Bilag 3: Kundens tekniske plattform

1 Beskrivelse IKT driftsmiljø

1.1 IKTNH

IKT Nordhordland er IT driftsorganisasjon for 10 kommuner i Hordaland. IKTNH er organisert etter vertskommune modellen og Osterøy kommune har driftsansvar. Kommunene IKTNH drifter er: Austevoll, Austrheim, Fedje, Lindås, Masfjorden, Meland, Modalen, Osterøy, Radøy og Vaksdal.

1.2 Struktur

Datakommunikasjonen er bygd opp med 2 serverrom i Knarvik, der alle tjenesteserverne er plassert. I hver kommune er det et rom med utstyr for kommunikasjon til/fra de sentrale serverrommene i Knarvik og som et knutepunkt for datatrafikk lokalt i kommunen. Serverrommene i kommunene har rutere fra leverandør (BKK/Telenor) og svitsjer som driftes av IKTNH.
Alle serverrommene skal ha UPS – dvs. avbruddsfri strømforsyning. Noen av de kommunale serverrommene har redundante linjer fra sin bredbåndleverandør.

2 Oppbygging av dagens IKT-løsning

2.1 Servertilgang

Datasystemene for de 10 kommunene i SING-samarbeidet er sentralisert og utstyr som servere, lagring, backup er plassert i felles serverrom i Knarvik.
Serverrommene i Knarvik er sikret med løsninger for tilgangskontroll, brannslukking og driftsstabilitet med UPS (batteristrøm) og nødstrømsaggregat. UPS sikrer driftsstrøm ved korte strømstans og dieselaggregat vil fortsette å sikre strømforsyning ved lengre utfall. Mellom serverrommene er det etablert fiber via 2 ulike føringsveier. BKK leverer linje til begge serverrom via ulike føringsveier. Telenor leverer kun linje til det ene serverrommet, men det planlegges å etablere redundant løsning i løpet av 2. kvartal 2018.

2.2 Sonemodell

Datanettverket er i hovedsak delt opp i 5 ulike soner:
- sikker sone med servere for fagsystem i helsesektor og andre personsensitive opplysninger
- intern sone med servere og klienter for administrativt nett
- pedagogisk sone for elevmaskiner
- teknisk sone for teknisk utstyr som for eksempel låsesystem, vann- og avløp og ventilasjon.
- management sone for administrasjon av IKTNH sitt utstyr.
- publikum sone for tilgang for gjester og usikre enheter

Tilgang til fagsystem i sikker sone går gjennom en Citrix Netscaler løsning der fagsystemene er gjort tilgjengelig via publiserte applikasjoner på Citrix XenApp terminalservere.

Til fagsystemene i intern sone går man inn enten direkte fra lokal PC eller fra Windows Terminalservere
i intern sone.

2.3 Domene- og AD-struktur

Det er etablert et felles Windows-domene, kalt *sing.local*. Dette domenet danner en logisk ramme for datautstyr som servere, PCer, skrivere m.m. Felles katalogtjeneste for data-objekter som brukerkontoer og grupper for tilgangsstyring m.m. er basert på Microsoft Active Directory – kalt AD. Katalog
(AD)-strukturen er basert på domenekontrollere i de ulike sonene. Et og samme AD brukes i indre soner (intern, pedagogisk, sikker, teknisk og management). Tilgang til tjenestene i AD er definert i forhold til brukernes stilling og sikkerhetsnivå.

2.4 Lokasjoner

Servere og lagringsløsning for kommunesamarbeidet er lokalisert til 2 serverrom i Knarvik; Lindås rådhus (lokasjon 1) og «Dampen» industribygg, Hagellia 6 (lokasjon 2).
I daglig bruk av datasystemet er det full drift/produksjon på begge lokasjoner, der servere og lagring blir utnytta med ca. halv last/kapasitet i kvart serverrom.
Til sammen vil de to lokasjonene fungere som en «Disaster Recovery» løsning, der utstyret på den ene lokasjonen alene vil ha kapasitet til å holde alle servertjenester i drift, om nødvendig.
Det er etablert leid mørk fiber levert av BKK til og mellom lokasjonene med 2 x 10GB hastighet. Det er to linjer med ulike føringsvei mellom lokasjonene.

