



Handleiding - SODA

Auteur: Stephanie Aertsen, Renée Cambré, Frederik Geysen, Nastasia Vandepierre,
Tom Cobbaert, Bert Lemmens en & Prof. dr. Frank Scheelings
Versie van 5-02-2014

Inhoudsopgave

1. Beleid	3
1.1 Acquisitiebeleid	5
1.2 Preserveringsbeleid	8
1.3 Communicatieplan	11
1.4 Ordeningsplannen	13
2. Zelfevaluatie	16
3. Ontvangst aanbod	19
3.1 Registreer het aanbod	21
3.2 Is de overdrager de wettige eigenaar?	23
3.3 Toetsing aan het acquisitieprofiel?	24
4. Prospectie	26
4.1 Voorbereiding prospectie	29
4.2 Interview overdrager	31
4.3 Visuele controle	34
4.4 Systeem- en bestandsanalyse	36
5. Sluit overeenkomst	40
6. Overdracht	46
6.1 Administratieve overdracht	48
6.1.1 Toekennen Persistent Identifier	50
6.1.2 Overdrachtslijst	52
6.1.3 Breng organisatiestructuur in kaart	54
6.1.4 Registratie	56
6.2 Fysieke overdracht	58
6.2.1 Overdracht via netwerk	61
6.2.2 Overdracht via draagbaar medium	64
6.2.3 Door de overdrager	66
6.2.4 Door de archiefdienst	69
7.10 Veiligheidskopie	71
7. Schonen	75
7.1 Controleer de integriteit	77
7.2 Decomprimeer gecomprimeerde bestanden	79
7.3 Verwijder versleutelingen	81
7.4 Verwijder geïnfecteerde bestanden	83
7.5 Verwijder dubbels	86
7.6 Verwijder lege mappen	88
7.7 Verwijder systeembestanden	90
7.8 Selectie	92
7.9 Uniformiseer de bestandsnamen	94
8. Formalisering	98

9. Creëer een containerbestand	100
10. Opslag	102

1. Beleid

(Laatst gewijzigd: 24-01-2014)



Wat?

In deze eerste fase van het Stappenplan voor de Overdracht van Digitaal Archief is het de bedoeling dat men een beleid ontwikkelt voor de aanvaarding, verwerving en preservering van digitale archieven.

Waarom?

Organisatiestructuren en werkprocessen met het op oog digitaal archief moeten beleidsmatig verankerd zijn, ongeacht de grootte van organisatie en budget.

Wanneer?

Het uitstippelen of bijsturen van het beleid is dus een eerste voorwaarde om een succesvolle overdracht en bewaring te organiseren. Het is dan ook de eerste stap van [SODA](#).

Hoe?

Het beleid wordt hier opgedeeld in vier onderdelen:

1. het [acquisitiebeleid](#) richt zich op de verwerving van digitale archieven;
2. het [preserveringsbeleid](#) betreft logischerwijs de bewaring van de data in hun context;
3. het [communicatieplan](#), gericht op de proactieve omgang tussen de archiefdienst en haar potentiële archiefvormers;
4. de [ordeningsplannen](#).

Meer lezen?

[COOK, T., Byte-ing Off What You Can Chew: Electronic Records Strategies for Small Archival Institutions, Archifacts, 2004](#)

1.1 Acquisitiebeleid

(Laatst gewijzigd: 23-01-2014)



Wat?

Het acquisitiebeleid voor digitaal archief is een onderdeel van de algemene acquisitiepolitiek die de archiefdienst voert. Acquisitie is het geheel van activiteiten van een archiefbeheerder gericht op het overnemen in bruikleen of eigendom van archiefbescheiden in een archiefbewaarplaats. We maken een onderscheid tussen actief en passief acquisitiebeleid.

- Bij actieve acquisitie gaat de archiefdienst zelf op zoek naar te verwerven archieven;
- bij passieve acquisitie wacht de archiefdienst een aanbod af.

Het acquisitiebeleid bestaat uit een inhoudelijk acquisitieprofiel en technische bepalingen. Beiden moeten op beleidsniveau vastgelegd worden.

Waarom?

Een acquisitieprofiel is - indien duidelijk omschreven - een nuttig instrument om te bepalen of een aangeboden archief voor acquisitie in aanmerking komt. Het biedt de archiefdienst de mogelijkheid aan doelgerichte collectievorming te doen. Technische bepalingen helpen het [preserveringsbeleid](#) uit te werken en te handhaven.

Wanneer?

Het opstellen van een acquisitiebeleid maakt deel uit van de eerste stap binnen SODA, namelijk [1. Beleid](#). Het is een voorwaarde voor een succesvolle overdracht en bewaring.

Hoe?

1. Inhoudelijk acquisitieprofiel:

- Voer een bestandsanalyse uit van het reeds verworven archief.
 - Kwantificeer eerst je collectie: aantal archieven, aantal strekkende meter, aantal gigabytes...
 - Ga vervolgens na hoe volledig je collectie is, over welke periode ze loopt het, wat is het historisch belang ervan is.
- Onderzoek de historische ontwikkelingen in je eigen werkgebied. Om praktische redenen beperkt dit zich tot een literatuurstudie.
- Vergelijk ten slotte de resultaten van de bestandsanalyse met die van het historisch onderzoek.
 - Deze vergelijking laat toe de representativiteit te staven van zowel de reeds verworven collectie als van de nog te verwerven bestanden.
 - Bij passieve acquisitie kunnen deze gegevens gebruikt worden ter ondersteuning van de beslissing om het aangeboden archief al dan niet te aanvaarden.
 - Bij actieve acquisitie worden ze gebruikt om doelgericht naar bepaalde archieven op zoek te gaan.

2. Technische bepalingen:

- Ga na voor welke types van [bestandsformaten](#) en gegevensdragers je archiefdienst is uitgerust met het oog op duurzame bewaring.
 - Houd hierbij niet alleen rekening met de technische infrastructuur, maar ook met de aanwezige kennis, expertise en financiële middelen.
 - Maak een zo uitgebreid mogelijke lijst op van [bestandsformaten](#) en digitale dragers die geschikt zijn voor acquisitie. Deze bepalingen kunnen ook aan bod komen in het [preserveringsbeleid](#).

Meer lezen?

[Archiefwiki, acquisitie](#)

[AIMS Work Group. 2012. AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship, Collection Development, p. 4](#)

[DE HART, C., Een kwestie van kiezen. Acquisitieplannen- en profielen in het Nederlandse archiefwezen, onuitgegeven scriptie, Amsterdam, 2012](#)

[Oud papierprijs of cultureel erfgoed? Naar een gecontroleerde verwerving en afvloeiing van archieven en documenten. Rijckheyt, centrum voor regionale geschiedenis, Heerlen, 2008](#)

[HILTON, C., THOMPSON, D., Collecting born-digital archives at the Wellcome Library, Ariadne, Nummer 50, 2007](#)

[HILTON, C., THOMPSON, D., Further experiences in collecting born-digital archives at the Wellcome Library, Ariadne, Issue 53, Oktober 2007](#)

[LUGER, T., Handreiking voor het schrijven van een collectieplan, Instituut Collectie Nederland, Amsterdam, 2008](#)

1.2 Preserveringsbeleid

(Laatst gewijzigd: 22-01-2014)



Wat?

[Preserveringsbeleid](#) is het geheel van activiteiten dat zorgt voor het technische en intellectuele behoud van digitale informatieobjecten.

Waarom?

Een archiefdienst moet over een uitgeschreven preserveringsbeleid beschikken om een duurzame bewaring van digitaal archief te kunnen garanderen.

- Hierdoor vergroot de kans op aanbod van digitaal archief.
 - Enerzijds is het een instrument voor de interne werking.
 - Anderzijds werkt dit het vertrouwen van overdragers in de hand.
- Bovendien is het een instrument dat willekeur tegengaat.
 - Continuïteit van beheer wordt verzekerd.
 - Bij wisseling van personeel, blijven de procedures dezelfde.

Wanneer?

Het preserveringsbeleid en de daarbij horende procedures moeten opgesteld zijn vooraleer de archiefdienst digitaal archief kan ontvangen.

Hoe?

In een preserveringsplan moeten ten minste de volgende zaken worden uitgewerkt:

- De manier waarop digitaal archief overgedragen wordt ([overdracht](#));
- De manier waarop digitaal archief geschoond wordt ([schonen](#));

- De manier waarop veiligheidskopieën en back-ups gemaakt en bewaard worden;
- Wat er gebeurt met bestandsdragers die mee overgedragen worden (afstoten of bewaren);
- Wat er gebeurt met overbodige, geïnfecteerde en corrupte bestanden, dubbels, enzovoort;
- Wat er gebeurt met vertrouwelijke en gevoelige informatie;
- Hoe bestanden bewaard worden (digitaal depot) en een welke bewaarstrategie daarbij gehanteerd wordt (emulatie, concersie, migratie,...);
- Welke bestanden toegankelijk gemaakt worden en de manier waarop;
- Bepalingen met betrekking tot intellectuele rechten van zowel het archiefvormer als de archiefdienst (archief vs. de metadata door de archiefdienst aangemaakt);
- Een beschrijving van de hardware en software die gebruikt worden.

Een preserveringsbeleid kan opgesteld worden aan de hand van de Preservation Planning Tool [PLATO](#). Deze online toepassing doorloopt vier stappen:

1. het bepalen van vereisten
2. het onderzoeken van alternatieven
3. het analyseren van alternatieven
4. een preserveringsstrategie

Opgelet!

In het preserveringsbeleid kunnen ook de technische bepalingen met betrekking tot de infrastructuur, middelen en expertise van de archiefdienst worden opgenomen. Hieruit leidt men af welke categorieën van digitale bestanden de archiefdienst in staat is om te aanvaarden en duurzaam te bewaren: Een onderdeel wat ook al aan bod kwam in het technische luik van het [acquisitiebeleid](#).

De meeste van deze bepalingen worden ook opgenomen in de [overeenkomst](#). Zodoende is de overdrager op de hoogte van mogelijke ingrepen die op het digitaal archief kunnen gebeuren.

Meer lezen?

[AIMS Work Group. 2012. AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship, Collection Development](#)

[Archiefwiki, ED3 \(Eisen Duurzaam Digitaal Depot\)](#)

[BOUDREZ, F., Digitaal Archiveren en Digitale Duurzaamheid, Expertisecentrum DAVID vzw, Antwerpen, 2009](#)

[BOUDREZ, F., DEKEYSER, H., Handboek: Digitaal archiefbeheer in de praktijk, Bewaarstrategieën, Stadsarchief Antwerpen, 2004](#)
[Digital Preservation Policies: Guidance for archives, The National Archives, Surrey, 2011](#)
[PLATO, Preservation Planning Tool](#)
[PARADIGM, Workbook on Digital Private Papers, Digital Preservation Strategies, Bodleian Library, 2007](#)

1.3 Communicatieplan

(Laatst gewijzigd: 22-01-2014)



Wat?

In deze stap maak je je beleid kenbaar aan de buitenwereld:

- het grote publiek
- stakeholders
- (potentiële) archiefoverdragers

Waarom?

Door proactief te communiceren vermijdt men steeds op de zelfde vragen te moeten antwoorden. Bovendien worden het professionele imago van je instelling en een vlotte samenwerking met de overdragers gestimuleerd.

Wanneer?

Communicatie met overdragers begint reeds vóór het eerste contact. Het is een onderdeel van de permanente werking van je archiefinstelling.

Hoe?

Voorzie online de nodige documentatie met betrekking tot het acquisitie- en conserveringsbeleid van de archiefdienst.

- Acquisitieprofiel
- Bepalingen m.b.t. uitstel van overdracht
- Bepalingen m.b.t. samenwerking met andere archiefdiensten
- Bepalingen m.b.t. selectie

- Bewaarstrategie

Voorzie ook tips waarmee archiefoverdragers zich kunnen voorbereiden op de [prospectie](#) en hun eigen archiefbeheer kunnen organiseren (zie [DigiGids@home](#), [DigiGids@work](#) en [ordeningsplannen](#)).

Communiceer volgens welke procedures digitaal archief kan worden overgedragen. Vermeld ook contactgegevens van de verantwoordelijke(n) voor deze processen.

Meer lezen?

[THOMAS, S., Guidelines for library staff assisting donors to prepare their personal digital archives for transfer to NSLA libraries, National Library of Australia, 2011.](#)

1.4 Ordeningsplannen

(Laatst gewijzigd: 23-01-2014)



Wat?

In deze stap probeert men potentiële overdragers aan te moedigen om hun archieven correct te ordenen. Hiertoe voorziet men [ordeningsplannen](#) als instrument waarmee toekomstige overdragers structuur kunnen geven aan hun archieven. Een ordeningsplan is een structuur voor de ordening van het archief, gebaseerd op de taken en activiteiten binnen de organisatie.

In het kader van het project dat tot dit stappenplan heeft geleid, werden ordeningsplannen opgesteld voor drie soorten verenigingen: theatergezelschappen, sportverenigingen en belangenverenigingen (zie [DigiGIDS@work](#)).

- Onder 'theatergezelschap' verstaat men een organisatie die zich toelegt op het creëren, repeteren en spelen van theatervoorstellingen voor een publiek.
- Met 'sportvereniging' wordt een organisatie bedoeld, met als primaire doelstelling de beoefening van sport en het ondersteunen van atleten.
- 'Belangenvereniging' worden gedefinieerd als organisaties die een duidelijk omschreven maatschappelijk idee, doel of belang verdedigen. Dit kan een politieke actiegroep zijn, maar ook een migrantenorganisatie, halebivereniging, automobilistenvereniging, ...

Waarom?

Een goed ordeningsplan is een groot voordeel met het oog op bewaring van de context van alle bestanden. Het ordeningsplan verleent de medewerkers van een organisatie een logische structuur voor de ordening van hun digitale bestanden. Het vereenvoudigt de doorzoekbaarheid en de bewaring van documenten, waardoor alle stappen in het

acquisitie- en conserveringsproces vlotter kunnen verlopen.

- De documenten zijn op een overzichtelijke manier geordend, waardoor ze sneller teruggevonden worden.
- Door documenten over een bepaalde zaak samen te bewaren, ontwikkel je volledige dossiers die je de toegang geven tot alle informatie m.b.t. die zaak. Het bijeenbrengen van alle gerelateerde informatie geeft ieder document een duidelijke context.
- Elk document krijgt een duidelijke plaats in de structuur. Bovendien worden dubbels vermeden.
- Door het gebruik van hetzelfde ordeningsprincipe weet iedere medewerker waar hij zijn documenten moet bewaren. Bij afwezigheid van een personeelslid wordt het voor andere personeelsleden meteen ook eenvoudiger om zijn werk verder te zetten.
- Het vereenvoudigt het zoekingswerk bij het opmaken van beleidsplannen en subsidiedossiers.

Wanneer?

- Het opstellen van een ordeningsplan kan gebeuren binnen een project, waarbij je bijvoorbeeld voor je meest relevante types archiefvormers modellen uitwerkt.
- Het opstellen van ordeningsplannen kan ook ad hoc gebeuren, op basis van een vraag van een archiefvormer.

Hoe?

Algemene richtlijnen en uitgangspunten voor dit plan:

1. Het plan is opgebouwd van algemeen naar bijzonder.
2. Maak een onderscheid tussen interne werking en externe taken.
3. Probeer alle documentatie rond specifieke activiteiten en taken samen te houden voor een efficiënte werking.
4. Plaats documenten maar op één plaats. Verkies een snelkoppeling in plaats van dubbel klasseren als een document op verschillende plaatsen thuishoort.
5. Het plan hoort een weerspiegeling van de taken en activiteiten van de organisatie te zijn.
6. Verbind het ordeningsplan met het klassement voor papieren documenten zodat het effectief één bestand vormt. Dit geeft je een beter overzicht en toegang tot het volledige dossier.

De uitgewerkte [ordeningsplannen](#) voor theatergezelschappen, sportverenigingen en belangenverenigingen zijn breed opgevat. Onderdelen die niet toepasbaar zijn op de

organisatie, kunnen weggelaten worden. Raadpleeg [DigiGIDS@work](#) voor meer informatie bij gebruik van het ordeningsplan. Hier vindt men ook suggesties voor bewaartermijnen. Daarnaast wordt aangeduid welke onderdelen gevoelige en persoonlijke informatie kunnen bevatten en op welke onderdelen auteursrechten rusten. Dit heeft gevolgen voor de toegankelijkheid en openbaarheid van de stukken (zie stap 5: [Sluit overeenkomst](#)).

Meer lezen?

