

# ***Basisprocessen voor een digitaal archiefdepot***

Filip Boudrez  
Expertisecentrum DAVID vzw  
Antwerpen, 2006

## **0. INHOUD**

---

1. Inleiding.....	1
2. Opname en verwerking.....	2
2.1 Controles.....	2
2.2 Transformatie van SIP tot AIP.....	3
2.3 Veiligheidsmaatregelen.....	3
2.4 Beschrijven.....	4
3. Beheer van archiefdocumenten en hun metadata.....	4
3.1 Opslagmedia.....	4
3.2 Bit preservation.....	4
3.3 Metadata.....	4
3.4 Preserving access.....	5
3.5 Technology watch.....	5
3.6 Verzekeren betrouwbaarheid digitaal archiefdepot.....	5
3.7 Verzekeren authenticiteit digitale archiefdocumenten.....	5
3.8 Vernietigen.....	6
4. Beschikbaar stellen.....	6
4.1 Opzoeken.....	6
4.2 Samenstellen van de aanvraag.....	6
4.3 Aantonen authenticiteit digitale archiefdocumenten.....	6
4.4 Gebruikersondersteuning.....	6

## **1. INLEIDING**

---

Voor de langetermijnarchivering van digitale archiefdocumenten is een digitaal depot nodig. Een digitaal depot is niet zomaar een technische infrastructuur waarbinnen digitale archiefdocumenten worden beheerd, maar maakt deel uit van een digitaal archiveringssysteem en krijgt dus mee vorm door de visie op langetermijnarchivering, de kwaliteitsvereisten, de normen en de procedures die hiervoor worden gehanteerd. Het digitaal archiveringssysteem moet ervoor zorgen dat digitale archiefdocumenten op het tijdstip van raadpleging leesbaar, begrijpbaar voor mens en computer, bruikbaar en geloofwaardig zijn. Het digitaal depot geeft dit archiveringssysteem mee gestalte.

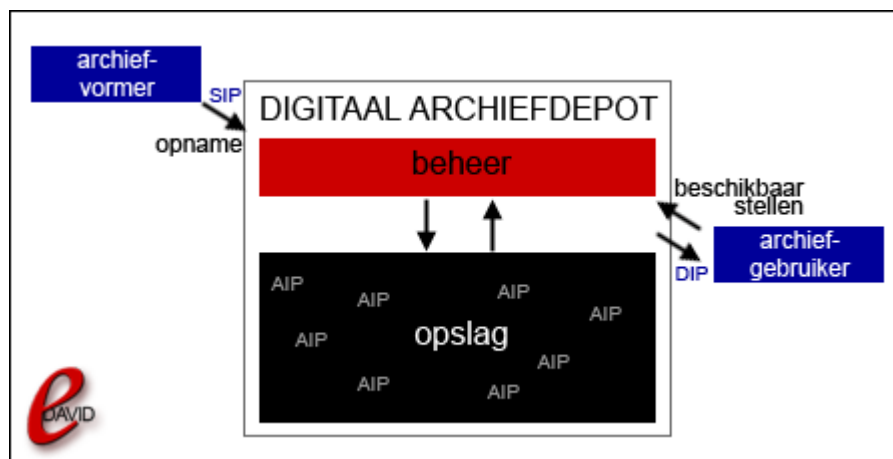
De kern van een digitaal depot wordt gevormd door drie processen, zijnde:

- de opname en verwerking van digitale archiefdocumenten en hun metadata in het digitaal archiefdepot (input)
- de lange termijn opslag en het beheer van de digitale archiefdocumenten en hun metadata
- het beschikbaar stellen van digitale archiefdocumenten en hun metadata die in het digitaal archiefdepot worden beheerd (output)

Dit document geeft voor elk van deze drie processen een overzicht van de activiteiten die mee het proces en bijgevolg het digitaal archiefdepot vormen. Het informatie- en het functioneel model van de OAIS-norm zijn een belangrijke leidraad bij het uitbouwen van de processen binnen een digitaal archiveringssysteem en het vormgeven van een digitaal archiefdepot. Dit overzicht met

basisprocessen volgt dan ook de drie functies die binnen het functioneel model van de OAIS-norm worden onderscheiden: opname, beheer en terbeschikkingstelling. De beschreven processen of functies kunnen op tal van wijzen worden toegepast en corresponderen dus niet noodzakelijk met de modules binnen het systeemmodel voor een operationeel digitaal archiefdepot. Zo kan één procesfunctie door verschillende modules worden uitgevoerd, of kan één module meerdere procesfuncties (tegelijk) uitvoeren.

