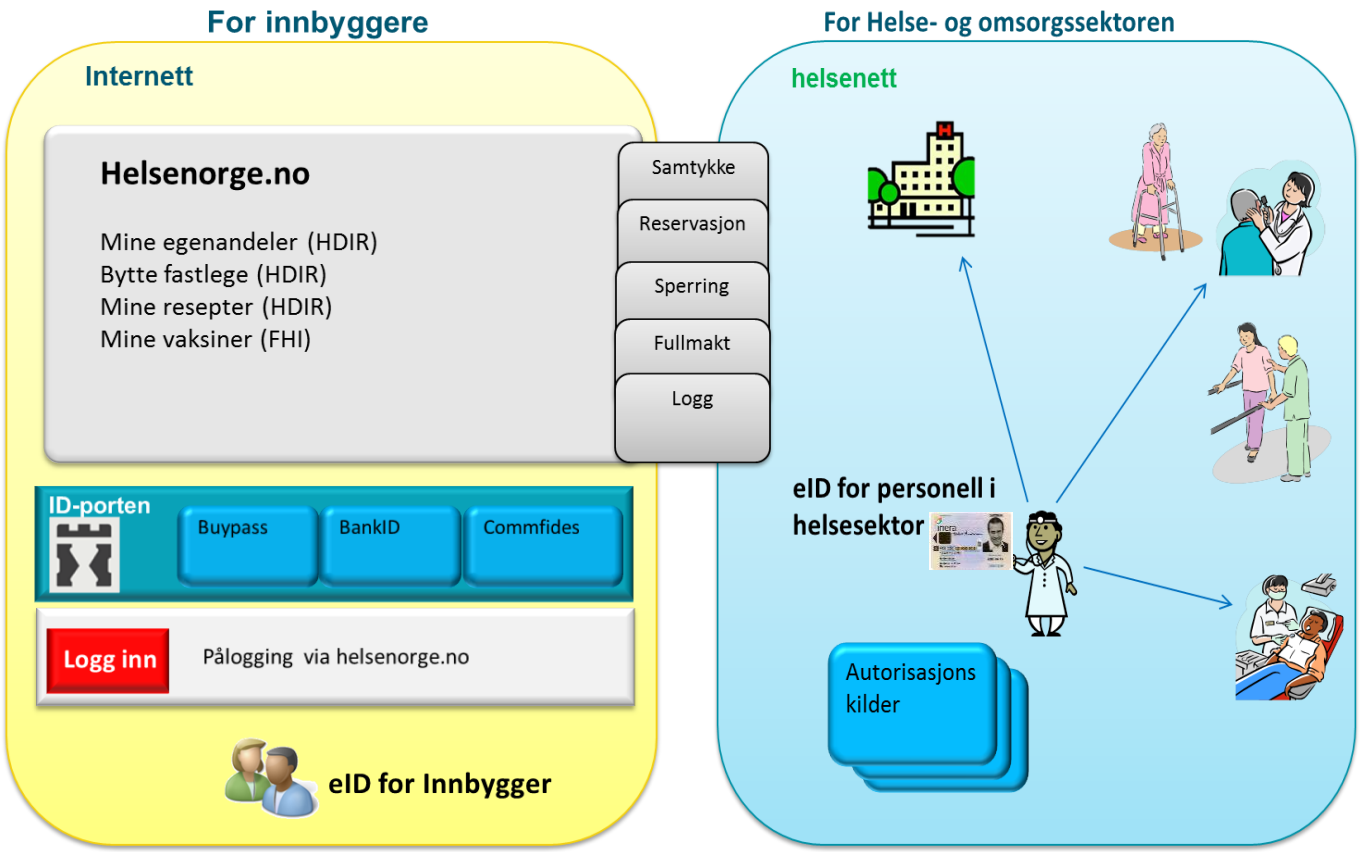
Mona Holsve Ofigsbø

Agenda

- Forstudie: Nasjonal sikkerhetsinfrastruktur for helse- og omsorgssektoren
  - Fokus og avgrensinger
- Informasjonsdeling på tvers av virksomhetsgrenser
  - Asynkron meldingsutveksling
  - Synkron meldingsutveksling
- Identitets- og tilgangsstyring, innebygd personvern
  - Felleskomponenter for helse- og omsorgssektoren

