HELSE NORD IKT

SSA T – Bilag 1 C – Krav til løsningene

Anskaffelse av løsning for IDM og SSO

Dato:

Innholdsfortegnelse

Ordliste/forkortelser

Nr.	Forkortelse	Forklaring
1.	BAS3	Brukeradministrasjonssystem versjon 3.
2.	Brukerident	En unik ID for brukeren i en gitt applikasjon
3.	Campus	Campus er navnet på e-læringsplattformen som brukes ved alle helseforetakene i Helse Nord
4.	ClockWork	Innkjøps- og logistikksystem
5.	DIPS Classic	EPJ/PAS system
6.	D-nummer	11-sifret nummer som tildeles personer som ikke har fødselsnummer, men som trenger å bli oppført i Folkeregisteret, og som ikke skal registreres som bosatt i Norge.
7.	DocMap	Kvalitetssystem/Prosedyre- og avvikssystem
8.	Elements	Sak- og arkivsystem som skal erstatte ePhorte.
9.	GAT	Ressursstyring- og arbeidstidssystem
10.	HelseID	Felles påloggingsløsning for ansatte i helsesektoren. Se https://www.nhn.no/helseid/
11.	Helsepersonellregisteret (HPR)	Helsemyndighetenes nasjonale register over autorisert helsepersonell med autorisasjon eller lisens etter helsepersonelloven, og veterinærer og fiskehelsebiologer med autorisasjon eller lisens etter dyrehelsepersonelloven.
12.	HF	Helseforetak
13.	HN IKT	Helse Nord IKT
14.	Hovedidentitet	Den primære unike brukeridenten i IDM-løsningen, i de tilfeller en bruker har flere brukeridenter.
15.	HPE Service Manager	IT Service Management system. Også kjent som GoHjelp blant sluttbrukere. Systemet leveres av Micro Focus.
16.	IAM	Identity and Access Management. I dette dokumentet brukt for å beskrive fagområdet
17.	IDM	Identity Management. I dette dokumentet brukt for å beskrive en delmengde av IAM-området.
18.	IDP	Identity Provider. Den som leverer/bekrefter bruker og identitet når en bruker aksesserer en SP.
19.	Integrasjonstest	Integrasjonstesting utføres hos leverandøren for å bekrefte at moduler i ett system samspiller m.h.t krav og design.
20.	JWT	JSON Web Token
21.	Kildesystem	System som er kilde til informasjon for IAM-løsningen.
22.	Latens (latency)	Ren nettverksmessig ventetid. For denne anskaffelsen skal latens måles i millisekund tur-retur.
23.	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.

24.	Legacyapplikasjon	Tykk applikasjon som ikke har støtte for moderne token-basert SSO eller Windows Integrated Authentication.
25.	Medarbeider	Ansatt, sluttbruker, bruker, studenter, hospitanter, innleide osv. Alle som har en form for avtale i virksomheten.
26.	Målsystem	System som er mottaker av informasjon fra IAM-løsningen.
27.	Offboarding	Prosess for å sikre en effektiv avslutning av arbeidsforhold. Offboarding starter når leder mottar en melding om avslutning og slutter når medarbeider har sluttet.
28.	Onboarding	Prosess for å sikre en helhetlig mottakelse av alle nyansatte. Onboarding starter når leder har valgt en ny medarbeider og slutter når medarbeider er produktiv.
29.	OU	Organisational Unit i MS Active Directory
30.	PAM	Privileged Access Management
31.	Personregisteret (PREG)	Helse- og omsorgssektorens kopi av det sentrale folkeregisteret
32.	RESH	Register over enheter i spesialisthelsetjenesten (RESH) inneholder det administrative organisasjonskartet for den statlige finansierte helsetjenesten i Norge.
33.	RHF	Regionalt Helseforetak
34.	Sectra RIS/PACS	Radiologisystem
35.	SP	Service Provider. Den som tilbyr en tjeneste som aksepterer innfederering av eksterne brukere.
36.	SSO	Single sign-on
37.	STS	Security Token Service, se http://en.wikipedia.org/wiki/Security_token_service
38.	Systemintegrasjonstest	Systemintegrasjonstest er en test der en tester at systemets integrasjoner mot andre systemer fungerer m.h.t krav og design. Utføres etter systemtest.
39.	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.

0. Informasjon om kravtyper og utfylling

De oppstilte krav til leverandørens ytelser er beskrevet og klassifisert etter følgende standard:

Betegnelse	Forklaring
Krav	Dette er feltet der Kunden beskriver kravet tekstlig.
Kravtype	**Obligatoriske krav (O-krav) –** er absolutte krav som må være oppfylt for at tilbudet kan anses å tilfredsstille kravspesifikasjonen. Dersom et O-krav ikke er oppfylt vil tilbudet bli avvist. Disse kravene poengsettes ikke i evalueringen. **Obligatorisk krav (OE -krav)** er absolutte krav som må være oppfylt for at tilbudet kan anses å tilfredsstille kravspesifikasjonen. Dersom et OE-krav ikke er oppfylt vil tilbudet bli avvist. Tilbudet som oppfyller OE-kravet best vil få flest poeng. Obligatoriske krav angis av oppdragsgiver i kolonnen for "Krav-type" som «O» eller «OE». **Evalueringskrav (E-krav)** er ikke minstekrav. Tilbudets oppfyllelse av E-krav vil bli evaluert og det tilbudet som oppfyller E-kravet best vil få flest poeng. Evalueringskrav angis av oppdragsgiver i kolonnen for "Krav-type" som "E".

Beskriv (**B**)	Angir at Leverandøren i dokumentene for løsningsbeskrivelse, skal gi en utdypende beskrivelse av hvordan tilbudt løsning ivaretar kravet. For hvert krav som krever beskrivelse i Bilagene (angitt med B) skal det gis en utdypende beskrivelse av kravinnfrielsen i SSA T – Bilag 2 C eller i andre bilag der det er eksplisitt angitt.
Utfylling av Leverandørens tabellbesvarelse:	I Leverandørens tabellbesvarelse (SSA T - Bilag 2B og 2C) skal Leverandøren angi innfridde krav med bokstav J for JA eller Bokstav N for NEI. Kommentarfeltet kan også hvis ønskelig benyttes for å gi korte, supplerende opplysninger til avkrysningen.

0.1 Besvarelse av dette dokumentet

I dette dokumentet skal leverandørene fylle ut de krav som er relevant for sin leveranse. Dersom Leverandøren kun skal levere tilbud på delområde A (IDM) besvares Kapittel 1 og 2. Dersom leverandør kun skal levere tilbud på delområde B (SSO) besvares Kapittel 3. Dersom leverandør leverer tilbud på delområde C (IDM og SSO) må alle kapitel besvares.

