Elektronisk logistikk- og kvalitetsstyringssystem for Sterilavdelingen ved OUS

Saksnummer: 2018/691

T Bilag 3a: Kundens tekniske plattform

Versjon 1.0, Juli 2019

Innhold

1 Innledning

Dette dokumentet beskriver på et overordnet nivå IKT-plattformen etablert ved Oslo universitetssykehus HF («Kunden»). Sykehuspartner HF er Kundens tjenesteleverandør, og er ansvarlig for etablering, drift og forvaltning av IKT-plattformen, samt mange av Kundens løsninger etablert i plattformen. Tjenesteleverandørens driftsansvar inkluderer datasentre etablert hos Kunden og fellesregionale datasentre etablert for helseforetakene i Helse Sør-Øst. Kunden har i tillegg enkelte lokale drifts og forvaltningsenheter med ansvar for IKT-systemer, bl.a. tilknyttet medisinskteknisk utstyr (MTU), laboratorievirksomhet og stråleterapi.

Leverandører gjøres oppmerksom på at IKT-plattformen er i kontinuerlig videreutvikling, og at endringer og oppgraderinger av infrastrukturen vil kunne forekomme i løpet av avtaleperioden.

1.1 Grønn IT

Helse Sør-Øst ønsker å fremme bærekraftig bruk av IT og forholder seg til føringer fra Grønn IT (https://www.ikt-norge.no/bransjenormer-guider/gronn-it/) ved anskaffelse, etablering, drift og forvaltning av IKT-plattformen og løsninger etablert i IKT-plattformen.

1.2 Livssyklus

Helse Sør-Øst er opptatt av at løsninger skal kunne vedlikeholdes og videreutvikles løpende, såkalt «Lifecycle Management». Operativsystem og programvare vil normalt støttes i gjeldende hovedversjon, samt forrige hovedversjon (n, n-1). Dette gjelder eksempelvis komponenter og tjenester:

- levert av Kundens tjenesteleverandør, og ikke inngår i leveransen av løsningen
- levert som en del av løsningen
- levert av 3.part

Løsningen må derfor kontinuerlig oppdateres og vedlikeholdes for å imøtekomme dette prinsippet. Merk at dette også medfører at løsningen må støtte løpende patching og oppgraderinger i Kundens tekniske plattform.

2 Arkitekturprinsipper

Helse Sør-Øst anser visse egenskaper som viktige for alle løsninger som skal innføres. Disse egenskapene er nedfelt som arkitekturprinsipper, og er nærmere beskrevet i følgende dokumenter:

- DIFIs «Overordnede IT arkitekturprinsipper for offentlig sektor»
- DIFIs «Arkitekturprinsipper for samhandling»
- Nasjonal IKT «Arkitekturprinsipper i spesialisthelsetjenesten»

3 Datasenter

Kunden har to hovedlokalisasjoner som hver inneholder to separate georedundante datasentre (SHKR):

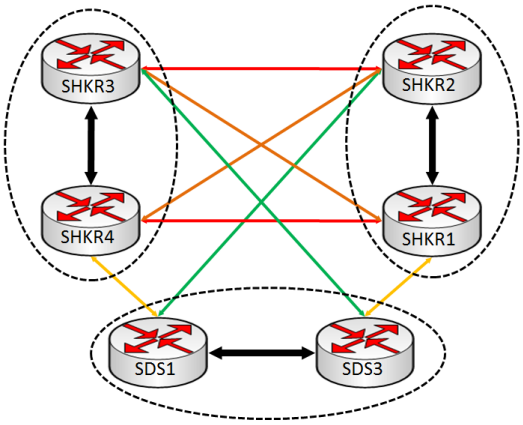
- OUS Rikshospitalet: SHKR1 og SHKR2
- OUS Ullevål Sykehus: SHKR3 og SHKR4

Det er etablert to fellesregionale datasentre (SDS) i Helse Sør-Øst:

- SDS1 lokalisert hos Digiplex
- SDS3 lokalisert hos Basefarm

Det er i tillegg etablert et eksternt datasenter for katastrofebackup (kald backup), SDS2 på Ahus.

Kundens lokale datasentre er knyttet sammen med fellesregionale datasentre som illustrert under:



FIGUR 1 - FIBERKOBLINGER SHKR OG SDS

4 Nettverksinfrastruktur

4.1 Overordnet

Kundens nettverk er bygd opp med nettelementer fra Extreme Networks (tidligere Avaya). Det er utstrakt bruk av Shortest Path Bridging (SPB) i nettverket. SPB gjør at ethvert VLAN kan trekkes til en hvilken som helst annen del av nettverket som et L2VSN (L2 Virtual Service Network) uten å måtte rekonfigurere alle noder underveis.

I Kundens nettverk benyttes også Fabric Attach og Fabric Connect for å automatisere nettverkskonfigurasjon, både for trådløst og trådbasert nettverk.

De fellesregionale datasentrene (SDS) benytter nettelementer fra Cisco og bruk av MPLS. Dette gjør at kommunikasjonen mellom Kundens nettverk og HSØ forøvrig er basert på IPv4 og ikke lag-2.

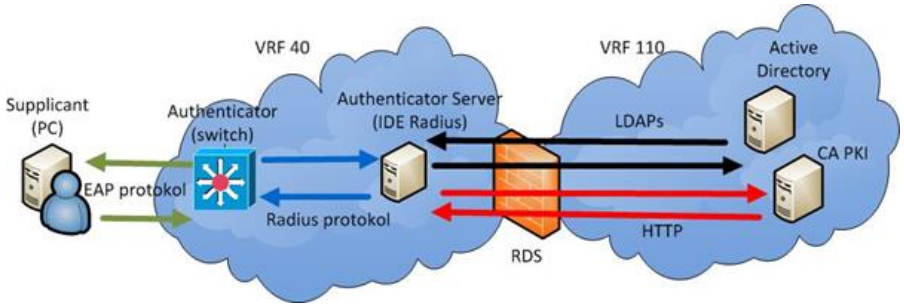
4.2 Brannmurer

Det er standardisert på Cisco brannmurer internt, mens det benyttes brannmurer fra Palo Alto ut mot Internett. Cisco brannmurene er konfigurert med TCP «idle timeout» på to timer i Kundens nettverk, og Idle timeout på 1 time i de fellesregionale datasentrene.

4.3 Aksesskontroll

Det benyttes IEEE 802.1X EAP-TLS på alle kablede og trådløse nett hos Kunden. For utstyr som ikke støtter IEEE 802.1x benyttes MAC autentisering for å tildele riktig VLAN. Enheter som feiler på autentisering plasseres i dag i gjestenettet, men en karantenesone er under etablering. Bruk av EAP-TLS autentisering ved bruk av maskinsertifikater benyttes i dag kun for standardiserte PC-klienter, som plasseres i samme VLAN. Løsningen er under endring for også å kunne styre maskiner inn i separate VLAN basert på X.509 OU.

CRL sjekk og VLAN tildeling gjøres av en Avaya IDE RADIUS. DNS maskinnavn slås også opp i AD med LDAP via den samme RADIUS.



FIGUR 2 - OVERORDNET DATAFLYT .1X

4.4 Lastbalansering

Alteon benyttes som lastbalanserer i Kundens lokale datasentre (SHKR), mens F5 BigIP benyttes i fellesregionale datasentre (SDS). Det er en pågående prosess for å skifte ut lastbalanserere fra Alteon med F5 også i lokale datasentre.

4.5 Trådløst nettverk

Kundens trådløse nettverk er etablert med utstyr fra Extreme Networks. De samme sikkerhetsprinsipper og sikkerhetsmekanismer som er innført for kablet nettverk er også etablert for trådløse nett.

Følgende SSID og tilhørende nettverk finnes:

SSID	Beskrivelse	Autentisering
Intern-OUS	Internt OUS nettverk for administrative og kliniske tjenester	IEEE802.1X/EAP-TLS + AD
HelseSorOst	Gjestenett for pasienter og pårørende	Ingen, men captive portal med brukerautentisering er under etablering
Eduroam	Verdensomspennende nettverk for akademisk- og forskningsrelatert virksomhet	Autentisering skjer via Eduroam og avhenger av brukers tilhørighet til en organisasjon som inngår i Eduroam-samarbeidet

4.6 Regionalt WAN mottak

Alle eksterne nettverksforbindelser, inklusive VPN-basert fjernaksess for ansatte og leverandører, termineres på regionalt WAN mottak. Regionalt WAN mottak er en del av kjerneinfrastrukturen som er levert av Kundens tjenesteleverandør.

Det er kun IPv4 trafikk som er mulig mellom WAN mottak og Kundens nettverk.

5 PC-klienter

5.1 Standard PC-klienter

Windows 7 64-bit benyttes i dag som operativsystem på standard PC-klienter, men det pågår en prosess for å oppgradere standard PC-klienter til Windows 10, planlagt ferdigstilt Q1 2020. Brukere tillates ikke å være lokale administratorer, og det er kun godkjent programvare som tillates kjørt på klientene.

Standard PC-klient benytter lokal Windows brannmur, samt System Center Endpoint Protection (SCEP) for antivirus/antimalware. Det tillates ikke klient-til-klient trafikk.

Det er sperret for tilkoblet periferiutstyr som identifiseres som lagringsenheter, eksempelvis optiske drev eller USB-tilkoblet lagring. Krypterte USB lagringsenheter fra IronKey tillates, forutsatt at dette er bestilt gjennom og administrert av Kundens tjenesteleverandør. Alle bærbare PC-klienter er krypterte med BitLocker Drive Encryption.

5.2 MTU Klient

En MTU-klient defineres som en klient som i utgangspunktet er “single-purpose”, og benyttes til dedikerte oppgaver i tilknytning til MTU, eksempelvis for:

- overvåking eller styring av et MTU
- kjøring av MTU-relaterte klientapplikasjoner for etterbehandling av data hvor MTU er datakilde
- pre-prosessering av data som skal benyttes av MTU.

Det benyttes Windows 7 som standard (Engelsk Windows 7 Enterprise med SP 1 og 64 bit-utgave, med mulighet for norsk språkpakke). Bruk av Windows 10 er under planlegging. MTU-klienter kan ikke primært benyttes til kontor-administrative oppgaver, men det kan tilgjengeliggjøres en Citrix-arbeidsflate som gir brukeren tilgang til administrative og kliniske fagsystemer.