- Illustrasjon -

IKT-infrastrukturer

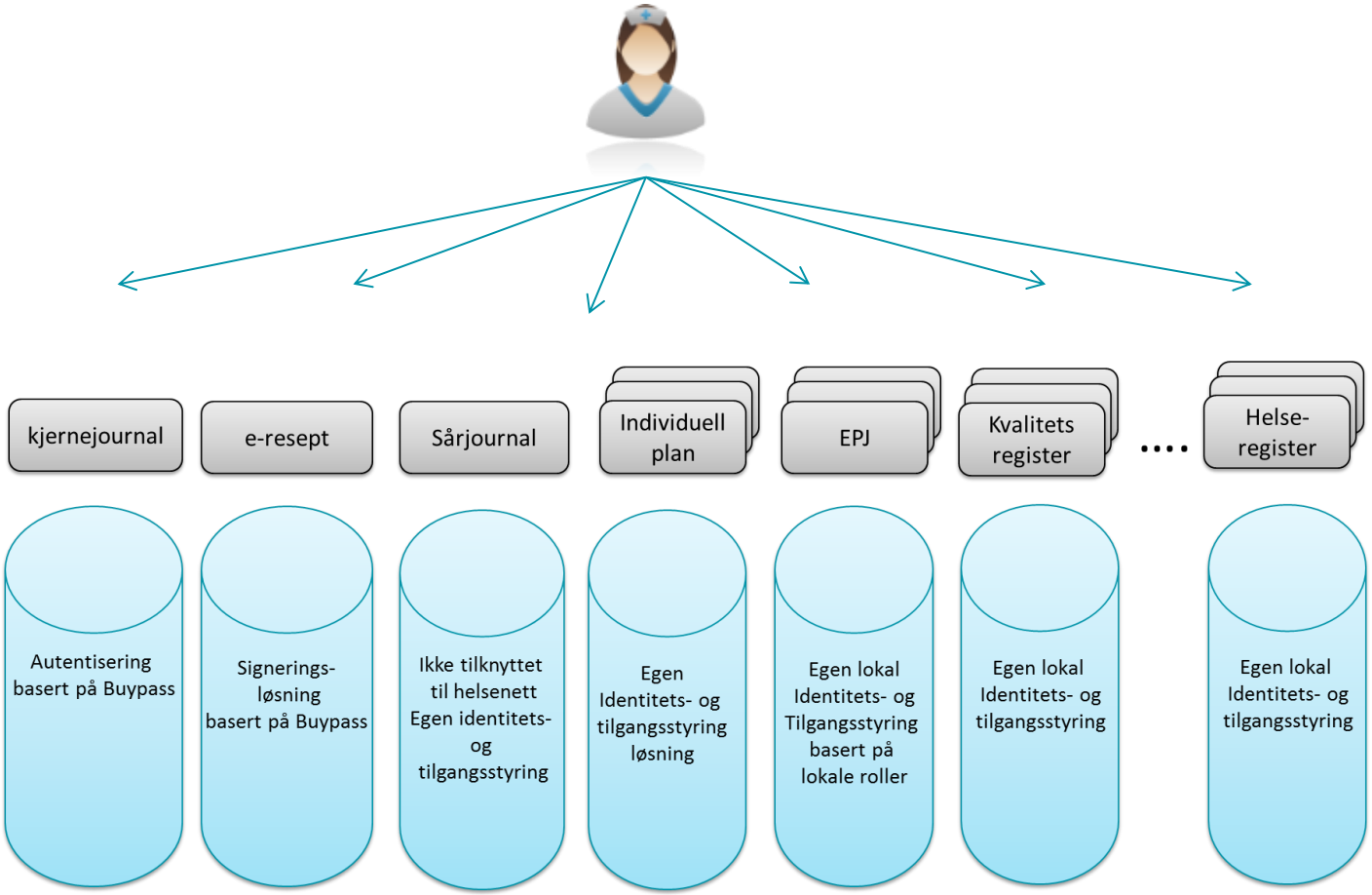


Bakgrunn

1. Statsbudsjettet, S.prp 1 (2012-2013), kap 720
   - *«Det foreslås å etablere sikker identifisering av helsepersonell. En mulig løsning kan være etablering av et profesjonskort med eID (høyt sikkerhetsnivå). Løsningen må etableres i henhold til en nasjonal sikkerhetsinfrastruktur og omfatte alle aktørene i sektoren. Løsningene skal understøtte både lokale og nasjonale behov som f.eks. e-resept, nasjonal kjernejournal og tilgang til opplysninger på tvers av virksomhetsgrenser»*
2. Meld.st nr.9 (2012-2013) Én innbygger – én journal
   - Helsepersonell skal ha en enkel og sikker tilgang til pasient- og brukeropplysninger
   - Innbyggerne skal ha tilgang på enkel og sikre digitale tjenester
   - Data skal være tilgjengelig for kvalitetsforbedring, helseovervåkning, styring og forskning
