



DAVID

Wat archiveren en hoe? Op zoek naar de rol van PKI voor digitale archieven

Sofie Van den Eynde



FACULTEIT RECHTSGELEERDHEID
INTERDISCIPLINAIR CENTRUM VOOR RECHT EN
INFORMATICA
TIENSESTRAAT 41
B-3000 LEUVEN



Stadsarchief
Stad Antwerpen

Versie 1.0

Wettelijk depot D/2001/9.213/4

Leuven, juni 2001

Inhoudstafel

I. Inleiding	4
II. OAIS Reference Model	4
A. Achtergrond	4
B. waarom OAIS als uitgangspunt?	5
III. Wat moet er precies bewaard worden voor de bewaring op lange termijn van digitale informatie?	6
A. Inhoud	7
B. Voorstellingsinformatie	7
1. Fysieke laag	8
2. Binaire laag	9
3. Structuurlaag	10
4. Objectlaag	11
5. Applicatielaag	12
C. Interpretatieve informatie	13
1. Authenticiteits- en integriteitsgaranderende informatie	13
2. Herkomst van het informatieobject	13
3. Semantische informatie	14
4. Contextinformatie	14
D. Pakketinformatie	15
E. Pakketbeschrijving	15
IV. De verschillende fases van het digitale archiveringsproces	16
A. De spelers in het veld	16
1. De archiefvormer	17
2. De klant	17
3. De archiefinstelling	17
B. Vier fases	20
1. Invoer	20
2. Opslag	36
3. Toegang en Data Management	39
4. Beleid	45
V. Besluit: De rol van PKI bij digitale archieven	46

I. Inleiding

De bedoeling van dit document is in de eerste plaats om te onderzoeken hoe PKI (Public Key Infrastructure) een rol kan spelen bij de archivering van digitale informatie. PKI is een kader van procedures, policies, personeel en applicaties, gebaseerd op *Public Key Cryptography*, aan de hand waarvan digitale informatie(stromen) kan (kunnen) beveiligd worden. Klassiek vindt men in PKI-middens de volgende definitie terug: “PKI is een systeem dat aan gebruikers van elektronische communicatiemiddelen digitale sleutelparen (telkens bestaande uit een private key en een public key) ter beschikking stelt, aan de hand waarvan zij hun elektronische communicatie kunnen beveiligen en authenticeren. De techniek van de digitale handtekening is één van de vele toepassingen van dit systeem.¹” Deze definitie sluit vooral goed aan bij een e-commerce scenario, waarbij allerlei transacties moeten beveiligd worden, zodat het rechtsverkeer op een betrouwbare wijze kan verlopen. Het communicatieaspect is echter niet altijd aanwezig bij alle bewerkingen die er met digitale archiefstukken (moeten) gebeuren. De toepassing van PKI in een archiveringscontext, noopt daarom tot een uitbreiding van de klassieke definitie.²

Om het nut van PKI te evalueren voor de archiefwereld, is het nodig om een inzicht te krijgen in de levensloop van een digitaal archiefstuk en de stappen die daarbij moeten gezet worden. We trachten op een zo begrijpelijk mogelijke wijze in kaart te brengen welke acties er allemaal moeten ondernomen worden om digitale informatie permanent te bewaren. Hiervoor lieten we ons inspireren door het OAIS-Reference model.

II. OAIS Reference Model

A. ACHTERGROND

Het *Open Archival Information System* is een model dat tot stand is gekomen in de schoot van het *Consultative Committee for Space Data Systems (CCSDS)* en de *International Standardization Organization (ISO)*. Het CCSDS werd in 1982 opgericht door verschillende ruimtevaartorganisaties, waaronder NASA, met als doel zich bezig te houden met problemen rond informatiesystemen in de ruimtevaartsector. Sinds de jaren ‘60 hadden deze organisaties te kampen met verschillende technologische evoluties. In 1990 ging het CCSDS een samenwerking aan met ISO en werd lid van het technisch comité 20 (aircraft and space vehicles), subcomité 13 (space data and information transfer systems). ISO richtte zich tot SC 13 met het voorstel om een standaard te ontwikkelen met betrekking tot de archivering op

¹ Zie *A Practical Guide to Public Key Infrastructure*, Xcert International, 1999; <http://webopedia.internet.com/TERM/P/PKI.html>

² Door het gebrek aan uniforme PKI-standaarden op dit moment, vindt men zoveel verschillende definities terug van PKI als er betrokkenen zijn. Het communicatie-aspect komt echter steeds opnieuw terug.

lange termijn van digitale gegevens in het algemeen en met betrekking tot gegevens verzameld in het kader van de ruimtevaart in het bijzonder.

Het CCSDS trad op als coördinator bij het ontwerpen van een *Recommendation*. Er werd geopteerd voor de ontwikkeling van een *Reference Model* met de bedoeling om algemene concepten en termen te definiëren. Het model spitst zich niet enkel toe op de ruimtevaartgemeenschap, maar richt zich tot alle disciplines die te maken hebben met de bewaring op lange termijn van digitale data, o.a. de archiefwereld, maar ook digitale bibliotheken, wetenschappelijke informatie- en documentatiecentra enz. Het model richt zich tot verschillende groepen: ontwerpers van archiefsystemen, de gebruikers van digitale archieven (zowel de archiefvormers als de klanten), de personen die het beleid bepalen inzake archivering (bijv. de wetgever) en de ontwikkelaars van archiefstandaarden.

B. WAAROM OAIS ALS UITGANGSPUNT?

Waarom kiezen we het *OAIS Reference Model* als uitgangspunt om in kaart te brengen waar PKI zijn diensten kan bewijzen ten aanzien van een digitaal archief? Hiervoor zijn verschillende redenen:

1. Het *OAIS Reference Model* is goed onthaald door de verschillende disciplines die te maken hebben met de bewaring van digitale informatie op lange termijn. Heel wat digitale initiatieven o.a. uit de bibliotheekwereld³, maar ook uit de archiefwereld hebben het model geïmplementeerd voor de digitale bewaring van hun collecties. De bekendste organisatie uit de archiefsector die dit model aangenomen heeft is NARA, *the U.S. National Archives and Records Administration*. NARA inventariseert, bewaart en verschaft toegang tot de digitale documenten die aangemaakt worden door de verschillende departementen van de federale overheid van de Verenigde Staten. Men kan dus verwachten dat het *OAIS Reference Model* nadrukkelijk aanwezig zal zijn in heel wat toekomstige initiatieven met betrekking tot digitale archivering.
2. Het *OAIS Reference Model* is op dit moment een ISO ontwerp-standaard. Het werd voor goedkeuring overgemaakt aan ISO. Er wordt verwacht dat het binnen afzienbare termijn als volwaardige ISO-standaard zal aangenomen worden. Momenteel heeft het de status van *CCSDS Red Book*, wat wil zeggen dat het een *Draft Recommendation* is, die open staat voor commentaar. De term 'Open' slaat op het feit dat het model tot stand is gekomen in publieke fora en dat het open staat voor beoordeling door iedereen. Het slaat

³ O.a. het Nedlib-project (*Networked European Deposit Library*). Dit project wordt gefinancierd door het *Telematics Applications Programme* van de Europese Commissie en het wordt geleid door de Koninklijke Nationale Bibliotheek van Nederland. Een van de resultaten van dit project is de ontwikkeling van een model voor de ontwikkeling van een *Deposit System for Electronic Publications (DSEP)*, gebaseerd op het OAIS-model. De bedoeling was om de vereisten in kaart te brengen waaraan alle bibliotheken moeten voldoen, om zo tot een algemeen ontwerp te komen dat kan geïmplementeerd worden met oog voor de concrete situatie van de betreffende bibliotheek. Ook digitale archiveringsprojecten hebben ervoor gekozen om het OAIS-model toe te passen, zoals het Cedars-project in het Verenigd Koninkrijk (<http://www.leeds.ac.uk/cedars>).

geenszins op het feit dat een archief dat aan het model beantwoordt, onbeperkt toegankelijk zou zijn voor alle klanten.

