Vel bevart!

Rapport fra samarbeidsprosjektet DIAS
– Digital arkivpakkestruktur

Riksarkivaren
8. juni 2012

Innhold

1. INNLEDNING 4

1.1 Presentasjon av DIAS-prosjektet 4

1.2 Sammendrag av prosjektmål og resultater 4

2. GJENNOMFØRINGEN AV DIAS-PROSJEKTET 5

2.1 Bakgrunn for prosjektet 5

2.2 Mål og målgrupper 6

2.3 Organisering 7

2.4 Planutvikling og status for måloppfyllelse 8
2.4.1 Planutvikling 8
2.4.2 Initielle prosjektmål 8
2.4.3 Systemutviklingsprosjekt 2011-2012 9

2.5 Kompetansebygging 10

2.6 Norsk-svensk samarbeid 10

2.7 Ressursbruk og prosjektregnskap 11

3. KRAV SOM STILLES TIL DIGITALE ARKIVDEPOTER 12

3.1 Utfordringene ved langtidsbevaring av digital arkivinformasjon 12
3.1.1 Spesielle utfordringer knyttet til integritetssikring 12

3.2 Krav i foreliggende standarder 13
3.2.1 OAIS-standarden 13
3.2.2 TRAC-standarden 14
3.2.3 ”Core Principles” – Ti basiskrav til et digitalt arkivdepot 15

3.3 DIAS i relasjon til OAIS og TRAC 15

4. DIAS-PROSJEKTETS RESULTATER OG PRODUKTER 17

4.1 DIAS arkivpakker – Overordnet organisering 17

4.2 DIAS-pakkemodellen som en prosessmodell 18

4.3 Implementeringsstandarder og xml-skjemaer 20
4.3.1 Implementeringsmodell 20
4.3.2 Bruk av METS 21
4.3.3 Bruk av PREMIS 23
4.3.4 Oversikt over PREMIS Events, Rights og Agents 25
4.3.5 Bruk av EAD og EAC-CPF 27
4.3.6 Bruk av ADDML 28

4.4 Kravspesifikasjon til et forvaltningssystem for DIAS arkivpakker 28

4.5 Utvikling av ESSArch som et DIAS-tilpasset forvaltningssystem 29

4.6 Prosessmodeller for et DIAS-basert digitalt depot 30

5. IMPLEMENTERING AV ET DIAS-FORVALTNINGSSYSTEM 31

5.1 ESSArch-prosjektet – Opplegg og gjennomføring 31

5.2 ESSArchs plass og rolle i produksjonsmiljøet 31

5.3 Prosesser i et ESSArch-styrt digitalt depot 33

5.3.1 Initiell mottakskontroll 33
5.3.2 Innsjekking og pakkegenerering i ESSArch 36
5.3.3 Prosesser ved testing 38
5.3.4 Prosesser ved vedlikehold av arkivpakker 39
5.3.5 Prosesser ved fremstilling av bruksversjoner (DIP-er) 39
5.3.6 Logging av hendelser i forvaltningssystemets database 40

5.4 ESSArchs teknologiplattform og krav til utstyrsanskaffelser 44

6. DIAS FORVALTNINGSFORUM 45

6.1 Etablering av DIAS forvaltningsforum 45

6.2 Oppgaveramme for DIAS-forumet 45

VEDLEGG 1: OVERSIKT OVER PROSJEKTDELTAKERE 47

VEDLEGG 2: SAMLET REGNSKAP FOR DIAS-PROSJEKTET 49

1. INNLEDNING

1.1 Presentasjon av DIAS-prosjektet

DIAS (*Di*gital *a*rkivpakke*s*truktur) er gjennomført som et formalisert samarbeidsprosjekt mellom Riksarkivaren og 4 kommunale aktører – Oslo byarkiv, Bergen byarkiv, IKA Trøndelag og IKA Møre og Romsdal – for å etablere et felles norsk rammeverk for digitale arkivdepoter. Prosjektet, som har vært ledet av Riksarkivaren, ble startet i april 2010 med økonomisk støtte på 1 mill. kr. fra ABM-utvikling (nå Norsk kulturråd).

DIAS ble opprinnelig definert som et ettårig prosjekt. Men som resultat av stigende ambisjoner underveis, ble det besluttet utvidet til et toårig prosjekt. Utvidelsen ble gjort økonomisk mulig ved tilførsel av ekstra prosjektmidler fra Landslaget for lokal- og privatarkiver (LLP), IKA Trøndelag og Riksarkivaren.

Prosjektet har hatt en styringsgruppe og en prosjektgruppe med deltakere fra samtlige prosjektpartnere. I tillegg har det hatt en referansegruppe med deltakere fra andre instanser innenfor det norske arkivmiljøet. En egen prosjektorganisasjon under styringsgruppen ble etablert i november 2011 i tilknytning til utviklingen og implementeringen av et DIAS-basert forvaltningssystem.

1.2 Sammendrag av prosjektmål og resultater

DIAS-prosjektets hovedmål har vært:

- å spesifisere en struktur for arkivpakker som lar seg anvende for alle typer av digitale leveranser som mottas for bevaring av statlige og kommunale arkivdepoter,
- å utvikle hjelpemidler for praktisk bruk av denne bevaringsstrukturen.

Prosjektet har oppfylt alle målene i den opprinnelige planen som lå ved Riksarkivarens søknad 15.10.2009 til ABM-utvikling. Som resultat av prosjektet er det definert en omforent struktur for å bevare digitalt skapt arkivmateriale med opprettholdt integritet, lesbarhet og forståelighet. Bevaringsstrukturen skal kunne anvendes fleksibelt for alle typer av digitale avleveringer/deponeringer til Arkivverket og kommunale arkivdepoter. Prosjektet har også spesifisert xml-skjemaer som hjelpemidler til å generere DIAS-strukturerte arkivpakker. I tillegg har det utarbeidet en generell kravspesifikasjon til et system for å generere og vedlikeholde arkivobjekter med denne strukturen.

Utvidelsen av DIAS-prosjektet i forhold til den opprinnelige planen har bestått i å utvikle og implementere et forvaltningssystem som oppfyller prosjektets kravspesifikasjon, og som lar seg tilpasse for alternative lagringskonfigurasjoner og -medier i digitale arkivdepoter. Første versjon av systemet ble ferdigstilt for ordinær drift i Riksarkivet primo juni 2012 – som DIAS-prosjektets pilotinstallasjon. Prosjektet har med dette utviklet et forvaltningssystem som er klargjort for innføring og bruk i statlige og kommunale depoter. Systemet er basert på fri programvare, og vil også være fritt tilgjengelig for alle andre interessenter.

2. GJENNOMFØRINGEN AV DIAS-PROSJEKTET

2.1 Bakgrunn for prosjektet

Arkivverket har mottatt avleveringer av digitalt skapt arkivmateriale siden 1985. For kommunal sektor har imidlertid depotløsninger for digitalt materiale lenge representert et stort problem. Bare de største byarkivene og enkelte av de interkommunale arkivene har maktet å etablere depottjenester for å motta digitalt skapt arkivmateriale for bevaring. Presset for å få opp depotløsninger for kommunesektorens digitale arkivmateriale er stort. Men det er også behov for løsninger for å bevare digitalskapte privatarkiver. På dette viktige oppgaveområdet har heller ikke Arkivverket resultater å vise til.

De statlige avleveringsbestemmelsene[1] og normalinstruksen for arkivdepot i kommuner og fylkeskommuner[2] fastsetter hvordan digitalt arkivmateriale skal være strukturert, formatert og dokumentert ved overføring til arkivdepot. Men det eksisterer ikke tilsvarende regler og metodebeskrivelser for håndteringen av materialet når det forvaltes i digitalt depot. Behovet for å definere et slikt rammeverk var bakgrunnen for prosjektet *eArkivsamarbeidet*, som ble startet av 21 kommunale arkivinstitusjoner i 2004 med støtte fra ABM-utvikling. Prosjektet utarbeidet en metodehåndbok for kommunale arkivdepoter basert på arkivstandarden OAIS. Det var dermed også først ute med å anvende denne internasjonale arkivstandarden på offentlig forvaltningsnivå i arkiv-Norge. Prosjektets sluttrapport – *Minnehåndtering. Metode for digital langtidsbevaring i kommunal sektor* – ble utgitt av ABM-utvikling i 2007 som ABM Skrift # 43[3].

eArkivsamarbeidet initierte også prosjektet *OpenARMS* for å utvikle et OAIS-basert styringssystem for digitalt depot. Prosjektet ble gjennomført med Landslaget for lokal- og privatarkiver som prosjektansvarlig, og mottok støtte fra ABM-utvikling i 2005 og 2006. OpenARMS ble imidlertid ikke ferdigstilt etter planen.

IKA Trøndelag fulgte opp eArkivsamarbeidet med et prosjekt for å teste anvendeligheten av åpent tilgjengelige styringssystemer (”Open repository”-systemer) for digitalt depot. Prosjektet ble støttet av ABM-utvikling, men stilt i bero ved DIAS-prosjektets start.

Riksarkivet gjennomførte i 2008 – 2010 prosjektet Elmag-2 for å planlegge en modernisert depotløsning for Arkivverkets digitalt skapte arkivmateriale med on-line lagring på disk og kopier på tape (tape-roboter). Prosjektets sluttrapport ”Digitalt og autentisk” (01.03.2010)[4] spesifiserte også en struktur for lagring og vedlikehold av digitalt arkivmateriale basert på OAIS-standarden.

[1] http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-19991201-1566.htmll#map058 (lest 25.03.2012)

[2] http://www.arkivverket.no/arkivverket/Offentlig-forvaltning/Avlevering/For-kommuner/Normalinstruksen (lest 25.03.2012)

[3] http://www.abm-utvikling.no/publisert/abm-skrift/abm-skrift-43.html (lest 25.03.2012)

[4] http://www.arkivverket.no/arkivverket/Arkivbevaring/Elektronisk-arkivmateriale/Langtidslagring/Nytt-digitalt-depot (lest 17.02.2012)

Samarbeidet mellom Riksarkivaren og de fire kommunale aktørene i DIAS-prosjektet skjøt direkte ut av Riksarkivets Elmag-prosjekt. Prosjektsamarbeidet i DIAS begrenset seg i utgangspunktet til å følge opp Elmag-rapportens OAIS-baserte arkivpakkemodell, og da med det konkrete mål å spesifisere en felles arkivpakkestruktur for statlige og kommunale depoter. Etter denne avgrensede målsettingen innledningsvis har prosjektet likevel samlet i seg alle målene fra de tidligere kommunale prosjektene.

I prosjektsøknaden til ABM-utvikling ble det satt som et selvstendig mål å etablere et formalisert samarbeid om digitale arkivdepoter mellom Riksarkivaren og de sentrale aktørene fra kommunal sektor. Det ble lagt til grunn at et relativt konsentrert prosjekt om digital arkivpakkestruktur også ville samle i seg andre, helt sentrale problemstillinger knyttet til digital langtidsbevaring, og dermed bane vei for et bredere samarbeid om metodikk og verktøyutvikling for digitale arkivdepoter.

2.2 Mål og målgrupper

Målet for første del av DIAS-prosjektet har vært å spesifisere en arkivpakkemodell for hele variasjonsbredden av digitale arkiver som bevares på statlig og kommunal sektor. Den sentrale prosjektaktiviteten har her vært å tilpasse og komplettere arkivpakkestrukturen i Riksarkivets Elmag-rapport slik at den blir bredt anvendelig og skalérbar, og slik at den også kan brukes av arkivdepoter som fortsatt baserer seg på tradisjonell langtidslagring på bortsettingsmedier (CD-er og tape).

Det neste og oppfølgende målet for prosjektet har vært å utvikle hjelpemidler for praktisk bruk av denne bevaringsstrukturen, først og fremst i form av spesifikasjoner. Programvare-utvikling ble fra først av ikke planlagt som en del av DIAS-prosjektet, men den opprinnelige søknaden til ABM-utvikling holdt likevel muligheten åpen for å komme tilbake med en søknad om utviklingsmidler for dette formålet.

Med utvidelsen av DIAS til et toårig prosjekt ble program- og produktutvikling definert som et tilleggsmål. Å utvikle og implementere et forvaltningssystem for DIAS-strukturerte arkivpakker har formet seg som et hovedmål i prosjektets avsluttende fase fra våren 2011.

DIAS behandler ikke lagringsløsninger. Det har tvert i mot vært en viktig forutsetning at DIAS-prosjektets standarder og produkter skal kunne tilpasses for ulike lagrings-konfigurasjoner og -medier, herunder tradisjonell lagring på CD-er. Utviklingen av DIAS-prosjektets forvaltningssystem rokker heller ikke ved denne målsetningen. Systemet skal også kunne brukes av arkivdepoter som fortsatt baserer seg på tradisjonell langtidslagring på bortsettingsmedier. Men det er samtidig viktig å understreke at DIAS-prosjektet legger til rette for nye lagringsløsninger – som i Riksarkivets nye digitale depot.

DIAS behandler heller ikke struktur- og formatkrav til statlige og kommunale avleveringer/ deponeringer, men baserer seg på gjeldende bestemmelser. DIAS omfatter struktureringen og håndteringen av materialet i digitalt depot, og i prinsippet skal denne metodikken kunne anvendes for mottatt materiale i vilkårlig format og organisering. Det er likevel klart at prosjektets løsninger legger opp til en justering av statlige og kommunale avleveringsbestemmelser for å tilrettelegge for arkivdepotenes bruk av DIAS-metodikken.

Innledningsvis kan det også være behov for å presisere at DIAS ikke omfatter tilgjengelig-gjøring og bruk av bevart digitalt arkivmateriale, men begrenser seg til lagring og vedlike-

hold av digitale originaler i et sikringsmagasin. Det inngår imidlertid i DIAS å tilrettelegge versjoner for bruk – utenfor sikringsmagasinet for originaler i langtidslagringsformat.

Den umiddelbare målgruppen for DIAS-prosjektets resultater og produkter er prosjektpartnerne selv: Arkivverket, Oslo byarkiv, Bergen byarkiv, IKA Trøndelag og IKA Møre og Romsdal, som alle har operativ erfaring med digitalt arkivmateriale som depotinstitusjoner. Til gruppen av partnere med sentrale aktørroller på kommunal sektor hører dessuten Kommunearkivinstitusjonenes digitale ressurssenter (KDRS), som har deltatt i DIAS i prosjektets avsluttende fase.

Den primære målgruppen for DIAS er likevel alle statlige og kommunale arkivdepoter. DIAS-løsningene er direkte innsiktet på disse, og produktene er fritt tilgjengelige for dem.

Prosjektets ytre målgruppe er alle interesserte aktører på privat sektor. DIAS-produktene vil også være fritt tilgjengelige for disse, både i tilknytning til egne depotløsninger og ved avlevering av digitalt materiale til et offentlig arkivdepot.

2.3 Organisering

Prosjektet har hatt en styringsgruppe og en prosjektgruppe, hver med deltakere fra samtlige prosjektpartnere. I tillegg har prosjektet hatt en referansegruppe med deltakere fra andre instanser innenfor det norske arkivmiljøet. For utviklingen og implementeringen av DIAS-prosjektets forvaltningssystem ble det i oktober 2011 etablert en egen prosjektgruppe under styringsgruppen. For dette utviklingsarbeidet ble det også oppnevnt en egen referansegruppe. En oversikt over prosjektdeltakerne i DIAS følger som vedlegg 1.

- *DIAS-styringsgruppen* har vært ledet av Ole Gausdal fra Riksarkivet. Den har hatt 15 ordinære møter. For å sikre en nær kontakt med Kommunearkivinstitusjonenes digitale ressurssenter (KDRS) ble lederen invitert som fast møtedeltaker fra august 2011.
- *DIAS-prosjektgruppen* har utført prosjektets utrednings- og spesifikasjonsoppgaver. Den har vært ledet av prosjektlederen for DIAS, Trond Sirevåg fra Riksarkivet. Gruppen har hatt 18 ordinære møter, herav 5 over to dager.
- *Prosjektets referansegruppe* har hatt 3 møter, ett i 2010 og to i 2011.
- *Prosjektgruppen for utvikling, testing og akseptanse av DIAS-forvaltningssystemet* (”ESSArch-prosjektgruppen”) ble oppnevnt av styringsgruppen 07.10.2011. For dette prosjektet ble det utarbeidet et eget prosjektdirektiv. Prosjektgruppen har vært ledet av Terje Pettersen-Dahl fra Riksarkivet, og hatt deltakere fra det kommunale DIAS-miljøet og de berørte enhetene i Riksarkivet. Gruppen har hatt 11 møter.
- *Referansegruppen for utviklingsarbeidet* (”ESSArch-referansegruppen”) har hatt medlemmer fra det kommunale arkivmiljøet, statsarkivene og Riksarkivet. Gruppen har hatt ett møte.

Styringsgruppen oppnevnte en egen delegasjon for å vurdere mottatte leverandørtilbud og føre forhandlinger med tilbydere i forbindelse med at det i april-mai 2011 ble gjennomført en runde med offentlig tilbudsinnhenting på et DIAS-tilpasset forvaltningssystem.

I tilknytning til utviklingen og implementeringen av DIAS-forvaltningsystemet opprettet styringsgruppen en egen koordineringsgruppe med systemleverandøren, og oppnevnte DIAS-prosjektets medlemmer av gruppen.

2.4 Planutvikling og status for måloppfyllelse

2.4.1 Planutvikling

I prosjektsøknaden 15.10.2009 til ABM-utvikling ble prosjektet beregnet sluttført i løpet av 2010. En noe forsinket igangsetting medførte at sluttføringen allerede ved oppstart ble forskjøvet til 01.03.2011. I brev 21.09.2010 til ABM-utvikling søkte Riksarkivaren om adgang til å forlenge prosjektet til 01.11.2011 med en utvidet ramme som også omfattet programutvikling og kompetansebygging. ABM-utvikling ga samtykke til dette, og godkjente samtidig en overføring av udisponerte prosjektmidler til budsjettåret 2011.

