HELSE NORD IKT

SSA T - Bilag 1 A – Formål og overordnet beskrivelse

Anskaffelse av løsning for IDM og SSO

Dato:

Innholdsfortegnelse

Ordliste/forkortelse 3
1. Oppbygning av kravspesifikasjonen 5
1.1 Struktur 5
1.2 Besvarelse av krav 5
2. Formål med anskaffelsen 6
3. Beskrivelse av nåsituasjon 6
3.1.1 Utfordringer i dagens situasjon 6
3.1.2 Teknologi som understøtter dagens situasjon 8
4. Beskrivelse av målbildet 9
4.1.1 Grunnplattform IAM 11
4.1.2 Selvbetjening av tilganger 11
4.2 Arkitektur 12
4.3 Integrasjoner og informasjonsutveksling 12

Ordliste/forkortelse

Nr.	Forkortelse	Forklaring
1.	BAS3	Brukeradministrasjonssystem versjon 3.
2.	Brukerident	En unik ID for brukeren.
3.	ClockWork	Innkjøps- og logistikksystem
4.	DIPS Classic	EPJ/PAS system
5.	DocMap	Kvalitetssystem/Prosedyre- og avvikssystem
6.	Elements	Sak- og arkivsystem som skal erstatte ePhorte.
7.	GAT	Ressursstyring- og arbeidstidssystem
8.	HelseID	Felles påloggingsløsning for ansatte i helsesektoren. Se https://www.nhn.no/helseid/
9.	Helsepersonellregisteret (HPR)	helsemyndighetenes nasjonale register over autorisert helsepersonell med autorisasjon eller lisens etter helsepersonelloven, og veterinærer og fiskehelsebiologer med autorisasjon eller lisens etter dyrehelsepersonelloven.
10.	HF	Helseforetak
11.	HN IKT	Helse Nord IKT
12.	Hovedidentitet	Den primære brukeridenten, i de tilfeller en bruker har flere brukeridenter.
13.	HPE Service Manager	IT Service Management system. Også kjent som GoHjelp blant sluttbrukere. Systemet leveres av Micro Focus.
14.	IAM	Identity and Access Management. I dette dokumentet brukt for å beskrive fagområdet
15.	IDM	Identity Management. I dette dokumentet brukt for å beskrive en delmengde av IAM-området.
16.	IDP	Identity Provider den som leverer/bekrefter bruker og identitet når en bruker aksesserer en SP
17.	Integrasjonstest	Integrasjonstesting utføres hos leverandøren for å bekrefte at moduler i ett system samspiller m.h.t krav og design.
18.	JWT	JSON Web Token
19.	Kildesystem	System som er kilde til informasjon.
20.	Latens (latency)	Ren nettverksmessig ventetid. For denne anskaffelsen skal latens måles i millisekund tur-retur.
21.	Leder	Leder med personalansvar. I enkelte tilfeller kan det være annen ansvarlig med delegert myndighet. F.eks. Avdelingsoverlege som har delegert myndighet til kontorleder eller HR/Personal-ressurser.
22.	Legacyapplikasjon	Tykk applikasjon som ikke har støtte for moderne token-basert SSO eller Windows Integrated Authentication.

23.	Medarbeider	Ansatt, sluttbruker, bruker, studenter, hospitanter, innleide osv. Alle som har en form for avtale i virksomheten.
24.	Målsystem	System som er mottaker av informasjon.
25.	Offboarding	Offboarding starter når leder mottar en melding om avslutning og slutter når medarbeider har sluttet.
26.	Onboarding	Onboarding starter når leder har valgt en ny medarbeider og slutter når medarbeider er produktiv.
27.	OU	Organisational Unit i MS Active Directory
28.	PAM	Privileged Access Management
29.	Personregisteret (PREG)	Helse- og omsorgssektorens kopi av det sentrale folkeregisteret
30.	RESH	Register over enheter i spesialisthelsetjenesten (RESH) inneholder det administrative organisasjonskartet for den statlige finansierte helsetjenesten i Norge.
31.	RHF	Regionalt Helseforetak
32.	Sectra RIS/PACS	Radiologisystem
33.	SP	Service Provider. Den som tilbyr en tjeneste som aksepterer innføderering av eksterne brukere.
34.	SSO	Single sign-on
35.	STS	Security Token Service, se http://en.wikipedia.org/wiki/Security_token_service
36.	Systemintegrasjonstest	Systemintegrasjonstest er en test der en tester at systemets integrasjoner mot andre systemer fungerer m.h.t krav og design. Utføres etter systemtest.
37.	Systemtest	Systemtest er en black box-test som utføres hos leverandøren for å verifisere at systemet fungerer m.h.t krav og design sett fra en brukers ståsted. Utføres etter integrasjonstest.