3. Het hoge abstractieniveau van het *OAIS Reference Model* en het technologie-neutraal karakter maken het een uiterst geschikt middel om uit te leggen waaraan een digitaal archief moet voldoen om voldoende waarborgen te bieden voor leesbaarheid en toegankelijkheid op lange termijn, onafhankelijk van de praktische en technische organisatie van de archiefinstelling. Het is dan ook geen model dat onmiddellijk kan geïmplementeerd worden. Het is een organisatiemodel dat op alle mogelijke archieven kan toegepast worden, geen kant-en-klaar draaiboek voor het uittekenen van een digitaal ondersteunde archief functie in een bepaalde organisatie. Als algemeen uitgangspunt is een dergelijk model erg bruikbaar, aangezien er niet één beste oplossing bestaat voor de archivering van digitale informatie. Er zal archiefinstelling per archiefinstelling en afhankelijk van de te archiveren informatie in een concreet geval moeten bekeken worden hoe er aan de hand van het model voor een passende oplossing kan gekozen worden.⁴ Daarvoor zullen er verschillende archivistische en technologische keuzes moeten gemaakt worden. Iedere archiefinstelling zal ook een op maat gemaakt PKI-model moeten uittekenen, geïnspireerd door de gemaakte keuzes.

III. Wat moet er precies bewaard worden voor de bewaring op lange termijn van digitale informatie?⁵

In de papieren wereld is de papieren drager datgene wat men in eerste instantie bewaart. Het bewaren van het papieren document in goede staat is de enige en tevens een voldoende bewerking om de informatie die het bevat veilig te stellen voor de toekomst. In een digitale wereld gaat het echter niet op om de drager gelijk te stellen met de te bewaren informatie.⁶ Wanneer de juiste maatregelen genomen worden bij de archivering, overleeft digitale informatie immers de drager waarop zij is opgeslagen. De drager kan niet voor onbepaalde tijd bewaard worden omdat de levensduur ervan en van de hardware die nodig is om de drager te lezen, beperkt is. Een essentieel inzicht bij de bewaring van digitale informatie moet daarom zijn dat de bewaring zich enkel richt op de pure inhoud, meer bepaald op de data die deze inhoud voorstellen. In een digitale omgeving zullen die data steeds uit bitreeksen bestaan. Het zijn deze bitreeksen waarvoor de archivaris zorg moet dragen en niet meer zozeer voor de drager zelf. Het voorwerp van de bewaring heeft zich in de digitale wereld verlegd van de drager naar de data zelf.⁷

⁴ BAAK, P. en KOENEN, K., 'Het geheugen als actieve kracht. De archief functie binnen de digitale overheid', Programma Digitale Duurzaamheid, Den Haag, 1999, 13.

⁵ Dit deel kwam tot stand met de hulp van de onderzoeksgroep Document Architecturen van de afdeling Toegepaste Electronica en Optiek van de K.U.Leuven.

⁶ Dit is te wijten aan het feit dat bewaartermijnen de levensduur van digitale dragers te boven gaan. Dat de digitale drager tijdens de bewaartermijn moet vervangen worden, staat op voorhand reeds vast. Bij papier is dit veel minder zeker. Zeker wanneer er een goede kwaliteit van papier werd gekozen en dit papier in goede omstandigheden wordt bewaard, kan dit zelfs enkele eeuwen meegaan. Bewaartermijnen blijven meestal ver onder de levensduur van papier.

⁷ Dit wil natuurlijk niet zeggen dat er geen zorg moet besteed worden aan de digitale drager. Immers, ook al staat de te bewaren informatie in principe los van elke drager, toch vergt het bestaan van een

Voor de bewaring op lange termijn van digitale informatie is het uiteraard niet voldoende dat enkel die bitreeks geïdentificeerd en bewaard wordt in het archiefsysteem, die de informatie voorstelt waarvan de bewaring beoogd wordt. Opdat deze informatie voor een onbepaalde termijn efficiënt in zijn oorspronkelijke staat voorhanden zou zijn, moet er veel meer bewaard worden dan de inhoud alleen. Al deze informatie over de inhoud waarvan de bewaring beoogd wordt, noemt men 'metadata'. Het komt er dus op aan om een informatiepakket samen te stellen dat alle elementen bevat die noodzakelijk zijn om de inhoud leesbaar en beschikbaar te houden op lange termijn. Hoe zo'n informatiepakket er idealiter uitziet, bekijken we in de volgende secties. In deel IV analyseren we de verschillende fases bij de werking van een archiefsysteem dat gebruik wil maken van het OAIS-model.

Vooraf moet er opgemerkt worden dat de informatie die nodig is voor de lange termijn bewaring van digitale informatie (de inhoud), ook meestal bitreeksen zijn.⁸ Voorafgaand aan de archivering moeten er dus verschillende bitreeksen geïdentificeerd, geselecteerd en eventueel door de archivaris aangelegd worden.

A. INHOUD

Op de eerste plaats moet natuurlijk de informatie waarvan de bewaring beoogd wordt, zijnde de inhoud, geïdentificeerd worden. Wat wil men bewaren: een tekst, een e-mailbericht, meerdere databanken enz.? Voor de geselecteerde inhoud moet het achterliggende data-object geïdentificeerd worden. Data zijn de voorstellingsvorm van informatie en kunnen cijfers, letters, symbolen (leesbaar voor de mens) of bits (onleesbaar voor de mens) zijn. In een digitale omgeving zullen de data steeds bits zijn. De bitreeks die de te archiveren informatie voorstelt, moet uiteraard bewaard worden.

B. VOORSTELLINGSINFORMATIE

In een papieren omgeving vallen de data en de informatie samen: het geheel van de data is onmiddellijk begrijpelijk voor de mens. In een digitale omgeving is dit anders. Het geheel van bits moet eerst door een PC vertaald worden naar voor de mens begrijpelijke tekens. Bij de archivering van de inhoud moeten er bijgevolg maatregelen genomen worden die ervoor zorgen dat de bits die deze inhoud voorstellen, nog terug kunnen omgevormd worden naar voor de mens begrijpbare informatie. Dit is de problematiek van de leesbaarheid van de digitale informatie op korte termijn, ook wel de presenteerbaarheid genoemd. Met korte termijn bedoelen we dat de gearchiveerde digitale informatie vanaf het moment van de archivering (en op ieder moment daarna) leesbaar moet kunnen zijn. De impact van de veranderende technologie wordt in dit stadium nog niet mee in overweging genomen.

digitaal archiefstuk vanuit praktisch oogpunt een drager die de digitale informatie tijdelijk vasthoudt.