Som bidrag til å finansiere en programutvikling i prosjektets regi i 2011 besluttet Landslaget for lokal- og privatarkiver (LLP) og IKA Trøndelag – med aksept fra Norsk kulturråd – å skyte inn udisponerte ABMU-midler i DIAS-prosjektet.

I DIAS-prosjektets statusrapport 01.10.2011til Norsk kulturråd ble det fortsatt lagt til grunn at prosjektarbeidet skulle sluttføres innen utgangen av 2011, men samtidig presisert at tidsplanen måtte regnes som usikker inntil avtale med leverandøren av forvaltnings-systemet var på plass. I den endelige leverandøravtalen ble imidlertid sluttdatoen for programutviklingen fastsatt til 01.04.2012. Styringsgruppen besluttet på denne bakgrunn å sette 01.04.2012 som sluttdato for DIAS-prosjektet i sin helhet. Riksarkivaren innhentet Norsk kulturråds samtykke til å overføre udisponerte prosjektmidler – inkludert overførte midler fra LLP og IKA Trøndelag – til budsjettåret 2012.

For å skape rom for nødvendige justeringer og en tilfredsstillende uttesting av systemet besluttet styringsgruppen 27.03.2012 å utsette prosjektets sluttdato til 31.05.2012.

2.4.2 Initielle prosjektmål

DIAS-prosjektets initielle mål ble definert i prosjektplanen av 15.10.2009. Oversikten nedenfor viser status for oppfyllelsen av målene i den opprinnelige planen.

Mål i opprinnelig prosjektplan	*Status for måloppfyllelse*
1) Prosjektet skal utprøve den logiske arkivpakkemodellen fra Arkivverkets Elmag-prosjekt, og definere en omforent modell for statlige og kommunale depoter.	En omforent OAIS-basert bevaringsstruktur for alle aktuelle typer av digitale avleveringer/deponeringer til statlige og kommunale arkivdepoter var ferdig som arbeidsgrunnlag for videre prosjektaktiviteter i juni 2010.
2) Det skal treffes valg av implementeringsstandarder for prosjektets arkivpakke-modell.	Følgende implementeringsstandarder er valgt: *METS* for spesifisering av arkivpakkestruktur, organisering og innholdsoversikt, *PREMIS* for spesifisering av bevaringsmetadata (håndteringshistorikk i arkiv-depot), *EAD* for arkivbeskrivelse, *EAC-CPF* for arkivskaper- og aktørbeskrivelse og *ADDML* for teknisk beskrivelse av tabelluttrekk.

Mål i opprinnelig prosjektplan	*Status for måloppfyllelse*
3) Prosjektet skal spesifisere XML-skjema(er) for arkiv-pakkestrukturen.	Prosjektet har ferdigspesifisert egne XML-skjemaer for tilpasningen av METS og PREMIS for DIAS (*DIAS-METS* og *DIAS-PREMIS*). XML-skjemaer for EAD, EAC-CPF og ADDML brukes i sin fullstendige form, uten spesielle tilpasninger for DIAS. Men prosjektet har spesifisert "mapping" mellom feltopplysningene i Asta og EAD/EAC-CPF.
4) Det skal utformes en krav-spesifikasjon til programvare for å generere arkivpakker iht. DIAS-modellen med tilhørende XML-skjemaer.	Prosjektet har gått lenger enn dette, og utarbeidet en kravspesifikasjon til et fullstendig forvaltnings-system for DIAS-baserte arkivpakker i digitalt depot (23.11.2010).

DIAS-prosjektets spesifikasjoner følger som vedlegg i rapportens del 2:
- vedlegg 3: xml-skjemaet DIAS-METS
- vedlegg 4: xml-skjemaet DIAS-PREMIS
- vedlegg 5: Mapping mellom Asta og EAD
- vedlegg 6: Mapping mellom Asta og EAC-CPF
- vedlegg 7: Kravspesifikasjon til forvaltningssystem for DIAS-arkivpakker.

Spesifikasjonene er også publisert på egen DIAS-nettside.[5]

2.4.3 Systemutviklingsprosjekt 2011-2012

Med utgangspunkt i prosjektets kravspesifikasjon til et forvaltningssystem for DIAS-arkivpakker (23.11.2010) besluttet styringsgruppen å utvikle et slikt system i prosjektets regi. Beslutningen om å utvide prosjektet med dette som mål ble støttet av konklusjonene i en bestilt konsulentrapport fra LDB-Centrum ved Luleå Universitet. Rapporten ble levert 01.02.2011, og ga holdepunkter om at utviklingsprosjektet ville være realiserbart for DIAS-prosjektet mht. omfang og kostnader. I oppdraget ble LDB-Centrum bedt om å vurdere eksisterende åpen kildekode-baserte forvaltningssystemer (Open Repository-systemer) i forhold til DIAS-kravspesifikasjonen. I tillegg til å bekrefte at prosjektets kravspesifikasjon var adekvat og implementerbar, ga konsulentrapporten en oversikt over aktuelle basissystemer som klargjorde at et forvaltningssystem for DIAS kunne utvikles ved å tilpasse et eksisterende OpenRepository-system.

Et viktig motiv for å inkludere utviklingen av et generelt DIAS-forvaltningssystem i prosjektet var at dette også ville realisere mål fra andre ABMU-støttede prosjekter for å utvikle digitale depotløsninger for kommunal sektor. Dette var bakgrunnen for at DIAS-prosjektet i 2011 ble tilført fortsatt udisponerte ABMU-prosjektmidler som tilleggs-ressurser for å gjennomføre utviklingsarbeidet. Landslaget for lokal- og privatarkiver (LLP) vedtok å overføre kr. 355.000 til DIAS fra OpenArms-prosjektet, og IKA Trøndelag overførte kr. 103.000 fra prosjektet Test av depotstyringssystemer. Sammen med et ekstra tilskudd fra Riksarkivaren på kr. 250.000 har disse ekstramidlene gjort det mulig for prosjektet å utvikle et fullstendig og fritt tilgjengelig forvaltningssystem for DIAS-baserte arkivpakker.

[5] http://www.arkivverket.no/standarder/dias (lest 17.02.1012)

Tilbudsinvitasjon på et forvaltningssystem til DIAS på grunnlag av prosjektets kravspesifikasjon ble kunngjort på Doffin og EU-databasen TED 18.04.2011 etter prosedyren "Konkurranse med forhandling etter forutgående kunngjøring" (anskaffelsesforskriften § 14.-3, ledd c). Ved tilbudsfristens utløp 26.05.2011 forelå tilbud fra to leverandører. Etter parallelle møter med de to tilbyderne ble det besluttet å føre avsluttende kontraktforhandlinger med ES Solutions AB om utviklingsarbeid basert på systemet ESSArch, som brukes av det svenske riksarkivet. Utviklingsavtale og avtale om vedlikehold og programservice – begge basert på Difis statlige standarder – ble undertegnet 21.11.2011 med Riksarkivaren som formell avtalepart for DIAS.

Arbeidet for å utvikle og implementere en versjon av ESSArch som et DIAS-tilpasset forvaltningssystem startet i november 2011. Implementeringen har skjedd i Riksarkivet som ledd i et eget DIAS-prosjekt ("ESSArch-prosjektet") med ansvar for tilpasning, testing og akseptanse av systemet. I ESSArch-prosjektet ble DIAS og Riksarkivets Elmag-prosjekt kombinert. Riksarkivets systeminnføring var samtidig DIAS-prosjektets pilotinstallasjon. Etter avsluttende akseptansetest ble systemet ferdigstilt for ordinær drift i Riksarkivet fra juni 2012, og samtidig klargjort som DIAS-prosjektets allment tilgjengelige produkt.

2.5 Kompetansebygging

Det er lagt vekt på å bygge opp egen kompetanse som ledd i DIAS-prosjektet. En viktig ledetråd har vært at prosjektet ikke kunne nøye seg med å få utviklet produkter for digitale depoter. Like viktig er det å bidra til å bygge opp kompetansen som kreves for å mestre produktene, og da spesielt med tanke på vedlikehold og videreutvikling av implementeringsstandardene METS og PREMIS og DIAS-forvaltningssystemet ESSArch.

Følgende tiltak er gjennomført som ledd i prosjektet egen kompetansebygging:
- Et seminar med Karin Bredenberg om METS og den svenske implementeringsmodellen ble arrangert i Riksarkivet 14.06.2010.
- Medlemmer av prosjektgruppen deltok 19.-23.09.2010 på iPRES-konferanse i Wien.
- Styringsgruppen foretok 19.-20.10.2010 en studiereise til Stockholm med seminarer i Stockholms stadsarkiv og det svenske riksarkivet.
- Kontaktseminar med det svenske riksarkivet ble arrangert i Oslo 24.-25.02.2011.

Ekstern kompetansebygging i de kommunale DIAS-miljøene har vært sterkt vektlagt gjennom organiseringen av ESSArch-prosjektet. Styringsgruppen har også planlagt en egen lanseringskonferanse for DIAS senere i 2012 med kommunenes administrasjonssjefer og arkivpersonale som de sentrale målgruppene.

2.6 Norsk-svensk samarbeid

Det svenske riksarkivet benytter en arkivstruktur med de samme implementeringsstandardene som DIAS. Det har gitt verdifull bistand til utviklingen av DIAS-prosjektets arkivpakkemodell og XML-skjemaer, og foretatt kvalitetssikringen av skjemaene DIAS-METS og DIAS-PREMIS v/Karin Bredenberg.

Det svenske riksarkivet leder et samarbeidsprosjekt med svensk kommunal sektor (ENSAM-prosjektet) for å spesifisere fellesløsninger for arkivpakkestruktur tilsvarende

DIAS. Når DIAS-prosjektet dessuten har valgt å bygge på det svenske riksarkivets forvaltningssystem ESSArch, åpnes perspektiver for et enda bredere samarbeid med det svenske arkivmiljøet.

2.7 Ressursbruk og prosjektregnskap

I søknaden til ABM-utvikling 15.10.2009 ble DIAS-partnernes egen ressursinnsats i et (opprinnelig planlagt) ettårig prosjektet stipulert til 3 årsverk. Riksarkivaren skulle etter planen skyte inn 2 årsverk. Hver av de fire kommunale deltakerne ble forventet å bidra med et kvart årsverk. Prosjektmidlene fra ABM-utvikling skulle dekke konsulentkostnader og reisevirksomhet, herunder studiereiser.

Prosjektpartnernes samlede egeninnsats i DIAS-prosjektet er beregnet til 4,7 årsverk. Gjennomførte prosjektmøter, herunder studiereisemøter og tilbudsforhandlinger, utgjør alene 2 ¼ årsverk – gitt at alle møter regnes som en full dag pr. deltaker**.** Av den totale arbeidsinnsatsen har Riksarkivaren bidratt med 3,1 årsverk, de kommunale partnerne med 1,6 årsverk samlet. Både den samlede arbeidsinnsatsen over to år og fordelingen på prosjektpartnerne er godt i tråd med anslagene i den opprinnelige planen for et ettårig prosjekt. I begge tilfeller har ressursinnsatsen økt med ca. 50 % i forhold til planen fra 2009.

Regnskap for DIAS-prosjektets disponering av tildelte budsjettmidler følger som vedlegg 2. Prosjektregnskapet viser at konsulentbistand utgjør i underkant av 60 % av utgiftene. I den opprinnelige prosjektplanen ble 85 % av utgiftene beregnet til konsulentbistand. I forhold til planen fra 2009 har det med andre ord skjedd en vridning fra konsulenttjenester til møtereiser og kompetanseutvikling. Utvidelsen av prosjektet i 2011 til også å omfatte programutvikling, skulle i utgangspunktet innebære en økt bruk av konsulenttjenester. Men både for å ivareta konsensus- og kompetansebygging ble også dette utviklingsprosjektet (ESSArch-prosjektet) organisert med intensive møter – og tilsvarende utgifter til møtereiser.

3. KRAV SOM STILLES TIL DIGITALE ARKIVDEPOTER

3.1 Utfordringene ved langtidsbevaring av digital arkivinformasjon

Langtidsbevaring av digitalt arkivmateriale representerer store utfordringer, og medfører en rekke risikofaktorer. Hovedutfordringene ved digital arkivering og bevaring gjelder:

1) *Lagringssikkerhet,* dvs. sikkerhet for at informasjon holdes digitalt intakt. De elektroniske lagringsmedienes korte levetid nødvendiggjør en jevnlig overkopiering (migrering) til nye databærere og verifisering av den tekniske integriteten. I lagringssikkerhet ligger også kravet om å ivareta konfidensialitet iht. fastsatte tilgangsbestemmelser.
2) *Opprettholdt lesbarhet,* dvs. at digitalt kodede data fortsatt er teknisk tolkbare for tilgjengelig maskin- og programutrustning, og lar seg fremstille som meningsfylt informasjon – på tross av IT-utviklingens hyppige teknologiskifter, som typisk medfører at nye utstyrsgenerasjoner ikke kan fremstille informasjon fra eldre.
3) *Opprettholdt integritet*, dvs. at informasjonsinnholdet er bevart uendret.
4) *Opprettholdt autentisitet*, dvs. at informasjonsinnholdet bringer med seg de opplysninger om sin identitet, opphavs- og brukssammenheng som kreves for at det skal være forståelig qua arkivmateriale, og at det dessuten lar seg bekrefte at informasjonen er bevart med opprettholdt integritet – og dermed er hva den utgir seg for å være.

DIAS behandler ikke lagringsløsninger, men ivaretar funksjoner uavhengig av lagringsopplegg og medievalg. Det er likevel grunn til å understreke at lagring på disk innebærer nye former for sårbarhet og nye utfordringer mht. lagringssikkerhet. Behovet for eksterne sikkerhetskopier ble sterkt aktualisert ved terroraksjonen mot Regjeringskvartalet 22.07.2011.

Utviklingen internasjonalt har medført en mye sterkere vektlegging av kravene til arkivinformasjonens pålitelighet. Dette krever mekanismer for en ubrutt autentisitets- og integritetssikring gjennom alle livsfaser fra saksbehandling til langtidslagring i arkivdepot.

3.1.1 Spesielle utfordringer knyttet til integritetssikring

Digitalt arkivmateriale må være bevart med et uendret logisk informasjonsinnhold. Sjekksummer kan brukes for å bekrefte at digital informasjon er lagret fysisk uendret, men digital bevaring uten *fysiske* endringer er umulig. Digitale arkiver kan ikke bevares statiske. For å opprettholde lesbarheten må de være i en prosess med transformasjon gjennom hele livssyklusen – til fundamental forskjell fra papirarkiver.

Det eksisterer ingen enkel metode tilsvarende sjekksummer for å bekrefte et uendret *logisk* innhold. Hvordan kan vi da stole på at arkivmateriale som et arkivdepot har omskapt, fortsatt er autentisk? Hvordan garderer vi oss når det settes søkelys på hva et arkivdepot har hatt *mulighet* for å endre? På hvilke måter lar det seg bekrefte at arkivdepotet har nøyd seg med å foreta tekniske endringer som sies å være utført som ledd i et nødvendig vedlikehold?

OAIS-standarden definerer et rammeverk for arkivbevaring som også omfatter integritetssikring av logisk informasjonsinnhold. Løsningene konkretiseres i standarden TRAC. For arkivdepoter medfører TRAC-løsningene nitide og arbeidskrevende rutiner – for nettopp å kompensere for mangelen på enkle metoder for integritetssikring "fra naturens hånd".

3.2 Krav i foreliggende standarder

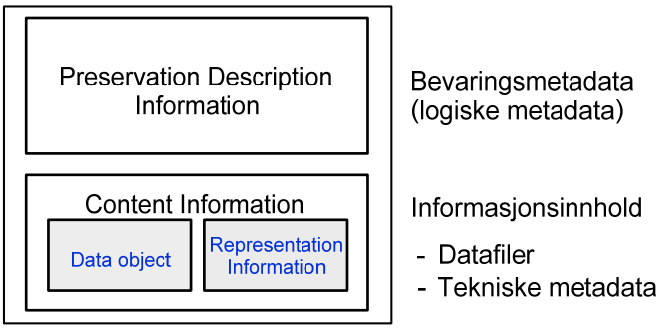
3.2.1 OAIS-standarden

Prinsippene, terminologien og de funksjonelle beskrivelsene i arkivstandarden OAIS – *Reference Model for an Open Archival Information System*[6] (ISO 14721: 2003) ligger til grunn for nær all digital arkivbevaring, eller hevdes å gjøre det. OAIS er en modell for å innlemme, administrere og bruke bevart arkivmateriale i et arkivdepot. Den beskriver et depots funksjoner, prosesser og informasjonsflyt med fokus på integritetssikring, og definerer opplegg for vedlikehold innenfor et kontrollert miljø. OAIS-modellen beskriver bevaringsobjekter med vekt både på deres konseptuelle og tekniske aspekter.

Hvert bevaringsobjekt skal iht. OAIS lagres som en autonom og selvdokumenterende *arkivpakke,* fast forbundet med alle tilhørende logiske og tekniske metadata. Slik skal bevaringsobjektet fortsatt kunne fremstilles, og slik skal det fortsatt være forståelig og autentisk som arkivmateriale.

Et bevaringsobjektet i OAIS kan være et enkelt dokument eller et samlet datauttrekk fra en database. OAIS skiller mellom tre typer av arkivpakker: *Submission Information Package* (SIP) for objektet som depotet mottar som aksesjon, *Archival Information Package* (AIP) for versjonen som innlemmes for bevaring i arkivdepotet, og *Dissemination Information Package* (DIP) for en AIP (eller flere) som gjøres tilgjengelig i bruksversjon. Når et arkivdepot genererer en ny AIP, krever OAIS at den mottatte SIP-versjonen bevares i tillegg. Den skal bevares uendret og integritetssikret – for alltid – for å muliggjøre en ettersporing av depotets operasjoner.

En OAIS-arkivpakke har to grunnelementer: 1) informasjonsinnhold *(Content Information)* med datafiler og tekniske metadata (Representation Information), og 2) bevaringsbeskrivende metadata *(Preservation Description Information)* med underkategorier for logisk arkivbeskrivelse, kontekst, bevaringshistorikk i depot og integritetssikring. Denne modellen bestående av bevaringsobjektets data, tekniske metadata for å fremstille dem og "logiske" metadata for å forstå dem som arkivmateriale, er illustrert i figuren til høyre.



OAIS er en referanse- og begrepsmodell med metadata-kategorier, men ikke en implementeringsmodell med konkrete forslag til metadata. Slike metadata og annen tilleggsfunksjonalitet er imidlertid spesifisert i ulike oppfølgingsstandarder til OAIS, blant annet for å

[6] http://public.ccsds.org/publications/archive/650x0b1.pdf (lest 17.02.2012)

beskrive arkivpakkestruktur (METS) og bevaringsmetadata (PREMIS). TRAC, som følger opp anvisningene i OAIS om integritets- og autentisitetssikring mm., behandles nedenfor.

3.2.2 TRAC-standarden

TRAC – *Trustworthy Repository Audit and Certification - Criteria and Checklist*[7] – formulerer 90 kriterier som et arkivdepot må oppfylle for å oppnå status som pålitelig og tiltrodd. Rapporten ble utarbeidet av USAs riksarkiv og organisasjonen for forskningsbiblioteker (RLG) i 2007 som grunnlag for et sertifiseringsopplegg for digitale depoter. En ISO-standard basert på TRAC er nært forestående: ISO/DIS 16363 (CCSDS 652-R-1) – *Trusted Digital Repositories (TDR) Checklist*[8].

For å oppnå en sertifisering etter kravene i TRAC må et digitalt depot være gjenstand for innsyn og evaluering. Det må selv aktivt kunne dokumentere og demonstrere sin evne til å oppfylle kravene, herunder krav som TRAC stiller til styringsforpliktelser og ansvarlighet, langsiktighet og organisatorisk levedyktighet, økonomi og finansiell bærekraft. En egen ISO-standard med krav til sertifiserende instanser er under utvikling.[9]

TRAC konkretiserer og videreutvikler OAIS-kravene til integritetssikring. I sin administrasjon av digitale objekter må et depot kunne demonstrere at bevart informasjonsinnhold fortsatt samsvarer med opprinnelig mottatt innhold. Depotoperasjoner som resulterer i transformerte arkivpakker, må følgelig være ettersporbare. Opprinnelige arkivpakker må bevares, og det må finnes forbindelser mellom disse og senere transformerte versjoner.

Et viktig bakteppe for TRAC-standarden var O. J. Simpson-saken i USA i 1995, hvor retten underkjente Simpsons fingeravtrykk som bevis. Det var nok å påvise at behandlingsrutinene kunne gitt politiet *mulighet* for manipulasjon. Normen blir at den som skaper eller forvalter informasjonen, selv må bekrefte dens autentisitet. For arkivdepoter innebærer dette en omsnudd bevisbyrde. Iht. TRAC må de selv kunne produsere verifiserende dokumentasjon for å eliminere grunnlaget for tvil eller spekulasjon om arkivbestandens integritet, dvs. om feil, uautoriserte endringer og andre uforsvarlige operasjoner som er mulige i et arkivdepot. For å etterleve TRAC kreves et forebyggende vedlikeholdsarbeid med kontinuerlig beskyttelse mot uautoriserte hendelser, fulldokumenterte rutiner med loggføring av depotoperasjoner og sporing av endringer for å muliggjøre tilbakespoling til tidligere versjoner.

Ved å etterleve TRAC vil et arkivdepot kunne bekrefte at informasjonsinnhold er bevart uendret fra og med mottak. Dette er avgjørende for et arkivdepots pålitelighet og troverdighet. Det gir ingen garanti for at innholdet er autentisk i seg selv, men for arkivdepotets renommé har dette ikke samme fatale betydning[10].

---

[7] TRAC (*Trustworthy Repository Audit and Certification – Criteria and Checklist)* er utarbeidet av RLG – Research Libraries Group og NARA – National Archives and Records Administration.
Ref.: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf (lest 17.02.1012).

[8] ISO/DIS 16363: Sluttutkast er utarbeidet av den amerikanske romfartsorganisasjonen CCSDS (sept. 2011).
Ref.: http://public.ccsds.org/publications/archive/652x0m1.pdf (lest 17.02.2012)

[9] *Requirements for Bodies providing Audit and Certification*.
Ref.: http://public.ccsds.org/publications/archive/652x1m1.pdf (lest 17.02.2012).

[10] TRAC (og OAIS-modellen) har imidlertid funksjonalitet for å dokumentere om, og eventuelt hvordan arkivmateriale er blitt integritets- og autentisitetssikret forut for en aksesjon, både i det opprinnelige produksjonssystemet og gjennom prosessen med fremstilling av en arkivversjon (SIP) for avlevering.

3.2.3 "Core Principles" – Ti basiskrav til et digitalt arkivdepot

Standardopplegg for en sertifisering av arkivdepoter med utgangspunkt i TRAC er under utarbeidelse, men har ikke fått sin endelige form. Det har vært litt ulike oppfatninger blant bevaringsorganisasjoner internasjonalt om kriteriene for et sertifiseringsopplegg bør være så ambisiøse og finmaskede som i TRAC. Fire sentrale bevaringsorganisasjoner – The Digital Curation Center (U.K), DigitalPreservationEurope (EU), NESTOR (Tyskland) og Center for Research Libraries (USA) – ble i 2007 enige om å formulere 10 basiskrav til et digitalt arkivdepot. Kravene var imidlertid generelle, og ikke konkrete sertifiserings-kriterier.

I følge disse *Ten Core Principles of Trust Repository Design*[11] må et arkivdepot være i stand til å oppfylle følgende krav:

1) være forpliktet til et kontinuerlig vedlikehold av digitale objekter for sine definerte oppdragsgivere og brukermiljøer,
2) kunne vise og bekrefte at det er organisatorisk skikket til å oppfylle sine forpliktelser, også økonomisk, bemanningsmessig og praktisk,
3) kunne påta seg kontraktbaserte og juridiske rettigheter, og ivareta ansvaret for dem,
4) ha et effektivt og smidig policy-rammeverk,
5) anskaffe og overføre digitale objekter iht. bekjentgjorte kriterier som avspeiler depotets forpliktelser
6) opprettholde og sikre de bevarte digitale objektenes integritet, autentisitet og anvendelighet over tid,
7) skape og vedlikeholde nødvendige metadata om operasjoner som er foretatt på digitale objekter under bevaring – i tillegg til [metadata om] relevant produksjons-, tilgangs- og brukskontekst forut for bevaring,
8) oppfylle nødvendige krav til tilgjengeliggjøring,
9) ha et strategisk program for planleggingen og utførelsen av forvaltningsoppgavene knyttet til bevaring og vedlikehold,
10) ha en adekvat tekniske infrastruktur for å ivareta sikkerheten og det kontinuerlige vedlikeholdet av de bevarte digitale objektene.

3.3 DIAS i relasjon til OAIS og TRAC

DIAS-prosjektet har spesifisert en arkivpakke- og prosessmodell som en definert bruks-måte av OAIS. Det har valgt tilgjengelige implementeringsstandarder for å realisere modellen. DIAS-modellen angir hvordan eksisterende standarder skal anvendes i en arkivpakke. DIAS-strukturen kan dermed betegnes som en standard for bruk av standarder.

Det som mest av alt karakteriserer DIAS-strukturen og prosessmodellen, er dens fokus på integritetssikring og oppfølging av kravene i TRAC – Trustworthy Repository Audit and Certification.

DIAS-spesifikasjonene og DIAS-forvaltningssystemet begrenser seg om å følge opp kravene i TRAC som omfatter organiseringen av arkivobjekter og behandlingsprosessene i tilknytning til dem (TRAC, del B: Administrasjon av digitale objekter). Prosjektet har ikke

[11] *Ten Core Principles*: http://www.digitalpreservationeurope.eu/platter.pdf (lest 18.02.2012).

gått videre inn på TRAC-kravene til arkivdepoters styringsforpliktelser, organisatoriske levedyktighet og finansielle soliditet (TRAC, del A). Men disse kravene er viktige. Det er derfor også viktig å understreke at løsningene i DIAS er innrettet innenfor de rammekrav til organisasjon og infrastruktur som defineres TRAC.

4. DIAS-PROSJEKTETS RESULTATER OG PRODUKTER

4.1 DIAS arkivpakker – Overordnet organisering

DIAS spesifiserer en OAIS-struktur ved å benytte følgende implementeringsstandarder:

- METS[12] for å beskrive en arkivpakkes indre struktur og beholderen som omslutter den
- PREMIS[13] for bevaringsmetadata og annen forståelsesinformasjon
- EAD[14] for (logisk) arkivbeskrivelse
- EAC-CPF[15] for aktørbeskrivelse
- ADDML[16] for tekniske metadata (fil- og postbeskrivelse for tabelluttrekk).

DIAS-arkivpakker skal inneholde metadata-filer basert på disse standardene samt deres respektive xml-skjemaer. For METS og PREMIS har prosjektet spesifisert tilpassede versjoner av skjemaene – kalt DIAS-METS[17] og DIAS-PREMIS[18] – for anvendelses-måtene som beskrives nedenfor i dette kapittel 4. For de tre øvrige standardene brukes xml-skjemaer slik de foreligger publisert for hver av disse standardene.

DIAS-modellen omfatter følgende typer av informasjonspakker – hver med ”flagg” for pakketype:

- SIP *(Submission Information Package)*: en overføringspakke (leveringspakke) med informasjonsinnhold og metadata.
- AIP *(Archival Information Package)*: en ordinær arkivpakke (bevaringspakke) i arkivdepot med informasjonsinnhold og metadata.
- AIC *(Archival Information Collection)*: en overordnet ”samlepakke” i arkivdepot som er tilknyttet flere underordnede AIP-er (i DIAS: flere ”generasjoner” av samme AIP). En AIC inneholder bare metadata. Tilknyttede AIP-er utgjør dens informasjonsinnhold.
- AIU *(Archival Information Unit)*: En forenklet tilleggspakke til en AIP som bare inneholder metadata.
- DIP *(Dissemination Information Package)*: En arkivpakke i visnings- og bruksversjon.

---

[12] METS (*Metadata Encoding & Transmission Standard.)*. Spesifisert av Digital Library Federation, og vedlikeholdes av Library of Congress. Ref.: http://www.loc.gov/standards/mets/ (lest 17.02.2012).

[13] PREMIS (*Preservation Metadata: Implementation Strategies*). Utviklet av Online Computer Library Center (OCLC) og Research Libraries Group (RLG), og vedlikeholdes av Library of Congress. Ref.: http://www.loc.gov/standards/premis/ (lest 17.02.1012).

[14] EAD (*Encoded Archival Description).* Vedlikeholdes av Library of Congress i samarbeid med The Society of American Archivists. Ref.: http://www.loc.gov/ead/. (lest 19.02.2012).

[15] EAC-CPF (*Encoded Archival Context – Corporate bodies, Persons, and Families).* Ref.: http://eac.staatsbibliothek-berlin.de/schema/cpf.xsd (lest: 20.02.2012).

[16] ADDML *(Archival Data Description Markup Language).* Utviklet og vedlikeholdes av Riksarkivet. Ref.: http://www.arkivverket.no/arkivverket/Arkivbevaring/Elektronisk-arkivmateriale/Standarder/ADDML (lest 20.02.2012)

[17] http://www.arkivverket.no/standarder/METS (lest 21.02.2012)

[18] http://www.arkivverket.no/standarder/PREMIS (lest 22.02.2012)

De ulike typene av DIAS-arkivpakker skal bygge på følgende xml-skjemaer:

- *En AIP* skal ha filer basert på skjemaer for DIAS-METS, DIAS-PREMIS, EAD og EAC-CPF, dessuten for ADDML så sant ADDML er relevant for informasjonsinnholdet.
- *En AIC* skal bygge på samtlige skjemaer unntatt ADDML.
- *En AIU* skal bygge på skjemaer for DIAS-METS, DIAS-PREMIS og de andre metadatakategorier som inngår i AIU-en.
- For å følge DIAS må *en SIP* bygge på DIAS-METS, DIAS-PREMIS og ADDML (når ADDML er relevant). EAD og EAC-CPF kreves ikke, men arkivskaperen må likevel kunne registrere arkiv- og aktørbeskrivelse som en del av SIP. Statlige og kommunale avleveringsbestemmelser krever pr. dato ikke at en SIP skal følge DIAS.

Følgende regler gjelder for organisering og bruk av DIAS arkivpakker:

1. Alle filer i en arkivpakke tilknyttes sjekksummer. Samlet pakkesjekksum lagres utenfor pakken.
2. Ved innlemmelse i digitalt depot skal en AIP (og en eventuelt lagret DIP) alltid være tilknyttet en overordnet AIC. Tilknytningen skal skje ved bruk av en peker fra AIC (structMap i AIC), ikke ved innbygging av arkivpakken i AIC.
3. En AIC skal kunne ha tilknyttet flere generasjoner (versjoner) av samme AIP, og ha et ”flagg” som viser hvilken AIP-generasjon som er gjeldende, aktiv versjon.
4. En AIU kan brukes som tillegg til en AIP. Den skal da være knyttet til AIP-ens overordnede AIC – og bare til denne. Dens relasjon til en AIP skal vises av AIC-en.
5. En AIU skal få status som inaktiv når vedkommende AIP blir inaktiv. Flere generasjoner av en AIU skal kunne referere til samme aktive AIP, men en ny generasjon skal gjøre den foregående inaktiv.
6. Innholdet i en AIC skal kunne oppdateres – i motsetning til en AIP og en AIU, hvor endring krever at det genereres en ny generasjon (eventuelt en AIU som tillegg til en AIP når endringer bare omfatter metadata i pakken).
7. En tilrettelagt bruksversjon av en arkivpakke (DIP) skal kunne knyttes til en AIC på samme måte som en AIP og AIU.
8. Hver AIP, AIU og (eventuelt) DIP pakkes som en samlet tar-fil. Samlet pakkesjekksum skal være av tar-filen, og lagres i overordnet AIC. En SIP pakkes også som tar.
9. En AIC skal *ikke* pakkes som tar, men den skal være organisert som en METS-fil, og eventuelle andre xml-skjemaer skal være innbakt i METS. Samlet pakkesjekksum for AIC skal være av METS-filen.

4.2 DIAS-pakkemodellen som en prosessmodell

Ved å angi hvordan eksisterende standarder skal anvendes i en arkivpakke kan DIAS betegnes som en standard for bruk av standarder. Men DIAS-modellen for arkivpakker er i tillegg utformet som en prosessmodell, – en prosessmodell for integritetssikring.

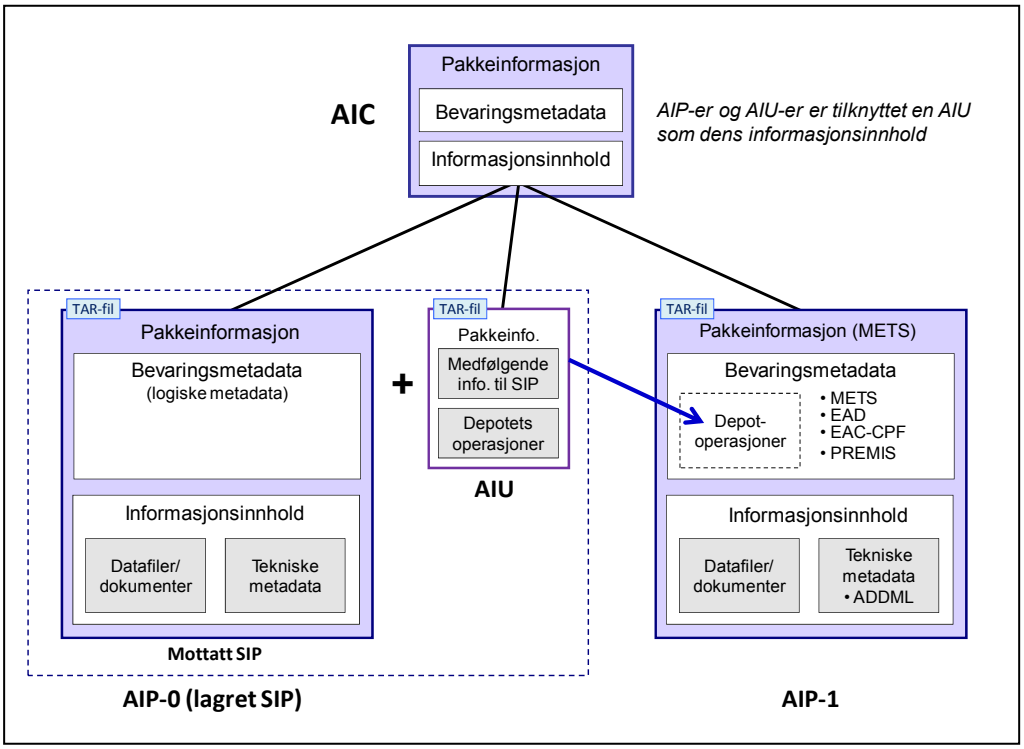
Sjekksummer kan brukes til å bekrefte at digital informasjon er lagret fysisk uendret, men digital bevaring uten endringer på fysisk representasjonsnivå er ikke mulig. Sjekksummer kan ikke verifisere et uendret logisk informasjonsinnhold etter en fysisk transformasjon av

informasjon, og det hjelper da lite om endringen er begrenset til en teknisk omformatering som ledd i et nødvendig vedlikehold for å opprettholde lesbarheten. DIAS løser integritets-problematikken ved å bygge på resepten fra TRAC: Alle operasjoner i et arkivdepot skal dokumenteres som tillegg – uten å endre eksisterende informasjon fysisk. Sjekksummer kan da brukes på alle filer, og tjene som mekanismer for verifisering. Ubrutt integritet kan bekreftes ved kontroll mot eldre versjoner og dokumentasjon av utførte depotoperasjoner.

