KDRS digitalt depot

Spesifikasjon av tjenesten

Versjoner:

20110830	Versjon 1.0	Første versjon publisert	Tor Eivind Johansen
20170823	Versjon 1.1	Oppdatert versjon	Tor Eivind Johansen
20180619	Versjon 1.2	Oppdatert versjon	Tor Eivind Johansen
20200214	Versjon 1.3	Oppdatert kapasiteter og noen justeringer	Tor Eivind Johansen

Innledning

KDRS skal tilby sine medlemmer et digitalt depot for elektroniske arkiv. Dette dokumentet beskriver hvordan denne tjenesten leveres til medlemmene på et overordnet nivå.

Det er mange ønsker fra medlemmene som ikke er mulige å realisere på bakgrunn av kostnaden som er tilknyttet. Det har derfor vært viktig at de kravene som er blitt prioritert er reelle slik at digitalt depot kan realiseres innenfor de rammene som KDRS har mulighet for.

Digitalt depot

Digitalt depot for elektroniske arkiv er et av KDRS sine prioriterte oppgaver. Det digitale depotet vil i første runde etableres som et digitalt infrastruktur prosjekt, og deretter utvikles med flere tjenester tilknyttet etter hvert.

Digitalt depot som beskrives her er den løsningen som tilbys pr. juni 2018.

Tilgjengelighet

Digitalt depot skal være operativ innenfor normal kontortid. Med dette menes det mellom kl 8:00 og 15:30 alle arbeidsdager. Det aksepteres at systemet er nede for teknisk service med en dag pr. måned når dette varsles 6 dager før servicen gjennomføres.

Krav til oppe tid (eksklusiv service) skal være 98 % innenfor kontortid.

Det skal være mulig å komme i kontakt med support personell hos KDRS mellom kl 8:00 og 15:30. Det er etablert en egen e-post for tekniske spørsmål i tillegg til at det er mulig å ta telefonisk kontakt. Hendelser og avvik kan meldes på hjelp@kdrs.no og vil da logges automatisk i vårt oppfølgingssystem.

Oppstår det feil i systemet etter kl 15:30 vil feilretting ikke påbegynnes før neste arbeidsdag. Mens feilretting pågår vil tjenesten, eller deler av tjenesten ikke være tilgjengelig.

Driftsmeldinger vil bli kunngjort på https://www.kdrs.no/driftsmeldinger.

Månedsrapporter på oppetid på tjenesten er tilgjengelig på https://www.kdrs.no/oppetid-digitalt-depot.

Sikkerhet

Digitalt depot er etablert i en egen sikkerhetssone. Det vil ikke være tilgang til internett fra denne sonen. Oppkobling fra medlem til sikker sone skjer med VPN oppkobling med to-faktor autentisering. Overføring av data vil skje via verktøyet ETA som overfører arkivpakken direkte fra medlemmets dataområde (lokalt) via en kryptert tunell inn til sikker sone hvor det digitale depotet er. Når selve overføringen i ETA er kryptert, og når dette skjer gjennom en VPN tunell, vil overføringen være dobbelt kryptert.

Basert på gode erfaringer har det også blitt åpnet for mulighet til overføring med FileZilla noe som har vist seg å gi en høyere overføringshastighet. Denne overføringen skjer også gjennom VPN tunellen.

Pålogging til forvaltningssystemet (ESSArch EPP) skjer med brukernavn og passord.

Sikring av utstyr og driftsmiljø

Digitalt depot er plassert i flere datarom, blant annet sammen med andre bedrifters utstyr. Alt utstyr tilhørende KDRS er derfor låst inne i eget skap (rack). Datarommet er utstyrt med nødvendig kjøling og brannmelder. Datarommet har adgangskontroll system med logging. Miljøparameter som temperatur etc. måles og logges av KDRS utstyr. Alle KDRS skap (4 stk.) er utstyrt med alarmer, slik at hvis dører eller vegger åpnes, gis det alarmer til KDRS sitt overvåkningssystem.

Det er ikke etablert aggregat for datarommene slik at utstyret ikke vil fungere ved strømstans. Utstyret er sikret med batteri backup (UPS) for å kunne få en kontrollert nedkjøring ved strømbrudd. All omkringliggende nettverks infrastruktur og internett vil falle ut ved strømstans i hovedserver rom i Trondheim.