⁸ In sommige gevallen zou men ervoor kunnen opteren deze bijkomende informatie als *hard copy* te bewaren, omdat zij steeds moet beschikbaar blijven. Het is natuurlijk de uitdaging om te zorgen dat ook de heel belangrijke gegevens op lange termijn in digitale vorm kunnen bewaard worden, zodat er uiteindelijk niets meer op papier moet bijgehouden worden.

Alle metadata die nodig zijn om de data leesbaar te houden op korte termijn, noemt men in het OAIS-model de ‘voorstellingsinformatie’. De voorstellingsinformatie maakt het mogelijk om de bits te herleiden naar voor de mens algemeen bekende data, zoals tekens, getallen, tabellen enz. De voorstellingsinformatie voegt dus betekenis toe aan de bits en deze informatie moet toelaten om de bitreeks te converteren in meer betekenisvolle informatie. Er moet een lange weg afgelegd worden van de data die op de drager staan naar de voor de mens begrijpelijke boodschap. In de informaticawereld wordt dit gewoonlijk voorgesteld aan de hand van vijf lagen van software, die nodig zijn om deze omzetting te kunnen voltooien.⁹ Elke hogere laag van software is afhankelijk van de resultaten van de bewerkingen in de lagere lagen.

1. Fysieke laag

a) *Beschrijving*

Alle digitale informatie, al dan niet reeds gearchiveerd, staat hoe dan ook op een drager. Door het ongrijpbare en vluchtige karakter van digitale informatie, lijkt deze enkel te bestaan op het beeldscherm dat als tijdelijke drager fungeert. Toch is er steeds een drager die deze informatie op een meer permanente wijze vasthoudt.¹⁰ De drager van gearchiveerde informatie hangt af van de wijze waarop de informatie werd gearchiveerd. Het is mogelijk dat de informatie op een externe drager werd gezet voor archiveringsdoeleinden bijv. op een CD-rom (= een optische drager) of op een diskette (= een magnetische drager). In de archieven van de toekomst zal digitale informatie echter vooral in een netwerkomgeving gearchiveerd worden. De drager is dan bijv. de harde schijf van de server.

De functie van de fysieke laag bestaat erin om de informatie die op de drager staat, om te zetten naar een drageronafhankelijke bitreeks. De wijze waarop de informatie op de drager is weergegeven, kan immers niet door de computer gelezen worden. In het geval van een optische drager, gaat het bijv. om kleine kuiltjes in de schijf. Op een magnetische drager is de informatie voorgesteld aan de hand van magnetische ladingen.¹¹ De software die gebruikt wordt in de fysieke laag, zegt dus hoe je de bitreeks van de drager moet halen. Deze software is opgeslagen in chips die zich bevinden in de apparatuur die gebruikt wordt om de drager te lezen.

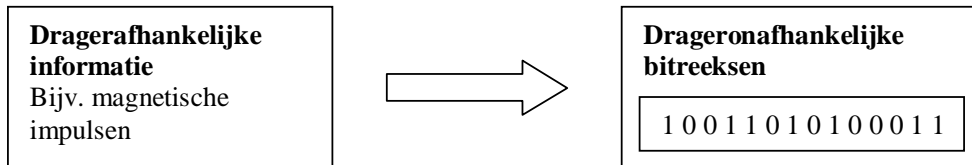
⁹ Reference Model for an Open Archival Information System, annex E.

¹⁰ VAN DEN EYNDE, S., *Digitale archivering: een juridische stand van zaken. Deel 1*, Leuven, ICRI, 2001, 58.

¹¹ Optische dragers zijn dragers van informatie die op een schijf wordt vastgelegd in de vorm van kleine kuiltjes, die bij het inlezen door een laserstraal wordt afgetast. De lichtreflecties worden omgezet in een elektrisch signaal dat de oorspronkelijke data reproduceert. Optische dragers hebben twee grote voordelen nl. hun informatiedichtheid en bijgevolg hun hoge opslagcapaciteit en de contactloze uitlezing van de data, waardoor slijtage bijna volledig wordt uitgesloten. Magnetische dragers zijn dragers die bestaan uit een magneetband die onder invloed van een magneetkop (een spoel die door middel van elektrische stroom een magnetisch veld oproept) wordt gemagnetiseerd. Hierdoor vertonen de microscopisch kleine deeltjes op de band een bepaald patroon.

b) *Te archiveren metadata*

Informatie over de software die nodig is om de drager te kunnen lezen, moet mee gearchiveerd worden. De meeste hardware ondersteunt de software die nodig is voor de meest courante dragers, omdat er daarvoor standaarden zijn ontwikkeld. Het is dan voldoende om naar die standaarden te verwijzen. Zo is er de ISO 9660-standaard voor CD-roms.¹² De meeste CD-roms zijn in ISO 9660 formaat beschreven. Deze standaard beschrijft onder andere de wijze waarop de informatie op de CD-rom is opgeslagen.



2. **Binaire laag**

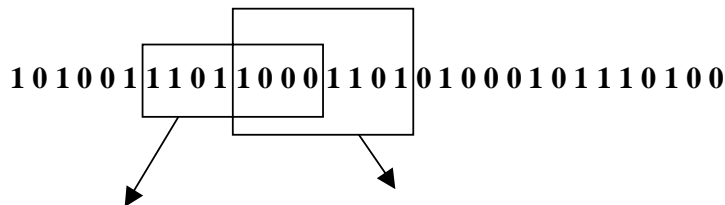
a) *Beschrijving*

In de binaire laag worden de lange bitreeksen opgedeeld in stukken van beperkte lengte. De software die in deze laag gebruikt wordt, bepaalt welke opeenvolgingen van 1-en en 0-en samen horen om betekenis te kunnen krijgen in een volgende laag. Simpelweg gezegd komt het er op neer dat in deze laag wordt gezegd hoe de bits moeten worden gegroepeerd tot ‘pakketjes’ of *bytes*. Het bestandssysteem, ook wel *file system* genoemd, is de software die hiervoor wordt aangewend. Het bestandssysteem is een onderdeel van het besturingssysteem. Er bestaan verschillende soorten bestandssystemen. Sommige systemen groeperen de bits per acht, andere per zestien, per tweëëndertig enz.

b) *Te archiveren metadata*

Informatie over het gebruikte bestandssysteem moet voorhanden zijn. Een bepaald bestandssysteem draait meestal niet onder één bepaald besturingssysteem, maar ieder besturingssysteem heeft gewoonlijk wel een voorkeur voor een bepaald bestandssysteem. Windows NT bijv. functioneert met NTFS (*NT File System*) als bestandssysteem, terwijl Windows 95 werkt met FAT (*File Allocation Table*).

Meestal zal de informatie over het soort bestandssysteem niet apart mee moeten gearchiveerd worden, vermits het besturingssysteem uit zichzelf ‘weet’ hoe de bits gegroepeerd worden. In principe moet men dus enkel de naam en de versie van het besturingssysteem mee archiveren.