3. Meld.st 10 (2012-2013) God kvalitet – trygge tjenester
4. Meld.st.11 (2012-2013) Personvern – utsikter og utfordringar
5. Forslag til ny pasientjournallov og helseregisterlov (på høringsfrist 15 okt. 2013)
   - Bakgrunn: Samhandlingsreformen, St.meld 9, St. meld 10, St. meld 11, "Gode helseregister - bedre helse«, Regjeringens digitaliseringsprogram
   - *«For å legge til rette for sikker og effektiv elektronisk kommunikasjon av helseopplysninger, er det viktig å sikre en helhetlig IKT-arkitektur i sektoren. «*

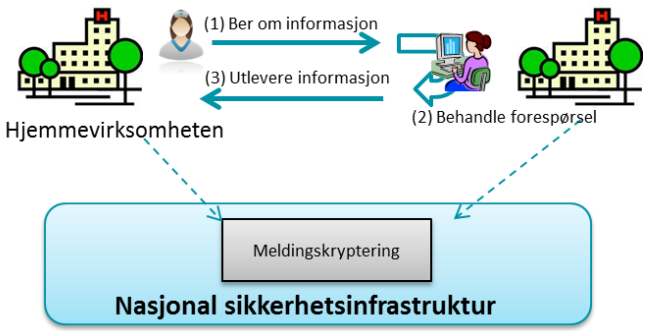
- Illustrasjon -

Nåsituasjon



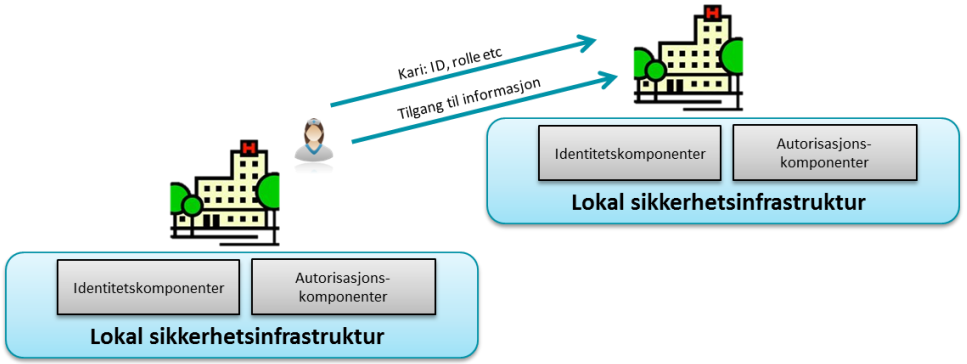
Informasjonsdeling

1. Manuell utlevering av informasjon
   «Asynkron meldingsutveksling»



Fordeler	Ulemper
Eksisterende system	Ikke egnet til sanntidskommunikasjon
Egnet til ikke tidskritiske kommunikasjon	Kopier lagres i flere systemer
	Ikke oppdatert informasjon

