Bilag 3.

SYSTEMBESKRIVELSE

HSØ STANDARD PLATTFORM (HSØ-SP)

Godkjent av:

Navn	Rolle	Stilling	Dato
Cato Rindal	IKT	Direktør	21.09.2012
Jarle Kasbo	Arkitektur	Seksjonsleder	21.09.2012

Innholdsfortegnelse

Liste over figurer og tabeller

ENDRINGSLOGG

Versjon	Dato	Kapittel	Endring	Produsent	Dato
1.0	20.09.12	Alle	Ferdigstilt versjon	J. Flaten	20.09.12

REFERANSER TIL ANDRE DOKUMENTER

Nr.	Dokumentnavn	Dok.id.	Versjon	Arkiv	Dato

1 DETTE DOKUMENTET

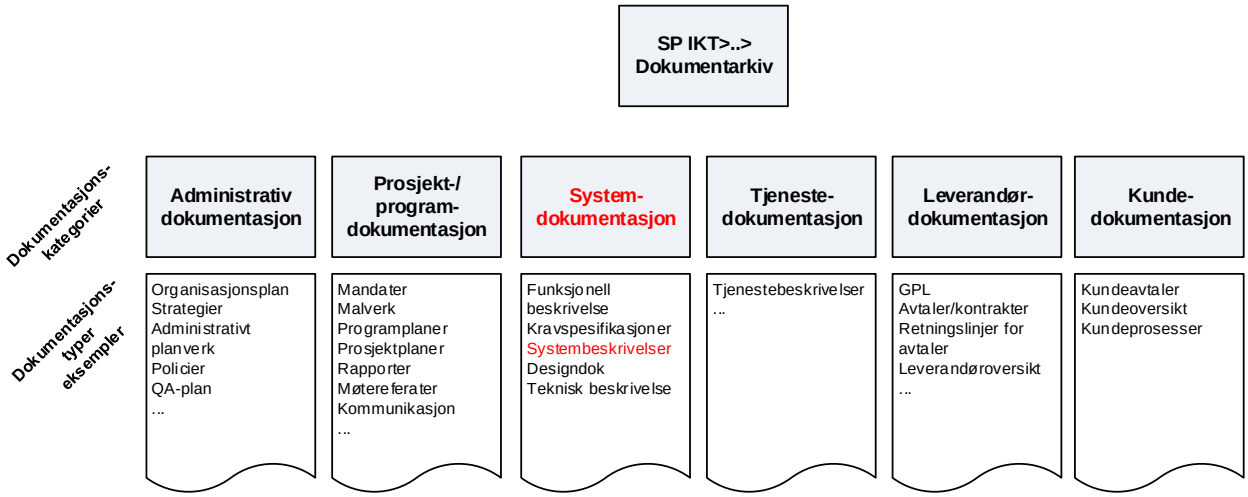
1.1 Introduksjon

Dette dokumentet beskriver Helse Sør-Øst Standard Plattform (HSØ-SP). Formålet er å etablere en omforent beskrivelse av plattformen som breddes gjennom program IKT-Plattform. Dokumentet skal gjenspeile den operative plattformen («as-is») som tilbys helseforetalene, og som til enhver tid breddes og videreutvikles. Dokumentet vil derimot ikke beskrive hva som til enhver tid er implementert på de ulike helseforetakene.

1.2 Målgruppe

Målgruppen for dette dokumentet vil være prosjekter og helseforetak som ønsker å få ett innsyn i hvordan plattformen er bygget opp, og hvilken funksjonalitet som er inkludert.

1.3 Dokumentets struktur og tilhørighet



Dette dokumentet tilhører dokumentkategori Systemdokumentasjon og er av type Systembeskrivelse.

1.4 Dokumentets oppbygging

Dette underkapittelet beskriver dokumentets oppbygging på følgende måte:

➢ Kapittel 1 Dette dokumentet	Kapittelet beskriver dette dokumentets oppbygging
➢ Kapittel 2 Introduksjon	Beskriver dette dokumentets bakgrunn eller introduksjon
➢ Kapittel 3 Min arbeidsplass/ Standard Skrivebord	Kapittelet beskriver klientplattformen i plattformen.
➢ Kapittel 4 Identitets- og Tilgangsstyring	Kapittelet beskriver hvordan identitets- og tilgangsstyring håndteres i plattformen.

➢ Kapittel 5 Integrasjonstjeneste	Kapittelet gir en beskrivelse av integrasjonstjenesten som er definert i plattformen.
➢ Kapittel 6 Støttetjenester	Kapittelet beskriver plattformens støttetjenester som henholdsvis server, lagring, backup mm.
➢ Kapittel 7 Datasenter	Kapittelet gir en oversikt over føringer for plassering av plattformens roller i henhold til ulike størrelser på datarom.
➢ Kapittel 8 Datakommunikasjon	Kapittelet beskriver tjenestene tilhørende området nettverk og datakommunikasjon i plattformen.
➢ Kapittel 9 Telekommunikasjon	Kapittelet beskriver tjenestene tilhørende omtådet telekommunikasjon i plattformen.
➢ Kapittel 10 Navnestandarder	Kapittelet beskriver navnestandarder som benyttes i plattformen.
➢ Kapittel 11 Produkter	Dette kapittelet gir en oversikt over produktene som er benyttet for å realisere tjenestene beskrevet i dette dokumentet.
➢ Kapittel 12 Forkortelser og definisjoner	Dette kapittelet gir en oversikt over forkortelser og definisjoner som er benyttet i dokumentet.
➢ Kapittel 13 Vedlegg 1: Tilleggstjenester	I dette vedlegget beskrives enkelte tilleggstjenester som tilbys på plattformen.
➢ Kapittel 14 Vedlegg 2: Pågående utviklingsaktiviteter	I dette vedlegget beskrives kort pågående utviklingsaktiviteter som vi medføre endringer på plattformen i tiden fremover.

1.5 Om gjeldende versjon

Beskrivelsen har et overordnet teknisk perspektiv. Produkter som realiserer plattformen er i størst mulig grad beskrevet i tabellform under kapittel 11.

1.6 Videre forvaltning

Beskrivelsen av Helse Sør-Øst Standard Plattform eies av Sykehuspartner, og forvaltes av Sykehuspartner Arkitektur. Dokumentet skal revideres og tilgjengeliggjøres halvårlig for å gjenspeile den operative plattformen («as-is»). Ved større endringer på plattformen vil det kunne forekomme revisjoner utenfor denne syklusen.

Det pågår arbeid for å beskrive forvaltningsmodellen for dette dokumentet. Resultatet av dette arbeidet vil gjenspeiles i neste versjon av dokumentet.

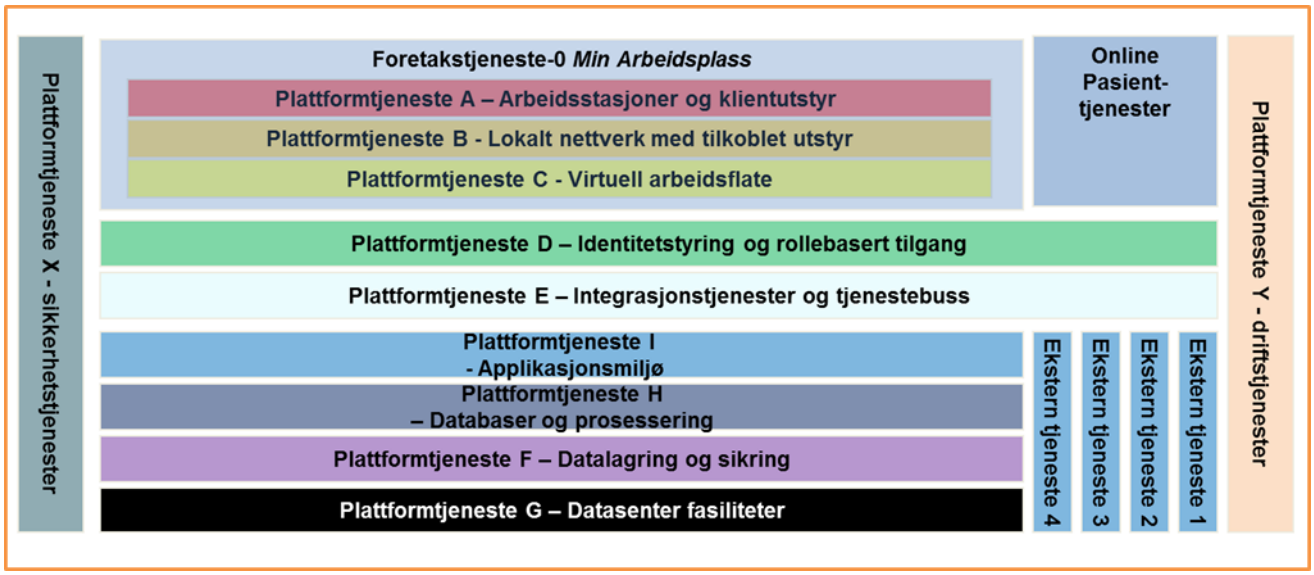
Kontaktperson for dette dokumentet er Torfinn Myhre.

2 INTRODUKSJON

2.1 Definisjon

Med "IKT-plattform" menes det teknologiske miljøet som er nødvendig for at IKT-tjenestene skal kunne anvendes på en sikker og hensiktsmessig måte. Plattformen danner grunnlaget for kjøremiljø, distribusjon og presentasjon av applikasjoner og tjenester, samt datalagring.

Plattformen representeres i program IKT-plattform ved modellen nedenfor:



Figur 2.1 – 1 Modell for HSØ-SP

Hvert lag i modellen representerer en plattformtjeneste, og summen av plattformtjenester utgjør HSØ-SP. Hver plattformtjeneste omfatter teknologi (maskinvare og programvare), arbeidsprosesser og styring.

Plattformtjeneste	Beskrivelse	Sted for beskrivelse
0 - Min arbeidsplass	..skal gi tilgang til effektivt og brukervennlig IT-verktøy på avtalte lokasjoner	Kapittel 3
D - Identitetsstyring og rollebasert tilgang	..skal gi en korrekt og effektiv forvaltning og kontroll av brukere og deres tilgang til nødvendig informasjon og IKT tjenester	Kapittel 4
E - Integrasjonstjenester og tjenestebuss	..skal gi en effektiv måte å samhandle, dele informasjon og anvende IKT tjenester på tvers av helseforetak, tjenesteleverandører og forvaltningsnivåer	Kapittel 5
I - Applikasjonsmiljø	..skal understøtte et effektivt og fleksibelt kjøremiljø for applikasjoner	Kapitel 6

H - Databaser og prosessering	..skal gi en optimal og stabil logisk lagring, prosessering og behandling av strukturerte og ustrukturerte data IKT systemene	Kapittel 6
F - Datalagring og sikring	..skal gi en sikker fysisk lagring og beskyttelse av alle data som behandles og anvendes av IKT systemene	Kapittel 6
G - Datasenter fasiliteter	..skal gi tilstrekkelig fleksible, sikre og robuste datasenter og datarom som gir IKT systemene et optimalt og stabilt fysisk miljø	Delvis i kapittel 7
X - Sikkerhetstjenester	..skal sikre at konfidensialitet, integritet, tilgjengelighet og sporbarhet oppfylles på en standardisert og effektiv måte og i tråd med eksterne (lovpålagte) og interne (policies og styringsdokumenter) krav i.h.t tilfredsstillende sikkerhetsnivåer	Eget dokument
Y - Driftstjenester	..driftstjenester skal gi sikre, forutsigbare, stabile og kostnadseffektive drift- og overvåkningsløsninger	Eget dokument, FDV

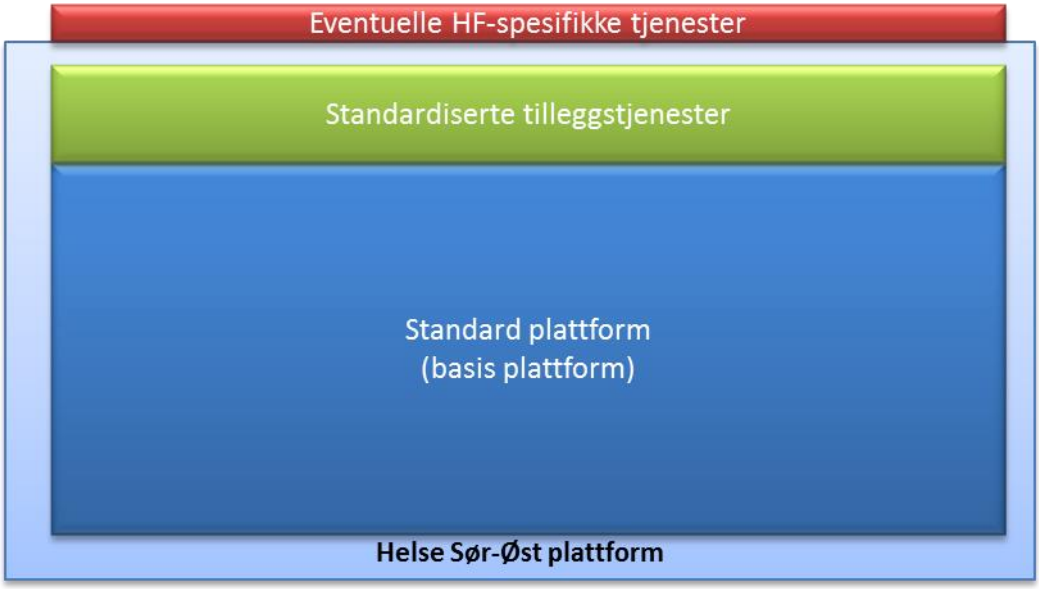
Tabell 2.1 – 1 Plattformtjenester

'Med "Online pasienttjenester" menes muligheten for å kunne eksponere IKT-tjenester til klienter som ikke inngår i Min arbeidsplass.

Med "Ekstern tjeneste" menes muligheten for å kunne tilby tjenester fra eksterne tjenestetilbydere gjennom plattformen, eksempelvis sømløs tilgang til Personalportalen fra Blugarden

2.2 Avgrensning og omfang

Helse Sør-Øst Standard Plattform omfatter alle deler og komponenter av plattformen som er standardisert for alle helseforetak. Det vil kunne være deler av plattformen som ikke alle foretak har behov for, og derfor vil plattformen ha en obligatorisk del som er basis for alle foretak, og en valgfri del som består av tilleggstjenester/løsninger som kan avropes. Det kan også forekomme tilfeller hvor ett foretak har spesielle behov som vanskeliggjør standardiserte løsninger, og disse kategoriseres som HF-spesifikke løsninger (se figur nedenfor). Det skal foreligge grundig analyse og en forankret beslutning før det etableres HF-spesifikke løsninger. Hovedregelen er at alle komponenter og løsninger er standardiserte og felles, og det er kun disse som inngår i definisjonen av Helse Sør-Øst Standard Plattform.



Figur 2.2 – 1 Omfang av plattformen

Standard plattform:	Obligatoriske plattformtjenester og løsninger for alle helseforetak
Standardiserte tilleggstjenester:	Valgfrie løsninger, som f.eks. pull-print og samordnet kommunikasjon
HF-spesifikke tjenester:	Eventuelle løsninger som kun benyttes på enkelte helseforetak

I gjeldende versjon av dokumentet, beskrives dagens operative versjon av plattformen fra et overordnet teknisk perspektiv, og standard tilleggstjenester er lagt i vedlegg.

2.3 Innholdsklassifisering og sonemodell

Sonemodellen i HSØ er utviklet for å understøtte de funksjonelle krav som stilles til en moderne IT-løsning innen helse, samtidig som sikkerheten ivaretas og er i henhold til gjeldende lover, regler og føringer.