¹² <http://www.iso.ch> Zie de zeer volledige webpagina over CD's: <http://www.disctronics.co.uk/cdref/cd-rom/cdromspec.htm>

WEL

NIET

3. Structuurlaag

a) Beschrijving

Deze laag is enkel van belang wanneer men een computerprogramma wil gaan archiveren. Een computerprogramma is digitale informatie die in een bepaalde programmeertaal is opgemaakt en waarmee de computer allerlei bewerkingen kan uitvoeren. Deze laag definieert hoe de bytes waaruit het programma bestaat, moeten gecombineerd worden tot op zich staande gehelen waarnaar de computer zich kan richten en die de computer kan interpreteren, zoals bijv. primitieve datatypes. Primitieve datatypes zijn de bouwstenen van software. Men spreekt onder andere van *characters* (karakters), *integers* (gehele getallen) en *reals* (kommagetallen). Een reeks van informatie die uit dezelfde datatypes bestaat, noemt men een *array*. Een voorbeeld van informatie uit deze laag die moet gearchiveerd worden, zou de omschrijving kunnen zijn van wat het programma onder een geheel getal verstaat (zie schema). De informatie over hoe de software is opgebouwd, zit vervat in de programmeertaal waarin de software is opgesteld.

Wanneer men het gearchiveerde programma na een bepaalde periode opnieuw nodig heeft, is (informatie over) de programmeertaal niet voldoende om het programma bruikbaar te houden. Er zal er ook programmatuur nodig zijn die de broncode van het programma kan omzetten in code die leesbaar is voor de computer. De programmeertaal waarin de broncode is opgesteld, is immers niet leesbaar voor de computer. Het programma kan enkel draaien via de voor de mens onleesbare code die achter de broncode schuil gaat. Dergelijke programma's die de broncode van software kunnen omzetten naar computercode, noemt men *compilers* of *interpreters*.

b) Te archiveren metadata

Bij de archivering van de broncode van een computerprogramma moet er informatie over de compiler gearchiveerd worden, zodat het na jaren nog mogelijk is om het computerprogramma te laten draaien op de computer. Want indien de te gebruiken compiler onbekend is, wordt de broncode onbruikbaar. Ook informatie over de gebruikte programmeertaal wordt best mee gearchiveerd, omdat hierin is gedefinieerd hoe de software moet geïnterpreteerd worden. Het heeft geen zin dat de broncode op zich leesbaar is voor de computer dankzij de omzetting naar machinetaal door de *compiler*, als niet duidelijk is hoe de elementen van die machinetaal moeten samengelezen en geïnterpreteerd worden.

1 0 0 1 0 1 1 1	1 0 0 1 0 1 1 1	1 0 0 1 0 1 1 1	1 0 0 1 0 1 1 1	= INTEGER
-----------------	-----------------	-----------------	-----------------	-----------

2^{32} gehele getallen zijn er mogelijk als een geheel getal op deze wijze is vastgelegd in de programmeertaal

4. Objectlaag

a) *Beschrijving*

Binaire code op zich (bits en bytes) is niet begrijpbaar voor de computer. Aan iedere bitreeks beantwoordt er een hexadecimale code. Bij het inlezen van de informatie door de computer gebeurt er automatisch een omzetting van de bitreeks naar hexadecimale code. Deze code heeft wel betekenis voor de computer. Het hexadecimale talstelsel gebruikt zestien basisnummers alvorens deze basisnummers te combineren om het zeventiende nummer aan te duiden. Onderstaande tabel geeft een vergelijking van het decimale, het hexadecimale en het binaire talstelsel. Het vetgedrukte nummer geeft telkens aan waar de combinatie van de nummers begint.

Binair	hexadecimaal	decimaal
0	0	0
1	1	1
10	2	2
11	3	3
100	4	4
101	5	5
110	6	6
111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15
1111	10	16

In deze laag wordt er software gebruikt om semantiek toe te voegen aan de structuur. Hexadecimale code is niet begrijpbaar voor de mens. Het bestandsformaat waarin de informatie is opgemaakt, bepaalt welk hexadecimaal getal overeenstemt met een bepaald voor de mens verstaanbaar gegeven (bijv. de letter A). Er moet dus een omzetting plaatsvinden. Er bestaan vele bestandsformaten, zowel open als gesloten bestandsformaten. Van een open bestandsformaat is algemeen bekend hoe de omzetting gebeurt en dus welke voor de mens verstaanbare data bij welke hexadecimale cijfers horen. Bij een gesloten bestandsformaat weet enkel de uitvinder van het formaat hoe de omzetting gebeurt. JPEG (voor beeldbestanden), MPEG (voor bewegende beelden en geluidsbestanden) zijn bijv. open

bestandsformaten; Doc (voor tekstbestanden) en EBCDIC (ondersteund door IBM) zijn dan weer vendorafhankelijke bestandsformaten.

c) Te archiveren metadata

Een vermelding van het bestandsformaat moet mee gearcheveerd worden, zodat later de conversie nog steeds correct kan gebeuren naar voor de mens begrijpbare data. Er wordt best ook een beschrijving van het bestandsformaat mee gearcheveerd met het oog op de veroudering ervan waardoor het niet meer ondersteund wordt. Wanneer er een standaard bestaat over het bestandsformaat, kan het volstaan om een verwijzing naar deze standaard te archiveren.¹³ Men moet er dan wel op letten dat men de verwijzing naar de juiste (versie van de) standaard archiveert.

4A = k
92 = K
7D = ?

5. Applicatielaag

a) Beschrijving

Nu de informatie op een voor de mens verstaanbare wijze aanwezig is in de computer, betekent dat nog niet dat deze informatie ook waarneembaar is voor de gebruiker. Daarvoor is de laatste laag nodig, die zich op het hoogste niveau bevindt. In deze laag bevindt zich de applicatiesoftware, die als interface fungeert naar de gebruiker toe en die de betekenisvolle informatie waarneembaar maakt voor de gebruiker.

b) Te archiveren metadata

Een vermelding van de te gebruiken (versie van de) applicatiesoftware moet mee gearcheveerd worden.

Applicatiesoftware	Bestandsformaat
Adobe Photoshop	Beeldbestandsformaten o.a. JPEG, TIFF
Notepad	Tekstbestandsformaten
Word	Doc-bestanden
...	

Datgene wat we tot hier beschreven hebben, wordt in het OAIS-model de structurele voorstellingsinformatie genoemd. In dit model bestaat er nog een tweede soort voorstellingsinformatie: nl. de semantische voorstellingsinformatie. Dit is de informatie

¹³ Bijvoorbeeld ISO/IEC 10646. ISO/IEC 10646 is de eerste geofficialiseerde standaard van een bestandsformaat (Unicode) dat alle characters van iedere taal in de wereld een unieke code toekent.
<http://www.nada.kth.se/i18n/ucs/unicode-iso10646-oview.html>
<http://www.unicode.org>
<http://www.mulberrytech.com/papers/unicode>

zonder dewelke de inhoud niet begrijpbaar is voor de mens. Deze informatie behandelen wij onder de categorie van de interpretatieve informatie.

C. INTERPRETATIEVE INFORMATIE

De voorstellingsinformatie is nodig om de leesbaarheid of de presenteerbaarheid van de gearchiveerde digitale informatie te garanderen. Aan de hand van deze metadata kan men achterhalen en voorstellen welke voor de mens verstaanbare data er schuil gaan achter de binaire data. Dit is wat men verstaat onder leesbaarheid op korte termijn van digitale informatie.

Opdat men aan deze voor de mens verstaanbare data ook nog een betekenis zou kunnen toekennen, is er echter bijkomende informatie nodig. Deze metadata noemt men de interpretatieve informatie. Het zijn alle gegevens die ervoor zorgen dat men zich een mening kan vormen over de gearchiveerde inhoud o.a. met betrekking tot de authenticiteit, de relatie van de inhoud tot de omgeving waarin hij werd gecreëerd, de herkomst van de informatie... Deze informatie is niet in de eerste plaats bestemd om te worden verwerkt door de software van de computer, maar om te worden verwerkt door de mens, zodat deze zich een oordeel kan vormen over het digitale archiefstuk.