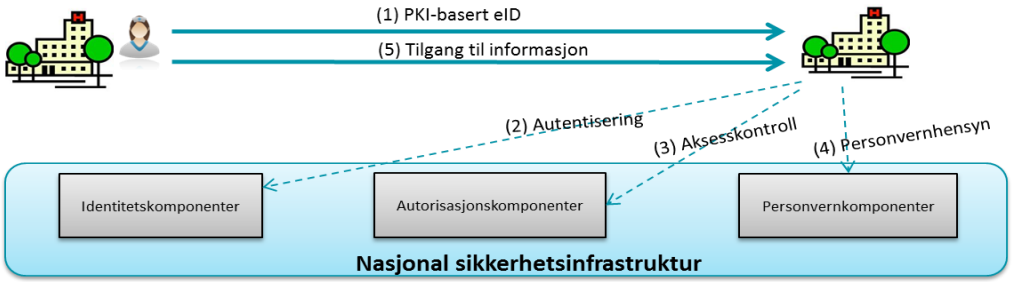
2. Automatisert tilgangskontroll
   basert på virksomhetens tilgangskontroll
   «Synkron meldingsutveksling»



Fordeler	Ulemper
Fungerer mellom virksomheter som har tillit til hverandre	Tillitsmodell hvor alle stoler på hverandre
Sanntidskommunikasjon	Tilgangsstyrer kun på autentisering av virksomheten
	Skalerer dårlig mhp sektorens behov for samhandling
	Utfordringer med grensesnitt, avtaleverk etc

Informasjonsdeling forts.

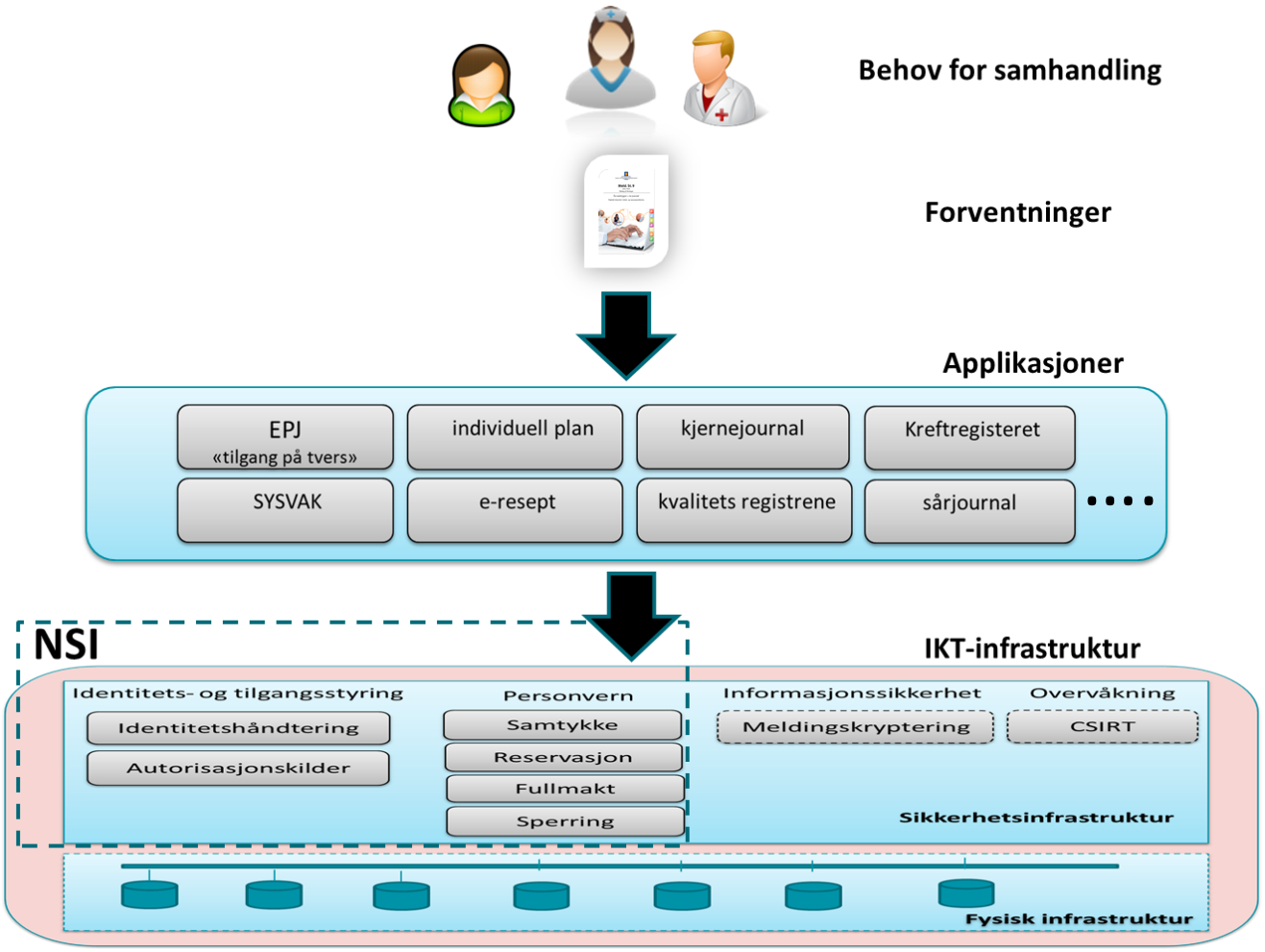
3. Automatisert tilgangskontroll basert på felleskomponenter
   «Synkron meldingsutveksling»