1. Oppbygning av kravspesifikasjonen

1.1 Struktur

Denne kravspesifikasjonen er delt inn i flere områder i den hensikt å gi tilbyderne mest mulig detaljert informasjon om de mål og krav oppdragsgiver har. Det er derfor satt opp informasjon om dagens situasjon/hva tilbyder kan legge til grunn for leveransen, en overordnet gjennomgang av ønsket fremtidig løsning, samt detaljerte krav basert på informasjon gitt i kapitlene om ønsket fremtidig løsning og standard krav for alle IKT-anskaffelser/prosjekter i Helse Nord IKT.

Kravspesifikasjonen består av 3 dokumenter:

- Bilag 1 A – Formål og overordnet beskrivelse (dette dokumentet)
- Bilag 1 B – Generelle krav for IKT anskaffelser i HNIKT
- Bilag 1 C – krav til løsningene som skal leveres (IDM og SSO)
    - Kapittel 1 og 2 er spesifikke krav til IDM
    - Kapittel 3 er spesifikke krav til SSO

Disse dokumentene inneholder alle informasjon og/eller kravpunkter som skal danne grunnlaget for tilbyders besvarelse. Vi forventer at tilbyder gir en utfyllende beskrivelse på alle krav som tilbyderen mener er viktig for vår beslutning og/eller som kan gi oss alternative perspektiver til de krav som er uttrykt i våre kravspesifikasjoner.

I Bilag 1 B og 1 C er det listet detaljerte krav i tabell, samt klassifisering. Alle krav skal besvares i henholdsvis SSA-T bilag 2 B og C, med mindre det eksplisitt er anvist at kravet skal besvares i andre kontraktsbilag.

Tjenester og ytelser knyttet til leveranse/implementering av løsning skal gis i SSA-T bilag 7 A, samt 7B og eller 7C – iht. de anvisninger som gis der.

1.2 Besvarelse av krav

Besvarelsens oppbygging og nummerering skal følge kravspesifikasjonens og kravteksten skal beholdes. Tilbyderen er selv ansvarlig for å beskrive alle nødvendige løsningselementer for å få en komplett beskrivelse av leveransen, selv om ikke alle disse skulle være kravsatt.

Der tilbyder f.eks. av plasshensyn ikke finner det hensiktsmessig å legge beskrivelser av løsninger og forbehold inn i selve kravtabellen, kan beskrivelsene utferdiges som vedlegg til det respektive bilaget. I så fall skal referanse til hvor beskrivelsene ligger gis i kravtabellen, og det skal i beskrivelsene klart fremkomme hvilket krav som utdypes.

2. Formål med anskaffelsen

Målet med anskaffelsen er å realisere grunnkomponenter innenfor et IAM-målbilde og sikre effektiv identitets- og tilgangsstyring, samt enkel og sikker pålogging for regionens brukere. Anskaffelsen legger opp til et leverandørstyrt implementeringsprosjekt av grunnplattform, samt provisjonering og SSO for et utvalg målsystemer.

Løsning for identitet og tilgangsstyring (IDM):

- Grunnplattform for identitet- og tilgangsstyring, integrert mot Bluegarden som kildesystem, samt mot Active Directory, med automatisk opprettelse av brukerkonto og standard tilganger og rettigheter (e-post, Skype, filområder og grupper).
- Løsning og endrede arbeidsprosesser som håndterer oppretting, provisjonering og tilbaketrekning av digitale identiteter og tilganger mot de administrative systemene Elements, Gat og DocMap og de kliniske systemene DIPS og Sectra.
- Løsning (selvbetjeningsportal) med prosess- og arbeidsflytstøtte for bestilling, orkestrering og håndtering av tilganger og utstyr, integrert mot Clockwork (utstyrsbestilling av PC og mobil) og HPE Service Manager (for tilganger som gis manuelt).