Løsningen er designet for å møte kravene i lovgivningen og forskriftene om beskyttelse av sensitive og kritiske data. I HSØ-SP er det også lagt vekt på det stadig økende behovet for mobilitet og tilgang til Internett og å kunne tilby funksjonalitet, tilgjengelighet og fleksibilitet.

2.3.1 Innholdsklassifisering

Data klassifiseres i fire ulike nivåer, i HSØ-SP kalt «Kontekster». Disse nivåene beskrives ytterligere i tabellene nedenfor.

Type informasjon	Maksimal konsekvens	Relevante kriteria
Sensitive personopplysninger Virksomhetskritisk informasjon	4	• 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	• 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	• 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	

Tabell 2.3 – 1 Klassifisering av informasjon

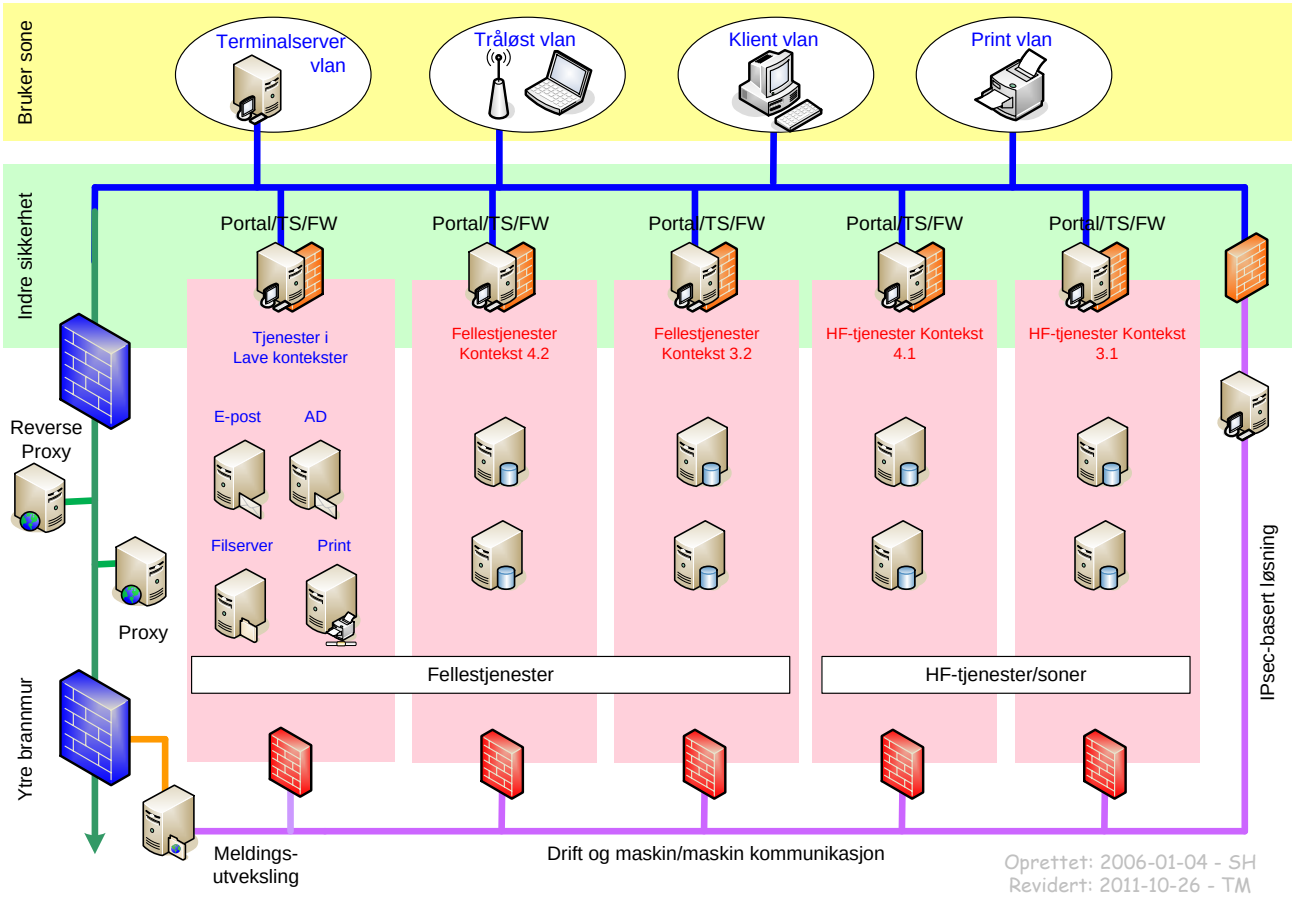
Videre er nivåene ytterligere inndelt som følger:

Type informasjon – krav til konfidensialitet/integritet	Kategori	
Sensitive personopplysninger og virksomhetskritiske data	4.1 <HF>	4.2 Felles
Personopplysninger som den enkelte kan oppfatte som sensitive, fødselsnummer. Virksomhetssensitive opplysninger.	3.1 <HF>	3.2 Felles
Intern informasjon	2	
Åpen informasjon	1	

Tabell 2.3 – 2 Kontekstmodell

2.3.2 Sonemodell

I HSØ-SP etableres det nettverksmessige skiller med barrierer mellom ulike kategorier av systemer og klienter skilles ut i egne, HF-spesifikke, klientsoner. Barrierene som beskytter de enkelte sonene kan være tradisjonell brannmur, terminalserver, webservice eller annen skillemekanisme. Der det benyttes tradisjonell brannmur mellom klienter og tjenester åpnes det spesifikt per port fra klientsone mot den enkelte server. Dette gir en betydelig lavere risiko enn når klientene står sammen med serverne. For eksempel vil et eventuelt virusangrep fra en klient ha liten mulighet til å utnytte svakheter og hull i upatchede servere, servere uten antivirus osv. nettopp fordi tilgangen mot den enkelte server/tjeneste er begrenset til den eller de porter som er nødvendig. Andre eventuelle svakheter vil dermed ikke være eksponert for angrep fra klienter eller klientnett.



Figur 2.3 – 1 Sonemodell i HSØ-SP

3 MIN ARBEIDSPLASS / STANDARD SKRIVEBORD

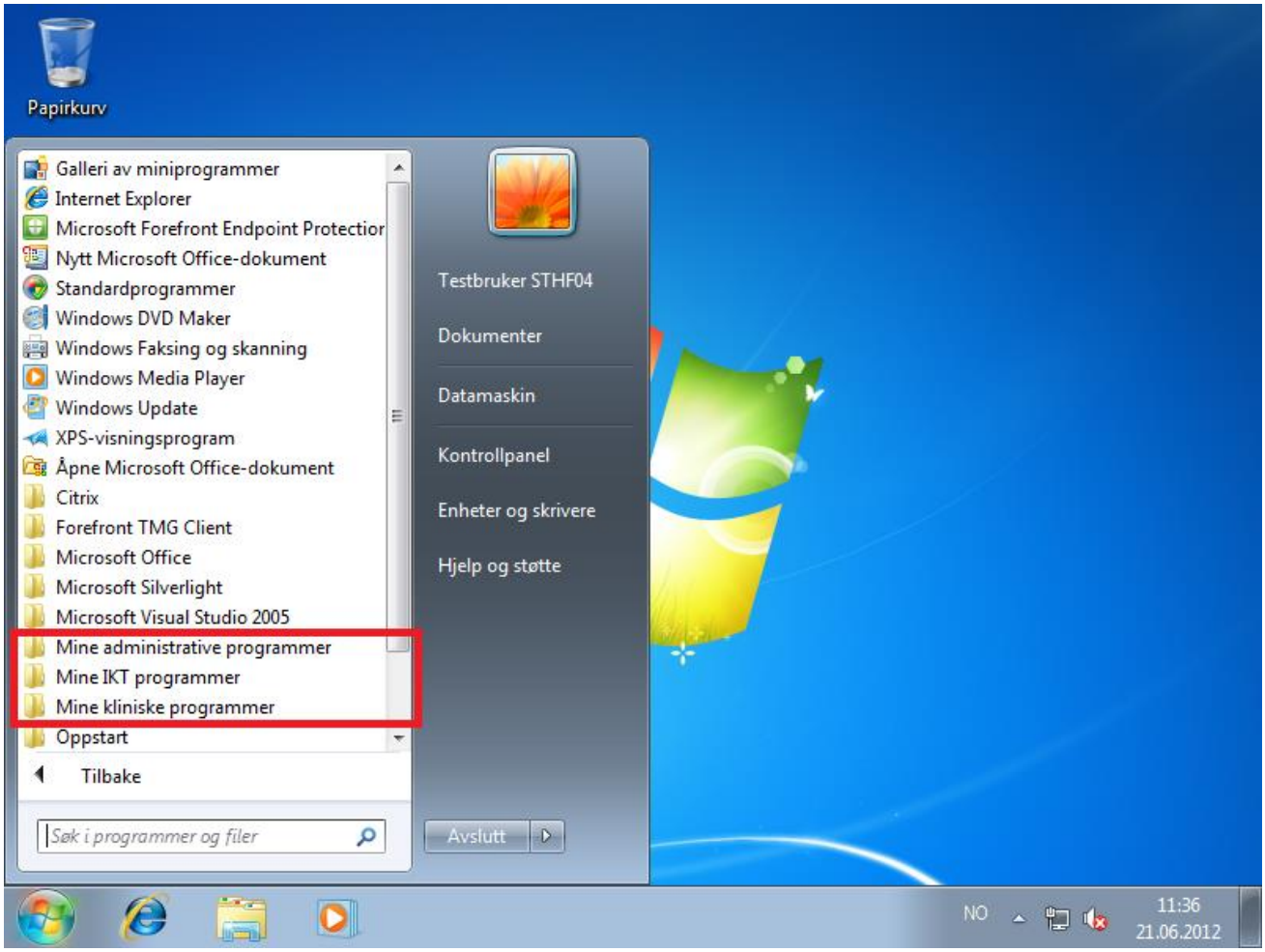
3.1 Arbeidsflate

3.1.1 Skrivebord og startmeny

Skrivebordet brukeren får i HSØ-SP er uten program-snarveier. Programmene startes fra Startmenyen enten fra den avanserte søkefunksjonen eller ved å bla seg gjennom menyen.

Snarveier til applikasjonene som er distribuert til maskinen ligger under følgende menyer:

- Administrative systemer: «Mine administrative programmer»
- IKT-systemer: «Mine IKT programmer»
- Fagsystemer: «Mine kliniske programmer»



Figur 3.1 – 1 Arbeidsflate basert på Windows 7

3.1.2 Filtilgang og stasjonsbokstav

Ved innlogging får brukeren, i tillegg til sitt personlige område, en kobling mot avdelings-/fellesområder. Hva som er tilgjengelig under avdelings-/fellesområdene avhenger av brukerens rettigheter. Dette kommer automatisert fra Lønn og Personalsystemet (PAGA). Endringer på organisasjonstilhørighet i PAGA vil også resultere i endrede tilganger til avdelings-/fellesområder.

Følgende stasjoner kobles opp for brukeren:

- Personlig filområde: P:
- Avdelingsområde: O:
- Programområde: S:

3.2 Tilgang til tjenester

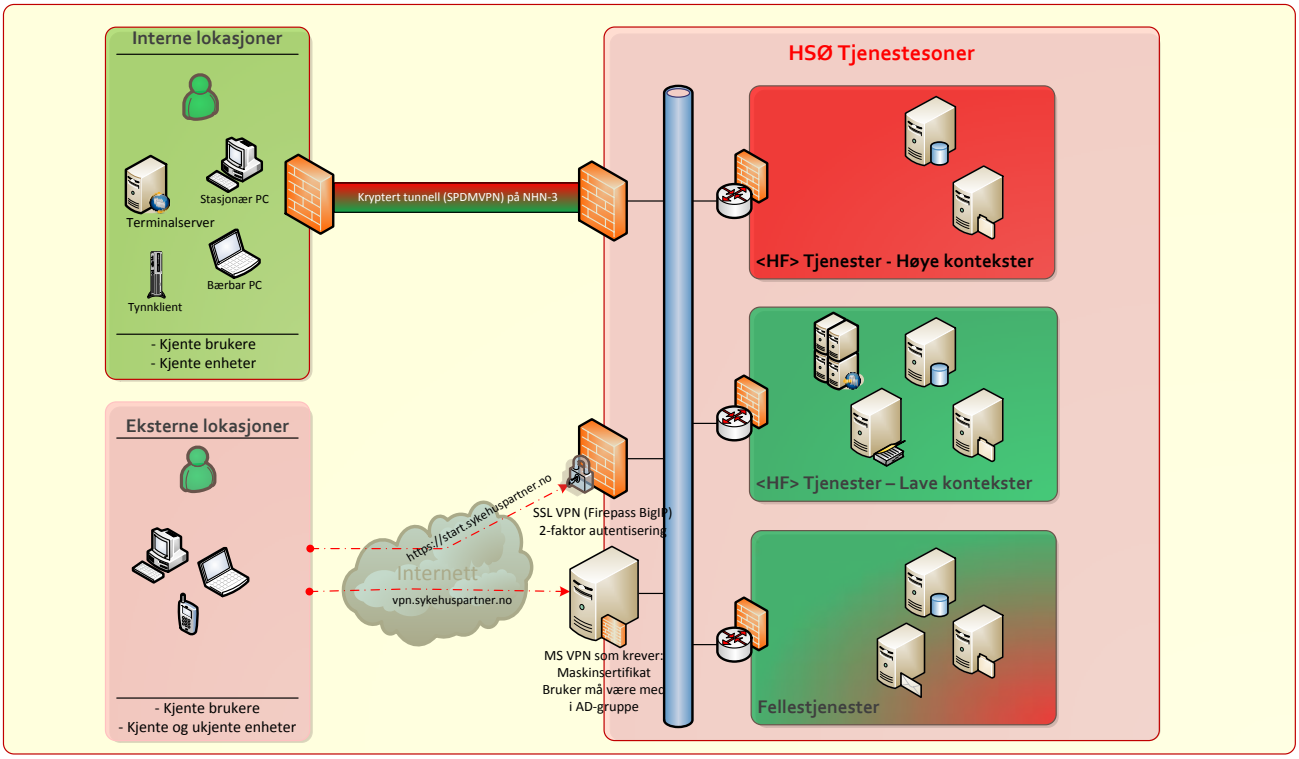
Plattformen er tilrettelagt for å muliggjøre tilgang til tjenester fra interne, sikrede nettverk og klienter så vel som fra lokasjoner og enheter utenfor foretakets/Sykehuspartners kontroll. Plattformen er bygget for å gi foretakene stor grad av fleksibilitet kombinert med høyt sikkerhetsnivå. Illustrasjonen under viser hvordan plattformern tilgjengeliggjør tjenester for brukere både fra interne nettverk på foretakenes respektive lokasjoner og over Internett fra lokasjoner utenfor foretakene.

Kommentarer til ekstern tilgang:

Ilustrasjonen viser kun hvordan HSØ-plattformen muliggjør tilgang til tjenester fra eksterne lokasjoner over Internett. Det enkelte helseforetak beslutter og bestiller hvilke systemer som skal være tilgjengelig og hvilke brukere som skal gis tilgang.