Onderstaand overzicht is ook afgestemd op de opslagmethode voor digitale archiefdocumenten die eDAVID in 2005 ontwikkelde. In deze opslagmethode vormen XML-containers, bevattende de essentiële metadata en de verschillende verschijningsvormen van digitale archiefdocumenten, de Archive Information Packages (AIP) of de basiseenheden van het digitaal archiefdepot. Binnen deze implementatiewijze vormen de AIP's een fysieke eenheid<sup>1</sup>. Deze opslagmethode bouwt verder op de DAVID-digitale bewaarstrategie en is mee op het OAIS-informatiemodel gebaseerd.



## 2. OPNAME EN VERWERKING

### 2.1 Controles

- inhoud van de transfert:
  - volledigheid: zijn alle geselecteerde digitale archiefdocumenten aanwezig?
  - stemt de overdrachtslijst overeen met de inhoud van de neerlegging:
    - zijn alle getransfereerde (componenten van) digitale archiefdocumenten in de overdrachtslijst geregistreerd en gedocumenteerd?
    - zijn alle digitale archiefdocumenten vermeld in de overdrachtslijst aanwezig in de transfer?
  - is de inhoud van de transfert geschoond?
    - bevat de neerlegging computerbestanden (bijv. systeembestanden) die geen component van één of meerdere digitale archiefdocumenten zijn?
    - zijn er nog lege folders aanwezig?
    - zijn er nog dubbels aanwezig?
    - zijn er nog reserve- of veiligheidskopieën aanwezig?
- geldigheid van de SIP's:
  - verificatie van de bitintegriteit van de getransfereerde digitale objecten

<sup>1</sup> F. BOUDREZ, *Digitale containers voor het digitale archiefdepot*, Antwerpen, 2005 ([http://www.expertisecentrumdavid.be/docs/digitale\\_containers.pdf](http://www.expertisecentrumdavid.be/docs/digitale_containers.pdf)).

- identificatie van de digitale objecten met onbekend bestandsformaat
- validatie van de digitale objecten en hun bestandsformaat
- validatie van de getransfereerde representatie(s) van de digitale archiefdocumenten:
  - zijn de voorgeschreven of afgesproken representaties aanwezig?
  - zijn de aanwezige representaties conform het voorgeschreven profiel?
  - zijn de representaties conform de formele formaatspecificatie?
  - zijn paswoorden en/of encryptie verwijderd?
- validatie van de aangeleverde metadata:
  - zijn de metadata conform het voorgeschreven of het overeengekomen formaat?
  - zijn de vereiste metadata aanwezig?
  - zijn de metadata correct?
- aanwezigheid computervirussen: zijn de getransfereerde digitale objecten vrij van computervirussen?
- bewaken van de bitintegriteit van de digitale objecten tijdens hun quarantaineperiode en in afwachting van verwerking tot AIP's.

## 2.2 Transformatie van SIP tot AIP

- verwijderen van computerbestanden (bijv. systeembestanden) die niet tot de overeengekomen overdracht behoren
- migratie:
  - indien nodig, migratie van de digitale informatieobjecten naar geschikt archiveringsformaat
  - documenteren van de migratie
  - validatie van de migratie
- inkapseling:
  - verpakken van de originele en gemigreerde verschijningsvormen en hun essentiële metadata in één XML-container
  - toevoegen van beschrijvende metadata over het archiefdocument of het archiefbestanddeel aan de AIP
  - documenteren van de inkapseling
  - validatie van de inkapseling
  - toekennen van een uniek ID aan de AIP
- metadata:
  - opname van de getransfereerde metadata in RKMS
  - aanvullen van de getransfereerde metadata: expliciteren van de archiefcontext

## 2.3 Veiligheidsmaatregelen

- voorzien van een quarantaine periode voor anti-viruscontrole
- registreren van de bitintegriteitsinformatie:
  - berekenen checksums
  - vastleggen pariteitsinformatie
- veiligheidskopie maken van de digitale archiefdocumenten en hun metadata
  - mirroring: replicatie / duplicatie
- back-up maken van de getransfereerde of verwerkte digitale archiefdocumenten

## 2.4 Beschrijven

- toevoegen beschrijvingen aan RKMS:
  - registreren van de relatie tussen digitale objecten en digitale archiefdocumenten
  - extractie identificerende, beschrijvende, authenticatie en technische metadata uit SIP/AIP en de digitale objecten
  - (geautomatiseerd) toevoegen van beheersmetadata
  - linken archiefbestanddelen aan context, ISAAR, en representation information authority records
  - vastleggen bewaartermijnen
  - vastleggen ACL
- permanente koppeling tussen archiefdocumenten en hun metadata voorzien
- koppelen unieke ID's digitale objecten met:
  - hun metadata
  - hun (fysieke) vindplaats
- aanpassen van het retrieval-systeem:
  - updaten van de indexen

