Sykehuspartner | HELSE SØR-ØST

Bilag 3D
til vedlegg 5

Kundens tekniske plattform – Identitet og tilgangsstyring

Innovasjonspartnerskapet

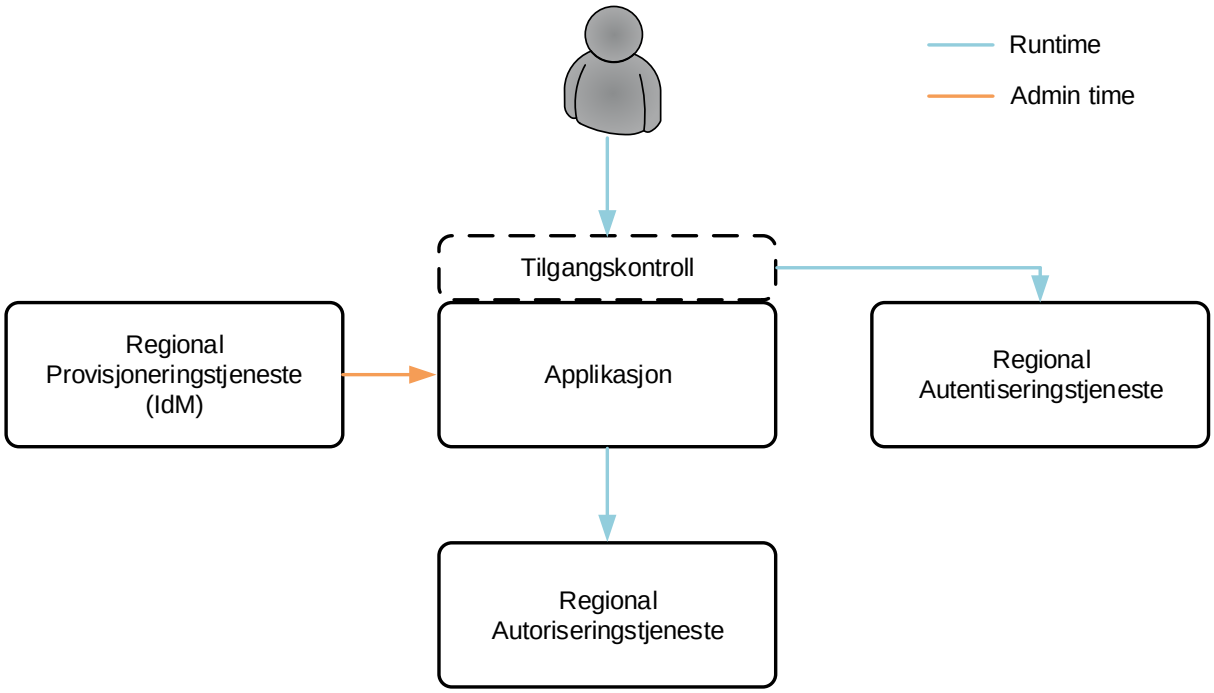
«Kontrolltårn for planlegging og gjennomføring av operasjoner på sykehus» i Oslo Universitetsykehus HF