Som illustrasjonen viser er det to tilgangsløsninger. Disse løsningene har ulike egenskaper og krav:

- **SSL VPN** - https://start.sykehuspartner.no
  - Portal med publiserte applikasjoner (tilgjengeliggjør Citrix XenApp, WEB og filområder). 2-faktor autentisering: One Time Password (OTP) til registrert mobiltelefon i tillegg til brukernavn og passord på nettverket.
- **MS VPN** – vpn.sykehuspartner.no
  - Prekonfigurert som «VPN» under nettverkskoblinger på alle maskiner i HSØ-SP
  - Løsningen gir brukeren tilgang til det interne nettverket. Prinsippielt er dette som om maskinene var tilkoblet det interne nettverket på foretakets lokasjon, men reglene for hva som skal være tilgjengelig besluttes av hvert enkelt foretak. Likeledes kan ulike grupper av brukere ha ulike tilganger. For eksempel kan man gi en gruppe brukere tilgang til ikke-sensitive systemer og en gruppe med «opphøyde rettigheter» tilgang også til spesifiserte løsninger med sensitive data. OBS! Dette overstyrer ikke applikasjonenes egne autentiserings-mekanismer.
  - MS VPN krever, i tillegg til at brukeren har aktiv konto i SIKT AD, SIKT-sertifikat på maskinen og at brukeren er medlem i AD-gruppe som tillater VPN-bruk..



Figur 3.2 – 1 Tilgang til tjenester

Forklaring til Figur 3.2 - 1

Begrep	**Forklaring**
Interne lokasjoner	Lokasjoner tilhørende respektive helseforetak hvor datamaskin er tilkoblet foretakets nettverk
Eksterne lokasjoner	Alle lokasjoner som ikke faller inn under «Interne lokasjoner». Herunder ligger typisk hjemmekontor og hjemmesykehus, men også HSØ-nettverk på andre foretak enn serverne/tjenestene som benyttes finnes.
Kjente brukere	Aktiv brukerident finnes i SIKT AD
Kjente enheter	Typisk PC som er medlem av SIKT AD
Ukjente enheter	Typisk brukers private PC, nettbrett eller SmartPhone
HSØ Tjenestesoner	Omfatter alle nettverk i den regionale løsningen.
<HF> Tjenester	Nettverkssoner (vlan) som kun inneholder ett foretaks servere og tjenester. Disse sonene er kun tilgjengelig fra respektive foretaks maskiner og brukere.
Høye kontekster	Med «høye kontekster» menes Kontekst 3 og 4.
Lave kontekster	Kontekst 1 og 2.

Fellestjenester	Soner for fellesregionale systemer. Sonene er tilgjengelig fra alle brukersoner i hele HSØ.
Fargekoder for tjenestesoner	Rød = Soner for sensitive data Grønn = Soner for ikke-sensitive data
Fargekoder for brukersoner	Grønn = Interne soner Rød = Ukjente/usikre soner

3.2.1 Klienttyper

Klienttype	Beskrivelse	Applikasjonstilgang	Sikkerhet og autentisering
Stasjonære maskiner	Tradisjonelle klienter basert på Intel/Windows.	Tykk og tynt	Passord Maskinsertifikat
Bærbare maskiner	Mobile klienter basert på Intel/Windows. Maskinene er som oftest personlige.	Tykk og tynt. Mulighet for tilgang til applikasjoner eksternt.	Passord Maskinsertifikat Diskkryptering
Tynne klienter	Klienter med et nedstrippet operativsystem som brukes til å aksessere arbeidsflate i datasenter.	Tynn arbeidsflate enten basert på publisert skrivebord eller virtuell maskin.	Passord Maskinsertifikat
Smarttelefoner	Telefoner som brukes til å aksessere e-post og kalender.	Direkte tilgang fra telefonen til tjenester i datasenteret.	PIN-kode SIM Passord telefon Mulighet for å slette enhet på avstand.
Pasientterminal	Nedlåst klient som brukes av pasienter	Applikasjoner tilgjengelig i kioskmodus eller lignende.	Nedlåst isolert klient.

3.2.1.1 Stasjonære maskiner

Dette er tradisjonelle stasjonære maskiner, basert på Intel/Windows, hvor hovedvekten av brukerens arbeidsflate presenteres tykt, men det kan være innslag av tynne applikasjoner.

I Sykehuspartners varekatalog finnes det til en hver tid gjeldende modeller.

3.2.1.2 Bærbare maskiner

Dette er maskiner som brukes av mobile brukere. Klientene er basert på intel/Windows. Maskinene er ofte personlige. Arbeidsflaten er lik som på stasjonære maskiner, men med ekstra krav til vpn og eksterne løsninger. Det settes også egne sikkerhetskrav til bærbare maskiner som diskkryptering.

I Sykehuspartners varekatalog finnes det til en hver tid gjeldende modeller.

3.2.1.3 Tynne klienter

Dette er klienter for å aksessere tynn arbeidsflate, enten tradisjonell terminalserver eller virtuell desktop. De tynne klientene bør støtte enkelt oppsett ved hjelp av DHCP.

I Sykehuspartners varekatalog finnes det til en hver tid gjeldende modeller.

3.2.1.4 Smarttelefoner

Smarttelefonene brukes for å aksessere e-post og kalender. Telefonene må settes opp med pin-kode både på sim-kort og telefon.

I Sykehuspartners varekatalog finnes det til en hver tid gjeldende modeller.

3.2.1.5 Pasientterminal

Dette er klienter som er ment for pasienter basert på Intel/Windows. Arbeidsflaten er en nedlåst klient i kioskmodus.

Per dags dato er ikke denne type klient i varakatalogen til Sykehuspartner.

3.2.1.6 Operasjonsstuemaskin

Dette er klienter basert på Intel/Windows som er sertifiserte til å stå utplassert inne på operasjonsstuer. Ellers er den lik som en stasjonær maskin.

3.2.2 Terminalservere (TS)

3.2.2.1 Logisk struktur og skille mellom foretak

I HSØ-SP er alle terminalserverne del av samme, felles «farm» for alle foretak, men serverne er foretaks-spesifikke på en slik måte at:

- TS'ene inneholder kun applikasjoner for respektive foretak
- Det er kun brukere fra respektive foretak som får nettverksmessig tilgang til foretakets TS'er
- TS'er tilhørende ett foretak har ikke nettverksmessig tilgang mot andre foretaks tjenester

Unntak er tjenester plassert i lavnivå sikkerhets-soner som er tilgjengelig på tvers av foretakene.

3.2.2.2 Brukergrensesnitt

Brukerne får ikoner til TS-appliksjoner publisert på PC'ens startmeny sammen med eventuelle lokal-installerte applikasjoner. Dette gir en sømløs integrasjon av applikasjoner installert lokalt og på TS og brukergrensesnittet likt.

3.3 Klient- og sesjonssikkerhet

3.3.1 Sikrer og funksjonelle klienter

Klientene skilles ut i dedikerte klientnett som er HF-spesifikke. Klienter som tilfredsstiller kravene til sikkerhet (kap 3.5.2) får direkte tilgang til internett. Tilgangen er beskyttet med proxy-servere, web-filtrering og skanning for skadelig kode i tillegg til antivirus-programmer som skanner klienter, servere og internett-trafikk for virus.

3.3.2 Oppdatering av klienter

Det er etablert en løsning for distribusjon av sikkerhetsoppdateringer til klientene i Microsoft System Center Configuration Manager (SCCM). Denne løsningen er etablert med utgangspunkt i at det skal være enkelt å håndtere oppdateringer og definisjonsfiler (antivirus) for alle type windows klienter for alle foretak på et sentralt sted. SCCM gjør det enkelt å differensiere klientene hvis det skulle være behov for det, jmf. medisinsk tekniske klienter.

3.3.3 Network Access Protection (NAP)

Network Access Protection (NAP) brukes for å hindre uautoriserte klienter eller klienter uten godkjent patch-nivå og antivirus-nivå tilgang til nettverket. Før klienten får tilgang til nettverket verifiseres det at:

- Maskinen tilhører HSØ (sertifikat)
- Oppdaterte sikkerhetspatcher er installert
- Antivirus-service går
- Definisjonsfil for antivirus er oppdatert

Mangler maskinen siste patcher eller antivirus-filer forsøkes dette oppdatert før maskinen gis tilgang til nettverket. Dersom maskinen ikke oppnår status «compliant» (godkjent) vil maskinen bli tilkoblet et karantenenett (802.1x) eller få tilgang til internt nett, men kun med tilgang til oppdateringstjenester (DHCP enforcement).

OBS! Per d.d (nov 2011) er NAP bare tatt i bruk i såkalt «deferred mode» hvor det kun varsles og logges om klienten er «compliant» eller ikke. Klienter som ikke er «compliant» vil i denne modus ikke bli utestengt eller sendt til karantene-nett.

3.3.4 Kryptering av bærbare maskiner

Harddisk/filer på bærbare maskiner hvor det kan lagres data skal krypteres.

3.3.5 Lokale rettigheter på maskiner

I HSØ-SP har brukerne ikke administrator-rettigheter på maskinene og vil ikke kunne installere eller avinstallere programmer. Dette gjelder både stasjonære og bærbare maskiner.

3.3.6 Skjermsparere

Regelen for bruk av klienter som benyttes av flere brukere er at man logger ut når man forlater maskinen. Siden det av ulike årsaker likevel skjer at brukere forlater maskiner uten å logge av er det innført ulike tekniske løsninger for å minimere ulempene og beskytte systemene mot uautorisert innsyn.

Skjermsparere med krav om passord for å få tilgang til maskinen igjen er en viktig del av sikkerheten på arbeidsstasjonene. I HSØ-SP er det definert en generell standard for hvor lenge en maskin skal være inaktiv før skjermsparer aktiveres og låser maskinen. Denne tiden er satt til 15 minutter. Det er imidlertid situasjoner hvor 15 minutter er for kort tid og hvor det er forsvarlig å utvide innslagstiden. Likeledes er det tilfeller hvor 15 minutter er for lenge, for eksempel fordi en maskin står slik plassert at det er stor fare for uautorisert tilgang. Det forsøkes så langt det er mulig å standardisere valgene samtidig med at funksjonen tilpasses behov, mens man samtidig sørger for å gjøre administrasjonen og styringen rundt dette overkommelig.

Følgende standarder og regler er etablert:

- Standard skjermsparer slås på etter 15 minutters inaktivitet.
- For maskiner som står uskjermet slås skjermspareren på etter 1 minutts inaktivitet.
- For maskiner hvor 15 minutter forårsaker vesentlige ulemper er det mulig å har 60 minutters inaktivitet før innslag. Dette kan kun tillates på maskiner som er på lokasjoner godt sikret mot uatorsert tilgang.
- Skjermsparer med “Logg av” funksjon

3.3.6.1 Skjermsparer med “Logg av” funksjon

Det eksisterer en løsning tilknyttet skjermsparer som gjør det mulig for en bruker å logge ut en allerede innlogget bruker hvor maskinen er låst av skjermspareren. Det er viktig å være oppmerksom på at denne funksjonen ikke kan brukes for å logge av bruker når maskinen er låst av bruker med Windowstast+L eller Ctrl+Alt+Del/Lås maskin.

3.3.6.2 “Bytt bruker” funksjon

«Bytt bruker» er standard funksjonalitet i nyere Windows klient-operativsystemer. Funksjonen tillater flere aktive brukersesjoner på samme maskin (omtrent som en terminalserver). En problemstilling knyttet til funksjonen «bytt bruker» er at det lett kan bli flere samtidige sesjoner enn maskinen har kraft til å håndtere. Resultatet blir da en treg maskin eller at denne fullstendig stopper opp og ikke fungerer.

På grunn av noen kompatibilitetsutfordringer med «bytt bruker» er funksjonen deaktivert på visse maskiner. For eksempel støtter ikke talegjenkjenning «bytt bruker» og funksjonen er derfor deaktivert på maskiner med talegjenkjenning.

3.3.6.3 «Bytt bruker med terminering av inaktive sesjoner»

For at det ikke skal bli for mange aktive sesjoner på en klient på grunn av «bytt bruker» vil det kun være tillatt med et visst antall aktive sesjoner. De eldste sesjonene vil termineres.

3.4 Roaming / mobilitet

Med roaming menes muligheten til å kunne arbeide fra forskjellige lokasjoner og det finnes forskjellige scenarier.

3.4.1 Scenarier

Brukere av bærbar maskin som tar denne med mellom lokasjoner og hjemmekontor.

HSØ plattformen har gode muligheter for dette. En HSØ klient vil på alle lokasjoner hvor det finnes et HSØ nett (kabel eller trådløst) kunne nå tjenester som er plassert i kontekst 2. Dette inkluderer e-post, personlige hjemmeområde, eventuelle intranett og andre tjenester tilhørende samme kategori. Hovedregelen er at man ikke når systemer med sensitive data på tvers av HF. For tilgang til tjenester og data i høye kontekster

(sensitive) er det mulig å benytte VPN dersom foretaket tillater dette. På samme måte vil det være mulig fra Internett å nå HSØ ressurser via VPN. Det er foretakene selv som avgjør hvilke tjenester som skal være tilgjengelig fra driftede og ukjente klienter. Det er også foretakene selv som er ansvarlige for at disse tjenestene er tilstrekkelig sikret. HSØ-SP vil understøtte tilgjengeliggjøringen av de tjenestene som foretaket bestiller.

Fjerntilgang fra driftede klienter (VPN)

For tilgang til tjenester fra driftede klient så tilbys en fjerntilgang basert på tykk VPN tilgang. Denne fjerntilgangen er i hovedsak rettet mot administrative brukere som benytter bærbare maskiner. Denne tjenesten benytter maskinsertifikat i tillegg til brukernavn og passord for autentisering. Foretakene bestemmer selv hvilke tjenester de ønsker å gjøre tilgjengelig via denne tjenesten.

Portalløsning brukes også for tilgang til tjenester fra driftede klienter.

Fjerntilgang fra ukjente klienter

For tilgang til tjenester fra ukjente klienter så benyttes det en portalløsning. Denne tjenesten benytter to-faktor autentisering med engangskode i tillegg til brukernavn og passord. Via denne tjenesten kan brukere aksessere interne tjenester som skal være tilgjengelig fra ukjente klienter. Brukerne vil kun se de tjenestene som de har tilgang til.

Fjerntilgang til e-post fra driftede klienter

For fjerntilgang til e-post fra driftede klienter tilbys muligheten for å benytte lokalt installert e-postklient, som overfører trafikken gjennom en kryptert forbindelse. Denne fjerntilgangen er i hovedsak rettet mot administrative brukere som benytter bærbare maskiner. Denne tjenesten muliggjør direkte tilkobling av e-postklienten mot e-postløsningen over internett. Tjenesten benytter brukernavn og passord for autentisering, samt medlemskap i tilhørende tilgangsgruppe for autorisasjon.

3.5 Tilgang til internett

3.5.1 Generelt

Tilgangen til internett leveres ved hjelp av en proxy-løsning. Proxy-servere krever autentisering av bruker for å kunne gi tilgang til internett. Denne autentiseringen gjøres ved hjelp av innebygget autentisering i klientoperativsystemet, og virker derfor sømløst for brukeren. I tillegg benyttes en egen klientprogramvare tilknyttet proxy-løsningen som muliggjør internett tilknytning for applikasjoner som i utgangspunktet ikke støtter bruk av proxy-servere. Ved å kreve autentisering på internett tilgangen så muliggjør dette for logging av trafikk med sporbarhet, samt differensiering av internett tilgang basert på tilgangsgrupper fra katalogtjenesten. Internett tilgangen beskyttes med web-filtrering og skanning for skadelig kode som skanner og eventuelt stopper trafikken før den kommer inn til klienten.

3.5.2 Krav for tilgang til internett

For at en klient skal kunne få tilgang til internett må den oppfylle følgende krav:

- Operativsystemet må være nyere enn Windows XP
- Klienten må følge ordinært driftsrutine med tanke på antivirus patching og group policy.
- Fellesbruker kan ikke brukes.