Løsning for enkel og sikker pålogging (Single Sign-On og federering):

- Løsning med støtte for autentisering og SSO av brukere i flere kanaler (web, nettverk/AD, mobil, nettbrett etc.) med ulike sikkerhetsnivå (SMS, smartkort, mobilapp etc.) tilpasset nasjonal autentiseringsløsning (Helse-ID).
- Løsning for SSO for regionale systemer; DIPS, Sectra og Bluegarden.

Implementeringsprosjektet skal ikke realisere det fulle IAM-målbildet angitt i kapittel 4, men i tillegg til realisering av grunnplattform og funksjonalitet for utvalgte målsystemer skal prosjektet legge til rette for at Helse Nord IKT i samarbeid med leverandør har et grunnlag for å realisere det totale målbildet på sikt, der så mange målsystemer som mulig benytter grunnplattformen.

3. Beskrivelse av nåsituasjon

Identitetshåndtering og tilgangsstyring handler om at rett person får tilgang til rett tjeneste til rett tid og sted.

3.1.1 Utfordringer i dagens situasjon

Kapittelet oppsummerer funnene fra kartleggingen av dagens prosesser knyttet til onboarding, endring og offboarding, som inkluderer identitets- og tilgangsstyring:

- **Manuell**
  Det er manuelle rutiner i dagens prosesser.
  - Ledere kan bestille tilganger og utstyr manuelt og ustrukturert i form av f.eks. e-post eller telefon.

- Systemspesifikke brukeradministratorer kan utføre manuelle rutiner ved oppretting, endring og sletting av brukerkonto og –tilganger.

- **Ressurskrevende**
  Det er ulike aktører involvert i dagens prosesser.
  - Systemspesifikke brukeradministratorer på de ulike helseforetakene (HF) som kan opprette, endre og slette brukerkonto og -tilganger i ulike applikasjoner.
  - Brukerstøtte i Helse Nord IKT som kan opprette, endre og slette brukerkonto- og tilganger i ulike applikasjoner.
  - Utstyrsadministratorer som kan registrere og utstede utstyr.
  - Øvrige administratorer som kan registrere informasjon i administrative systemer.
  - Ledere som kan sende bestillinger til de ulike aktørene, og følge opp gjennomføringen av bestillingene.
  - Medarbeidere som kan være mottaker og sluttbruker i prosessene.

- **Tidkrevende**
  Arbeidsflyt i dagens prosesser kan ta for lang tid.
  - Saksgang som kan være lang som en følge av mange aktører, manuelle rutiner og manglende oversikt.

- **Uoversiktlig**
  Det kan være manglende strukturert oversikt over oppgaver som skal utføres i dagens prosesser.
  - Helse Nord har manglende strukturert oversikt over identitets- og tilgangsstyring som ledere kan bruke ved bestilling av tilganger. Det kan ha ført til manglende oversikt over:
    - Antall henvendelser om brukeroppretting og –sletting
    - Hvilken informasjon som brukes ved oppretting av nye brukere
    - Antall systemspesifikke brukeradministratorer som oppretter og sletter brukere
    - Hvilke tilganger en bruker har totalt
  - Helse Nord har manglende strukturert oversikt over oppgavene som leder og medarbeider skal utføre i onboarding eller offboarding. F.eks. Bestille tilganger og utstyr.
  - Ledere kan ha utviklet egne huskelister, sjekklister osv. for å få en form for oversikt.
  - Dårlig oversikt kan føre til at ledere bruker mye tid på å purre på bestillingene.

- **Ad-hoc**
  Oppgavene i dagens prosesser kan utføres lite strukturert.

- Det kan være manglende prosesstøtte for ledere som er hovedansvarlig for prosessene.
- Oppgavene kan bli utført på ulike måter og ulike tidspunkter fra gang til gang.
- Det kan føre til større risiko for manglende eller forsinket utførelse av oppgavene.
- Medarbeidere kan ikke iverksette oppgaver selv i strukturert form (ingen selvbetjening).

I dag kan brukerkonto i Active Directory (AD) opprettes både før og samtidig som arbeidsavtale utarbeides, og dermed kan leder bestille nødvendige tilganger og utstyr før arbeidsavtale er signert.

Oppsummert tar det for lang tid før ny medarbeider har gjennomført onboarding som f.eks. nødvendige tilganger og utstyr. Det kan føre til at ny medarbeider ikke er produktiv raskt nok, og dårlig ressursutnyttelse for arbeidsgiver. I tillegg kan offboarding og sletting av tilganger være mangelfull, fordi det kan være like tungvint og motivasjonen er ikke like sterk som ved onboarding og oppretting av tilganger når leder ønsker medarbeider produktiv.

3.1.2 Teknologi som understøtter dagens situasjon

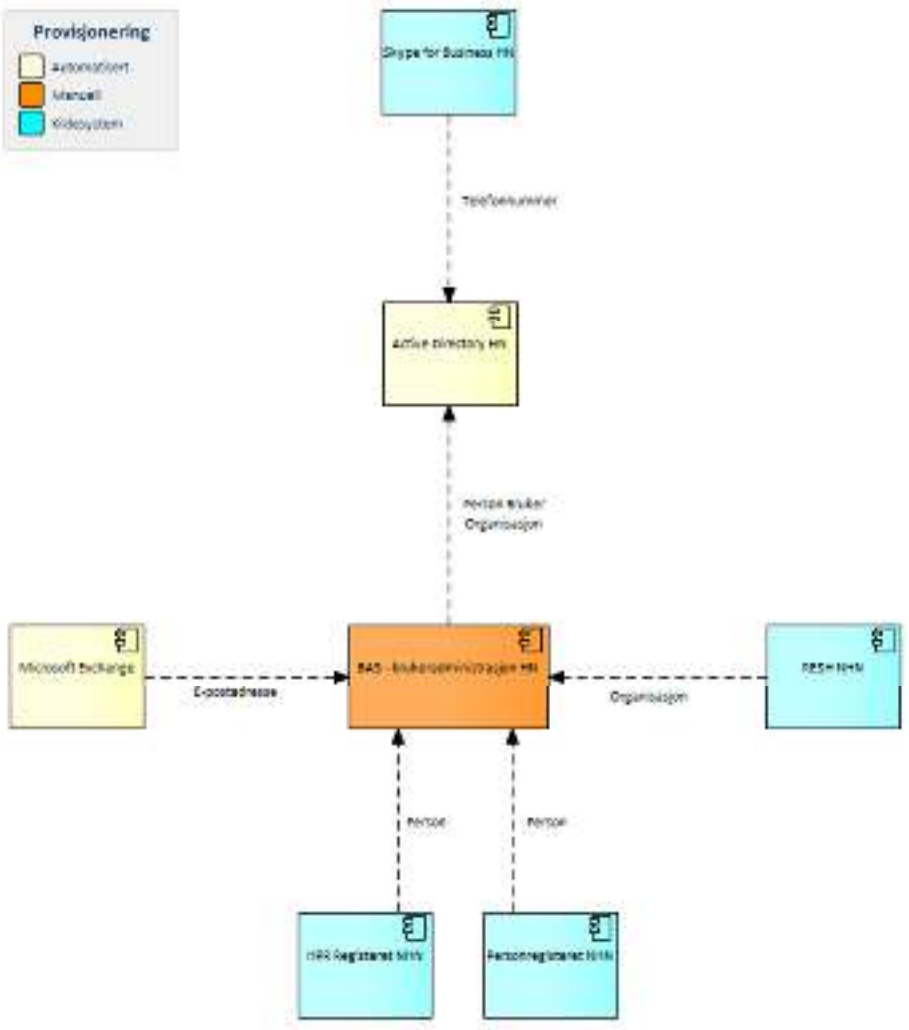
Dagens tilgangsstyring i Helse Nord er fragmentert og gjøres av flere ulike roller i mange forskjellige systemer i organisasjonen. Likevel er deler av prosessen sentralisert rundt et egenutviklet brukeradministrasjonssystem (BAS3) som forsyner AD med bruker- og tilgangsinformasjon. Tilgangen til dette systemet er distribuert ut til helseforetakenes ledere på klinikk- og avdelingsnivå som enten har påtatt seg rollen som brukeradministrator selv, eller delegert denne videre til annet personell. Det vil si at tilgang til Helse Nords domene samt enkelte IT-systemer styres gjennom denne løsningen og bestemmes av brukeradministratorer ute i organisasjonen. Løsningen er også integrert med Helse Nord IKTs saksbehandlingssystem (HPE Service Manager) slik at det for noen IT-systemer kan opprettes saker for opprettelse av brukerkontoer med tilhørende tilgang. Andre IT-systemer som hverken er automatisert eller saksbehandles gjennom BAS3, tilgangsstyres manuelt av superbrukere eller applikasjonsforvaltere i helseforetakene. Disse kontaktes via e-post eller telefon av brukeradministratorene for opprettelse og endring av tilgang til personell. Denne beskrivelsen gir et overordnet bilde av hvordan dagens tilgangsprosess fungerer. Systemene som er omtalt og listet under kan derfor omtales som sentrale i dagens tilgangsprosess:

- Active Directory (AD)
- Brukeradministrasjonssystem (BAS3)
- HPE Service Manager

I tillegg til AD og HPE Service Manager er BAS3 også integrert med Personregisteret, Helsepersonellregisteret, RESH-registeret, Microsoft Exchange og Skype. De to første

benyttes for å verifisere personopplysninger før det opprettes et brukerobjekt, RESH benyttes som organisasjonsmaster, Microsoft Exchange for å generere e-postkonto for brukeren samt aktivere Skype for business brukerkonto. I tillegg opprettes det også et hjemmeområde via integrasjon med filserver.

Figuren under illustrerer dataflyten mellom de sentrale systemene for tilgangsstyring.



Figur 1: Dataflyt mellom de sentrale komponentene for tilgangsstyring

4. Beskrivelse av målbildet

Det overordnede målbildet for IAM i Helse Nord gjengitt i Figur 2 er tatt fram for å kunne understøtte scenariene under. Anskaffelsen med tilhørende implementering vil være en viktig del av realisering av HN sin målarkitektur for IAM, men ikke dekke hele.

Realiseres delvis (systemspesifikt) som del av anskaffelsen:

- Tilgang til egne tjenester for eget personell

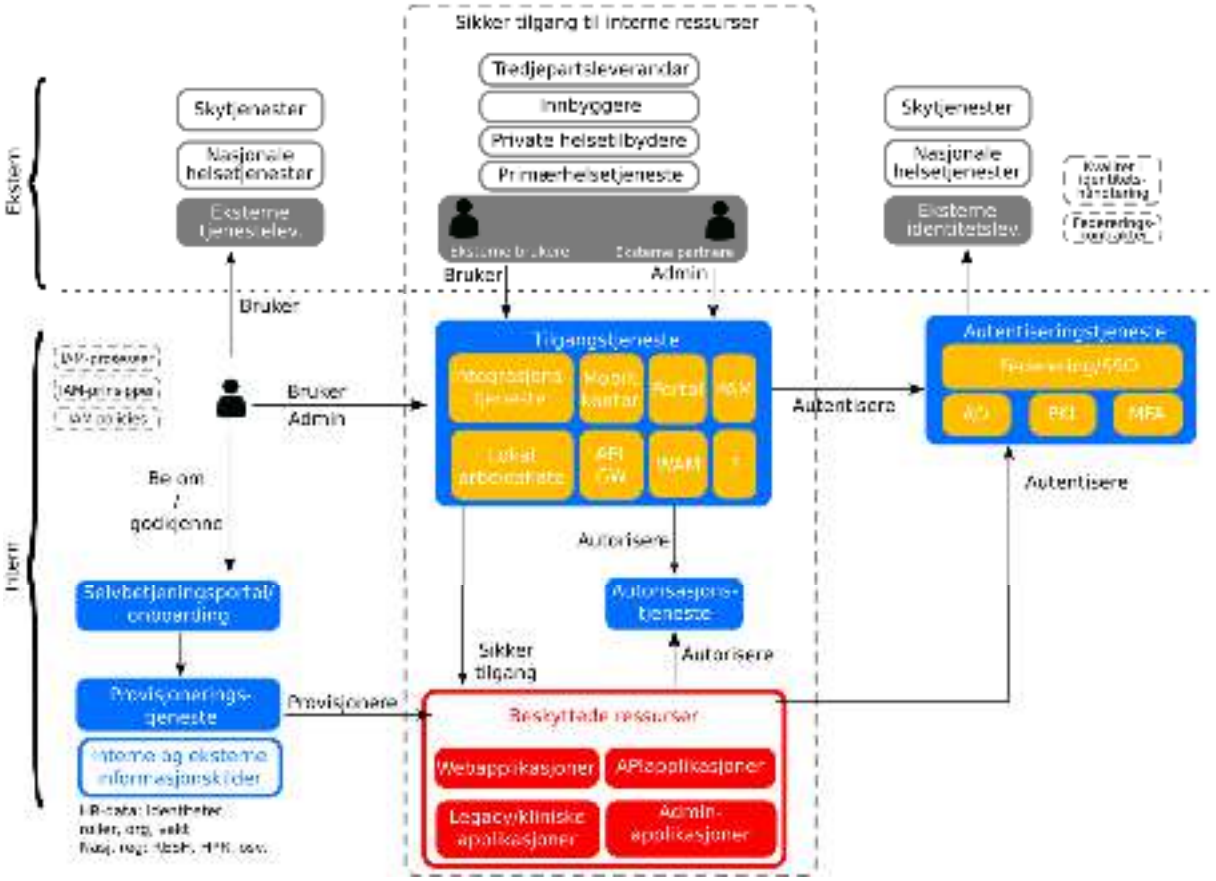
- Tilgang til egne tjenester for eget personell via mobil/smartenhet
- Selvbetjeningsportal for bestilling av tilgang
- Provisjonering av brukere og tilganger til HN-applikasjoner
- Tilgang til eksterne tjenester for egen regions personell
- Single sign-on

Realiseres senere, men basert på grunnplattformen som anskaffes:

- Fjernaksess for eget personell
- Tilgang til nasjonale tjenester for egen regions personell
- Tilgang til interne tjenester for personell fra andre deler av helsesektoren
- Tilgang til interne tjenester for innbyggere

Realiseres i parallell anskaffelse (PAM), med integrasjoner mot IDM

- Privilegerte tilganger for interne
- Leverandørtilgang



Figur 2: Målbilde IAM. Blå bokser er arkitekturbyggeklosser. Gule bokser er deltjenester som realiserer byggeklossene.

Anskaffelsen skal ikke dekke alle deler vist i Figur 2. Autorisasjonstjeneste er ikke omfattet, det samme gjelder Lokal arbeidsflate, API GW, Mobilt kontor, Integrasjonstjeneste, PAM (i parallell anskaffelse), Portal, AD og PKI.

Identitets- og tilgangsstyring er en viktig del av en helhetlig onboarding og offboarding av medarbeidere. Det er ønskelig å støtte opp og effektivisere flere av arbeidsprosessene ved onboarding og offboarding enn prosjektet skal realisere. Kort oppsummert innebærer fremtidsbildet at ledere og medarbeidere kan løse oppgaver og aktiviteter knyttet til onboarding og offboarding i én løsning/ett grensesnitt. Det krever fleksibilitet og integrasjoner mellom de ulike løsningene som skal gi sluttbrukerne én løsning/ett grensesnitt.

4.1.1 Grunnplattform IAM

IAM-plattformen er ment å være navet i identitetshåndtering og tilgangsstyring i HN. Autorativ informasjon om ansatte vil komme fra et utvalg systemer/registre, eksempelvis Bluegarden (Navn, fødselsnummer), AD (epostadresse, brukernavn), men gjøres tilgjengelig for andre systemer av IAM-plattformen. Dette vil foregå i form av provisjonering til systemlokale brukerdatabaser, men på sikt er målet at dette skal skje i form av standardiserte tokens. På sikt bør også autorisasjoner forvaltes av IAM-plattformen, selv om også disse kan ha sitt autoritative opphav i andre registre/systemer.