Innholdsfortegnelse

1 Identitet og tilgangsstyring

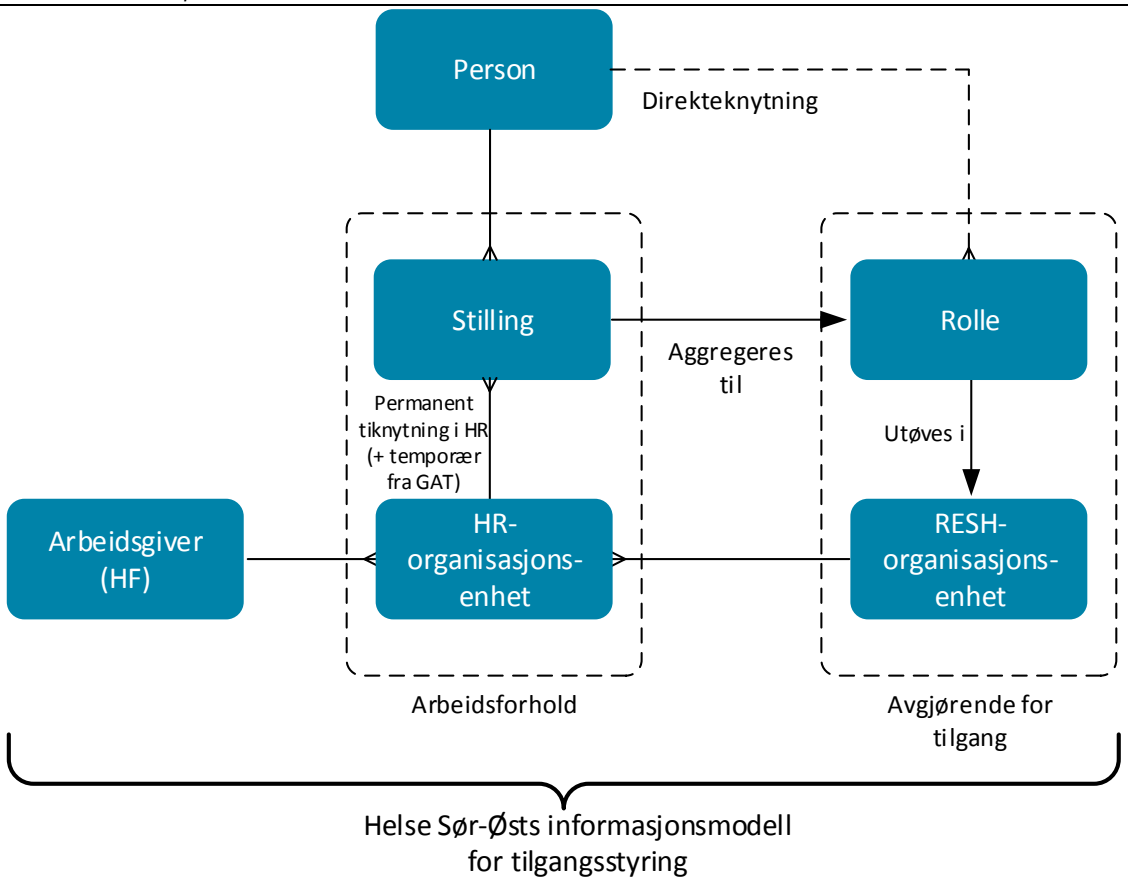
Identitet- og tilgangsstyring (IAM) i Helse Sør-Øst består av flere komponenter og tjenester, men de tre viktigste tjenestene er Regional Provisjoneringstjeneste, Regional Autentiseringstjeneste og Regional Autoriseringstjeneste. Disse tjenester er helt avhengige av og dermed integrert med autoritative informasjonskilder og prosesser.

Regional provisjoneringstjeneste benyttes til å provisjonere nødvendige brukerattributter til applikasjoner som har intern brukerdatabase. Applikasjonen håndterer selv brukersesjon mot applikasjonen og sørger for at bruker autentiserer seg med Regional Autentiseringstjeneste. Applikasjonen spør Regional autoriseringstjeneste om tilgang dersom intern tilgangskontrollmekanisme ikke kan avgjøre tilgang.



Figur 1, overordnet topologi - IAM for applikasjon

Helse Sør-Østs informasjonsmodell for tilgangsstyring baseres på personers arbeidsforhold (kan ha flere), aggregert/tilordnet rolle og organisasjonstilknytninger, hvor de to sistnevnte er avgjørende for tilgang.