[AMVB: Ordeningsplannen Ordeningsplan, Archiefwiki](#)

[BOUDREZ, F., Digitaal Archiveren: richtlijn & advies nr.3. Mappenstructuur en bestandsnamen voor digitale documenten](#)

[SOYEZ, S. en LAYEUX, M., Orde of wanorde? Basisregels en aanbevelingen voor de ordening van documenten bij uw instelling, Rijksarchief, 2011](#)

[VANDENBERGHE, A., Richtlijnen mappenstructuur, Zorgbedrijf Antwerpen, 2011
Gemeenschappelijk klassement, Bestuurszaken](#)

[JACQUEMIN, M., Archiveren... Wat? Archiveren... Waarom? Archiveren... Hoe?,
Rijksarchief, s.d.](#)

[Hoe lang moet ik documenten bewaren?, Vlaanderen.be](#)

2. Zelfevaluatie

(Laatst gewijzigd: 23-01-2014)



Wat?

Evalueer je organisatie om te achterhalen of ze klaar is voor een duurzame verwerving en bewaring van digitale archieven. In deze stap worden zowel het [beleid](#), als je mogelijkheid om dit in de praktijk om te zetten, geëvalueerd.

Zorg bij de evaluatie voor input van zowel het management als van de vakgebonden experts binnen je organisatie.

Waarom?

Door een cyclisch proces van evaluatie en remediëring komen de sterke en zwakke punten van je archiefdienst aan de oppervlakte, waarna je aan de minpunten kan werken totdat je organisatie in staat is tot duurzame digitale verwerving en bewaring.

Wanneer?

De archiefdienst evalueert zichzelf vooraleer ze digitaal archief aanvaardt.

Hoe?

De evaluatie gebeurt aan de hand van het [Scoremodel digitale duurzaamheid](#). Dit model is een online toepassing ontwikkeld door [DEN](#) en [PACKED vzw](#). Aan de hand van vragenlijsten geeft het aan welke de sterke en zwakke punten zijn van je organisatie en formuleert het aanbevelingen voor het verkleinen van deze risico's. Na het doorlopen van de toepassing wordt een rapport gegenereerd. Dit rapport laat de archiefdienst toe te beoordelen of ze klaar is voor het aanvaarden van overdrachten. Nadat de zwakke punten zijn bijgewerkt, wordt het Scoremodel opnieuw toegepast. Doorloop dit cyclische

proces totdat de omstandigheden voor duurzame verwerving en bewaring gunstig zijn.

Voor het doorlopen van deze toepassing kan men een account aanmaken; het is echter ook mogelijk de procedure anoniem te doorlopen. Voor beide methoden staan instructies op de [home page](#). Vanuit je account kan je je eerder gegenereerde rapporten raadplegen.

Scoremodel

Maak een nieuw rapport aan. Vul de gegevens van je organisatie in en geef het rapport een titel. Klik op *volgende*.

Doorloop in de verschillende secties. Dit zijn zeven pagina's met multiple choice vragen. Vul bij alle vragen een antwoord in. De vragen zijn opgedeeld in de volgende secties:

1. **Mandaat en beleid:** In deze fase positioneer je je instelling: hoe kadert het bewaren van digitale bestanden in de doelstellingen van de organisatie?
2. **Bewaarstrategie:** In deze fase worden de bewaarmethoden in grote lijnen onderzocht.
3. **Kennis en organisatie:** In deze fase wordt nagegaan in hoeverre de juiste expertise aanwezig is in de organisatie.
4. **Opslagbeheer:** In deze fase wordt de fysieke bewaring onderzocht.
5. **Opname:** In deze fase worden de [ingest](#)-procedures onderzocht.
6. **Planning en kwaliteitscontrole:** In deze fase wordt onderzocht in welke mate de preservingsstappen gedocumenteerd en gecontroleerd verlopen.
7. **Toegankelijkheid:** In deze fase wordt gepeild naar de toegankelijkheid van de bewaarde digitale documenten.

Aan elke vraag wordt een risiconiveau toegekend: hoog, normaal of laag (zie voorbeeld). Hoe hoger het niveau, hoe belangrijker de implicaties.

Daarnaast wordt bij elke vraag meer toelichting gegeven aan de hand van contextinformatie, duiding betreffende het risico en één of meerdere voorbeelden. Deze toelichtingen vind je in de verschillende tabbladen naast de vraag (zie voorbeeld).

Nadat je de zeven secties hebt doorlopen, wordt een samenvattend overzicht weergegeven (zie voorbeeld). Dit is een lijst van scores die je behaalde op de afzonderlijke secties. Klik op *Genereer* om een eindrapport te maken.

Het rapport voorziet een grafische weergave van je resultaten, een overzicht van je werkpunten (*actieplan*) en een overzicht van je antwoorden (*resultaten*). Het hoofdstuk *actieplan* formuleert suggesties naar mogelijke acties ter verbetering van je beleid (zie

voorbeeld). Het gegenereerde rapport kan je opslaan in [PDF](#)-formaat.

Met de acties die het Scoremodel bij je minpunten formuleert, kan je vervolgens aan de slag gaan. Remedieer je mindere punten en doorloop het Scoremodel vervolgens opnieuw. Herhaal het proces totdat je een gunstige score behaalt.

Opgelet!

Interpreteer een resultaat van 50% niet als geslaagd! Streef naar een zo hoog mogelijke score. Wees streng voor jezelf en houd hierbij rekening met het aangegeven risiconiveau.

3. Ontvangst aanbod

(Laatst gewijzigd: 22-01-2014)



Benodigheden

- [SODA Invulformulier](#)
- [Acquisitieprofiel](#)

Wat?

In deze fase wordt een concreet aanbod van digitaal archief geregistreerd. Daarnaast moet uit een analyse van het geregistreerde archief blijken of de overdrager de wettige eigenaar van het archief is, en of het archief past in het acquisitieprofiel van de instelling. Pas wanneer op beide vragen een positief antwoord naar voren komt, kan men de overdracht aanvaarden.

Waarom?

Als archiefdienst is het niet mogelijk om alles te bewaren. Wanneer het aangeboden archief inhoudelijk of technologisch niet voldoet aan je acquisitieprofiel, is het archief niet relevant voor die archiefdienst. In dit geval verwijst je de overdrager beter door naar een andere archiefinstelling.

Ongeacht de uiteindelijke beslissing om een aanbod al dan niet te aanvaarden, is het interessant om de contactgegevens van de overdrager en/of de archiefvormer te registreren. Deze kunnen in de toekomst van pas komen in het kader van actieve acquisitie of wanneer het acquisitieprofiel of de technische mogelijkheden van het archief gewijzigd zijn.

Wanneer?

Deze stap in de procedure hangt logischerwijs samen met het moment waarop de archiefdienst een aanbod krijgt in het kader van passieve acquisitie, of wanneer men archief tracht te verwerven in het kader van actieve acquisitie.

Hoe?

Zie verdere uitwerking in de volgende stappen:

1. [Registreer het aanbod](#)
2. [Is de overdrager de wettige eigenaar?](#)
3. [Toetsing aan het acquisitieprofiel](#)

Meer lezen?

[THOMAS, S., Faster Access to archival collections in NSLA libraries. Guidelines for providing rapid access to recent receipts, National Library of Australia, Maart 2011](#)

[THOMAS, S., Guidelines for library staff assisting donors to prepare their personal digital archives for transfer to NSLA libraries, National Library of Australia, 2011](#)

3.1 Registreer het aanbod

(Laatst gewijzigd: 23-01-2014)



Benodigheden

- [SODA invulformulier](#)

Wat?

Via een aanvraagformulier komt een aanbod binnen voor de overdracht van digitaal archief. Dit formulier komt overeen met het onderdeel *ontvangst aanbod* in het [SODA invulformulier](#). Dit kan je eventueel in vereenvoudigde vorm aanbieden.

Waarom?

De registratie van het aanbod legt belangrijke metadata vast. Zelfs wanneer acquisitie achteraf niet mogelijk blijkt, heb je via registratie informatie opgeslagen die later van pas kan komen, wanneer bijvoorbeeld het [acquisitiebeleid](#) wordt herzien.

Wanneer?

Het aanbod wordt geregistreerd op het moment dat je het ontvangt.

Hoe?

Registreer de gegevens met betrekking tot het aangeboden archief, de overdrager en de archiefvormer in het [SODA invulformulier](#). Door de gegevens hier in te vullen, worden ze automatisch gemapped naar een [EAD/PREMI](#)S-metadataprofiel. Vul dit tabblad van het formulier correct en volledig in. Neem bij onduidelijkheid contact op met de potentiële overdrager en vraag om verduidelijking.

Opgelet!

ISIL-code Bewaarplaats:

- [ISIL](#) is de afkorting voor 'International Standard Identifier for Libraries and Related Organizations'. Aan de hand van deze code kan elke instelling uniek geïdentificeerd worden. Een ISIL code kan je aanvragen via <http://isil.kbr.be/home.php?lang=nl>.

Datering [ISO 8601](#):

Volgens deze ISO-norm worden tijdsbepalingen op een gestandaardiseerde manier weergegeven, in dalende orde van grootte.

- Voor data betekent dit:
 - <jaartal (4 cijfers)>-<maand (2 cijfers)>-<dag (2 cijfers)>
 - JJJJ-MM-DD
 - Bijvoorbeeld: 1989-02-22
- Periode tussen twee data weergeven:
 - <begindatum>/<einddatum>
 - JJJJ-MM-DD/JJJJ-MM-DD
 - Bijvoorbeeld 2012-04-10/2013-01-23

De datum van het digitaal archief kan voor verwarring zorgen bij de registratie. De datum van creatie van bestanden wordt niet automatisch bewaard. De begin- en einddatum die je in het aanvraagformulier registreert, wordt beter gebaseerd op de data van de laatste wijziging van de bestanden.

Wanneer blijkt dat het aangeboden materiaal uit meerdere archieven bestaat, maak je hierin een onderscheid. Vul dan voor elke archiefvormer een aparte fiche in.

3.2 Is de overdrager de wettige eigenaar?

(Laatst gewijzigd: 22-01-2014)



Wat?

Onderzoek of de overdrager de wettige eigenaar van het aangeboden archief is.

Waarom?

Je kan alleen archief aanvaarden uit handen van de persoon of instelling die het recht heeft om het over te dragen.

Wanneer?

Deze stap vindt plaats nadat de aanvraag tot overdracht geregistreerd werd.

Hoe?

Dit doe je door de relatie tussen de overdrager en de archiefvormer te controleren. Wanneer uit dit onderzoek blijkt dat de overdrager niet de eigenaar is, en geen recht heeft om over de overdracht te beslissen, kan deze vanzelfsprekend niet aanvaard worden.

3.3 Toetsing aan het acquisitieprofiel?

(Laatst gewijzigd: 22-01-2014)



Benodigheden

- [Acquisitieprofiel](#)

Wat?

Het aangeboden archief wordt inhoudelijk getoetst aan het acquisitieprofiel van de instelling. Wanneer het hieraan niet voldoet, wordt de overdrager doorverwezen naar andere archieven.

Waarom?

Je kan enkel archief aanvaarden op wanneer het past binnen de inhoudelijke en technische vereisten van je acquisitieprofiel.

Wanneer?

Toets het aangeboden archief aan het acquisitieprofiel nadat je het geregistreerd hebt.

Hoe?

Vergelijk het aangeboden archief met het acquisitieprofiel. Hou hierbij rekening met:

- De inhoud van het aangeboden archief:
 - Hebben de bestanden een waarde op lange termijn?
 - Passen de bestanden inhoudelijk in het acquisitieprofiel?
- De context van het aangeboden archief
 - Wie is de archiefvormer?

- Hebben de bestanden nog bewijswaarde?
- Is het archief exemplarisch voor een bepaalde periode, gebeurtenis of stroming in de geschiedenis?
- De structuur van het aangeboden archief
 - Hebben de bestanden een ordening waaruit bepaalde bevoegdheden van de archiefvormer blijken?
- Technologische toestand
 - Past de technologische toestand van de bestanden in de mogelijkheden van de archiefinstelling?

Opgelet!

Bij hybride archieven (een combinatie van analoog en digitaal gevormd archief) moet men kiezen welke versie bijgehouden wordt.

Wanneer de archiefvormer digitaal aangemaakte en bewaarde bestanden afprint en bewaart, zijn de analoge bestanden slechts schaduwarchief. Wanneer deze papieren documenten niet geannoteerd zijn, kan het digitale bestand als moederbestand worden beschouwd en worden de papieren documenten niet langer bewaard.

Meer lezen?

[PARADIGM, Workbook on Digital Private Papers, Appraisal and Disposal, Bodleian Library, 2007](#)

4. Prospectie

(Laatst gewijzigd: 23-01-2014)



Benodigheden?

- [SODA invulformulier](#)
- [Draagbaar werkstation](#)
- Eventueel digitale camera
- Eventueel dictafoon

Wat?

Voer een prospectie uit om de technische staat van het archief te beoordelen. Besluit nadien of je voor de duurzame bewaring van dit archief de nodige middelen en infrastructuur in huis hebt.

Waarom?

Prospectie is nodig om een overwogen en gemotiveerde beslissing inzake acquisitie mogelijk te maken. Bovendien krijg je in deze fase een beeld van de acties die nodig zullen zijn voor de acquisitie en bewaring.

Wanneer?

Het moment waarop de prospectie doorgaat, is afhankelijk van het acquisitiebeleid.

- Bij een actieve acquisitie wordt actief geprospecteerd naar interessante archieven en archiefvormers.
- Bij een passieve acquisitie start de prospectie pas vanaf het moment dat er een aanbod is.

Deze handleiding gaat uit van een passieve acquisitie.

Hoe?

Aan de prospectie gaat een voorbereiding vooraf. Na deze voorbereiding vindt de eigenlijke prospectie plaats in drie stappen.

1. Ten eerste is er een [interview met de overdrager](#),
2. ten tweede vindt een [visuele controle](#) plaats,
3. ten slotte wordt een [systeem- en bestandsanalyse](#) uitgevoerd.

Binnen deze drie fasen wordt gepeild naar verschillende factoren, die nodig zijn om het archief in een technische context plaatsen. De factoren waarmee rekening wordt gehouden, zijn:

- De inhoud en het bereik: de omvang en vorm van het digitale archief en de relatie tot het analoge archief.
- Het ICT-beheer van de archiefvormer
- De toestand en de eigenschappen van de noodzakelijke hardware, software en hulpbestanden

Documenteer de resultaten in het [SODA invulformulier](#).

Toets deze gegevens af aan je [acquisitieprofiel](#) en bepaal aan de hand hiervan of de overdracht aanvaard kan worden. Wanneer de technische afweging negatief uitdraait, wordt het archief geweigerd. De archiefdienst kan in dit geval geen duurzame bewaring van de digitale archieven garanderen.

Opgelet!

In de praktijk krijgt een archiefdienst mogelijk te maken met een aanbod dat inhoudelijk perfect past binnen het acquisitieprofiel, maar waarvan de bewaring technisch nog niet haalbaar is (bijvoorbeeld omdat het grotendeels uit verouderde bestanden bestaat die niet geopend kunnen worden). Hier kan de inhoudelijke afweging primeren tegenover de technische.

- Idealiter is in het [acquisitiebeleid](#) vastgelegd in welke mate de archiefdienst technische uitzonderingen op het acquisitieprofiel aanvaard.

Eventueel kan je in dat geval om uitstel van overdracht vragen. Zo heb je de tijd om de overdracht technisch beter voor te bereiden. Dit impliceert echter dat extra afspraken

moeten worden gemaakt. Deze worden vastgelegd in de [overeenkomst](#).

Meer lezen?

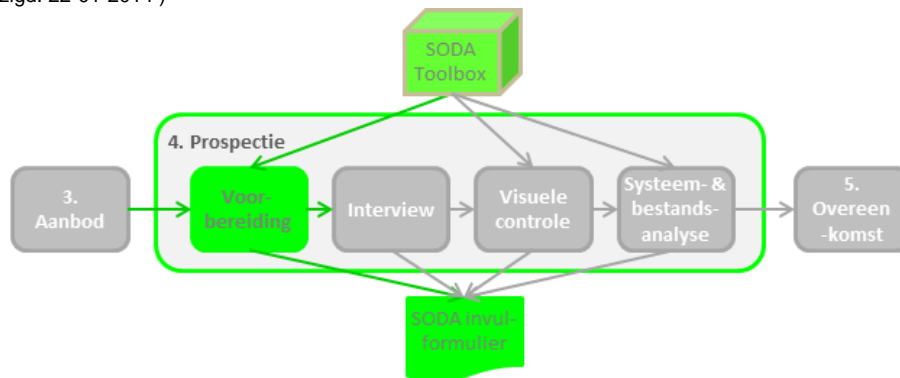
[AIMS Work Group. 2012. AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship, Collection Development](#)

[Digital Lives: Report of Interviews With The Creators of Personal Digital Collections](#)

[HILTON, C., e.a. 'Trust me, I'm an archivist : experiences with digital donors', Ariadne, Issue 65, oktober 2010](#)

4.1 Voorbereiding prospectie

(Laatst gewijzigd: 22-01-2014)



Wat?