MTU-klienter etableres i egne MTU-klientsoner iht. sonemodellen etablert i Kundens nettverk, og kan ha redusert eller endret funksjonalitet fra OUS Standard klient mht.:

- Antivirus
- Sikkerhetspatching
- Lokal lagring – inkl. lagring av sensitiv informasjon
- Backup
- Klientoppsett som skyldes softwaremessige krav fra leverandør, som f.eks. manglende støtte for RES og SCCM
- Utvidede eller tilpassede tilganger og rettigheter
- Funksjonsbrukerkonseptet (fellesbruker, typisk påloggінger som går over flere skift eller tilrettelagt etter arbeidsprosesser)
- Skjermsparer og automatisk låsing
- Forvaltning:
    - fjernaksess for Kundens ansatte med MTU drifts- og forvaltningsansvar
    - fjernaksess for leverandører av MTU
- Internettilgang

Det benyttes i hovedsak tre varianter av Windows 7 MTU-klient:

- MTU-Standard – er basert på Kundens standard Windows 7 PC-klient, men har mulighet for enkelte tilpasninger i konfigurasjon mht. sikkerhet, drift og forvaltning. Dette er foretrukken MTU-klienttype.
- MTU-GPO - Denne klienttypen brukes hvis en eller flere av tjenestene SCCM, RES og SCEP ikke kan/bør benyttes. Klienten blir i stedet herdet med et sett GPO-er og er så langt det er mulig fjernadministrert.
- MTU-Ren - Dette er en frittstående klientvariant, som ikke kan være medlem av domenet og benytter ikke GPO.

For å beskytte MTU klienter med funksjonsbruker (konstant pålogget PC med upersonlig bruker) mot utilsiktet innsyn, samt logge brukeraktivitet, er det under utvikling en AD-styrt skjermlås, som kan låses opp av alle identifiserte brukere som tilhører riktig AD gruppe.

5.3 Funksjonsbruker

Kunden har etablert et standardisert konsept for håndtering av fellesbrukere på operativsystem, kalt «funksjonsbruker».

Det ønskes fortrinnsvis å unngås bruk av funksjonsbrukere på operativsystemet, og benytte individuelle brukere for å bedre sikre tilgang, kontroll og sporbarhet. For enkelte bruksområder vil det derimot være hensiktsmessig å benytte funksjonsbruker, eksempelvis i sammenheng med PC-klienter som benyttes til aktiviteter som pågår over flere arbeidsskift.

Det er for funksjonsbruker etablert en rekke begrensninger:

- Funksjonsbruker er knyttet til én spesifikk PC-klient, og PC-klienten er satt opp med auto-pålogging. PC-klienten kan ikke benyttes for individuell pålogging når satt opp med funksjonsbruker
- Det er ikke tilgang til internett
- Det er ikke tilgang til filområder
- Det er ikke tilgang til epost
- Det stilles som krav at applikasjoner som gir tilgang til personopplysninger skal være sikret med individuell pålogging mot sentral autentiseringsløsning (IAM eller AD)
- Tilgang til filområder, epost o.a. applikasjoner kan skje gjennom en Citrix arbeidsflate, med krav om individuell pålogging av bruker

5.4 Distribusjon og patching av programvare

Til administrasjon, distribusjon og patching av *lokalt installert* programvare benyttes Microsoft System Center Configuration Manager i MSI-format. Microsoft App-V benyttes for sentralt *strømmede* applikasjoner. Programmene pakkes i MSI/App-V format ved hjelp av AdminStudio. App-V er preferert metode for applikasjonsdistribusjon.

Applikasjoner som skal distribueres til flere standard PC-klienter, skal normalt pakkes av Kundens tjenesteleverandør og distribueres gjennom godkjente distribusjonsmetoder. Alle applikasjoner som skal benyttes må «whitelistes» i RES One Suite.

5.5 Dynamisk arbeidsflate

RES One Suite fra Ivanti, i senere versjoner endret navn til Ivanti Workspace Control (ivanti.com), benyttes for å tilpasse og levere arbeidsflaten ut fra funksjonelle behov og brukerens organisatoriske tilhørighet. Herunder ligger tilgjengeliggjøring og «whitelisting» av applikasjoner.

5.6 Internettaksess

Internett aksess tillates fra PC-klienter på port 80 og 443 (http/https), og det benyttes URL filtrering på ytre brannmur (Palo Alto). Internet Exporer 11 er standard nettleser, og det er ikke tillatt med lokalt installert Java runtime.

Ved innføring av Windows 10 vil standard nettleser bli Microsoft Edge.

Google Chrome er innført som sekundærnettleser for Windows 7, og vil videreføres som sekundærnettleser for Windows 10.

5.7 Utskrift

Sentralisert utskriftsløsning er basert på Canon Uniflow Pull print/follow-me print, og det benyttes primært multifunksjonsskrivere etablert i sentrale områder.

For behov som ikke dekkes av sentralisert utskriftsløsning, som etikettskrivere og spesialskrivere, kan disse etableres lokalt. Dette forutsetter gjennomført risikovurdering.

5.8 AD struktur

OUS benytter ett felles domene for alle nye tjenester: ous-hf.no

Det finnes fortsatt andre domener i bruk, men disse er under avvikling og skal ikke benyttes ved etablering av nye tjenester.