Figur 2, informasjonsmodell for tilgangsstyring

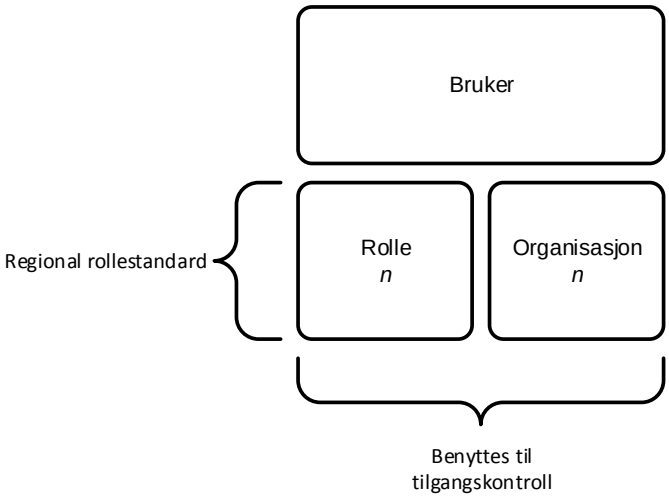
2 Regional provisjoneringstjeneste (IDM)

Dersom systemet/applikasjonen krever dedikert brukerdatabase må regional provisjoneringstjeneste benyttes for å administrere brukere og tildele tilganger i applikasjonen. Gitt det store antallet ansatte i Helse Sør-Øst er dette helt nødvendig for å automatisere og sentralisere brukeradministrasjonen. Det er en målsetning om å oppnå en automatiseringsgrad på 80% for tildeling av tilganger. Automatisering for fjerning av tilgang skal være tilnærmet 100%. Dette oppnås med at tjenesten er integrert med informasjonskilder beskrevet senere.

Regional provisjoneringstjeneste er en regional implementasjon av Quest One Identity Manager, som inneholder den sammenstilte metakatalogen med informasjon, regler (policy) og logikk for hvordan provisjonering av brukere foretas til applikasjonene. Eksempelvis AD og Exchange, men også kliniske applikasjoner som DIPS (EPJ) og Medikamentell Kreftbehandling (MKB).
REST-API basert på SCIM-standarden er foretrukket som provisjoneringsgrensesnitt.

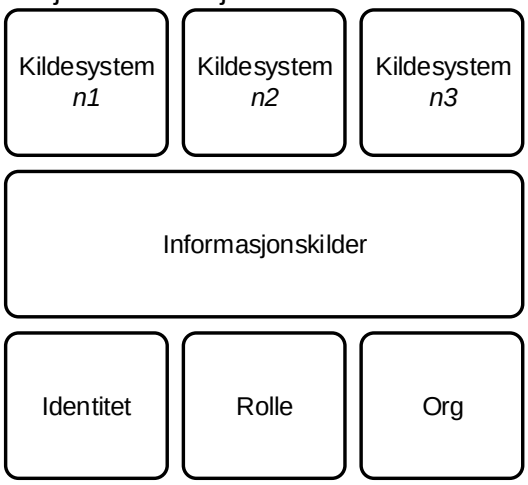
Applikasjonene benytter sammensetningen av tre forskjellige attributter for å gi tilgang til applikasjonen. Brukerident (brukerid), rolle (fra Regional rollestandard) og organisasjon (RESH) er de påkrevede attributtene for entydig identifisering av bruker.
Brukere tildeles én eller flere roller og org-tilknytninger i applikasjonen for å støtte at én og samme bruker kan ha flere arbeidsforhold og/eller roller i samme helseforetak (HF) eller på tvers av helseforetak. Merk at rolle og org-tilknytninger ikke aggregeres, hverken internt i samme HF eller

på tvers av HF. Bruker opptrer kun i én kontekst per sikkerhetssesjon. Det er mulighet for å gi brukere individuelle utvidede roller.



Figur 3, rolle og org

Informasjonskilder:
Viktige attributter for å muliggjøre provisjonering, autentisering og autorisering kommer fra ulike informasjonskilder. Informasjonskildesystemene er autoritative for sin informasjon og tilgjengeliggjør nødvendige attributter for IAM-tjenestene. Eksempel på slik informasjon er identitets-, rolle-, og organisasjonsinformasjon.