Tijdens deze stap bereidt de archiefinstelling zichzelf en de overdrager voor op de prospectie.

Waarom?

Het doel van deze stap is de prospectie bij de overdrager ter plaatse zo vlot mogelijk te laten verlopen.

Wanneer?

De voorbereiding voor de prospectie kan starten van zodra een aanbod voor overdracht binnen komt.

Hoe?

Bereid jezelf voor op de prospectie.

- Bestudeer de reeds verworven informatie betreffende de overdrager en het over te dragen archief. Zo kan je je een beeld te vormen van te verwachten aandachtspunten.
- Vul het eerste deel van het [SODA invulformulier](#) (Checklist prospectie - 2.1 Identificatie) in.
- Controleer of de nodige prospectietools zijn geïnstalleerd op je [draagbaar werkstation](#).
 - Bijvoorbeeld [DROID](#) of [ManifestMaker](#).

Voorzie daarnaast de overdrager van richtlijnen aan de hand waarvan hij je prospectiebezoek kan voorbereiden. Idealiter stel je deze richtlijnen online ter beschikking.

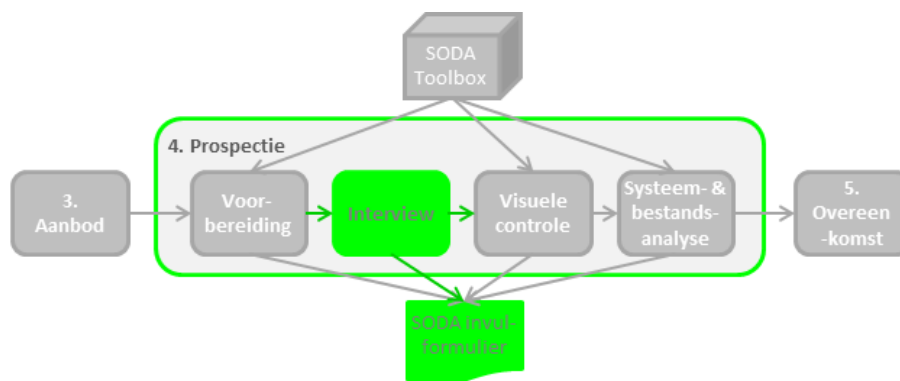
- De overdrager moet hierbij vooral een aantal zaken verzamelen
 - Alle dragers waarop zich over te dragen archief bevindt of kan bevinden
 - Alle paswoorden en encryptiesleutels waarmee over te dragen archiefbestanden versleuteld zijn
 - Documentatie over de werking van noodzakelijke software, hardware en hulpbestanden
 - Informatie over het systeembeheer en softwarebeheer van de organisatie.

Meer lezen?

[THOMAS, S., Guidelines for library staff assisting donors to prepare their personal digital archives for transfer to NSLA libraries, National Library of Australia, november 2011](#)

4.2 Interview overdrager

(Laatst gewijzigd: 23-01-2014)



Benodigheden?

- [SODA invulformulier](#) (Checklist Prospectie)
- Eventueel een dictafoon

Wat?

Een eerste fase van de eigenlijke prospectie is het interviewen van de overdrager met betrekking tot het aangeboden digitaal archief. Hier worden vragen gesteld die peilen naar de technische kenmerken van het digitale archief. De antwoorden worden geregistreerd in het [SODA invulformulier](#).

Waarom?

Het interview heeft als doel de inhoud, het bereik en de oude orde van het archief te achterhalen. Tijdens het interview probeer je zoveel mogelijk achtergrondinformatie over de organisatie en haar archief te verzamelen.

Sommige gegevens, zoals paswoorden, kunnen enkel door middel van het interview achterhaald worden. Daarom is het interview een noodzakelijke stap.

Bovendien komen er tijdens een gesprek met de overdrager vaak nog allerlei zaken naar boven waaraan de overdrager niet meteen dacht. Het interview is daarnaast een ideale gelegenheid voor de archiefdienst om prospectie uit te voeren naar nieuw archief of naar aanvullingen op het aangeboden archief.

Wanneer?

De overdrager wordt geïnterviewd wanneer de [voorbereiding](#) op de prospectie is afgerond.

Hoe?

Stel tijdens het interview ten minste de volgende vragen, en documenteer de antwoorden in het [SODA invulformulier](#) (checklist prospectie):

Inhoud en bereik (2.2)

- Welke documenten worden analoog opgemaakt?
 - Welke documenttypes worden gebruikt?
- Welke documenten worden digitaal opgemaakt?
 - Welke bestandtypes worden gebruikt?
- Wat zijn de inhoudelijke relaties tussen het analoge en het digitale archief?
- Zijn er overlappingen tussen het analoge en het digitale archief?
 - Zijn er digitale documenten die systematisch worden geprint?
 - Zijn er analoge documenten die systematisch worden gedigitaliseerd?
- Welke talen worden gebruikt in het archief?
- Vergeet niet na te gaan of bij het archief ook de volgende zaken behoren:
 - E-mails (webmail, outlook, ...)
 - Digitale agenda's
 - Webpagina's of Blogs
 - Informatie op sociale netwerksites
 - Informatie op foto/document sharing sites

Organisatie ICT (2.3)

- In welk jaar werd de overstap gemaakt van analoog naar digitaal?
- Wie was/is verantwoordelijk voor systeembeheer en -ondersteuning?
- Wie was/is verantwoordelijk voor softwarebeheer en -updates?
- Wie was/is verantwoordelijk voor back-ups?
 - Wanneer werden digitale bestanden gearchiveerd?

Architectuur ICT (2.4)

- Welke toepassingen worden gebruikt voor het maken en beheren van documenten?
- Welke gebruikersnamen of -profielen worden op de systemen of op bepaalde software

gebruikt?

- Welke paswoorden zijn noodzakelijk om toegang te krijgen tot bepaalde gebruikersprofielen, bestanden of systemen?
 - Werden bepaalde bestanden versleuteld d.m.v. encryptie?

Software (2.6)

- Welke documentatie over de software is er beschikbaar?
- Welke software updates hebben plaatsgevonden?

Registreer de antwoorden van de overdrager in het [SODA invulformulier](#) onder het tabblad 'Prospectie'.

Om het interview vlot te laten voorlopen, kan je het ook opnemen. Op die manier kunnen de antwoorden achteraf rustig geanalyseerd en gedocumenteerd worden.

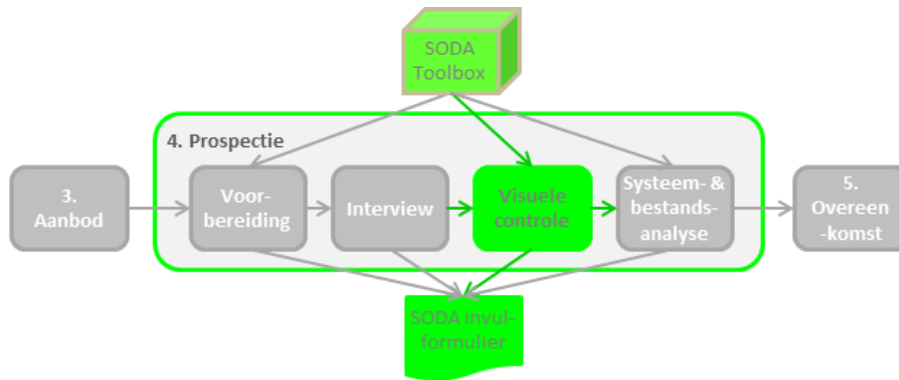
Meer lezen?

[AIMS Work Group. 2012. AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship, Collection Development](#)

[THOMAS, S., Guidelines for library staff assisting donors to prepare their personal digital archives for transfer to NSLA libraries, National Library of Australia, november 2011](#)

4.3 Visuele controle

(Laatst gewijzigd: 23-01-2014)



Benodigheden

- Checklist Prospectie ([SODA invulformulier](#))
- Eventueel digitale camera

Wat?

Tijdens de visuele controle documenteer je hetgeen je met het blote oog kan vaststellen. Tijdens deze fase zet je dus geen computers aan.

Waarom?

Deze stap laat toe:

- een controle uit te voeren op de juistheid van de informatie die je uit het interview haalde
- de fysieke bawaarlocatie te bestuderen en risico's te identificeren.

Wanneer?

De visuele controle vindt plaats na het [interview met de overdrager](#) en gaat vooraf aan een [systeem- en bestandsanalyse](#).

Hoe?

Noteer alle kenmerken die visueel vastgesteld kunnen worden. Maak eventueel foto's om latere verwerking of controle van deze fase mogelijk te maken.

Tijdens de visuele controle documenteer je de volgende bevindingen in het [SODA invulformulier](#)

Inhoud en bereik (2.2)

- Hier wordt gepeild naar de bewaringsconditie van het digitale archief. Concreet houdt dit in dat je gaat kijken in welke omstandigheden de externe dragers bewaard worden.

ICT beheer (2.3)

- Onderzoek op welke media de bestanden oorspronkelijk bewaard werden
- Onderzoek ook (voor zover dit vast te stellen is zonder de computer aan te zetten) welke toepassingen gebruikt werden voor het creëren en het beheren van documenten.

Hardware (2.5):

- Controleer de hardware die exclusief toegang verleent tot bepaalde bestanden.
 - Om welke types hardware gaat het? (server, pc, externe harde schijf, dvd, ...)
 - Wat is het merk van de hardware?
 - Welke poorten zijn beschikbaar om verbinding te maken met de hardware?
- In deze fase kan je aan alle hardware al een uniek nummer toekennen, om er later correct naar te kunnen verwijzen.

Software (2.6)

- Is er nog beschikbare (analoge) documentatie over de software aanwezig, voor zover die software exclusief toegang verleent tot bepaalde bestanden.

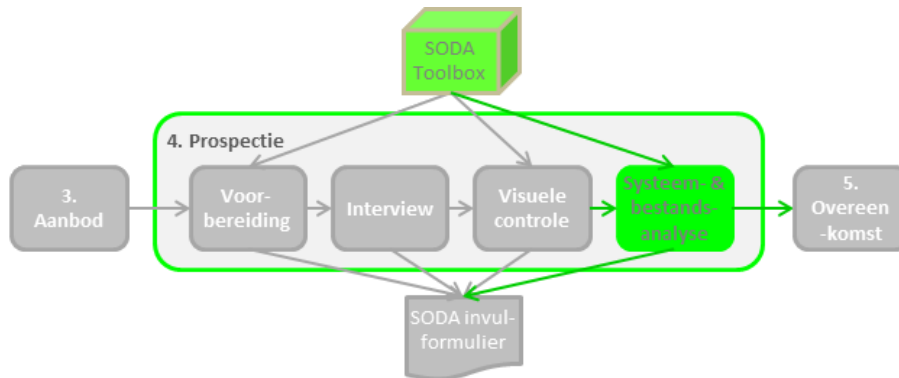
Hulpbestanden (2.7)

- Is er nog beschikbare documentatie over de hulpbestanden aanwezig?

Toets tegelijk je visuele vaststellingen aan de antwoorden die de overdrager gaf op de overeenkomstige vragen tijdens het interview. Vraag om verduidelijking waar nodig.

4.4 Systeem- en bestandsanalyse

(Laatst gewijzigd: 23-01-2014)



Benodigheden?

- [draagbaar werkstation](#)
- [SODA invulformulier](#)

Wat?

Indien je toegang krijgt tot het systeem kan je een systeem- en bestandsanalyse uitvoeren. Tijdens deze analyse worden de bestanden geopend en wordt in het systeem gekeken, zowel manueel als met behulp van prospectietools op je [draagbaar werkstation](#). De resultaten worden gedocumenteerd in het [SODA invulformulier](#) (Checklist prospectie). Hierbij worden de gegevens uit het interview en de visuele controle getoetst aan je bevindingen.

Waarom?

Een systeem- en bestandsanalyse is de enige manier om je eerder verkregen informatie met zekerheid te bevestigen. Bovendien krijg je hier al een zicht op de eigenlijke archiefdocumenten, hun structuur en hun toestand. Deze analyse is noodzakelijk voor een gemotiveerde beslissing inzake acquisitie.

Wanneer?

De systeem-en bestandsanalyse is de laatste stap van de [prospectie](#).

Hoe?

Analyseer de onderstaande zaken. Documenteer je bevindingen in het [SODA invulformulier](#) (checklist prospectie).

ICT beheer (2.4)

- Zijn de systeemdatum en tijd correct ingesteld?
 - Documenteer dit zonder de tijdsinstellingen aan te passen!
 - Je vindt de tijdsinstellingen terug in het configuratiescherm van je apparaat.
- Controleer welke bestanden op welke media worden bewaard.
- Controleer welke toepassingen werden gebruikt voor het maken en beheren van documenten.
- Controleer de paswoorden

Hardware (2.5)

- Controleer de hardware die exclusief toegang verleent tot bepaalde bestanden. Met deze informatie kan je gemakkelijk de specificaties terugvinden indien dit nodig zou zijn voor toekomstige conserveringshandelingen.
- Welke specifieke instellingen gebruikt de hardware?
- Hoe groot is de opslagcapaciteit van de hardware?

Software (2.6)

- Maak een overzicht van het besturingssysteem en andere systeemsoftware (systeemondersteuningsprogramma's zoals utilities of compressieprogramma's,... en systeemontwikkelingsprogramma's) met aanduiding van de versie zoals die geïnstalleerd is in de hardware. Vermeld hierbij de updates die het besturingssysteem doorheen de tijd ontvangen heeft.
- Geef aan elke software een uniek nummer om correcte verwijzingen mogelijk te maken.
- Om welke types software gaat het?
 - Wat is de officiële naam van de software?
 - Wat is de precieze versie van de software?

Hulpbestanden (2.7)

- Geef elk hulpbestand een uniek nummer om correct te kunnen verwijzen.
- Om welke hulpbestanden gaat het? (validatiebestand, stylesheet, codec, font, ...)
 - Wat is de naam van het hulpbestand?

Tijdens de bestandscontrole kijken we naar de eigenlijke archiefdocumenten. De

bestandsanalyse gebeurt deels manueel en deels met behulp van tools.

Ga manueel na hoe groot de omvang van het archief is:

- Wat is de omvang van de digital born bestanden (in MB, GB)?
- Wat is de omvang van de gedigitaliseerde bestanden (in MB, GB)?
- Wat is dan de totale omvang van het digitale archief (in MB, GB)?

Tools worden in deze fase gebruikt voor:

- Het berekenen van [checksums](#)
- Het identificeren van [bestandsformaten](#)
- Het creëren van een [directory list](#)

Twee tools die deze mogelijkheden aanbieden zijn:

- [DROID](#) (Windows, Linux, OSX)
- [ManifestMaker](#) (Windows, Linux, OSX)

Installeer de nodige tool op je [draagbaar werkstation](#), of gebruik de virtual box. Deze bevat [DROID](#).

Documenteer in het [SODA invulformulier \(2.8\)](#)

- Welke prospectiehandelingen worden gesteld
- Welke tools je daarbij hanteert
- Wanneer deze handelingen werden gesteld
- Of deze handelingen succesvol waren
- Welke opmerkingen hierbij worden gemaakt

Voeg kopieën toe van de logs die hierbij werden aangemaakt!

Opgelet!

- Wanneer het gaat om verouderde dragers waarvan de overdrager niet over de corresponderende leesapparatuur beschikt, zal de archiefdienst geen bestandsanalyse kunnen uitvoeren vooraleer de bestanden op het werkstation staan (na de [Fysieke overdracht](#)).
- Noteer naast het merk en type van de computer ook basisgegevens van de configuratie, zoals processor, RAM geheugen en grafische kaart. Het laatste, de

grafische kaart, is enkel belangrijk wanneer het computer veel grafische bestanden bevat (vb. architectenarchief, grafische vormgeving, beeldarchief, ...).

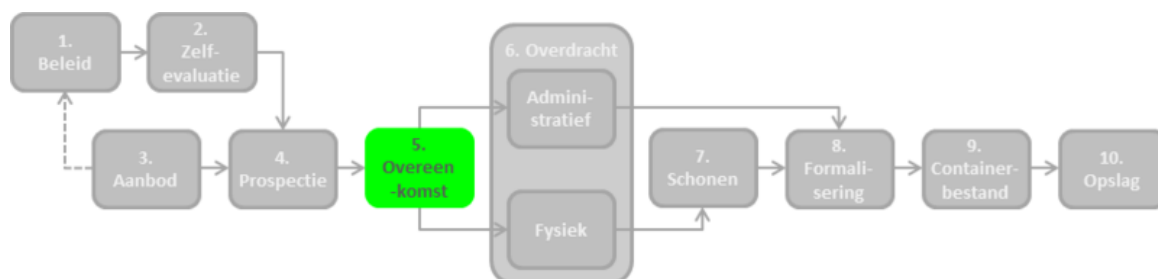
- Het kan zinvol zijn om, mits toestemming van de overdrager, screenshots te maken. Dit kan helpen om systeeminformatie vast te leggen en dienen als visueel hulpmiddel.
- Wanneer je merkt dat de datum verkeerd is ingesteld, documenteer dit zonder de datum te veranderen. De datum aanpassen zorgt op termijn voor heel wat verwarring m.b.t. de datum van creatie van de digitale bestanden, dus laat de datum onaangepast!
- Vergeet niet de logs te bewaren die werden aangemaakt bij het toepassen van de tools!