Fordeler	Ulemper
Sanntidskommunikasjon	Overgangsperioder må ivaretas
Identitet og autorisasjon blir kontroller før tilgang gis	
Små aktører blir ivaretatt gjennom nasjonale løsninger	
Skalerer til sektorens behov for deling av informasjon	
Nasjonale autorisasjonskilder er påbegynt	

Sikkerhetsinfrastruktur som del av IKT-infrastrukturen

- Illustrasjon -



Fokus i forstudien

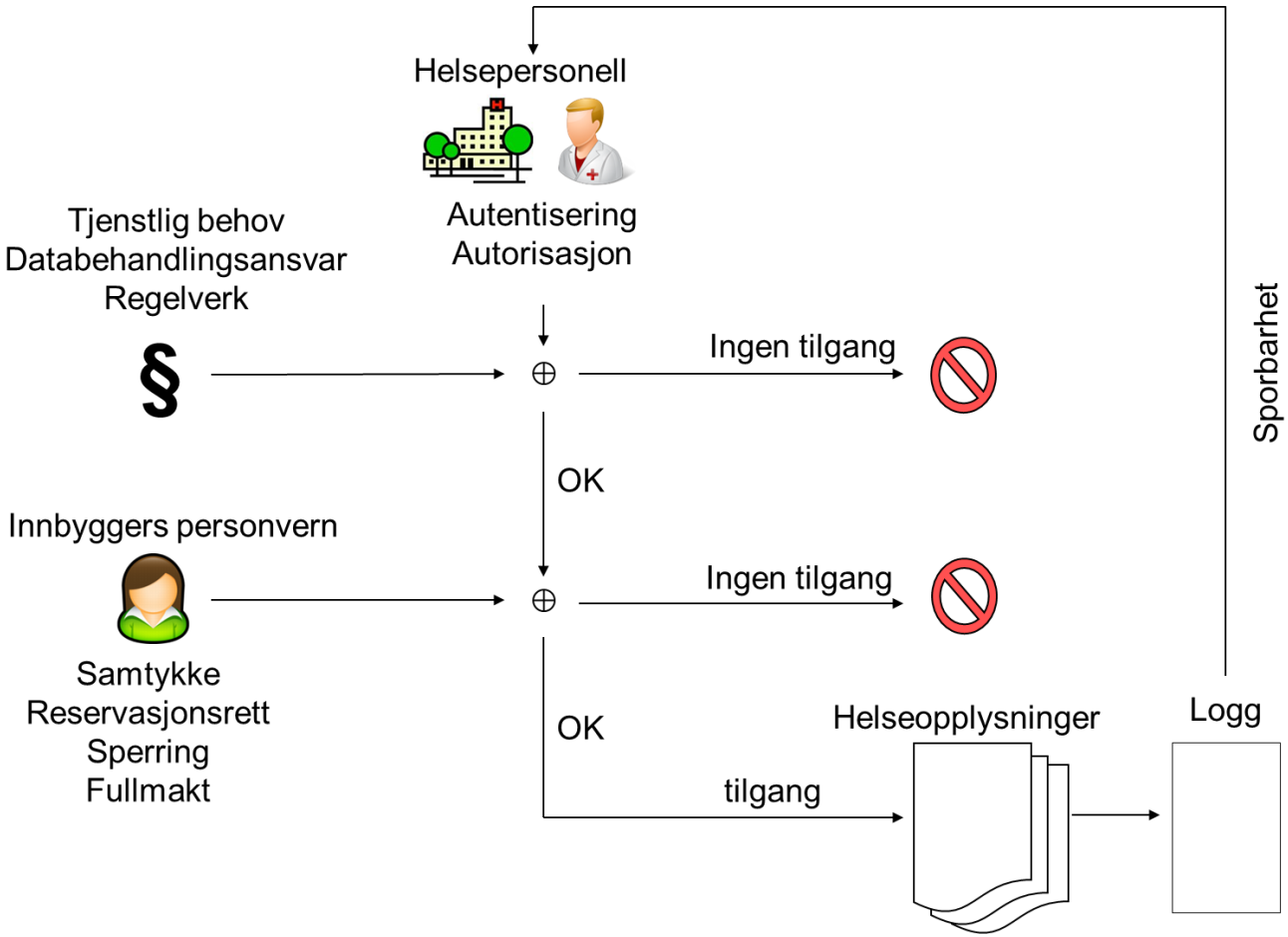
Sikkerhetsinfrastrukturen er selve grunnmuren for elektronisk samhandling og en forutsetning for en enhetlig og sikker deling av informasjon mellom IT-systemer i sektoren.