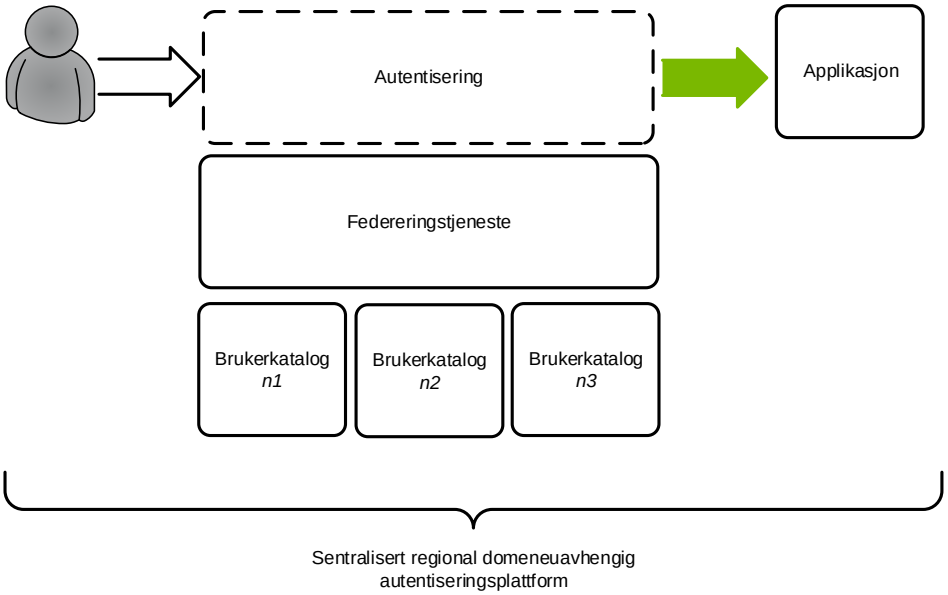
Figur 4, Informasjonskilder

Regional provisjoneringstjeneste benytter en rekke informasjonskilder for å innhente informasjon om ansatte og organisasjonsstruktur. Det regionale HR-systemet Personalportalen (PAGA) benyttes som primærkilde for ansattidentiteter i HSØ. Andre viktige informasjonskilder er de nasjonale registrene RESH (Register for enheter i spesialisthelsetjenesten) og HPR (Helsepersonellregisteret), og lokal installasjon av GAT (turnusplanlegging) på hvert enkelt helseforetak. Private/ideelle sykehus' HR-system er også en informasjonskilde som provisjoneringstjenesten benytter før de gis tilganger på regional plattform.

3 Regional autentiseringstjeneste (ID-FED)

Applikasjonene benytter Regional autentiseringstjeneste for autentisering. Løsningen er en sentralisert regional domeneuavhengig autentiseringsplattform som består av en federeringstjeneste. Dette muliggjør bruk av kun én brukerid på tvers av Helse Sør Østs

helseforetak, noe som øker kontrollen samtidig som det gir økt brukervennlighet -ingen behov for å huske flere brukerkontoer og passord samt muligheten for single sign-on. Kilde til autentisering er Active Directory internt, men autentisering av eksterne partnere og borgere gjøres basert på offentlig godkjent nivå 4-autentisering..



Figur 5, autentisering

Autentiseringstjenesten sørger for sikker overføring av identitetsinformasjon som støtter opp under Single Sign-On mot applikasjonene ved å utstede et sikkerhetstoken. Sikkerhetstokenet inneholder nødvendige attributter for å gi initiell autorisering til å bruke applikasjonen. Produktet som benyttes er PingFederate og standardene SAML og OpenID Connect støttes for federering.