1. Authenticiteits- en integriteitsgaranderende informatie

Vooreerst zijn er de metadata die de integriteit en de authenticiteit van het informatieobject aantonen. Deze informatie bevat de middelen aan de hand waarvan kan gecontroleerd worden of de gearchiveerde inhoud authentiek en integer is en documenteert deze authenticatiemiddelen. Werd er bijv. door de auteur van een document een elektronische handtekening gebruikt als authenticatietechniek, dan moet deze elektronische handtekening omgeven worden met de nodige randinformatie en zo opgeslagen worden. Deze informatie is typisch voor een digitaal archiefstuk. In de papieren wereld wordt de integriteit gegarandeerd door de drager. Authenticiteit blijkt er uit het gebruik van allerlei technieken zoals stempels, zegels, handtekeningen, watermerken, legalisatie van handtekening, enz. die eveneens met de drager verbonden zijn.

Aan de hand van deze metadata kan men zich een oordeel vormen over de integriteit en de authenticiteit van de gearchiveerde informatie.¹⁴ Men kan er al dan niet een ‘echt’ stuk in zien.

2. Herkomst van het informatieobject

¹⁴ Hoe deze authenticiteitsgaranderende informatie eruit ziet in de digitale context en hoe deze informatie leesbaar gehouden wordt, is het onderwerp van een volgende DAVID-rapport.

Deze metadata documenteren de historiek van het informatieobject, zowel over de periode dat het archiefstuk zich bij de archiefvormer bevond, als over de periode in het archiefsysteem: wie is de archiefvormer, in welke sector situeert het stuk zich, functie van het stuk, wie heeft de verantwoordelijkheid (gehad) over het stuk tijdens het eerstelijnsarchiefbeheer,...

3. Semantische informatie

Deze informatie is de semantische voorstellingsinformatie in de zin van het OAIS-model, waar we hierboven naar verwezen. Het zijn de metadata die absoluut noodzakelijk zijn opdat de doelgroep de inhoud zou kunnen begrijpen. Zonder deze informatie is de inhoud voor hen betekenisloos. De doelgroep zal voor iedere archiefinstelling verschillend zijn. Voor publiekrechtelijke archiefbewaarplaatsen zal de doelgroep erg ruim zijn en omvat potentieel alle Belgische burgers. De sectie archief van een documentatieafdeling binnen een bedrijf zal daarentegen een kleinere en duidelijkere omschreven doelgroep hebben.

Nemen we het voorbeeld van een tekst die is opgemaakt in een vreemde taal. Afhankelijk van de doelgroep zal de klant de vreemde taal herkennen. Een zeer ruime doelgroep zal een Engelse of Franse tekst waarschijnlijk herkennen als een Engelse of Franse tekst. Dit is niet meer zo evident wanneer de tekst is opgemaakt in het Spaans of Portugees. Wanneer het daarentegen gaat om de archiefafdeling van een vertaalbureau, dan zal de doelgroep wellicht veel meer talen herkennen. In sommige gevallen zal men dus mee moeten archiveren om welke taal het gaat.

Een ander voorbeeld vinden we in de in het kader van het DAVID-project uitgevoerde *case* van de kiezersregisters. Een van de velden van het kiezersregister bestaat uit het postnummer van de gemeente waar de kiesgerechtigde zijn woonplaats heeft. Voor de naam van de gemeente, horend bij het postnummer, bestaat er geen veld. Omdat de postnummers over de jaren heen kunnen wijzigen, is het nuttig om de namen van de bijhorende gemeenten mee te archiveren, of op zijn minst het tijdstip waarop deze postnummers geldend zijn. Anders is het onmogelijk om een betekenis toe te kennen aan de viercijferige nummers.

Deze informatie is op zich niet typisch voor een digitaal archiefstuk. Ook voor het papieren kiezersregister is het nuttig om de betekenis van de postnummers mee te archiveren. Deze metadata worden slechts typisch voor de digitale context, indien de informatie onbegrijpbaar is juist omwille van het feit dat ze in digitale vorm is opgemaakt. In heel wat toepassingen van de stad Antwerpen worden er bijv. codes gebruikt met de bedoeling om geheugenruimte uit te sparen. Zo worden er in de bevolkingstoepassing van Antwerpen wel meer dan twintig verschillende codetabellen gebruikt, onder andere een codetabel waarmee het land van herkomst wordt aangeduid. Er is dan vereist dat het voor de klant duidelijk is of een 'F' Frankrijk of Finland betekent. Deze betekenissen moeten bijgevolg in de semantische informatie worden opgenomen.

4. Contextinformatie

Tenslotte zijn er de metadata die relatie van het informatieobject beschrijven tot de omgeving waarin het werd gecreëerd. Deze metadata zijn, in tegenstelling tot de semantische informatie, niet noodzakelijk opdat de klant de inhoud op zich zou kunnen begrijpen, nl. een betekenis zou kunnen toekennen aan de voor de mens begrijpbare tekens. De contextinformatie is bestemd om deze betekenis te kunnen plaatsen in een ruimer kader en omvat informatie zoals de reden waarom het informatieobject werd gecreëerd en hoe de verhouding is tot andere informatieobjecten, die elders bestaan.

Deze informatie is niet typisch voor een digitale archiefcontext. Ook voor een papieren archiefstuk moet er bijgehouden worden hoe het zich verhoudt tot de andere stukken in en buiten het archief. Deze metadata kunnen gebruikt worden bij het samenstellen van de pakketbeschrijving.

D. PAKKETINFORMATIE

De inhoud, de voorstellingsinformatie en de interpretatieve informatie, vormen samen het te bewaren informatiepakket. De pakketinformatie is nodig om de verschillende onderdelen van het informatiepakket die op de drager staan, te kunnen afbakenen en te identificeren als samenhangend. Pakketinformatie behoort niet tot het te bewaren informatiepakket omdat ze niet bijdraagt tot de leesbaarheid en de begrijpbaarheid van de informatie waarvan de bewaring in de eerste plaats beoogd wordt. Het is een hulpmiddel om efficiënt met het informatiepakket te kunnen omgaan.

Pakketinformatie kan bijv. bestaan uit de beschrijving van afspraken die er gemaakt zijn voor het toekennen van bestandsnamen of uit de beschrijving van de structuur van directories. Wanneer de bestanddelen van een informatiepakket de inhoud uitmaken van verschillende bestanden van een CD-rom, dan moet in de pakketinformatie terug te vinden zijn hoe de bestandsstructuur van de CD-rom eruit ziet.