Meer lezen?

[PARADIGM, Workbook on Personal Digital Archives, Working with record creators, Bodleian Library, 2007](#)

5. Sluit overeenkomst

(Laatst gewijzigd: 23-01-2014)



Benodigheden

[SODA invulformulier](#)

Wat?

Een overdracht is de procedure waarbij een archiefbeheerder archiefbestanddelen onder de verantwoordelijkheid van een andere archiefbeheerder plaatst. In tegenstelling tot overheden, zijn particuliere archiefvormers niet verplicht tot het overdragen van hun archief. Voor de meeste modaliteiten betreffende bewaring en vernietiging van deze bestaat geen wettelijke basis. Veel hangt daarom af van de contractuele bepalingen.

Een overdrachtsovereenkomst is het resultaat van een onderhandeling die wordt voorbereid aan de hand van het [SODA invulformulier](#).

Waarom?

Het is noodzakelijk om de rechten en plichten van zowel de overdrager als de archiefinstelling vast te leggen, voordat wordt overgegaan tot de daadwerkelijke overdracht van de bestanden. Hierdoor zijn beide partijen op de hoogte van elkaars verwachtingen én van de wettelijke bepalingen waaraan voldaan moet worden bij het overdragen, bewaren en ter beschikking stellen van het archief.

Wanneer?

De onderhandelingen gebeuren na de prospectie. Pas na het ondertekenen van de overdrachtsovereenkomst door beide partijen kan tot de eigenlijke overdracht worden overgegaan.

Hoe?

1. Voorbereiding
 - Aan de hand van het [SODA invulformulier](#) worden de grote lijnen reeds uitgezet.
 - Ga nu met de overdrager aan tafel zitten, bespreek de volgende punten en schrijf alle afspraken neer in de overeenkomst.
 - Het onderstaande overzicht is slechts indicatief, het werd niet opgesteld door een jurist.
2. Leg vast tussen welke actoren de overeenkomst gesloten wordt.
 - Noteer daarvoor de naam en contactgegevens van de overdrager, archiefvormer en archiefinstelling.
 - Vergewis je ervan dat de overdrager ook effectief de eigenaar van het archief is en alle rechten hierop bezit.
3. Identificatie van het archief
 - Bepaal welke archiefbestanddelen zullen worden overgedragen.
 - Noteer de gegevens die nodig zijn om het over te dragen archief te identificeren en te registreren.
 - Dit zijn de gegevens die worden ingevoerd in het eerste onderdeel van de [checklist overdracht](#).
 - Ga ook na of er materiaal van andere archiefvormers met het archiefbestand vermengd is.
 - Spreek desgevallend af wat hiermee dient te gebeuren.
4. Aard van de overdracht
 - Bepaal of het gaat om een schenking of een bewaargeving.
 - Een schenking is een overdracht in eigendom;
 - bij een bewaargeving blijft de bewaargever de juridische eigenaar over het archief.
 - Stel in het geval van een bewaargeving vast wat de minimumperiode is waarin de archiefdienst over het archief mag beschikken, of leg een vergoeding voor terugname vast. Zo voorkomt men dat de overdrager zijn archief meteen na de ordening of ontsluiting terugvordert.
 - Een schenking is voor de archiefdienst over het algemeen interessanter.
 - Bepaal eveneens of het gaat om een éénmalige overdracht, of om een structurele(?) periodieke overdracht.
 - Geef in het laatste geval ook aan welke aanvullingen zullen volgen en op welke tijdstippen.
5. Fysieke overdracht
 - Bepaal wanneer de administratieve overdracht en de fysieke overdracht zullen plaatsvinden.

- Geef ook aan via welke weg de fysieke overdracht zal plaatsvinden (zie Stap 6: [Overdracht](#)).
 - Via een netwerk of via een draagbaar medium?
 - Door de overdrager of door de archiefdienst?
 - Spreek af dat eventuele bestaande archieftoegangen (ordeningsplannen, oude inventarissen, ...) mee worden overgedragen.
 - Tracht de overdrager er ook toe te overhalen overtollige hard- en software mee over te dragen, voor zover deze noodzakelijk is voor de verdere bewerking van het archief.
 - Geef aan waar het archief en de veiligheidskopieën bewaard zullen worden (zie Stap 10. [Opslag](#)).
 - Op een server van de instelling?
 - Op een externe server?
 - Op een virtuele server?
6. Engagement
- Geef aan welk engagement de archiefdienst aangaat ten aanzien van het archief, de overdrager en de archiefvormer.
 - Men moet zich ten minste engageren voor een duurzame bewaring en het bewaken van de authenticiteit en integriteit van de archiefstukken.
 - Verwijs hierbij ook naar het [preserveringsplan](#) van de instelling.
 - Men kan de intentie verklaren om het archief binnen een redelijke termijn te ontsluiten, al is een onmiddellijke ontsluiting meestal moeilijk in de praktijk te brengen.
7. Uitvoeren van bewerkingen op het archief
- Geef aan welke bewerkingen op het archief zullen worden uitgevoerd in de pre-ingest fase.
 - Maak goede afspraken over het al dan niet verwijderen van dubbels, lege mappen, systeembestanden, geïnfecteerde bestanden, oneigenlijk archief, ... (zie Stap 7. [Schonen](#)).
 - Bepaal de aansprakelijkheid bij problemen in verband met schadelijke of illegale inhoud.
 - Ga na of er door de archiefvormer al een voorafgaande selectie werd uitgevoerd.
 - Bespreek toekomstige bewerkingen op het archief in het kader van selectie, bewaring en ontsluiting.
 - Bepaal welke stukken voor vernietiging in aanmerking komen, en onder welke voorwaarden.
 - Vergeet niet te bepalen wie de verantwoordelijkheid en de kosten zal dragen voor (al dan niet voorziene) bewerkingen in de toekomst.
8. Openbaarheid, auteursrecht en privacy

- Geef aan dat de archiefinstelling het recht heeft om het overgedragen archief te ontsluiten en om het openbaar en toegankelijk te maken.
 - Aanvaard hierbij geen al te hoge openbaarheidstermijnen.
 - Bepaal indien van toepassing specifiek welke stukken (tijdelijk) niet toegankelijk gemaakt mogen worden.
 - De archiefdienst verklaart de auteursrechten, portretrechten en de privacywetgeving te respecteren en erop toe te zien dat onderzoekers het zelfde doen.
 - Verwijs hiervoor naar de vigerende wetgeving en eventueel naar het leeszaalreglement van je archiefinstelling.
 - **Privacywet:** Garandeert de bescherming van de persoonlijke levenssfeer en de verwerking van persoonsgegevens. Deze gegevens mogen niet zonder toestemming verwerkt en gedeeld worden. Personeelsdossiers, persoonlijke evaluaties, arbeidscontracten, medische gegevens en alle stukken in verband met gevoelige (o.a. etnische afkomst, politieke opvattingen, levensbeschouwelijke overtuiging), gezondheids- (alle gegevens betreffende fysieke of psychische gezondheidstoestand) en gerechtelijke gegevens mogen niet met iedereen gedeeld worden.
 - **Auteursrecht:** Beschermde rechten van de maker van een origineel werk. Enkel hij of degenen aan wie hij de rechten overgedragen heeft, mag beslissen hoe, waar en wanneer zijn werk verveelvoudigd en publiek gemaakt wordt. Auteursrecht blijft gelden tot 70 jaar na de dood van de auteur (of langstlevende auteur in het geval van een samenwerking).
 - **Portretrecht:** Bepaalt dat iedere geportretteerde het recht heeft te beslissen of zijn afbeelding al dan niet gepubliceerd of verspreid mag worden. Portretrecht blijft gelden tot 20 jaar na het overlijden van de geportretteerde.
- Omdat digitaal archiveren altijd neerkomt op het reproduceren van de stukken, is het nodig dat men zich bewust is van eventuele auteursrechtelijke bescherming van de stukken. Voor auteursrecht kan de archiefdienst zich beroepen op een uitzondering in de wet in het kader van culturele archiefwerking. Een kopie van een auteursrechtelijk beschermd stuk mag worden opgenomen in een digitaal depot wanneer voldaan is aan alle volgende voorwaarden:
 1. Het werk is op een toegelaten manier publiek gemaakt; dit wil in dit geval zeggen dat de auteur zijn werk ooit publiek heeft gemaakt.
 2. De erfgoedinstelling valt onder het begrip publiek toegankelijke musea, bibliotheken, archieven.
 3. De reproductie heeft de bewaring van cultureel en wetenschappelijk erfgoed tot doel.
 4. De erfgoedinstelling heeft geen oogmerk op economisch of commercieel

voordeel.

5. De reproductie betekent geen hinder aan de normale exploitatie van het werk.
 6. De reproductie betekent geen onredelijke schade aan de wettige belangen van de auteur.
- Voor privacy stelt zich het probleem van het principiële verbod op verwerking van persoonsgegevens. Deze verwerking is wel onder voorwaarden toegestaan voor historische en wetenschappelijke doeleinden. In sommige gevallen mogen persoonsgegevens verwerkt worden. Voorwaarden voor de verwerking van persoonsgegevens:
 1. De betrokkene heeft schriftelijk ingestemd
 2. Er is toelating van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer
 3. De gegevens werden door de betrokkene zelf openbaar gemaakt
 4. De gegevens staan in verband met het publieke karakter van de betrokkene
 5. De betrokkene kan niet gevonden worden
 - Deze lijst is vaak echter voor interpretatie vatbaar. Contacteer bij twijfel steeds de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (zie ook de brochures van de Commissie, infra). Maak in de overeenkomst een onderscheid tussen interne verwerking in de archiefdienst, en wat later aan de buitenwereld wordt getoond in het kader van ontsluiting.

Opgelet

- Stel de overeenkomst op in twee exemplaren.
- Documenteer alle beslissingen en voeg er eventueel voorgaande correspondentie en de [checklist onderhandelingen](#) aan toe.
- Rechtvaardig de verwerving door deze te kaderen in je acquisitiebeleid.

Meer lezen?

Privacy:

- [Wet van 1992 op de bescherming van de persoonlijke levenssfeer](#)
- [Wet op de verwerking van persoonsgegevens](#)
- [Website van de Commissie voor bescherming van de persoonlijke levenssfeer](#)
- [Brochure 'Privacy, een vademecum voor de onderzoeker'](#)
- [Brochure 'Hoe de privacywet toepassen in historisch onderzoek'](#)

Auteurs- en portretrechten:

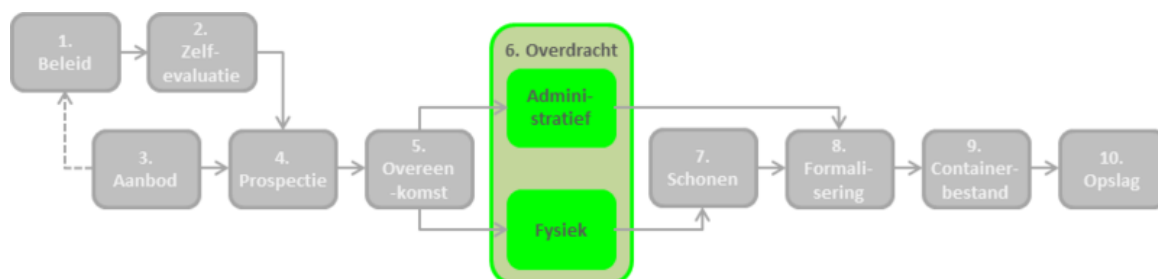
- [Wet van 1994 betreffende het auteursrecht en de naburige rechten](#)
- [Wet van 1998 betreffende de rechtsbescherming van databanken](#)

Juridische aspecten van digitaal archiveren:

- [eDavid handboek](#)
- [eDavid: Contract met betrekking tot verlening van een niet-exclusieve licentie in verband met de vermogensrechten op een auteursrechtelijk beschermd werk aan het digitaal depot](#)
- [Schaule: Organisatorische aspecten bij het bouwen en het beheren van een digitaal depot](#)

6. Overdracht

(Laatst gewijzigd: 23-01-2014)



Benodigheden

- [Overdrachtslijst](#)
- [SODA invulformulier](#)
- [Workstation](#)
- [Draagbaar workstation](#)
- Overdrachtsmedium
- [Leesapparatuur](#)

Wat?

In deze stap wordt de beslissing tot acquisitie uitgevoerd. De overdracht bestaat uit twee processen die deels parallel verlopen:

- de [administratieve overdracht](#)
- de [fysieke overdracht](#)

Wanneer?

De overdracht gebeurt nadat een [overdrachtsovereenkomst](#) is gesloten. Het afronden van de overdracht is het moment waarop, in het geval van een schenking, de eigendom van - en verantwoordelijkheden voor het archief, overgaan op de archiefdienst.

Waarom?

Wanneer het archief niet wordt overgedragen kan de archiefdienst geen goede bewaaromstandigheden verzekeren en is er eigenlijk ook geen sprake van acquisitie.

Hoe?

Zie verdere uitwerking in de volgende stappen:

1. [Administratieve overdracht](#)
2. [Fysieke overdracht](#)
3. [Veiligheidskopie](#)

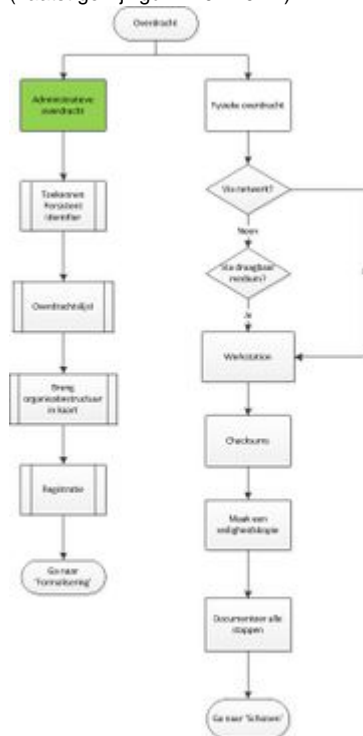
Meer lezen?

[OWENS, T., More Product, Less Process for Born-Digital Collections: Reflections on CurateCamp Processing](#)

[ERWAY, R., You've Got to Walk Before You Can Run: First Steps for Managing Born-Digital Content Received on Physical Media, OCLC Research, 2012](#)

6.1 Administratieve overdracht

(Laatst gewijzigd: 22-01-2014)



Administratieve overdracht

Benodigheden

- [SODA invulformulier](#)
- [Overdrachtslijst](#)

Wat?

Tijdens de administratieve overdracht

- wordt een Persistent Identifier (PID) toegekend aan de digitale objecten;
- wordt de overdrachtslijst gemaakt of gecontroleerd;
- wordt de organisatiestructuur in kaart gebracht;
- worden beschrijvende en technische metadata geregistreerd.

Waarom?

De overdracht moet administratief verwerkt worden om het te registreren in het archiefbeheerssysteem. Het is noodzakelijk voor latere opvolging.

Wanneer?

De administratieve overdracht vindt parallel met de [fysieke overdracht](#) plaats.

Hoe?

Zie verdere uitwerking in de volgende stappen:

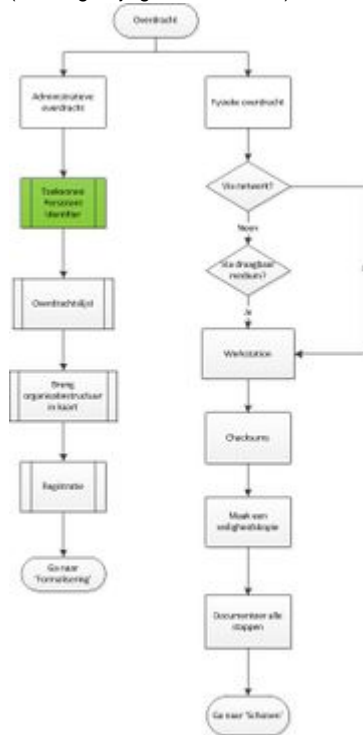
1. [Toekennen Persistent Identifier](#)
2. [Maak overdrachtslijst](#)
3. [Bring organisatiestructuur in kaart](#)
4. [Registreer](#)

Meer lezen?

[PARADIGM, Workbook on Personal Digital Archives, Working with record creators, Bodleian Library, 2007](#)

6.1.1 Toekennen Persistent Identifier

(Laatst gewijzigd: 23-01-2014)



Persistent Identifier

Wat?