2.5 Servere

Maskinvare for servere er standardisert på DELL og HP. Dell servere er i hovedsak blade-servere, plassert i 2 stk Dell M1000e Bladecenter. Tilsvarende er HP-servere i hovedsak blade-servere i 2 stk HP C7000 Bladecenter. Det er også installert noen Dell Poweredge og HP Proliant rack-servere. Det er et mål å virtualisere flest mulig av servere i fremtiden og de fleste eksisterende fysiske servere vil bli konvertert til virtuelle på sikt.
I begge serverrommene er 5 og 6 stk Dell M630 servere satt opp som ESXi-hoster i et Vmware vSphere 5.5/6.0 virtualiseringsmiljø. ESXi-hostene er tilknyttet et Dell Compellent SC4020 SAN på hver lokasjon.
Servere utenom Vmware har lokal lagring.
DELL- og HP Bladecenter har flere 10GB kommunikasjonskanaler til HP kjernesvitsjer (HP-5820AF) i en nettsentrisk løsning.

2.6 Virtualisering

VMware-løsningen har vSphere 5.5 og 6.0 Enterprise Plus installert på 11 stk Dell M630 blade-servere.
Disse ESXi-hostene er utstyrt med 2 CPU (à 12 kjerner) og 300-500 GB RAM kvar. Det virtuelle miljøet har ca 250 servere og blir administrert med vCenter server på hver lokasjon. Det er plassert 5 og 6 stk hoster i hvert serverrom, der hver lokasjon har kapasitet til å kjøre hele produksjonsmiljøet dersom den ene lokasjonen går ned.

2.7 Lagring

Lagringsløsningen for SING er basert på 2 stk DELL Compellent SAN. Disse har per i dag lagringskapasitet på ca. 75 TB hver. Compellent lagringssystemene er direkte tilkoplet DELL Bladecenter på hver lokasjon. Data blir replikert mellom de to systemene kontinuerlig og servere på den ene lokasjonen kan knytte seg mot lagringssystemet på den andre lokasjonen, om nødvendig.

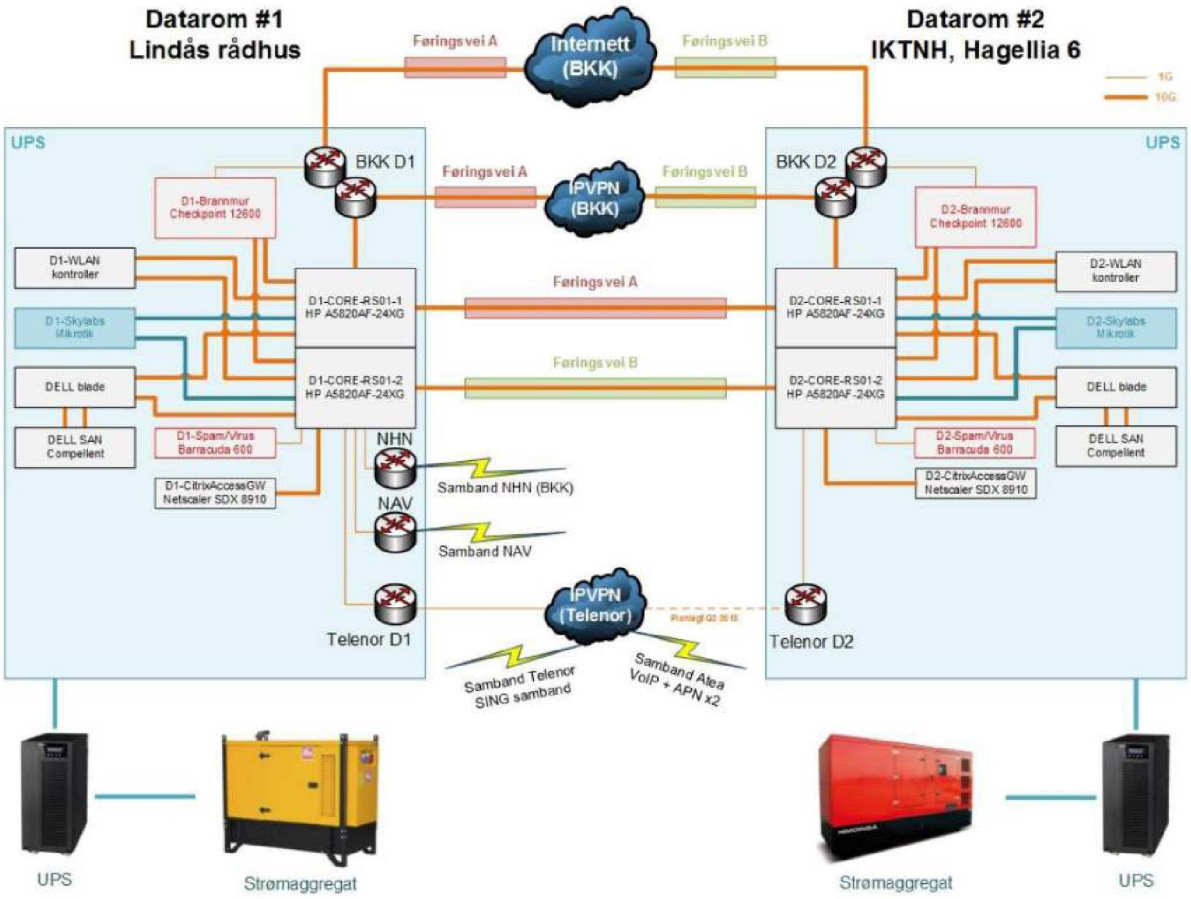
2.8 E-post

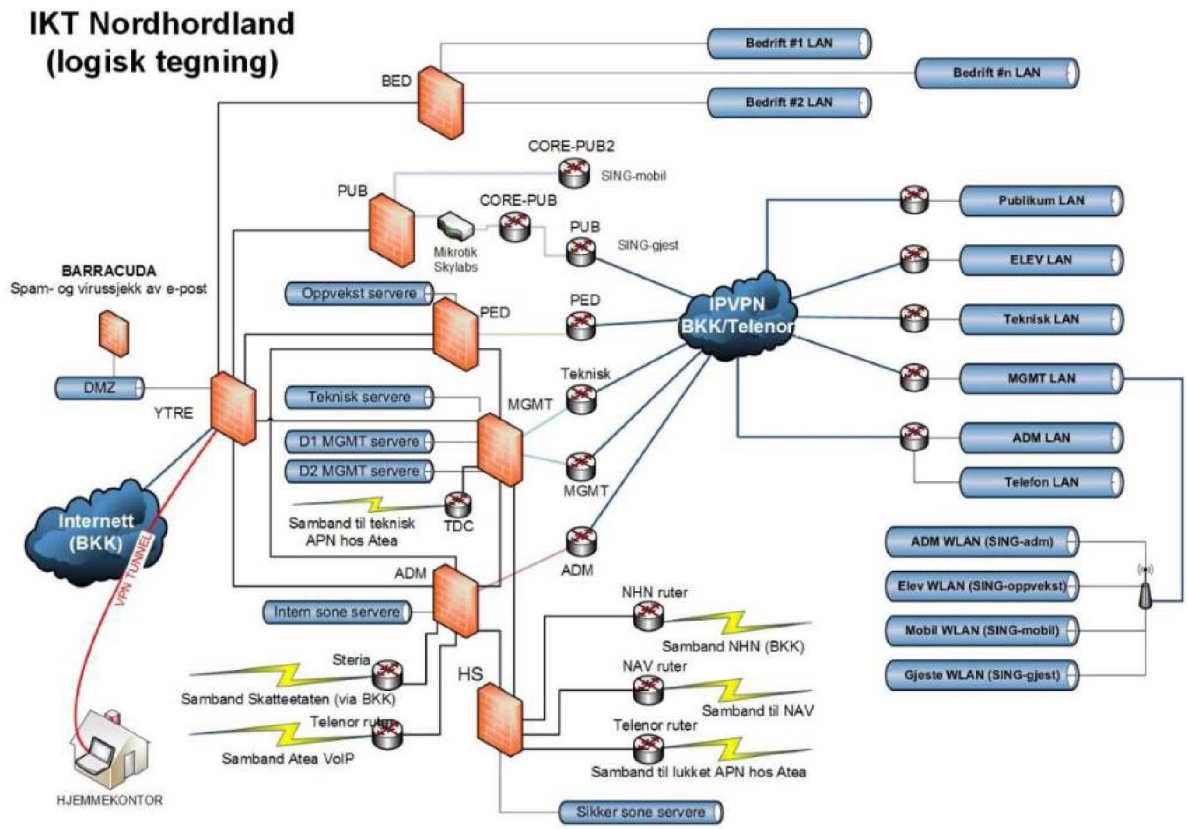
E-post løsningen er basert på Microsoft Exchange 2013. To separate hoster i VmWare med egne disker.
Hostene er plassert i hvert sitt serverrom og knyttet opp i felles DAG. Exchange inneholder 4 datastore og har en samlet kapasitet på ca. 14 TB (datastore og loggfiler).

2.9 Nettverk

Kommunene i samarbeidet har siden 2004-2005 hatt en samordnet fiberoppkobling mot internett – forløperen til dagens SING-nett. Mot internett er det satt opp brannmur som skanner all trafikk.
Kommunikasjonen mellom de ulike lokasjonene er basert på en kombinasjon av
- IP-VPN levert av BKK
- IP-VPN levert av Telenor
- trådløse samband levert av Nettstar
- trådløse samband hvor kommunene eier infrastrukturen selv
- egen fiber infrastruktur
- ADSL og bruk av VPN tunneler inn til sentrale serverrom.

For tilgang fra utsiden av SING-nettet benyttes i dag - for interne brukere - en CheckPoint løsning som gir VPN tilgang inn i nettet. Den er knyttet mot Active Directory og gir tilgang basert på basis av definert tilgangsnivå.
Tilgang til lokale nettverk skal i hovedsak foregå via Ethernet med minimum Cat.5e-kabling. På en del av våre lokasjoner er tilgang til nettverket likevel basert på trådløse aksesspunkt. Det er en uttalt målsetning - ut fra et drifts- og vedlikeholdsmessig synspunkt - at alle nettverk skal være kablet. Trådløse nett kan etableres som supplement der det ut fra funksjonshensyn er optimaliserende.


Datarom #1
Lindås rådhus
Føringsvei A
Internett
(BKK)
Føringsvei B
Datarom #2
IKTNH, Hagellia 6
1G
10G
UPS
BKK D1
Føringsvei A
IPVPN
(BKK)
Føringsvei B
BKK D2
UPS
D1-Brannmur
Checkpoint 12600
D2-Brannmur
Checkpoint 12600
D1-WLAN
kontroller
D2-WLAN
kontroller
D1-Skylabs
Mikrotik
D2-Skylabs
Mikrotik
D1-CORE-RS01-1
HP A5820AF-24XG
Føringsvei A
D2-CORE-RS01-1
HP A5820AF-24XG
DELL blade
D1-CORE-RS01-2
HP A5820AF-24XG
Føringsvei B
D2-CORE-RS01-2
HP A5820AF-24XG
DELL blade
DELL SAN
Compellent
D1-Spam/Virus
Barracuda 600
NHN
D2-Spam/Virus
Barracuda 600
DELL SAN
Compellent
D1-CitrixAccessGW
Netscaler SDX 8910
Samband NHN (BKK)
NAV
D2-CitrixAccessGW
Netscaler SDX 8910
Samband NAV
IPVPN
(Telenor)
Telenor D1
Telenor D2
Samband Telenor
SING samband
Samband Altea
VoIP + APN x2
UPS
Strømaggregat
Strømaggregat
UPS



2.10 Sykesignalanlegg / alarmhåndtering på institusjoner

Det finnes ulike løsninger for signalanlegg rundt om i kommunene – i hovedsak lokale løsninger. IKTNH har vært med å legge til rette for installasjon og drift av løsninger basert på teknologi fra bl.a. Ascom, Mitel og Mobicall.

2.11 Sikkerhet

2.11.1 Sikkerhet mot uautorisert tilgang til nettverket

Trafikken er inndelt i ulike nettområder basert på 6 definerte brukerkategorier:

- Administrativt nett
- Elevnett / pedagogisk nett
- Publikum / gjestenett
- Sikker sone nett
- Management
- Teknisk nett

Sikkerheten for tilgang til graderte soner ivaretas av ytterligere identifikasjon ved pålogging.
Det er lagt til rette for sikker tilgang for leverandører for bistand under installasjon og ved feilretting.

2.11.2 Brannmur

Brannmuren gir sikkerhet for inntrenging av uvedkommende i nettet ved:

- klient-to-site VPN
- site-to-site VPN
- SSLVPN for leverandører

- 2-faktor autentisering gjennom Secure Envoy
- Applikasjonskontroll
- URL filtrering
- IPS – forebygge inntrenging
- Anti-Bot
- Anti-Virus
- Identitetskontroll
- Trussel emulering
- endepunktsjekk
- 2 fysiske bokser – på fysiske lokasjoner
- logisk inndeling i flere virtuelle brannmurer

2.11.3 Nettverksdesign som tar i seg:

- kablet nett gir tilgang for
• datamaskiner
• skrivere
• telefoner
• management på nettverksutstyr
• tilgang til IP-basert teknisk utstyr
- trådløst nett gir tilgang
• datamaskiner (ansatte, elever, gjester, leverandører etc.)
• skrivere
• Telefoner
• Håndholdt utstyr (PDA, nettbrett, smart-telefoner, etc.)
- løsning for gjester og publikum som kun skal nå internett – felles for kablet nett og trådløst nett
- skanning av dokumenter fra utelokasjoner til sentrale servere – både i administrativt nett og til sikker sone

2.11.4 Mobilkommunikasjon - APN:

Det er etablert APN fra vår leverandør av telefoni for sikker kommunikasjon fra mobile enheter som nettbrett, stasjonære trygghetsalarmer, pumpestasjoner, renseanlegg m.m. Denne kommunikasjonen termineres i våre datarom. Det er ulike APN for trafikk mot tekniske installasjoner kontra trafikk som håndterer sensitiv informasjon.

3 Eksisterende EPJ-løsninger i pleie- og omsorgssektoren for kommunene Lindås, Meland, Radøy og Vaksdal

Lindås og Vaksdal bruker fagsystemet Visma Profil (p.t. versjon 8.30), mens Meland og Radøy har Acos Cosdoc (p.t. versjon 12).

Visma Profil har integrasjoner med VAR Healthcare prosedyrebibliotek, Personregister (Folkeregister gjennom NHN), SvarUT og import av FEST legemiddelkatalog, Diagnoseregistere (ICP-2 og ICD-10) og Nettoinntekt.

Acos Cosdoc har integrasjoner med VAR Healthcare prosedyrebibliotek, ICNP og import av vareregister fra Farmalogg, Diagnoseregistere (ICP-2 og ICD-10) og Nettoinntekt.

Kommunene har løsning for skanning fra multifunksjonsmaskiner (kopimaskiner) til EPJ.

Felles e-meldingstjener har installert Visma Link til bruk både for Profil og Cosdoc.

Servere for EPJ er plassert i «sikker sone» og består av databaseserver, applikasjonsserver/Webserver for støttefunksjoner, filserver for tekstmaler og mellomlagring, og terminalservere for applikasjonsklient (Visma Profil) eller nettleser (Acos Cosdoc).

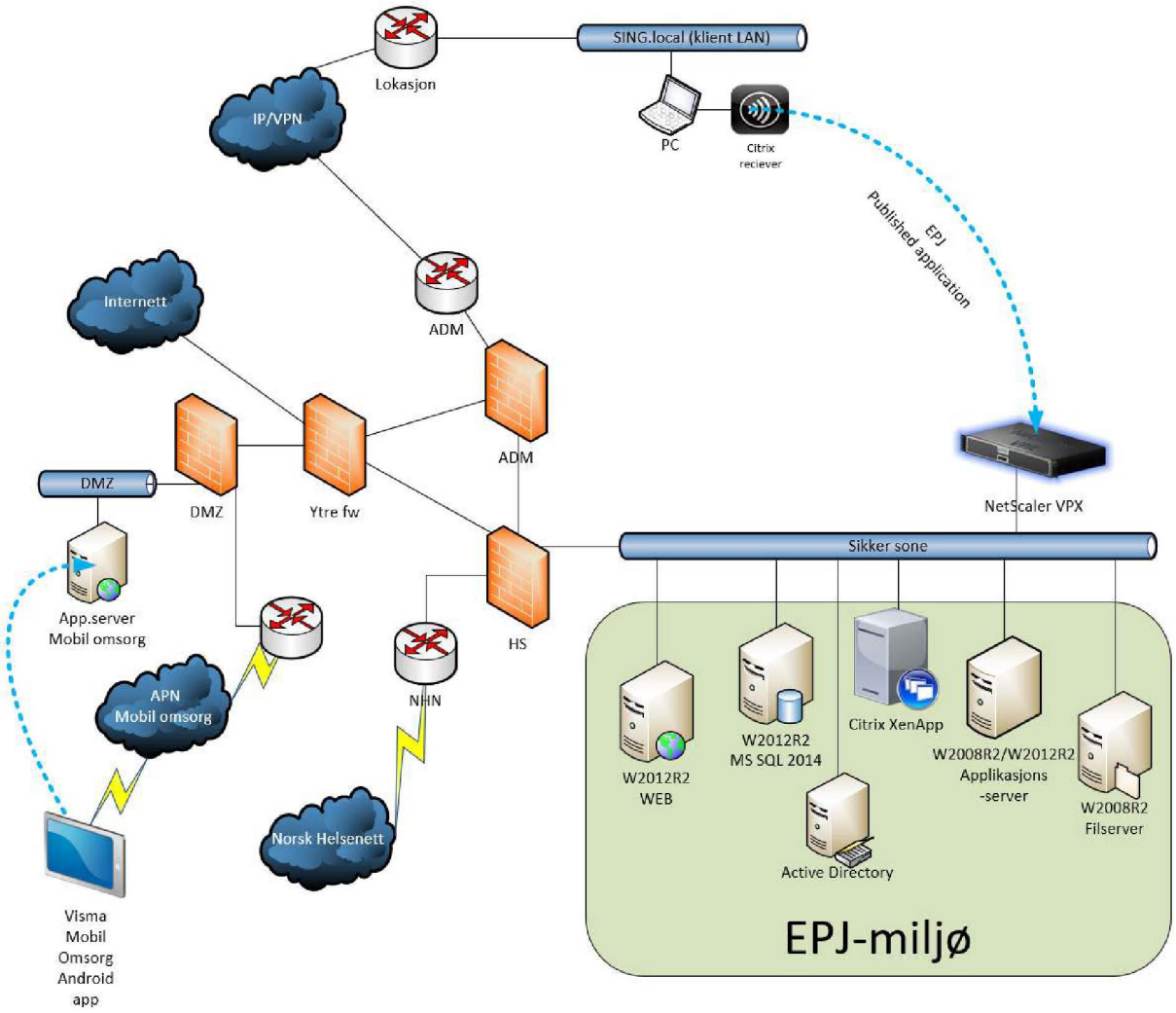
Applikasjoner kjører på MS Windows 2012 R2 terminalservere med Citrix Xenapp 7.13 overbygning. Snarveier til applikasjonene publiseres/distribueres til klient-PC'er i Web-grensesnitt.

Tilgang til sikker sone og EPJ-systemene går gjennom Citrix Netscaler applikasjonskontrollere. Det er startet et prosjekt i kommunene for autentisering med smartkort mot AD og sikker sone, med lokal PKI/sertifikat infrastruktur og for autentisering for systemer/tjenester i Norsk Helsenett med sertifikater fra Buypass.

Lindås og Vaksdal har løsning for hjemmetjeneste fra Visma, kalt Mobil Omsorg. Denne benytter APP'er på nettbrett og kommuniserer inn gjennom lukket APN i mobilnettet til servere i vårt nett. Nettbrettene kjører Android versjon 4 eller nyere.

Utskrift skjer til sikker utskrift/follow-me løsning, basert på sesjonsskrivere i Citrix.

Systemskisse - EPJ infrastruktur



4 SERVERE for EPJ i Meland og Radøy:

4.1 ACOS COSDOC

4.1.1 Databasetjener

MS Windows 2012 R2
MS SQL server 2014
SQL-instans pr kommune

Acos Cosdoc produksjonsbase – Cosdoc produksjonsbasen er grunnpilaren i journalsystemet til organisasjonen.

Acos Cosdoc kursdatabase – Cosdoc kursbase er en kopi av produksjonsbasen gor Cosdoc hvor sentitiv informasjon er slettet.

4.1.2 Applikasjonstjener

MS Windows 2012 R2
MS Windows IIS
Applikasjons tjener for ACOS produkter benyttes for å holde ulike applikasjoner og tjenester som er nødvendige for å benytte ACOS sin produktportefølje.

E-meldinger, Adresseregister, Ligningsopplysninger, Sumrapporter

4.1.3 Filtjener

MS Windows 2008

Kataloger for tekstmaler, brukerdokumentasjon, NAF Vareregister m.m.

5 SERVERE for EPJ i Lindås og Vaksdal:

5.1 VISMA PROFIL

5.1.1 Databasetjener

MS Windows 2012 R2
MS SQL server 2014
SQL-instans pr kommune

EPJ produksjonsdatabase
Visma Samhandling Arkiv database
Visma Adresseregister database

5.1.2 Applikasjonstjener #1

MS Windows 2008 R2
MS Windows IIS

Portal til VSArkiv, VAdresseregister, IPLOS Sumrapporter

5.1.3 Applikasjonstjener #2

MS Windows 2012 R2
MS Windows IIS

Visma Mobil Omsorg

5.1.4 Filtjener (samme som for Acos Cosdoc)

MS Windows 2008

Kataloger for tekstmaler, brukerdokumentasjon, FEST-register, diagnoseregistere, nettoinntekt m.m.