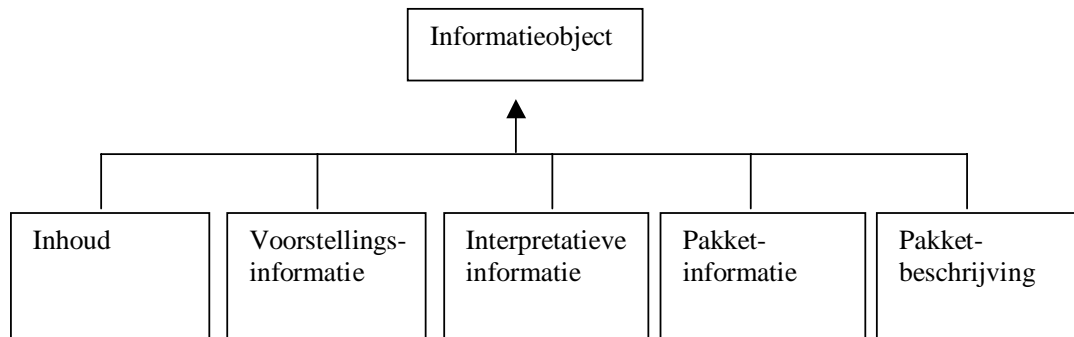
Na een migratie waarbij het informatiepakket overgezet wordt naar een andere drager met een andere structuur, dan blijft de pakketinformatie in principe niet behouden. Deze moet opnieuw vastgelegd worden voor het informatiepakket op de nieuwe drager.

E. PAKKETBESCHRIJVING

Pakketbeschrijvingsinformatie bestaat uit metadata die het informatiepakket beschrijven om de gezochte, relevante informatie snel te kunnen terugvinden. Het bevat alle informatie die nodig is om een klant toe te laten om gearchiveerde informatie die voor hem mogelijk van nut is, te vinden, te analyseren en op te vragen. De bron van de pakketbeschrijvingsinformatie is de inhoud en de interpretatieve informatie en wordt daaruit door de archivaris afgeleid. De pakketbeschrijvingsinformatie dient als input voor de toegangsmiddelen, zoals zoekfuncties en autoreply-systemen. Het is een hele reeks van gegevens over de inhoud en moet voor ieder type archiefstuk afzonderlijk bepaald worden. Vaak voorkomende gegevens uit de

pakketbeschrijving zijn: archiefvormer, datum van aanmaak, titel, functie van het archiefstuk, trefwoorden, openbaarheidsstatus...

In het OAIS-model worden al deze verschillende soorten metadata voorgesteld in de **classificatie van informatieobjecten**. Ook de metadata (voorstellingsinformatie, interpretatieve informatie, pakketinformatie en pakketbeschrijving) worden beschouwd als een informatieobject.



IV. De verschillende fases van het digitale archiveringsproces

In deel III gingen we na welke informatieobjecten er vereist zijn voor de bewaring op lange termijn van digitale informatie, zodanig dat deze informatie leesbaar, begrijpbaar en toegankelijk is voor alle klanten uit de doelgroep. In dit deel beschrijven we de verschillende functionele fases die in een digitaal archiveringsproces aan bod komen, gebaseerd op de classificatie van de informatieobjecten. Of met andere woorden: welke acties moet men allemaal ondernemen om een efficiënte bewaring van het informatiepakket mogelijk te maken? De bedoeling van deze denkoefening is ons dichterbij te brengen bij de identificatie van de typische problemen, waarvoor PKI een oplossing kan bieden.

A. DE SPELERS IN HET VELD

Tot hiertoe hebben we naar de personen die een rol spelen in het digitale archiveringsproces steeds gerefereerd als ‘men’. Maar welke partijen zijn er eigenlijk precies betrokken in het digitale archiveringsproces? Het OAIS-model onderscheidt drie betrokken partijen: de archiefvormer (*producer*), het Open Archival Information System en de klant (*consumer*).¹⁵ We verkiezen om niet te spreken over ‘consument’, maar over ‘klant’. Deze term is in de Nederlandse archiefterminologie algemeen gangbaar geworden, waaruit blijkt dat archiefinstellingen zich meer dan vroeger als dienstverleners zijn gaan opstellen.

¹⁵ OAIS-Reference model, 2.8, 2.9, 2.10, 4.11, 4.42.

1. De archiefvormer

De archiefvormer is diegene die de te archiveren informatie heeft aangemaakt of ontvangen. Hij vervult vooral een rol in de eerste fase van het digitale archiveringsproces nl. de fase van de invoer (*ingest*) in het archief. In het DAVID-project gaat het om de Vlaamse instellingen en diensten in de mate dat zij als archiefvormer optreden. Hieronder vallen zowel de Vlaamse overheidsbesturen die in toepassing van de archiefwet hun archiefstukken niet mogen vernietigen (bijv. steden en gemeenten), als de instellingen en organisaties die op eigen initiatief een archiefbeleid voeren (bijv. de archiefafdeling van het Katholiek Documentatie- en Onderzoekscentrum¹⁶).

2. De klant

De klant is een lid van de doelgroep ten behoeve waarvan de informatie bewaard wordt. De klant komt vooral voor in de laatste fase van het digitale archiveringsproces nl. de fase van de toegang. De doelgroepen voor de benutting van archieven zijn zeer verschillend: de ambtenaar op zoek naar een zaak die vroeger door zijn dienst werd behandeld, de persoon of overheidsdienst die zijn rechten wil veiligstellen, de burger die recht heeft op de blijvende openbaarheid van de bestuursdocumenten, de geïnteresseerde leek op zoek naar zijn *roots*, de wetenschappelijke navorser die een bepaald aspect van het maatschappelijk leven in het verleden wenst te onderzoeken¹⁷ enz. Het leesbaar en toegankelijk maken van archiefstukken vergt voor elke doelgroep een andere benadering.

3. De archiefinstelling

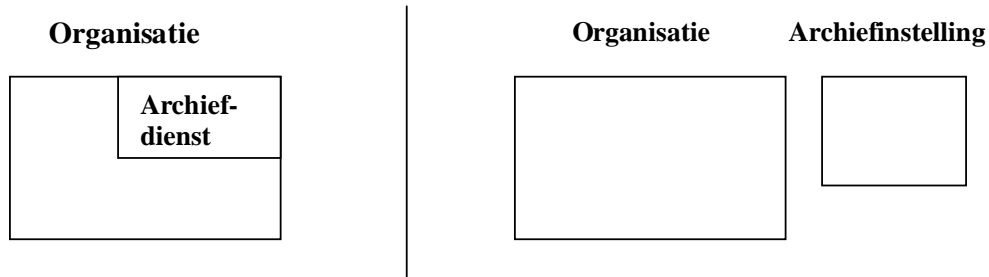
De archiefinstelling is de organisatie van personen en systemen, die de verantwoordelijkheid heeft om informatie te bewaren en toegankelijk te maken en te houden voor de doelgroep. De archivaris staat aan het hoofd ervan. Er bestaan twee organisatievormen voor archiefinstellingen. De archiefinstelling kan los van de archiefvormer bestaan als afzonderlijke entiteit (bijv. het algemeen Rijksarchief), waaraan de archiefvormer de informatie ter archivering afgeeft. Een archiefinstelling bevindt zich op een andere plaats dan de archiefvormende organisatie. Het archief kan ook een functie zijn binnen de organisatie waarvan de informatie moet bewaard worden. Men spreekt dan over een 'archiefdienst'. De archiefdienst is meestal gevestigd in de archiefvormende organisatie, maar dit is niet noodzakelijk zo.¹⁸

Hoewel het element plaats zijn belang verliest in de digitale wereld, zullen deze organisatievormen ook blijven bestaan wanneer archiefinstellingen volop digitale archiefstukken zullen gaan archiveren, niet alleen omdat men met papieren archiefstukken zal blijven geconfronteerd worden, maar ook omdat de archivaris en de archief functie als instelling van belang zal blijven.