In deze fase wordt aan het archief een persistent identifier (PID) toegekend. Een dergelijke PID is een uniek nummer dat aan een digitaal object wordt toegekend. Dit nummer blijft permanent en uitsluitend naar het digitale object verwijzen en staat los van de bewaarlocatie.

In dit geval verwijst de PID naar het archief als geheel. Met het zelfde nummer zal later worden verwezen naar de SIP-container. De PID is in feite de equivalent van het archiefnummer of het overdrachtsnummer bij analogo archief.

Waarom?

Door het toekennen van een PID kan het archief, samen met de metadata, onder alle omstandigheden correct geïdentificeerd worden.

Wanneer?

Ken een persistent identifier toe van zodra het archief op het werkstation is ontvangen (zie [Fysieke overdracht](#)). Vanaf dit moment is het digitale archief onlosmakelijk verbonden met haar PID.

Hoe?

Dit identificatienummer wordt handmatig toegekend. Gebruik hiervoor een gestandaardiseerde en gecodeerde notatie. Leg deze notatie vast in je beleid en wees hierin consequent.

Dit nummer kan de volgende gegevens bevatten:

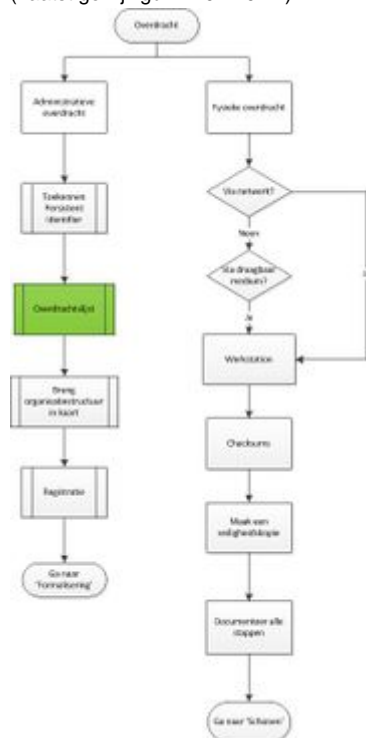
- Een generiek volgnummer
- De afgekorte naam van je instelling
- Het jaartal
- Een code die aangeeft dat het om digitale documenten gaat
- Een code die aangeeft dat het om archief gaat
- ...

Meer lezen?

[Richards, K., White, R., Nicolson, N. & Pyle, R., A Beginner's Guide to Persistent Identifiers](#)
[PARADIGM, Workbook on Digital Private Papers, Administrative and preservation metadata, Bodleian Library, 2007](#)

6.1.2 Overdrachtslijst

(Laatst gewijzigd: 22-01-2014)



Overdrachtslijst

Wat?

Bij de overdracht hoort een overdrachtslijst. In deze overdrachtslijst wordt een opsomming gegeven van de bestanden en/of bestandsdragers die worden overgedragen.

Waarom?

Een overdrachtslijst vormt een essentieel onderdeel van de audit trail van het archief. De audit trail is een controlespoor waarin alle stappen die het archief heeft ondergaan, worden gedocumenteerd.

Het vormt, samen met het nakijken van de checksums, bovendien een eerste controle om na de overdracht te achterhalen of het archief volledig is overgedragen.

Wanneer?

De overdrachtslijst wordt opgesteld vooraleer het archief fysiek wordt overgedragen.

Hoe?

- Wanneer tijdens de [prospectie](#) een [bestandsanalyse](#) is uitgevoerd, kan de directory list dienen als voorlopige overdrachtslijst.
- Is er geen bestandsanalyse gebeurd, stel dan zelf een voorlopige overdrachtslijst op, bijvoorbeeld met een omschrijving van de verschillende bestandsdragers die overgedragen worden.

De (voorlopige) overdrachtslijst wordt in drievoud opgemaakt

- een exemplaar voor de overdrager
- een exemplaar voor de archiefdienst
 - dit kan als voorlopige toegang dienen
- een exemplaar dat aan het overdrachtdossier wordt toegevoegd
 - zowel digitaal als analoog.

Opgelet!

Na het [schonen](#) van het digitale archief wordt een nieuwe directory list gemaakt. Bezorg deze als definitieve overdrachtslijst aan de overdrager; dit zijn de uiteindelijke bestanden die in het depot worden opgenomen. Deze definitieve overdrachtslijst wordt tevens de plaatsingslijst: ze geeft de volgorde weer waarin de bestanden in de bestandscontainer staan.

Meer lezen?

[PARADIGM, Workbook on Personal Digital Archives, Working with record creators, Bodleian Library, 2007](#)

6.1.3 Breng organisatiestructuur in kaart

(Laatst gewijzigd: 22-01-2014)



Breng organisatiestructuur in kaart

Wat?

Het in kaart brengen van de organisatiestructuur sluit deels aan bij het klassieke institutionele onderzoek dat je toepast in het kader van ontsluiting van archieven. In dit onderdeel probeer je de structuur van de organisatie te achterhalen, met aandacht voor taken, handelingen, archiefproductie.

Waarom?

Het inplannen van deze stap op dit moment heeft een aantal voordelen:

- Je documenteert de organisatiestructuur op een moment dat de materie vers in het geheugen zit.
- Je doet dit op een moment dat je de aandacht van de archiefvormer hebt.
- Zo voorkom je dat jij of je opvolger, in het kader van inventarisering, voor later

institutioneel onderzoek van nul moet beginnen.

- Door de organisatiestructuur tijdens de overdracht in kaart te brengen, bespaar je dus op termijn tijd en win je kwaliteit.

Wanneer?

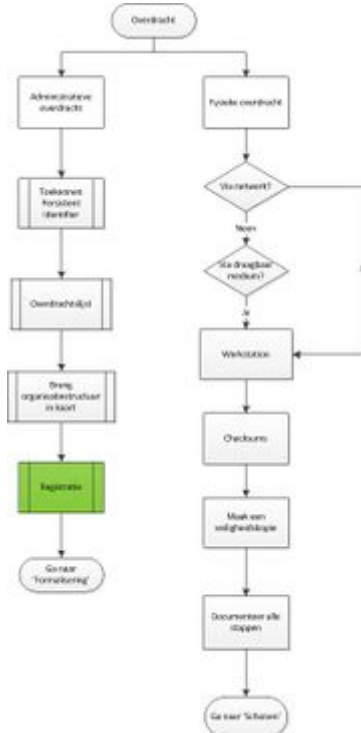
Het in kaart brengen van de organisatiestructuur maakt deel uit van de [administratieve overdracht](#).

Hoe?

Informatie over de organisatie en haar structuur kan je halen uit organogrammen, beleidsdocumenten, het [interview met de overdrager](#) of zelfs (gedeeltelijk) op de website van de organisatie. Uiteraard zullen ook de archiefdocumenten zelf veel (expliciete en/of impliciete) informatie bevatten, maar deze zijn op het moment van overdracht meestal nog niet structureel doorzoekbaar.

6.1.4 Registratie

(Laatst gewijzigd: 22-01-2014)



Registratie

Benodigheden

[SODA invulformulier](#)

Wat?

Registreer alle verzamelde metadata in het [SODA invulformulier](#).

Waarom?

Door te registreren kan je later correct en uniform verwijzen en gefundeerde preserveringsbeslissingen nemen.

Wanneer?

Het registreren van de overdracht maakt onderdeel uit van de [administratieve overdracht](#)

en verloopt parallel met de [fysieke overdracht](#).


Hoe?

1. Documenteer een aantal administratieve gegevens over de fysieke en administratieve overdracht.
 - Het identificatienummer waarmee het overgedragen archiefbestand wordt geregistreerd in het aanwinstenregister.
 - De URI waarmee het archief uniek geïdentificeerd wordt.
 - De naam waarmee het archief wordt aangeduid.
 - De datum waarop het archief fysiek verworven wordt.
 - De datum waarop het archief administratief verworven wordt.
 - Een verwijzing naar de overdrachtsovereenkomst.
2. Documenteer gegevens over het conserveringsniveau dat op het archief van toepassing is.
 - Conserveringshandelingen die van toepassing zijn op het archief.
 - Verantwoording van het conserveringsniveau.
 - Datum waarop het conserveringsniveau werd toegekend.
3. Documenteer de binnenkomst van het archief op de harde schijf van het werkstation.
4. Documenteer het resultaat van de integriteitscontrole van het digitale archief na binnenkomst
5. Documenteer het maken van een veiligheidskopie na de fysieke overdracht.

6.2 Fysieke overdracht

(Laatst gewijzigd: 22-01-2014)



 Fysieke overdracht

Benodigheden

- [Werkstation](#)
- [Draagbaar werkstation](#)
- [Leesapparatuur](#)

Wat?

De fysieke overdracht bestaat uit een aantal stappen die ondernomen worden om het digitale archief te kopiëren naar het [werkstation](#), met aandacht voor de integriteit, de volledigheid en de authenticiteit van het archief. Het digitale archief wordt op het werkstation in een quarantaineomgeving gezet om het veilig verder te bewerken.

Waarom?

Wanneer het archief niet fysiek wordt overgedragen, kan de archiefdienst geen goede

bewaarmstandigheden garanderen en is er geen sprake van acquisitie.

Wanneer?

De fysieke overdracht begint nadat de [onderhandelingen](#) met de overdrager in orde zijn en is afgerond wanneer overgegaan wordt tot het [schonen](#). Ze verloopt parallel met de [administratieve overdracht](#).

Hoe?

Vooraleer je gegevens op je workstation ontvangt, is het raadzaam je virusdefinities te updaten. Gebruik hiervoor een anti-virustool uit je [Toolbox](#). Mogelijkheden zijn:

- [ClamAV](#)
- [ClamWin](#)

Leg tijdens de onderhandeling de manier van overdracht vast. Het is aangewezen om de manier van overdracht zo snel mogelijk te achterhalen, dit heeft immers implicaties voor de verdere procedure. De manier van overdracht is afhankelijk van de middelen en de expertise van zowel de overdrager als de archiefdienst. Hier zijn drie mogelijkheden. De methode hangt af van twee factoren, namelijk *wie* het uitvoert en de gebruikte *methode*:

- [Ontvangst via netwerk \(1\)](#)
- [Ontvangst via een draagbaar medium](#)
 - [Door de overdrager \(2\)](#)
 - [Door de archiefdienst \(3\)](#)

Opgelet!

De overdrager zal bezorgd zijn over de veiligheid van de data. [Encryptie](#) kan overwogen worden om de veiligheid van de bestanden tijdens de transfer te garanderen. Reconstructieschakels als deze kunnen echter best zoveel mogelijk vermeden worden.

Het workstation waarop het archief ter bewerking terecht zal komen is een quarantaineomgeving. Het is afgesloten van je lokale servers en netwerk.

- Zo voorkom je dat geïnfecteerde bestanden de andere data besmetten.
- Zo voorkom je dat je lokale netwerk gehackt wordt via een eventuele FTP-server

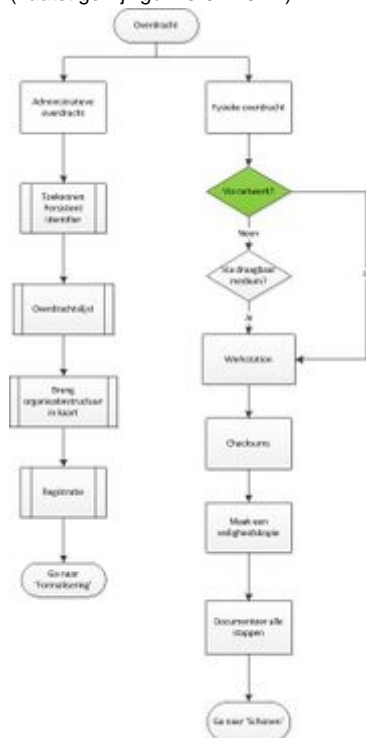
Meer lezen?

[AIMS Work Group. 2012. AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship](#)

[PARADIGM, Workbook on Personal Digital Archives, Accessioning digital and hybrid personal archives, Bodleian Library, 2007](#)

6.2.1 Overdracht via netwerk

(Laatst gewijzigd: 23-01-2014)



Overdracht via netwerk

Benodigheden

- [FTP-server](#)

Wat?

In deze stap wordt het digitale archief doorgestuurd van de overdrager naar de archiefdienst via een extern netwerk.

Een netwerk is een systeem om computers te verbinden en gegevens met elkaar te laten uitwisselen. Meestal bestaat zo'n computernetwerk uit een server en clients.

Onderscheid wordt gemaakt tussen een intern en een extern netwerk:

- Een intern netwerk is een netwerk binnen een bepaalde omgeving; binnen een organisatie/bedrijf (bijvoorbeeld intranet). Op die manier kan op een vrij eenvoudige manier archief overgedragen worden naar een centrale archiefdienst binnen de

organisatie. Dit geldt uiteraard enkel wanneer de archiefdienst tot de interne structuur van de archiefvormer behoort. Deze aanpak behoort niet tot de scope van het project.

- Een extern netwerk wordt opgezet wanneer de archiefdienst archief via netwerk wil ontvangen van externe organisaties of personen. In dit geval moet de archiefdienst over een [FTP](#)-server beschikken en de overdrager over een FTP-client.

Waarom?

Digitaal archief overdragen via een netwerk heeft een aantal voordelen ten opzichte van het overdragen door middel van externe dragers:

- Minder risico op dataverlies omdat je niet aan de slag moet met externe dragers (externe dragers kan je makkelijker verliezen of beschadigen).
- Niemand hoeft zich te verplaatsen.
- Het is meteen duidelijk wat de overdrager wil schenken; met name alles wat op de server opgeladen wordt.

Wanneer?

Deze stap maakt onderdeel uit van de [fysieke overdracht](#).

Hoe?

1. Creëer een FTP-adres
 - De archiefdienst creëert een FTP-adres waarnaar het archief kan worden overgedragen.
 - Dit kan een eigen server, of een 'dedicated server' zijn.
 - Een dedicated server is de server die men huurt. Ze bevindt zich bij de provider of in een extern datacenter. In de huurprijs zitten hardware, besturingssysteem, bandbreedte en eventueel beheerdiensten.
 - Voor het opzetten van een FTP-server kan je een tool gebruiken. Op de Virtuele Box staat bijvoorbeeld FileZilla.
2. Communiceer technische eisen met de overdrager.
 - Bestanden die via het netwerk overgedragen worden, moeten voldoen aan een aantal kenmerken
 - Bijvoorbeeld: alles in één map met een bepaalde bestandsnaam?
3. Communiceer het FTP-adres naar de overdrager
 - de overdrager downloadt een FTP-client en ontvangt het FTP-adres de archiefdienst om de overdracht te kunnen uitvoeren.

4. Registreer ontvangst

- Verhuis de op de FTP-server ontvangen bestanden naar het werkstation waar ze verder bewerkt zullen worden. (Zie [SODA invulformulier](#) (4.3))

5. Maak [checksums](#) en controleer deze

- Bereken nieuwe checksums en vergelijk ze met de lijst die je tijdens de prospectie genereerde.
- Wanneer je zelf geen (volledige) systeem- en bestandsanalyse hebt kunnen uitvoeren, vraag dan aan de overdrager om een lijst met checksums mee over te dragen. Deze checksums moeten vóór de overdracht gemaakt worden.
- De checksums controleer je via een tool op het [draagbaar werkstation](#).

Mogelijkheden zijn:

- [Jacksum](#)
- [Checksum Checker](#)
- [Fsum Frontend](#)
- [ExactFile](#)

Opgelet!

Bij het opzetten van een FTP-server verleen je externe gebruikers toegang tot een toestel binnen je organisatie. Om veiligheidsredenen is het daarom aangewezen dat het werkstation, waarop de FTP-server werkt, geen toegang geeft tot je lokale servers!

Waar kan je best een dedicated server huren? Het is moeilijk om hierover een eenduidige aanbeveling te geven. [Contacteer PACKED vzw](#) voor verdere informatie.

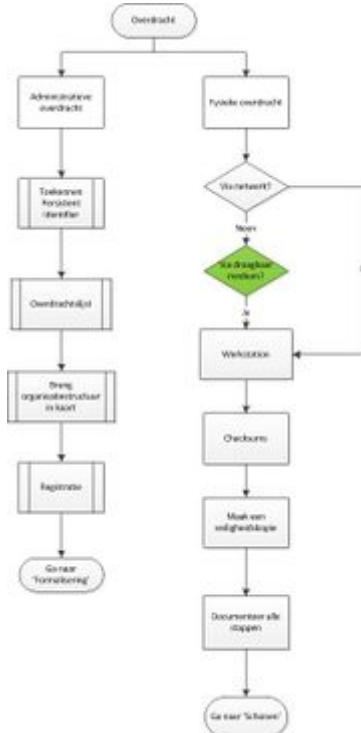
Wanneer jij of de overdrager [encryptie](#) van de bestanden nodig acht, gebruik dan een SFTP-server. SFTP staat voor *Secure File Transfer Protocol*, een veiliger variant van [FTP](#). Een SFTP-protocol maakt gebruik van encryptie bij de verzending. Dit zorgt voor een beveiligde overdracht, maar voegt een reconstructieschakel toe.