For å ivareta en uavbrutt integritetssikring slik at den også blir verifiserbar, er prosess-modellen i tilknytning til arkivpakkemodellen i DIAS spesifisert på følgende måte:

- En SIP skal bevares uendret slik den ble mottatt – for alltid. Den skal innlemmes samlet og sjekksumsikret i digitalt depot som generasjon 0 av en arkivpakke (AIP-0).
- Operasjoner i depot fra og med mottak av SIP – herunder sjekksumgenerering av SIP, kontroll av eventuell medfølgende SIP-sjekksum og depotets testing av SIP-innhold – dokumenteres utenfor AIP-0 sammen med SIP-ens medfølgende info-fil. Denne tilleggsinformasjonen lagres enten i en AIU tilknyttet AIP-0 (via overordnet AIC), eller i en ny generasjon av den fullstendige arkivpakken: AIP-1. AIP-1 bevares da i tillegg til AIP-0.
- Ved senere konverteringer/transformeringer bevares en ny generasjon av vedkommende AIP som nytt tillegg. En ny AIP skal genereres ved enhver endring (omformatering) av informasjonsinnhold. Eventuelle AIU-er til foregående generasjon innarbeides.

Denne DIAS-prosessmodellen er illustrert i figuren nedenfor.



Figuren viser alternativet hvor en mottatt SIP ble lagret som AIP-0 uten samtidig generering av en DIAS-organisert AIP-1. I dette tilfellet kreves en AIU i tillegg for å unngå noen form for endring av AIP-0 og dens samlede pakkesjekksum. Ved en senere generering av AIP-1 inn-arbeides AIU i denne. Behovet for en AIU bortfaller når AIP-0 og AIP-1 genereres samtidig. Når/hvis metadata senere endres for AIP-1, kan de på tilsvarende måte lagres i en tilknyttet AIU – og da for å bevare AIP-1 uendret, og unngå eller utsette generering av en full AIP-2.

Et arkivdepot som langtidsbevarer materiale på CD-er, vil med utgangspunkt i denne modellen også kunne praktisere en enkel løsning hvor CD-er med en mottatt SIP innlemmes uendret som AIP-0, og tilhørende AIU-informasjon bevares på en tilleggs-CD.

4.3 Implementeringsstandarder og xml-skjemaer

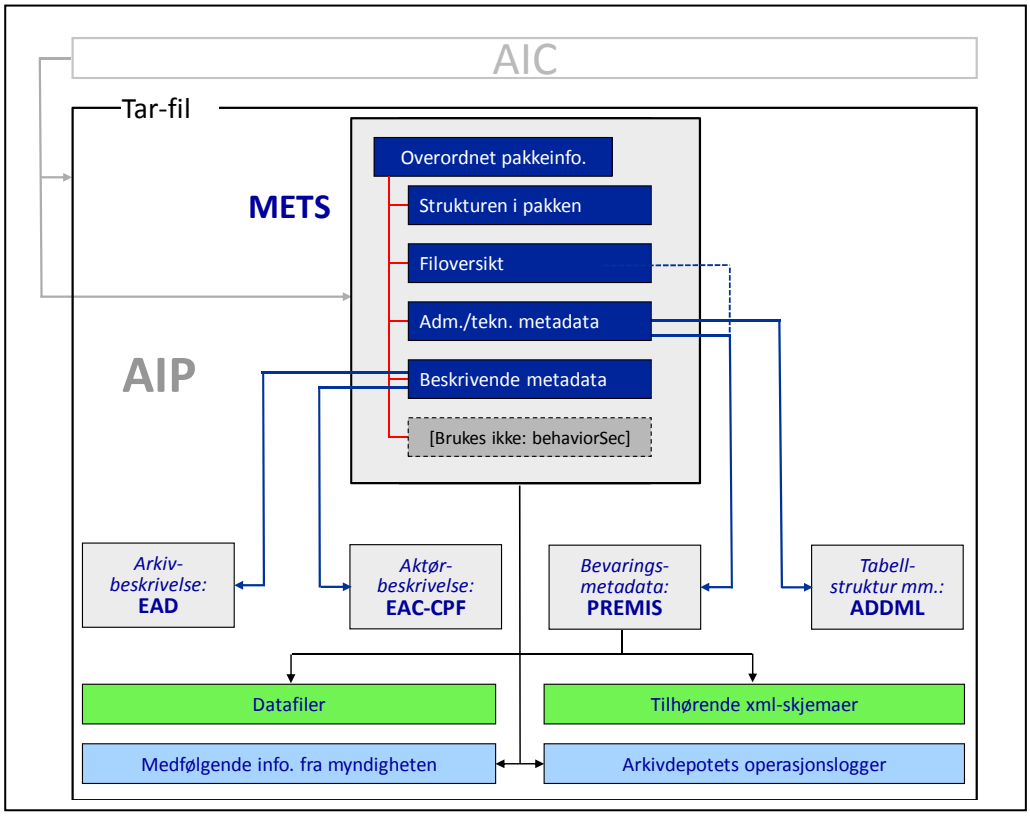
Arkivpakker genereres ved hjelp av xml-skjemaene som er utviklet for hver av implementeringsstandardene i DIAS. Pakkegenereringen utføres av DIAS-forvaltningssystemet. For arkiv- og aktørbeskrivelser foreligger også hjelpemidler for å generere xml-filer (iht. EAD og EAC-CPF) før en SIP hentes inn for behandling av forvaltningssystemet, jf. punkt 4.3.5.

4.3.1 Implementeringsmodell

METS definerer det ytre laget (”containeren”) og strukturen i DIAS-baserte arkivpakker. I en DIAS-arkivpakke skal xml-skjemaene for *DIAS-PREMIS, EAD, EAC-CPF og ADDML* være underordnet METS-skjemaet som delskjemaer.

PREMIS, som omfatter bevaringsmetadata, kan benytte sin egen container, men i DIAS-modellen innordnes PREMIS ved å tilknyttes samlet til METS (nærmere bestemt til admSec/digiprovMD i METS). Som i den svenske modellen skal alle de øvrige metadata-kategoriene være tilknyttet METS som ”plug-ins”, enten ved innkapsling i METS eller som utenforliggende objekter som METS refererer til.

Figur: Organisering av implementeringsstandarder i DIAS arkivpakke (AIP)



En AIP i DIAS bruker de samme implementeringsstandardene som det svenske riksarkivet (SRA). Forskjellen er at SRA ikke benytter AIC-er og AIU-er i tillegg – foreløpig. Organiseringen av pakken defineres i METS. I dette eksemplet er metadatafilene plassert utenfor METS, med METS-referanser til objektene. Dette vil være en bruksmåte for arkivpakker med større metadata-filer.

Det foreligger få alternativer til de implementeringsstandarder som er valgt av DIAS, om noen. Prosjektets initielle valg var om det skulle bruke eksisterende standarder eller skreddersy løsninger med egendefinerte xml-skjemaer for DIAS. Ulempen med standardene som foreligger, er at de er omfattende og forholdsvis kompetansekrevende. Med unntak for ADDML har standardene utspring i bibliotekverdenen – med sikte på et bredt anvendelsesområde, men dermed også med en rekke elementer uten relevans for DIAS.

Et arbeid for å utvikle helt egendefinerte DIAS-standarder ville heller ikke vært fritt for omkostninger, men fremfor alt ville slike løsninger vært krevende å vedlikeholde. Det avgjørende argumentet for å bygge på standarder som METS og PREMIS i DIAS er at de tilrettelegger for et videre vedlikehold av DIAS-strukturen. For hver av standardene er det etablert regimer for vedlikehold basert på brukererfaring. Konvensjoner er også under etablering for arkivdepoters anvendelse av standardene, og på det punktet har spesielt det svenske riksarkivet ytet viktige bidrag. Med de valg som prosjektet har gjort, kan vedlikehold og videreutvikling av DIAS-spesifikasjonene bygge på internasjonalt standardiseringsarbeid, og trekke på andre miljøer som bruker standardene.

Etter svensk mønster er det imidlertid lagt vekt på å gjøre implementeringen av standarder enklest mulig, bl.a. ved å knytte PREMIS samlet til METS.

4.3.2 Bruk av METS

I tillegg til å beskrive den indre strukturen i en arkivpakke-container knytter METS sammen metadata og informasjonsinnhold i pakken. Tilpasningen av METS for DIAS er spesifisert i skjemaet DIAS-METS, jf. rapportens del 2, vedlegg 3.[19]

Følgende øvrige valg er truffet om bruken av METS i DIAS:

1) Som container-filformat velges tar-format[20].

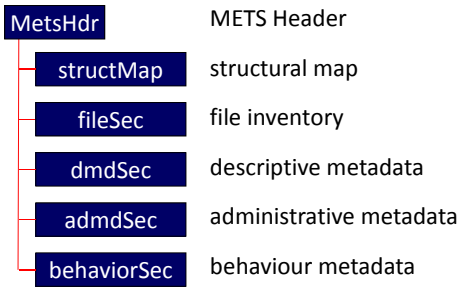
2) I en AIP og en AIU skal de ulike kategoriene av metadata innbygges i METS *eller* refereres fra METS. I en AIC skal metadatakategoriene alltid innbygges i METS.

3) Alternativet med å konvertere alle binærfiler (ikke-XML-filer) til Base64 velges ikke.

4) Følgende roller brukes i METS:

SUBMITTER	Ansvarlig organ for overføring
PRESERVATION	Depot
PRODUCER	Teknisk uttrekksprodusent (leverandør)
IPOWNER	Eier/rettighetshaver av materialet
CREATOR	METS-produsent (teknisk)
ARCHIVIST	Opprinnelig arkivskaper

Figur: Seksjoner i METS



Seksjonene File Section (fileSec), Descriptive Metadata (dmdSec) og Administrative Metadata (amdSec) i METS speiler logiske kategorier i OAIS: henholdsvis Content/ Packaging Information, Descriptive Information og Preservation Description Information.

[19] Tilgjengelig også på nettadressen: http://www.arkivverket.no/standarder/METS (lest 21.02.2012)

[20] tar – *tape archive format*. Utbredt format for å innpakke filer i en samlefil (tar-fil)

DIAS har også valgt denne METS-strukturen som grunnlag for definisjonen av fysisk fil-struktur i en AIP. Xml-filer og tilhørende skjemaer (xsd-malfiler) som definerer struktur og innhold, grupperes av praktiske grunner sammen. Med Noark-5-filer som eksempel [N-5] er denne filstrukturen slik:

tar-fil
- dias-mets.xml
- dias-mets.xsd
- descriptive_metadata/
  - ead.xml
  - ead.xsd
  - eac-cpf.xml
  - eac-cpf.xsd
- administrative_metadata/
  - dias-premis.xml
  - dias-premis.xsd
  - arkivuttrekk.xml [N-5]
  - addml.xsd [N-5]
  - repository_operations/
    - testrapport.pdf
    - logg.pdf
    - testnotat.pdf
    - ...
- content/
  - arkivstruktur.xml [N-5]
  - arkivstruktur.xsd [N-5]
  - endringslogg.xml [N-5]
  - loepende_journal.xml [N-5]
  - offentlig_journal.xml [N-5]
  - metadatakatalog.xsd [N-5]
  - ...
  - systemhåndbok.pdf
  - documents/
    - dokument1
    - dokument2
    - ...

DIAS-METS skal ha et logisk kart (structMap) på toppnivået med referanse til innhold (Content) og innholdets plassering i fysiske filer (Content). Følgende struktur for dette formålet er fastsatt i structMap – på AIP-nivå:

structMap
- contentInformation
  - contentDataObject
    - dokument1
    - dokument2
    - ...
    - arkivstruktur.xml [N-5]
    - endringslogg.xml [N-5]
    - loepende_journal.xml [N-5]

offentligJournal.xml [N-5]
...
systemHaandbok

representationInformation
arkivstruktur.xsd [N-5]
metadatakatalog. xsd [N-5]
...

I structMap definerer METS bare Content-filer. Metadatafiler skal ligge i amdSec. Dette gjelder også filer som omfatter depotoperasjoner. Med Noark-5 som eksempel vil amdSec typisk omfatte følgende skjemafiler og filer fra depotoperasjoner:

arkivuttrekk.xml [N-5]
premis.xml
testrapport.pdf
endringslogg.xml
andre filer fra depotoperasjoner

4.3.3 Bruk av PREMIS

PREMIS implementerer kategorien bevaringsmetadata (Preservation Description Information) i OAIS-modellen, og definerer metadata for å støtte forståelighet, autentisitet og identitet. PREMIS omfatter ikke logisk arkivbeskrivelse (”descriptive” metadata), heller ikke tekniske metadata. PREMIS spesifiserer operasjoner gjennom arkivobjektets livssyklus, og bare PREMIS har godt utbygde funksjoner for å dokumentere operasjoner og hendelser som utføres i et arkivdepot. Proveniens i PREMIS er primært håndterings- og bevaringshistorikken i depot. Tilpasningen av PREMIS for DIAS er spesifisert i skjemaet DIAS-PREMIS, jf. rapportens del 2, vedlegg 4.[21]

PREMIS har 5 hovedkategorier av metadata som er innbyrdes relatert:

Intellectual Entity – det logiske bevaringsobjektet, f.eks. en bok eller database,
Object – fysisk bevaringsobjekt (undergrupper er *file, bitstream* og *representation*),
Events – hendelser/operasjoner som *Object* er gjenstand for,
Rights – fastsatte bestemmelser om depotets rettigheter i forhold til *Object,*
Agents – organisasjoner, personer eller programvare tilknyttet *Events* eller *Rights.*

Events har knytning til de *Objects* og *Agents* som de enkelte hendelser berører.

I DIAS hører ulike typer logiske *Events* hjemme både i lagringssystemet (typisk medie-migrering og verifisering), i forvaltningssystemet (typisk virussjekk og flytting av objekter mellom kontrollområder) og i arkivpakker, – i det siste tilfellet både på AIP-, AIC- og AIU-nivå. Events på AIP- og AIU-nivå skal ha knytning til filer i disse pakkene. Events på AIC-nivå skal være relatert til hele AIP-er og AIU-er. Den viktigste typen av Events på AIP-nivå er dokumentasjon av operasjoner som medfører en transformering av innhold i forhold til foregående AIP-generasjon.

Følgende valg er truffet om bruken av PREMIS i DIAS *(PREMIS-betegnelser er kursivert)*:

[21] Skjemaet finnes også på nettadressen: http://www.arkivverket.no/standarder/PREMIS (lest 22.02.2012).

1) *Events* i PREMIS på AIP-nivå skal omfatte filer som er endret eller tilføyd i forhold til foregående AIP. Tilknyttede typer av events *(eventType)* blir *migrering* og *verifisering/ validering* etter formatkonvertering og utført sjekksum-verifisering.

2) *Events* i PREMIS på AIC-nivå skal omfatte innlemmelse av AIP-er og AIU-er i depot – og bare dette.

3) Samtlige hendelser i depot som registreres f.o.m. mottak av en SIP, skal i AIP bevares i en samlet event-logg utenfor PREMIS. Også alle *Events* i PREMIS skal inngå (repeteres) i denne samlede loggen kalt Depotoperasjoner. Med en mer detaljert operasjonslogg utenfor PREMIS unngår man å definere alle hendelser som elementer i PREMIS. Det legges til grunn at den samlede event-loggen Depotoperasjoner kan produseres av DIAS-forvaltningssystemet (ESSArch).

4) "Depotoperasjoner" som egen event-logg for endringer brukes ikke i en AIC. Uthenting av en AIC fra depot logges utelukkende i DIAS-forvaltningssystemet (ESSArch).

5) Opplysninger om "user rights" og generelle tilgangsbestemmelser skal ligge i EAD. *Rights* i PREMIS skal begrenses til arkivdepotets rettigheter i forhold til objektet.

6) *Rights* i AIP skal brukes for å definere rettigheter på objektnivå (filnivå). På overordnet AIC-nivå brukes bare EAD. Rights skal være av typen *Statute.* Her skal de samme 4 elementene som i EAD kunne angis: Klausulkategori (type restriksjon), Hjemmel, Varighet (År) og Flagg (om restriksjonen gjelder hele pakken eller ikke).

7) Flagg som viser at graderte opplysninger, sensitive personopplysninger eller andre taushetsbelagte opplysninger forekommer i en arkivpakke, må finnes på AIC-nivå (i EAD) og i forvaltningssystemet. Asta forutsettes å ha tilsvarende flagg og eventuelt mer detaljerte opplysninger.

8) Ved uthenting av arkivpakker fra depot skal PREMIS knytte rettigheter til definerte formål med uthentingen. PREMIS skal ha en verdiliste over slike formål. Uthenting av en AIP med flagg = Deponert (på AIC-nivå) skal eksempelvis muliggjøre vedlikehold, men ikke generering av en DIP.