Overføring og kapasitet

Digitalt depot hadde ved etablering en startkapasitet på omlag 20 TByte lagringsplass. Dette var i henhold til de tilbakemeldingene KDRS har fått fra våre medlemmer være tilstrekkelig i om lag tre år fram i tid da dette ble planlagt i 2013. Utstyret som er anskaffet kan utvides, og KDRS har nå utvidet kapasiteten til 96 TByte brutto lagringskapasitet, noe som en effektiv lagringskapasitet på om lag 55TByte. All data lagres i RAID system slik at en fysisk disk kan feile uten datatap. Ved feil på en fysisk disk skal en reservedisk automatisk ta over og data reetableres med feiltoleranse.

Alle lokasjoner har fibertilknytning med 1Gbit hastighet fra UNINETT. Kapasiteten kan økes ved behov.

Sikkerhetskopiering

Det tas sikkerhetskopi en gang pr. døgn fra produksjonssystem til en diskløsning i et annet datarom i Trondheim. Sikkerhetskopien vil bli tatt over egen privat nettverksforbindelse til et datarom som er fysisk lokalisert i et annet bygg. Maskinvare for sikringskopi og lagringsenheter er alarmbelagt med direkte overføring til KDRS overvåking samt SMS til KDRS personale.

Programvaren Veeam Backup and Replication benyttes til dette formålet.

Elektromagnetisk stråling

Alle data i digitalt depot vil lagres på magnetiske media. Dette medfører at kraftig elektromagnetisk stråling fra strålevåpen eller atombomber kan ødelegge data – både i digitalt depot og på sikkerhetskopier. For å redusere denne risikoen er det etablert en egen server med båndlager i fjellhallen til Arkivverket ved Sognsvann og det er etablert en tilsvarende lagringsenhet er lokalisert i fjellhallen til Nasjonalbiblioteket. Dette er en avstand på 100 mil noe som vil medføre redusert risiko for at elektromagnetisk stråling vil kunne ødelegge alle kopiene av innholdet i det digitale depotet.

Arkivpakkene overføres til båndlanger i Oslo og i Mo i Rana direkte under lagring på hovedmaskin. Når lagringsprosessen er avsluttet, er også kopiene i Oslo og Mo i Rana lagret. Lagringen skjer på magnetbånd av typen LTO6. Hvert medlem har eget sett med magnetbånd. All overføring mellom hovedmaskin i Trondheim og maskinene i Oslo og Mo i Rana skjer via fast oppkoblet VPN nett med 256 bits nøkler. Overføringen mellom systemene skjer med https og dataene som overføres er derfor dobbelt kryptert ved denne overføringen.

Oppkobling til KDRS

Overføringen av data fra medlemmene til KDRS skje med en sikker overføring basert på VPN med to-faktor autentisering. Alle brukere vil få en app til smart telefonen som må benyttes til generering av en nøkkel som benyttes ved innlogging. Det er etablert en sentral brukeradministrasjon hos KDRS for å håndtere alle påloggінger samt mulighet for at bruker selv kan bytte passord med jevne mellomrom. Passord utløper etter 52 uker og må da settes på nytt.

Administrasjonssystem

Forvaltningssystemet for digitalt depot som KDRS benytter er ESSArch fra ES Solution. Dette er det samme systemet som Arkivverket benytter samt Bergen byarkiv. Dette systemet håndterer arkivpakkene med den strukturen slik det er besluttet i DIAS prosjektet.

Overvåkning og konfigurasjonsstyring

Det er etablert driftsovervåkning av alle tjenestene ved hjelp av programvaren PRTG fra selskapet Paessler AG. Ved problemer vil dette systemet rapportere avviket, med prioritert til driftspersonalet. Ved kritiske hendelser vil meldinger sendes på SMS til driftspersonale.

Konfigurasjonsstyring gjennomføres ved hjelp av programvaren OTRS, som også håndterer hendelser og avvik.

Overførings tjeneste – FileSender

For å forenkle hverdagen hos våre medlemmer er det etablert en tjeneste som kan overføre store filer fra et sted til et annet. Utfordringen med å sende USB minnepenner og harddisker har med ført at data har kommet på avveie og data har gått tapt.

FileSender muliggjør for alle medlemmer med tilgang til Digitalt depot, å sende eller motta store filer, typisk en kryptert arkivpakke. Alle som har tilgang til tjenesten kan sende en invitasjon f.eks. til en i kommunen om at en kryptert arkivpakke kan sendes til et medlem. Tjenesten forenkler innhenting av arkiver, og effektiviserer denne delen av arbeidsprosessen.

Risikovurderinger

Det er gjennomført risikovurderinger for tjenestene som er etablert.