Meer lezen?

http://nl.wikipedia.org/wiki/File_Transfer_Protocol

6.2.2 Overdracht via draagbaar medium

(Laatst gewijzigd: 23-01-2014)



Overdracht via draagbaar medium

Benodigheden

- overdrachtsmedia
- [werkstation](#)
- [draagbaar werkstation](#)
- [leesapparatuur](#)

Wat?

Digitaal archief kan:

- overgedragen worden op de originele verwijderbare draagbare media.
- door de overdrager zelf gemigreerd zijn naar een nieuw draagbaar medium voor de overdracht.
- door de archiefdienst op locatie naar een extern medium gekopieerd worden.

Door middel van forensische technieken kunnen verwijderde data teruggevonden worden op bestandsdragers. Wanneer de overdrager de bestanden op voorhand echter gemigreerd heeft naar een nieuwe drager, kan zulke informatie niet meer teruggehaald worden.

Waarom?

Het gebruiken van een draagbaar medium is eenvoudiger dan het opzetten van een netwerk. Wanneer het archief van op de originele drager wordt gekopieerd, kan je overigens een [disk image](#) maken.

Wanneer?

Deze stap maakt onderdeel uit van de [Fysieke overdracht](#).

Hoe?

Zie uitwerking in volgende stappen:

- Overdracht [door de overdrager](#)
- Overdracht [door de archiefdienst](#)

Meer lezen?

[ERWAY, R., You've Got to Walk Before You Can Run: First Steps for Managing Born-Digital Content Received on Physical Media, OCLC Research, 2012](#)

6.2.3 Door de overdrager

(Laatst gewijzigd: 23-01-2014)

Wat?

De overdrager draagt zelf zijn/haar archief over door middel van een draagbaar medium. Dit kan op twee manieren:

- De bestanden worden aangeleverd op externe bestandsdragers. In de praktijk komt dit het meest voor.
- De volledige computer wordt aan de archiefdienst geschonken, bijvoorbeeld een volledige Windows pc of Apple Mac.

Waarom?

Een overdrager kan zelf archief naar een (nieuwe) externe drager migreren omdat hij/zij op die manier controle wil behouden over de bestanden die overgedragen worden.

Wanneer?

Deze stap maakt deel uit van de [fysieke overdracht](#) en gebeurt parallel met de [administratieve overdracht](#).

Hoe?

1. Communiceer technische eisen
 - Bezorg de overdrager richtlijnen met betrekking tot de technische eisen om digitaal archief te kunnen ontvangen.
 - Bijvoorbeeld:
 - De externe drager is uitgerust met een kabel die de archiefdienst kan aansluiten.
 - De overdrager stelt (al dan niet tijdelijk) de noodzakelijke leesapparatuur ter beschikking.
 - Vraag de overdrager om een lijst met checksums mee over te dragen, tenzij je deze zelf al genereerde tijdens de prospectie.
2. Sluit het draagbaar medium aan op het [werkstation](#).
3. Maak de [checksums](#), indien dit nog niet gebeurde tijdens de [prospectie](#).
 - Gebruik hiervoor een tool uit je [toolbox](#). Mogelijkheden zijn:
 - [Jacksum](#)
 - [Checksum Checker](#)
 - [Fsum Frontend](#)

- [ExactFile](#)
- 4. Kopieer de bestanden van de externe dragers naar het werkstation.
 - Bij volledige computers en originele externe harde schijven is het aangewezen om een [disk image](#) te maken van de harde schijf, als hiervoor toestemming verkregen is.
 - Registreer in het [SODA invulformulier](#) de datum en de manier waarop het archief naar het werkstation is gekopieerd.
- 5. Maak hiervan nieuwe checksums en vergelijk ze met de checksums van die voor de overdracht werden gegenereerd.
- 6. Afstoten of bewaren fysieke dragers?
 - Beslis wat met de originele drager moet gebeuren na de overdracht
 - Teruggave aan de overdrager?
 - Bijhouden?
 - De bestanden en de drager worden als twee aparte entiteiten bewaard.
 - Ken meteen een uniek nummer toe aan de bestandsdrager.
 - Documenteer de relatie tussen de drager en het digitale archief.
 - Vernietigd?
 - Bestanden: d.m.v. tool.
 - De bestandsdragers zelf worden op een gecontroleerde manier vernietigd.
 - Beslissingen over dragers die al dan niet als aparte entiteit in de collectie worden beschreven, zijn in het [acquisitieprofiel](#) opgenomen. Men kan bijvoorbeeld bepalen dat uitzonderlijke (bijvoorbeeld geannoteerde) dragers bewaard worden.
 - Wanneer volledige (verouderde) computers geschonken worden, kan het interessant zijn om deze te bewaren met het oog op een computermuseumstrategie. Deze strategie vereist wel een gedegen ICT-kennis.

Opgelet!

Ongeacht welk lot de dragers te wachten staat (bewaren, vernietigen, terugschenken), elke stap wordt zorgvuldig gedocumenteerd! Gebruik hiervoor het [SODA invulformulier](#).

Meer lezen?

[AERTSEN, S., Digigids@work, AMVB, 2012](#)

[AIMS Work Group. 2012. AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship](#)

[BOUDREZ, F., Magnetische dragers voor het archief, Antwerpen, 2002](#)

[BOUDREZ, F., CD's voor het archief, Antwerpen, 2001](#)

[ELFORD, e.a., Media Matters: developing processes for preserving digital objects on physical carriers at the National Library of Australia, Québec, 2008](#)

[GUERRERO, M., Removable Media and the use of Digital Forensics, Bentley Historical Library, 2012](#)

[KIRSCHENBAUM, M., e.a., Digital Materiality: Preserving Access to Computers as Complete Environments, iPRES, San Francisco, 2009](#)

6.2.4 Door de archiefdienst

(Laatst gewijzigd: 23-01-2014)

Wat?

Je gaat op locatie de bestanden van het lokaal systeem kopiëren naar een [draagbaar werkstation](#).

Waarom?

De overdrager kan om verschillende redenen niet in staat zijn om de overdracht zelf te regelen en daarom de archiefdienst inschakelen om het archief te komen ophalen.

Dit creëert nieuwe kansen voor de archiefdienst, die nu eventueel een [disk image](#) van het lokaal systeem kan nemen.

Wanneer?

Deze stap maakt deel uit van de [fysieke overdracht](#) en gebeurt parallel met de [administratieve overdracht](#).

Hoe?

1. Communiceer technische eisen
 - Bezorg de overdrager richtlijnen met betrekking tot de technische eisen om het archief eenvoudig te kunnen kopiëren van het lokaal systeem naar het [draagbaar werkstation](#).
 - Deze eisen komen vaak overeen met de eisen uit de richtlijnen voor de [prospectie](#)
 - Bepaal locaties van digitale bestanden op niet-verwijderbare media of breng alle bestanden samen op één locatie.
2. Sluit het [draagbaar werkstation](#) aan op het lokaal systeem. Het draagbaar werkstation bestaat uit een softwarepakket om de overdracht te ondersteunen. Een extra partitie is voorzien om de bestanden naar te kopiëren.
3. Maak checksums, voor zover dit nog niet gebeurde tijdens de prospectie.
 - Gebruik hiervoor een tool uit de [toolbox](#). Mogelijkheden zijn:
 - [Jacksum](#)
 - [Checksum Checker](#)
 - [Fsum Frontend](#)
 - De lijst met checksums wordt mee met het archief overgedragen.
4. Kopieer de bestanden naar de daartoe aangewezen partitie op het draagbaar

werkstation.

- Documenteer de datum (PREMIS event: capture) in het [SODA invulformulier](#).
- Indien mogelijk maak je een disk image én een gewone kopie van de mappenstructuur.

5. Maak nieuwe checksums en controleer met de voorgaande.

Opgelet!

Leg op beleidsniveau vast welke eisen gelden voor de overdrager die zijn/haar archief wil laten ophalen.

Een disk image kan interessant zijn voor een duurzame bewaring en biedt de mogelijkheid om op een later moment forensische technieken te gebruiken. Vraag wel steeds de schriftelijke toestemming aan de overdrager. Een disk image is een kopie van de volledige harde schijf (of externe drager zoals CD-ROM, DVD, USB, ...), gecomprimeerd in één bestand. Een image heeft als voordeel dat het de integriteit en de structuur van de data beter verzekerd. Wanneer bij de overdracht een image gemaakt is, kan die bewaard worden als eerste veiligheidskopie doorheen de hele procedure.

Meer lezen?

[KIRSCHENBAUM, M., OVENDEN, R., REDWINE, G., Digital Forensics and Born-Digital Content in Cultural Heritage Institutions, Washington D.C., CLIR, 2010](#)

7.10 Veiligheidskopie

(Laatst gewijzigd: 23-01-2014)



Veiligheidskopie 1



Veiligheidskopie 2

Wat?

Een veiligheidskopie is een reservekopie waar je naar kan teruggrijpen wanneer data verloren of gewijzigd zijn.

Waarom?

Tijdens het overdragen en bewerken van uw archief kan veel mislopen:

- Fouten kunnen in uw hardware en software opduiken;
- Uw bestanden kunnen met virussen geïnfecteerd zijn;
- Uw bestanden kunnen gehackt worden;
- Bestanden kunnen per ongeluk verwijderd worden;
- Calamiteiten zoals brand, overstroming of een stroompanne kunnen dataverlies veroorzaken!

Wanneer?

Maak een veiligheidskopie telkens wanneer je stopt met het bewerken van het digitale archief. In de praktijk komt dit vaak neer op de volgende cesuren waarbij idealiter een veiligheidskopie genomen wordt:

1. Wanneer het digitale archief op het werkstation ontvangen is;
2. Wanneer het archief geschoond is, maar nog niet in een containerbestand opgenomen. Hou deze kopie bij tot een geslaagde opname in het containerbestand gegarandeerd is;
3. Wanneer het archief volledig en veilig in het containerbestand is opgenomen.

Hoe?

1. Genereer [checksums](#) of gebruik de checksums die in een vorige fase gemaakt zijn.
 - Gebruik hiervoor een tool uit je [toolbox](#). Mogelijkheden zijn:
 - [Jacksum](#)
 - [Checksum Checker](#)
 - [Fsum Frontend](#)
2. Kopieer data van het werkstation naar een bestandsdrager/server
 - Wanneer je data manueel kopieert, worden niet alle geassocieerde (meta)data mee overgedragen. Het is van belang dat de manier waarop de veiligheidskopie gemaakt is, gedocumenteerd wordt!
 - Gebruik hiervoor het [SODA invulformulier](#).
 - Zet de data in een zip-gecomprimeerde map. Dit kan helpen om metadata met betrekking tot het bestandssysteem te bewaren (o.a. timestamps, directory structuren, toegangsrechten).
3. Controleer de veiligheidskopie op haar volledigheid
 - Bereken en vergelijk checksums

- Identificatie van de bestanden
 - vergelijk bestandsformaten en de datum met die van de originele bestanden, in de mate van het mogelijke.
 - Gebruik hiervoor een tool (bijvoorbeeld [DROID](#) of [Manifest Maker](#))
- 4. Leg vast welke drager gebruikt wordt
 - Houdt hierbij rekening met de omvang van de data en hoe de veiligheidskopieën worden gemaakt;
- 5. Bewaar veiligheidskopieën los van je organisatienetwerk. Hiervoor zijn verschillende mogelijkheden:
 - Huur een externe, dedicated server bij een provider.
 - Gebruik een netwerkschijf ([NAS](#)).
 - Gebruik een extern medium.
- 6. Leg vast op welke locatie de veiligheidskopieën bewaard worden
 - Bewaar de veiligheidskopieën op externe locaties, zodat deze niet vernietigd worden bij calamiteiten.

Opgelet!

Veiligheidskopieën mogen niet gecomprimeerd worden!

- Veiligheidskopieën hebben immers niet als doel om bestanden te archiveren, maar om op kortere termijn verloren of gewiste digitale bestanden te herstellen.

Overschrijf nooit oude back-ups met nieuwe!

- Overschrijven kan fragmentatie (het niet aaneensluiten van clusters van een bestand op een harde schijf) en datacorruptie in de hand werken.

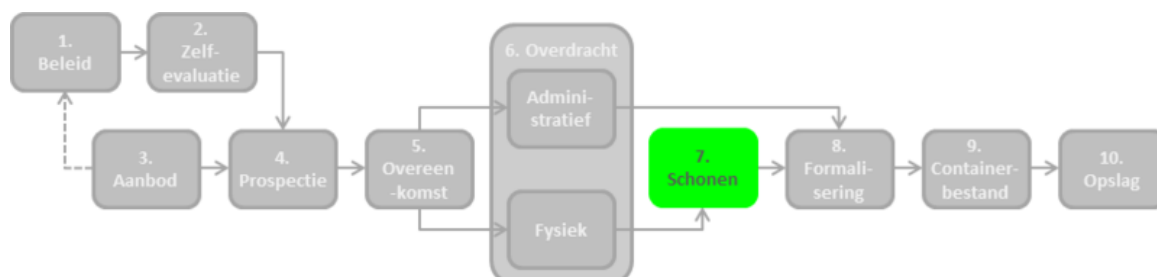
Leg op [beleidsniveau](#) een procedure vast voor het maken van veiligheidskopieën, hoe en wanneer veiligheidskopieën gemaakt worden. Het volgen van zulke procedures zorgt voor een gestandaardiseerde manier van veiligheidskopieën maken.

Meer lezen?

[AERTSEN, S., Een Back-up maken, In: DigiGIDS@work, AMVB, Brussel, 2012](#)
[ERWAY, R., You've got to walk before you can run: First steps for managing Born-Digital Content received on physical media, OCLC Research, Dublin Ohio, augustus 2012](#)
[VAN DEN EYNDE, V., CORTI, L., WOOLLARD, M., BISHOP, L., HORTON, L., Managing and Sharing Data: A Best Practice Guide for Researchers, UK Data Archive, Essex, 2011](#)

7. Schonen

(Laatst gewijzigd: 22-01-2014)



Wat?

Tijdens deze fase worden bestanden en mappen gedecomprimeerd, gecontroleerd op virussen, beveiligingen verwijderd, overbodige bestanden verwijderd en de bestandsnamen genormaliseerd. Optioneel kan je ook een formele selectie doorvoeren. Na het schonen wordt een veiligheidskopie gemaakt, alvorens het archief in een digitale container te verpakken.

Waarom?

In deze stap worden zo veel mogelijk reconstructieschakels uitgeschakeld, om zo de digitale bestanden doorheen de tijd op een duurzame manier te bewaren. Daarnaast wordt, door het verwijderen van overtollig materiaal, de vindbaarheid van de bestanden bevorderd.

Wanneer?

Het archief wordt geschoond nadat een [veiligheidskopie](#) werd gemaakt van het volledige archief dat op het [werkstation](#) werd ontvangen.

Hoe?

Zie verdere uitwerking in de volgende stappen:

1. [Controleer de integriteit](#)
2. [Decomprimeer gecomprimeerde bestanden](#)
3. [Verwijder versleutelingen](#)
4. [Verwijder geïnfecteerde bestanden](#)

5. [Verwijder dubbels](#)
6. [Verwijder lege mappen](#)
7. [Verwijder systeembestanden](#)
8. [Selectie](#)
9. [Uniformiseer de bestandsnamen](#)
10. [Veiligheidskopie](#)

Opgelet!

Spreek op voorhand met de overdrager af wat er met de bestanden gebeurt die tijdens het schonen uit het archief verwijderd worden: gaan deze terug naar de overdrager of worden ze vernietigd?

7.1 Controleer de integriteit

(Laatst gewijzigd: 22-01-2014)



Integriteit

Benodigheden?

- [toolbox](#)

Wat?

In deze stap wordt de bitintegriteit van de bestanden gecontroleerd.

- **Integriteit:** integriteit betekent dat de vorm, inhoud en structuur bij raadpleging van een archiefstuk of archiefbestanddeel gelijk zijn aan de vorm, inhoud en structuur op het tijdstip dat het werd ontvangen of opgemaakt.
- **Bitintegriteit:** een bit is de kleinste eenheid voor informatie. Het kan een 1 of een 0 zijn. Meerdere opeenvolgende bits vormen een bitstream. Wanneer in die opeenvolging van nullen en enen iets wijzigt, is de bitintegriteit van dat bestand gecorrumpieerd.

Waarom?