9) I en AIC skal samlede AIP- og AIU-sjekksummer lagres i PREMIS.

I en AIP (alternativt en SIP) kan PREMIS *Object* være av typen *File* og dessuten av typen *Representation* (for et sett av dokumentfiler).

I en AIU skal relasjoner beskrives på samme måte som for en AIP. For øvrig vil det ikke være elementer som inngår i PREMIS-filen.

I en DIP skal *Relationships* og *Rights* brukes som i AIP. *Events* brukes for å dokumentere DIP-ens opprinnelseshistorie og konstruksjon.

4.3.4 Oversikt over PREMIS Events, Rights og Agents

Den første oversikten nedenfor viser:
1) hvilke hendelser som skal inngå som Events i PREMIS
2) hendelser som – inkludert disse og i tillegg til disse – skal finnes i event-loggen Depotoperasjoner *utenfor* PREMIS i en AIP/AIU.

En mer detaljert oversikt over Depotoperasjonene utenfor PREMIS vises i kapittel 5.3.6. Tabellen under 5.3.6 viser dessuten hendelser som skal være logget i forvaltningssystemets database (ESSArch) i tillegg til å finnes i event-loggen Depotoperasjoner.

***PREMIS Events** og andre hendelser som skal dokumenteres i arkivpakker:*

	Hendelse	***Hendelsestype i PREMIS***	***1) Events i PREMIS***	***2) Depot-operasjoner***	***Kommentar***
Initiell mottakskontroll					
1	Mottak av SIP	Capture		x	
2	Integritetskontroll av SIP og medfølgende info.	Fixity check Validation		x	Sjekksum-generering og sjekksum-verifisering
3	Visuell kontroll av SIP	Validation		x	Kontroll av at avtalte filer inngår i SIP
4	Virussjekk av SIP	Virus check		x	Virus-skanning etter karantene-periode
5	Generering av operasjonslogg(er)			x	Logg for operasjoner utført i mottaksfasen
6	Overføring av SIP med tilleggsinfo. og opera-sjonslogg til depotsystem			x	Tilrettelegging for import til depotsystem
Innsjekking til depotsystem					
7	Innsjekk av SIP med til-leggsinfo. til depotsystem	Fixity check Validation		x	Import
8	Integritetskontroll og validering ved innsjekking	Fixity check Validation		x	Sjekksum-generering/ Sjekksum-verifisering
9	Utsjekking for testing på eget arbeidsområde og ny innsjekk etter testing	Replication		x	Eksport/import
10	Integritetskontroll av filer etter utført testing	Fixity check Validation		x	Sammenligning av SIP-filer før og etter test.
Test av SIP på arbeidsområde					
11	Kontroll av hver enkelt SIP-fil	Fixity check Validation		x	En hendelse pr. test som utføres.
12	Evt. endring i materialet foretatt som ledd i testing	Adjustment	AIP	x	En hendelse for hver endring som utføres.

	Hendelse	***Hendelsestype i PREMIS***	***1) Events i PREMIS***	***2) Depot-operasjoner***	***Kommentar***
13	Innhenting av tilleggs-informasjon	Capture		x	En hendelse for hver innhenting (inkl. til-latelser til å gjøre endringer i materialet.
14	Endring av metadata	Adjustment	AIP/ AIU	x	En hendelse for hver endring som utføres.
15	Bearbeiding av katalog-struktur	Adjustment		x	
16	Klargjøring for innsjekk til depotsystemet med logg for utførte testoperasjoner			x	Import – styrt fra depotsystemet
Skape og innlemme AIP/AIC					
17	Utveksling av informasjon med andre systemer				Utveksling med ASTA (og evt. andre syst.).
18	Generere arkivpakke: AIP-0, AIP-1 (eller AIU) og AIC	Creation	AIC	x	
19	Innlegging i lagrings-systemet (DSM)	Ingestion	AIC	x	Innlegging av AIC med tilknyttede pakker
Vedlikehold av arkivpakke					
20	Kopiering fra DSM arbeidsområde	Replication		x	Kopiering av AIP og tilhørende AIC
21	Formatkonvertering	Migration	AIP	x	
22	Endring av klausulering	Adjustment	AIP/ AIU	x	Kan være nedgradering, oppheving av klausul, endring fra deponering til avlevering, etc.
23	Kassasjon av materiale	Disposal	AIP	x	Av hele eller deler.
24	Innsjekking til depot-systemet etter operasjoner			x	Import – styrt fra depotsystemet
25	Pakking og innlegging i DSM. Endret AIP lagres som tillegg. Endret AIC oppdaterer foregående	Ingestion	AIC	x	Innlegging av AIC med tilknyttede pakker
Annet vedlikehold av pakker					
26	Fjerning av en AIU/AIP	Deletion		x	Fjerning eller sletting av en pakke i DSM.
Skape en DIP					
27	Kopiering fra DSM til arbeidsområde (via kontrollområde)	Replication		x	Kopiering av AIP og tilhørende AIC

Hendelse		Hendelsestype i PREMIS	1) Events i PREMIS	2) Depot-operasjoner	Kommentar
28	Tilpasse innhold for DIP	Adjustment		x	
29	Innsjekking til depot-systemet (med operasjonslogg)			x	Import – styrt fra depotsystemet
30	Generering av DIP med sjekksumm(er)	Creation		x	
31	Eksport av DIP til utvekslingsområde	Replication		x	
32	Oppdatering av AIC	Adjustment	AIC	x	
33	Lagring av AIC i DSM, evt. sammen med DIP dersom denne skal lagres	Ingestion	AIC	x	Behovet for å lagre en DIP i DSM vil være varierende.

***PREMIS Rights** i digitalt depot:*

(Depotets) Rettighet	Premis	Kommentar
Endre status fra deponering til avlevering		
Endring av gradering/ klausulering		
Rett til å innhente tillatelse fra arkiveier		

***PREMIS Agents** i digitalt depot:*

Agent	Premis	Kommentar
Forvaltningssystemet	Software	
Saksbehandler	Person	Avdeling/Seksjon
Arkivskaper	Organization / Person	Institusjon
Uttrekksprodusent	Person / Organization	Firma/Institusjon

4.3.5 Bruk av EAD og EAC-CPF

EAD[22]– *Encoded Archival Description* – brukes til å beskrive bevaringsobjektene logisk som arkivmateriale. EAD kan regnes som et utvekslingsformat for ISAD(G), men omfatter en rekke elementer i tillegg. DIAS skal utveksle EAD-informasjon med Asta eller et tilsvarende arkivinformasjonssystem.

EAC-CPF[23] – *Encoded Archival Context – Corporate bodies, Persons, and Families* – brukes til å beskrive arkivskapere og andre aktører med tilknytning til arkivobjekter, og supplerer EAD. DIAS skal også utveksle EAC-CPF-informasjon med Asta.

[22] Ref. til xml-skjema for EAD: http://www.loc.gov/ead/ead.xsd (lest 01.03.2012)

[23] Ref. til xml-skjema for EAC-CPF: http://eac.staatsbibliothek-berlin.de/schema/cpf.xsd (lest 01.03.2012)

DIAS bruker de to xml-skjemaene for EAD og EAC-CPF i sin fullstendige form, uten egne norske tilpasninger. Men ikke alle elementene skal være "mappet" til Asta. Prosjektet har samarbeidet med Asta-stiftelsen om dette, og deretter spesifisert en oversikt over hvordan EAD- og EAC-CPF-filer produseres fra Asta. Disse oversiktene, som inngår blant DIAS-prosjektets produkter[24], er tatt inn i rapportens del 2 som vedlegg 5: *Mapping mellom EAD og Asta* og vedlegg 6: *Mapping mellom EAC-CPF og Asta*.

DIAS-forvaltningssystemet genererer xml-filer iht. skjemaene for de ulike metadata-kategoriene i DIAS, herunder for EAD og EAC-CPF. Men det kan være behov for å generere EAD- og EAC-CPF-filer for Asta-utveksling allerede ved SIP-mottak i arkiv-depot, som i Arkivverkets rutineopplegg. Betty-systemet, som utvikles av et annet samarbeidsprosjekt mellom Riksarkivaren og kommunale aktører, har hjelpemidler for dette. Løsningene vil dessuten bli distribuert som selvstendige "app-er" for å kunne brukes helt uavhengig av Betty, og de vil dermed også være tilgjengelige som verktøy for å generere EAD- og EAC-CPF-filer ved fremstillingen av en SIP.

4.3.6 Bruk av ADDML

ADDML[25] – *Archival Data Description Markup Language* – er Arkivverkets egenutviklede standard for teknisk beskrivelse av poststrukturerte datafiler i tabelluttrekk (teknisk "datasett-beskrivelse"). I gjeldende ADDML-versjon 8.2 er det lagt til muligheter for overordnede beskrivelser av andre typer filer og for kontekstuell informasjon. Noark-5 anvender ADDML med disse tilleggselementene i *arkivuttrekk.xml*.

I DIAS er det også vurdert å inkludere MIX[26] for teknisk beskrivelse av foto/bildeformater, tilsvarende den svenske modellen. Seksjon for Digitalt depot i Riksarkivet vurderer å inn-arbeide dokumentformater, herunder MIX, i ADDML. Prosjektet har valgt å ikke inkludere MIX eller andre standarder for bildeformater i den første versjonen av DIAS.

4.4 Kravspesifikasjon til et forvaltningssystem for DIAS arkivpakker

Prosjektet har utarbeidet en generell kravspesifikasjon til et forvaltningssystem for DIAS-arkivpakker, jf. rapportens del 2, vedlegg 7. Forvaltningssystemet skal anvende DIAS-pakkestrukturen og støtte prosjektets prosessmodell for integritetssikring i digitalt depot.

Et DIAS-forvaltningssystem skal etter kravspesifikasjonen ha følgende hovedegenskaper:

- Det skal generere alle typer av arkivpakker som inngår i DIAS-modellen på grunnlag av de spesifikke xml-skjemaer som er definert for DIAS-strukturen.
- Det skal kunne utføre integritetssikring ved å generere sjekksummer for filer/objekter og samlede arkivpakker, og ved å verifisere sjekksummer.
- Det skal håndtere arkivpakker innenfor et kontrollert miljø, og styre alle operasjoner og all brukertilgang ved mottak, testing, generering og vedlikehold av arkivpakker i digitalt depot.

[24] Mapping-oversiktene er også tilgjengelige på http://www.arkivverket.no/standarder/dias (lest 01.03.2012)

[25] http://www.arkivverket.no/arkivverket/Arkivbevaring/Elektronisk-arkivmateriale/Standarder/ADDML (lest 25.02.2012)

[26] MIX – NISO Metadata for Images in XML Schema – Technical Metadata for Digital Still Images Standard. Ref.: http://www.loc.gov/standards/mix/ (lest 25.02.2012)

- Det skal styre all innlemmelse av arkivpakker i digitalt depots lagringssystem, all uthenting av arkivpakker fra lagringssystemet og all eksport av arkivpakker eller arkivpakkeinformasjon fra digitalt depot.
- Det skal dokumentere utførte operasjoner ved mottak, testing, generering, innlemmelse/ uthenting, vedlikehold og eksport av arkivpakker, og det skal integritetssikre operasjonsloggene på linje med innholdet i arkivpakkene.
- Det skal ha en database med informasjon om alle arkivpakker i digitalt depot og utførte operasjoner i tilknytning til dem.
- Det skal gi mulighet for fremsøking av arkivpakker i digitalt depot og mulighet for å produsere rapporter med definerte nøkkelopplysninger om lagrede arkivpakker.
- Som *opsjon* skal systemet også ivareta lagringsadministrasjon. Det skal kunne kopiere/ migrere objekter til ulike medier (disk, tape, CD/DVD), identifisere og synkronisere lagrede versjoner av samme objekt på ulike medier, verifisere mediemigrering og detektere alle former for korrumpering eller tap av data.

Opsjonen for lagringsadministrasjon er i utgangspunktet ment for depoter uten egne systemer for dette (f.eks. for administrasjon av SAN lagringsnett). Med denne funksjonen skal forvaltningssystemet kunne brukes som et samlet depotstyringssystem både for enkle og avanserte lagringsløsninger.

4.5 Utvikling av ESSArch som et DIAS-tilpasset forvaltningssystem

På grunnlag av den foreliggende kravspesifikasjonen har prosjektet i siste fase også utviklet et forvaltningssystem for DIAS-arkivpakker. Utviklingen av DIAS-forvaltnings-systemet har bygget på systemet ESSArch fra leverandøren ES Solutions AB. ESSArch, som brukes av det svenske riksarkivet, er blitt tilpasset for DIAS slik at det oppfyller samtlige punkter i prosjektets kravspesifikasjon. Systemet håndterer også lagrings-administrasjon. Det skal dermed kunne brukes av alle aktuelle statlige og kommunale arkivdepoter uavhengig av om de har egne løsninger for å administrere fysisk lagring.

Tilpasningen og videreutviklingen av ESSArch for DIAS er utført på oppdragsbasis av leverandøren ES Solutions som ledd i et implementeringsprosjekt i Riksarkivet fra høsten 2011. Systemet, som ble klargjort for ordinær drift i Riksarkivet fra 08.06.2012, er basert på fri programvare. Programvaren er lisensiert som GNU General Public License version 3 (GPLv3). DIAS-versjonen av ESSArch vil følgelig være fritt tilgjengelig for alle inter-esserte. Brukere vil også fritt kunne tilpasse systemet videre – mot å publisere tilleggene.

Riksarkivaren har inngått avtale med ES Solutions om vedlikehold av DIAS-versjonen av ESSArch. Kommunale depoter har adgang til å tegne egne vedlikeholdsavtaler, men i første omgang legges det opp til å bruke Riksarkivarens avtale som en sentral vedlikeholdsavtale også for kommunale depoter. All leverandørkontakt forutsettes da kanalisert via en sentral instans i Riksarkivet. For å nyte godt av avtalen må kommunale brukere dessuten avstå fra individuelle tilpasninger. Men det legges samtidig opp til en samlet videreutvikling av ESSArch for det norske brukermiljøet. For dette formålet har samarbeidspartnerne i DIAS startet et oppfølgingsprosjekt for å etablere et forum for å forvalte DIAS-prosjektets standarder og forvaltningssystem. Organiseringen og oppgave-rammen for DIAS forvaltningsforum behandles videre i kapittel 6, nedenfor.

4.6 Prosessmodeller for et DIAS-basert digitalt depot

Til DIAS-prosjektets produkter hører også prosess- og rutineopplegg tilpasset for arkivdepoter som bruker DIAS-forvaltningssystemet ESSArch. Prosessmodellen beskrives nærmere i kapittel 5 – i to varianter: som en basismodell for et digitalt arkivdepot, og som den videre utbygde prosessmodell som brukes av Riksarkivet.

5. IMPLEMENTERING AV ET DIAS-FORVALTNINGSSYSTEM

5.1 ESSArch-prosjektet – Opplegg og gjennomføring

Prosjektet for å implementere ESSArch som et DIAS-tilpasset forvaltningssystem startet i november 2011, og ble sluttført 8. juni 2012 etter gjennomført akseptansetest i Riksarkivets testmiljø. Ved ESSArch-implementeringen har to prosjektløp vært kombinert: DIAS-prosjektets systemutvikling og Arkivverkets Elmag-prosjekt. Innføringen av ESSArch i Riksarkivet har samtidig vært DIAS-prosjektets pilotinstallasjon.

Utviklingsarbeidet har vært basert på DIAS-prosjektets kravspesifikasjon til et forvaltningssystem og ES Solutions' leveransespesifikasjon i inngått avtale om programutvikling. Planen for implementeringsprosjektet ble fastsatt i "Prosjektdirektiv for ESSArch-innføring i Riksarkivet 2011-2012" (07.10.2011). Prosjektmålene har vært følgende:

- foreta de nødvendige utstyrsanskaffelser og organisatoriske tilpasninger for å tilrettelegge et miljø for uttesting av ESSArch i et digitalt arkivdepot,
- utarbeide en testplan for ESSArch, og følge opp denne testplanen gjennom 6 definerte iterasjoner for å bekrefte at systemet fungerer iht. prosjektets kravspesifikasjon og leverandørens løsningsspesifikasjon,
- verifisere gjennom testingen at DIAS-prosjektets xml-skjemaer fungerer for sine formål,
- foreta en nødvendig justering av systemfunksjoner i ESSArch som resultat av testingen,
- konkretisere og justere DIAS-prosjektets prosessmodell hvor utviklingsarbeidet og testingen avdekker behov for dette,
- gjennomføre en avsluttende akseptansetest for ESSArch iht. en omforent testplan,
- etablere et ferdig produksjonsmiljø for ESSArch i tilknytning til Riksarkivets digitale sikringsmagasin,
- bekrefte at ESSArch også vil være egnet for bruk i kommunale arkivdepoter.

ESSArch-prosjektet er gjennomført i samsvar med denne planen, og første versjon av ESSArch for DIAS ble godkjent etter gjennomført akseptansetest 08.06.2012. Depoter utenfor Riksarkivet anbefales likevel å vente med å sette systemet i drift til det foreligger en ny og utbedret versjon senere i 2012.