1. Identitetshåndtering
2. Autorisasjonsinformasjon
3. Innebygd personvern for innbygger

} *Automatisert tilgangskontroll for informasjonsdeling på tvers av virksomhetsgrenser*

- Illustrasjon -

Tilgangskontroll



Autentisering

a) Hva

Verifisering av din identitet

a) Hvorfor

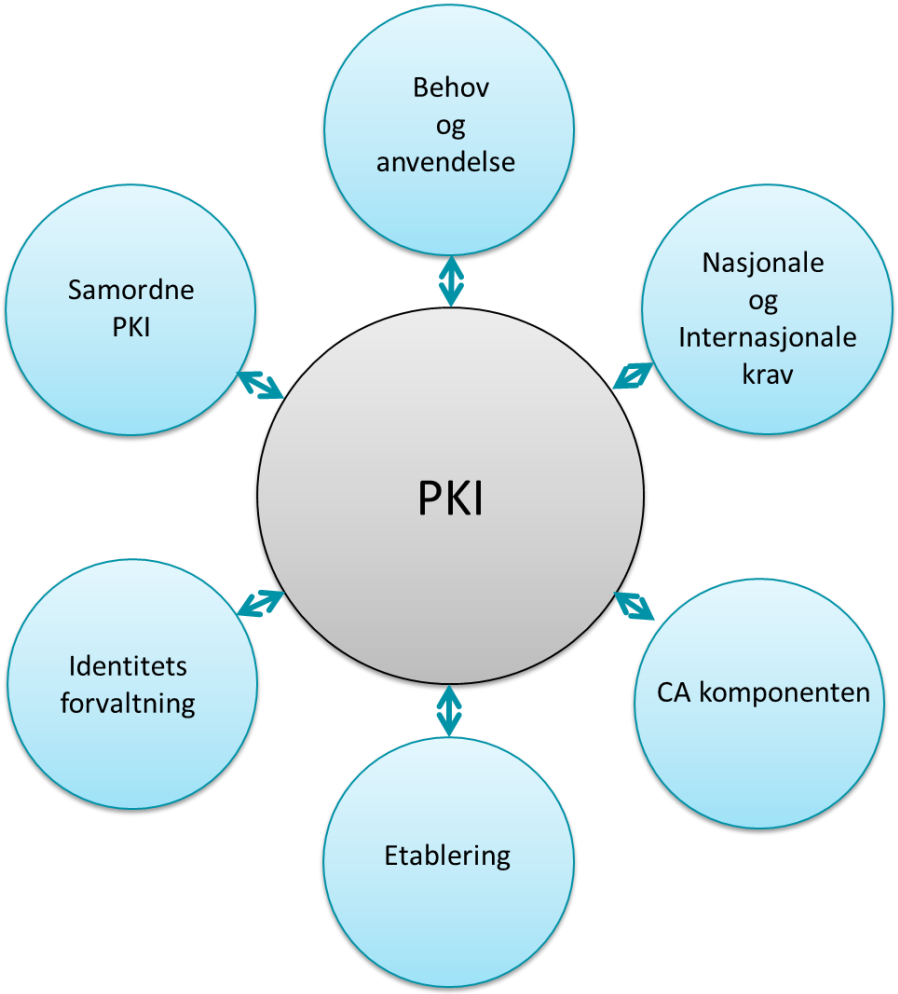
- Muliggjøre kontroll av personers autorisasjoner.
- Knytning mellom handling og person som utgjør handlingen (sporbarhet).