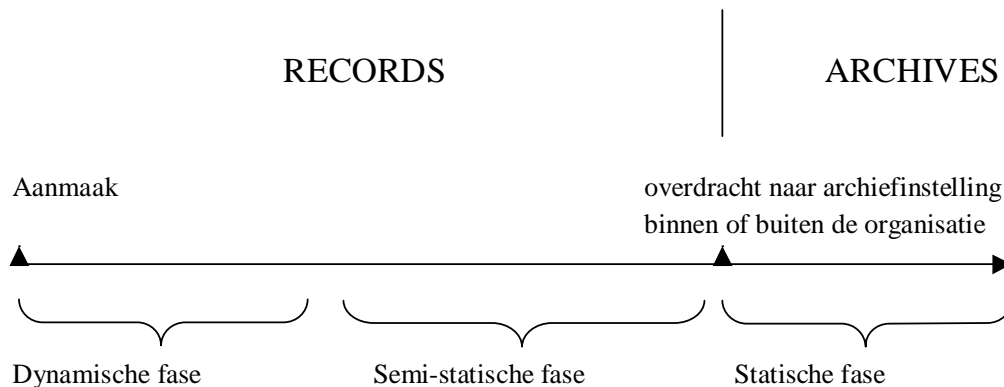
¹⁶ <http://www.kuleuven.ac.be/kadoc/archief/kdcaren.htm>

¹⁷ <http://arch.arch.be/TAKEN.HTML>

¹⁸ Het Stadsarchief Antwerpen bijvoorbeeld, maakt juridisch gezien deel uit van de archiefvormer, nl. de administratie van de stad Antwerpen, maar bevindt zich op een aparte locatie.



De vraag is gerezen of de archiefinstelling als zodanig inderdaad nog zal blijven bestaan in de digitale wereld. De speciale eigenschappen van digitale informatie lijken immers een einde te maken aan het onderscheid tussen *records* and *archives*, tussen de *records manager* en de archivaris. Deze tweedeling is ontstaan tijdens de Franse Revolutie, die de archieven van het Ancien Régime van hun primaire functies heeft beroofd en er historisch archief van heeft gemaakt.¹⁹ De archieftaal is doordrongen geraakt van dit onderscheid, dat afkomstig is uit de Angelsaksische literatuur. De Duitstaligen noemen het recente archief *Registraturgut* en het permanent te bewaren archief *Archivgut*. In de Nederlandse taal wordt dit onderscheid aangeduid door te verwijzen naar bepaalde fasen in de levensloop van een archiefstuk. Men spreekt van dynamisch archief als men verwijst naar de stukken die nog courant gebruikt worden door de archiefvormer en waarbij de dossiers waarvan ze deel uitmaken voortdurend worden aangevuld. Semi-statisch archief (soms ook wel semi-dynamisch archief genoemd) bevindt zich nog steeds onder de verantwoordelijkheid van de archiefvormer, maar wordt niet meer courant gebruikt. Tijdens deze fase kunnen er in de organisatie voor deze *records* tussenarchieven worden ingericht om een eerstelijnsarchiefbeheer te kunnen voeren. Archieven in de statische fase tenslotte, zijn overgedragen aan een archiefinstelling, die speciaal is uitgerust voor de permanente bewaring van de archieven die niet voor vernietiging zijn aangewezen.



¹⁹ THOMASSEN, T., 'Archivarissen en records managers: zelfde professie, verschillende verantwoordelijkheden', in *Naar een nieuw paradigma in de archivaliek*, HORSMAN, P.J., KETELAAR, F. en THOMASSEN, T. (ed.), Stichting archiefpublicaties, jaarboek 1999, 186.

Ook de wetgeving is afgesteld geraakt op dit onderscheid. De archiefwet heeft voor de archiefstukken van de Rijksbesturen een overbrengingstermijn van honderd jaar ingevoerd. Dit wil zeggen dat de stukken geacht worden gedurende honderd jaar nog een administratief nut te hebben voor de archiefvormende overheid en dat ze gedurende deze termijn in principe bij de overheid zelf (of bij diens archiefdienst) moeten bewaard worden. In samenspraak met de archiefinstellingen wordt deze termijn nochtans doorgaans verkort.²⁰ Ook in de openbaarheidswetgeving wordt het onderscheid bevestigd tussen bestuursdocumenten die zich nog bij de overheid bevinden en de bestuursdocumenten die reeds werden overgedragen aan de archiefinstelling. Art. 11 van de Wet van 11 april 1994 betreffende de openbaarheid van bestuur (B.S. 30 juni 1994) bepaalt dat haar bepalingen ook van toepassing zijn op de bestuursdocumenten die in een archief zijn neergelegd, behalve wanneer het om het Rijksarchief gaat of om het Rijksarchief in de Provinciën. Eenzelfde bepaling vinden we terug in de Wet van 12 november 1997 betreffende de openbaarheid van bestuur in de provincies en de gemeenten (B.S. 19 december 1997).

Moet dit onderscheid nu opgeheven worden met de komst van digitale archiefstukken? Het proces van digitale archivering moet immers beginnen nog vóór de te archiveren informatie is aangemaakt. Reeds in de ontstaansfase van digitale informatie moeten er bijzondere maatregelen worden genomen om een efficiënte en permanente bewaring van informatie mogelijk te maken. Het vastleggen van een aantal essentiële metadata zal vaak slechts kunnen gebeuren in de loop van de dynamische of de semi-statische fase, zoals bijvoorbeeld gegevens over het formaat of over een migratie die werd uitgevoerd. Zo gesteld, lijken de beroepen van de *records manager* en de archivaris met elkaar te versmelten in het digitale tijdperk. Niets is minder waar. De functie van de archivaris is onontbeerlijk, ook in een digitale omgeving. Naarmate digitale archiefstukken ouder worden, verandert hun functie en rijzen er vragen over het nut van hun verdere bewaring. Enkel een geschoolde archivaris kan oordelen over de archiefwaarde ervan. De idee van een archiefstuk dat op bepaald moment onder hoede van een archivaris wordt geplaatst omdat de bewaring verantwoord is, blijft dus behouden. Het statisch archief blijft ook in het digitale tijdperk de bestemming voor de informatie die geen onmiddellijk nut meer heeft voor het bedrijfsproces. Ook de *records manager* blijft behouden als de functie die deel uitmaakt van het bedrijfsproces van een organisatie, in die zin dat hij de informatie in een goede en geordende staat ter beschikking houdt voor de uitvoering van de taken van de organisatie.

Wat er wel moet veranderen, is de afwachtende houding van de archivaris. Het heeft geen enkele zin meer, en het is zelfs af te raden, dat de archivaris wacht totdat de digitale archiefstukken in hun laatste rustplaats arriveren, zijnde de archiefinstelling. Een digitaal archief *rust* niet, in de archiefinstelling niet, maar eerder ook niet.²¹ Het is dit wat men in de literatuur bedoelt men het verdwijnen van het onderscheid tussen de dynamische, de semi-dynamische en de statische fase van het archiefstuk.²² De fases op zich blijven behouden,

²⁰ SUETENS, S., 'De archiefwet' in X. (ed.), *Mediarecht Boeken*, afl. 7, 1996, 19.

²¹ THOMASSEN, T., *o.c.*, 187.