For brukerne skal det i størst mulig grad være sømløst om de aksesserer en lokal, regional, nasjonal eller ekstern tjeneste. Dette er tenkt løst ved hjelp av SSO og federering. Implementasjonsmessig vil dette måtte ta høyde for eksisterende systemer, slik at dette vil kunne være en blanding av ulike teknologier. For federering med andre deler av helsesektoren forutsettes bruk av Helse-ID. Her vil tilgang gå begge veier, helsepersonell fra andre helseregioner skal også kunne få tilgang til HN sine systemer. Innbyggeres tilgang til interne tjenester hos HN vil formidles av innbyggerportalen helsenorge.no, hvor ID Porten brukes som identitets- og autentiseringsløsning.

4.1.2 Selvbetjening av tilganger

En del av grunnplattformen for IAM er håndtering av identiteter, og opprette, endre og fjerne tilganger (både system- og fysiske tilganger). Dette skal provisjoneres ut gjennom provisjoneringsfunksjonaliteten i IAM-plattformen uten videre handlinger. Samtidig er det behov som ikke dekkes gjennom automatisert tilgangsstyring, men som kan dekkes gjennom selvbetjening uavhengig av IAM-løsningen.

For selvbetjening er målet at medarbeidere i størst mulig grad skal kunne håndtere behov for tilganger selv uten involvering av brukerstøtte, leder osv. En medarbeider skal kunne bestille tilganger uavhengig av om de provisjoneres automatisk eller manuelt. I tillegg må bestillingene kunne godkjennes av leder eller de(n) som forvalter de aktuelle

tilgangene. Medarbeideren skal kunne se hvilke bestillinger som er utført, status på bestillingene, purre på bestillingene, få varsler osv. Det skal også være mulig for medarbeideren å se hvilke tilganger de har til enhver tid. Slike funksjonaliteter skal også være mulig å bruke ved behov for utstyr knyttet til arbeidsforholdet som f.eks. PC, mobil og parkeringskort.

Ledere ønsker også støtte til og effektivisering av sine arbeidsoppgaver, og det er ønskelig at leder kan håndtere medarbeidernes behov for tilganger ut fra de samme prinsippene som beskrevet ovenfor. Dette vil være spesielt aktuelt i en preboardingfase hvor medarbeideren ikke vet sitt tilgangsbehov. En leder skal kunne bestille tilganger på en medarbeider både i egen og andres enheter. Leder skal også få en oversikt over hvilke tilganger medarbeidere har til enhver tid, og motta varsler på oppgaver som må følges opp av ulike årsaker.

Senere er det ønskelig å se nærmere på hvordan de resterende aspektene ved onboarding, f.eks. opplæring og personaldokumentasjon, kan effektiviseres gjennom større grad av selvbetjening.

4.2 Arkitektur

Regjeringen har, ved fremleggelsen av Digitaliseringsprogrammet – På nett med innbyggerne og St. meld nr. 19 (2008-2009) – Ei forvaltning for demokrati og fellesskap, besluttet syv overordnede IT-arkitekturprinsipper. Prinsippene skal fungere som et sett med felles retningslinjer for alt arbeid med IT i offentlig sektor.

Styret i Helse Nord RHF har vedtatt at Nasjonal IKT sine arkitekturprinsipper skal gjelde for hele regionen (styresak 66-2008). Arkitekturprinsippene som er vedtatt av HN IKT bygger derfor på Nasjonal IKTs prinsipper og er utformet slik at de ikke skal være i motstrid med prinsippene for offentlig sektor generelt, og helsesektoren spesielt, slik disse er formulert fra Difi og Helsedirektoratet. Prinsippene skal legges til grunn ved etablering av nye IT-løsninger eller ved vesentlige ombygginger av eksisterende IT-løsninger. Dersom prinsippene fører til vesentlige uønskede konsekvenser, kan de helt eller delvis fravikes. Slike avvik skal kunne forklares.

4.3 Integrasjoner og informasjonsutveksling

Helse Nord har etablert en tjenesteorientert arkitektur, basert på bl.a. sluttrapport Nasjonal IKT, fra Tiltak 12 – Nasjonal Systemarkitektur:" Tjenesteorientert arkitektur i spesialisthelsetjenesten", og understøttes også av arkitekturprinsippene, spesielt nr. 3 "Tjenesteorientering" og nr. 4 "Interoperabilitet".

Integrasjoner skal i størst mulig grad ta sikte på å følge de gjeldende prinsipper, og spesielt gjelder dette ved å etablere gjenbrukbare tjenester basert på standardiserte grensesnitt.