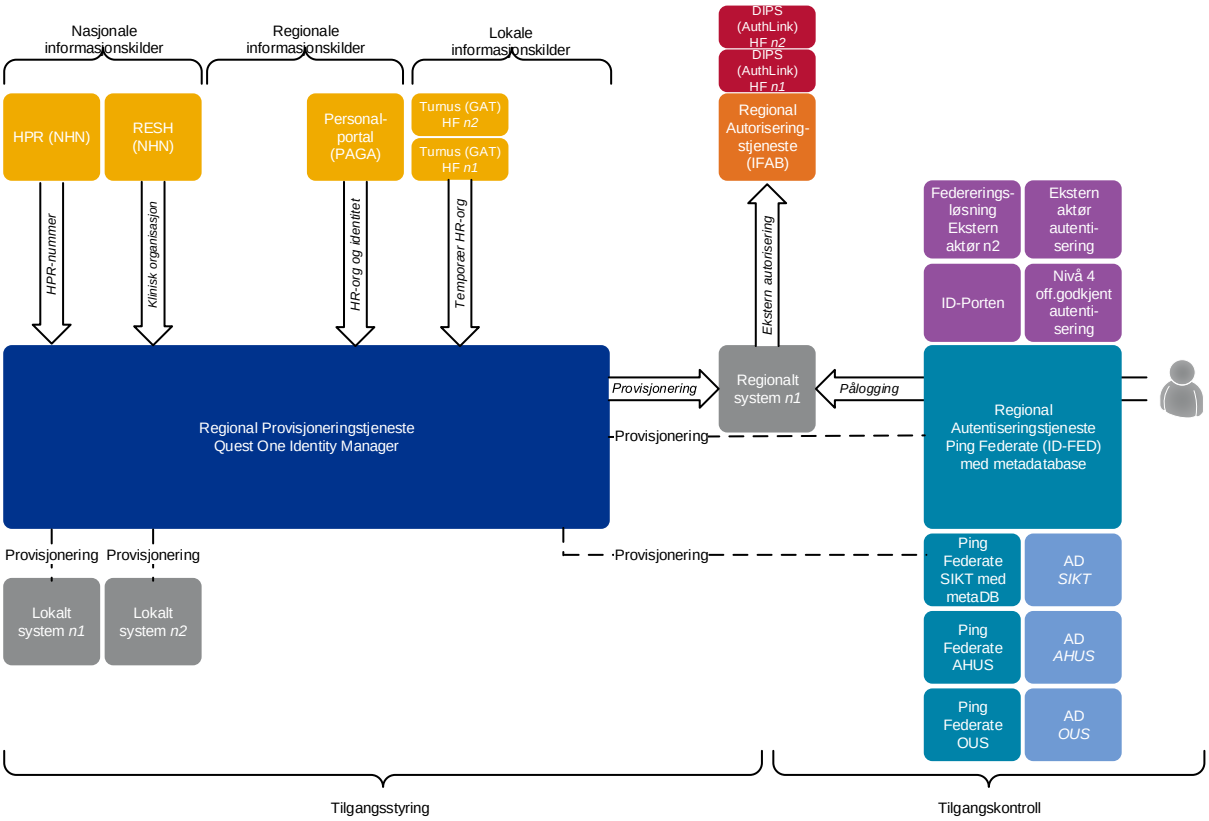
4 Regional Autoriseringstjeneste

For å etterleve sikkerhetskrav er autorisering nødvendig. Det er autoriseringen som avgjør hva sluttbruker får tilgang til i applikasjonen og systemet mht. funksjonalitet og data, eksempelvis hva sluttbruker kan utføre av arbeid (funksjoner) på hvilke pasienter (data).

Hver enkelt klinisk applikasjon gir selv implisitt tilgang til brukeren basert på valgt rolle og organisasjonstilknytning under pålogging og interne tilgangskontrollmekanismer (autorisering). Det er altså rollen og organisasjonstilknytningen som avgjør hva brukeren har implisitt tilgang til i en applikasjon. Det samme tilstrebes for administrative applikasjoner.

Dersom applikasjonen ikke kan avgjøre tilgang internt må Regional autoriseringstjeneste benyttes for å gi/avgjøre tilgang. Tjenesten er i dag en begrenset dynamisk autoriseringstjeneste basert på XACML for kliniske systemer som kan avgjøre om det finnes en aktiv behandler/pasient-relasjon for brukeren, gitt at pasienten er registrert i PAS/EPJ-systemet DIPS.

Komponentoversikt i figur:



Figur 6, IAM-komponentoversikt