3.5.3 HF-spesifikke proxyservere

På bakgrunn av at flere foretak benytter eksterne tjenester som pr. i dag benytter brukers eksterne IP adresse for "autentisering", så er det etablert HF-spesifikke proxy løsninger. Dette betyr at hvert foretak får sin egen dedikerte proxyserver som benyttes til all internett trafikk. Det er proxyserveren sin eksterne IP adresse som eksponeres mot internett, og som derfor benyttes for autentisering inn mot disse eksterne tjenestene.

Selv om hvert foretak får sin dedikerte proxyserver, så administreres disse sentralt og benytter i størst mulig grad et felles regelsett.

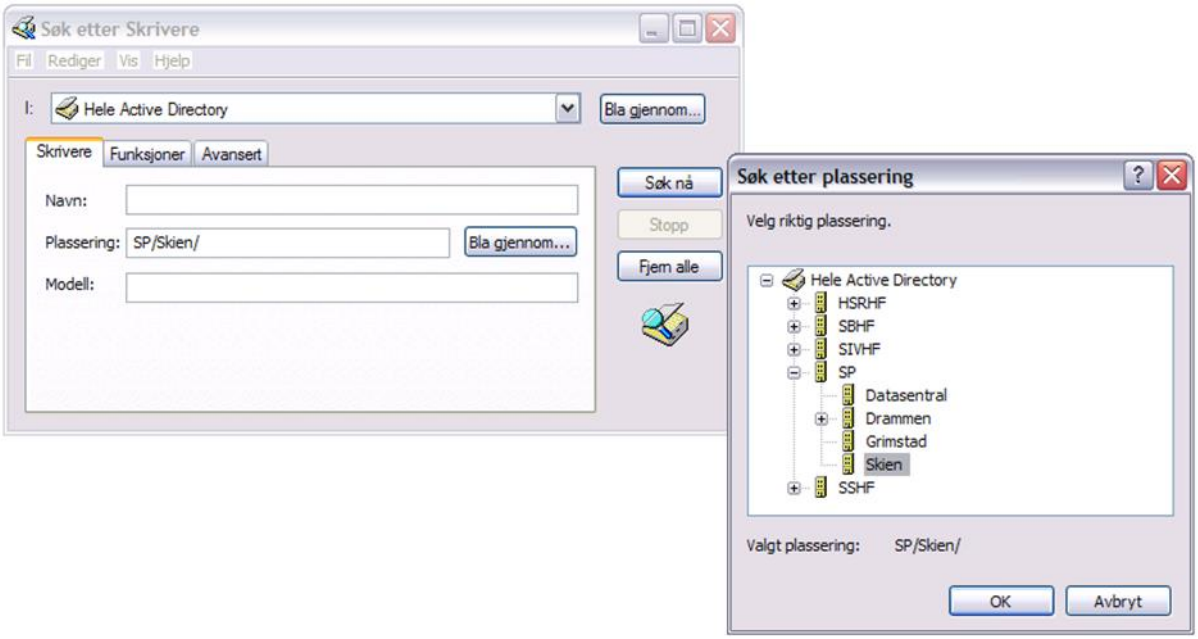
3.6 Fjernadminstrasjon av klienter

Det er etablert en løsning for fjernadministrasjon av klienter. Dette gjør at driftspersonell kan koble seg opp mot brukerens maskin i forbindelse med brukerstøtte. Tilkobling til maskinen krever godkjenning av brukeren på brukerens maskin. Ved hjelp av denne løsningen kan driftspersonell både se brukeren skjerm når brukeren demonstrerer problemet, og samtidig overta styringen av mus og tastatur dersom dette er nødvendig.

3.7 Utskrift

Utskrift baseres på innebygget print-funksjonalitet i klientens operativsystem. Et skript er utarbeidet for å tildele skrivere basert på gruppetilhørighet. Som standard vil da Sykehuspartners driftspersonell kunne administrere skrivertildeling sentralt.

I tillegg kan brukere selv legge til skrivere. Alle skrivere spesifiseres med plassering slik at de er lett å finne for brukerne ved hjelp av Printer Location funksjonen i Active Directory.



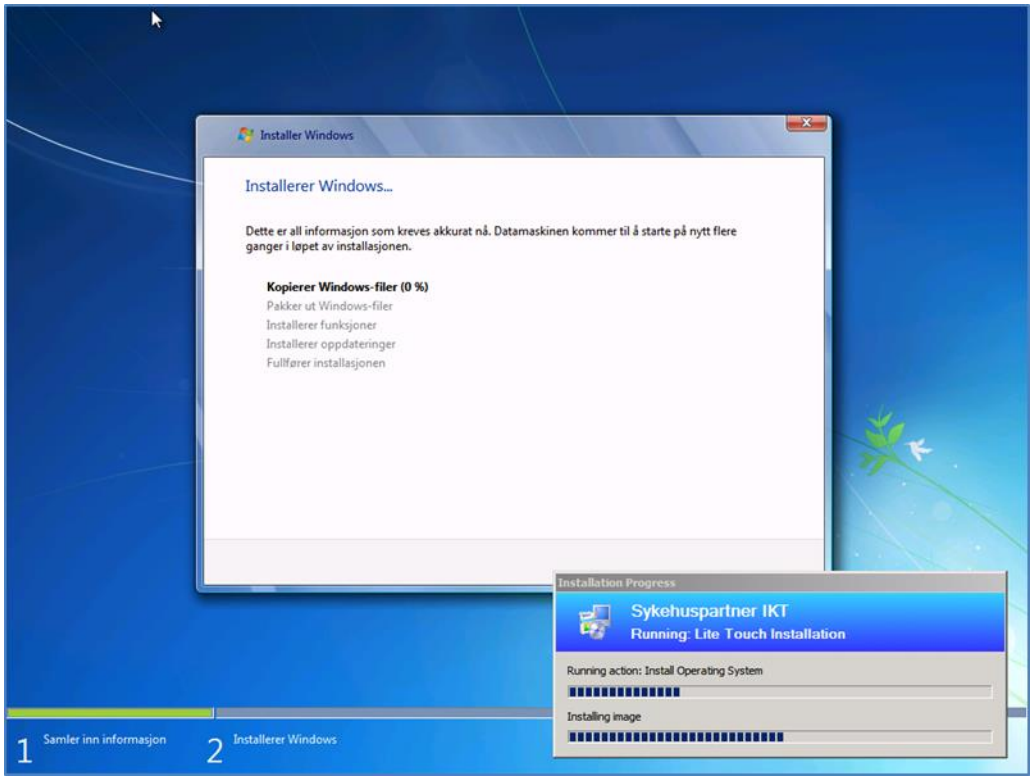
Figur 3.7 – 1 Skriver plassering

Multifunksjonsskrivere kan anskaffes av helseforetakene, og scanning kan tilbys dersom leverandør og produkt støtter dette. Fax, scan og kopi inngår ikke som en standard i plattformen.

3.8 Automatisert installasjon av klienter og programvare

3.8.1 Distribusjonsløsning for operativsystem

Det er etablert en løsning for automatisert installasjon av maskiner. Denne tjenesten benytter oppstart fra nettverk for å starte en strippet versjon av klientoperativsystemet som lastes inn i minnet på maskinen. SCCM brukes for å administrere løsningen. Alt styres sentralt og ingen valg gjøres lokalt, såkalt zero-touch. Det er laget en applikasjon som teknikerne som ruller ut maskiner kan bruke for enkelt å betjene utrullingene.



Figur 3.8 – 1 Distribusjon av operativsystem

3.8.2 Distribusjonsløsning for applikasjoner (SCCM)

I HSØ benyttes SCCM (System Center Configuration Manager) som verktøy for å distribuere applikasjoner. Distribusjonen styres av et samspill mellom SCCM-server og agent installert på den enkelte klient.

Applikasjoner i HSØ distribueres i hovedsak til maskin og ikke til bruker. Hver enkelt maskin meldes inn i AD-grupper for samtlige applikasjoner som skal være tilgjengelig på maskinen og følger ikke bruker.

MSI-pakker for SCCM plasseres på DIST-serverne tilhørende foretaket. De distribuerte DIST-serverne på foretakslokasjonene vedlikeholdes automatisk fra sentrale servere i regionalt datasenter. DIST-servere plasseres på lokasjoner hvor det ellers ikke er servere eller datarom for å få en mest mulig optimal ytelse for brukerne både ved «tanking», oppdateringer og applikasjons-distribusjon. Hvilke lokasjoner som får slike servere avhenger i vesentlig grad av antall brukere på lokasjonen kombinert med båndbredde mot sentrale serverrom. Se for øvrig kap. 7.1 for serverdesignet på de forskjellig type lokasjonene.

4 IDENTITETS- OG TILGANGSSTYRING

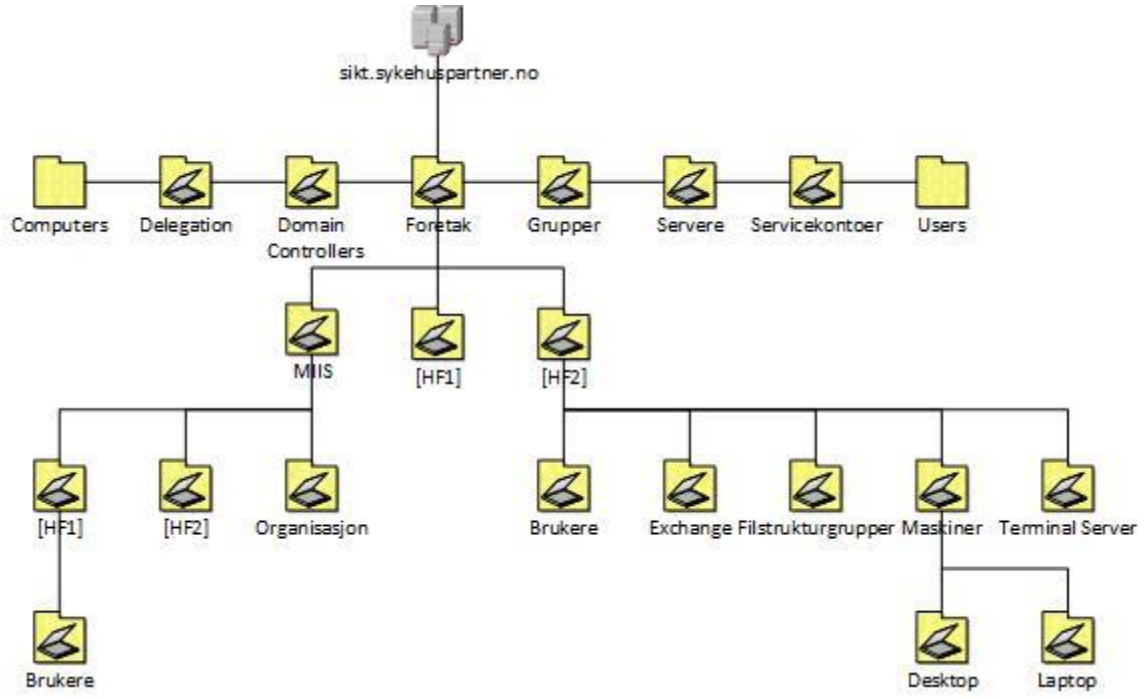
4.1 Katalogtjeneste

Katalogtjenesten benyttes for håndtering av brukere, brukerrettigheter, og ressurskontroll, og gir muligheter for å administrere maskiner, kjøre script og tilpasse lokale oppsett. Tjenesten består av en database som lagrer og organiserer bruker-, maskin- og gruppeobjekter med mer. Katalogtjenesten er sentral under pålogging til maskiner og tjenester innenfor en IKT plattform, og vil derfor anses som en kritisk funksjon. Ved å benytte én felles katalogtjeneste i regionen vil man kunne tilby en felles database med oversikt over alle brukere og grupper i regionen, som dermed kan benyttes for tilgangsstyring inn til tjenester og ressurser.

4.1.1 Logisk struktur

Forest, Domener og Organizational Units (OU) bygger opp den logiske strukturen i en katalogtjeneste basert på Active Directory. Helse Sør-Øst sin katalogtjeneste består av en Single Domain Forest, men vil også inneholde knytninger til flere Forests i forbindelse med omlegging av helseforetakene. Domenet sikt.sykehuspartner.no er strukturert slik at hvert enkelt helseforetak (HF) eksisterer under egne Origanizational Units (OU). Denne inndelingen muliggjør en enklere styring av Group Policyer samt andre foretaksspesifikke tilpasninger selv om disse eksisterer innenfor et og samme domene i katalogtjenesten. I tillegg muliggjør dette en oversiktlig metode for delegering av rettigheter innenfor enkelte foretak.

Figuren under viser de viktigste delene av OU strukturen i domenet sikt.sykehuspartner.no.



Figur 4.1 – 1 Katalogtjeneste logisk struktur

OU	Beskrivelse
Foretak	Inneholder alle ressurser for de forskjellige foretak som er på løsningen.
Foretak / MIIS	Objekter under her administreres automatisk av metakatalogen (MIIS, beskrevet i kapittel 4.2) og endringer må ikke skje manuelt.
Foretak / MIIS / Organisasjon	Inneholder alle organisasjonsgrupper som stammer fra PAGA og som opprettes av metakatalogen.
Foretak / MIIS / [HF] / Brukere	Inneholder brukere som administreres automatisk av metakatalogen.
Foretak / [HF] / Brukere	Inneholder brukere som opprettes manuelt.
Foretak / [HF] / Exchange	Inneholder ressurskontoer (møterom og lignende) samt grupper tilhørende disse.
Foretak / [HF] / Filstrukturgrupper	Inneholder egne tilgangsgrupper for styring av rettigheter i filstrukturene til helseforetaket.
Foretak / [HF] / Grupper	Inneholder applikasjonsgrupper, sikkerhetsgrupper og distribusjonslister som vedlikeholdes manuelt.
Foretak / [HF] / Maskiner	Det finnes flere ”Maskiner” OU’er for forskjellige type maskiner og OS. Disse brukes for å sette maskin GPO (Group Policy Objekter).
Foretak / [HF] / Terminal Server	Inneholder eventuelt foretakets terminalservere

Tabell 4.1 – 1 OU struktur

4.1.2 Fysisk struktur

Den fysiske strukturen i katalogtjenesten gjenspeiler normalt kommunikasjonslinjer og fysiske lokasjoner. Dette er gjort for å optimalisere prosesseringen av synkronisering og regelsett. Det gjør blant annet at klienter skal kunne benytte instanser av tjenester som er plassert i geografisk nærhet til klienten der dette er mulig. Eksempel på slike tjenester er f.eks. påloggingsserver til katalogtjenesten, samt distribusjon- og filservere.

4.2 Metakatalog

Det er etablert en metakatalog for identitetshåndtering. Denne metakatalogen leser brukerinformasjon fra Helse Sør-Øst sitt personalsystem (PAGA) og populere dette til katalogtjenesten. Metakatalogen utfører følgende oppgaver:

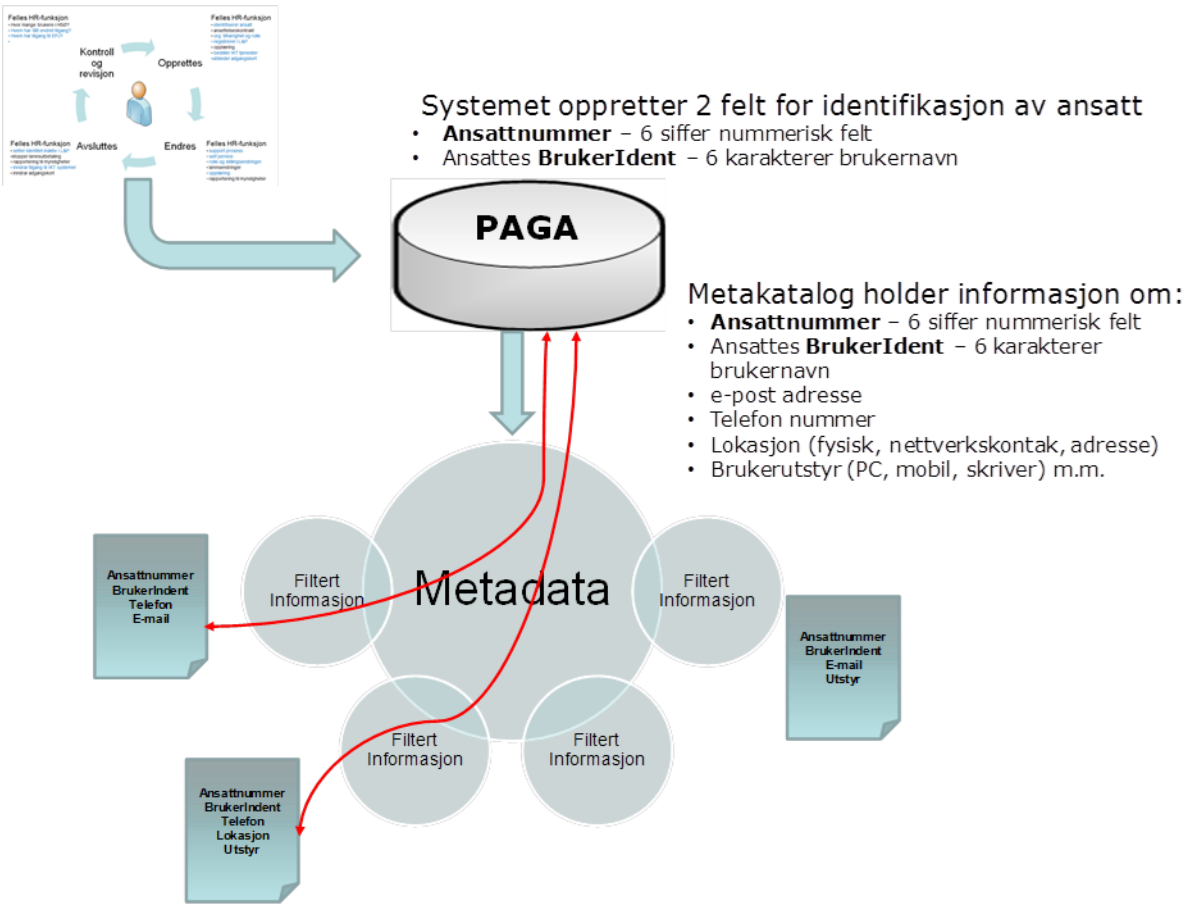
- Oppretter og vedlikeholder brukerkontoer i katalogtjenesten
- Oppretter og vedlikeholder brukernes postbokser i e-postløsningen
- Oppretter brukernes hjemmeområder på filserver
- Oppretter og vedlikeholder organisasjonsgrupper i katalogtjenesten på bakgrunn av organisasjonsstruktur i personalsystemet

Dette betyr at mye av brukeradministrasjonen utføres av personalavdelingen gjennom personalsystemet. Enhver endring av struktur i metakatalogen vil derfor medføre endringer i katalogtjenesten eller på filområder.

Organisasjonsstrukturen fra personalsystemet benyttes for å lage distribusjonslister i e-postløsningen og filområder på fellesområdet. Sikkerhetsgruppene som lages fra personalsystemet (som er de samme som blir distribusjonslister) benyttes til å sette rettigheter på filstrukturen. Sikkerhetsgruppene fra personalsystemet benyttes også i andre sammenhenger. Det kan for eksempel være å gi rettigheter til programmer og programdata.

Endringer på brukerkontoer skal ikke foregå i katalogtjenesten, og eventuelle utførte endringer vil bli overskrevet ved kjøring av neste uttrekk fra personalsystemet. Unntakene gjelder stort sett endring av brukers passord og å gi en bruker tilgang til tjenester/applikasjoner.

Eksterne konsulenter skal registreres i personalsystemet på lik linje med vanlige ansatte, og vil automatisk få opprettet brukerkonto på grunnlag av disse dataene.



Figur 4.2 – 1 Metakatalog som kilde

4.2.1 Brukere med arbeidsforhold på flere foretak

Det er besluttet at det skal benyttes én felles brukerident pr. ansatt i Helse Sør-Øst. Dette skaper flere problemstillinger i forbindelse med ansatte som har flere arbeidsforhold innenfor helseregionen. Det er derfor besluttet at inntil man har en god løsning for håndtering av disse problemstillingene, så vil det opprettes unike brukeridenter pr. foretak hvor man har et arbeidsforhold. Konsekvensen av dette er at brukere med flere arbeidsforhold får flere brukerkontoer (inklusive e-post).

For hovedarbeidsforholdet opprettes og vedlikeholdes tilhørende brukerident av metakatalogen på bakgrunn av informasjon fra PAGA. Mens for de sekundære arbeidsforholdene benyttes det manuelle rutiner, og vedlikehold.

4.3 Identitetsføderasjon

Identitetsføderasjon er en teknologi som har til hensikt å muliggjøre portabilitet av identitetsinformasjon på tvers av ellers autonome sikkerhetsdomener. Målet er å tilby sømløs og sikkert tilgang til tjenester i et sikkerhetsdomene for brukere som befinner seg i et annet sikkerhetsdomene. Dette skal gjøres uten at brukeren blir bedt om å utføre en ny pålogging, og uten å medføre dobbel brukeradministrasjon. Løsningen baserer seg på at tjenester i et sikkerhetsdomene stoler på autentisering av brukeren som er gjort i det sikkerhetsdomene der brukeren er definert, og gir brukeren tilgang til tjenesten på bakgrunn av informasjon som oversendes fra brukerens sikkerhetsdomene i forbindelse med tilkoblingen til tjenesten.

I HSØ-SP er det etablert en sentralisert tjeneste for identitetsføderasjon. Hensikten med denne tjenesten er å kunne tilby sømløs tilgang til fellestjenester og eventuelt eksterne tjenester, basert på brukerautentiseringen som utføres i brukerens lokale brukerkatalog. Dette muliggjør en sømløs tilgang til felles webtjenester på tvers av eksisterende IKT plattformer, frem til regionen er samlet på en felles IKT plattform. I tillegg vil denne tjenesten benyttes for å sikre en sømløs tilgang til eksterne webtjenester som for eksempel Personalportalen, uten av brukeren blir bedt om å utføre en ny pålogging mot den eksterne tjenesten.

Denne tjenesten for føderering av identiteter er etablert på med tanke på regional drift og overvåkning, samt en sentralisert tilkobling av eksterne tjenester som deretter kan konsumeres på tvers av IKT plattformene i regionen.

4.4 Sertifikater

Det er i HSØ-SP tatt i bruk to typer sertifikater:

- Offentlige sertifikater

Disse sertifikatene er kjøpt fra Verisign og benyttes på eksterne tjenester som skal kunne konsumeres fra klienter som ikke tilhører HSØ-SP, slik som hjemme PCer og maskiner på nettkafé.

- Private sertifikater

Det er etablert en intern sertifikatserver på HSØ-SP. Sertifikater fra denne sertifikatserveren benyttes først og fremst ved tilkobling til fjerntilgangsløsningen for HSØ maskiner og WLAN, da disse tjenestene krever sertifikater for autentisering. I tillegg benyttes sertifikater fra denne sertifikatserveren til tjenester som benytter kryptert kommunikasjon slik som HTTPS. Maskinsertifikater deles ut automatisk til alle klienter og servere i domenet via Group Policy. Alle klienter og servere som er medlem av katalogtjenesten stoler automatisk på sertifikater fra denne sertifikatserveren.

Ved en mer omfattende bruk av sertifikater, f.eks. ved bruk av smartkort for autentisering mot klientene på HSØ-SP så bør det etableres en komplett PKI infrastruktur med flere nivåer av sertifikatservere.

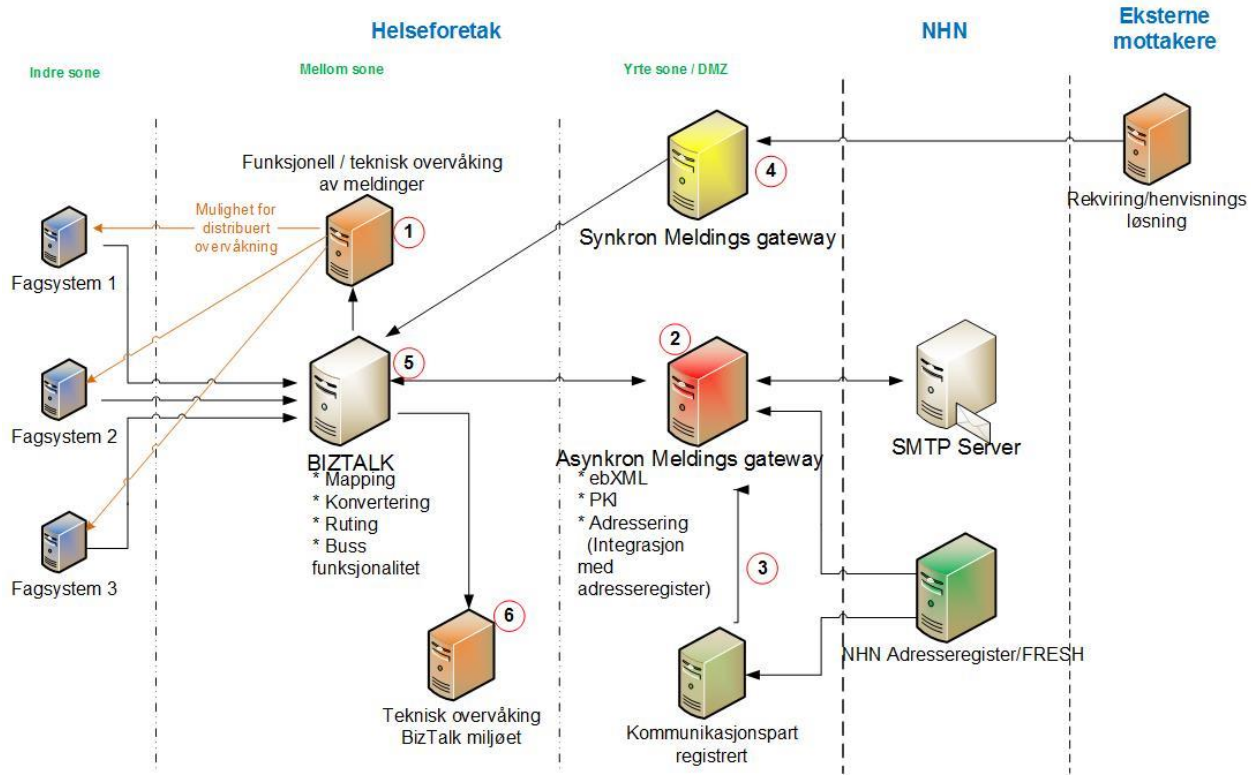
5 INTEGRASJONSTJENESTE

Den tekniske integrasjonsplattformen består av komponenter som understøtter funksjonell, robust og sikker informasjonsutveksling mellom applikasjoner i et helseforetak, og mellom helseforetak og eksterne parter som f.eks. primærhelsetjenesten.

Hovedkomponentene er:

- Integrasjonsmotor for ruting, konvertering og transformasjon
- Teknisk monitorering/overvåking
- Funksjonell monitorering/overvåking
- Meldingsgateway/kryptering og signering for ekstern kommunikasjon
- Kommunikasjonspartregister

I gjeldende versjon av HSØ-SP, vil det ved omlegging vurderes gjenbruk av eksisterende integrasjonstjenester eller nyetablering. Standardiserte komponenter gjelder også ved nyetablering, og målbildet for integrasjonstjenesten (utarbeidet i program IKT-plattform) vil ligge til grunn for beslutninger og produktvalg.



Figur 5 - 1 Logisk fremstilling av integrasjonskomponenter.

Samhandlingsscenarioer som støttes i integrasjonsplattformen:

- Internt i helseforetaket
- Mellom helseforetak og primærhelsetjenesten
- Mellom helseforetak og kommunehelsetjenesten

- Mellom helseforetak
- Mellom helseforetak og kvalitetsregistre
- Mellom helseforetak og myndigheter
- Mellom helseforetak og ansatte (sms fra GAT)
- Mellom helseforetak og pasienter (timepåminnelser)

Tabellen nedenfor viser tilgjengelige integrasjoner.

Intern i helseforetak	Rekvisisjon medisinsk biokjemi
	Rekvisisjon mikrobiologi
	Rekvisisjon radiologi
	Svar medisinsk biokjemi
	Svar mikrobiologi
	Svar medisinsk biokjemi
	Svar radiologi
	Folkeregisteroppslag
Eksternt	Rekvisisjon medisinsk biokjemi
	Rekvisisjon radiologi
	Henvisning
	Svar medisinsk biokjemi
	Svar mikrobiologi
	Svar radiologi
	Epikrise
	Svar patologi
	Oppgjørskrav HELFO
	NPR-rapportering
	Neonatalmelding
	Avbruddsmelding

Figur 5 – 2 Tilgjengelige integrasjoner

MERK! Integrasjonsplattformen vil kunne støtte andre samhandlingsscenarier, og katalogen over støttede integrasjoner kan utvides etter behov gjennom utviklingsprosjekter.

6 STØTTETJENESTER

Dette kapittelet omhandler komponenter knyttet til plattformtjenestene Applikasjonsmiljø, Databaser og prosessering, Datalagring og sikring, samt andre basis tjenester i plattformen.

6.1 Server

Det er etablert en standard for hvordan nye servere skal konfigureres. Den gjeldende standarden for servere justeres i henhold til utviklingen innenfor produktområdene. Som standard leveres en server med et gitt konfigurasjonsoppsett i henhold til Gjeldende Produktliste (GPL), samt agenter for overvåking og detektering av ondsinnet kode. I tillegg herdes serverne i henhold til prosedyrer for serverherding, og oppdateres i henhold til gjeldende godkjente sikkerhetsoppdateringer. Installering av virtuelle servere og allokering av virtuell kapasitet blir utført av Sykehuspartner ut i fra bestilling fra kunde.

6.1.1 Servervirtualisering

Alle nye servere vil etableres som virtuelle servere. Dette skyldes at virtualisering er en fremtidsrettet og velutviklet teknologi. Virtualisering gir enklere administrasjon, økt sikkerthet og bedre tilgjengelighet. Virtualisering gir også gevinster som for eksempel kort leveringstid på nye servere, og gir et skalerbart og fleksibelt miljø.

På bakgrunn av dette er det etablert infrastruktur for virtualisering av servere både i regionale datarom, men også ute på mindre lokasjoner. Dette gjør det enklere å regionalisere driften av serverne, samtidig gjør bruk av virtualisering også at man blirmer uavhengig av den underliggende maskinvaren, og dermed mindre sårbar.

Ved å benytte virtuell infrastruktur bygger man høyere tilgjengelighet på alle servere, samtidig som kompleksiteten ikke øker slik den gjør ved å bygge tilgjengelighet med tradisjonell cluster teknologi. Dette gjør også at man velger å flytte tjenester som krever høy tilgjengelighet vekk fra komplekse cluster løsninger, og over på virtuell infrastruktur.

6.1.2 Fysiske servere

Det vil fortsatt være tjenester som er avhengig av å kjøre på fysiske servere, enten fordi programvaren ikke støtter det, eller at leverandøren ikke supporterer det. I tillegg vil det være tjenester som har definerte oppetidskrav i SLA som tilsier at tjenestene må etableres med cluster teknologi for å kunne tilby det ønskede tjenestenivået.

6.2 Lagring og backup

6.2.1 Lagring

Sykehuspartner benytter i dag både blokkbasert og filbasert lagring. Blokkbasert lagring leveres i flere nivåer. Det benyttes autotiering mellom nivåene internt i lagringsenheter for å oppnå den ytelsen og responsen som ønskes. På filbasert lagring benyttes policy baserte regelsett for å flytte filer til det lagringsmediet der filen høre hjemme basert på regelsettet. (Eksempel: filer som ikke er aksessert på 6 mnd kan automatisk migreres til tregere disk). På HSØ-SP er det standardisert både på verktøy, arbeidsmetodikk og lagringsmedier, dette for å jobbe mest mulig effektivt sentralt mot lagringsenheter. På HSØ-SP benyttes virtualiseringsteknologi og tynn provisjonering innen lagring. For å bygge effektive løsninger må løsningene være relativt store, og det er da en fordel å konsolidere lagring fra mange mindre løsninger til færre store løsninger.

Der blokkbasert lagring deles ut direkte til hoster, gjøres dette via dedikert fiberbasert lagringsnett. Sykehuspartner standardiserer på produkter innen SAN svitsjer og hostbuss adaptere som er en del av dette nettverket. Blokkbasert lagring deles ut som lagring til objektbasert lagring via Network Attached Storage (NAS). NAS tilgjengelig gjør filsystemer for filbasert lagring via ordinært LAN.

SP standardiserer på 3 nivå blokkbasert lagring, og tre nivå filbasert lagring som tilbys kunder.

Type	**Disk**	**Bruksområde**
Type A	Høyhastighetsdisk	Høyhastighetsdisk til databaser og store filservere.
Type B	Høyhastighetsdisk	Høyhastighetsdisk til produksjonsdisk på filserver og standard server.
Type C	Disk	Benyttes til arkiv, backup og staging.

Tabell 6.2 – 1 Lagringsnivåer

SAN er også blitt en særdeles viktig komponent i en virtualisert infrastruktur, ettersom all data lagres ned til SAN for å være tilgjengelig på tvers av maskinvaren som understøtter den virtuelle infrastrukturen. Dette betyr også at bruken av SAN kapasitet øker betydelig i forbindelse med at mer og mer skal virtualiseres.

6.2.2 Backup

Backupløsningene standardiseres produktmessig, slik at det benyttes samme produkt på alle driftsinstallasjoner. Det benyttes teknologier som VAPI mot virtualiseringsplattformer, snapshot teknologier, integrasjon mot VSS. Det benyttes deduplisering både på klientside og serverside. Langsiktig mål bilde er innføring av arkivløsninger med replikering. Det vil bety at statiske data i arkiv som er duplisert vil anses som sikre i form at de vil ligge geografisk spredd, med lås mot sletting. De dynamiske data som ikke ligger i arkiv, vil det bli tatt ordinær backup av.

Sykehuspartner leverer i dag en standard backup policy for tjenester. Det leveres custom backup policy for ønsker som ikke passer inn i standard policy. All backup må bestilles. Det må defineres hva det skal tas backup av. Det er ingen automatikk i slike prosesser.

Bestilling av sikkerhetskopiering av anviste data til tape, følger dette mønsteret:

- Full backup en gang i uken, varighet 3 måneder.
- Inkrementell backup 6 dager i uken, varighet 1 måned.
- Full månedsbackup en gang i måneden, varighet ett år.

6.3 Database

Det er etablert en infrastruktur hvor Sykehuspartner kan tilby databasetjenester på flere databaseplattformer. Det er valgt foretrukne databaseplattformer for å kunne standardisere denne tjenesten. Det kan også tilbys tjenester på andre databaseplattformer, men da etter vurdering i hvert enkelt tilfelle.

Avhengig av antall brukere på databasen, størrelsen på databasen og oppetidskrav tilbys det ulike konfigurasjonsalternativ for disse databasene.

Tjenester som utføres i forbindelse med drift av databasene er optimalisering og tuning, tjenesterapportering på utvalgte databaser, backup og eventuelt restore, endringsstyring, oppsett av databasene og eventuelt terminering.

6.4 Filserver

På HSØ-SP er foretakets dataområder splittet slik at hjemmeområder og profilområder er plassert i Kontekst 2 (Tabell 2.3), og fellesområder og programområder i Kontekst 4 (se tabell). Dette medfører behovet for minst to filservere pr. lokasjon/foretak.

For ikke å belaste WAN-linjer unødig og for nærhet til data plasseres det lokale filservere til hjemmekataloger og profiler for brukere med tilknytning til foretakets hoved lokasjon, og i Regionalt Datasenter (pr. i dag identifisert med SDS) for brukere tilknyttet øvrige lokasjoner. Fellesområder og programområder (filbaserte databaser og lignende) ligger på felles server for alle i foretaket som er plassert i SDS.

Prinsipper:

- Filserverne settes opp til kun å vise de filer og mapper som den enkelte bruker har tilgang til.
  - På denne måten blir fellesområder og andre lignende dataområder mer oversiktlige for brukerne.
- Kun ett helseforetak pr. filserver
- Ikke benytte norske tegn i navn på filshare.

6.4.1 Struktur og dataområder

Distribuert Filsystem (DFS) benyttes for å skjule den fysiske strukturen med server navn i Universal Naming Convention (UNC) filbanene. Strukturen for dataområder pr. foretak ser slik ut:

DFS-share	**Stasjonsbokstav på klient**
\\sikt.sykehuspartner.no\Data\<HF>\ Brukere	(P:)
\\sikt.sykehuspartner.no\Data\<HF>\ Felles	(O:)
\\sikt.sykehuspartner.no\Data\<HF>\ Profiler	
\\sikt.sykehuspartner.no\Data\<HF>\TSProfiler	
\\sikt.sykehuspartner.no\Data\<HF>\ Programmer	(S:)
\\sikt.sykehuspartner.no\Data\<HF>\ Programdata	

Figur 6.4 – 1 DFS strukur

For helseforetak der det er behov for å plassere ut filservere på flere lokasjoner, er det etablert følgende standard for dataområdene på disse filserverne:

DFS-share	**Stasjonsbokstav på klient**
\\sikt.sykehuspartner.no\Data\<HF>\<GEOKODE>\Brukere	(P:)
\\sikt.sykehuspartner.no\Data\<HF>\<GEOKODE>\Profiler	
\\sikt.sykehuspartner.no\Data\<HF>\<GEOKODE>\TSProfiler	

Figur 6.4 – 2 DFS strukur (opsjon)

Disse dataområdene brukes på følgende måte:

- Hjemmeområder og profilområder defineres på det enkelte brukerobjekt og settes av metakatalogen (se kap 4.2 for forklaring på metakatalog)
- Fellesområder og programområder kobles opp av HF spesifikt logonskript
- Terminalserverprofiler (TSProfiler) styres som regel via Group Policy Objekter knyttet til den enkelte terminalserver løsning.

6.4.2 Hjemmeområder og profilområder

På hjemmeområdene og profilområdene (Profiler og TSProfiler) har man valgt å strukturere dataområdene under forbokstav i fornavnet til brukeren. På denne måten vil man få en mer fleksibel måte å spre dataområdene i forbindelse med vekst på datamengden. Dette gir en veldig skalerbar håndtering av disse dataområdene. Dette betyr også at man har valgt å koble opp filshare mot DFS strukturen ved å benytte bokstav som monteringspunkt.

Strukturen i DFS for disse dataområdene pr. foretak vil derfor se slik ut:

\\sikt.sykehuspartner.no\Data\<HF>\brukere\A

\\sikt.sykehuspartner.no\HF\Profiler\A

\\sikt.sykehuspartner.no\HF\TSProfiler\A

Strukturen lokalt på filserverene for disse dataområdene vil se slik ut:

Dataområde	**Filshare**
D:\Data\<HF>\Brukere\A	HF-BrukereA$
D:\Data\<HF>\Profiler\A	HF-ProfilerA$
D:\Data\<HF>\TSProfiler\A	HF-TSProfilerA$

Figur 6.4 – 3 Filstruktur for personlige områder

6.4.3 Fellesområder

På fellesområdene har man valgt å strukturere dataområdene pr. klinikk. På denne måten vil man få en mer flesibel måte å spre dataområdene i forbindelse med vekst på datamengden. Dette gir en veldig skalerbar håndtering av fellesområdene. Dette betyr også at man har valgt å koble opp filshare mot DFS strukturen ved å benytte klinikk som monteringspunkt.

Strukturen for hjemmeområdene pr. foretak vil derfor se slik ut:

\\sikt.sykehuspartner.no\Data\HF\felles

\\sikt.sykehuspartner.no\Data\HF\felles\Klinikk

\\sikt.sykehuspartner.no\Data\HF\felles\Klinikk\Avdeling

\\sikt.sykehuspartner.no\Data\HF\felles\Klinikk\Felles

Strukturen lokalt på filserverene for disse dataområdene vil se slik ut:

Dataområde	**Filshare**
D:\HF\Felles\klinikk	HF-Klinikk$

Figur 6.4 – 4 Filstruktur for fellesområder

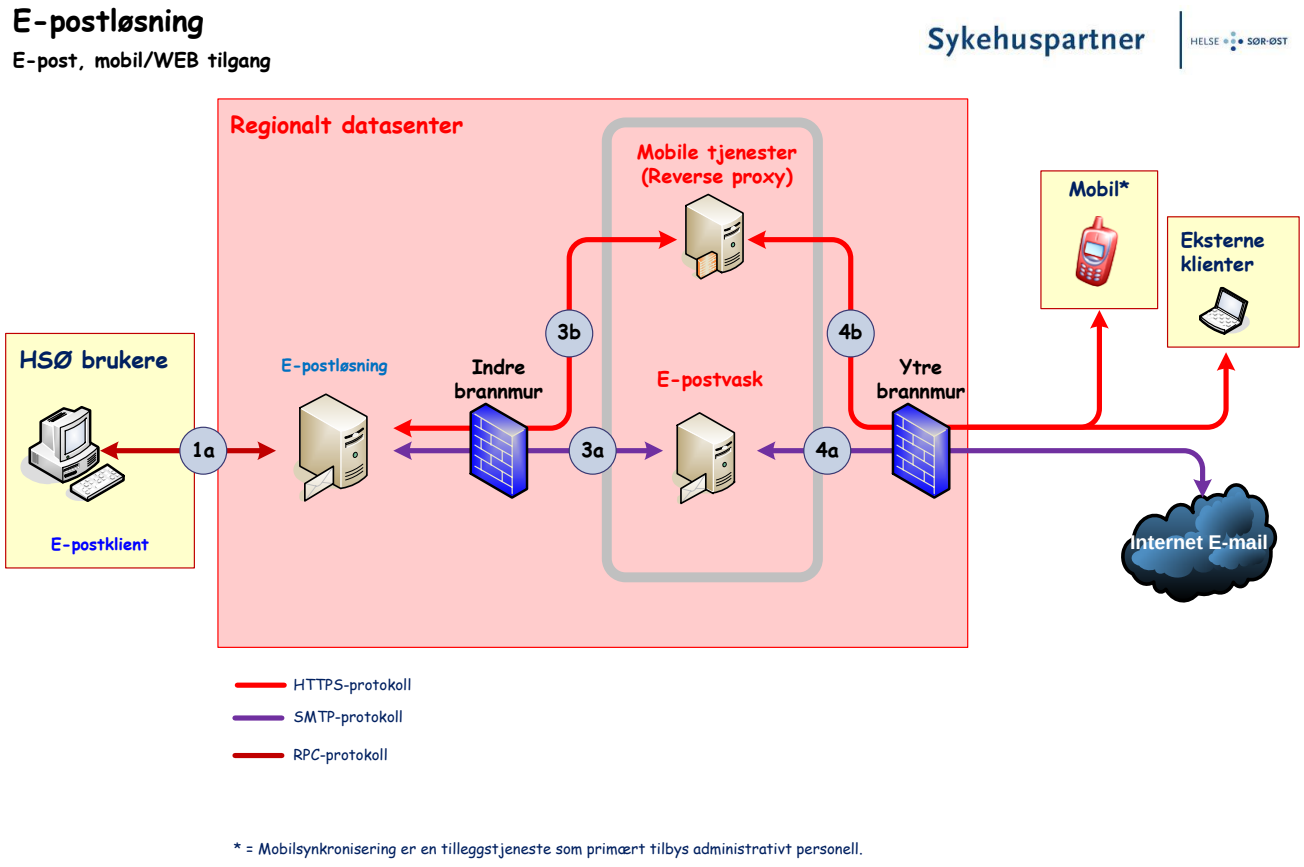
6.5 E-post

På HSØ-SP er det etablert en sentralisert løsning for håndtering av E-post og kalender. Denne løsningen benyttes av alle foretak på plattformen. Løsningen inkludert alle roller og tjenester er etablert på infrastruktur i regionalt datarom. Selv om alle foretak benytter den samme infrastrukturen, så er foretakene delt inn i egne

lagringsgrupper og postboks databaser som gjør at man får et logisk skille på foretakene sine data. Derimot benyttes det felles servere for transport av e-post uavhengig av foretak.

Løsningen er likevel etablert på en slik måte at det vil være mulig å skille ut et enkelt foretak på egne servere dersom det skulle komme krav om dette.

Ved siden av å benyttes til e-postutveksling, informasjon og kalender for alle foretak på HSØ-SP, så fungerer også denne tjenesten som plattform for utveksling av e-post og eventuelt kalenderinformasjon for applikasjoner og systemer som er etablert på denne plattformen.



Figur 6.5 – 1 E-postløsing

7 DATASENTER

7.1 Lokasjoner og serverroller

Dette kapittelet oppsummerer hvilke server roller og tjenester som skal være fysisk tilstede på lokasjoner av forskjellig type og størrelse.

Et utgangspunkt for design av løsningen har vært et ønske om størst mulig grad av sentralisering. Det er imidlertid flere forhold som gjør at en 100% sentralisering ikke vil være mulig:

- Krav om at en lokasjon skal være autonom

Viktige tjenester skal være tilgjengelig selv om sentral løsning er utilgjengelig

- Mangelfull båndbredde og høy forsinkelse i nettverket

7.1.1 Regionalt datarom

Her skal alle sentraliserte tjenester plasseres. Dette inkluderer regionale fellestjenester, og mange av infrastrukturtjenestene tilhørende HSØ-SP. Dette er foretrukket lokasjon for etablering av nye tjenester innenfor regionen. Her bygges infrastrukturen med fokus på høy oppetid og redundans for å kunne tilby den grad av tilgjengelighet som kreves av sentraliserte tjenester. Dette er også et felles kontaktpunkt mot internett for foretakene.

Sentrale datarom vil også ha alle server roller som brukes av organisasjoner/lokasjoner uten egen lokal serverinfrastruktur.

Eksempler på tjenester:	E-post
	Integrasjonsløsning
	Fil (sentraliserte filservere)
	Internett tilgang

7.1.2 Hovedlokasjon

Kjennetegn:	Hovedlokasjoner med egne datarom som inneholder et eller flere kritiske fagsystemer. Etablerer lokale installasjoner av tjenester som er kritiske for å sikre pålogging til klient og lokalt plasserte fagsystemer ved et eventuelt bortfall av kommunikasjon mot Sentral Datasentral.
Server(e):	Domenekontroller
	Printserver
	Filserver
	Terminalservere (dersom foretaket har bruk for dette)
	Distribusjonsserver (OS og Applikasjon, ref. kap. 3.8)

7.1.3 Stor lokasjon

Kjennetegn:	Store lokasjoner med mange brukere som på grunn av båndbredde ikke kan belaste nettverket med all kommunikasjon. Etablerer printserver og filserver lokalt ved behov, for å spare belastningen på WAN forbindelse.
Server(e):	Distribusjonsserver (OS og Applikasjon)

Printserver (ved behov)

Filserver (ved behov)

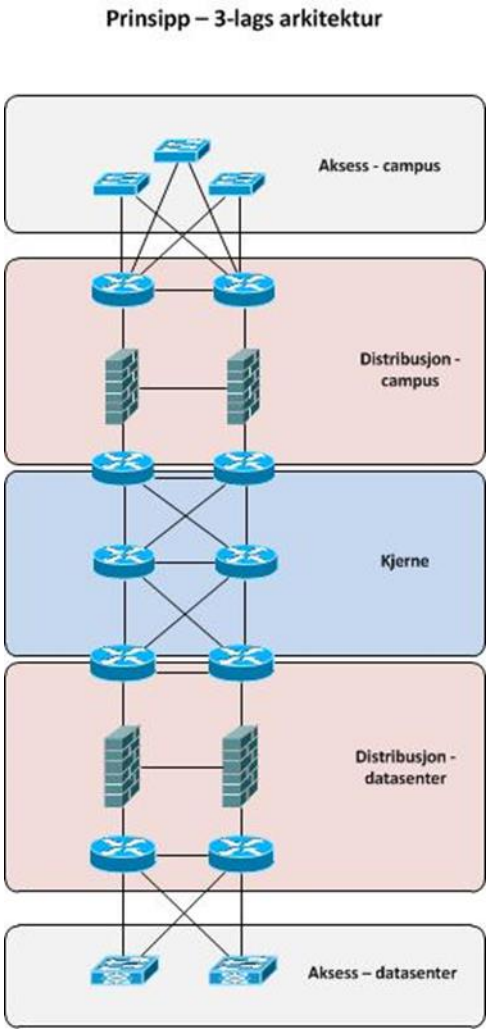
7.1.4 Liten lokasjon

Kjennetegn:	Lokasjoner med få brukere. Konsumerer de fleste tjenester fra foretakets hovedlokasjon eller Sentral Datasentral. Har ikke noe eget datarom som egner seg for plassering av lokale tjenester. Etablerer distribusjonsserver ved behov, for å spare belastningen på WAN forbindelse.
Server(e):	Distribusjonsserver (OS og Applikasjon, ved behov)

8 NETTVERK

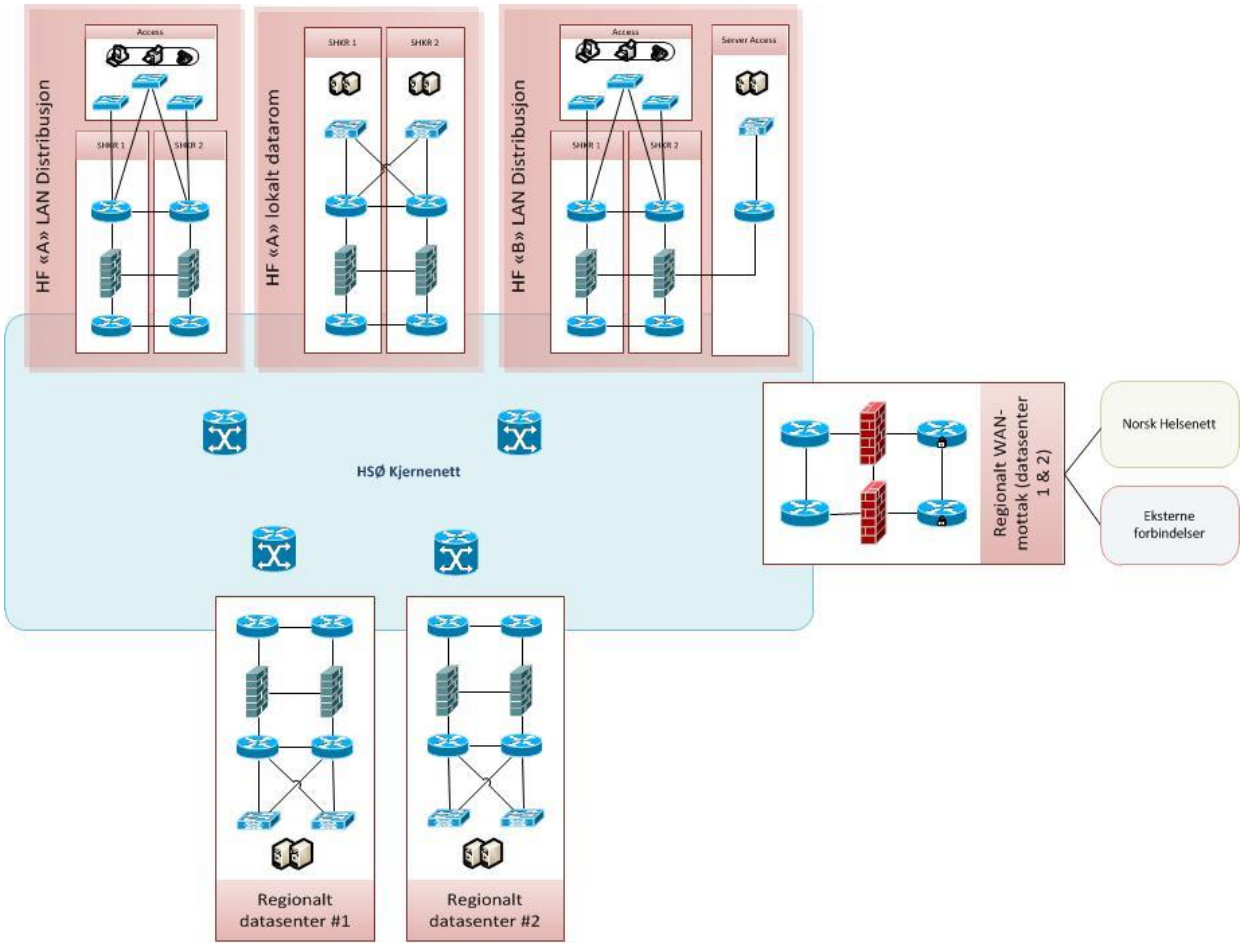
8.1 Oversikt

Den etablerte nettverksplattformen er basert på en 3 lags arkitektur bestående av et aksesslag for tilkobling av endeutstyr (klienter og servere), et distribusjonslag med ruter og brannmur, og en kjerne som ruter trafikk mellom klientnett og datasenternes servernettverk. Se figur 9.1-1.



Figur 8.1 - 1 Prinsipp – 3-lags arkitektur

Figur 9.1-2 viser prinsipp for HSØ-nettverket. Designet består av moduler som kobles på et regionalt kjernenett. Grovt sett er det snakk om to typer moduler som representerer nettverket ute på HF'ene, og to typer moduler som representerer regionalt datasenter.



Figur 8.1 – 2 Overordnet nettverksdesign

Modulen “HF LAN Distribusjon” består av et aksesslag for tilkobling av endeutstyr, og et distribusjonslag bestående av rutere mot klientnettet, brannmurer som skal beskytte klientnettet mot omverden og være sikkerhetsmekanisme mellom de ulike klientsegmentene som opprettes, samt kantrutere som er grensesnitt mot kjernenettet.

Modulen “HF lokalt datarom” er i prinsippet bygd opp på samme måte som klientnettet med serveraksess og serverdistribusjon. Trafikk mellom campus LAN og lokalt datarom går alltid gjennom kjernenettet, noe som innebærer at VLAN ikke kan traversere hele nettet.

På noen HF vil det av kostnads- og størrelsesmessige forutsetninger være aktuelt å etablere en kombinasjon av disse modulene hvor en begrenset server-aksess kobles til brannmuren i LAN-distribusjonen (ref. figur).

Modulen “Regionalt datasenter” er SP sitt sentrale datasenter og er bygd opp på samme måte som det lokale datarommet.

Modulen “Regionalt WAN-mottak” er mottak for øvrige lokasjoner i et HF eller HF som ikke er direkte tilkoblet kjernen, men som når sentrale tjenester gjennom regionens WAN. WAN’et baserer seg på IPVPN fra Norsk helsenett, og kryptering og virtualisering i forhold til sonemodell etableres ved hjelp av DMVPN.

8.2 Klientnettverk

Et klientnettverk består av et aksesslag for tilkobling av endeutstyr og et distribusjonslag som består av en virtuell ruter (VRF) som terminerer et eller flere virtuelle nett (VLAN), og en brannmur som beskytter klientnettverkene mot omverdenen. Et klientnettverk er i så måte å betrakte som et segment i et Campus LAN.

8.2.1 Aksesslaget for klient

Aksesslaget for klienter er basert på svitsjer som enten er stacket eller er chassis-baserte. Hovedpoenget er at svitsjene skal framstå som en enhet. De kobles redundant og lastdelende til distribusjonslaget ved hjelp av aggregerte trunker (LACP). Spanning tree benyttes ikke.

Det leveres 10/100/1000 Mbps autosense med støtte for Power over Ethernet (802.3af eller 802.3at) til klientene, noe som betyr at de fleste klienter vil få 1 Gigabit kapasitet. Kapasitet fra kantsvitsjene til distribusjonslaget vil bli minimum 2 x 10 Gigabit.

Kantsvitsjene er rene lag 2-enheter så det skal ikke rutes trafikk i dette laget. De ulike segmentene vil skilles gjennom VLAN, og kantsvitsjene skal støtte 802.1x for autentisering og automatisk tildeling av VLAN avhengig av autorisasjonen på utstyret som kobles til nettet.

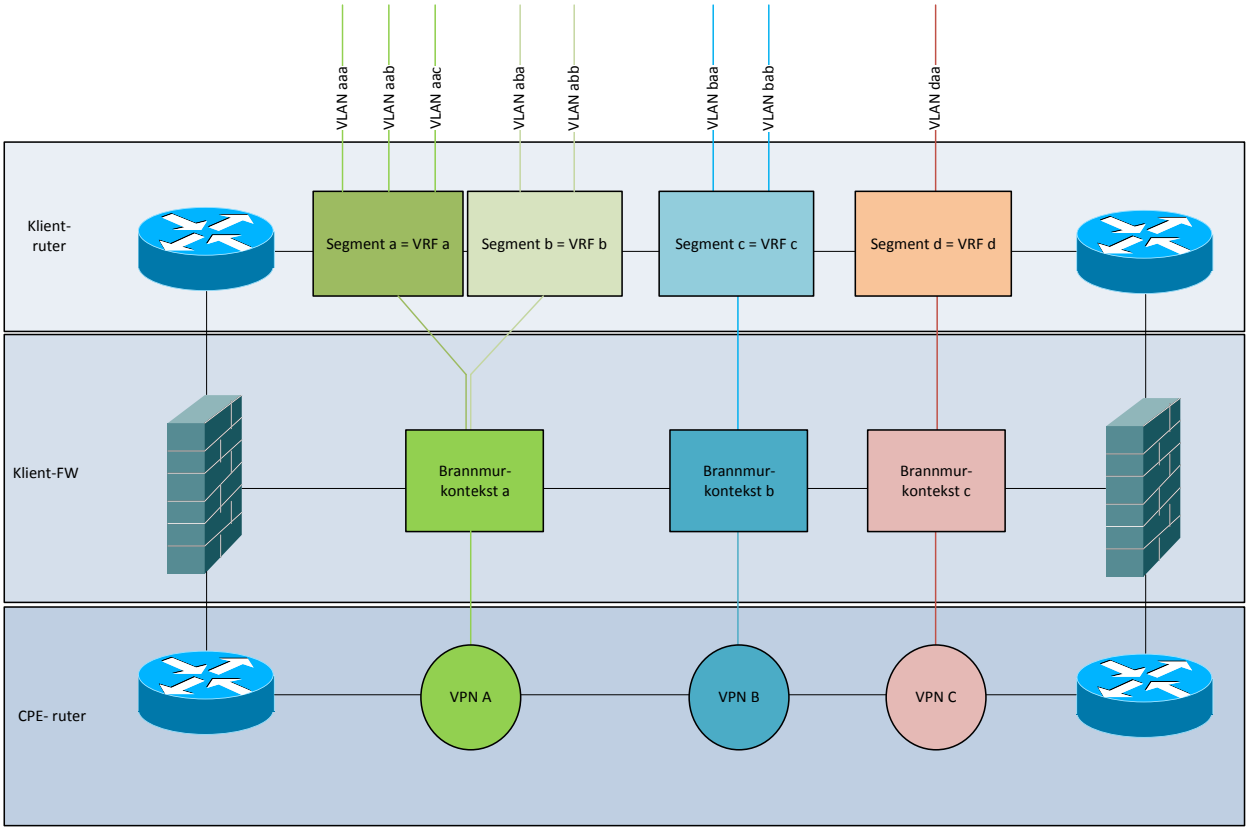
Hvilke segmenter som opprettes avgjøres av soneinndelingen som blir bestemt.

I aksesslaget vil trafikken bli merket for prioritering ende til ende (QoS).

8.2.2 Distribusjonslaget for klient

Distribusjonslaget bygges opp av svitsjeclustere med rutingfunksjonalitet. Distribusjonslaget består logisk av en ruter som tar i mot trafikk i et segment fra alle kanstvitsjer og ruter trafikken over til en brannmur. Det er en VRF per segment og brannmuren har en virtuell brannmur-kontekst per VRF. Bak brannmuren står det en ny ruter som er koblingen mot kjernenettet og har Multiprotocol Label Switching Provider Edge (MPLS PE) funksjonalitet. Fysisk løses dette gjerne enklere, med f.eks. en boks med alle disse funksjonalitetene innebygd.

Mot kjernen av nettet er redundansen basert på rutingteknologi, med en dynamisk rutingprotokoll (f.eks BGP).



Figur 8.2 – 1 Distribusjonslaget for klient

Figur 9.2 – 1 viser sammenhengen mellom VLAN i aksesslaget, VRF og brannmur i distribusjonslaget og VPN i kjernen.

Det er et en-til-en forhold mellom VPN (DMVPN for WAN-tilkoblet lokasjon eller IPVPN for kjerne-tilkoblet lokasjon) og brannmur-kontekst. En brannmur-kontekst kan ha flere VRF'er tilkoblet, så lenge de tilhører samme tilgangsnivå. En VRF terminerer en eller flere VLAN.

For eksempel vil en standard klient være tilknyttet VRF a (ref figur), og medisinsk-teknisk utstyr til VRF b. Disse er igjen knyttet til samme brannmur-kontekst, men vil ha egne regelsett for mer spesifikk tilgangsstyring. VRF c og d kan typisk være gjestenett og karantene-nett. De forskjellige VPN'ene er koblet opp mot VPN'er i datasenterne gjennom kjernenettet.

Multicast vil bli støttet i segmenter hvor det er et behov, f.eks. TV-distribusjon.

8.3 Trådløst nettverk

Det trådløse nettet bygges opp etter standard oppsett med såkalt tynne aksesspunkter ute på Campus og kontrollere plassert i lokalt datasenter på et HF. På mindre lokasjoner/installasjoner benyttes kontrollere plassert i regionalt datasenter. Kontrollerne etableres redundant, og aksesspunkter fordeles mellom kantsvitsjer på en måte som gjør at konsekvensene av at en kantsvitsj skal falle bort, blir redusert kapasitet og ikke bortfall av tjenesten. Bortfall av en kontroller vil normalt føre til redusert kapasitet, men i kritiske områder kan det tilbys tilstrekkelig kontrollertetthet for å kunne opprettholde kapasiteten.