## 3. BEHEER VAN ARCHIEFDOCUMENTEN EN HUN METADATA

---

### 3.1 Opslagmedia

- continue en systematische monitoring van de kwaliteit, de performantie en de degradatie van de gebruikte opslagmedia
- preventief refreshen van de opslagmedia
- beheren/controleren van de storage hiërarchie
- controleren hard- en softwarecomponenten voor het lezen van de gegevens op de opslagmedia

### 3.2 Bit preservation

- continue en systematische monitoring van de aanwezigheid en de bitintegriteit van bewaarde digitale objecten (ook in mirrors)
  - zijn alle digitale objecten nog aanwezig?
  - zijn alle digitale objecten nog intact?
- bij vaststellen fout in de bitopslag:
  - terugplaatsen veiligheidskopie, of
  - verbeteren van de fout dmv de pariteitsinfo, of
  - restoren back-up

### 3.3 Metadata

- continue en systematische monitoring van de bitintegriteit van de metadata binnen het RKMS
- continue en systematische monitoring van de links, pointers of referenties tussen:
  - gerelateerde metadata
  - een digitaal archiefdocument en zijn metadata
- up-to-date houden / aanvullen van preservation description information en representation information
- beheren relatie computerbestanden, archiefdocumenten en hun vindplaats

### **3.4 Preserving access**

- onderhouden van een digitale bewaarstrategie voor de digitale archiefdocumenten en hun metadata (inclusief RKMS):
  - plannen van een migratiepad
  - plannen van emulatieprogramma's
- verzamelen en bewaren van viewers
- verzamelen en bewaren van representation information:
  - aanvullen authority records

### **3.5 Technology watch**

- tijdig aanpassen/vervangen van:
  - hard- en softwarecomponenten van het digitaal depot
  - de toegepaste geschikte archiveringsformaten
  - de gebruikte emulatieprogramma's
- up-to-date houden van representation information
- ondersteunde import- en exportformaten (SIP en DIP) voor de metadata

### **3.6 Verzekeren betrouwbaarheid digitaal archiefdepot**

- documenteren van:
  - de tools die worden gebruikt
  - de systeemarchitectuur van het digitaal archiefdepot
  - de toegepaste opslagmethode:
    - organisatie van de digitale objecten binnen het digitaal archiefdepot
    - het metadata-datamodel
- verzekeren transparantie
- definiëren gebruikersgroepen, rollen en hun rechten
- definiëren welke acties zijn toegelaten en welke niet
- bijhouden audit-trail op de acties binnen het digitaal archiefdepot
- certificering (peer review?)
- disaster recovery:
  - mirror bewaren off site
  - back-ups maken

### **3.7 Verzekeren authenticiteit digitale archiefdocumenten**

- voorkomen van (onrechtmatige) wijzigingen van de digitale archiefdocumenten en hun metadata: fixeren van de content
- aantonen dat archiefdocumenten niet werden gewijzigd, maar nog identiek zijn
- voorkomen dat archiefdocumenten worden verwijderd vooraleer hun bewaartermijn is verstreken
- documenteren van:
  - de archiefbewerkingen
  - het continue beheer van de archiefdocumenten binnen het digitaal archiefdepot ('chain of custody')

### **3.8 Vernietigen**

- uitvoeren van de vernietigen na verstrijken van de bewaartermijn
- registreren van de uitgevoerde vernietigingen

## **4. BESCHIKBAAR STELLEN**

---

### **4.1 Opzoeken**

- beschikbaarstellen archieftoegangen
- verwerken van de gebruikersverzoeken
- lokaliseren van de gevraagde archiefdocumenten
- beheren toegangscontrole

### **4.2 Samenstellen van de aanvraag**

- transformatie van de AIP tot DIP:
  - samenstellen archiefdocument in gewenste verschijningsvorm: maken van een (raadplegings)kopie; extractie uit AIP
  - validatie van de (raadplegings)kopie
  - selecteren van de metadata die aan de archiefgebruiker wordt bezorgd
  - archiefgebruiker de kopie en de bijhorende archiefbeschrijvende metadata bezorgen: i.c. de metadata op documentniveau met een link naar de archiefcontext
- verificatie/authenticatie van de DIP: aantonen betrouwbaarheid of authenticiteit van het bewaarde en het beschikbaar gestelde digitaal object

### **4.3 Aantonen authenticiteit digitale archiefdocumenten**

- archief gebruikers bewijs leveren dat de digitale archiefdocumenten authentiek zijn:
  - metadata verstrekken
  - DIP tekenen met archiefsleutel
  - kopie certificaat bezorgen

### **4.4 Gebruikersondersteuning**

- ter beschikking stellen viewer(s)
- ondersteuning aanbieden (help?, FAQ, gebruikersinstructies)