1. Spesifikke krav for IDM

1.1 Funksjonell

1.1.1 Generelle krav

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
IDM-F1	Tilbudt løsning skal skalere til minimum 30.000 brukere, 300.000 andre enheter/objekter som f.eks. grupper og 100 integrasjoner mot eksterne datakilder.	O	B
IDM-F2	IDM-løsningen skal etablere og vedlikeholde en database bestående av brukerobjekter med attributter hentet fra autoritative kildesystemer. Databasen skal også inneholde data om Helse Nords organisasjonsenheter med tilhørende attributter. Denne databasen skal fungere som masterdatabase for målsystemer, slik at disse ikke henter informasjon direkte fra de autorative kildesystemene.	O	B
IDM-F3	Et målsystem skal kunne være autoritativt kildesystem for enkeltattributter. Det skal kunne settes opp logikk for hvilke attributter som hentes fra hvilke systemer.	O	B
IDM-F4	For brukere som ikke kan hentes fra et kildesystem, skal det opprettes et brukerobjekt med attributter direkte inn i masterdatabasen.	O	B
IDM-F5	IDM-løsningen skal være autorativ kilde for enkeltattributter og enkelttilganger i målsystemene ved at det i masterdatabasen på brukere og organisasjonsenheter, kan registreres og vedlikeholdes supplerende opplysninger som ikke er tilgjengelig fra andre kilder.	O	B

IDM-F6	Synkronisering av data mellom kilde- og målsystem som er satt opp i IDM-løsningen skal kunne stoppes/settes på vent og igangsettes igjen ved behov. En synkronisering satt til å kjøre i et bestemt tidsintervall skal kunne igangsettes manuelt ved behov.	O	B
IDM-F7	Det skal være mulig for Kunden å eksportere alle data som benyttes i IDM-løsningen. Tjenesten bør være automatiserbar og tilgjengelig i hele avtaleperioden. Beskriv hvilken eksportmetode Leverandøren tilbyr til bruk ved overføring av data til ny leverandør eller til Kunden.	OE	B
IDM-F8	Det bør være mulig for Kunden å importere data og konfigurasjon fra andre IDM-løsninger. Tjenesten bør være automatiserbar. Beskriv hvilken importmetode Leverandøren tilbyr til bruk ved overføring av data og konfigurasjon fra tidligere løsning/Leverandør.	E	B
IDM-F9	IDM-løsningen skal håndtere driftsstans som oppstår tilfeldig og utilsiktet mens en attributt-synkronisering pågår mot et eller flere målsystemer. Leverandøren bes beskrive hvordan uønskede konsekvenser av et slikt avbrudd for kilde- eller målsystemer som er tilknyttet IDM-løsningen kan reduseres.	OE	B
IDM-F10	IDM-løsningen skal på en enkel og sikker måte gi en ny bruker informasjon om brukernavn og passord for førstegangs pålogging til arbeidsflate/domene.	OE	B
IDM-F11	Det skal være mulig for en medarbeider å selv resette domenepassord på enkel og sikker måte, uten å være pålogget. Passordet skal leveres på en sikker måte.	OE	B

1.1.2 Livssyklushåndtering av identiteter

For å kunne automatisere mest mulig av administrasjon av brukertilgangene i Helse Nord er det nødvendig å få kontroll på brukeridentitetene i organisasjonen. I dette innbefattes det at alle formalia for å gi tilgang er i orden. Se vedlegg 1 «IAM Målarkitektur», kapittel 5.2.1 «Onboarding/enrollment» for mer informasjon.

Ved å sentralisere denne håndteringen kan det oppnås bedre kontroll på hvilke kontoer som tilhører hvilke medarbeidere, og sikre at alle kontoer som tilhører en medarbeider blir behandlet på en enhetlig måte. Dette er en forutsetning for å kunne ha kontroll over og styre medarbeideres tilgang til organisasjonens IT-systemer. Ved å koble disse kontoene sammen med informasjon om medarbeideren, som for eksempel startdato, sluttdato og hvilken enhet vedkommende er ansatt i vil man kunne automatisere en del av prosessene med tanke på opprettelse, endring og stenging av brukerkontoer. Man vil kunne sikre at kontoer automatisk blir opprettet i det en person starter å jobbe i organisasjonen, nødvendige endringer kan gjøres hvis arbeidsforholdet endrer seg, og kontoer kan deaktiveres i det en person slutter eller går ut i permisjon.

Sentralisering av denne håndteringen vil også føre til at informasjon som er duplisert ut i flere målsystemer er konsistent. Samtidig vil det ved å automatisere disse opprettelsene og endringene av brukerkontoer lette hverdagen for organisasjonens mange brukeradministratorer.

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
IDM-F12	En medarbeider skal ha samme brukeridentitet gjennom hele sin ansettelse, også ved "reansettelse" – dvs. at medarbeider har et ansattforhold og slutter for så å bli ansatt igjen på et senere tidspunkt.	O	
IDM-F13	IDM-løsningen skal ivareta at en brukeridentitet ikke kan gjenbrukes av nye medarbeidere.	O	
IDM-F14	Det skal være mulig å generere en brukeridentitet automatisk og sikre at denne ikke kolliderer med eksisterende brukeridentiteter i tilknyttede systemer. F.eks. første bokstav i fornavn, to første bokstaver i etternavn og et løpenummer fra en gitt verdi. IDM-løsningen skal støtte forskjellige navnestandarder for den digitale identiteten.	O	B

IDM-F15	IDM-løsningen skal håndtere endring av D-nummer, fødselsnummer og annet gyldig offisielt identifikasjonsnummer.	O	
IDM-F16	IDM-løsningen skal støtte flere brukeridentiteter pr. medarbeider og applikasjon. Disse brukeridentitetene må knyttes til en entydig hovedidentitet. Det skal være mulig å knytte hovedidentitet fra IDM-løsningen til de forskjellige lokale identitetene i målsystemene samt automatisk oppdatere disse når endringer forekommer.	O	B
IDM-F17	IDM-løsningen skal skille på forskjellige kategorier av brukere, f.eks. faste ansatte, vikarer og innleide konsulenter.	OE	B
IDM-F18	IDM-løsningen skal innhente opplysninger om nye eller eksisterende medarbeidere og organisasjonsenheter fra ulike autoritative kildesystemer. Leverandør bes beskrive de integrasjonsgrensesnitt IDM-løsningen støtter.	OE	B
IDM-F19	IDM-løsningen skal innhente opplysninger om nye eller eksisterende medarbeidere og organisasjonsenheter fra Bluegarden lønn og personalsystem gjennom et integrasjonsgrensesnitt. Grensesnittet skal etableres mot gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget	O	B
IDM-F20	IDM-løsningen skal støtte innhenting av opplysninger om vakter og fravær for medarbeidere fra GAT gjennom et integrasjonsgrensesnitt. Grensesnittet skal etableres mot gjeldende integrasjonsspesifikasjon for Helse Nord.	O	B

	Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget		
IDM-F21	IDM-løsningen skal støtte innhenting av folkeregisteropplysninger fra sentralt register gjennom et integrasjonsgrensesnitt. Grensesnittet skal etableres mot gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget	O	B
IDM-F22	IDM-løsningen skal støtte innhenting av opplysninger fra Helsepersonellregisteret gjennom et integrasjonsgrensesnitt. Grensesnittet skal etableres mot gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget	O	B
IDM-F23	IDM-løsningen skal støtte innhenting av organisasjonsopplysninger fra RESH gjennom et integrasjonsgrensesnitt. Grensesnittet skal etableres mot gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget	O	B

1.1.3 Forvaltning av roller og tilganger

For å kunne styre tilganger på en strukturert måte er det behov for å bygge opp en modell for tilgangskontroll i Helse Nord. En slik modell må kunne basere seg på roller som inngår i et rollehierarki. Dette vil si at det skal være mulig å etablere roller på flere nivåer som igjen er knyttet til tilgangsprofiler. Det skal ikke være nødvendig å etablere tilganger på alle nivåer, men rollene skal kunne arve rettigheter fra overliggende nivåer. I tillegg til roller skal tilganger også kunne gis med bakgrunn i andre attributter.

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)

IDM-F24	Det skal være mulig å bygge opp et rollehierarki der policyer og regler benyttes for å skape relasjoner og knytninger mellom roller.	O	B
IDM-F25	Det bør være mulig å visualisere hele rollemodellen med avhengigheter og tilganger.	E	B
IDM-F26	Det skal være mulig å opprette/endre/slette/aktivere/deaktivere roller og koble disse mot grupper og tilganger.	O	B
IDM-F27	Det skal være mulig å opprette/endre/slette/aktivere/deaktivere roller frem i tid og med start og sluttdato.	O	B
IDM-F28	Det skal være mulig for en rolleadministrator å tildele roller og tilganger til alle medarbeidere i en enhet eller gruppe av enheter.	O	B
IDM-F29	Det skal være mulig for en rolleadministrator å modellere roller uten at dette påvirker kjørende miljøer.	O	B
IDM-F30	Det bør være mulig for en rolleadministrator å versjonere og sammenligne endringer på roller.	E	B
IDM-F31	Det bør være mulig for en rolleadministrator å simulere nye roller i produksjonsmiljø, uten at dette påvirker kjørende systemer.	E	B
IDM-F32	Det bør være mulig for en rolleadministrator å migrere roller mellom produksjonsmiljø og testmiljøer, og rulle tilbake en migrering.	E	B
IDM-F33	Det skal være en søkefunksjon for roller som gir rolleadministrator mulighet for en god oversikt over roller og hva de gir av tilganger og relasjoner til andre roller.	OE	B
IDM-F34	Det bør være mulig å importere og eksportere rollemodell til/fra andre IDM-systemer gjennom et standardisert format.	E	B
IDM-F35	Tilgang for en bruker skal kunne kontrolleres gjennom andre attributter enn kun rolle. F.eks.	O	B

	at brukeren har vakt, pasientrelasjon, gyldig helsepersonellautorisasjon og lignende.		

1.1.4 Provisjonering av brukere og tilganger

Informasjon om brukere og tilganger knyttet til disse skal opprettes ett sted. Med bakgrunn i denne informasjonen skal en ved hjelp av en sentral enhet kunne opprette og endre brukerkontoer og tilganger i andre systemer. På denne måten oppnås det at informasjon om medarbeidere er konsistent og det legges til rette for å automatisere prosesser for tildeling av tilganger og rettigheter. Se vedlegg 1 «IAM målarkitektur», kapittel 5.2.5 «Provisjonering av brukere og tilganger til HN-applikasjoner» for mer informasjon.

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
IDM-F36	Medlemskap til en eller flere roller skal kunne tildeles manuelt eller automatisk utfra gitte attributter som f.eks. organisasjonstilhørighet og/eller stilling.	O	B
IDM-F37	Det skal være mulig å gi en medarbeider tilganger, f.eks. til et målsystem, filområde eller lignende, som ikke er basert på rolle.	O	
IDM-F38	Når en medarbeider tildeles eller mister en rolle eller tilganger generelt, skal IDM-løsningen sørge for at tilganger oppdateres i aktuelle målsystemer.	O	
IDM-F39	Når en medarbeider endrer stilling eller organisasjonstilhørighet, så skal alle roller og tilganger tilhørende stillingen automatisk trekkes tilbake samt nye tildeles.	O	
IDM-F40	En medarbeider skal ved registrert dato for fratredelse fra stilling automatisk miste de tilganger og rettigheter som følger av stilling og organisasjonstilhørighet.	O	
IDM-F41	IDM-løsningen skal håndtere at en medarbeider har flere ansettelsesforhold samtidig. F.eks. at en sykepleier har to ulike	OE	B

	arbeidsforhold (ulike stillinger) på to ulike avdelinger ved samme eller forskjellige juridisk enhet/helseforetak.		
IDM-F42	Det skal være mulig å utføre endring på identiteter og tilganger frem i tid. F.eks. å opprette brukere, deaktivere brukere eller tildele en tilgang som aktiveres eller deaktiveres ved en gitt dato.	O	
IDM-F43	Endringer av attributter eller logikk/regler i IDM-løsningen skal kontinuerlig behandles, og endringer skal umiddelbart leveres til målsystemene tilknyttet IDM-løsningen.	OE	B
IDM-F44	Det skal være mulig å ha brukerobjekter som ikke er kontrollert av IDM-løsningen. F.eks. brukere i Active Directory som ligger under en viss OU eller visse grupper.	O	B
IDM-F45	Automatisk tildeling av tilganger skal defineres og administreres sentralt på en brukervennlig måte. Leverandøren bes beskrive hva som kan ligge til grunn for automatisk tildeling av tilganger.	OE	B
IDM-F46	Provisjoneringsregler skal defineres og administreres sentralt på en brukervennlig måte, og det skal være mulig å sette gyldighetsperioder på dem.	OE	B
IDM-F47	Det bør være mulig å versjonskontrollere regler for provisjonering.	E	B
IDM-F48	Provisjoneringsregler skal kunne uttrykke komplekse sammenhenger mellom tilgangsattributtene i IDM-løsningen og tilgangene i målsystemene.	O	B
IDM-F49	Nye brukerobjekter skal provisjoneres til målsystemer når brukerobjektet inneholder de nødvendige attributter iht. oppsatte regler.	OE	B
IDM-F50	IDM-løsningen skal basert på oppsatte regler automatisk opprette brukerkonto, e-post,	O	B

	skypetilgang, hjemmeområde og gruppetilhørighet.		
IDM-F51	IDM-løsningen skal provisjonere til: • Microsoft Active Directory • Microsoft Exchange Provisjonering skal skje gjennom et standardisert integrasjonsgrensesnitt.	O	B
IDM-F52	Det bør være mulig å gjøre endringer utenfor IDM-systemet (både på objekter og attributter) i de provisjonerte målsystemene, uten at dette stopper provisjonering og uten at endringen overskrives med mindre dette er eksplisitt konfigurert.	E	B
IDM-F53	IDM-løsningen skal kunne provisjonere til Helse Nord sin DIPS-installasjon gjennom gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget.	O	B
IDM-F54	IDM-løsningen skal kunne provisjonere til Helse Nord sin Docmap-installasjon gjennom gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget.	O	B
IDM-F55	IDM-løsningen skal provisjonere til Helse Nord sin GAT-installasjon gjennom gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget.	O	B
IDM-F56	IDM-løsningen skal provisjonere til Helse Nord sin Sectra RIS/PACS installasjon gjennom gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget.	O	B
IDM-F57	IDM-løsningen skal provisjonere til Helse Nord sin Elements-installasjon gjennom gjeldende integrasjonsspesifikasjon for Helse Nord.	O	B

	Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget.		
IDM-F58	Det bør være mulig å provisjonere til den komplette og framtidige systemporteføljen til Helse Nord, utover de målsystemer som er eksplisitt nevnt andre steder. Provisjoneringen bør skje gjennom standardiserte grensesnitt.	E	B
IDM-F59	Det skal være mulig å hente ut alle brukere eller utvalgte brukere fra et målsystem for å synkronisere opp mot IDM-brukerbase (reconciliation).	O	B
IDM-F60	IDM-løsningen skal gjennom provisjonering støtte funksjonalitet som opprette, endre, deaktivere og aktivere brukerkontoer, samt sette passord i målsystemer. Leverandøren bes beskrive den funksjonaliteten som IDM-løsningen kan tilby i forbindelse med provisjonering.	O	B
IDM-F61	IDM-løsningen bør kunne provisjonere til Microsoft Azure Active Directory.	E	B
IDM-F62	Det bør være mulig å kjøre script som en del av provisjonering. Scriptet bør kunne gi status tilbake til IDM-løsningen.	E	B

1.1.5 Sette opp arbeidsflyt

Prosesser for identitets- og tilgangsstyring skal kunne uttrykkes som arbeidsflyt (workflow). Målet er å ha fleksibilitet til å sette opp og tilpasse arbeidsflyt på en enkel og sikker måte i IDM-løsningen, og at arbeidsflyt er mest mulig hensiktsmessig i forhold til arbeidsprosessene i Helse Nord.

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
IDM-F63	En arbeidsflyt skal kunne bestå av både automatiserte og manuelle oppgaver som kan	O	

	settes opp til å bli utført i en bestemt rekkefølge.		
IDM-F64	Det skal være mulig å opprette arbeidsflyt i henhold til Kundens arbeidsprosesser. Det skal være mulig å skreddersy arbeidsflyt pr. enhet/foretak.	O	B
IDM-F65	Det skal være mulig å definere og administrere arbeidsflyt sentralt på en brukervennlig måte, og det skal være mulig å sette gyldighetsperioder på dem.	OE	B
IDM-F66	Det bør være mulig å versjonskontrollere arbeidsflyt.	E	B
IDM-F67	Det skal være mulig å starte en arbeidsflyt basert på både regel- og hendelsesstyrt endring (f.eks. endring i autorative kildesystemer eller manuell tildeling).	O	B
IDM-F68	Det bør være mulig å starte en arbeidsflyt for revisjon av tilganger som er gitt til medarbeidere ved en enhet. Arbeidsflyten bør også støtte kvittering av utført revisjon.	E	B
IDM-F69	IDM-løsningen bør støtte purring og eskalering på oppgaver i en arbeidsflyt.	E	B
IDM-F70	Tildeling av en rolle eller tilgang skal kunne ha flere godkjenningsinstanser før den iverksettes. En godkjenningsinstans skal kunne bestå av én eller flere ansatte som har ansvar for godkjenning av tilgang innen et funksjonsområde. Evt. kan godkjenning skje automatisk om visse kriterier er oppfylt.	O	B
IDM-F71	Det skal være mulig å gi varsler som en del av en arbeidsflyt basert på regelstyrte eller hendelsesstyrte prosesser. F.eks. at en medarbeider slutter eller endrer stilling. Innhold og formatering av meldingen skal kunne tilpasses enhet/rolle brukeren er	OE	B

	tilknyttet og de ulike system brukeren har fått tilgang til. Leverandør bes beskrive hvordan slike meldinger tilpasses og formidles, og hvilke leveringsmekanismer for varsler som støttes.		
IDM-F72	Det skal være mulig å sende e-poster som en del av en arbeidsflyt basert på regelstyrte eller hendelsesstyrte prosesser.	OE	B
IDM-F73	Det bør være mulig å definere variabler som kan brukes fortløpende i arbeidsflyten, f.eks. for skreddersøm av innhold i e-post og varsler.	E	B
IDM-F74	Det bør være mulig å sende varsler til en medarbeider som ikke har en aktiv brukerkonto.	E	B
IDM-F75	IDM-løsningen bør kunne varsle om uregelmessigheter og avvik, f.eks. utgått HPR-autorisasjon.	E	B

1.1.6 Logging

Sporing på brukernivå gjennom alle lag i systemet er viktig for å kunne se hvem som har vært inne når og hva som har blitt gjort. Det skal for alle vesentlige hendelser være mulig å identifisere tidspunkt, identitet og hva som er utført. Både vellykkede og mislykkede påloggingsforsøk, leseoperasjoner og endringer skal logges. Loggen skal gi tilstrekkelig informasjon til å følge opp sikkerhetsbrudd.

Nr.	**Krav**	**Kravtype (O/OE/E)**	**Beskriv (B)**
IDM-F76	Det skal være mulig å logge alle hendelser i IDM-løsningen. Det skal være mulig å logge hvem som har utført hva og når det ble gjort. F.eks. endring i tildelt rolle, tilganger, endringer i IDM-oppsettet, rollemodeller og forsyningsregler, samt mislykkede forsøk på pålogging og endring av informasjon.	O	B

IDM-F77	Loggene skal være tilgjengelig i IDM-verktøyet for enkelt å kunne presenteres i et brukergrensesnitt eller i rapporter.	OE	B
IDM-F78	Det skal være mulig å oppdage, rapportere og håndtere uautoriserte og uvanlige endringer i de forsynte systemene og sette i gang en arbeidsprosess basert på denne hendelsen, f. eks. generere en alarm.	OE	B
IDM-F79	All av- og pålogging til IDM-løsningen bør logges med brukerident, klient-IP, tidspunkt og handling. Leverandør bes beskrive hvordan dette ivaretas.	E	B

1.1.7 Rapportering

Det er behov for en rapporteringsmodul som skal brukes til generering av rapporter og presentasjon av informasjon om brukere og tilganger. Informasjon skal kunne vises i et web-grensesnitt, sendes til utskrift og/eller eksporteres i forskjellig format. Det er også behov for et fleksibelt søk, og en sorteringsfunksjon som for eksempel gjør det mulig å søke på personressurser/enheter eller tilganger.

Rapporteringssystemet skal være fleksibelt, og det skal være mulig å lage nye rapporter eller endre på eksisterende rapporter. En generert rapport må kunne lagres og brukes ved f.eks. senere analyser om hvordan tilgangsstyringen håndheves.

Nr.	**Krav**	**Kravtype (O/OE/E)**	**Beskriv (B)**
IDM-F80	Det skal være rapporteringsfunksjonalitet i IDM-løsningen. Leverandøren bes beskrive hvilke standardrapporter og tilpasningsmuligheter som leveres.	OE	B
IDM-F81	Det skal være mulig å eksportere data til Helse Nord sitt datavarehus (SAS) for bruk til virksomhetsrapportering.	O	B

IDM-F82	Det skal være et web-grensesnitt hvor rapporter kan genereres, vises, distribueres, eksporteres til PDF, og skrives ut. Leverandøren bes beskrive hvilke målplattformer som støttes av web-grensesnittet, og hvorvidt web-grensesnittet benytter spesiell teknologi (f.eks. plugins) som begrenser kryssplattformstøtte.	OE	B

1.1.8 Selvbetjeningsportal

Medarbeidere og ledere i Helse Nord har behov for en brukervennlig og prosesstøttende selvbetjeningsportal under on- og offboarding av medarbeidere, samt for å håndtere endringer (f.eks. endret tilgangsbehov) i løpet av et arbeidsforhold. Leder og medarbeider ønsker blant annet å tildele, fjerne, bestille og avbestille tilganger og utstyr, få oversikt over tilganger, følge opp bestillinger og oppgaver osv. Selvbetjeningsfunksjonalitet skal kunne knyttes til arbeidsflyt som skal være enkel å sette opp og tilpasse.

Se også kapittel 5.2.4 «Selvbetjeningsportal for bestilling av tilgang», kapittel 5.2.1 «Onboarding/enrollment» og kapittel 6.4 «Selvbetjeningsportal/onboarding» i vedlegg 1 «IAM målarkitektur».

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
IDM-F83	Det skal være mulig å administrere hvilke roller og tilganger som skal være tilgjengelige for forskjellige typer sluttbrukere i selvbetjeningsportalen.	O	B
IDM-F84	Det skal være mulig å endre utvalgte attributter i sin brukerprofil selv i selvbetjeningsportalen.	O	
IDM-F85	Selvbetjeningsportalen skal støtte autentisering av bruker gjennom Single Sign-On (SSO).	O	
IDM-F86	Selvbetjeningsportalen bør være tilgjengelig på internett, og det bør være mulig å autentisere seg mot selvbetjeningsportalen ved hjelp av ID-portens sikre autentiseringsmekanismer.	E	B

	Når medarbeideren logger på selvbetjeningsportalen før startdato skal man få tilgang til en begrenset del for å utføre definerte oppgaver. Når medarbeideren logger på selvbetjeningsportalen etter startdato skal aktivitet som er utført før startdato inkluderes i selvbetjeningsportalen.		
IDM-F87	Det skal være mulig å integrere funksjonalitet fra andre systemer i selvbetjeningsportalen. Se case 7 i kap. 3.1.7. for mer informasjon.	O	B
IDM-F88	Det skal være mulig å gjenbruke funksjonalitet i selvbetjeningsportalen i andre systemer/portaler. Se case 7 i kap. 3.1.7. for mer informasjon.	O	B
IDM-F89	Brukergrensesnitt til selvbetjeningsportalen skal kunne utformes med Helse Nord sin profil uten at tilpasningene forsvinner ved oppgradering. Det skal også være enkelt å tilpasse uten hjelp fra leverandør.	OE	B
IDM-F90	Det skal være mulig å integrere arbeidsflyt som spesifisert i kapittel 1.1.5 i selvbetjeningsportalen, f.eks. godkjenne en bestilling.	OE	B

1.1.8.1 Brukerfunksjonalitet

Leder og medarbeider har ulike behov for funksjonalitet i selvbetjeningsportalen, og det er ønskelig å definere ulik brukerfunksjonalitet for ulike brukere. En medarbeider ønsker størst mulig grad av selvbetjening og oversikt, og en leder ønsker i tillegg å utføre oppgaver og brukeradministrasjon på sine medarbeidere.

Nr.	**Krav**	**Kravtype (O/OE/E)**	**Beskriv (B)**
IDM-F91	Det skal være mulig for medarbeider å få oversikt over egne:	OE	B

	• Brukerkontoer og tilganger i ulike fagapplikasjoner. • Utstyr som er bestilt via selvbetjeningsportalen. • Oppgaver, tilganger og utstyr som er i ferd med å gå ut på dato/tid. • Brukerprofil (F.eks. personalia). • Overordnet og detaljerte oversikt over bestillinger som er under behandling.		
IDM-F92	Det skal være mulig for leder å få oversikt over medarbeidere som er knyttet til sin enhet i selvbetjeningsportalen.	OE	B
IDM-F93	Det skal være mulig for leder å få oversikt over følgende i selvbetjeningsportalen: • Aktive brukerkontoer og tilganger på medarbeidere. • Tildelt utstyr på medarbeider. • Oppgaver, tilganger og utstyr som er i ferd med å gå ut på dato/tid. • Overordnet og detaljert oversikt over bestillinger som er under behandling på medarbeidere.	OE	B
IDM-F94	Det skal være mulig for leder å delegere oppgaver i selvbetjeningsportalen til en stedfortreder eller andre.	O	B
IDM-F95	Det bør være mulig for leder å få oversikt over felles regionale oppgaver som medarbeider må utføre i forbindelse med onboarding og offboarding.	E	B
IDM-F96	Det bør være mulig for leder å legge til oppgaver på medarbeidere i forbindelse med onboarding og offboarding både før og etter startdato.	E	B

1.1.8.2 Tildele og fjerne tilganger og utstyr

Helse Nord har som mål å i størst mulig grad automatisere tildeling og tilbaketrekking av tilganger og utstyr via IDM-løsningen. Samtidig er det behov for å tilrettelegge for funksjonalitet i selvbetjeningsportalen slik at leder på vegne av medarbeider og

medarbeideren selv kan tildele tilganger og utstyr. I tillegg skal det være mulig å fjerne tilganger og avbestille utstyr dersom disse ikke lengre anses som nødvendig for medarbeideren. Dette forutsetter at det er mulig å definere hvilke tilganger og utstyr som leder og medarbeider kan administrere via portalen.

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
IDM-F97	Det skal være mulig for medarbeider å selv tildele og fjerne tilganger der det er definert som mulig.	O	B
IDM-F98	Det bør være mulig for medarbeider å selv tildele og fjerne utstyr der det er definert som mulig.	E	B
IDM-F99	Det skal være mulig for leder å tildele roller og tilganger som er relevant for sin enhet.	O	B
IDM-F100	Det bør være mulig for leder å tildele utstyr som er relevant for sin enhet.	E	B
IDM-F101	Det skal være mulig for leder å tildele og fjerne tilganger til medarbeidere i sin enhet.	O	B
IDM-F102	Det bør være mulig for leder å tildele og fjerne utstyr til medarbeidere i sin enhet.	E	B
IDM-F103	Det skal være mulig for leder å søke opp medarbeidere i andre enheter, og tildele og fjerne tilganger på dem som er tilknyttet enheten som leder har ansvar for.	O	B
IDM-F104	Det bør være mulig for leder å søke opp medarbeidere i andre enheter, og tildele og fjerne utstyr på dem som er tilknyttet enheten som leder har ansvar for.	E	B

1.1.8.3 Bestille tilganger og utstyr

Helse Nord har som mål å i størst mulig grad automatisere tildeling og tilbaketrekking av tilganger og utstyr, samt legge til rette for selvbetjent tildeling og tilbaketrekking av tilganger og utstyr. Samtidig er det behov for å ha en bestillingsfunksjonalitet i

selvbetjeningsportalen som kan håndtere bestillinger som ikke lar seg automatisere av IDM-løsningen eller direkte tildeles av lederen og medarbeideren selv. F.eks. vil det fortsatt være systemspesifikke brukeradministratorer på de ulike helseforetakene som må opprette, endre og stenge brukerkontoer med tilhørende tilganger manuelt i de ulike fagsystemene.

Medarbeider og leder (på vegne av medarbeider) skal kunne utføre en bestilling, se status og sende purringer på bestillingen. Det skal også være mulig å få opp informasjon om hva en tilgang betyr, som støtte for medarbeideren og lederen ved bestilling.

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
IDM-F105	Det skal være mulig for medarbeider å bestille eller avbestille tilganger. Det skal være mulig å bestille tilganger for en tidsbegrenset periode.	O	B
IDM-F106	Det bør være mulig for medarbeider å bestille eller avbestille utstyr. Det bør være mulig å bestille utstyr for en tidsbegrenset periode.	E	B
IDM-F107	Det skal være mulig for leder å bestille og avbestille tilganger til en medarbeider. Det skal være mulig å bestille tilganger for en tidsbegrenset periode.	O	B
IDM-F108	Det bør være mulig for leder å bestille og avbestille utstyr til en medarbeider. Det bør være mulig å bestille utstyr for en tidsbegrenset periode.	E	B
IDM-F109	Det skal være mulig for leder å godkjenne eller avvise bestillinger fra en medarbeider.	O	B
IDM-F110	Det bør være mulig å legge inn en kommentar (fritekst) når en bestilling opprettes, godkjennes eller avvises.	E	B
IDM-F111	Det skal være mulig å spesifisere om en bestilling av tilgang krever en begrunnelse eller ikke.	O	B
IDM-F112	Det skal være mulig å purre på bestillinger.	O	B

IDM-F113	Det skal være mulig å informere involverte ressurser automatisk når en bestilling endrer status.	O	B
IDM-F114	Det skal være mulig å informere involverte ressurser når en rolle eller tilgang aktiveres eller deaktiveres.	O	B
IDM-F115	Det bør være mulig å informere involverte ressurser når utstyr er klar for utlevering.	E	B
IDM-F116	Det skal være mulig å definere skjema for manuell tilgangs- og utstyrsbestilling som kan sendes pr. e-post eller som sak i saksbehandlingssystemet til behandling.	O	B
IDM-F117	Det bør være mulig å overlevere nytt brukernavn og passord til fagapplikasjoner som ikke er integrert med IDM-løsningen på en sikker måte.	E	B
IDM-F118	Det bør være mulig for en medarbeider å sperre innlogging for sin hovedidentitet selv (f.eks. ved mistanke om passord eller MFA-token på avveie).	E	B
IDM-F119	Det bør være mulig for en medarbeider å endre domenepassord selv på en enkel måte når medarbeideren er pålogget.	E	B
IDM-F120	Det bør være mulig for medarbeider å bestille resetting av passord til fagapplikasjoner som ikke er integrert med IDM-løsningen på en enkel måte. Passordet bør overleveres på en sikker måte.	E	B
IDM-F121	Det bør være mulig å kvittere ut manuelle tilgangs- og utstyrsbestillinger slik at man kan se status i selvbetjeningsportalen.	E	B
IDM-F122	Det bør være mulig for leder å få en oversikt i selvbetjeningsportalen over alle typer administratorer som håndterer bestillinger rundt tilganger og utstyr.	E	B

IDM-F123	IDM-løsningen skal integrere seg mot HPE Service Manager for saksbehandling av tilgangsbestillinger som krever manuell håndtering (dvs. ikke støttes gjennom automatisk provisjonering), gjennom et integrasjonsgrensesnitt. Grensesnittet må etableres mot gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget.	O	B
IDM-F124	IDM-løsningen bør kunne integrere seg mot Clockwork for saksbehandling av utstyrsbestillinger (PC og mobil) gjennom et integrasjonsgrensesnitt. Grensesnittet må etableres mot gjeldende integrasjonsspesifikasjon for Helse Nord. Dokumentasjon fås utlevert etter bestemmelser gitt i konkurransegrunnlaget.	E	B

1.2 Ikke-funksjonell

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
IDM-IF1	Språket i selvbetjeningsportalen skal være norsk med teknisk støtte for samiske tegn. Det skal også være mulig å velge engelsk språk.	O	
IDM-IF2	Selvbetjeningsportalens sluttbrukergrensesnitt bør støtte de vanligste mobile og stasjonære operativsystemer med varierende skjermoppløsning, forskjellige nettlesere, begrenset båndbredde/minne/CPU. Dersom ikke all funksjonalitet i selvbetjeningsportalen støttes på alle plattformer/versjoner må disse avvikene dokumenteres.	E	B

	Leverandør bes beskrive hvordan dette ivaretas. Dersom det er avvik i støtte mellom sluttbrukergrensesnitt og drifts-/administrative brukergrensesnitt skal leverandøren beskrive dette.		
IDM-IF3	Selvbetjeningsportalens sluttbrukergrensesnitt bør ha responsivt design, slik at layout dynamisk tilpasser seg forskjellige skjermstørrelser.	E	B
IDM-IF4	Selvbetjeningsportalens sluttbrukergrensesnitt skal støtte standard webteknologier (F.eks. HTML, CSS, Javascript). Leverandør bes beskrive hvilken klientside-teknologi som selvbetjeningsportalen bruker. Spesielle avhengigheter som f.eks. plug-ins må spesifiseres.	OE	B
IDM-IF5	Integrasjonsgrensesnittene skal være robuste mot nettverksproblemer, og kan fortsette uten behov for manuelle inngrep etter at problemene er løst.	O	
IDM-IF6	Grensesnittene skal støtte sikkerhet i integrasjonene (tilgangskontroll, kryptering og integritetskontroll) så langt målsystemene tillater det.	O	B
IDM-IF7	Integrasjonsgrensesnittene skal håndtere multiple endringer på samme objekt. F.eks. at en gruppeendring på en bruker kommer før den forrige gruppeendringen er ferdig, på den samme brukeren.	O	B
IDM-IF8	Grensesnittene skal støtte større endringer (f.eks. endre på 3000 brukere) i løpet av et batchvindu på 1 time. F.eks. at alle brukere skal meldes ut av en gruppe i Active Directory og inn i en ny gruppe.	O	B

	Leverandør bes opplyse og beskrive hvis grensesnittene håndterer dette forskjellig.		
IDM-IF9	Grensesnittene skal håndtere ugyldige eller ukjente objekter på en robust måte.	O	B
IDM-IF10	Beskriv hvilke provisjonerings- og andre integrasjonsgrensesnitt løsningen støtter og begrunn godt hvilke av disse som Helse Nord bør standardisere på for sin framtidige systemportefølje.	OE	B

2. Brukerhistorier selvbetjeningsportal

2.1 Introduksjon

Helse Nord benytter brukerhistorier for å synliggjøre intensjonen bak anskaffelsen, samt innhente informasjon om hvordan brukergrensesnittet i selvbetjeningsportalen skal fungere.

Leverandøren utfordres til å benytte disse brukerhistoriene i sin besvarelse for å illustrere hvordan disse underbygges og forbedres med den foreslåtte løsning. **Legg ved skjermbilder som viser konkret hvordan løsningen fungerer.**

Vi gjør oppmerksom på at brukerscenarioene vil inneholde beskrivelser og komponenter som ligger utenfor omfanget av anskaffelsen, da intensjonen er å gi et overordnet bilde av en fremtidig ønsket løsning. Leverandøren bes derfor, i de ulike besvarelsene, synliggjøre hvilke områder som ikke dekkes av tilbudt løsning, samt å beskrive hvordan grensesnittet mot slike områder dekkes.

Oppbygging av brukerhistoriene følger i hovedsak denne formen:

> *«**Som** leder **ønsker jeg å** registrere en ny ansatt **slik at** brukerkonto, tilganger og utstyr kan bestilles automatisk»*

Følgende tabell inkluderer de viktigste interessentene for selvbetjeningsportalen. Merk at alle ansatte i Helse Nord kan spille rollen som medarbeider.

Interessent	Beskrivelse
Medarbeider	Er alle de medarbeidere som benytter løsningene i Helse Nord sin tekniske infrastruktur. Medarbeideren har ofte lav teknisk kompetanse. Medarbeiderens hovedinteresse er enkle, stabile og raske tjenester.
Leder	Mellomleder i et helseforetak som bestiller tjenester på vegne av sine ansatte. Leders hovedinteresse er å hjelpe sine ansatte å utføre sine oppgaver på en best mulig måte.
Administrator	Er den ressursen som skal sikre at tjenester etableres og driftes i Helse Nord IKT på en god, effektiv og sikker måte. Administrators hovedinteresse er å enkelt kunne oppfylle bestillinger og endringer som kommer, og være sikker på at han kjenner konsekvensen på endringer i løsningen.
Utvikler	Den personen som skal skreddersy selvbetjeningsportalen. Utviklers hovedinteresse er å lage enkle og gode tjenester for medarbeidere.

2.1.1 Case 1: Ansette ny medarbeider

«Som leder ved Universitetssykehuset Nord-Norge, Kreftpoliklinikken ønsker jeg å hjelpe min nyansatte kreftsykepleier Anne Pedersen i gang på en smidig måte. Jeg ønsker å bestille tilganger, adgangskort og utstyr (PC/mobil) på forhånd, slik at hun kan komme i produktivt arbeid snarest mulig.

Jeg kan navigere meg gjennom en katalog av mulige applikasjoner, systemtilganger og utstyr.

Jeg ønsker hjelp til å bestemme de korrekte tilgangene og utstyr for Anne.»

1. Vis hvordan den tilbudte løsningen hjelper lederen gjennom prosessen med å bestille tilganger og utstyr som nevnt ovenfor. Det er ønskelig at det skal være mulig for lederen å få opp automatisk forslag til utstyr og tilganger basert på kjente attributter (f.eks. stilling/rolle og arbeidssted), og at det er mulig for leder å enkelt legge til eller fjerne elementer i bestillingen.
2. Vis hvordan påloggingsdetaljer som bruker-ID og passord kan gis til nyansatt etter automatisk registrering og aktivering av konto. Ta utgangspunkt i at nyansatt på dette tidspunkt ikke har tilgang på jobb-e-post.
3. Vis hvordan de involverte i onboarding-prosessen varsles når de må gjøre eller ta stilling til noe, eller når en bestilling er utført (forutsetter integrasjon mot Service

Manager for tilgangseffektuering og Clockwork for effektuering av utstyrsbestillinger (PC/mobil).

4. Vis hvordan status på bestillinger vises i lederens grensesnitt, og hvordan purringer kan sendes.

2.1.2 Case 2: Ansatt ber om tilgang til applikasjoner/systemer ut over standard gitt fra kjente attributter

*«Som kreftsykepleier ved Universitetssykehuset Nord-Norge, Kreftpoliklinikken har jeg behov for tilgang til **Clockwork** (logistikk- og innkjøpssystem) og **Nissy** (pasienttransportsystem), ettersom disse ikke er inkludert som standard i min gjeldende tilgangsprofil.»*

Jeg kan navigere meg gjennom en katalog av mulige applikasjoner og systemtilganger.

*Jeg ser at tilgang til både **Clockwork** og **Nissy** må godkjennes av min nærmeste leder, og at disse forespørslene i tillegg må begrunnes.»*

1. Vis hvordan den tilbudte løsningen hjelper den ansatte gjennom prosessen med å bestille tilgang til applikasjonene nevnt ovenfor.
2. Vis hvordan det kan fremgå av løsningen at tilgang til:
    a. **Clockwork** må begrunnes før den kan godkjennes av leder, for deretter å automatisk opprettes til målsystemet
    b. **Nissy** må begrunnes før den kan godkjennes av leder, for så å bli manuelt opprettet i målsystemet
3. Vis hvordan den tilbudte løsningen hjelper leder og administrator gjennom prosessen å vurdere, godkjenne og opprette tilgang til **Clockwork** og **Nissy**.
4. Vis hvordan de involverte varsles når deres oppmerksomhet er påkrevd, samt når tilgang er innvilget/avslått.

2.1.3 Case 3: Tilpasse selvbetjeningsportal

«Som utvikler ønsker jeg å tilpasse portalen til Helse Nords grafiske profil og skreddersy den tilgjengelige funksjonaliteten, slik at medarbeiderne kjenner seg igjen i løsningen og enkelt kan bruke standardfunksjonalitet som å endre passord og å foreta bestillinger.»

1. Vis hvordan utvikler kan gjøre visuelle tilpasninger ved hjelp av standard web-teknologi.
2. Vis hvordan utvikler kan skreddersy menyer, legge til og fjerne funksjonalitet som allerede eksisterer i selvbetjeningsportalen.

3. Vis hvordan utvikler kan integrere funksjonalitet fra et annet system som ikke er en del av selvbetjeningsportalen, men som fra et medarbeider-ståsted logisk hører hjemme her.
4. Vis hvordan tilpasninger nevnt i de forrige punktene ivaretas på tvers av programvareoppdateringer.

2.1.4 Case 4: Få oversikt over ansatte

«Som leder ved Universitetssykehuset Nord-Norge, Kreftpoliklinikken ønsker jeg en oversikt over mine ansattes arbeidsforhold med status på onboarding, tilganger og status på førstegangs/regelmessig bakgrunnssjekk eller faglige autorisasjoner. Jeg ønsker å kunne se status på deloppgaver (f.eks. introduksjonskurs ikke gjennomført) og purre på den som har ansvar for deloppgaven.»

1. Vis hvordan lederen enkelt kan få et overblikk over status for sine ansatte, samt hvordan lederen kan få tilgang på mer detaljert informasjon.
2. Vis hvordan involverte automatisk kan bli varslet om ting som krever oppfølging.

2.1.5 Case 5: Bytte glemt passord

«Som medarbeider ønsker jeg å endre passord fordi jeg har glemt det.»

1. Vis hvordan medarbeider selv kan endre passord. Demonstrer hvordan brukervennlighet og sikkerhet ivaretas i en situasjon der medarbeideren ikke husker sitt nåværende passord.
2. Vis hvordan passordregler vises i brukergrensesnittet.

2.1.6 Case 6: Bytte passord som har utløpt eller er i ferd med å utløpe

«Som medarbeider ønsker jeg å endre mitt passord som har utløpt eller er i ferd med å utløpe.»

1. Vis hvordan medarbeider selv kan endre passord ved å oppgi det eksisterende passordet.
2. Vis hvordan passordregler vises i brukergrensesnittet.

2.1.7 Case 7: Et mulig fremtidig målbilde

Leder: «Jeg ønsker at ny medarbeider skal kunne utføre oppgaver før startdato dersom ønskelig av medarbeideren selv. Det er allerede definert felles oppgaver som nye medarbeidere kan gjøre før startdato. F.eks. e-læringskurs i informasjonssikkerhet i Campus. Jeg ønsker også å definere hva ny medarbeider kan gjøre før startdato, som er spesielt for vår enhet. F.eks. lese et informasjonshefte om Kreftavdelingen.»

Medarbeider: «Jeg ønsker å elektronisk signere arbeidsavtale, helseattest og taushetserklæring. Samtidig ønsker jeg å ta e-læringskurs i informasjonssikkerhet i Campus før jeg begynner. Jeg ønsker også å lese om den nye arbeidsplassen og mine arbeidsoppgaver. Jeg ønsker oversikt og status på alle oppgavene jeg skal utføre på samme sted selv om jeg må utføre enkelte oppgaver andre steder via løsningen.»

1. Det er mange ulike områder som påvirkes ved pre-, on- og offboarding av medarbeidere. Eksempelet oppsummerer kort kompleksiteten ved preboarding av ny medarbeider. Vis hvordan IDM-løsningen kan støtte/bidra til et slikt mulig fremtidsbilde enten via innebygget funksjonalitet eller ved å integrere funksjonalitet fra andre systemer.

3. Spesifikke krav for SSO og federering

3.1 Funksjonell

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
	SSO		
SSO-F1	Løsningen må kunne gjenbruke Windows domene-/AD-pålogging til å gjøre SSO mot andre applikasjoner.	O	
SSO-F2	Løsningen må støtte multifaktorautentisering.	O	B
SSO-F3	Løsningen bør støtte eksterne multifaktormekanismer via standardiserte protokoller, som RADIUS.	E	B
SSO-F4	Beskriv hvilke mulige faktorer / påloggingsmetoder løsningen støtter direkte.	E	B
SSO-F5	Løsningen må støtte autentisering med X509-sertifikater.	O	
SSO-F6	Løsningen må kunne sjekke gyldighet av sertifikat ved påloggingsforsøk. Dette	O	

	inkluderer sjekk av revokeringsstatus vha. CRL eller OCSP.		
SSO-F7	Løsningen må støtte bruk av smartkort som bærer for sertifikater.	OE	B
SSO-F8	Løsningen bør støtte adaptiv SSO. Med adaptiv SSO menes at bruken av MFA og hva brukeren gis tilgang til kan avhenge av hvor brukeren logger på fra, hvilke enheter som benyttes, tidspunkt og andre faktorer. Leverandør bes beskrive hvordan løsningen støtter adaptiv SSO, og hvilke faktorer som vurderes.	E	B
SSO-F9	Avhengig av hvordan en bruker autentiserer seg må det kunne settes ulike sikkerhetsnivåer for sesjonen.	O	B
SSO-F10	Det skal kunne styres av policies for hvilke systemer, brukere etc. SSO og MFA skal aktiveres.	O	
SSO-F11	Løsningen bør støtte forenklet pålogging innenfor samme arbeidsøkt som det er gjennomført en fullverdig autentisering. Leverandør bes beskrive hvordan dette kan gjøres.	E	B
SSO-F12	For systemer som benytter felleskontoer bør løsningen kunne spore hvilken bruker som benyttet felleskontoen. Leverandør bes beskrive hvordan dette kan løses.	E	B
SSO-F13	Løsningen bør støtte raskt brukerbytte (<5sek) på klienter der personlige brukere benyttes, men der hvem som er innlogget vil kunne skifte ofte. Leverandør bes beskrive hvordan dette kan løses.	E	B
SSO-F14	Løsningen bør kunne understøtte autentisering ved operasjoner internt i applikasjoner / arbeidsflyt. Dette kan være for å bekrefte identitet, eller fordi et høyere sikkerhetsnivå er påkrevd for operasjonen. Eksempelvis tilgang til nasjonal kjernejournal fra DIPS krever høyere tilgangsnivå enn kun til DIPS. Leverandøren bes beskrive hvordan dette kan løses.	E	B

SSO-F15	Når en bruker logger seg ut av sin opprinnelige innlogging (den som ga grunnlag for videre SSO) bør sesjoner opprettet gjennom SSO også avsluttes.	E	B
SSO-F16	Løsningen bør kunne gi SSO for applikasjoner publisert gjennom Kundens Citrix-baserte webportalløsning.	E	B
SSO-F17	Leverandøren skal implementere SSO mot Helse Nord sin installasjon for Bluegarden Personalportal (ekstern tjeneste) Dokumentasjon på grensesnitt fås utlevert etter bestemmelser gitt i konkurransegrunnlaget.	O	B
SSO-F18	Leverandøren skal implementere SSO mot Helse Nord sin DIPS-installasjon. Dokumentasjon på grensesnitt fås utlevert etter bestemmelser gitt i konkurransegrunnlaget	O	B
SSO-F19	Leverandøren skal implementere SSO mot Helse Nord sin Sectra-installasjon. Dokumentasjon på grensesnitt fås utlevert etter bestemmelser gitt i konkurransegrunnlaget	O	B
	Legacyapplikasjoner		
SSO-F20	Løsningen må muliggjøre SSO for "legacy"-applikasjoner. Dvs. applikasjoner som ikke er webbaserte, og som ikke støtter moderne autentiseringsprotokoller.	O	
SSO-F21	Legacy SSO, som angitt i krav SSO-F20, må minimum kunne gjøres mot applikasjoner som kjører på Windows 7 og Windows 10.	O	
SSO-F22	Det må kunne legges til støtte for SSO for legacy applikasjoner som løsningen ikke har støtte for "ut av boksen".	O	
SSO-F23	Det bør være enkelt/lite tidkrevende å innføre SSO for en legacyapplikasjon løsningen ikke har støtte for "ut av boksen". Leverandøren bes beskrive hvordan dette kan gjøres. Slik innføring bør kunne gjøres uten leverandørbistand.	E	B

SSO-F24	Løsningen må støtte SSO for webapplikasjoner som ikke støtter moderne autentiserings-protokoller. Leverandør bes beskrive hvordan dette kan gjøres. Slik innføring bør kunne gjøres uten leverandørbistand.	OE	B
SSO-F25	Det bør være mulig å «brande» legacy SSO. Dvs. at brukeren for eksempel får opp en kundekonfigurerbar splashscreen e.l. ved automatisert innlogging til legacyapplikasjon.	E	B
	Federering		
SSO-F26	Helse Nord tilbyr tjenester til eksterne, og har behov for at egne brukere får tilgang til eksterne tjenester. Løsningen må derfor kunne fungere både som IDP og SP i en federeringssammenheng. (Se vedlegg 1 «IAM Målarkitektur» for beskrivelse av relevante scenarier.)	O	B
SSO-F27	Løsningen må støtte SAML 2.0 både for intern SSO mot målsystemer som støtter dette, og for federering.	O	
SSO-F28	Løsningen må støtte OpenID Connect (OIDC) både for intern SSO mot målsystemer som støtter dette, og for federering.	O	
SSO-F29	Løsningen bør tilby sømløs støtte for pålogging til mye brukte eksterne skytjenester.	E	B
SSO-F30	Kunden planlegger å benytte STS-tjenester mot HelseID (OpenID Connect JWT-basert token) for federering av autentisering mot nasjonale tjenester og andre helsevirksomheter, og vise versa. Løsningen må understøtte dette.	O	B
SSO-F31	De ulike sluttbrukerrettede delene av løsningen (raskt brukerbytte, autentiseringsfaktorer osv.) bør være intuitive og brukervennlige.	E	B

3.2 Ikke-funksjonell

Nr.	Krav	Kravtype (O/OE/E)	Beskriv (B)
SSO-IF1	Adminkontoer i løsningen bør provisjoneres gjennom IDM/AD. Admintilgang til løsningen bør kunne styres gjennom kundens fremtidige PAM-løsning.	E	B
SSO-IF2	Løsningen bør kunne håndtere 5000 samtidige brukersesjoner, uten at det går utover ytelsen (økt påloggingstid f.eks.).	E	B
SSO-IF3	Det må være mulig å enkelt skalere løsningen for å håndtere flere (samtidige) brukere . Leverandøren bes beskrive hvordan løsningen best skaleres.	OE	B
SSO-IF4	Det skal være rapporteringsfunksjonalitet i løsningen. Leverandøren bes beskrive hvilke standardrapporter og tilpasningsmuligheter som leveres.	OE	B

4. Vedlegg

Vedlegg 1: IAM målarkitektur