5.2 ESSArchs plass og rolle i produksjonsmiljøet

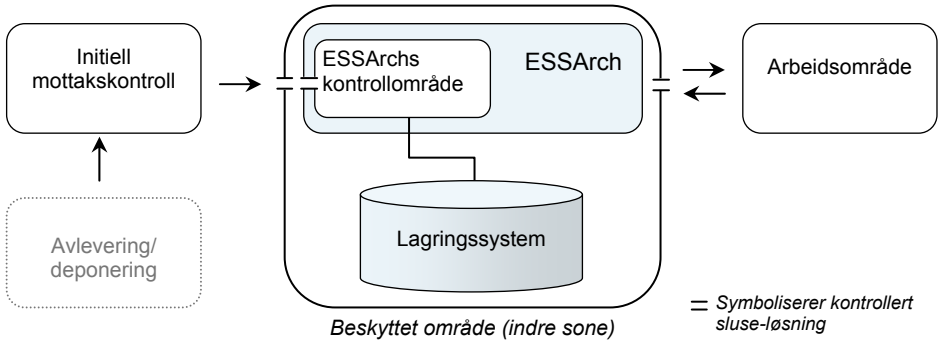
ESSArch genererer og vedlikeholder arkivpakker innenfor et kontrollert miljø, og styrer all innlegging og uthenting av arkivpakker i det digitale depotets lagringssystem. ESSArch styrer også all import og eksport av informasjon til/fra forvaltningssystemets områder. Importerte objekter integritetssikres med sjekksummer som grunnlag for å verifisere at de

er bevart uendret. Ved import blir sjekksum-generering og verifisering utført automatisert av ESSArch. For mellomlagring av informasjon som er importert for videre bearbeiding, har ESSArch et dedikert "kontrollområde" (ESSArchs eget arbeidsområde) som utelukkende systemet har tilgang til.

ESSArchs styringsregime omfatter imidlertid ikke alle prosesser og rutineopplegg i et digitalt depot. Utenfor ESSArchs " jurisdiksjon" ligger for det første den initielle kontrollen ved mottak av SIP-er, som typisk vil omfatte registrering, 3 ukers virus-karanténe og etterfølgende virus-skanning. En karanténeperiode er nødvending for at programvaren for virus-skanning skal være oppdatert. Skanningen foretas på en fritt-stående PC for å unngå faren for infisering av annet utstyr. Import ("innsjekking") til ESSArch skjer først etter mottakskontrollen, men importen forutsettes også å omfatte en samlet logg for de utførte operasjonene ved mottakskontrollen.

Utenfor ESSArchs kontroll ligger dessuten operasjonene ved den tekniske testingen av mottatt materiale. I dette tilfellet eksporterer ESSArch en kopi til et utenforliggende arbeidsområde – etter først å ha innsjekket og lagret materialet integritetssikret med sjekk-summer på kontrollområdet. Etter testingen importerer ESSArch materialet med tilføyde operasjoner og testlogg, og foretar en verifisering mot "originalen" på kontrollområdet. Slik opprettholder ESSArch integritetskontrollen av materialet gjennom testfasen. Det er selve utførelsen av testoperasjonene som ligger utenfor ESSArchs kontrollregime. Modellen åpner også for å sette testingen helt eller delvis bort til en ekstern part.

Figur: ESSArchs plass og rolle i produksjonsmiljøet



ESSArchs rolle i prosessmodellen er å fungere som det digitale depotets operasjonssenter, med spesiell vekt på å ivareta kravene til integritetssikring. Modellen bygger også på forut-setninger om prosessene utenfor ESSArch, blant annet at ESSArch skal bevare logger og annen dokumentasjon fra disse operasjonene. Men for øvrig skal arkivdepoter kunne tilpasse den samlede prosessmodellen med utgangspunkt i ulike krav og behov.

Kravene til integritetssikring og lagringssikkerhet i et digitalt depot er fundamentale. Men når det gjelder *konfidensialitetssikring* og *tilgangsstyring*, vil behov og ambisjoner kunne variere, i og med at ulike bestandskategorier av arkivmateriale stiller ulike krav til beskyttelsesnivå. Beskyttelsesnivået i et depot som bevarer offentlig arkivmateriale må likevel forutsettes å være høyt, og avspeile at bestanden typisk vil inkludere personsensitiv informasjon og annet taushetsbelagt materiale. Dette er lagt til grunn i figuren ovenfor. Lagringssystemet og ESSArch utgjør her et felles, beskyttet område hvor både tilgang og eksport/import av informasjon skjer gjennom en kontrollert sluse (i praksis en brannmur). Tilgang til ESSArchs kontrollområde er særskilt sikret innenfor denne sonen.

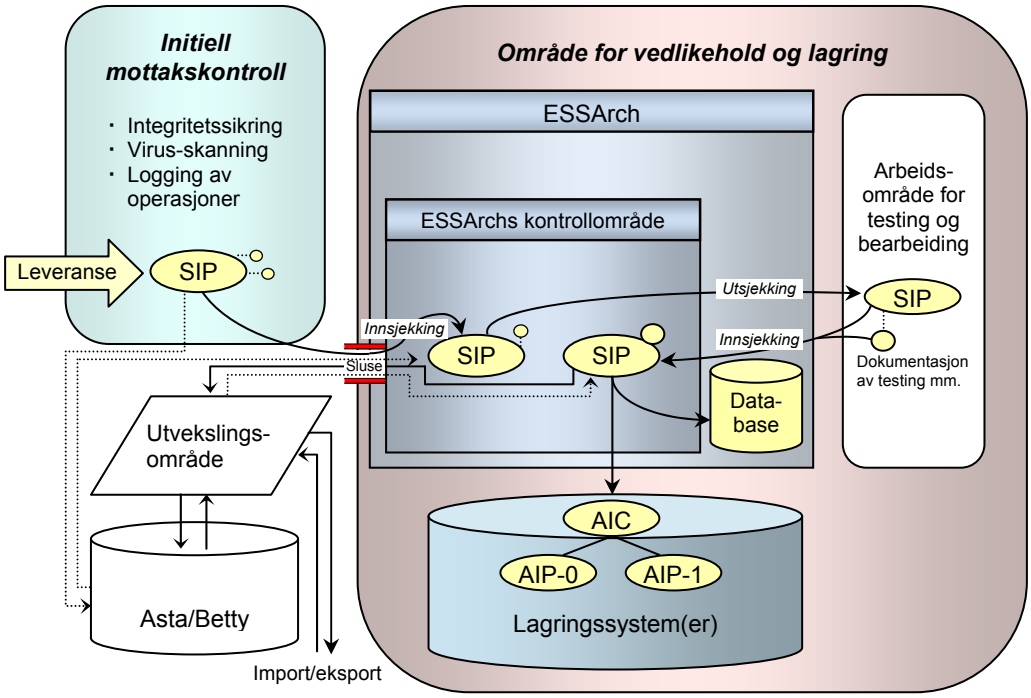
Kravene til konfidensialitetssikring og tilgangsstyring i digitalt depot må også gjelde for tilknytningen av kontormiljøer. Med det beskyttelsesnivå som indikeres i figuren ovenfor, vil tilknyttede arbeidsstasjoner måtte være dedikerte, og ikke kunne kommunisere direkte med annet utstyr. I tillegg kreves fysiske sikkerhetstiltak i kontormiljøet på nivå med sikkerhetsopplegget for digitalt depot.

5.3 Prosesser i et ESSArch-styrt digitalt depot

Nedenfor beskrives prosesstadiene og arbeidsflyten i et digitalt depot med ESSArch som forvaltningssystem. Under hvert prosesstadium beskrives først en basis prosessmodell, og deretter prosessmodellen som er implementert i Riksarkivets digitale depot.

Figuren nedenfor illustrerer basismodellen for et digitalt depot med ESSArch som sentralt styringssystem.

Figur: Prosesser i digitalt depot



Drabanter til en SIP (tilknyttede gule kuler) representerer medfølgende informasjon i separate enheter (info-fil ved avlevering og tilleggsinformasjon som dokumenterer depotoperasjoner etter mottak).

5.3.1 Initiell mottakskontroll

Operasjonene ved arkivdepotets mottak av en SIP vil normalt omfatte:

a) registrering (inkludert journalføring),
b) en enkel kontroll av at informasjonsinnholdet er som fastsatt eller avtalt (forutsetningsvis uten å åpne filer), og at nødvendig dokumentasjon medfølger,
c) integritetssikring av den mottatte SIP-en ved å generere en samlet sjekksum, evt. også ved å bruke denne til å verifisere en medfølgende SIP-sjekksum fra avgiveren,
d) gjennomføring av viruskontroll etter en periode med karanténe (normalt 3 uker),
e) eventuell registrering av arkivbeskrivelse i Asta e.l. arkivinformasjonssystem,
f) registrering av hendelser som er utført på SIP som ledd i mottakskontrollen,

g) kontroll av tilhørende info-fil (”info.xml”) som skal leveres med en SIP,
h) tilrettelegging av SIP med medfølgende dokumentasjon og mottakskontrollens operasjonslogger for innsjekking i ESSArch.

Tidspunktet for integritetssikring er et springende punkt. En samlet SIP-sjekksum må genereres umiddelbart ved mottak for at arkivdepotet skal kunne garantere for – og senere aktivt bekrefte – at materiale er bevart uendret fra og med mottak. Sjekksum-generering forut for karanténen og virus-skanningen medfører fare for infisering av utstyr. Men det vil svekke integritetssikringens troverdighet om den derfor utsettes i anslagsvis en måned til innsjekkingen i ESSArch, hvor sjekksummer genereres som ”Standard Procedure”. Dette bare av den enkle grunn at det lar seg påvise at mediene da har passert gjennom mange hender – med ditto muligheter for manipulasjon.

Genereringen av en sjekksum ved mottak vil lettere kunne utskytes dersom SIP-en har en medfølgende sjekksum, noe som vil komme til å bli et krav til avleveringer fra offentlige organer[27]. Depotets sjekksum produseres da for å verifisere avhenderens. Men også en utsatt verifisering av en medfølgende sjekksum kan åpne muligheter for manipulering[28]. Dersom en tidlig verifisering viser at avhenderens sjekksum er korrumpert, gir dette i seg selv grunn til å avvise SIP-en, og da trengs heller ingen viruskontroll.

Det problematiske ved integritetssikringen i dag er at mottakskontroll gjennomgående er basert på manuelle rutiner. Materiale avleveres/deponeres på bortsettingsmedier (inkludert flyttbare disker), og bringes fysisk til ulike behandlingsinstanser, til sist til ESSArch for innsjekking. Elektronisk SIP-overføring vil muliggjøre en mer automatisert kontroll, men det er foreløpig ikke definert prosessopplegg for dette – så langt elektroniske overføringer er gjennomførbare med tanke på volum og nettkapasitet. De manuelle rutinene i mottaks-fasen forsterker behovet for å utføre integritetssikringen på et tidligst mulig tidspunkt. De gjør det også desto mer nødvendig å dokumentere utførte operasjoner ved mottaks-kontrollen. Siden det er fysiske medier som behandles i denne fasen, blir det særlig viktig å dokumentere at den fysiske sikringen av mediene har hindret uautorisert kopiering og kompromittering av informasjon.

Ved mottak vil det være naturlig å registrere opplysninger i Asta eller et tilsvarende arkiv-informasjonssystem, men forutsetningene kan variere ganske mye når det gjelder et arkiv-depots styring av prosessen ved fremstilling og overføring av arkivuttrekk. Innholdet kan være kjent og nærmere definert gjennom vedtak eller avtaler, og i dette tilfellet vil det også være naturlig å oppdatere Asta i mottaksfasen. Men det andre ytterpunktet vil være et depot som mottar de avleveringer/deponeringer som viser seg å komme fra tilknyttede arkivskapere. Asta-registrering kan da måtte vente til det konkrete innholdet åpenbarer seg i testfasen.

[27] Som et første steg sendte Riksarkivaren 08.02.2012 ut et rundskriv om krav til sjekksum ved overføring av arkivuttrekk til Riksarkivet. Det ble fastsatt at arkivuttrekket (informasjonsinnholdet) skal være pakket som en tar-fil (inntil 1 TB), og at en samlet sjekksum for tar-filen basert på algoritmen SHA-256 skal følge i en separat overført fil kalt info.xml. Denne filen, som etter gjeldende avleveringsbestemmelser også skal inneholde overordnet informasjon om avleveringen/deponeringen, skal sendes på e-post til Riksarkivets postmottak. For arkivuttrekk som følger Noark 5-standarden, gjelder egne bestemmelser. I dette tilfellet skal info.xml innholde sjekksum for filen arkivuttrekk.xml i arkivuttrekket.

[28] f.eks. ved å bytte ut avhenderens sjekksom med en nygenerert sjekksum etter at innhold er endret. For å eliminere en slik mulighet kreves mao. stramme rutiner for en umiddelbar og sikker lagring av SIP-ens medfølgende sjekksum.

Når Asta oppdateres ved SIP-mottak, kan det – gitt at hjelpemidler er tilgjengelige[29] – produseres en EAD-fil med arkivbeskrivelse og en EAC-CPF-fil med aktørbeskrivelse som skal innlemmes i arkivpakken (AIP) når denne senere genereres av ESSArch. Dette er den ene av to alternative måter å fremstille en arkivpakkes EAD- og EAC-CPF-filer på. Den andre er å bruke ESSArch til produsere de to metadatafilene når arkivpakker genereres, jf. punkt 5.3.2. De to alternative metodene er inntegnet som prikkede linjer i figuren under punkt 5.3, foran. Når EAD og EAC-CPF produseres med utgangspunkt i Asta, kreves en tilbakemelding fra ESSArch for å oppdatere Asta med ID-nummer for vedkommende AIC i lagringssystemet. Dette skjer ved at ESSArch eksporterer informasjonen til et eget utvekslingsområde hvor Asta (Betty) kan innhente den, jf. figuren under punkt 5.3.

Prosessmodell i Riksarkivet

I Riksarkivets prosess- og rutineopplegg skal samlet sjekksum for en SIP genereres umiddelbart etter at den er mottatt og registrert av arkivtjenesten. Operasjonen skal attesteres av to personer, og sjekksummen skal sikres ved å lagres på saken i arkivsystemet. Når sjekksum medfølger fra avhenderen (i separat sending), foretas en verifisering mot Riksarkivets sjekksum. Også SIP-ens medfølgende sjekksum lagres i arkivsystemet.

Faren for infisering av annet utstyr som vil foreligge når sjekksum genereres forut for karanténen og virus-skanningen, minimaliseres i Riksarkivet ved å generere sjekksummen på samme frittstående PC som brukes til virus-skanning. Faren for infisering er da i utgangspunktet den samme som ved gjennomføringen av viruskontroll, men det blir nødvendig å foreta en etterfølgende (første gangs) virussjekk for å forsikre at PC-en fortsatt er ren. Uidentifisert "malware" vil dessuten først kunne åpenbare seg etter karanteneperioden. Men PC-en for virus-skanning lever uansett i stadig fare for infisering[30]. Flere virus-skannere brukes dersom dette leddet viser seg å bli en flaskehals.

Virus-PC-en skal ikke laste inn innhold, men generere sjekksum av innholdet slik det ligger på avleveringsmediet (CD, DVD, disk). Operasjonen foretas uten å åpne filer i SIP-en. Begge deler bidrar til å begrense faren for å infisere PC-en, men viktigere er det likevel at PC-en ikke infiserer avleveringsmediet om den selv skulle være infisert. Denne risikoen elimineres ved å sperre for skrivetilgang til SIP-ens medium.

I Riksarkivet skal materiale som avleveres/deponeres, på forhånd være kartlagt og registrert i Asta. Opplysningene legges inn i Asta via Betty, og flagges som "Eksternt arkiv" i Asta. Ved mottak av en SIP skal innholdsbeskrivelsen kontrolleres mot arkiv- og aktørbeskrivelsen i Asta/Betty. Deretter ajourføres og kompletteres opplysningene i Asta/Betty, typisk med utfyllende opplysninger om klausul og rettigheter som kan være gitt i SIP-ens medfølgende info-fil. Til sist skal det fremstilles en EAD-fil med arkivbeskrivelse og en EAC-CPF-fil med aktørbeskrivelse ved hjelp av Betty. Disse filene tilrettelegges for innsjekking i ESSArch som tilleggsobjekter til SIP-en.

Den senere testingen av en SIP skal blant annet bekrefte at innholdet er som fastsatt i arkivbeskrivelsen, og testingen skal til vanlig ikke medføre noe behov for å oppdatere

[29] Teknisk genereres EAD- og EAC-CPF-filer av Betty-systemet, som skal arbeide mot Asta. Som ledd i Betty-utviklingen er det også laget selvstendige "app-er" for dette formålet.

[30] Det foreligger flere muligheter for å motvirke faren for infisering før og under virus-skanningen. Ved bruk av virtualisering kan operasjoner utføres som egne sesjoner innenfor et lukket miljø. Programmiljøet vil også kunne tilbakestilles til det opprinnelige etter utført skanning, og dermed eliminere all infisering

opplysningene i EAD- og EAC-CPF[31]. ESSArch skal kunne innarbeide EAD- og EAC-CPF-filene i arkivpakker (AIP-er) slik de ble mottatt fra den initielle kontrollen. Men Asta må oppdateres med to typer av opplysninger når en ny arkivpakke innlemmes i lagrings-systemet: lagrings-ID for vedkommende AIC, og informasjon om at avleveringen er godkjent etter testing. Godkjenningen skal medføre at status i Asta endres ved at flagg for "Eksternt arkiv" fjernes. Via utvekslingsområdet kommuniseres disse opplysningene til Betty (for oppdatering av Asta) ved innlemmelsen av arkivpakken i lagringssystemet.

Den initielle mottakskontrollen avsluttes ved at følgende objekter importeres og innsjekkes av ESSArch[32]:

- mottatt SIP (på avleveringsmediet)
- avsenderens info-fil til SIP og eventuell medfølgende sjekksum til SIP
- sjekksum generert av Riksarkivet ved mottak
- EAD- og EAC-CPF-filer fra Betty/Asta
- Hendelseslogger fra virus-skanning og integritetskontroll (sjekksumgenerering og eventuell verifisering av medfølgende sjekksum) via overføringsområde.