De bitintegriteit van het archief wordt gecontroleerd om zich ervan te verzekeren dat het archief volledig en ongecorrumpieerd is overgedragen. Het controleren van de bitintegriteit vormt een onderdeel van de permanente kwaliteitscontrole.

Wanneer?

Het controleren van de bitintegriteit gebeurt minstens elke keer wanneer het archief naar een andere locatie wordt gekopieerd.

Het controleren van de integriteit is een eerste stap in het [schonen](#) van het archief.

Hoe?

Het controleren van bitintegriteit gebeurt door middel van [checksums](#).

Om checksums te controleren, moeten ze in eerste instantie aangemaakt zijn. Dit is idealiter tijdens de [bestandsanalyse](#) (prospectie) gebeurd, of de overdrager draagt een lijst met checksums mee over. Wanneer het archief is overgedragen, worden nieuwe checksums gegenereerd. Deze nieuwe lijst wordt vergeleken met de vorige lijst om anomalieën op te sporen. Wanneer de checksum niet meer identiek is met het vorige, is het bestand corrupt.

De checksums controleer je via een tool op je [toolbox](#). Mogelijkheden zijn:

- [Jacksum](#)
- [Checksum Checker](#)
- [Fsum Frontend](#)

Opgelet!

- Corrupte bestanden kunnen verwijderd worden, met het oog op de doorzoekbaarheid van de bestanden.
- Een andere optie is om te documenteren welke bestanden corrupt zijn en ze in het archief te behouden.
 - Corrupte bestanden kunnen immers geen andere bestanden contamineren en de kans bestaat altijd dat in de toekomst een methode ontwikkeld wordt om de bitintegriteit van corrupte bestanden te herstellen.

De integriteit van de bestanden werd reeds gecontroleerd wanneer de bestanden op het [werkstation](#) ontvangen zijn. Wanneer je meteen overgaat tot het [schonen](#), zonder het werkstation uit te schakelen, is het niet noodzakelijk om hier terug checksums te controleren. Als er echter een periode verstrijkt tussen de overdracht en het schonen, moeten de checksums wel opnieuw gecontroleerd worden omdat er een risico op dataverlies bestaat.

7.2 Decomprimeer gecomprimeerde bestanden

(Laatst gewijzigd: 22-01-2014)



Compressie

Benodigheden?

- [toolbox](#)

Wat?

In deze stap zal je compressie van de data ongedaan maken. Datacompressie is een algoritme dat de omvang van bestanden verkleint, zodat ze minder geheugen in beslag nemen:

- Bij [lossy compressie](#) treedt dataverlies op. Informatie en kwaliteit gaan verloren.
- Bij [lossless compressie](#) treedt geen dataverlies op. De gecomprimeerde bestanden blijven echter relatief groot.
- Bij visually lossless compressie treedt wel gegevensverlies op, maar laat dit voor het menselijk oog of oor geen zichtbare sporen na. Toch moet dit worden beschouwd als een vorm van lossy compressie.

Archiefbestanden kunnen afzonderlijk gecomprimeerd zijn (bijvoorbeeld [LZW](#), [JPEG](#) of [ZIP](#) in een [TIFF](#) of [PDF](#)-bestand), maar vaak gebeurt het dat verschillende archiefdocumenten in gecomprimeerde mappen verpakt zitten (.tar, .zip). Welke compressie toegepast werd, kan je afleiden uit de extensie van de bestanden of mappen.

Waarom?

Digitale archivering is een reconstructieproces. Hoe meer schakels in dat proces zitten, hoe moeilijker het wordt om toekomstige leesbaarheid van die bestanden te garanderen. Wanneer bij één van deze schakels iets mis loopt, kan het bestand onleesbaar worden. Het risico bestaat dat vele compressiealgoritmes verouderd en overbodig geraken en op

die manier een onherstelbare schakel vormen in het reconstructieproces.

Wanneer?

Het decomprimeren van gecomprimeerde bestanden is de eerste stap in de workflow schonen na de [integriteitscontrole](#). Het is aangewezen om eerst alle gecomprimeerde bestanden uit te pakken vooraleer verder te gaan met schonen. In de gecomprimeerde mappen kunnen zich immers nog andere mappen en verschillende bestanden bevinden.

Hoe?

Decomprimeren gebeurt aan de hand van tools.

In de [toolbox](#) zit software om bestanden en mappen te decomprimeren. Je kan hiervoor ook zelf software installeren op je werkstation. Deze procedure gaat uit van het gebruik van [7-zip](#). Een alternatief is [PeaZip](#).

Opgelet!

Wanneer veel mappen versleuteld zijn, kan je eerst de [encryptie](#) wegwerken. De kans bestaat dat in versleutelde mappen ook gecomprimeerde mappen/bestanden zitten die de software niet zal decomprimeren zolang ze in de versleutelde map zitten. Omgekeerd kan ook: in gecomprimeerde mappen kunnen zich versleutelde bestanden/mappen bevinden. Wanneer zulk scenario zich aandient, herhaal dan gewoon de stappen decomprimeren en [versleutelingen verwijderen](#).

Meer lezen?

[POPPE, J., Handboek digitaliseren van documenten. Technische aspecten en kwaliteitseisen, FARO, 2011](#)

[BOUDREZ, F., Digitaal archiefbeheer in de praktijk, EDAVID, 2004](#)

7.3 Verwijder versleutelingen

(Laatst gewijzigd: 22-01-2014)



Versleuteling

Benodigheden?

- Interview overdrager ([SODA invulformulier](#))
- [toolbox](#)

Wat?

In deze fase worden versleutelde mappen en bestanden gedeblokkeerd.

Waarom?

Versleutelde bestanden en mappen kunnen niet worden geopend. Het verwijderen van de [versleutelingen](#) is dus noodzakelijk voor zowel het achterhalen van de inhoud als voor het uitvoeren van verdere preserveringshandelingen.

Wanneer?

Dit gebeurt na het [decomprimeren van gecomprimeerde mappen en bestanden](#).

Hoe?

Het verwijderen van versleutelingen gebeurt manueel.

Aan de hand van de informatie die je verkreeg tijdens de [prospectie](#) (interview overdrager), deblokkeer je handmatig de bestanden en mappen die met een wachtwoord of een encryptiesleutel beveiligd zijn.

Opgelet?

Het is mogelijk dat zich in de versleutelde mappen opnieuw gecomprimeerde bestanden of mappen bevinden. Decomprimeer in dat geval opnieuw de gecomprimeerde mappen en/of bestanden. Herhaal deze cyclus tot er geen versleutelde of gecomprimeerde mappen meer in het archief bevinden.

7.4 Verwijder geïnficeerde bestanden

(Laatst gewijzigd: 23-01-2014)



viruscontrole

Benodigheden?

- [toolbox](#)

Wat?

Voor de fysieke overdracht werden reeds de virusdefinities van het ([draagbaar](#)) [werkstation](#) geüpdatet. Nu worden de overgedragen data op virussen gecontroleerd. Hiervoor bestaan twee methoden:

- Het scannen van de bestanden
 - De antivirussoftware scant alle bestanden op de computer en vergelijkt deze met een databank waarin alle gekende virussen opgelijst zijn.
 - Bij een overeenkomst is het bestand met het overeenkomstige virus uit de databank geïnficeerd.
 - De antivirussoftware kan dan het virus verwijderen, het geïnficeerde bestand in quarantaine plaatsen zodat het virus zich niet kan verspreiden, of het hele bestand verwijderen;
- Het identificeren van verdacht gedrag van computerprogramma's
 - Deze techniek dient om niet bekende virussen te detecteren.
 - Deze methode wordt minder vaak gebruikt omdat ze niet altijd even betrouwbaar blijkt.

Waarom?

Virussen kunnen dataverlies veroorzaken. De controle op virussen en malware vormt een belangrijke kwaliteitscontrole bij de overdracht van digitaal archief. Alle bestanden moeten virusvrij zijn vooraleer ze in een digitaal depot terecht komen om te voorkomen

dat zij geen andere bestanden contamineren.

Wanneer?

Een eerste viruscontrole gebeurt tijdens het schonen, de bestanden bevinden zich in de quarantaineomgeving op het [werkstation](#).

Een viruscontrole gebeurt pas na verwijdering van [compressie](#) en [versleutelingen](#): in gecomprimeerde of versleutelde mappen kunnen zich immers nog virussen bevinden.

Hoe?

Controleer de overgedragen bestanden op virussen met een actuele antivirussoftware.

Gebruik een anti-virustool uit de [toolbox](#). Mogelijkheden zijn:

- [ClamAV](#)
- [ClamWin](#)

Opgelet!

Antivirussoftware loopt steeds achter de feiten aan. Zij bieden een antwoord op reeds bestaande virussen en malware.

- Het is dus aangewezen om voor recente bestanden na de viruscontrole de bestanden nog een periode in de quarantaineomgeving te houden zodat nieuwe virussen bij een volgende update van de antivirussoftware wel herkend worden.
- In de praktijk zal dit niet zo dwingend zijn, omdat het meestal over oude bestanden gaat.

Bij de keuze van een antivirussoftware is het belangrijk dat je rekening houdt met oude of verouderde virussen. Veel producenten verwijderen na verloop van tijd oude virussen uit hun databanken, hoewel verouderde bestanden deze virussen nog wel kunnen bevatten!

Zorg ervoor dat uw antivirussoftware regelmatig geüpdatet wordt. Werk hiervoor een procedure uit.

Wanneer virussen niet verwijderd kunnen worden, worden de geïnfecteerde bestanden helemaal verwijderd uit het archief. Afhankelijk van wat in de overeenkomst is vastgelegd, worden de bestanden vernietigd of teruggeven.

- Soms kan het echter van belang zijn om deze bestanden wel in een inactieve staat op te nemen in het containerbestand (bijvoorbeeld voor later onderzoek). Documenteer steeds wat met de geïnfecteerde bestanden gebeurt.

Meer lezen?

[AIMS Work Group. 2012. AIMS Born-Digital Collections: An Inter-Institutional Model for Stewardship](#)

7.5 Verwijder dubbels

(Laatst gewijzigd: 22-01-2014)



Dubbels verwijderen

Benodigheden?

- [toolbox](#)
- [SODA invulformulier](#)

Wat?

Vaak worden dezelfde bestanden in verschillende mappen bewaard waar ze niet thuis horen. Tijdens deze fase wordt door middel van softwaretools gezocht naar dubbele mappen en bestanden die verwijderd mogen worden.

Waarom?

Dubbels nemen onnodige ruimte in. Het verwijderen van overbodige bestanden komt de ordening van het digitaal archief, en dus ook de doorzoekbaarheid van bestanden ten goede.

Wanneer?

Dubbels worden verwijderd nadat [compressie](#), [encryptie en paswoorden](#) verwijderd zijn uit mappen en bestanden.

Hoe?

Bij het toekennen van [checksums](#) krijgt elk uniek bestand een unieke checksum toegekend. Wanneer twee bestanden een identieke checksums hebben, gaat het om eenzelfde bestand.

Voor het identificeren en het verwijderen van dubbels bestaan er verschillende softwaretools. Die tools gaan op zoek naar identieke checksums om dubbels te herkennen.

Gebruik hiervoor een tool in je [toolbox](#). Mogelijkheden zijn:

- [FSLint](#)
- [YADFR](#)
- [Duplicate File Searcher](#)

Documenteer welke dubbels je verwijderd hebt, wanneer en waarom. Bewaar een logbestand van deze handeling (zie metadataformulier).

Opgelet!

Dubbele bestanden (dus bestanden met een identieke checksum) kunnen wel een andere bestandsnaam hebben.

Bij het verwijderen van dubbels moet de beslissing genomen worden welke dubbels juist verwijderd worden, welke versie van de dubbels juist het moederbestand is. Het is daarom raadzaam om aan de hand van de technische metadata (cf. directory list) de oudste versie van de dubbels te identificeren en deze als moederbestand te bewaren.

Enige voorzichtigheid is geboden bij het verwijderen van dubbels. Dubbels kunnen in verschillende dossiers thuishoren. Daarom is het aangewezen om eerst na te gaan waar de dubbels zich juist bevinden:

- Wanneer dubbels in eenzelfde map zitten, kunnen ze sowieso verwijderd worden.
- Wanneer dubbels in verschillende mappen voorkomen, kunnen ze deel uitmaken van dat dossier. Hiervoor is een inhoudelijke selectie nodig. Dit valt echter buiten de scope van deze handleiding.

Wanneer je toch alle dubbels verwijderd, documenteer dit dan zorgvuldig. Leg eventueel links naar het moederbestand waar de dubbels verwijderd zijn.

Meer lezen?

[AIMS white paper](#)

7.6 Verwijder lege mappen

(Laatst gewijzigd: 22-01-2014)



Lege mappen verwijderen

Benodigheden?

- [toolbox](#)

Wat?

In deze fase worden lege mappen verwijderd. Ze bevatten immers geen archief.

Waarom?

Het verwijderen van lege mappen bevordert de overzichtelijkheid en de doorzoekbaarheid.

Wanneer?

Lege mappen worden verwijderd nadat je [geïnfecteerde](#) en [dubbele](#) bestanden uit het archief hebt gehaald.

Hoe?

Voor het verwijderen van lege mappen gebruik je een tool.

Gebruik de software op je [toolbox](#). Je kan ook zelf een tool downloaden. Mogelijkheden zijn:

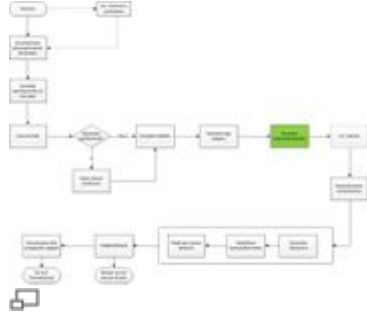
- [FSLint](#)
- [RED](#)

Opgelet!

- Lege mappen kunnen op zich belangrijke contextinformatie toevoegen aan een archief!
 - Documenteer daarom welke mappen je uit het archief hebt verwijderd, en waar deze zich bevonden in de directory list!
- Bewaar de logs die bij deze handeling werden aangemaakt.

7.7 Verwijder systeembestanden

(Laatst gewijzigd: 23-01-2014)



Verwijder
systeembestanden

Wat?

In deze fase worden overbodige systeembestanden uit het archief verwijderd.

Waarom?

Systeembestanden hebben geen inhoudelijke waarde voor de rest van het archief en kunnen dus zonder problemen verwijderd worden. Zij hebben geen archiefwaarde.

Wanneer?

Dit gebeurt na het verwijderen van [lege mappen](#) en [dubbele bestanden](#).

Hoe?

Deze handeling wordt manueel uitgevoerd. Dit gebeurt op basis van de informatie en documentatie over de software, die je tijdens de [prospectie](#) ([interview](#) en [systeemanalyse](#)) achterhaalde.

Voor het opsporen van sommige systeembestanden kan je eventueel de checksums gebruiken. Er bestaan zogenaamde 'forensic hash databases' waarin checksums van bekende systeembestanden zijn opgeslagen (zie bijvoorbeeld [National Software Reference Library](#)). Door de [checksums](#) in deze databank te vergelijken met de checksums van je archiefbestanden, kan je systeembestanden opsporen.

Opgelet!

Systeembestanden worden vaak verborgen om te voorkomen dat deze per ongeluk gewijzigd worden. Zorg er daarom voor dat alle bestanden in de map zichtbaar zijn.

Sommige systeembestanden kunnen op termijn nog wel nuttig zijn, bijvoorbeeld wanneer encapsulatie als bewaarstrategie gehanteerd wordt (containerbestand).

7.8 Selectie

(Laatst gewijzigd: 23-01-2014)



Selectie

Wat?

Dit is een optionele tussenstap in de workflow schonen. Hier voer je fysiek een formele selectie uit, waartoe eerder werd beslist op basis van het bestemmingsbeginsel.

Waarom?

Het principe van een eerste ordening op basis van de archiefvormer vindt zijn grondslag in het bestemmingsbeginsel. Dit stipuleert dat ieder archiefstuk deel uitmaakt van het archief waarin het bij ontvangst of opmaken is opgenomen.

Wanneer?

Een inhoudelijke selectie gebeurt eigenlijk nog voor het archief aanvaard wordt: bij het aanbod wordt meteen een inhoudelijke prospectie uitgevoerd waarbij het aangeboden archief wordt getoetst aan het [acquisitieprofiel](#).

Hoe?

Het gaat hier om een vormelijke selectie en niet om een inhoudelijke!

- Wanneer archieven van verschillende archiefvormers door elkaar lopen (bijvoorbeeld een verenigingsarchief en een persoonsarchief op eenzelfde computer), worden deze van elkaar gescheiden.
- Per archiefvormer werd reeds een apart metadataformulier ingevuld. Dit wil zeggen dat wanneer je tijdens de [prospectie](#) verschillende archiefvormers identificeert, je meteen ook verschillende metadataformulieren invult.
 - Tijdens het schonen kan een dergelijke vormelijke selectie fysiek uitgevoerd worden.