SP har satt en grense på maks 8 SSIDer og har i sin standard i dag 2 i bruk, "SIKT" for ansatte og "HelseSørØst" for gjester. Ved hjelp av 802.1x-autentisering og dynamisk VLAN-tildeling kan en SSID brukes av flere typer endeutstyr med forskjellige tilgangsnivåer.

Det kan være naturlig å lage en egen SSID for f.eks. AGV'er (automatisert transport) og eventuelt andre spesielle behov, men holdt innenfor maksimumsgrensen.

8.4 Kjernenettverk (HSØ Kjernenett)

Et sykehus sitt kjernenett (ref. figur 9.1-1) er en del av regionens kjernenett og kobler de forskjellige modulene sammen (figur 9.1-2). Dette nettet er basert på samband av typen mørk fiber eller leide bølgelengder. Nettet skal ha høy kapasitet, med tilstrekkelig båndbredde. Nettet er bygd opp av MPLS P rutere, som transporterer ulike VPN mellom regionens lokasjoner, med regionalt datasenter som et naturlig knutepunkt. P-ruterne er plassert rundt i regionen, typisk i datarom på de større sykehusene.

Dette nettet leveres av Sykehuspartner i samarbeid med valgt entreprenør og linjeleverandør.

8.5 Servernettverk

Prinsippet for oppbygging av lokalt datasenter på et HF lokasjon/sykehus er det samme som for oppbyggingen av klientnettet. Se figurer i kapittel 8.1. Produktvalget vil være noe annerledes. Det legges også opp til noe mer funksjonalitet i distribusjonslaget, som lastbalansering (Application Delivery Controllers) og sikkerhetsovervåkning (IDS).

SP implementerer den til enhver tid gjeldende sonemodellen.

9 TELEKOMMUNIKASJON

Dette området er ikke beskrevet i første versjon av dokumentet, men bli inngå i en senere versjon av dokumentet.

10 NAVNESTANDARDER

Det er etablert navnestandarder for de vanligste behovene på HSØ-SP. Dette kapittelet inneholder en oversikt over disse.

10.1 Navnestandarder for klienter

Navngiving av maskiner i basis plattform skal være i henhold til følgende oppbygning:

PC<Syremerkenummer>

<Syremerkenummeret> brukes uten de foregående 0'ene i nummeret.

Eks: **PC305**

10.2 Navnestandard for skrivere

Navngiving av skrivere i basis platform skal være i henhold til følgende oppbygning

<Lokasjon>-<Avdeling>-<Type><Syremerkenummer>

Hvor <Lokasjon> er basert på GEO-koder. <Avdeling> er avdelingen skriveren er plassert på eller er i nærheten av. <Type> angir S=Sort, F=Farge. <Syremerkenummeret> brukes uten de foregående 0'ene i nummeret.

Eks: **DRM-KIR-S425**

SKE-MED-F4535

10.3 Navnestandard i katalogtjeneste

Alle OU og grupper skal ha norske navn. Der hvor det norske navnet inneholder Ø, Æ, Å skal disse byttes ut med bokstavene O, AE, A.

Generelle forkortelser som benyttes i flere type navn:

- Lokasjoner

For å angi lokasjoner benyttes GEO-koder som består av tre bokstaver. Oversikt over disse finnes blant annet på http://www.unece.org/fileadmin/DAM/cefact/locode/no.htm

- Organisasjoner (eksempler)
  - ✓ HSORHF Helse Sør-Øst RHF
  - ✓ PiVHF Psykiatrien i Vestfold HF
  - ✓ SiVHF Sykehuset i Vestfold HF
  - ✓ SP Sykehuspartner
  - ✓ SSHF Sørlandet sykehus HF
  - ✓ STHF Sykehuset Telemark HF
  - ✓ VVHF Vestre Viken HF

10.4 Navnestandard for servere

Navngiving av servere i HSØ-SP skal være i henhold til følgende oppbygning:

<Lokasjon>-<Funksjon>-<Løpenummer>

Hvor <Lokasjon> er basert på GEO-koder, <Funksjon> er serverens hovedfunksjon i henhold til tabellen xx og <Løpenummer> er et fortløpende tosifret nummer for å få navnet unikt.

Eks: **SDS-DC-01** Domenkontroller i regionalt datarom.

11 PRODUKTER

Beskrevet i kapittel	Byggekloss / komponent	Produkt/leverandør	Versjon	Status
Kap. 3 - Min Arbeidsplass	Operativsystem klient	Microsoft Windows	7	Gjeldende
Kap. 3 - Min Arbeidsplass	Antimalware	Microsoft Forefront Endpoint Protection	2010	Gjeldende
Kap. 3 - Min Arbeidsplass	Klientoppdatering	Microsoft System Center Configuration Manager	2007 R2	Gjeldende
Kap. 3 - Min Arbeidsplass	Diskkryptering	Microsoft Bitlocker		Gjeldende
Kap. 3 - Min Arbeidsplass	Kontorstøtte	Microsoft Office	2007	Gjeldende
Kap. 3 - Min Arbeidsplass	Basiskonfigurasjon	Adobe Reader	10	Gjeldende
Kap. 3 - Min Arbeidsplass	Basiskonfigurasjon	Citrix Online Plug-in	12.1.0.30	Gjeldende
Kap. 3 - Min Arbeidsplass	Basiskonfigurasjon	Adobe Flash	10	Gjeldende
Kap. 3 - Min Arbeidsplass	Basiskonfigurasjon	Adobe Shockwave	11.5	Gjeldende
Kap. 3 - Min Arbeidsplass	Basiskonfigurasjon	Sun Java Runtime	1.6_29	Gjedende
Kap. 3 - Min Arbeidsplass	Basiskonfigurasjon	F5 FirePass Component Installer		Gjeldende
Kap. 3 - Min Arbeidsplass	Basiskonfigurasjon	Microsoft Forefront Threat Management Gateway Client	7.0.7734	Gjeldende
Kap. 3 - Min Arbeidsplass	Basiskonfigurasjon	SCCM Agent	2007 SP2	Gjeldende
Kap. 3 - Min Arbeidsplass	Terminal Server	Citrix XenApp		I bruk
Kap. 3 - Min Arbeidsplass	VPN klient	Microsoft Forefront Threat Management Gateway	2010	Gjeldende
Kap. 3 - Min Arbeidsplass	Internett – proxy	Microsoft Forefront Threat Management Gateway	2010	Gjeldende
Kap. 3 - Min Arbeidsplass	Portalløsning	F5 Firepass		I bruk
Kap. 3 - Min Arbeidsplass	Portalløsning	F5 Big-IP		Gjeldende
Kap. 3 - Min Arbeidsplass	Fjernadministrasjon	Microsoft Configuration Manager Remote Control	2007 R2	Gjeldende

Kap. 3 - Min Arbeidsplass	Print	Microsoft Windows Print		
Kap. 3 - Min Arbeidsplass	Network access control	Microsoft Windows Server	2008 R2	Gjeldende
Kap. 3 - Min Arbeidsplass	Distribusjonsserver	Microsoft Windows Server, Windows Deployment Services	2003 R2	I bruk
Kap. 3 - Min Arbeidsplass	Distribusjonsserver	Microsoft Windows Server, Windows Deployment Services	2008	I bruk
Kap. 3 - Min Arbeidsplass	Distribusjonsserver	Microsoft Windows Server, Windows Deployment Services	2008 R2	Gjeldende
Kap. 3 - Min Arbeidsplass	Administrasjon	Microsoft Deployment Toolkit	2010	Gjeldende
Kap. 3 - Min Arbeidsplass	Distribusjonsserver	Microsoft System Center Configuration Manager	2007 R2	Gjeldende
Kap. 3 - Min Arbeidsplass	Pakkeverktøy	Wise Package Studio		Gjeldende
Kap. 4 – Identitets- og tilgangsstyring	Katalogtjeneste	Microsoft Windows Server (Active directory)	2003 R2	I bruk
Kap. 4 – Identitets- og tilgangsstyring	Katalogtjeneste	Microsoft Windows Server (Active directory)	2008	I bruk
Kap. 4 – Identitets- og tilgangsstyring	Metakatalog	Microsoft Identity Integration Server	2003	I bruk
Kap. 4 – Identitets- og tilgangsstyring	Sertifikatserver	Microsoft Windows Server, Certificate Services	2003 R2	I bruk
Kap. 4 – Identitets- og tilgangsstyring	Sertifikatserver	Microsoft Windows Server, Active Directory Certificate Services	2008	I bruk
5 - Integrasjonstjeneste	Integrasjonsmotor	Microsoft Biztalk	2009	Gjeldende
Kap. 5 - Integrasjonstjeneste	Teknisk monitorering/overvåking	Communicate MTM		I bruk
Kap. 5 - Integrasjonstjeneste	Teknisk monitorering/overvåking	Communicate MTM		I bruk
Kap. 5 - Integrasjonstjeneste	Meldingsgateway	Communicate ebXML/PKI		I bruk

Kap. 5 - Integrasjonstjeneste	Meldingsgateway	Dips Communicator		I bruk
Kap. 5 - Integrasjonstjeneste	Kommunikasjonspartregister (integrert mot FRESH)	ePartner		I bruk
Kap. 5 - Integrasjonstjeneste	Kommunikasjonspartregister (integrert mot FRESH)	Dips Communicator		I bruk
Kap. 6 - Støttetjenester	Operativsystem Server	Microsoft Windows Server	2008 R2	Gjeldende
Kap. 6 - Støttetjenester	Operativsystem Server	RedHat Enteprise Linux	6	Gjeldende
Kap. 6 - Støttetjenester	Virtualiseringsteknologi	VMware vSphere	4.1	Gjeldende
Kap. 6 - Støttetjenester	Overvåking	Microsoft System Center Operations Manager	2007	Gjeldende
Kap. 6 - Støttetjenester	Filserver	Microsoft Windows Server	2003 R2	I bruk
Kap. 6 - Støttetjenester	Filserver	Microsoft Windows Server	2008	I bruk
Kap. 6 - Støttetjenester	Filserver	Microsoft Windows Server	2008 R2	Gjeldende
Kap. 6 - Støttetjenester	E-postserver	Microsoft Exchange Server	2007	Gjeldende
Kap. 6 - Støttetjenester	Brannmur for e-post	Microsoft Forefront Threat Management Gateway	2010	Gjeldende
Kap. 6 - Støttetjenester	Antivirus og spam-filter	Symantec Brightmail		I bruk
Kap. 6 - Støttetjenester	Antivirus og spam-filter	Microsoft Forefront Security for Exchange Server	2010	Gjeldende
Kap. 6 - Støttetjenester	Databasemotor	Oracle	11g	Gjeldende
Kap. 6 - Støttetjenester	Databasemotor	Microsoft SQL Server	2008 R2	Gjeldende
Kap. 6 - Støttetjenester	Databasemotor	Sybase		I bruk
Kap. 13 – Vedlegg 1: Tilleggstjenester	Instant messaging	Microsoft Office Communcations Server	2007 R2	Gjeldende
Kap. 13 – Vedlegg 1: Tilleggstjenester	Webkonferanse	Microsoft LiveMeeting	2007	Gjeldende
Kap. 13 – Vedlegg 1: Tilleggstjenester	Mobilsynk	Microsoft Exchange Server	2007	Gjeldende

Kap. 13 – Vedlegg 1: Tilleggstjenester	Webmail	Microsoft Exchange Server	2007	Gjeldende

Tabell 11 – 1 Produkter

12 FORKORTELSER OG DEFINISJONER

12.1 Introduksjon

Dette kapittelet definerer dokumentets forkortelser og begrepsdefinisjoner.

12.2 Forkortelser

Dette underkapittelet definerer dokumentets forkortelser – se tabell 12.2 – 1.

1. Forkortelse	2. Definisjon
HSØ	Helse Sør-Øst
IKT	Informasjons Kommunikasjons Teknologi
SP	Sykehuspartner
V	Versjon

Tabell 12.2 – 1 Forkortelser

12.3 Definisjoner

Dette underkapittelet definerer dokumentets begreper – se tabell 12.3 – 1.

Begrep	Definisjon
SAN	Storage Area Network – Dedikert nettverk som benyttes for å tilgjengeliggjøre blokk-baserte lagringsenheter.
NAS	Network Attached Storage – Nettverkstilkoblede lagringsenheter som benyttes ved filbaserte protokoller som f.eks. standard fildeling i Windows.
LAN	Local Area Network – lokalnettverk som i sin videste betydning betyr nettet som kobler sammen endeutstyr på en fysisk lokasjon.
Forest	Øverste nivå i den logiske strukturen for Active Directory. Benyttes for å gruppere underliggende domener.
WAN	Wide Area Network – Sammenkobling av to eller flere LAN. I HSØ vil det typisk utgjøres av alle lokasjoner som ikke er direkte tilkoblet kjernenettet.
VLAN	Virtual LAN – brukes for å kunne segmentere opp et LAN i flere brukernett uten å måtte bygge flere fysiske LAN. I stedet brukes den samme fysiske infrastrukturen for å distribuere alle nettene.
WLAN	Wireless LAN – Trådløst nett
Domener	Den grunnleggende enheten (byggesteinen) i Active Directory. Hovedfunksjonen til et domene er å kontrollere tilgang til nettverkets objekter.

Organizational Units	Objekter som kan inneholde andre objekter. OU gjør det mulig å gruppere objekter lokalt i et domene.
Power over Ethernet (PoE)	Teknologi for å bruke switchene til å strømsette endeutstyr, som f.eks telefoner og trådløse aksesspunkter
Brannmurkontekst	En virtuell brannmurinstans. En fysisk brannmur kan deles opp i flere virtuelle kontekster med separate regelsett og innstillinger.
VPN	Virtual Private Network – brukes for å koble sammen LAN uavhengig av underliggende teknologi. Trafikken tunneleres fra ende til ende. I HSØ benyttes IPVPN gjennom kjernenettet og DMVPN gjennom WAN.
Spanning Tree	Teknologi som muliggjør redundant oppkobling av aksessswitcher
SSID	Service Set IDentifier – kan sammenlignes med VLAN for trådløst nett. Et trådløst aksesspunkt kan ha opptil 16 forskjellige SSID'er
VRF	Virtual Router Forwarding – brukes for å dele en fysisk router opp i flere virtuelle routere med hver sin routing-tabell.
MPLS	Multi Protocol Label Switching – teknologi for raskt å distibuere pakker i et større kjernenett

Tabell 12.3 – 1 Definisjon av begreper

13 VEDLEGG 1: TILLEGGSTJENESTER

13.1 Sanntidskommunikasjon

På plattformen er det etablert en tilleggstjeneste for samhandling som tilbyr funksjonalitet rundt sanntidskommunikasjon og webkonferanser. Tjenesten er pr. d.d. (september 2012) kun tilbudt til Sykehuspartner, Helse Sør-Øst RHF, Pasientreiser og Sunnaas sykehus HF.

13.2 E-post mobile tjenester

Plattformen tilbyr pr. i dag to mobile tilleggstjenester for e-post. Disse tjenestene er tenkt for administrative brukere som ikke behandler sensitiv informasjon i e-post.

13.2.1 Mobilsynkronisering

Synkronisering av e-post, kalender, kontakter og oppgaver til mobile enheter. Denne tjenesten benytter brukernavn og passord for autentisering. Samt medlemskap i tilhørende tilgangsgruppe for autorisasjon. Tjenesten krever at de mobile enhetene benytter låsekode ved 30 minutters inaktivitet, og at de mobile enhetene kan fjernslettes ved tap av enhet.

13.2.2 Webmail

Web basert e-post klient som er tilgjengelig fra ukjente enheter. Denne tjenesten benytter brukernavn og passord for autentisering. Samt medlemskap i tilhørende tilgangsgruppe for autorisasjon.