5.3.2 Innsjekking og pakkegenerering i ESSArch

Inn- og utsjekking i ESSArch vil si å overføre eller kopiere materiale til og fra ESSArchs dedikerte kontrollområde.

Innsjekkingen i ESSArch av en ny SIP med tilknyttede objekter vil normalt kombineres med en tilrettelegging av materialet i ESSArch for testing på et utenforliggende arbeids-område. Etter innsjekk med tilhørende kontroll og sjekksum-generering foretas da først en utsjekking (eksport) av materialet til arbeidsområde for testing. Når denne testingen er gjennomført, foretas en ny innsjekking i ESSArch med påfølgende pakkegenerering.

Følgende ESSArch-operasjoner utføres ved innsjekking av SIP fra initiell mottakskontroll:

- SIP-en (i opprinnelig mottatt form) med alle medfølgende objekter fra avhenderen og all tilleggsdokumentasjon fra mottakskontrollen lagres på ESSArchs kontrollområde.
- SIP-en tildeles en unik ID.
- Integritetskontroll foretas. Sjekksummer genereres for verifisering.
- SIP-en utpakkes fra tar-format (når dette er brukt).
- Xml-filer i SIP-en valideres mot DIAS xml-skjemaer.
- SIP-en med tilhørende objekter utsjekkes (kopieres) til eksternt arbeidsområde for testing.
- Utførte operasjoner ved inn- og utsjekking loggføres.

[31] I tilfeller hvor testingen viser at innholdet avviker fra Asta-beskrivelsen, vil det som første trinn kreves en konsultasjon med de mottaksansvarlige om dette gir grunnlag for å avvise avleveringen.

[32] I Riksarkivets implementeringsprosjektet har løsningen vært å bringe objektene på fysiske medier til ESSArchs innsjekk-PC. Men en slik fysisk ombringing av medier mellom operasjoner i mottaksfasen medfører flere risikomomenter. Målet må være å håndtere alle prosesser – inkludert selve overføringen av SIP fra arkivskaper – innenfor et kontrollert nett. For overgangen mellom mottaks- og ESSArch-fasen tar Riksarkivet sikte på å innpasse en løsning hvor virus-kontrollerte filer sendes via lukket nett til PC-en for ESSArch-innsjekking med det dedikerte utvekslingsområdet for ESSArch som mellomstasjon.

Følgende ESSArch-operasjoner utføres ved pakkegenerering – i dette tilfellet når testing på eksternt arbeidsområde er utført med godkjent resultat:

- Materialet innsjekkes fra arbeidsområdet til ESSArchs kontrollområde, og den tilhørende tilhørende test-loggen og eventuell annen ny dokumentasjon (f.eks. en ADDML-fil som er oppdatert av testeren) integritetssikres med sjekksum.
- "Differansekontroll" utføres ved å (sjekksum-)verifisere innhentede objekter mot tilhørende "originaler" som ligger lagret på kontrollområdet.
- EAD- og EAC-CPF-filer genereres dersom disse ikke fulgte med SIP-en ved innsjekking fra mottakskontrollen. Filene eksporteres til utvekslingsområdet for å hentes inn av Betty/Asta for oppdatering. Oppdaterte EAD-og EAC-CPF-filer kommuniseres deretter fra Betty/Asta, og innsjekkes til ESSArchs kontrollområde for å kunne innlemmes i vedkommende arkivpakke. Alternativt til å eksporterte EAD/EAC-filer som forslag til Asta, kan operasjonen begrenses til å sende en forespørsel til Asta.
- En arkivpakke fremstilles. Dette gjøres gjennom følgende operasjoner:
  - En AIP-0 genereres som en eksakt kopi av vedkommende SIP slik den ble mottatt.
  - En AIP-1 bestående av SIP-ens informasjonsinnhold, arkivskaperens tilleggs-dokumentasjon (info-fil) og all dokumentasjon av depotoperasjoner fra og med mottak genereres av ESSArch iht. DIAS xml-skjemaer, pakkes som en tar-fil, kontrolleres og integritetssikres med samlet sjekksum.
  - Alternativt til en AIP-1 genereres en enkel AIU med følgende tillegg til AIP-0: arkivskaperens info-fil, all dokumentasjon av depotoperasjoner fra og med mottak og eventuelle tilføyde metadatafiler iht. DIAS xml-skjemaer (typisk ADDML). AIU-en pakkes som tar, kontrolleres og integritetssikres med samlet sjekksum.
  - En overordnet AIC genereres. Den skal ha referanser til tilknyttede AIP-er og eventuelle AIU-er. Den skal også vise hvilken AIP den enkelte AIU er relatert til. Samlede sjekksummer for de tilknyttede pakkene innarbeides i AIC-en. AIC-ens egen samlede sjekksum lagres i forvaltningssystemets database.
- AIC-konstellasjonens arkivpakker innlemmes i lagringssystemet. ESSArch kontrollerer lagringen og skriving av kopier til de tilleggsmedier som brukes for redundant lagring.
- Innlegging av objekter i lagringssystemet logges automatisk av ESSArch.
- Operasjonslogg og annen nøkkelinformasjon om arkivpakken i ESSArchs database oppdateres.
- Lagrings-ID for AIC og melding om at arkivpakken er godkjent og innlemmet i lagringssystemet kommuniseres til Betty/Asta – i de tilfeller EAD- og EAC-CPF-filene var generert av Betty/Asta.

Prosessmodell i Riksarkivet

Prosess- og rutineopplegget i Riksarkivets digitale depot følger beskrivelsen ovenfor – med unntak for genereringen av EAD/EAC-beskrivelser, som utføres initielt i Betty, jf. punkt 5.3.1, foran.

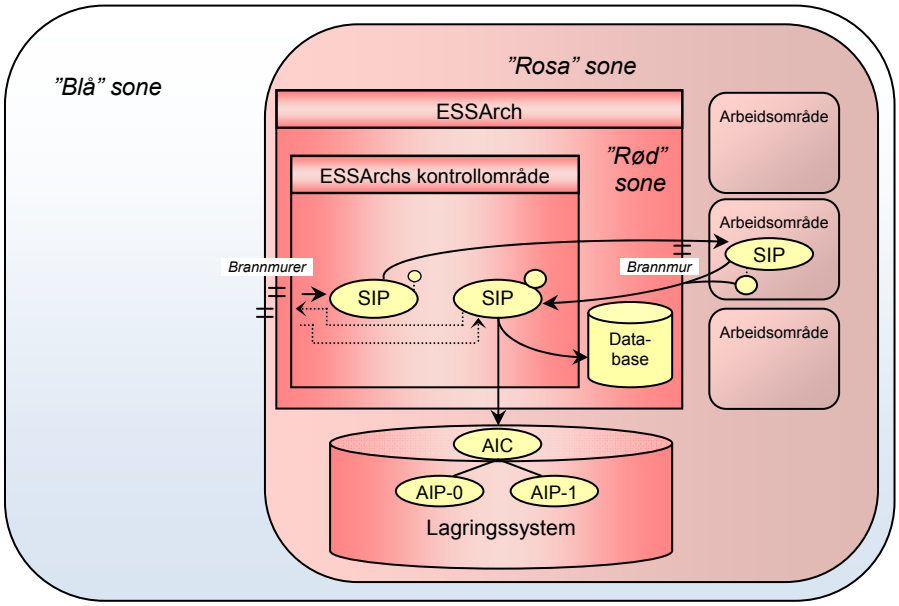
Det som særlig karakteriserer Riksarkivets opplegg, er det høye beskyttelsesnivået for digitalt depot. Lagringssystemet skal kunne håndtere informasjon gradert Begrenset etter sikkerhetsloven. All ugradert informasjon må da være tilsvarende beskyttet. Men iht. interne bestemmelser skal også ugradert informasjon som er taushetsbelagt eller inneholder sensitive personopplysninger, være beskyttet på nivå sikkerhetsgradert Begrenset.

Riksarkivets depotløsning er illustrert i figuren nedenfor. Lagringssystemet og ESSArch er organisert som et eget, særskilt sikret område uten direkte fysisk forbindelse med Arkiverkets lokale nett (ytre blå sone i figuren). En sertifisert brannmur styrer all informasjonsutveksling mellom digitalt depot og blå sone. Digitalt depot er igjen inndelt i to soner: en indre rød sone for ESSArch og lagringssystemet, og en ytre rosa sone. I Riksarkivets løsning er også arbeidsområdet for testing plassert innenfor den rosa sonen.

I tillegg til å styre utvekslingen med blå sone, kontrollerer brannmuren trafikken mellom rød og rosa sone. Figuren nedenfor viser *logiske* brannmurer, men en og samme fysiske brannmur administrerer samtlige porter (VLAN). Brannmuren styres fra ESSArchs kontrollområde, og all import og eksport til og fra ESSArchs kontrollområde utføres av en egen koordinator.

Beskyttelsesnivået for digitalt depot må også gjelde for tilknyttede kontorarbeidsplasser. I Riksarkivet brukes et dedikert arbeidsrom med arbeidsstasjoner som – via et sikret, lukket nett – utelukkende er oppkoblet mot rosa og rød sone. Rommet har kortleser for adgangskontroll. Alle operasjoner mot ESSArch i Riksarkivet må utføres i dette rommet. Nedlasting og uautorisert kopiering av informasjon er ikke mulig. Informasjon i lagringssystemet og på ESSArchs kontrollområde vil heller ikke kunne endres av medarbeidere – med overlegg eller utilsiktet.

Figur: Soneinndeling i Riksarkivets digitale depot



5.3.3 Prosesser ved testing

Testing består i å utføre prosedyrer for å verifisere at innholdet i en SIP er teknisk konsistent, korrekt og komplett, om det oppfyller definerte struktur- og formatkrav, og om det er tilknyttet de tekniske og logiske metadata som kreves for å bevare informasjonen med opprettholdt lesbarhet og autentisitet. Det kan også inngå i testingen å verifisere sjekksummer for enkeltfiler i en SIP.

Arbeidsområdet får seg tildelt testoppgaver fra ESSArchs kontrollområde. Kontrollområdet styrer også tilbakehentingen av informasjon. Eksport og import av objekter til/fra arbeidsområdet logges automatisk av ESSArch. Utførte aktiviteter under testingen skal kunne

registreres i en logg. Operasjonsloggen og dokumentasjon av testresultater skal kunne lagres integritetssikret med sjekksummer, og inngå i materialet som hentes tilbake til ESSArchs kontrollområde.

Arbeidsområdet ligger utenfor ESSArch, men testingen må likevel utføres innenfor et kontrollert og beskyttet område, og ivareta nødvendige krav til konfidensialitetssikring. For mange arkivdepoter kan kravet om konfidensialitetssikring ved testing være en betydelig utfordring.

Prosessmodell i Riksarkivet

I Riksarkivets digitale depot er arbeidsområdet for testing plassert *innenfor* den rosa sonen. Her brukes også dedikerte arbeidsområder for de enkelte testere, blant dem medarbeidere fra statsarkivene, jf. figur ovenfor. Testere får seg dedikert tildelt oppgaver fra kontroll-områdets koordinator. Alle operasjoner mot testområder i Riksarkivet må utføres fra eget, sikret arbeidsrom for digitalt depot. Statsarkiv-medarbeidere har tilgang til sine respektive arbeidsområder i Riksarkivets rosa sone via kryptert linje (VPN), men bare medarbeidere i Riksarkivet kan ha tilgang til ESSArch i tillegg til arbeidsområdet for testing.

Tilgangen til arbeidsområdene for testing er basert på terminal-aksess. Dette sperrer for nedlasting og uautorisert kopiering av informasjon. Terminal-aksess gjør det også nødvendig å ha alt tilgjengelig testverktøy plassert på en sentral test-server i rosa sone.

5.3.4 Prosesser ved vedlikehold av arkivpakker

En arkivpakke (AIP + AIC) skal kunne hentes ut fra digitalt depot for å vedlikeholdes eller oppdateres. Slik uthenting skjer ved import fra lagringssystemet til ESSArchs sentrale kontrollområde, og utføres alltid ved å *kopiere* objekter fra digitalt depot. En typisk funksjon i tilknytning til det langsiktige vedlikeholdet av AIP-er vil være format-konverteringer. Det vanlige vil da være at ESSArchs kontrollområde eksporterer en slik oppgave videre til arbeidsområdet, for deretter å hente inn resultatet.

En oppdatert versjon av en AIP innlemmes i digitalt depot ved eksport fra ESSArchs kontrollområde, og den lagres alltid som en ny versjon (”generasjon”) i tillegg til den foregående – som aldri kan overskrives. En tilføyd AIP krever også en tilhørende over-ordnet AIC i oppdatert versjon. En oppdatert AIC erstatter imidlertid foregående AIC-versjon. Lagring av en enklere AIU som alternativ til en ny AIP krever også oppdatering og ny innlegging av vedkommende AIC.

ESSArch logger all innlemmelse i, og all uthenting (kopiering) av objekter fra lagrings-systemet. ESSArch produserer samlede rapporter om prosessene mellom kontrollområdet og lagringssystemet, og om all eksport/import mellom kontrollområdet og omverdenen (rosa og blå sone).

5.3.5 Prosesser ved fremstilling av bruksversjoner (DIP-er)

En arkivpakke (AIP + AIC) skal kunne hentes ut fra digitalt depot for å tilpasses som en bruksversjon (DIP). Prosedyrene ved uthentingen er da de samme som ved vedlikehold og oppdatering. DIP-en kan genereres av ESSArch på kontrollområdet, eventuelt etter bearbeiding på arbeidsområdet, og den kan også innlemmes i lagringssystemet med knytning til en AIC på linje med AIP-er og AIU-er. Innlemmelse av en DIP i lagrings-systemet krever en oppdatering av vedkommende AIC, i likhet med tilføyde AIP-er og

AIU-er. Standardprosedyrene for uthenting av objekter fra lagringssystemet til ESSArch-kontrollområdet følges også når det er en lagret DIP som hentes ut for videre bearbeiding.

En DIP som er velegnet for bruk, kan være tidkrevende å lage, og derfor verdt å lagre i digitalt depot. Hovedpoenget med å lage en DIP er likevel å gjøre den praktisk tilgjengelig, og for dette formålet må den eksporteres fra digitalt depot til et område hvor dette er mulig. DIP-en kan for så vidt også bearbeides eller videreforedles utenfor digitalt depot, så langt tilgangsbestemmelser og konfidensialitetshensyn ikke hindrer dette. Men integritets-sikringen vil fortsatt være ivaretatt, siden ESSArch kan eksportere informasjonsinnhold sjekksumsikret og verifiserbart.

Formålet med å generere en DIP kan variere. Den kan lages for å gjøres bredt og mer permanent tilgjengelig, eller hentes ut for en spesialisert anvendelse uten større gjenbruks-verdi. Hvis den i det første tilfellet også skal gjøres aksessérbar via Asta, krever dette egne opplysninger om den tilgjengelige bruksversjonen i Asta, et eget lagringssystem for DIP-er med tilknytning til Asta og en praktisk inngang til lagringssystemet fra Asta.

Om originalversjonen av en DIP også skal lagres i digitalt depot, er et enkelt valg som kan treffes i hvert enkelt tilfelle – så langt en DIP bygger på én enkelt AIP. Mer problemtisk blir det i tilfeller hvor en DIP bygger på en kombinasjon av AIP-er. DIAS-prosjektet har ikke vurdert hvordan lagringen av slike konsoliderte DIP-er skal eller kan organiseres i digitalt depot. Dette vil også melde seg som et tema ved registrering i Asta, og det vil være naturlig å starte med å vurdere løsninger for dette.

5.3.6 Logging av hendelser i forvaltningssystemets database

Oversikten nedenfor viser de viktigste depotoperasjonene som skal være logget som hendelser i forvaltningssystemets database (ESSArch). Disse vises sammenstilt med hendelser som også skal finnes i event-loggen "Depotoperasjoner" i en AIP/AIU utenfor PREMIS (2) og Events som skal inngå i PREMIS (3), jf. kapittel 4.3.4, foran. De to sistnevnte hendelsestypene er nedenfor beskrevet noe mer detaljert enn i kapittel 4.3.4.

Alle forekomster av hendelser i oversikten er basert på Arkivverkets behandlingsprosess. Andre arkivdepoter vil både kunne fjerne og tilføye forekomster.

	Hendelse	***(1) Logg i ESSArch***	***(2) Depot-operasjoner***	***(3) Events i PREMIS***	***Kommentar***
Initiell mottakskontroll					
1	Mottak av SIP	x	x		
2	Mottak av info.xml (medfølgende fil til SIP)	x	x		
3	Integritetskontroll av SIP og info.xml	x	x		Sjekksum-generering og sjekksum-verifisering
4	Visuell kontroll av SIP	x	x		Kontroll av at avtalte filer inngår i SIP
5	Virussjekk av SIP og info.xml	x	x		Virus-skanning etter karantene-periode
6	Generering av operasjonslogg(er)	x	x		Logg for operasjoner utført i mottaksfasen

	Hendelse	***(1) Logg i ESSArch***	***(2) Depot-operasjoner***	***(3) Events i PREMIS***	***Kommentar***
7	Overføring av SIP, info.xml og operasjonslogg til ESSArch	x	x		Tilrettelegging for import til ESSArch
Innsjekking til ESSArch					
8	Innsjekking av SIP til ESSArch	x	x		Import
9	Integritetskontroll og validering ved innsjekking	x	x		Sjekksum-generering/ Sjekksum-verifisering
10	Endring av saksbehandler	x			
11	Lagring av SIP	x	x		Lagring før kopiering til arbeidsområde
12	Kopiering av SIP og info.xml til arbeidsområde	x			Utsjekking for testing på arbeidsområde
13	Innsjekking av SIP etter testing på arbeidsområde	x			Import av SIP og test-dokumentasjon
14	Differansekontroll etter test. Kontroll av innsjekk-ede filer fra arbeidsområde	x	x		Sammenligning av importert og lagret SIP
15	Generering av operasjonslogg(er)	x	x		Logg for operasjoner ved inn- og utsjekking
Test av SIP på arbeidsområde					
16	Utpakking av materialet	x			
17	Kontroll av hver enkelt fil	x	x		En hendelse pr. test som utføres.
18	Endring i materialet	x	x	AIP	En hendelse for hver endring som utføres.
19	Innhenting av tilleggs-informasjon	x	x		En hendelse for hver innhenting (inkl tillatelser til å gjøre endringer i materialet.
20	Endring av metadata	x	x	AIP/ AIU	En hendelse for hver endring som utføres.
21	Bearbeiding av katalogstruktur	x	x		
22	Brev til arkivskaper	x			Godkjenning eller avvisning.
23	Klargjøring av materiale for pakking	x			Klargjøring for pakke-generering etter import til ESSArch
24	Generering av operasjonslogg(er)	x	x		Dokumentasjon av testoperasjoner
25	Klargjøring for innsjekking til ESSArch	x	x		Import – styrt fra ESSArch

	Hendelse	***(1) Logg i ESSArch***	***(2) Depot-operasjoner***	***(3) Events i PREMIS***	***Kommentar***
Skape og innlemme AIP/AIC					
26	Utveksling av informasjon med andre systemer	x			Utveksling med ASTA og evt. andre systemer
27	Generere AIP(-1)	x	x	AIC	tar-pakket METS-fil
28	Generere evt. AIU	x	x	AIC	tar-pakket METS-fil
29	Generere AIP-0 av SIP			AIC	Pakking av uendret mottatt SIP
30	Generere AIC	x	x	AIC	METS-fil
31	Kontroll av pakking	x			Forvaltningssystemets kontroll av at pakkingen har gått rett.
32	Innlegging i lagrings-systemet (DSM)	x	x	AIC	Innlegging av AIC med tilknyttede pakker
33	Generere operasjonslogg	x	x		
Vedlikehold av arkivpakke					
34	Kopiering fra DSM til kontrollområde	x			Kopiering av AIP og tilhørende AIC
35	Kopiering til arbeidsområde	x	x		
36	Utpakking av AIP	x			
37	Formatkonvertering	x	x	AIP	
38	Endring av klausulering	x	x	AIP/ AIU	Kan være nedgradering, oppheving av klausul, endring fra deponering til avlevering, etc.
39	Kassasjon av materiale	x	x	AIP	Av hele eller deler.
40	Innsjekking til ESSArch etter operasjoner	x	x		Import – styrt fra ESSArch
41	Pakking og innlegging i DSM. Endret AIP lagres som tillegg. Endret AIC oppdaterer foregående	x	x	AIC	Innlegging av AIC med tilknyttede pakker
42	Generere operasjonslogg	x	x		
Annet vedlikehold		x			
43	Sjekksumkontroll i DSM – Digitalt sikringsmagasin	x			
44	Rapportering	x			
45	Dekryptering av hele pakken	x			
46	Fjerning av en AIU/AIP	x	x		Fjerning eller sletting av en pakke i DSM.

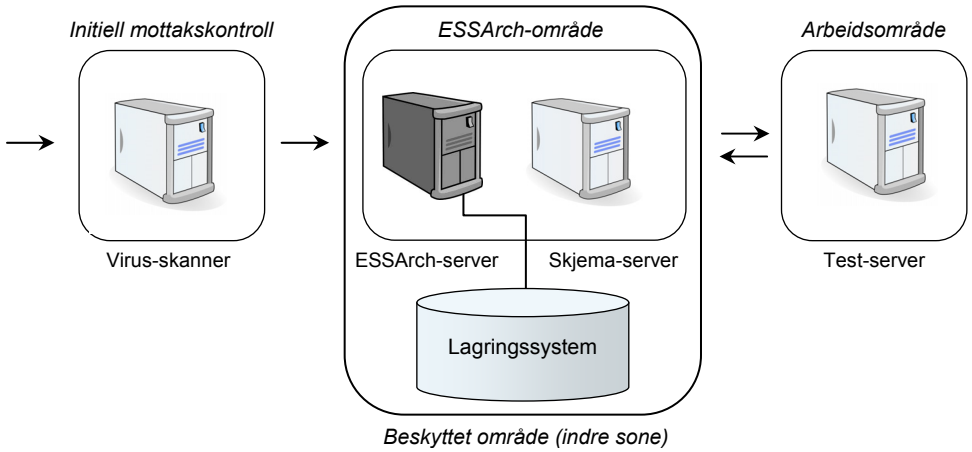
	Hendelse	***(1) Logg i ESSArch***	***(2) Depot-operasjoner***	***(3) Events i PREMIS***	***Kommentar***
47	Validering av en digital signatur	x			
Skape en DIP					
48	Kopiering fra DSM til arbeidsområde (via kontrollområde)	x	x		Kopiering av AIP og tilhørende AIC
49	Tilpasse innhold for DIP	x	x		
50	Innsjekking til ESSArch (med operasjonslogg)	x	x		Import – styrt fra ESSArch
51	Generering av DIP med sjekksumm(er)	x	x	x	
52	Eksport av DIP til utvekslingsområde	x	x		
53	Oppdatering av AIC	x	x	AIC	
54	Lagring av AIC i DSM, evt. sammen med DIP dersom denne skal lagres	x	x	AIC	Behovet for å lagre en DIP i DSM vil være varierende.
55	Generere operasjonslogg	x	x		
Mediemigrering					
56	Redigere migreringsjobb	x			
57	Gjennomføre medie-migrering	x	x		
58	Validere migrering	x	x		

5.4 ESSArchs teknologiplattform og krav til utstyrsanskaffelser

ESSArch er skrevet i programmeringsspråket Python, og systemet kjører på et Linux operativsystem (CentOS, x86_64). ESSArch bruker MySQL som database.

Minimumskravet til anskaffelser ved en ESSArch-installasjon er en *ESSArch-server*. Dette er Linux-serveren som ESSArch-programvaren installeres på. Riksarkivet har for sin produksjonsløsning anskaffet 3 servere i tillegg til denne. Figuren nedenfor viser server-installasjonene i tilknytning til Riksarkivets løsning.

Figur: Teknisk plattform for ESSArch forvaltningssystem



Test-serveren er en kraftfull applikasjonsserver for arbeidsområder med programvare for testoperasjoner, konvertering, verifisering og dokumentasjon. Test-serveren administrerer også rettigheter til testområder.

Skjema-serveren gjør xml-skjemaene i DIAS – nærmere bestemt DIAS-METS, DIAS-PREMIS, EAD, EAC-CPF og ADDML – tilgjengelige for bruk i Riksarkivets lukkede rød/rosa sone. Den kan også betegnes som en "falsk" Internett-server. Nye skjemaer installeres på serveren når det foreligger oppdaterte versjoner. Serveren håndterer også DNS navnetjeneste og NTP tidstjeneste. Det vil være mulig å installere ESSArch uten en egen skjema-server.

Virus-skanneren sjekker SIP-er for virus og annen ondartet programvare ved mottak. I Riksarkivet brukes den også til sjekksum-generering av SIP-er ved mottak.

I tillegg til denne server-konfigurasjonen har Riksarkivet anskaffet en redundant brannmur for trafikken mellom soner. Denne er ikke inntegnet i figuren.

Følgende øvrige anskaffelser er foretatt i tilknytning til Arkiverkets digitale depot:

- lagringsløsning med disk-systemer og tape-roboter med tilhørende styringssystemer,
- fiber og svitsjer til datarom,
- separat kabling mellom datarom og dedikert kontormiljø,
- kortlesere for arbeidsrom og rom med nettverkselektronikk,
- vpn-løsning for statsarkiv,
- dedikerte PC-er for kommunikasjon med digitalt depot (inkl. statsarkivene).

6. DIAS FORVALTNINGSFORUM

6.1 Etablering av DIAS forvaltningsforum

Ved prosjektets slutt besluttet DIAS-partnerne å omgjøre styringsgruppen til et permanent styringsforum for å forvalte DIAS-prosjektets standarder og produkter. Styringsforumet ble opprettet med virkning fra 01.04.2012, og ivaretok inntil 31.05.2012 denne funksjonen i tillegg til å være DIAS-prosjektets styringsgruppe.

Et eget prosjekt under styringsforumet for å planlegge etableringen og organiseringen av DIAS forvaltningsforums operative enheter ble startet 01.04.2012. Også prosjektet for å etablere DIAS-forumet ble startet med økonomisk støtte fra Norsk kulturråd. Etableringsprosjektet forutsettes gjennomført innen 01.04.2013.

6.2 Oppgaveramme for DIAS-forumet

Til støtte for det statlige og kommunale DIAS brukermiljøet er det behov for et permanent forum med tilknyttede operative enheter for å ivareta følgende oppgaver:

- vedlikeholde og videreutvikle DIAS-standardene (xml-skjemaene),
- forvalte ESSArch og ESSArch-avtalene for det samlede brukermiljøet,
- bygge DIAS- og ESSArch-kompetanse i fag- og driftsmiljøer.

Oppfølgingsoppgavene knyttet til *DIAS-standardene* vil i utgangspunktet være disse:

- vurdere behov for endringer eller tillegg i xml-skjemaer ut fra en vurdering av behov og praktisk-økonomiske implikasjoner,
- iverksette endringer i skjemaer eller styre iverksettelsen,
- vurdere implementering av endringer i relasjon til ESSArch,
- ivareta samordningsbehov med det svenske riksarkivet og andre.

Det må i denne sammenheng også vurderes om det bør etableres et forvaltningsregime uavhengig av DIAS-forumets operative enheter for å vedlikeholde DIAS-METS og DIAS-PREMIS som nasjonale standarder.

Oppfølgingsoppgavene i forhold til *ESSArch* omfatter for det første *vedlikehold* av systemet, nærmere bestemt:

- overvåke Riksarkivarens vedlikeholdsavtale for ESSArch med leverandøren – som en sentral avtale også for DIAS-prosjektet og det samlede DIAS-miljøet,
- etablere og drifte et sentralt apparat for mottak av ESSArch-feilmeldinger og andre henvendelser fra brukermiljøer,
- vurdere om feilmeldinger skal oppfølges og videreformidles til leverandøren med utgangspunkt i Riksarkivarens vedlikeholdsavtale,

- om nødvendig simulere en innmeldt feilsituasjon på et anlegg i Riksarkivets driftsmiljø for å skaffe grunnlag for en videre vurdering,
- gjøre avtaler med leverandøren om implementering når det foreligger oppgraderte programmoduler.

Vedlikeholdsavtalen for ESSArch omfatter også *brukerstøtte*. En sentral for mottak og videreformidling av feilmeldinger forutsettes å besvare henvendelser fra brukere, og om nødvendig videreformidle dem til leverandøren.

Videreutvikling av ESSArch blir et eget tema. Det er behov for en operativ enhet for vedlikehold som også kan legge fram forslag til utviklingstiltak med utgangspunkt i hendelser og avdekkede behov.

Når det gjelder *opplæring og kurs* må et elementært behov dekkes: Det må finnes en instans som sørger for at det foreligger materiell og ressurser som grunnlag for opplæring. En slik instans vil ha også en naturlig rolle mht. å arrangere kurs for fag- og driftspersonell.

Kjerneoppgavene for DIAS forvaltningsforum vil være vedlikehold og videreutvikling av DIAS-prosjektets produkter. Oppfølging av de kommunale brukermiljøene vil være tilleggsoppgaver. Men de sistnevnte forutsettes å kunne nedtrappes etter en etableringsfase. Det vil derfor også være behov for å utarbeide en utviklingsplan for DIAS-forumets oppgaver, og definere tidspunkter for å evaluere utviklingen i forhold til planen.

VEDLEGG 1: OVERSIKT OVER PROSJEKTDELTAKERE

Medlemmer av DIAS-styringsgruppen:

Anne Mette Dørum, Riksarkivet
Arnt Ola Fidjestøl, IKA Møre og Romsdal
Hans-Herman Fischer, Riksarkivet
Ole Gausdal, Riksarkivet *(leder for styringsgruppen)*
Karin Gjelsten, Bergen byarkiv
Kari Remseth, IKA Trøndelag
Olav Hagen Sataslåtten, Riksarkivet
Tore Somdal-Åmodt, Oslo byarkiv, senere Byrådsavd. for finans
Trond Sirevåg, Riksarkivet *(prosjektleder)*

F.o.m. august 2011 har Tor Eivind Johansen fra KDRS – Kommune-arkivinstitusjonenes digitale ressurssenter – vært fast deltaker på møtene.
F.o.m. januar 2012 har Robert Kalleberg fra Oslo byarkiv deltatt på møtene.

Medlemmer av DIAS-prosjektgruppen:

Hans Fredrik Berg, Riksarkivet
Jan Tore Helle, Bergen byarkiv
Terje Furuseth, Statsarkivet i Hamar (fra februar 2011)
Frode Kirkholt, Oslo byarkiv
Petter Pedryc, IKA Trøndelag
Terje Pettersen-Dahl, Riksarkivet
Trond Sirevåg, Riksarkivet *(prosjektleder)*
Børge Strand, Statsarkivet i Hamar (inntil januar 2011)
Torbjørn Aasen, IKA Møre og Romsdal

Medlemmer av DIAS-referansgruppen:

Lars Gaustad, Nasjonalbiblioteket
Endre Grøtnes, Difi - Direktoratet for forvaltning og IKT
Tor Eivind Johansen, KDRS (inntil august 2011)
Torleif Lind, LLP - Landslaget for lokal- og privatarkiv
Kjetil Reithaug, KS IKT-Forum
Øyvind Rekdal, Norsk arkivråd
Synne Stavheim, ABM-utvikling/Norsk kulturråd
Thomas Sødring, Høgskolen i Oslo
Sigmund Evjen, Oslo kommune/Byrådsavdeling for finans og næring

Deltakere fra styringsgruppen og prosjektgruppen:
Ole Gausdal, Olav Hagens Sataslåtten, Hans Fredrik Berg, Terje Pettersen-Dahl og Trond Sirevåg

Medlemmer av ESSArch-prosjektgruppen:

Hallstein Bakken, Riksarkivet/DD-seksjonen
Arne-Kristian Groven, Riksarkivet/Elark-seksjonen
Jan Tore Helle, Bergen Byarkiv
Helge Holte, Riksarkivet/DD-seksjonen
Tor Eivind Johansen, KDRS
Anthony Lærdal, Riksarkivet/DD-seksjonen
Terje Pettersen-Dahl, Riksarkivet/DD-seksjonen *(prosjektleder)*
Petter Svendsen, Riksarkivet/DD-seksjonen
Stian Skindlo, Riksarkivet/IT-avdelingen
Jørgen Skjånes, Riksarkivet/IT-avdelingen

Medlemmer av ESSArch-referansegruppen:

Mats Berggren, Riksarkivet i Sverige
Terje Furuseth, Statsarkivet i Hamar
Jan Tore Jørgensen, Statsarkivet i Kristiansand
Frode Kirkholt, Riksarkivet/IT-avdelingen
Tommy Maurud, Oslo Byarkiv
Olav Alexander Mjelde, Bergen byarkiv
Peter Pedryc, IKA Trøndelag
Terje Pettersen-Dahl, Riksarkivet/DD-seksjonen *(prosjektleder)*
Line Richardsen, KS-IKT
Jan Børre Solvik, IKA Trøndelag
Børge Strand, Statsarkivet i Hamar
Jacob Wisløff, Statsarkivet i Kongsberg
Torbjørn Aasen, IKA Møre og Romsdal

Prosjektets medlemmer av koordineringsgruppen med ESSArch-leverandøren:

Olav Hagen Sataslåtten, Riksarkivet *(leder)*
Tor Eivind Johansen, KDRS
Terje Pettersen-Dahl, Riksarkivet *(prosjektleder)*

VEDLEGG 2: SAMLET REGNSKAP FOR DIAS-PROSJEKTET

Status pr. 08.06.2012:

Inntekter:	*2010*	*2011*	*2012*	*Sum inntekter*
Bevilgning fra ABMU	1 000 000			
Overført fra LLP		355 000		
Overført fra IKA-Trøndelag		103 000		
Tilskudd fra Riksarkivaren			169 900	
				1 627 900

Utgifter:				
DIAS hovedprosjekt:	*2010*	*2011*	*2012*	*Sum utgifter*
Konsulentbistand: XML-skjemaer		202 000		202 000
Konsulentrapport: forvaltningssystemer		93 500		93 500
Møter og møtereiser	115 800	174 200	93 300	383 300
Konferanser og studiereiser	176 000			176 000
Materiell	11 400	7 100		18 500
DIAS: ESSArch-prosjektet:				
ESSArch-programutvikling			661 100	661 100
Møter og møtereiser		35 000	58 500	93 500
	303 200	*511 800*	*812 900*	
				1 627 900

Kommentar:

I 2012 ble kr. 250.000 mottatt som ekstra tilskudd til DIAS-prosjektet fra Riksarkivaren. Pr. 08.06.2012 var kr. 81.100 udisponert. Disse resterende midlene ble overført til det nye samarbeidsprosjektet DIAS forvaltningsforum, og skal dekke gjenstående reiseregninger o.a. fra sluttfasen i DIAS- og ESSArch-prosjektet. I DIAS-regnskapet er tilskuddet fra Riksarkivaren derfor redusert med kr. 81.100 til kr. 169.900.