Opgelet!

Inhoudelijke selectie gebeurt pas vanaf het moment dat het archief zich veilig in een containerbestand bevindt. Het is niet de bedoeling om in deze fase elk bestand op stukniveau te waarderen. Wanneer archieven fysiek gescheiden worden, documenteer dit dan per archief in de respectievelijke metadataformulieren ([SODA invulformulier](#)).

Meer lezen?

[Archiefwiki, Bestemmingsbeginsel](#)

[PARADIGM, Workbook on digital private papers, Appraisal and disposal, Bodleian Library, 2007](#)


[MAC DONALD, C., 'Selectie sharen!' Digitale archiefselectie als een shared service, verhandeling Universiteit van Amsterdam, 2008](#)

COPPENS, H., 'De ontsluiting van archieven. Richtlijnen en aanbevelingen voor de ordening en beschrijving van archieven in het Rijksarchief', Brussel, 1997

7.9 Uniformiseer de bestandsnamen

(Laatst gewijzigd: 23-01-2014)



 Uniformiseer
bestandsnamen

Benodigheden?

- [toolbox](#)

Wat?

In deze stap worden de bestandsnamen genormaliseerd en geuniformiseerd. Spaties, leestekens en vreemde tekens worden verwijderd of vervangen door underscores. Diakritische tekens worden vervangen door 'gewone' tekens. Gebruik bij normaliseren enkel de tekens: *ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz 1234567890 _*

Waarom?

Voordat de digitale bestanden in een container of in een depot kunnen worden opgenomen, moeten de bestandsnamen aan een aantal vormelijke kenmerken voldoen. Dit is noodzakelijk om automatische controles toe te laten.

Wanneer?

Dit gebeurt voordat de bestanden in een container worden opgenomen. Deze laatste stap in het schonen, is tevens de eerste stap in het gebruik van de [UGent SIP Creator](#).

Hoe?

Omdat het hernoemen van de bestanden gewoonlijk in bulk gebeurt, gebruik je hiervoor een tool.

- Deze handleiding gaat uit van het gebruik van de UGent SIP-Creator.
 - Deze staat ook op de [virtual box](#).
 - De UGent SIP-Creator bevat een renamer waarmee je een aantal formele regels kan bepalen om de bestanden die je in de bag wil stoppen te normaliseren.
- Een alternatief is [Métamorphose](#).

Van de SIP-Creator bestaat reeds een volledige [handleiding](#). Met het oog op de toepassing van deze tool binnen deze stap van SODA, worden hier een aantal specifieke tips voor het gebruik gegeven. Dit zijn slechts aanvullingen op de eigenlijke handleiding, lees deze daarom eerst volledig na!

Het hernoemen van bestanden is binnen UGent SIP-Creator een optionele stap. In de praktijk zal je archiefoverdracht echter altijd bestandsnamen bevatten die niet geschikt zijn om in een Bag op te nemen. Hierdoor zal het voor deze tool onmogelijk zijn de data aan je Bag toe te voegen. Het hernoemen van bestanden is dus een noodzakelijke stap binnen SODA. De interface om bestanden te hernoemen (via de knop 'open renamer'), biedt twee functies: hernoemen en hernummeren. We gebruiken in deze context enkel de eerste functie.

Vervang spaties

1. Selecteer de map met het geschoonde archief in de interface
2. Instellingen
 - Templates: 'Verwijder spaties'
 - Vervang: typ in dit veld een spatie
 - Door: typ een _
 - Negeer grote letters: UIT
 - Pas toe op onderliggende ...: AAN
 - Voorvoegsel: laat dit veld leeg
 - Navoegsel: laat dit veld leeg
 - Reguliere expressie: UIT
 - Bij fout: 'overslaan'
3. Klik eventueel op 'simuleer', om te controleren
4. Klik op 'OK'

Verwijder leestekens

1. Selecteer de map met het geschoonde archief in de interface
2. Instellingen
 - Templates: 'verwijder leestekens'
 - Vervang: Dit veld wordt nu automatisch ingevuld

- Door: typ een _, wanneer je leestekens wenst te vervangen door een liggend streepje, of typ niets, wanneer je ze wenst te verwijderen.
 - Negeer grote letters: UIT
 - Pas toe op onderliggende ...: AAN
 - Voorvoegsel: laat dit veld leeg
 - Navoegsel: laat dit veld leeg
 - Reguliere expressie: AAN
 - Bij fout: 'overslaan'
3. Klik eventueel op 'simuleer', om te controleren
 4. Klik op 'OK'

Overgebleven niet-conforme tekens verwijderen

Het automatische verwijderen van leestekens (zie hier boven), laat nog verschillende tekens door de mazen van het net glijpen.

Open de renamer en voeg alle mogelijke tekens afzonderlijk in om ze te laten vervangen door een alternatief.

- Instellingen voor het verwijderen van overgebleven karakters:
 - Templates: 'Verwijder leestekens'
 - Negeer grote letters: UIT
 - Pas toe op onderliggende ...: AAN
 - Voorvoegsel: laat dit veld leeg
 - Navoegsel: laat dit veld leeg
 - Reguliere expressie: AAN
 - Bij fout: 'overslaan'

De kans is groot dat in je bestandsnamen letters met accenten voorkomen. Deze moeten worden vervangen door hun accentloze variant. Voer daarom het volgende in in de velden 'Vervang' en 'Door'

- Vervang: [äåââ]
 - Door: a
- Vervang: [ëèèè]
 - Door: e
- Vervang: [ïîîî]
 - Door: i
- Vervang: [öóòò]
 - Door: o

- Vervang: [üúûû]
- Door: u
- Vervang: ç
- Door: c

Er zijn ook andere tekens die de renamer niet automatisch verwijdert. Deze kan je vervangen door een liggend streepje, door het volgende in te vullen:

- Vervang: [^\^&~.,µ?\\\$£§@%°=#²³]+
- Door: _

Nu zouden al je bestandsnamen geschikt moeten zijn om in een Containerbestand op te nemen.

Test

Je kan nu testen of de gegevens in een bag kunnen worden opgenomen (je hoeft nog niet klaar te zijn om de bag op te maken)

- Sluit de renamer interface en klik op 'nieuwe bag'
- Klik op 'ok'
- Klik naast 'Data toevoegen' op 'voeg toe', selecteer je hernoemde archiefbestanden en probeer ze toe te voegen.
 - Wanneer dit lukt, zijn de namen van je bestanden in orde.
 - Wanneer je een foutmelding te zien krijgt, zijn de namen nog niet cross-platvorm bruikbaar.

8. Formalisering

(Laatst gewijzigd: 22-01-2014)



Wat?

Nu het archief [geschoond](#) is, worden alle [overeenkomsten](#) en documentatie die tijdens de voorgaande stappen verzameld zijn, bij elkaar gebracht en gedocumenteerd.

Waarom?

Het is belangrijk dat niet enkel de digitale archiefbestanden worden bewaard, maar dat ook de context er duurzaam mee verbonden blijft. Het archief moet op het eind van deze procedure immers samen met de context (alle relevante overeenkomsten en metadata) in de container opgeslagen zijn.

Dit resultaat ziet er als volgt uit:

- SIP-Container
 - Archief + Metadata
 - Formulieren, Overeenkomsten, Logs

Wanneer?

De formalisering vormt de laatste stap vóór het [aanmaken van een containerbestand](#).

Hoe?

1. Verzamel alle overeenkomsten en documentatie zodat ze samen kunnen worden opgeslagen.
 - Formulieren
 - Het aanbodformulier en de beslissing tot acquisitie

- [SODA invulformulier](#)
 - Eventuele andere metadataformulieren
 - Overeenkomsten
 - [Overdrachtsovereenkomst](#)
 - De definitieve overdrachtslijst (al dan niet in de vorm van een directory list)
 - Logs
 - Alle logbestanden die door de gebruikte prospectie- en preserveringstools gegenereerd werden.
 - Voeg eventueel een integrale versie toe van het interview met de overdrager
 - Voeg de nodige documentatie toe over noodzakelijke software, hardware en hulpbestanden.
2. Vervolledig de metadata
- Ga na of de metadataformulieren volledig en correct zijn ingevuld.
 - Vul aan waar de informatie onvolledig is.
 - Vraag indien nodig input van de overdrager.

Opgelet!

Zorg ervoor dat naar alle logbestanden correct wordt gerefereerd in het [SODA invulformulier](#).

In principe zijn alle nodige metadata op dit moment reeds gekend en geregistreerd, en is de formalisering een louter samenbrengen ervan. In de praktijk zullen er echter vaak nog hiaten zijn in de metadata. Controleer daarom alle formulieren en overeenkomsten op hun volledigheid.

9. Creëer een containerbestand

(Laatst gewijzigd: 23-01-2014)



Wat?

Hier creëer je een containerbestand met de [UGent SIP-Creator](#).

SIP is een term uit het [OAIS-model](#). OAIS biedt een kader voor lange termijnbewaring van digitale data. SIP staat voor 'Submission Information Package', het is de verpakking waarmee de data worden opgenomen in een digitaal depot.

In deze stap wordt het overgedragen en geschoonde archief, samen met alle relevante documentatie (logs, metadataformulieren, overeenkomsten, ...) opgeslagen in een containerbestand.

Waarom?

Met de opslag in een containerbestand wordt de bewaartechniek van encapsulatie toegepast. Het archief wordt ingekapseld voor bewaring. Binnen de container zijn het archief en de context (in de vorm van metadata en documentatie) duurzaam met elkaar verbonden.

Wanneer?

Het maken van een containerbestand gebeurt nadat het archief is geschoond, en nadat alle nodige documentatie is samengebracht en aangevuld. Na de creatie van de SIP-Container, wordt deze als één geheel opgeslagen (zie stap 10: [opslag](#)).

Hoe?

Specifiek voor deze procedure ontwikkelde de UGent een SIP-Creator waarmee het

digitale archief en de bijhorende metadata in een container verpakt kunnen worden.

Om deze stap te doorlopen, pas je de uitgebreide [handleiding](#) van de UGent SIP Creator toe.

Eigenschappen:

1. De bestandsnamen worden geüniformiseerd met een Renamer.
 - Deze stap werd in principe reeds toegepast tijdens het [schonen](#).
2. Er wordt een koppeling voorzien tussen de bestanden en metadata (Bags).
3. De integriteit wordt gecontroleerd.
4. Er wordt een SIP gecreëerd.

Meer lezen?

Reference model for an Open Archival Information System (OAIS)

- <http://public.ccsds.org/publications/archive/650x0m2.pdf>
- http://en.wikipedia.org/wiki/Open_Archival_Information_System

http://projectcest.be/index.php/UGent_SIP_Creator:Wie%3F_Wat%3F_Hoe%3F_Waarm%3F

10. Opslag

(Laatst gewijzigd: 23-01-2014)



Wat?

In deze stap verhuist het containerbestand (SIP) van het werkstation naar een duurzame opslagplaats:

- Een [digitaal depot](#)
- Een duurzame serverlocatie

Wanneer?

Het opslaan van het containerbestand is de laatste fase van dit stappenplan. Door deze procedure te volgen heb je de archiefbestanden en hun metadata in een duurzame container samengebracht. Het containerbestand moet nu in een kwalitatief opslagsysteem terecht komen.

Waarom?

Door het volgen van deze handleiding heb je de nodige metadata vastgelegd om bewaring op lange termijn en bewerkingen met het oog op ontsluiting zo vlot mogelijk te laten verlopen. Concrete procedures met het oog op migratie en het toepassen van andere bewaarstrategieën mogen dan wel buiten de scope van dit stappenplan vallen, zonder opslag kan er evenwel geen sprake zijn van archivering.

Hoe?

In zekere zin wordt de cirkel van dit stappenplan hier rond gemaakt. Hoe je vanaf hier verder gaat, wordt immers bepaald door het beleid dat je in de eerste stap van de procedure hebt uitgestippeld (zie Stap 1: [Beleid](#)). In dit onderdeel worden verschillende

mogelijkheden voor opslag aangereikt.

Deze handleiding gaat zo veel mogelijk uit van het gebruik van open source tools. Voor de opslag van digitale archieven is het toepassen van dit principe echter niet evident. Enerzijds wordt dataopslag in eigen huis steeds moeilijker te organiseren, naargelang de hoeveelheid aan data toeneemt. Anderzijds zijn aan het uitbesteden van kwalitatieve dataopslag altijd kosten verbonden.

Algemene principes

- Organiseer je opslag met het oog op duurzame bewaring en duurzame, beveiligde toegang.
 - Formuleer hiertoe procedures voor de omzetting van bestanden naar nieuwe formaten.
- Voorzie mechanismen om de integriteit en authenticiteit van de bestanden onder alle omstandigheden te bewaren, te controleren en te herstellen.
- Beperk en spreid de risico's door het maken van veiligheidskopieën en door deze op verschillende fysieke locaties te bewaren.
- Vermijd volledige afhankelijkheid van één provider.

Alles begint met het uitbouwen van infrastructuur. Hou er rekening mee dat 'server' en 'digitaal depot' geen synoniemen zijn (zie [Glossarium](#))! Een server is een computer die via een netwerk diensten verleent aan andere computers. Een digitaal depot is een opslagsysteem dat speciaal gericht is op langdurige opslag en toegankelijkheid van bestanden. Niet elke server kan dus dienen als digitaal depot.

Ten slotte kan het steeds de moeite lonen om samenwerkingsverbanden aan te gaan met andere archiefinstellingen. Zo wissel je niet alleen expertise uit, maar kan je ook kosten delen.

Digitaal depot

Idealiter wordt de SIP-container opgeslagen in een digitaal depot. Zo een e-depot is het geheel van beleid, systemen en procedures die als doel hebben bestanden toegankelijk en leesbaar te houden op lange termijn. Het is dus méér dan een server.

- Het uitbouwen van een eigen digitaal depot binnen de organisatie, valt buiten de scope van dit project.
 - Voor meer richtlijnen hierover, zie o.a. [Scoremodel](#), [eDAVID](#) en [ED3](#).
- Soms is het mogelijk e-depotruimte van overheden of overkoepelende organisaties te gebruiken. Dit hangt uiteraard af van het werkingsgebied van je instelling.

- Het huren van e-depot service is ook een optie. In de toekomst zullen zich wellicht steeds meer providers voor deze service aanbieden.

Wanneer er geen middelen voorhanden zijn om het archief in een digitaal depot op te slaan, kan je de SIP-container voorlopig op een duurzame serverlocatie zetten.

Duurzame serverlocatie

Een open sourcetoepassing voor het bouwen van een eigen server is [FreeNAS Storage](#)

- Dit is een softwarepakket waarmee je een computer van de organisatie kan omvormen tot een Network Attached Server.
- Dit vereist evenwel een intensieve opvolging:
 - zaken als vervanging, stroomvoorziening en beveiliging moeten volledig zelf georganiseerd worden.
 - Kosten die je uitspaart door de dataopslag zelf te organiseren, moeten worden gecompenseerd met werkuren.
 - Bovendien is de verantwoordelijkheid voor het beheer van de servers niet te onderschatten.
- Om lange termijnbewaring te garanderen moeten onderhoudskosten structureel begroot worden.

Een veel aangeboden alternatief is de opslag op een virtuele server of cloud.

- Hierbij is de fysieke locatie van de bestanden niet bekend.
- Voor deze piste is terughoudendheid geboden wanneer het om archieven gaat.
 - In de praktijk worden bestanden fragmentarisch op verschillende plaatsen opgeslagen en telkens opnieuw samengesteld.
 - Het is niet duidelijk welke invloed deze reconstructieprocessen hebben op de lange termijnbewaring.
 - Bovendien zijn Amerikaanse providers onderworpen aan de zgn. Patriot Act, die niet conform is aan - en zelfs indruist tegen - Belgische en Europese privacyrichtlijnen.

Je kan ook een server huren bij een datacenter.

- Hierbij staat de provider in voor klimaatregeling, beveiliging, stroomvoorziening, technische expertise, enz.
- Het spreekt voor zich dat hier kosten aan verbonden zijn.
- Verdere instructies zijn afhankelijk van de beheerder van dit digitale depot.

Meer lezen?

- [PACKED: Basismodel Preserveringsplan](#)
- [eDAVID: opbouw digitaal depot](#)
- [eDAVID, S. Schaule: Organisatorische aspecten bij het bouwen en het beheren van een digitaal depot](#)
- [ED3: Eisen voor een Duurzaam Digitaal Depot](#)
- Over o.a. NAS en Cloud: <http://194.78.136.105/AMVB/docs/Arduin11.pdf>
- http://www.scoremodel.org/uploads/documents/DCA_D62_Best_practices_for_a_digital_storage_infrastructure_20130506_Version1.pdf
- <http://www.ncdd.nl/blog/?p=2347>