5.9 Central Driver Store

Det tillates ikke at standard PC-klienter kan laste ned drivere fra Internett for installasjon. Alle godkjente og oppdaterte drivere skal gjøres tilgjengelig i lokalt etablert Central Driver Store.

5.10 Fjernaksess for ansatte (Always-on VPN)

I fjernaksessløsningen for ansatte hos Kunden benyttes Big-IP Access Policy Manager sammen med Big-IP Edge Client. Tilgang autentiseres med ID-Porten på sikkerhetsnivå 4, og gir tilgang til Kundens nettverk fra bærbare PC-klienter. I tillegg kan bruker logge seg på virtuelle arbeidsflater basert på Citrix-terminalaksess.

Prinsippet for VPN-tilgang er at en PC-klient automatisk tilkobles Kundens nettverk via VPN (såkalt «Always-on») og alltid er underlagt de samme sikkerhetsbestemmelsene for nettverkstilganger uansett hvor i verden man befinner seg. Dette innebærer også at internettaksess alltid reguleres gjennom ytre brannmur (Palo Alto).

Det tillates ikke bruk av BYOD-enheter i Kundens nettverk, bortsett fra i Gjestenett.

6 Server

Servere kjøres i hovedsak som virtuelle maskiner under VMware. Operativsystem på nye servere skal være:

- Windows Server 2019 og Windows Server 2016
- Redhat Enterprise Linux (RHEL) 7.5

Andre versjoner av operativsystemene finnes fremdeles i drift, men vil gradvis migreres til siste støttede versjon eller utfases. Det er ikke ønskelig at nye løsninger etableres på eldre versjoner av operativsystemene, eller andre operativsystem.

7 Databaseplattform

Følgende databaseplattformer er støttet:

- Microsoft SQL Server 2016, inklusiv Always-On cluster
- Oracle 12, inklusiv Maximum Availability Architecture (MAA)

8 Lagring, backup og arkivering

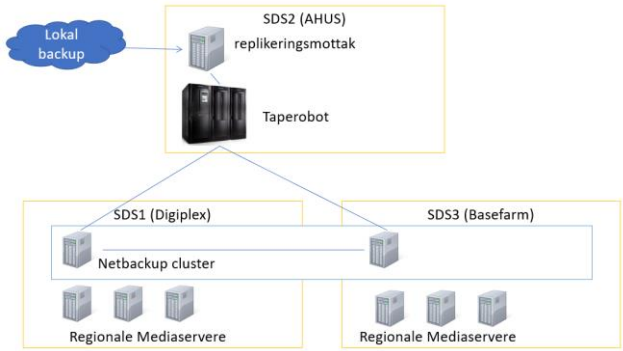
8.1 Lagring

Lagring kan foregå både på lokalt datasenter (SHKR) og fellesregionalt datasenter (SDS). Det benyttes både NAS- og SAN-basert lagring.

8.2 Backup

Symantec NetBackup benyttes for all backup.

Det er etablert to regionale backupmiljøer i SDS1 og SDS3, mens SDS2 benyttes til replikeringsmottak.



FIGUR 3 - BACKUP OG REPLIKERING PÅ SDS

Backupjobbene er normalt satt opp til å kjøre utenom normal arbeidstid (kl 17:00 til 05:00), med hovedtyngden av jobber etter midnatt. Jobber kan unntaksvis settes opp til å gå på dagtid, ved dokumenterte behov.

Det er definert forskjellige nivåer på backup (gull, sølv, bronse). De forskjellige nivåene vil normalt gjenspeile kritikaliteten til tjenesten.

Backupstatus blir overvåket daglig via NetBackup OpsCenter for både regionale og lokale backupmiljø.

8.3 Arkivering

Arkivering av lite brukt eller historiske data kan bestilles som opsjon.

9 Drift og forvaltning

9.1 Overordnet

Kundens tjenesteleverandør er drift- og forvaltningsansvarlig for Kundens tekniske plattform, og er normalt ansvarlig for drift og forvaltning av løsninger etablert i plattformen. Det er viktig at Leverandøren forholder seg til både de tekniske løsningene etablert i Kundens tekniske plattform, samt eksisterende rutiner, ved drift- og forvaltning av Løsninger etablert i Kundens tekniske plattform.

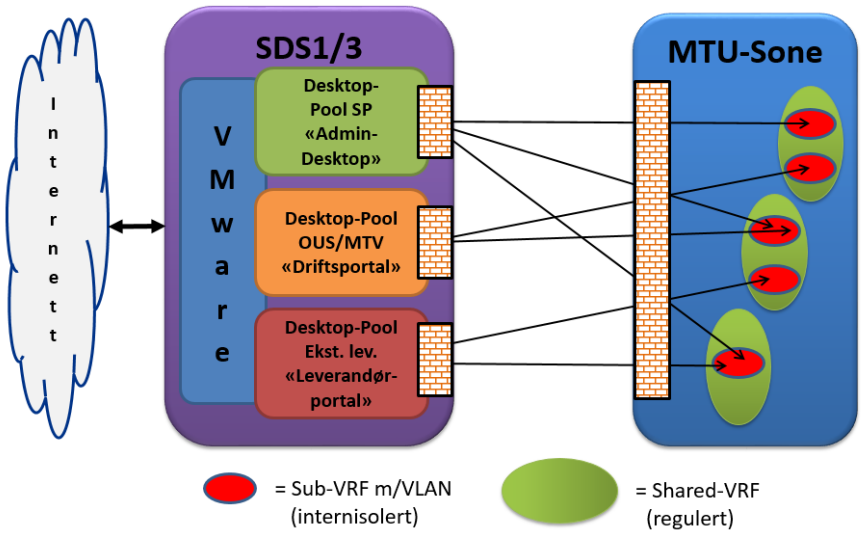
Det er i tillegg åpnet for prinsippet «delt forvaltning», der Kundens tjenesteleverandør kan tilby alt fra driftet nettverksaksess (Network as a Service) og opp til fulldriftet applikasjonsplattform (Software as a Service). Drift og/eller applikasjonsforvaltning på en tjenesteleveranse (klient/server/devicer/applikasjon) kan dermed utføres av en ekstern leverandør.

Typiske eksempler på slik delt forvaltning er løsninger for medisinskteknisk utstyr (MTU), byggteknisk utstyr (BTU) og administrativteknisk utstyr (ATU), der Kundens tjenesteleverandør har drift av Kundens tekniske plattform opp til ønsket nivå, mens Kunden forvalter systemløsningen. En dedikert serversone for løsninger med delt forvaltning er under etablering. Den sikrer nødvendig separasjon og tilgangskontroll i forhold til løsninger som driftes og forvaltes i sin helhet av Kundens tjenesteleverandør.

Drift og forvaltning skal ikke utføres via direkteaksess. I stedet er det etablert en obligatorisk managementløsning basert på Citrix XenDesktop som sikrer adgangs- og tilgangskontroll, samt nødvendig sporbarhet og logging på aktiviteter. For eksterne leverandører har man i tillegg en VPN-portal som krever 2-faktor autentisering ved påloggingsforsøk.

Kunden har i tillegg en standardisert «filsluse» for kontrollert og sikker overføring av godkjente data mellom Kunden og Leverandør.

Kundens tjenesteleverandør har etablert faste frysperioder hvor det er streng regulering av hvilke endringer som kan gjøres i infrastrukturen eller i etablerte løsninger. Ved større driftsmessige hendelser i Kundens plattform, kan det etableres midlertidige frysperioder.



FIGUR 4 - PRINSIPP FOR FORVALTNING AV MTU

9.2 Fjernaksess for leverandører

Helse Sør-Øst har standardisert på fjernaksess gjennom løsninger fra F5 BigIP og Citrix-terminalaksess for eksterne leverandører. Den benevnes «Leverandørportalen» og skal benyttes for all leverandørspesifikk drift og forvaltning der det ikke forutsettes personlig oppmøte i Kundens lokaler.

For å kunne bruke denne løsningen må Leverandør kunne benytte F5 BigIP web-plugin for SSL-VPN og Citrix Receiver web-klient på sine PC-er. En bruker av Leverandørportalen må være registrert i Kunden sitt personalsystem PAGA og bli tildelt en personlig bruker ID. Leverandøren får da tilgang til en aksesserver hos Kunden, hvor godkjente fjernstyringsprogram (RDP, SSH, WinSCP, UltraVNC) gjøres tilgjengelig. Ved spesielle behov kan annen programvare gjøres tilgjengelig etter godkjenning av Kunden.

All bruk av Leverandørportalen skal knyttes til personlige, identifiserte brukere hos Leverandøren. En bruker ID på Leverandørportalen er i utgangspunktet stengt, og åpnes kun etter avtale med Kunden og/eller med Kundens tjenesteleverandør. Åpninger gis for inntil 72 timer av gangen for vanlige supportbehov. Lengre intervaller (inntil 6 måneder) kan gis f.eks. ved installasjon, test og validering av større systemer

Bruk av Leverandørportalen forutsetter at det signeres taushetserklæring og inngås en Databehandleravtale mellom Kundens tjenesteleverandør og Leverandør.

9.3 Fjernaksess for drift og forvaltning

Kundens tjenesteleverandør gjør sin drift og forvaltning av Kundens tekniske plattform og løsninger etablert i plattformen via en «AdminDesktop» basert på Citrix XenDesktop.

Det er etablert en separat «Forvaltningsdesktop» for ansatte hos Kunden som har ansvar for drift og/eller forvaltning av internt etablerte løsninger, eksempelvis for MTU og BTU.

9.4 Overvåking

Kundens tjenesteleverandør har etablert sentraliserte løsninger for overvåking av Kundens nettverksinfrastruktur og IKT-plattform, samt underliggende komponenter og tjenester i Kundens tekniske plattform. Overvåking skjer gjennom en rekke agent-baserte og agentløse løsninger på forskjellige komponenter i infrastrukturen, hvor varsler og alarmer aggregeres opp i Micro Focus Operations Bridge.

9.5 Logging

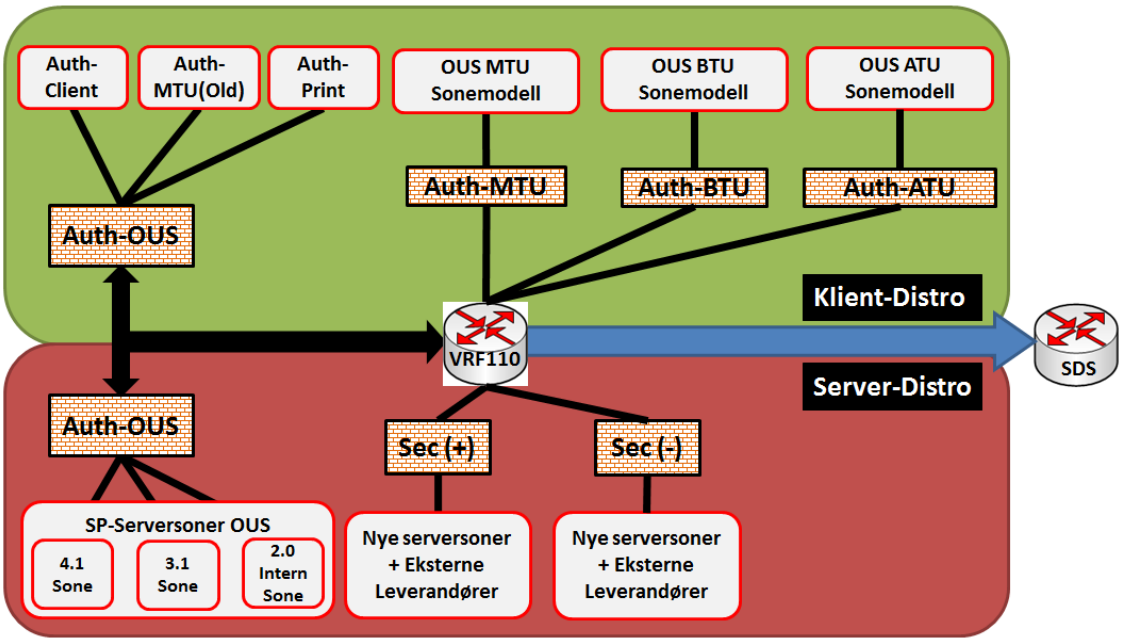
Det er sentralt og viktig for både Kunden og Kundens tjenesteleverandør systemer etablert i Kundens tekniske plattform kan tilby drifts- og forvaltningsrelatert loggfunksjonalitet på flere nivåer, eksempelvis ved feilsituasjoner eller varsler tilknyttet hardware, operativsystem, tjenester i systemet, feilhendelser og andre varsler som kan bidra til at feilsituasjoner unngås eller man i etterkant av feilsituasjoner kan fremskaffe informasjon relevant for å avdekke feilårsak.

Kundens tjenesteleverandør har etablert et sentralt loggmottak for håndtering av relevante system- og sikkerhetslogger fra Kundens systemer. Sentralt loggmottak er basert på Splunk.

10 Medisinskteknisk, byggteknisk og administrativteknisk utstyr

10.1 Sonemodell

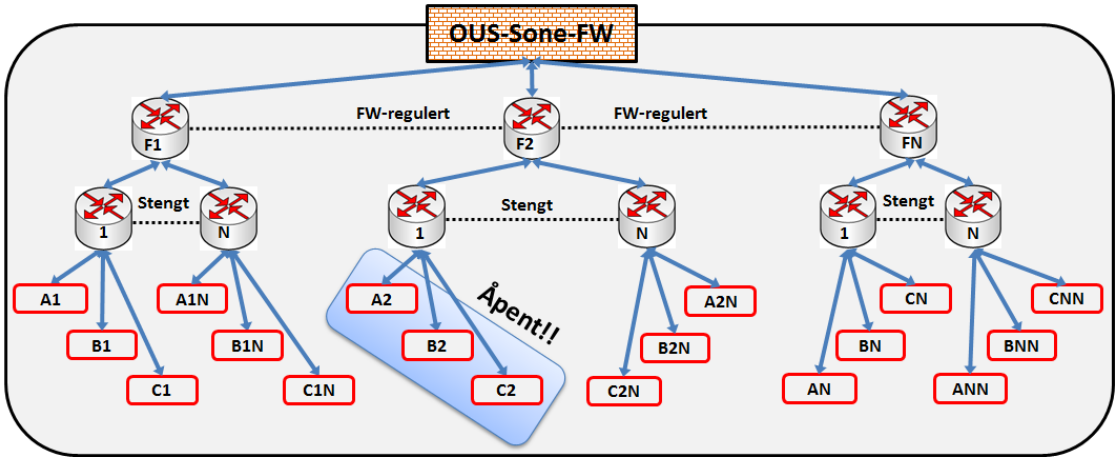
Det er etablert en sonemodell for bruk til MTU-, BTU- og ATU- løsninger, som ivaretar krav til sikkerhet, sporbarhet og delt forvaltning.



FIGUR 5 - PRINSIPP FOR SONEINNDELING PÅ ET SHKR

Sonemodellen separerer i to nivåer, dvs. med hovedsoner og underliggende soner i hver enkelt hovedsone:

- Mellom hovedsoner (nivå 1) reguleres datatrafikk gjennom brannmursregler
- Mellom underliggende soner pr hovedsone (nivå2) benyttes «Black Hole Routing» som lokal isolasjonsmekanisme å hindre trafikk mellom de underliggende sonene



FIGUR 6 - PRINSIPP FOR SONESEPARERING

Dette betyr at komponenter i en systemløsning som skal utveksle data enten må stå i:

- samme underliggende sone, eller

- ulike underliggende soner (i forskjellige hovedsoner), som tilgangsreguleres via brannmur utenfor hovedsonene

Hvis den etablerte løsningen trenger isolasjon fra andre løsninger i den samme underliggende sonen, må løsningen ha sin egen skallsikring, eksempelvis ved å benytte intern brannmur eller separat brannmursappliance. Dette er en konsekvens av at man ikke har mulighet for aksessregulering på VLAN-nivå.

Utveksling av data mellom løsninger etablert i sonemodellen eller med utenforliggende løsninger skal i størst mulig grad skje gjennom bruk av Regional integrasjonsplattform eller filsluse.

10.2 Medisinteknisk utstyr (MTU)

Medisinskteknisk utstyr (MTU) er definert som «*ethvert instrument, apparat, hjelpemiddel, materiell eller enhver gjenstand brukt til å diagnostisere, overvåke, behandle eller endre pasientens anatomi eller fysiologiske prosesser*».

Det er stor variasjon i datakommunikasjonsmetoder til MTU. Noe utstyr er direkte tilkoblet nettverket, mens mange løsninger består av en PC-klient tilknyttet instrument via USB, RS232, Firewire etc, eller indirekte tilknyttet via Ethernet via MOXA/Digiboks o.l. konverteringsløsninger.

OUS har etablert sikkerhetsprinsipper og mekanismer for å håndtere eventuelle avvik, da ikke all MTU følger etablerte standarder for datakommunikasjon.

10.3 Byggteknisk utstyr (BTU) og Administrativt teknisk utstyr (ATU)

Byggteknisk utstyr (som f.eks. SD-anlegg) og Administrativt teknisk utstyr (f.eks. parkeringssystemer, kioskløsninger o.l.) etableres i egne, separate nettverkssoner tilrettelagt for formålet, og håndteres etter samme prinsipp som medisinskteknisk utstyr.

11 Lisensiering

For løsninger som har en lisensieringsmekanisme, foretrekkes det at slike etableres sentralisert for å sikre effektiv lisensforvaltning. Dette innebærer at:

- bruk av fysiske lisensdongler søkes unngått, grunnet utfordringer dette medfører i et virtualisert driftsmiljø
- bruk av distribuerte lisensfiler søkes unngått, grunnet utfordringer dette medfører mht vedlikehold av lisensfiler og applikasjonspakker lisensfilen evt. inngår i

12 Informasjonssikkerhet og personvern

12.1 Overordnet

Kunden plikter å oppfylle lovreglene i norsk lovverk, og stiller strenge krav til oppfyllelse av relevant lovverk vedr. informasjonssikkerhet ved anskaffelse, etablering, drift, forvaltning og avhending av sine systemer. Informasjonssikkerhet handler om å sikre at informasjonen systemet behandler:

- ikke blir kjent for uvedkomne (konfidensialitet)
- ikke blir endret utilsiktet eller av uvedkomne (integritet)
- er tilgjengelig ved behov (tilgjengelighet)

Det stilles krav til at tilbudt løsning skal tilfredsstille krav i Personvernforordningen (GDPR) artikkel 25 – Innebygd personvern, se:

- Datatilsynets veileder for innebygd personvern - https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/programvareutvikling-med-innebygd-personvern/
- Datatilsynets informasjon om personvernforordningens krav til innebygd personvern til leverandører og utviklere i helse- og omsorgssektoren - https://www.datatilsynet.no/personvern-pa-ulike-omrader/forskning-helse-og-velferd/leverandorer-og-utviklere-i-helse--og-omsorgssektoren/
- GDPR – Article 25, Data protection by design and by default (på Engelsk) - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

Kunden er pålagt å etterleve Direktoratet for eHelse sin «Norm for informasjonssikkerhet» («Normen»), se:

- «Normen» - https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet
- «Normen» (på Engelsk) - https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet/documents-in-english

For å understøtte Kundens forpliktelser og lovkrav tilknyttet informasjonssikkerhet, har Helse Sør-Øst definert et sett krav til informasjonssikkerhet i «Ledelsessystem for Informasjonssikkerhet». Kravsettet inneholder krav til infrastruktur, systemer og tjenester, samt til leverandører og ansvarlige for drift og forvaltning av infrastruktur, systemer og tjenester for Kunden, se forøvrig:

https://www.helse-sorost.no/informasjonssikkerhet-og-personvern/ledelsessystem-for-informasjonssikkerhet

Leverandøren forutsettes å ha satt seg inn i disse prinsippene, og sikrer at disse kan etterleves.

Kundens tjenesteleverandør benytter ISO 27001 som forvaltningsstandard i sikkerhetsarbeidet.

12.2 Risikostyring

Før løsningen kan etableres, og ved alle endringer av løsningen, må det gjennomføres og foreligge en godkjent risikovurdering. Risikovurderingen bygger på løsningens endelige løsningsdesign, med alle tilhørende komponenter, tjenester og konfigurasjon, slik løsningen er planlagt etablert hos Kunden. Dette vil normalt utarbeides av Kundens tjenesteleverandør, i samarbeid med Kunde og Leverandør. Endelig godkjenning av risikovurdering gjøres av Kunden.

Det er en målsetning at man for MTU legger ISO/IEC 80001 («Risk Management of Medical Devices on a Network») til grunn.

12.3 IAM og tilgangsstyring

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

For nærmere beskrivelse, se *Bilag 3C: Kundens tekniske plattform – Identitet og tilgangsstyring.*

13 Integrasjon

For å sikre at den tekniske infrastruktur bygger opp under virksomhetsarkitekturen med fokus på tjenester, har Helse Sør-Øst etablert en SOA-Arkitektur for integrasjoner med Fagsystemer. Helse Sør-Øst har realisert SOA-Arkitekturen ved å etablere en regional integrasjonsplattform og en integrasjonspolicy. Integrasjonspolicyen legger klare krav og retningslinjer på hvordan integrasjoner skal etableres, og at disse skal gå gjennom integrasjonsplattformen.

For nærmere beskrivelse, se *Bilag 3B: Kundens tekniske plattform – Integrasjon*.

14 Forkortelser og begreper

Forkortelse / Begrep	Beskrivelse
AD	Active Directory – Microsofts katalogtjeneste for autentisering og autorisering av brukere innenfor et Windows domene

Forkortelse / Begrep	Beskrivelse
App-V	Microsofts teknologi for virtualisering og strømming applikasjoner.
ATU	Administrativteknisk utstyr
BTU	Byggteknisk utstyr
BYOD	Bring Your Own Device – privateide PC klienter, nettbrett eller mobiltelefoner, som ikke er eid av eller kontrollert av Kunden.
CDS	Central Driver Store
CRL	Certificatate Revocation List
DNS	Domain Name System - Systemtjeneste for å oversette mellom maskinnavn og IP-adresse
EAP-TLS	Extensible Authentication Protocol – benyttes i sammenheng med NAC
Fabric Attach	Extreme Networks implementering av IEEE Auto Attach, som benyttes for policybasert tilkobling og autorisering av støttede nettverkskomponenter i et Fabric Connect basert nettverk.
Fabric Connect	Extreme networks implementering av IEEE Shortest Path Bridging.
IAM	Identity and Access Management, Kundens systemer for sentral autentisering, autorisering og federering av brukere og rettigheter.
ID-porten	DIFI ID-porten benyttes for autentisering av brukere på sikkerhetsnivå 4 (BankID, BankID for mobil, Buypass og Commfides)
IDS	Intrusion Detection System
IEEE 802.1x	Standard for autentisering av maskinvare tilkoblet nettverk. Må ikke forveksles med standarder for trådløst nett (WLAN).
Kunden	I dette dokumentet benyttes dette som begrep for helseforetaket Oslo universitetssykehus
Kundens tjenesteleverandør	Det til enhver tid gjeldende selskap/organisasjon som har ansvar for drift- og forvaltningsansvar for Kunden sin samlede IKT-infrastruktur og IKT-tjenestekatalog. I denne sammenheng er tjenesteleverandør Sykehuspartner.
LDAP	Lightweight Directory Access Protocol – Standard protokoll for tilkobling/integrasjon mot Active Directory

Forkortelse / Begrep	Beskrivelse
MAC-adresse	Unik ID tildelt nettverksgrensesnitt på lag2 i OSI-modellen
MPLS	Multi Protocol Label Switching
MSI	Format for applikasjonspakker som skal installeres lokalt på PC-klient.
MTU	Medisinskteknisk utstyr
NAC	Network Access Control – Se IEEE 802.1x
PAGA	Kundens personalsystem
RADIUS	Remote Authentication Dial-In User Service – Nettverksprotokoll som benyttes for autentisering av maskiner ifm. bruk av NAC.
RDP	Remote Desktop Protocol – Microsoft protokoll for fjernstyring av Windows PC/server, tilgjengelig fra Leverandørportalen
SDS	Sentralt Datasenter - Helse Sør-Øsst fellesregionale datasentre driftet av Sykehuspartner.
SHKR	Sentralt Hovedkommunikasjonsrom - Datarom etablert i kundens lokaler.
SOA	Service Oriented Architecture
SPB	Shortest Path Bridging
SSH	Secure Shell - Applikasjonsprotokoll med kryptert kommunikasjon for tilgang til pålogging og kommandolinje på fjernstyrt klient/server
SSID	Service Set Identifier – trådløst nett
TAP	Test Access Point – kloning av nettverkstrafikk
UltraVNC	Fjernstyringsverktøy, tilgjengelig fra Leverandørportalen
VLAN	Virtual LAN - en måte for logisk inndeling av nettverk i separate broadcastdomener
VPN	Virtual Private Network – kryptert, privat nettverksforbindelse
WAN	Wide Area Network - i denne sammenhengen benyttet som termineringspunkt for VPN
WinSCP	Fjernstyringsverktøy tilgjengelig fra Leverandørportalen

Forkortelse / Begrep	Beskrivelse
X.509 OU	Standard for sertifikater benyttet i sammenheng med NAC for etablering av PC-klienter i riktig VLAN, hvor OU (organizational unit) attributtet benyttes for å identifisere sone