²² Zie o.a. HOFMAN, H., 'De digitale archivaris: een nieuwe wereld. De invloed van informatietechnologie op het archiefvlak', in *Naar een nieuw paradigma in de archivistiek*, HORSMAN, P.J., KETELAAR, F. en THOMASSEN, T. (ed.), Stichting archiefpublicaties, jaarboek 1999, 214.

maar de archivaris zal nu ook in de dynamische en in de semi-statische actief moeten tussenkomen. In de digitale wereld is archivering geen activiteit meer die pas plaatsvindt op het einde van de levensloop van het archiefstuk wanneer de beslissing is gevallen dat het moet bewaard blijven.

Bij overheidsinstellingen bestaat de neiging om het probleem van lange termijn-bewaring van digitale informatie bij de archiefinstellingen te leggen. Deze eenzijdige invalshoek moet vermeden worden wegens het records continuüm-karakter van digitale archiefstukken. Daarom lijkt het nuttig dat er in het kader van de Vlaamse Gemeenschap een samenwerkingsverband zou tot stand worden gebracht tussen de administraties en archiefinstellingen, teneinde records managers, IT managers en informaticaleveranciers binnen de overheid bewust te maken van dit probleem.²³ Dit moet ertoe leiden dat de archivaris in de toekomst meer zou betrokken worden bij het informatiebeleid van de overheid.

Besluitend kunnen we zeggen dat we met de term 'archiefinstelling' de functie bedoelen die instaat voor de permanente bewaring, in tegenstelling tot de zorg die aan de archiefstukken wordt besteed door de archiefvormende dienst. Een archiefinstelling kan een afzonderlijke entiteit zijn, of ze kan deel uitmaken van de archiefvormende organisatie. Ook na de digitale revolutie blijft de archiefinstelling in ieder geval behouden als expert inzake selectie van informatie met archiefwaarde, de permanente bewaring van deze informatie en het beschikbaar stellen ervan.

B. VIER FASES

1. Invoer

In deze fase wordt het archiefstuk ontvangen door de archiefinstelling en klaargemaakt voor opname in het archiefsysteem. De situatie zoals hierboven beschreven is ideaal. Er moet naar gestreefd worden dat al deze metadata voorhanden zijn en mee kunnen gearchiveerd worden. Maar de digitale informatie komt het archiefsysteem meestal zo niet binnen. Hierin ligt het onderscheid tussen een overgedragen informatiepakket, een te archiveren informatiepakket en een toegankelijk gemaakt informatiepakket. Deze verschillende concepten zijn nodig om te kunnen beantwoorden aan de realiteit dat de meeste overgedragen informatie niet voldoet aan de archiveringsvereisten op lange termijn, en tevens dat de toegankelijk gemaakte informatie niet noodzakelijk alle informatie (mag) bevat(ten) die door de archiefinstelling werd gearchiveerd.

a) Verschillende soorten informatiepakketten

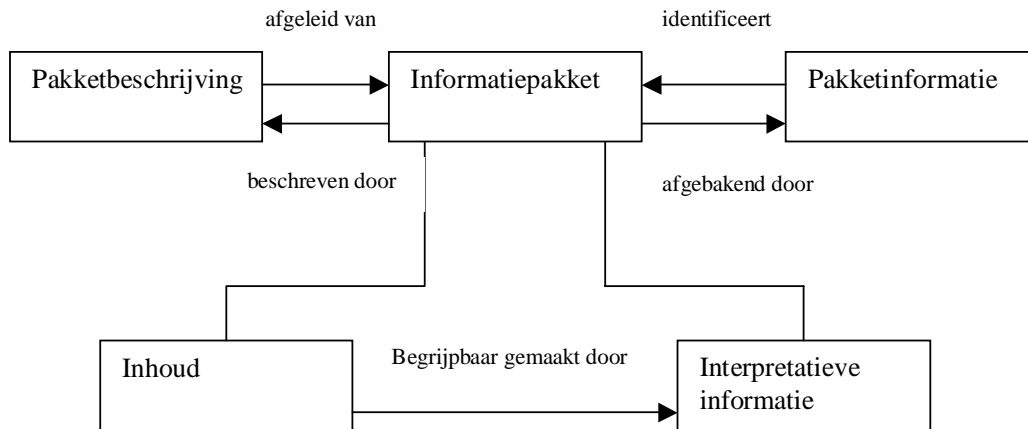
MCKEMMISH, S., 'Yesterday, Today and Tomorrow: a continuum of responsibility', beschikbaar op <http://www.sims.monash.edu.au/rcrg/publications/recordscontinuum/smckp2.html>

²³ Naar analogie met het Nederlandse programma 'Digitale Duurzaamheid'. Dit is een samenwerkingsverband tussen het Rijk, de provincies, de gemeenten en de waterschappen, en rijksarchiefdiensten.

1) Informatiepakket

Het basisconcept dat het OAIS-model gebruikt voor bewaring op lange termijn, is het 'informatiepakket'. Een informatiepakket bestaat uit twee soorten informatieobjecten, enerzijds de inhoud (met bijhorende voorstellingsinformatie) en anderzijds de interpretatieve informatie. Een informatie-objekt bestaat op zijn beurt uit data (nl. bits) en de bijhorende voorstellingsinformatie. Hierboven legden we uit dat er voor de inhoud voorstellingsinformatie nodig is om deze inhoud leesbaar te houden op korte en op lange termijn. Maar dit is natuurlijk eveneens zo voor alle andere informatie die er naast de inhoud ook nog moet bewaard worden. Deze informatie bestaat immers ook uit voor de mens onleesbare bits. Ook voor de interpretatieve informatie is er bijvoorbeeld voorstellingsinformatie nodig.

Ieder informatiepakket kan geassocieerd worden met twee andere soorten informatieobjecten, zijnde de pakketinformatie en de pakketbeschrijving. Onderstaande figuur stelt het concept 'informatiepakket' grafisch voor.



Ieder informatiepakket bevat maximum één inhoudelijk informatieobject, een interpretatief informatie-object, en wordt geassocieerd met exact één pakketinformatie-object. Het wordt ook geassocieerd met een onbeperkt aantal pakketbeschrijvingen die de toegang tot de inhoud vergemakkelijken.

2) Overgedragen informatiepakket

Het overgedragen informatiepakket is het informatiepakket dat door de archiefvormer aan de archiefinstelling wordt overgedragen. Dit informatiepakket is meestal niet geschikt voor onmiddellijke archivering omdat het niet aan alle archiveringsvereisten voldoet. Een

overdracht dient immers steeds in goede, geordende en toegankelijke staat te gebeuren. De overdracht is het moment bij uitstek om de staat van het archief na te gaan.²⁴

b) *Taken van de archiefinstelling tijdens de invoerfase*

Taak 1: het overgedragen informatiepakket ontvangen

De overdracht van digitale informatie kan op verschillende manieren gebeuren. Het is mogelijk dat de drager met daarop de digitale informatie aan de archiefinstelling wordt overgedragen. Deze manier leunt het dichtst aan bij de wijze van overdracht van papieren archiefstukken: een fysische verplaatsing van de drager brengt de te archiveren informatie tot in de archiefinstelling. Een tweede mogelijkheid bestaat erin dat de digitale informatie via een telecommunicatienetwerk van de archiefvormer naar de archiefinstelling wordt gezonden. In dit geval gaat het om een fysische verplaatsing van de bits via de informatiesnelweg, bijv. via het Internet. