

Vedlegg B

Kundens tekniske plattform - Standard Infrastruktur

Innholdsfortegnelse

1	Introduksjon	3
2	IKT Infrastrukturplattformer i Helse Sør-Øst	3
2.1	Dagens plattform (DP)	4
2.2	Kommunikasjon og samhandling mellom ulike miljøer i DP	4
2.3	Felles regional plattform (FP)	5
3	Felles regional plattform (FP)	5
3.1	Tilgjengelighet	6
3.2	Kjøremiljø	7
3.3	Formålsspesifikk infrastruktur	8
3.4	Applikasjonsarkitektur og tilgjengelighet	8
3.5	Sonemodell	9
4	Katastrofehendtering	10
5	Egenskaper i Felles regional plattform	10
5.1	Sikkerhet	10
5.2	Robusthet og autonomi	11
5.3	Elastisitet og skalerbarhet	12
5.4	Multitenancy	13
5.5	Selvbetjening	13
6	Sameksistens mellom Felles Regional Plattform og Dagens Plattformer (DP)	13
7	Komponenter og tjenester	13
7.1	Lokaler / Datasenter	14
7.2	Infrastrukturkomponenter	14
7.3	Server / Compute	16
7.4	Felles komponenter	18
7.5	Plattformtjenester	21
8	Klientenheter og arbeidsflater	22
8.1	Dynamisk Arbeidsflate	22
9	Leverandør- og driftstilgang	23

Figurliste

Figur 1 Skybasert leveransemodell	5
Figur 2 Felles administrasjon, drift og forvaltning for alle kjøremiljø	5
Figur 3 Lagdeling av plattformen	6
Figur 4 Tilgjengelighetsområder og tilgjengelighetssoner	7
Figur 5 Tradisjonell applikasjonsarkitektur	8
Figur 6 Modernisert applikasjonsarkitektur	8
Figur 7 Regional sonemodell	9
Figur 8 Fagvertikaler	9
Figur 9 Informasjonsklassifisering og anvendelse av sonemodellen	10
Figur 10 Tilgjengelighetsområder er katastrofe- håndteringsområde for hverandre.....	10
Figur 11 Autonomi og sentral plattform	11
Figur 12 Skalerbarhet og elastisitet.....	12
Figur 13 Komponenter og tjenester	14
Figur 14 Lokaler	14
Figur 15 Maskinvare	15
Figur 16 DC-LAN Spine/Leaf	15
Figur 17 DC-LAN - Overlay	15
Figur 18, Software Defined Storage	16
Figur 19, Software Defined Network.....	17
Figur 20 AD Domenestruktur	18
Figur 21 Konsept DDI.....	19
Figur 22 Generisk provisjoneringsverktøy.....	19
Figur 23 Brukerdomener	20
Figur 24 Tilgangskontroll	20

1 Introduksjon

Dette dokumentet gir en overordnet beskrivelse av Sykehuspartners infrastrukturtjenester og arkitekturlandskap.

2 IKT Infrastrukturplattformer i Helse Sør-Øst

Som en følge av både nasjonale og regionale målbilder for økt samhandling og deling av informasjon er det et pågående og langsiktig transformasjonsløp inne IT i Helse Sør-Øst som omfatter både applikasjons-, informasjons- og infrastrukturlagene. I tillegg til deling og samhandling kommer behovene for å møte nye behov drevet fram av den teknologiske utviklingen og forventninger og krav fra så vel helsepersonell som brukere av helsetjenestene.

Historisk har helseforetakene i Helse Sør-Øst

kronologisk ulike og til dels uavhengige plattformer som hver for seg betjener ett eller flere helseforetak, samt en ny og felles infrastruktur som hvor det langsiktige målet er at denne skal erstatte øvrige plattformer. Dette beskrives mer i detalj senere i dette dokumentet.

For å skille mellom den nye plattformen og de «gamle» brukes begrepene «Dagens plattform» (forkortet til DP) og «Felles plattform» (FP). Med mindre det foreligger godkjente vedtak for annet, etableres nye tjenester og anskaffelser i FP.

I dette dokumentet beskrives i hovedsak FP samt relevante grensesnitt og samhandling mellom DP og FP.

2.1 Dagens plattform (DP)

DP består av følgende plattformer:

AHUS: Betjener Akershus Universitetssykehus. Det finnes et begrenset antall tjenester fra SIKT til AHUS hvor det brukes AD trust for autentisering.

OUS: Betjener Oslo Universitetssykehus.

SIKT: Betjener alle øvrige helseforetak i Helse Sør-Øst, samt et mindre antall private virksomheter.

Hoveddomenene AHUS, OUS og SIKT inneholder alle brukere, brukerenheter og majoriteten av applikasjoner og tjenester for respektive helseforetak. I tillegg til disse finnes det et antall bakenforliggende domener, totalt opp mot tretti domener, som av ulike årsaker er adskilt fra hoveddomenene. Dette utdypes ikke i videre i dette dokumentet, men kan gis på forespørsel der det er relevant.

Den overordnede strategiske målsetningen i regionen er å samle alt inn i den nye fellesregionale plattformen. Det må derfor forventes kontinuerlige aktiviteter i overskuelig framtid med migrering, konsolidering og sanering som kan påvirke nye anskaffelser både med tanke på målarkitekturer og prosjektgjennomføring.

Sone- og sikkerhetsmodellene i de respektive miljøene i DP er ulik som en følge at disse, med unntak av hoveddomenene SIKT og OUS har blitt designet og kravstilt i regi av tidligere uavhengige sykehus som senere har blitt slått sammen til region Helse Sør-Øst. SIKT og OUS ble designet av Sykehuspartner og har grunnleggende en felles sone- og sikkerhetsmodell. Denne har igjen, og da i særlig grad i OUS blitt videreutviklet for å øke sikkerheten med mer moderne teknologiske løsninger.

2.2 Kommunikasjon og samhandling mellom ulike miljøer i DP

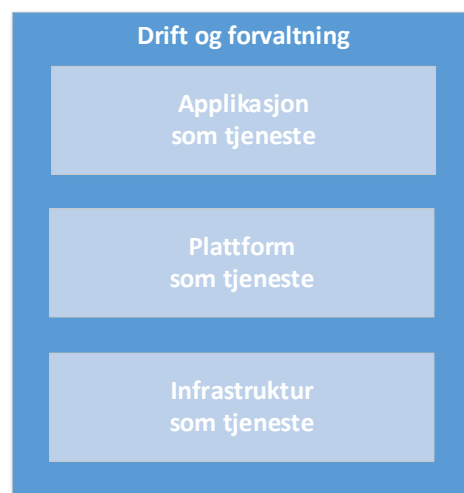
Kommunikasjon og dataflyt mellom hovedplattformene (SIKT, AHUS og OUS) går gjennom regionens integrasjonsplattform som er beskrevet i Bilag 3b Kundens tekniske plattform – Integrasjon, dog med visse unntak. Unntakene er også beskrevet i samme bilag.

Sykehuspartner drifter og overvåker infrastrukturen i alle plattformene i Helse Sør-Øst med enkelte unntak som ikke behandles i dette dokumentet med mindre det har relevans til anskaffelsen eller må ta hensyn til her med tanke på implementering og gjennomføring.

2.3 Felles regional plattform (FP)

Sykehuspartner har rigget et program kalt STIM som har i sitt mandat å etablere en ny infrastrukturplattform for Helse Sør-Øst. Den nye plattformen betegnes Felles Regional Plattform (eller bare Felles Plattform), forkortet til FP.

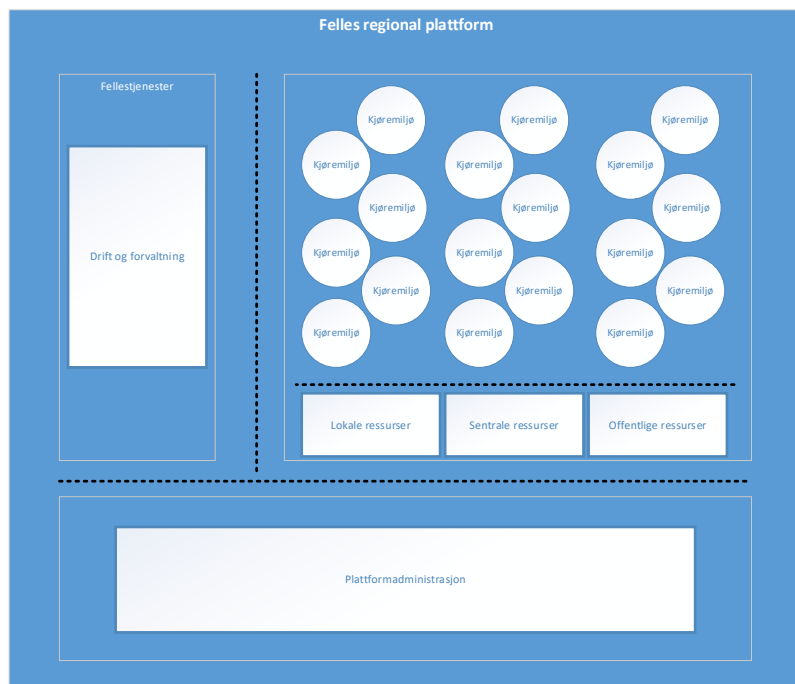
Felles regional plattform er en moderne, skalerbar og fleksibel plattform for regionale tjenester for helseforetakene i Helse Sør-Øst. Plattformen er designet for å støtte skybasert leveransemodell (Figur 1 Skybasert leveransemodell) av tjenester, og for å gi Sykehuspartner og helseforetakene i Helse Sør-Øst mulighet til å plassere tjenester og applikasjoner på sentrale, lokale eller på eksterne ressurser. Plattformen tilbyr administrasjon-, drift- og forvaltningstjenester på tvers av ressurslokasjon.



Figur 1 Skybasert leveransemodell

3 Felles regional plattform (FP)

Felles regional plattform (FP) er designet for å støtte skybasert



Figur 2 Felles administrasjon, drift og forvaltning for alle kjøremiljø

leveransemodell av tjenester, og for å gi Sykehuspartner og helseforetakene i Helse Sør-Øst mulighet til å plassere tjenester og applikasjoner på lokale ressurser, regionale ressurser eller på offentlige ressurser (public cloud). Plattformen tilbyr administrasjon-, drift- og forvaltningstjenester på tvers av ressursdomenene.

Figuren viser hvordan Fellestjenester og Plattformadministrasjon dekker og tilgjengeliggjør lokale-, regionale- og offentlige ressurser.

Felles regional plattform inkluderer også tradisjonell og formålsspesifikk infrastruktur. Dette for å ivareta krav til infrastruktur som ikke bør og/eller kan realiseres med en virtualisert infrastruktur. Krav av en slik art kan være relatert til lisensiering, kost, støtte fra leverandør og/eller ytelse.

Felles regional plattforms kjøremiljø spanner fra kritiske tjenester, til tjenester hvor applikasjonene kun utgjør ikke-kritiske støttefunksjoner. Ved å tilby en robust og tilgjengelig plattform sikrer Sykehuspartner at helseforetakenes krav til kvalitet ivaretas på avtalt nivået i alle driftssituasjoner, og for alle kritikalitetsnivå.

Felles regional plattform deles inn i flere logiske deler, på forskjellig abstraksjonsnivå, som vist i Figur 3 Lagdeling av plattformen.



Figur 3 Lagdeling av plattformen

Det øverste abstraksjonslaget er hele systemet Felles regional plattform. Felles regional plattform består av ett til flere tilgjengelighetsområder. Hvert tilgjengelighetsområde omfatter to eller flere tilgjengelighetssoner. Innenfor hver tilgjengelighetssone finnes en til flere kjøremiljø i en til flere cluster. Et kjøremiljø kan finnes innenfor et ressurs cluster, eller benytte flere ressurs cluster. Tilgjengelighetsområde, tilgjengelighetssone og kjøremiljø defineres i mer detalj i påfølgende delkapitler.

3.1 Tilgjengelighet

Helse Sør-Øst har en regional strategisk målsetning om å sentralisere og regionalisere applikasjoner og IT-tjenestene. Samtidig er det en erkjennelse av at ikke alt kan, eller bør konsolideres, og ikke alt kan, eller bør sentraliseres. FP bygges for å gi nødvendig fleksibilitet i infrastrukturen til å understøtte sentraliserte og lokale installasjoner (i.e. i foretakenes datarom), samt samhandling med skytjenester med tanke på å imøtekomme ulike krav til tilgjengelighet.

Primært plasseres systemer/applikasjoner i sentralt tilgjengelighetsområde, sekundært benyttes lokalt tilgjengelighetsområde som omfatter flere enn et HF. Tertiært benyttes tilgjengelighetsområde bestående av et HF. Dette for å begrense antall installasjoner, og dermed også begrense kompleksitet i forhold til drift og forvaltning, og grad av fragmentering i ressursbruk. Kost vil også være en faktor i denne sammenheng i den forstand at det vil være rimeligere å produsere tjenester i sentralt tilgjengelighetsområde enn i lokalt tilgjengelighetsområde.

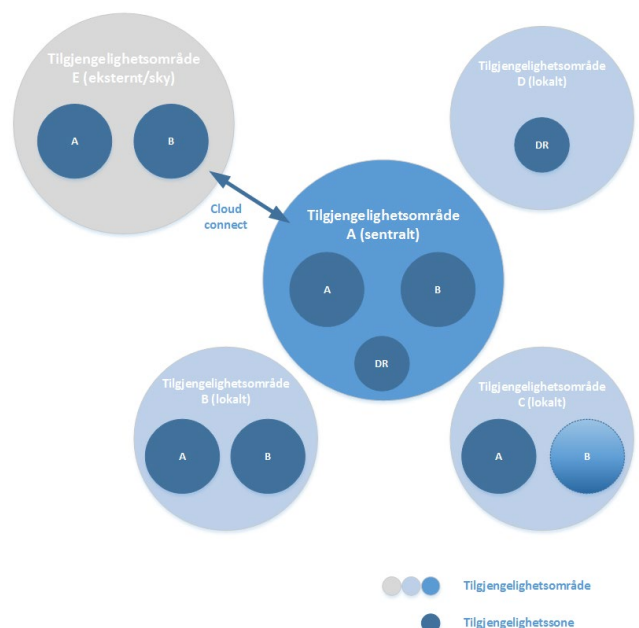
3.1.1 Tilgjengelighetsområder

Konseptuelt deles Felles regional plattform inn i tilgjengelighetsområder, som vist i *Figur 4 Tilgjengelighetsområder og tilgjengelighetssoner*.

- Sentral
- Lokal
- Ekstern

Sentralt område omfatter sentralt logisk datasenter. Et lokalt område omfatter minimum et datarom med nødvendige egenskaper/kvaliteter til å kunne kjøre lokale instanser av systemer. Et eksternt område er en offentlig sky-leverandør eller annen ekstern leverandør. Krav til tilgjengelighet og ytelse gjelder alle tilgjengelighetsområder.

Tilgjengelighetsområder benyttes for å ivareta foretakenes behov for lokal overlevelse, og utgjør minste enhet i forhold til dette, hvilket betyr at en lokal instans kan produseres innenfor et lokalt tilgjengelighetsområde. Et lokalt tilgjengelighetsområde kan omfatte ett eller flere HF.



Figur 4 Tilgjengelighetsområder og tilgjengelighetssoner

3.1.2 Tilgjengelighetssoner

Et tilgjengelighetsområde inneholder en eller flere tilgjengelighetssoner¹. En tilgjengelighetssone er en del av plattformen som håndterer applikasjonslast og/eller last for administrasjon av plattformen, og som er isolert på en slik måte at feil i sonen har begrenset påvirkning på aktivitet i andre soner.

Tilgjengelighetssoner som kjører produksjonslast i normal situasjon finnes typisk i par, mens tilgjengelighetssoner som håndterer katastrofesikring er enkle².

To tilgjengelighetssoner med samme rolle er etablert på fysisk adskilte lokasjoner innenfor sentralt tilgjengelighetsområde. Tilgjengelighetssone for katastrofesikring er etablert på annen fysisk lokasjon enn tilhørende tilgjengelighetssoner for produksjonslast.

For lokale tilgjengelighetsområder er denne tilgjengelighetssonen plassert i et annet tilgjengelighetsområde. For sentralt tilgjengelighetsområde befinner lokasjonen seg innenfor samme tilgjengelighetsområde.

En tilgjengelighetssone er å betrakte som et feildomene. Det vil allikevel finnes elementer i plattformen som gjør at feil i en tilgjengelighetssone vil kunne forplante seg til annen tilgjengelighetssone. Som eksempel vil bruk av lagringsbasert replikering/speiling mellom tilgjengelighetssoner medføre at feil i datagrunnlag repliseres/speiles mellom tilgjengelighetssoner. Håndtering av slike tilfeller vil være bruk av restore, og alternativt ekstra forsinket datakopi. Videre kan det tenkes tilfeller av feilkonfigurasjon på nettverkskomponenter som kan påvirke begge tilgjengelighetssoner innenfor et tilgjengelighetsområde.

3.2 Kjøretilgjengelighet

Kjøretilgjengelighet er en logisk byggeblokk i Felles regional plattform som er en samling av virtuelle ressurser en eller flere applikasjoner kan etableres på. Kjøretilgjengelighetene er policy og QoS styrt slik at et kjøretilgjengelighet ikke skal påvirke produksjonskapasiteten til et annet kjøretilgjengelighet. Et kjøretilgjengelighet kan etableres ved behov og kan bestå av en eller flere virtuelle servere, og kontainere, med nettverk og lagring tilgjengelig.

Følgende er eksempler på kjøretilgjengelighet:

- Kjøretilgjengelighet for en klinisk applikasjon
- Kjøretilgjengelighet for databaser/databasehotell
- Kjøretilgjengelighet for testformål

¹ Tilsvarende feildomene

² Mørke blå sirkler representerer feildomener

- Kjøremiljø for utviklingsformål

Et kjøremiljø kan utvides eller reduseres basert på definerte maler presentert som tjenester.

3.3 Formålsspesifikk infrastruktur

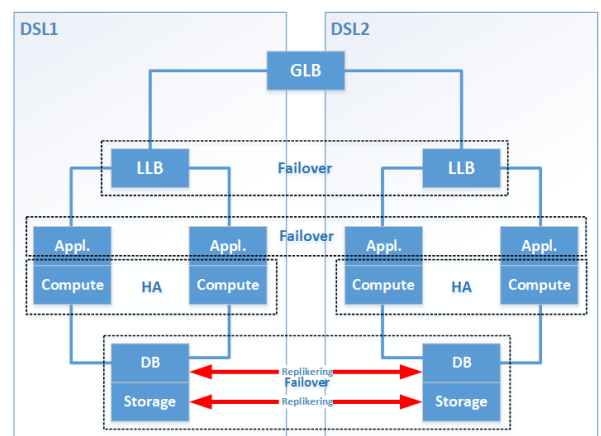
Som utgangspunkt skal formålsspesifikk infrastruktur benytte og forholde seg til samme felles komponenter som programvaredefinert del av plattformen. Dette for å standardisere og redusere antall komponenter som må finnes i plattformen. Pt. er det ikke kjent hva formålsspesifikk del består av, dette må håndteres per formål etter hvert som disse aktualiseres.

3.4 Applikasjonsarkitektur og tilgjengelighet

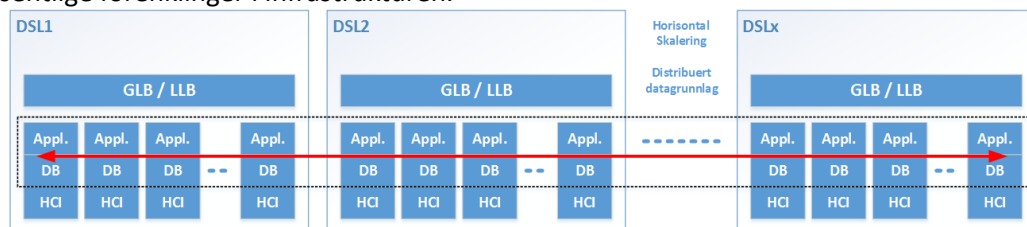
Applikasjonsarkitektur påvirker hvordan robusthet og tilgjengelighet oppnås. Tradisjonell 2/3-lags og silobasert applikasjonsarkitektur krever at det etableres og benyttes mekanismer i infrastrukturen for å håndtere feilsituasjoner.

Figur 5 Tradisjonell applikasjonsarkitektur viser tilgjengelighet med tradisjonell applikasjonsarkitektur mens Figur 6 Modernisert applikasjonsarkitektur viser en modernisert arkitektur.

Moderne applikasjonsarkitektur baseres normalt på transparent applikasjonslag og distribuert datalag. Videre inkluderes mekanismer for horisontal skalering, hvor robusthet er innebygget i applikasjon og mellomvare. Dette medfører noe mer kompleksitet i applikasjonsarkitekturen, men gir vesentlige forenklinger i infrastrukturen.



Figur 5 Tradisjonell applikasjonsarkitektur



Figur 6 Modernisert applikasjonsarkitektur

Felles Plattform understøtter både tradisjonell og modernisert arkitektur, men vil for førstnevnte ha økt kompleksitet i infrastrukturen. Nyanskaffelser kreves i tråd med en modernisert applikasjonsarkitektur.

3.5 Sonemodell

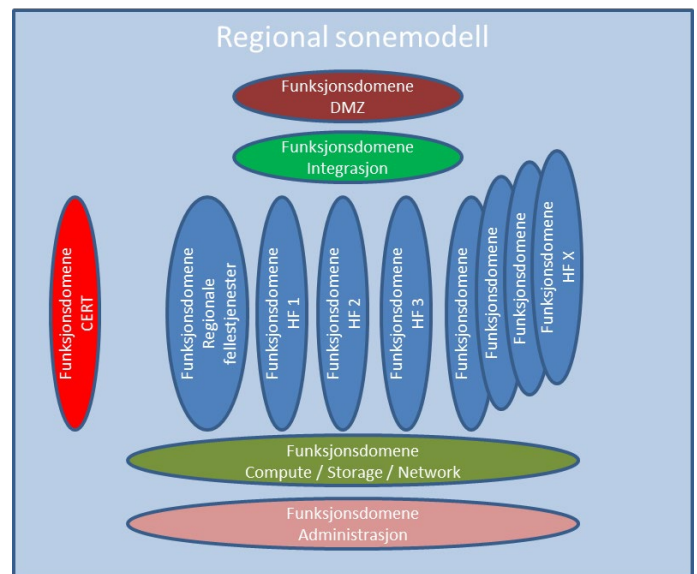
For Felles regional plattform har Helse Sør-Øst etablert en sonemodell for å skille mellom ulike tjenester og del av tjenester. Så lenge det finnes tjenester i DP vil sonemodellene i respektive DP-omener leve parallelt med den nye sonemodellen og det vil være vesentlig grad av samhandling og integrasjoner mellom tjenester og systemer i DP-omener og tjenester og systemer i ny Felles regional plattforms sonemodell.

Sonemodellen består av:

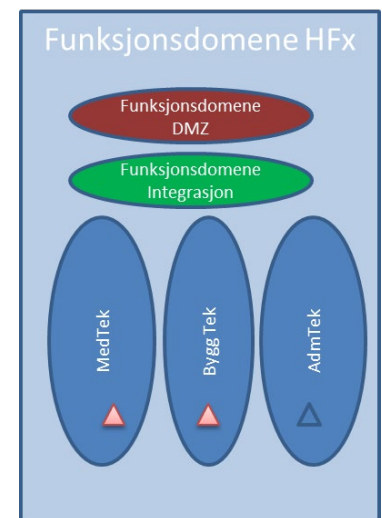
- Funksjonsdomene
 - Logisk domene for hvert enkelt helseforetak. Domenene reguleres etter juridisk og funksjonelt ansvar.
 - Eget funksjonsdomene for regionale tjenester.
 - Eget funksjonsdomene for administrasjon (separere produksjonstrafikk/tilgang fra administrasjonstrafikk/tilgang).
 - Kobles sammen via eget funksjonsdomene for integrasjon.
- Fagvertikaler
 - Innenfor helseforetakenes funksjonsdomener finnes det fagdomener. Disse vil typisk fungere som separasjon av medisinsk tekniske systemer (utstyr og applikasjoner), byggtekniske systemer (utstyr og applikasjoner) og administrativ tekniske systemer som kobles sammen via integrasjonslag internt i hvert funksjonsdomene.
- Sone
 - Sett med sonetyper som har definerte rammer for trafikkstyring og skjerming/sikring.

Alle funksjonsdomener kan inneholde alle vertikaler³, som kan ha alle soner (antall og typer etter behov).

Kommunikasjon mellom soner og domener går via brannmur og reguleres av definerte policies og regler for å ivareta kontroll og sikkerhet.



Figur 7 Regional sonemodell



Figur 8 Fagvertikaler

3.5.1 Informasjonsklassifisering og anvendelse av sonemodellen

Figuren viser regler for klassifisering av informasjon og anvendelse av modellen.

³ Gjelder ikke funksjonsdomene CERT.

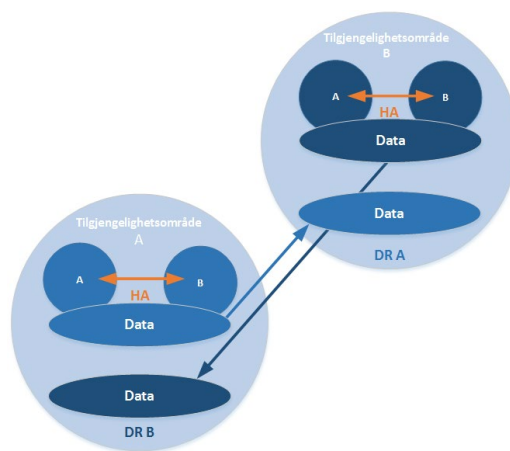
Type informasjon	Maksima l Konsekve ns	Minste godkjente Sonetype	Relevante kriterier fra styringssystemet for informasjonssikkerhet
Sensitive personopplysninger Virksomhetskritisk informasjon	4-RØD	Tilgang via F Lagring i G eller Tilgang og Lagring i H	- Hendelsen medfører tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse/integritet. - Hendelsen medfører manglende respekt for den enkeltes liv, integritet eller menneskeverd.
Personopplysninger , inkludert fødselsnummer Virksomhetssensitive opplysninger	3-ORANSJE	Tilgang via F Lagring i I eller Tilgang og Lagring i J	- Hendelsen medfører helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse/integritet. - Hendelsen medfører manglende tillit mellom pasient og helsevesen-/personell. - Hendelsen medfører helsehjelp med utilstrekkelig kvalitet.
Intern informasjon	2-GUL	Sonetype J	- Hendelsen medfører at personlig integritet og privatlivets fred ikke ivaretas. - Hendelsen medfører helsehjelp med utilstrekkelig kvalitet. - Hendelsen medfører betydelig økonomisk tap som kan gjenopprettes, eller tap av anseelse/integritet gjennom kompromittering av krenkende opplysninger.
Åpen informasjon	1-GRØNN	DMZ-Y Sonetype B	

Figur 9 Informasjonsklassifisering og anvendelse av sonemodellen

4 Katastrofehåndtering

Katastrofehåndtering er de prosesser, mennesker og verktøy som må på plass for å raskest mulig etablere normalproduksjon etter et samtidig bortfall av alle tilgjengelighetssoner (produksjon) innenfor et tilgjengelighetsområde. Felles regional plattform bygges som en høytilgjengelig løsning med geo-redundans med fysiske- og logiske adskilte tilgjengelighetssoner. Bortfall av en tilgjengelighetszone i et tilgjengelighetsområde er definert som en krise og ikke en katastrofe.

Katastrofen er et faktum ved bortfall av alle tilgjengelighetssoner i sentralt tilgjengelighetsområde og produksjon ikke kan re-etableres innen SLA-krav. I slike tilfeller må det benyttes en annen tilgjengelighetszone innenfor samme tilgjengelighetsområde. Samtidig må arbeid med å opprette normalproduksjon i opprinnelig tilgjengelighetsområde starte. For å risikoreducere omfanget av et dataangrep og korrupte data grunnet feil, vil sikkerhetskopiering/replikering av GNF-er og prioritet 1 og 2 systemer er gjøres med tidsintervall som minsker sjansen for overføring av korrupte data til nytt tilgjengelighetsområde.



Figur 10 Tilgjengelighetsområder er katastrofehåndteringsområde for hverandre

5 Egenskaper i Felles regional plattform

5.1 Sikkerhet

Felles regional plattform benytter en “zero-trust” sikkerhetsmodell alternativt til den mer tradisjonelle perimetersikringen. Der perimetersikringen har delt applikasjoner og informasjon inn i soner, hvor alle som er innenfor sonen kan stoles på og deler informasjon åpent med hverandre, er «zero-trust» en modell der ingen stoler på noen uavhengig av plassering.

For å realisere «zero-trust» benyttes mikrosegmentering slik at alle ressurser som skal ha tilgang til en applikasjon eksplisitt må be om tilgang. Tilgangsforespørselen lagres for audit formål uavhengig om tilgang blir gitt eller ikke.

Videre vil Felles regional plattform kryptere lagret informasjon og informasjon i transport med sterk kryptering. I denne sammenheng er det viktig å vurdere bruk av kryptering opp mot eventuelle konsekvenser dette har for f.eks. deduplisering på lagringsnivå.

Administrative tilganger styres fra IAM, og samtlige tilganger skal godkjennes og følge prosesser for tilgangskontroll. Tilgangskontroll utføres av PAM som også logger administrativ aktivitet.

Tilgangsstyring på tjenester styres på tjenestelaget.

Videre underbygges sikkerhet med trafikkinspeksjon og –kontroll, og bruk av teknologi for beskyttelse mot, og håndtering av ondsinnet kode, samt herding av operativsystem på alle relevante enheter.

I tillegg til krav fra sikkerhetsfunksjonene i Sykehuspartner kvalitetssikres Felles regional plattform mot CIS kontroller som er bidrag til å sikre etterlevelse av Normen.

5.2 Robusthet og autonomi

Felles regional plattform skal understøtte applikasjonsporteføljens krav til tilgjengelighet og ytelse, som definert i Sykehuspartner sine avtaler med HF-ene (SLA). Videre skal Felles plattform understøtte helseforetakenes behov for autonomi og lokal overlevelse.

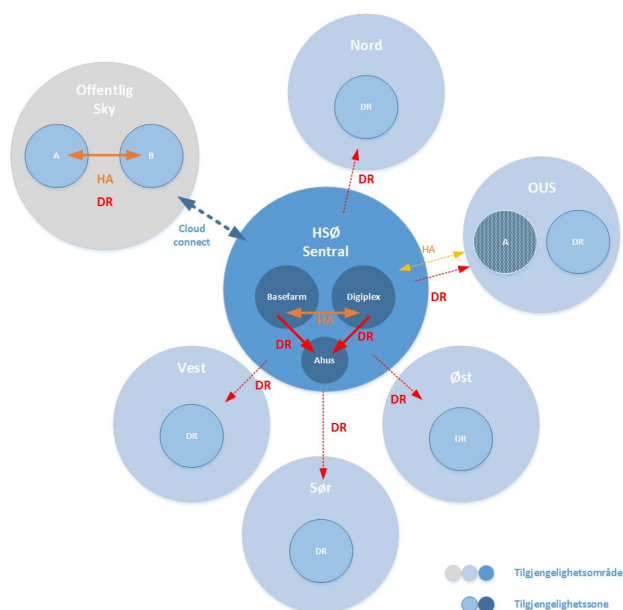
For å ivareta tilgjengelighet og lokal overlevelse er plattformen delt inn i tilgjengelighetsområder og tilgjengelighetssoner, som vist i *Figur 8 Autonomi og sentral plattform*, og som omtalt i kapittel 3.1.1 og 3.1.2.

Med lokal overlevelse i denne sammenheng forstås HF-enes tilgang til kritiske IT tjenester i tilfelle bortfall av sentralt (logisk) datasenter. Slik kan tilgang tilbys vha. installasjoner lokalt i tilgjengelighetsområdene for å kunne kjøre utvalgte systemer. I en katastrofesituasjon vil man ha redusert mulighet for aktiv drift og forvaltning innenfor et lokalt tilgjengelighetsområde, og fokus vil være å holde kliniske tjenester tilgjengelig mens feil knyttet til tilgang til sentralt tilgjengelighetsområde utbedres.

Fokus for HSØ er regionale fellestjenester, sentralt produsert og regionalt konsumert. En slik tilnærming gir effekter bl.a. i forhold til effektiv bruk av ressurser (reduert fragmentering), redusert kost knyttet til å etablere og opprettholde tilstrekkelig kvalitet på HF-lokale datarom, redusert kompleksitet i plattformen, enklere drift og forvaltning og raskere leveranser.

For å bidra til riktig tilgjengelighet for kritiske kliniske IT tjenester er Felles regional plattform bygget med geografisk redundans i sentralt tilgjengelighetsområde (HSØ sentral), med mulighet for ulike tilnærminger av aktiv-aktiv, aktiv-standby og aktiv-passiv. I tillegg til geo-redundans, er sentralt tilgjengelighetsområde delt inn i flere tilgjengelighetssoner med skillemekanismer mellom sonene slik at feil i en sone ikke forplanter seg til andre soner. Geo-redundans etableres mellom tilgjengelighetssoner avsatt for produksjon i normalsituasjon. Innenfor sentralt tilgjengelighetsområde er avstand og kommunikasjonskanal mellom datahaller slik at synkron kommunikasjon tillates, dvs. latens som tillater bruk av metro-cluster teknologi.

Arkitekturen tillater samme modell for lokale tilgjengelighetsområder som for sentralt tilgjengelighetsområde.



Figur 11 Autonomi og sentral plattform

I tillegg til geo-redundans inkluderer plattformen katastrofesikring (DR). For sentral del av plattformen (HSØ sentral) er DR-lokasjon innenfor samme tilgjengelighetsområde. For eventuelle øvrige tilgjengelighetsområder benyttes sentralt tilgjengelighetsområde for katastrofesikrings formål. Dette forutsetter at det finnes en kopi av aktuelt datagrunnlag i tilgjengelighetsområde benyttet for DR, samt ledig prosesseringskapasitet og nettverk til å etablere nødvendige kjøremiljø. For programvaredefinert del av Felles regional plattform etableres slike kjøremiljø basert på standardiserte blueprint og maler.

Arkitekturen tillater at man har tilgjengelighetssone for DR i lokale tilgjengelighetsområder for systemer som kjøres sentralt i normalsituasjon. Sistnevnte må ses i sammenheng med aktuelt system i forhold til bl.a. funksjonalitet for replikering av data.

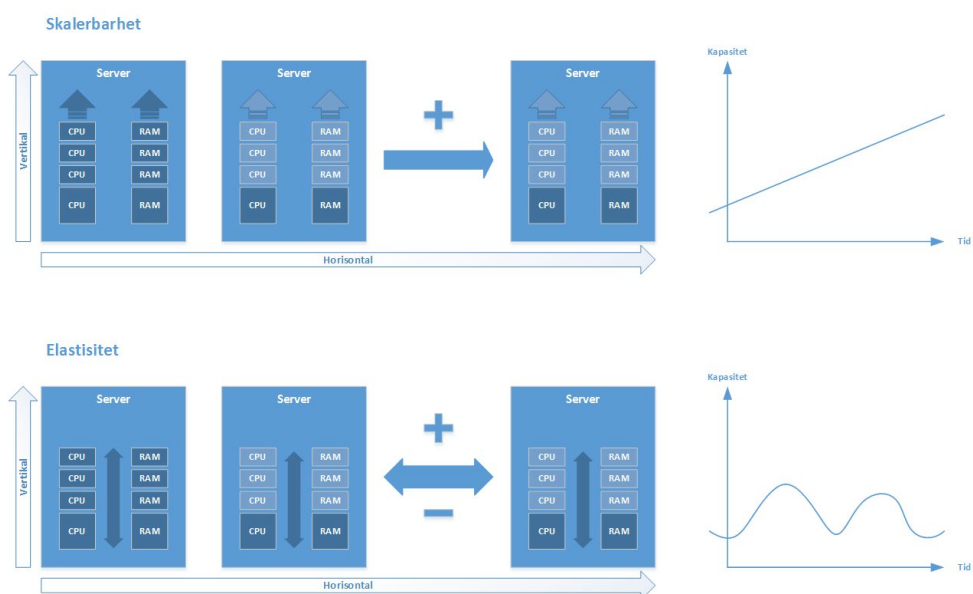
Robusthet er ikke en dedikert løsningskomponent, men en egenskap som adresseres innen hver komponent og understøttes av verktøy og felles komponenter(/tjenester), og operasjonelle rutiner.

I tillegg til lokasjonsredundans er Felles regional plattform bygget redundant innenfor hver lokasjon. Dette omfatter alt fra redundant grunnleggende infrastruktur (strøm, kjøling) til redundant tilkobling til nettverk og gruppering av prosesseringsressurser (cluster) som tillater vedlikehold av enkeltstående maskinvare enheter uten påvirkning på (kritiske) applikasjoner og systemer. Videre har plattformen egenskaper og mekanismer for å understøtte robusthet i forbindelse med (planlagt) vedlikehold. Slike mekanismer er typisk servermobilitet og godt beskrevne og utprøvde rutiner for oppdatering og oppgradering av SDDC komponenter fra leverandør.

5.3 Elastisitet og skalerbarhet

Skalerbarhet og elastisitet beskriver plattformens evne til å svare på endrede kapasitetsbehov for respektive tjenester og systemer på en sømløs måte. Dette kan skje automatisk basert på definerte regler eller som beslutnings-styrte endringer. Forutsetningen for å utnytte både skalering og elastisitet er at applikasjoner og tjenester har egenskaper som tillater endring av kapasitet (lagring, compute, nett). Kapasitets-økningen kan være horisontal, ved utvidelse av eksisterende miljø med nye ressurselementer (typisk servere og/eller containere), og/eller vertikal ved å øke tilgang til kapasitet innenfor eksisterende miljø.

Med *skalering* menes kapasitetsøkning mens *elastisitet* beskriver plattformens evne til å håndtere tidsbegrensede svingninger i kapasitetsbehov. Figurene under illustrerer forskjellene mellom skalerbarhet og elastisitet.



Figur 12 Skalerbarhet og elastisitet

5.4 Multitenancy

Programvaredefinert del av Felles regional plattform håndterer flere leietagere (tenants) på samme plattform, med tilstrekkelig skille mellom leietagere til at sikkerhet er ivaretatt. Skille mellom leietagere, på infrastruktur nivå, skjer hovedsakelig med mekanismer i programvaredefinert nettverk.

En leietager vil typisk være et HF og/eller spesifikt kjøremiljø. Systemer som har innebygget støtte for multiple leietagere (multi-tenancy) kjører som sentrale instanser i sentralt tilgjengelighetsområde. Systemer som ikke har innebygget støtte for multiple leietagere kjører primært i sentralt tilgjengelighetsområde, sekundært i lokalt tilgjengelighetsområde.

Der det er relevant stilles det krav til at nye systemer/applikasjoner har innebygget støtte for multi-tenancy.

5.5 Selvbetjening

Felles regional plattform tilbyr selvbetjening for å opprette virtuelle kjøremiljø. Ved hjelp av selvbetjening kan brukeren velge i hvilket Tilgjengelighetsområde kjøremiljøet skal opprettes og hvilke kvaliteter kjøremiljøet skal ha. Eksempler på kvaliteter er:

- Tilgjengelighet
- Ytelse
- Hyppighet på backup

Selvbetjeningen lister opp kjøremiljø, kvaliteter, landingssoner og versjoner som ligger spesifisert i løsningen sitt kildebibliotek.

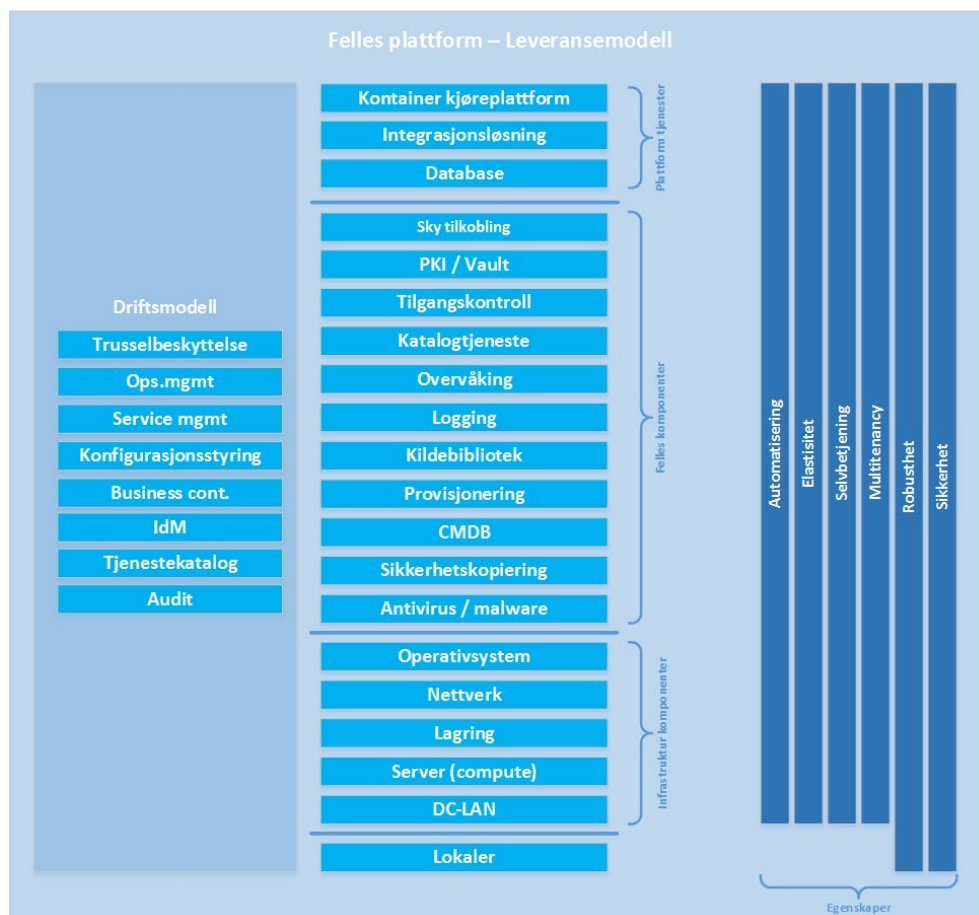
6 Sameksistens mellom Felles Regional Plattform og Dagens Plattformen (DP)

Felles regional plattform er etablert i parallell med DP. Over tid skal systemer som i dag kjører på eksisterende plattformer migreres til felles regional plattform.

Så lenge det eksistere tjenester i DP vil det være behov for integrasjon mellom DP og ny Felles regional plattform for at systemer skal kunne kommunisere på tvers. Sykehuspartners integrasjonsplattform er beskrevet i eget underbilag (T Bilag 3b). Integrasjoner og samhandling som ikke går via integrasjonsplattformen håndteres case-by-case. I forbindelse med nyanskaffelser stilles det krav til at leverandører beskriver behovet for denne typen integrasjoner og samhandling og beskriver disse.

7 Komponenter og tjenester

Felles plattform er delt opp i komponenter og tjenester, som vist i *Figur 11 Komponenter og tjenester*.



Figur 13 Komponenter og tjenester

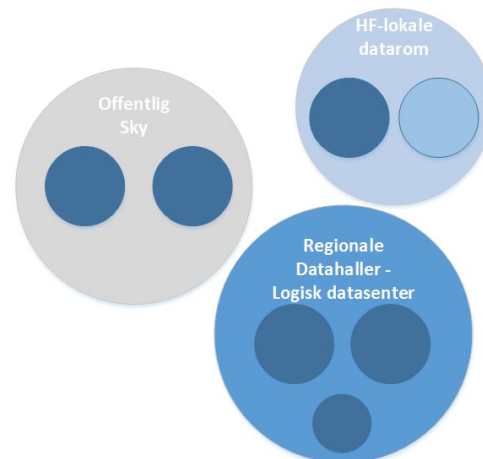
Disse er beskrevet ytterligere i påfølgende kapitler.

7.1 Lokaler / Datasenter

Programvaredefinert del av Felles plattform etableres på sentralt logisk datasenter, fordelt over tre fysiske og adskilte lokasjoner, samt på HF-lokale datarom der det er definert behov.

To sentrale lokasjoner benyttes for kjøremiljø i normalsituasjon, mens tredje sentrale lokasjon benyttes for DR formål.

Formålsspesifikk del av Felles regional plattform plasseres primært i sentralt tilgjengelighetsområde.



Figur 14 Lokaler

7.2 Infrastrukturkomponenter

Med infrastrukturkomponenter forstås

- Maskinvare
- Datasenter nettverk
- Server (compute)
- Lagring
- Nettverkstjenester
- Operativsystem
- Sikkerhetskopiering

Lagring, nettverk og server utgjør, sammen med verktøy for drift og forvaltning av disse, programvaredefinert del i Felles plattform. Utforming av disse tjenestene er beskrevet i påfølgende delkapitler.

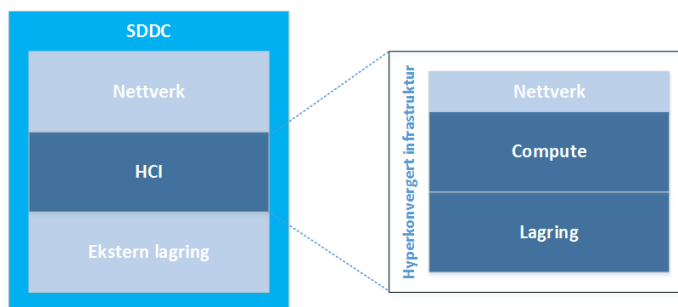
I tillegg kommer formålsspesifikk infrastruktur. Denne vil typisk inkludere samme type komponenter, men kan ha en annen implementering, eller også bestå av andre teknologikomponenter. Design for slike formål må håndteres per tilfelle. Også her er standardisering viktig for å redusere kompleksitet i løsning, og drift og forvaltning av denne.

7.2.1 Maskinvare

Maskinvare for Felles regional plattform er en kombinasjon av hyperkonvergent infrastruktur (HCI), konvergent infrastruktur (CI) og konvensjonell infrastruktur teknologi. Programvaredefinert del benytter HCI for lagring og server (compute), og konvensjonell infrastruktur i hovedsak for nettverk og lagring. CI, og konvensjonell infrastruktur, benyttes også for formålsspesifikke behov.

HCI benyttes som primær landingssone for programvaredefinert del. Der HCI ikke er formålstjenlig benyttes CI og/eller konvensjonell maskinvare. HCI benyttes for å understøtte automatisering knyttet til provisjonering av kjøremiljø og kapasitet generelt.

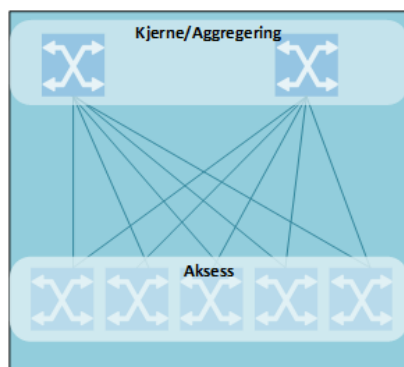
Plattformens evne til å ta inn eller skifte ut teknologi komponenter grenser til egenskapen robusthet, og skalering. Gitt at underliggende maskinvare for programvaredefinert del er basert på x86 teknologi vil denne egenskapen gjøre at skifte av teknologi generasjoner på f.eks. fysiske servere kan gjennomføres uten nedetid for konsumerende systemer. Egenskapen underbygges av SDDC støtte for flere teknologi generasjoner.



Figur 15 Maskinvare

7.2.2 DC LAN

Felles regional plattform benytter datasenter LAN infrastruktur (DC LAN) basert på Clos modellen, hvor alle spines er koblet til alle leafs. Dette gjør at man får en ikke-blokkerende infrastruktur hvor alle forbindelsene er aktive, både for båndbredde ytelse og rask failover internt i datasenteret.

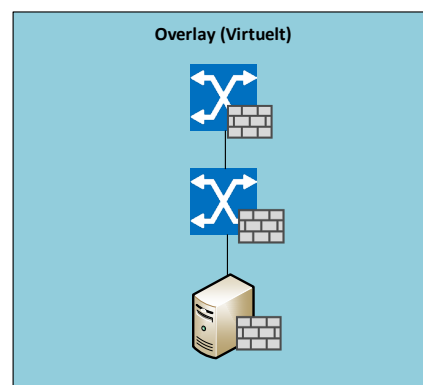


Figur 16 DC-LAN Spine/Leaf

Spine/leaf orkestreres via verktøy for å automatisere konfigurasjon ved bruk av «zero-touch» for lettere å skalere et datasenter nettverk, eller ved utbygging av flere datasentre. Underlaget skal transportere trafikk fra den virtuelle, programdefinerte plattformen og baremetals, ut til andre datasentre eller andre helseforetak via stamnett (Norsk Helse-Nett) (Figur 16 DC-LAN Spine/Leaf).

Overlayet på virtuell plattform forenkler automasjon av applikasjoner og tjenester ved at brannmur og lastbalanseringstjenester følger en template som er predefinert. Ved bruk av virtuelle brannmurer og lastbalansere forenkler dette prosessen og skaper sikkerhet på flere nivåer som støtter under en sonemodell og/eller zero trust prinsippet. (Figur 17 DC-LAN - Overlay).

Lastbalansering mellom datasentre gjøres ved bruk av en appliance som har kontroll på server/applikasjon på begge datasentrene, og har en oversikt over aktiv/ikke aktiv tjenester, og bruker DNS for lastbalansering. Intern lastbalansering leveres i software via det virtuelle overlayet hvor en tjeneste kan last balansere mellom to eller flere maskiner.



Figur 17 DC-LAN - Overlay

7.3 Server / Compute

Serverkapasitet leveres, som standard, vha. servervirtualisering med fleksibilitet i tildeling av ressurser (cpu, minne, nettverkskapasitet) og understøttelse av automatisert provisjonering og servermobilitet.

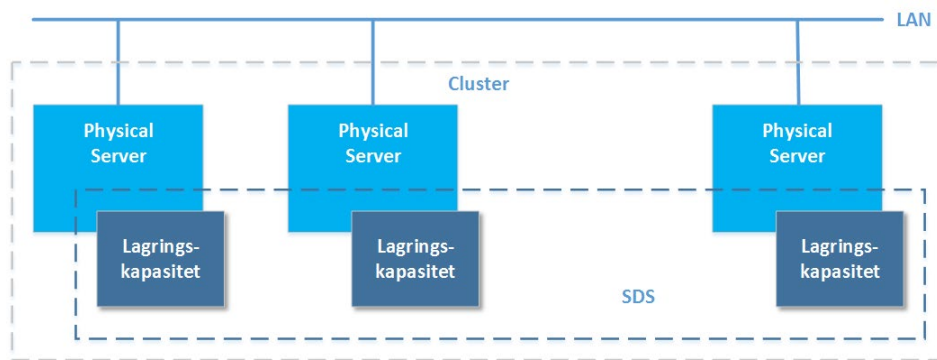
Programvaredefinert del av Felles regional plattform baseres utelukkende på servervirtualisering, med én og samme hypervisor teknologi.

For å bidra til riktig nivå av sikkerhet herdes hypervisor i henhold til gjeldende krav i Helse Sør-Øst.

Formålsspesifikk del av Felles plattform antas å benytte en kombinasjon av servervirtualisering og tradisjonell implementasjon med operativsystem direkte installert på maskinvare, samt servermodell definert av en spesialisert teknologikomponent (appliance). Servermodell blir her definert av formålet.

7.3.1 Lagring

I programvaredefinert del av FP tilbys hyperkonvergent infrastruktur hvor lagringskapasitet er en kombinasjon av lokal lagring på fysisk server og programvaredefinert kapasitet. *Figur 15, Software Defined Storage* illustrerer hvordan samlet lagringskapasitet kan benyttes på tvers av fysiske maskiner i cluster.



Figur 18, Software Defined Storage

Programvare definert lagring har funksjonalitet som man finner i høynivå (enterprise) tradisjonelle lagringsløsninger, slik som snapshot for hurtig tilgang til kopi av datasett eller for å understøtte sikkerhetskopiering; deduplisering og komprimering for å redusere behov for fysisk lagringskapasitet; kryptering for økt sikkerhet, samt funksjonalitet for replikering over avstand for å bygge robusthet og/eller understøtte katastrofesikring.

I Programvaredefinert del av Felles regional plattform leveres lagringskapasitet som

- programvaredefinert lagring (SDS),
- FibreChannel basert (FC/SAN) blokklagring,
- fillagring via tradisjonell filservere og NAS,
- og objektlagring via spesifikk løsning.

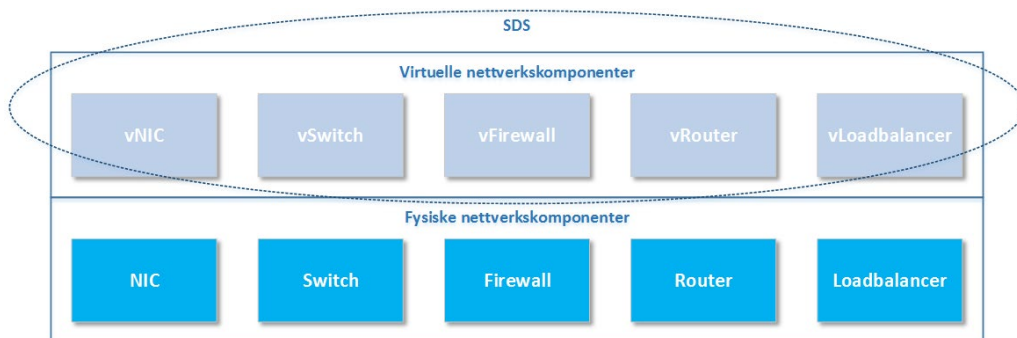
Programvaredefinert lagring benyttes som standard for programvaredefinert del.

Lagringskapasitet leveres også med tradisjonell teknologi for spesifikke formål. For å understøtte automasjon må denne typen lagring støtte programmatisk konfigurasjon og kontroll via tydelig definerte programmeringsgrensesnitt (API).

Formålsspesifikk del av Felles plattform vil kunne benytte både programvaredefinert lagring, tradisjonell lagring og lagring som del av en spesialisert teknologikomponent (appliance). Lagring er her definert av formålet.

7.3.2 Nettverk

Felles plattform benytter en kombinasjon av tradisjonell nettverksinfrastruktur og programvaredefinert nettverk. Tradisjonell nettverksinfrastruktur omtales i DC LAN. Her omtales programvaredefinert nettverk.



Figur 19, Software Defined Network

For synkronisering av tid, slik at alle relevante enheter har riktig og lik tid, benytter Felles regional plattform HSØ NTP tjeneste.

Lokal lastbalansering vil i hovedsak skje i det programvaredefinerte nettverket. Eventuelle behov for lokal lastbalansering for formålsspesifikk infrastruktur håndteres per behov.

7.3.3 Out-of-band

Felles plattform legger til rette for administrasjon av utstyr dersom normal aksess er nede for kritisk infrastruktur og serverdrift i sentrale og lokale datasentre via 4G.

7.3.4 Operativsystem

Felles regional plattform følger Sykehuspartners standardisering for operativsystemer. Det forutsettes at operativsystem, og versjonene av disse, har offisiell støtte fra produsent. For å sikre riktig bruk, implementasjon og konfigurasjon skal nye operativsystem, eller versjoner av eksisterende, godkjennes av Sykehuspartner før de tas i bruk.

For å bidra til riktig nivå av sikkerhet herdes alle operativsystem i henhold til Sykehuspartner sine retningslinjer, samt produsent og andre relevante tredjeparters sin anbefalte praksis. Operativsystem installeres, som standard, ved bruk av definerte image, og ikke med standard installasjonsmedia som utgangspunkt.

For å løpende ivareta kvalitet og konfigurasjon, og understøtte drift og forvaltning, inkluderer Felles regional plattform verktøy for administrasjon av operativsystem. Dette inkluderer konfigurasjonsstyring, med provisjonering i henhold til definert master/standard, og løpende kontroll mot denne etter installasjon. Videre inkluderes funksjonalitet for løpende oppdatering av støttede operativsystem.

Alle servere leveres som standard med:

- Herding i tråd med gjeldende krav i Helse Sør-Øst
- Regelmessig sikkerhetsoppdateringer
- Beskyttelse mot virus og skadevare
- Standard operativsystem i gjeldende versjon (N)
- Backup agent
- Lokal brannmur
- Logging

Godkjente operativsystem for servere:

- Microsoft Windows Server
- Redhat Linux

Operativsystem oppdateres i tråd med støtte for gjeldende (N) og forrige (N-1) versjon.

7.4 Felles komponenter

7.4.1 Antimalware

Beskyttelse mot skadevare følger en helhetlig sikkerhetsstrategi for best sikring av infrastrukturen hvor antimalware programvaren ikke er det eneste beskyttelseslaget i arkitekturen mot skadevare.

Operativsystem og virtualiseringsteknologi skal være:

- Herdet.
- Oppdatert.
- I henhold til sikkerhetskrav

Videre skal overvåkingsprogramvare være en del av strategien for beskyttelse mot skadevare, der maskinlæring og trusselanalyser gjennomgår infrastrukturen jevnlig for å detektere uvanlig systemoppførsel.

Operativsystem og virtualiseringsteknologi skal inneholde:

- Minst ett antimalware system
- Whitelisting funksjonalitet
- Beskyttes med brannmur

7.4.2 Katalogtjeneste

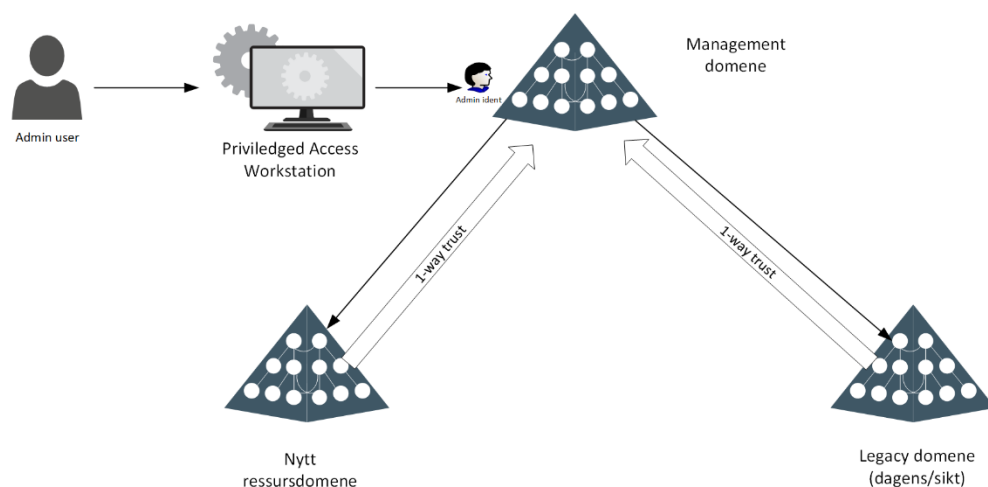
Katalogtjenesten skal benyttes for å gi en sentral administrasjon av ressurser i FP. Det tilrettelegges for å separere ressurser og objekter mot juridiske enheter, lokasjoner og enheter.

For å ivareta behov for differensierte plattformer benyttes det separate katalogtjenester for disse (test, utvikling og Pre-Prod).

I Felles regional plattform skilles ressurser og administrasjon i ulike AD forests (se *Figur 21 AD Domenestruktur*). Ad designet følger Microsofts «[Active Directory administrative tier model](#)»

Brukerkonti (unntatt admin-konti) ligger i DP-domenene på henholdsvis SIKT, OUS og AHUS og provisjoneres med Sykehuspartners IDM-løsning til Azure AD.

Alle tilganger mot infrastrukturen skjer fra Management-domenet via PAM. Dette inkluderer også infrastruktur i DP (dvs. AHUS, OUS og SIKT samt disses bakenforliggende domener).



Figur 20 AD Domenestruktur

7.4.3 Sikkerhetskopiering.

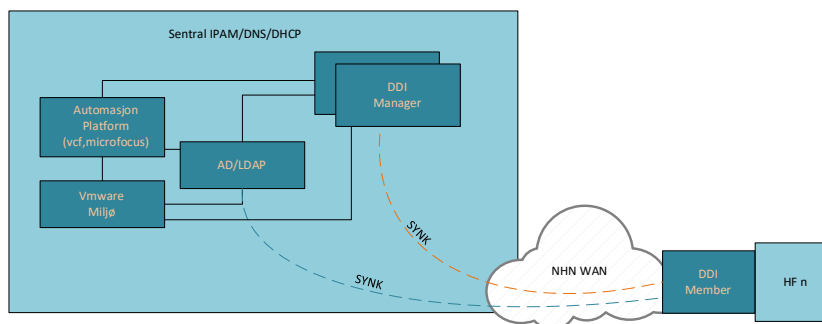
Sykehuspartner har valgt å ha en to-leverandør strategi for sikkerhetskopiering, og benytter programvare fra henholdsvis Veritas (NetBackup) og Micro Focus (Data Protector).

Backup-strategiske valg tas i samarbeid mellom tjeneste-ansvarlig og leverandør av respektive system.

7.4.4 IPAM

IPAM er generisk og delt, i den forstand at den dekker alle Sykehuspartners aktuelle behov og plattformer.

Som vist i Figur 17, Konsept DDI, er sentral løsning for IPAM/DNS/DHCP master/manager, med hoster på foretakene for å sikre lokal overlevelse.



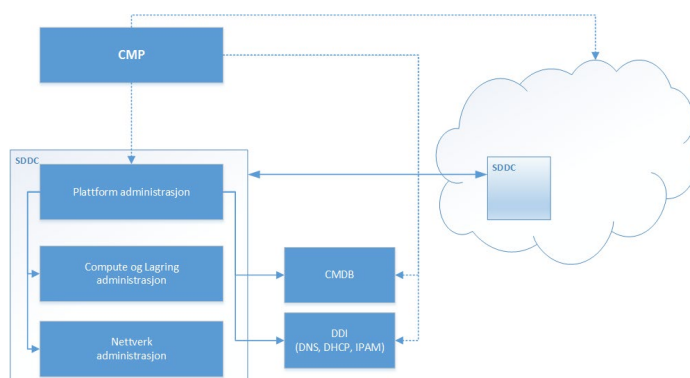
Figur 21 Konsept DDI

7.4.5 Provisjonering

Felles plattform har verktøy, funksjonalitet og kapabiliteter for provisjonering av infrastruktur tjenester og kapasitet. Provisjonering automatiseres, ved at ressurser kan bestilles via portal (selvbetjening), og ved at provisjoneringen baseres på maler og regelbøker. Automatisering av prosesser for provisjonering understøtter en mer effektiv drift og kortere ledetid for leveranser, samt økt standardisering og kvalitet.

Provisjonering kan deles mellom provisjonering av infrastruktur tjenester og kapasitet, og provisjonering av plattformtjenester (PaaS) og programvaretjenester (SaaS). Provisjonering av infrastruktur tjenester og kapasitet for den programvaredefinerte delene av plattformen er teknologispesifikk og dekkes av verktøyporteføljen som inngår.

Provisjonering av øvrige tjenester vil gjøres med en kombinasjon av teknologispesifikke verktøy og generiske verktøy. Generisk provisjoneringsverktøy er ikke innenfor omgang. Teknologi spesifikke verktøy kan i denne sammenheng typisk utgjøre grensesnitt til, og bli benyttet av, generisk provisjoneringsverktøy (CMP – Cloud Management Platform).



Figur 22 Generisk provisjoneringsverktøy

7.4.6 Plattform kildebibliotek

Felles regional plattform defineres og styres av kode i form av standard konfigurasjoner og programkode (f.eks. script). Videre benyttes standardiserte images og regelbøker ('playbooks') til installasjon og provisjonering. I sum utgjør dette et sett med godkjente objekter som forvaltes og administreres for å sikre at de til enhver tid gyldige objektene benyttes.

Omtalte objekter oppbevares, og administreres, i et sentralt kildebibliotek.

7.4.7 Logging

Felles regional plattform inkluderer sentralisert loggløsning både for operasjonelle formål og sikkerhetsformål hvor alle logger sendes til SP Sentralt Loggmottak⁴.

Det importeres data fra eksisterende loggkilder/applikasjoner og det forutsettes at nye loggkilder/applikasjoner benytter det sentrale loggmottaket. Loggfilene bearbeides med hensyn på metadata til tidsbaserte rapporter både for analyseplattform og andre applikasjoner.

Loggmottaket kan ta imot logger på flere format, og mest vanlige er Syslog og strukturerte tekstbaserte filer.

I loggmottaket lagres fortrinnsvis infrastrukturbaserte logger samt autentiserings-/påloggingsinformasjon.

7.4.8 Overvåkning

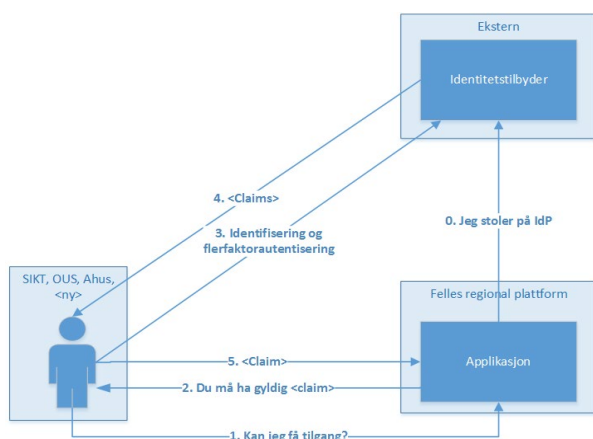
Felles plattform inkluderer overvåkningsløsning både for operasjonelle formål og sikkerhetsformål.

Operasjonell overvåking er relatert til tilgjengeligheten og funksjonen til komponenter og tjenester, og dekker i hovedsak overvåking av maskinvare enheter, lagring, server, nettverk, virtualiseringslag, operativsystem og applikasjoner for riktig funksjon og tilgjengelighet.

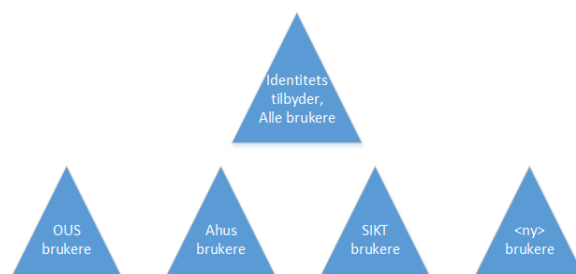
Sikkerhetsovervåking er relatert til hendelser og trusler, og dekker typisk overvåking av nettverksenheter, virtualiseringslag, server og klient.

7.4.9 Tilgangskontroll

For at brukere skal kunne benytte applikasjoner som ligger på flere plattformer, uten å logge seg på pånytt for hver gang, må Felles regional plattform støtte en uavhengig identitetstilbyder. Alle brukerne, på tvers av plattformene, vil være opprettet hos identitetstilbyderen.



Figur 24 Tilgangskontroll



Figur 23 Brukerdomener

Ved at applikasjonene på Felles regional plattform stoler på identitetstilbyderen og støtter innlogging til applikasjonen ved hjelp av <claims> trenger ikke sluttbruker å logge seg på applikasjoner selv om de ligger på en annen plattform (single sign-on).

7.4.10 PKI

Private Key Infrastructure (PKI) benyttes for å etablere funksjonalitet for utstedelse, administrasjon og bruk av digitale sertifikater. Anvendelsesområder for PKI er kryptering og autentisering, for å etablere tillit til organisasjonsenheter.

⁴ Splunk

7.4.11 Skytilkobling

Tilkobling mot skytjenester kan realiseres enten ved opprettelse av dedikerte linjer til skyleverandører som blir kryptert på vei ut fra datasentret, eller ved bruk av VPN tilknytning.

Cloud Access Security Broker (CASB) brukes for å beskytte skybaserte tjenester, brukere og applikasjoner. CASB.

Skytilkobling er avhengig av valg av skyleverandør(er). Detaljering, og materialisering, av slik(e) løsninger kan dermed først skje når valg av skyleverandør(er) er gjort.

7.5 Plattformtjenester

Felles regional plattform inkluderer et sett med plattformtjenester. Katalogen av plattformtjenester vil være under løpende utvikling og endring.

7.5.1 Database

Databasetjenester på Felles regional plattform tilbys på infrastruktur med ytelse og redundans i henhold til SLA for overliggende tjeneste. Databasen, og databasens underliggende infrastruktur, skaleres etter behov for endret funksjonalitet og/eller kapasitet.

Felles regional plattform leverer standardiserte databasetjenester med standardiserte konfigurasjoner.

Valg av tjeneste og konfigurasjon defineres av overliggende tjenestes SLA, som styrer krav til blant annet RPO og RTO, og funksjonalitet for HA og DR.

Primær plassering av databasetjenester er sentralt tilgjengelighetsområde i programvaredefinert del.

Godkjente databasevarianter:

- Microsoft SQL Server Standard/Enterprise
 - AlwaysOn benyttes for høytliggjengelighet
- Oracle Enterprise Edition
 - Oracle leveres fortrinnsvis på Red Hat Enterprise Linux.
 - Dataguard benyttes for høy tilgjengelighet

Støttede versjoner av respektive produkter følger livssyklusprinsippet om krav til N og N-1.

Alle databaseservere leveres med standard overvåkning av databasen.

7.5.2 Integrasjon

Integrasjonsløsning i Felles regional plattform er basert på prinsippet om en felles integrasjonsplattform (en logisk ESB – Enterprise Service Bus) for administrative systemer, kliniske systemer, xTU /spesialistsystemer på HF og eksterne parter.

Løsningen er beskrevet i SSA T Bilag 3b – Kundens tekniske plattform – Integrasjon.

7.5.3 Kontainer kjøreplattform

For å ivareta behov for bruk av kontainer teknologi inkluderer Felles regional plattform en kontainer kjøreplattform. Plattformen leveres både i form av felles kjøreplattform for containere, og som instansierte standard implementasjoner. Førstnevnte for å understøtte begrensede behov for å kjøre containere, og samtidig unngå multiple etableringer av kjøreplattform, sistnevnte for de formål som krever egen instans.

8 Klientenheter og arbeidsflater

Tilgang til fagsystemer eller interne nettverk i HSØ gis til administrerte klientenheter eller via administrerte, virtuelle arbeidsflater eller klienter.

8.1 Dynamisk Arbeidsflate

Dynamisk Arbeidsflate (DA) er en Sykehuspartner-utviklet løsning for bruker- og policy-styrt konfigurering av arbeidsflaten på administrerte klientenheter. Disse kan være fysiske eller virtuelle⁵ Windows klienter, virtuelle arbeidsflater⁶ eller mobile enheter.

Det er ønskelig at fagsystemer og datasett skal kunne gjøres tilgjengelig til sluttbruker via standard OS- eller nettleser-funksjonalitet, gjerne som skybaserte tjenester med lavest mulig krav til lokalt installerte komponenter. Applikasjoner som krever installasjon av lokale komponenter distribueres ved hjelp av ulike mekanismer basert på applikasjonspakker. Applikasjoner pakkes via Sykehuspartners foretrukne verktøy og standardiserte metoder, tilpasset respektive klientplattform-varianter som er i bruk.

8.1.1 Komponenter og støtteapplikasjoner

Ved behov for bruk av felleskomponenter⁷ eller felles-applikasjoner⁸ kreves det at det brukes godkjente produkter og at prinsippet med støtte av den til enhver tid gjeldende (N) og/eller forrige (N-1) versjon etterleves.

8.1.2 Administrerte mobile klienter (EMM)

Sykehuspartner har etablert en Enterprise Mobility Management (EMM) løsning som inkluderer administrasjon av enhetene fra Mobile Device Management (MDM) og administrasjon av applikasjoner fra Mobile Application Management (MAM).

Løsningen støtter operativsystemene IOS og Android med gjeldende versjoner (N og N-1).

Det skilles mellom følgende kategorier med ulike policies:

- Funksjonsenheter - MDM kontrollerte enheter
 - Med funksjonsenheter, også kalt rollebaserte enheter, menes mobiltelefoner som brukes av flere brukere i samme rolle. Disse enhetene konfigureres for å tilby oppgaverrelaterte funksjoner. For eventuell tilgang til personlig data logger brukeren inn i en «sikkerhetsboble» (kontainer) hvor personlige apper og data er tilgjengelig.
- Personlige enheter - MAM kontrollerte enheter
 - Personlige enheten som eies av helseforetaket, men er knyttet til den brukeren som skal benytte enheten. Enheten vil bli underlagt driftsregimet til MDM og underlagt de sikkerhetstiltak som er gjeldende. Med personlig enhet menes en mobiltelefon som benyttes av navngitt person.
- Apper og konfigurasjon:
 - Apper fra offentlig eller internt app-store gjøres tilgjengelig via EMM.

⁵ I dag brukes Citrix ZenDesktop

⁶ I dag brukes Citrix ZenApp

⁷ For eksempel Adobe Flash Player, Microsoft .Net eller Java

⁸ For eksempel Internett-utforsker eller Microsoft Office

9 Leverandør- og driftstilgang

For tilgang til systemer for administrative oppgaver benyttes Sykehuspartners løsning for Privilegert Tilgangsadministrasjon (PAM). Løsningen gjøres tilgjengelig for godkjente brukere både fra interne nettverk og over Internett via driftsportal.