b) Hvordan identifisere og autentisere på tvers av virksomheter

1. Kun identifisering av virksomhet - ingen identifisering av person
2. Identifisering av person i «hjemmevirksomheten»
3. Autentisering av person utført i «hjemmevirksomheten»
4. Omdirigering til «hjemmevirksomheten» for autentisering
5. Ny autentisering utføres i regi av virksomheten som skal gi tilgang

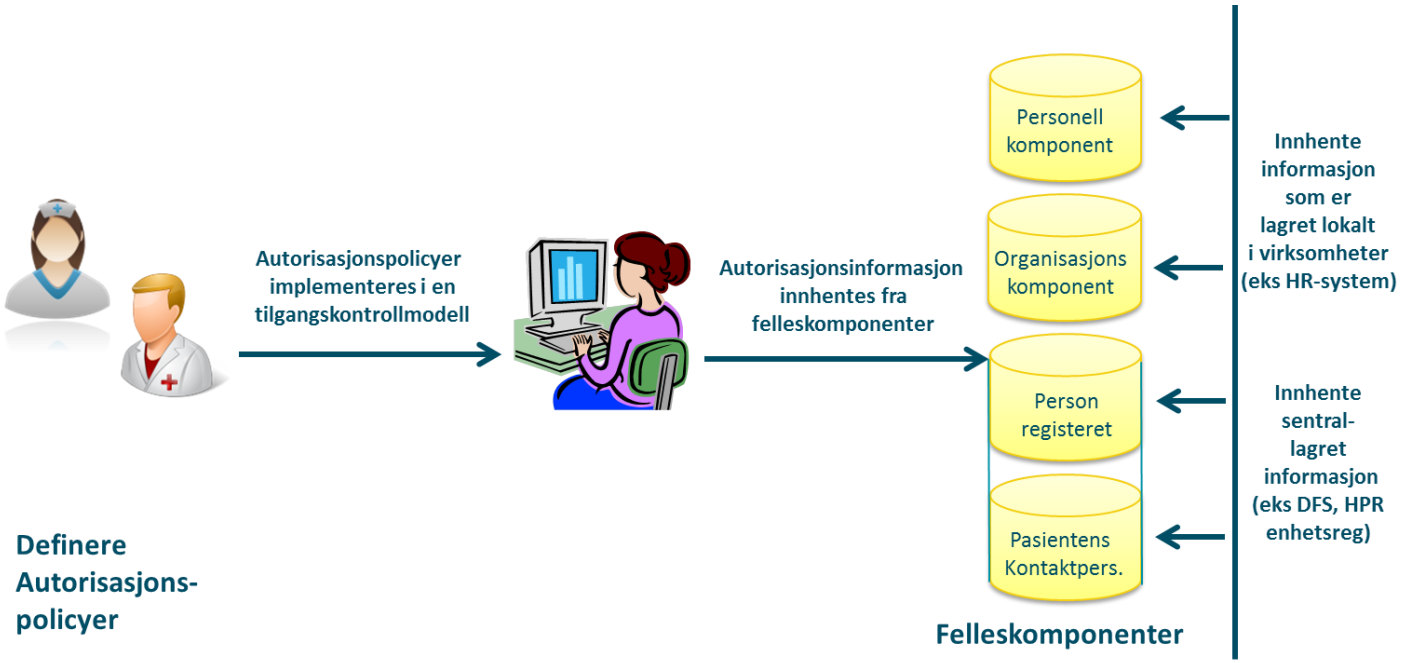
Autentisering forts.

Etablering av PKI basert eID

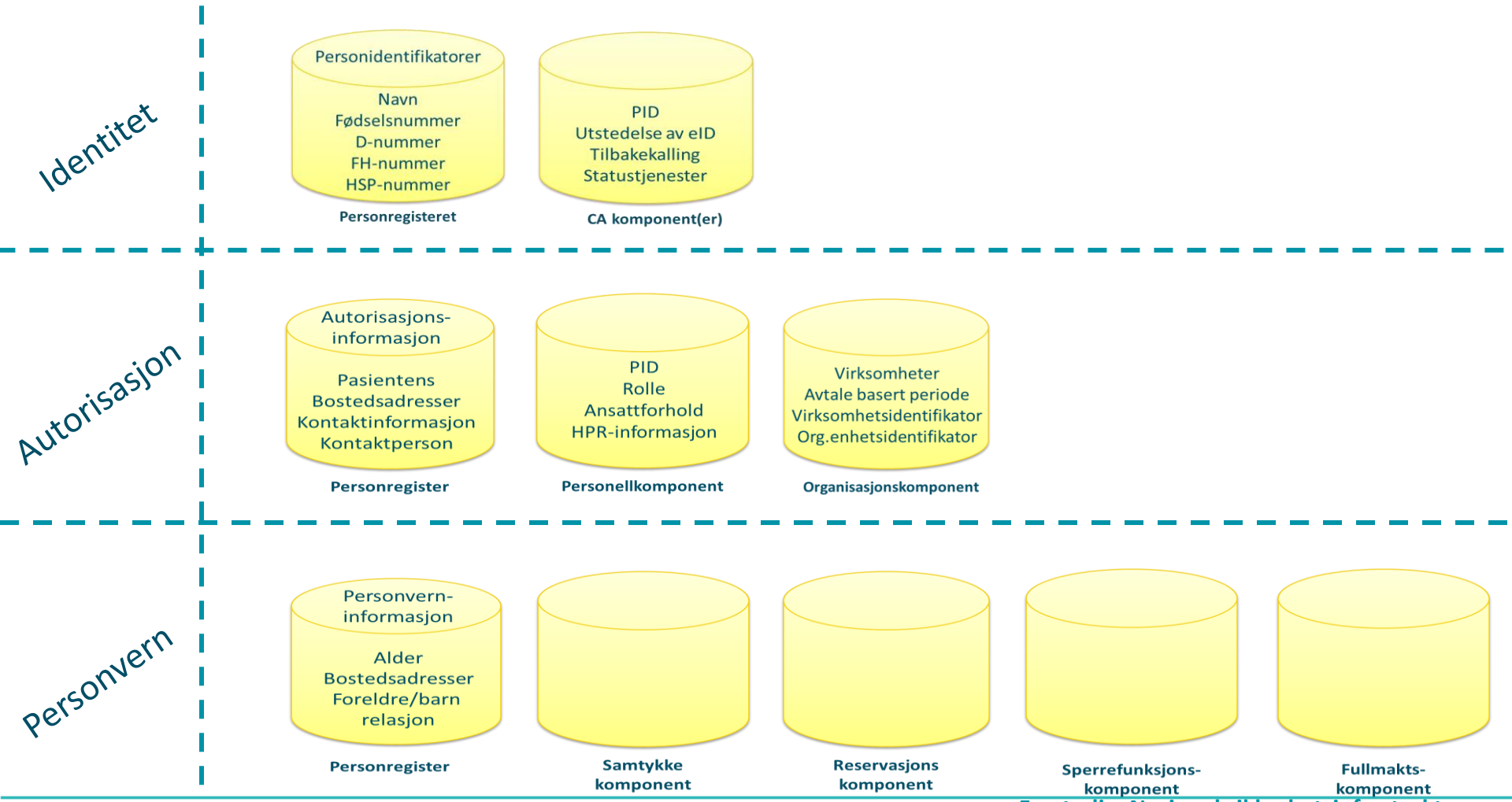


- Illustrasjon -

Autorisasjon



Komponenter for Identitets- og tilgangsstyring



Identifiserte områder fra forstudien

1. Komponenter for identitets- og tilgangsstyring
   - Personregister
   - CA
   - Personellkomponent
   - Organisasjonskomponent
   - Personvernkomponenter
2. Kravspesifikasjon for etablering av felleskomponenter
3. Konsekvensanalyse for de ulike autentiseringsnivåene
4. Vurdere samordning av PKI
5. Definere nasjonale autorisasjonspolicyer
6. Standardisere nasjonale roller

Takk for oppmerksomheten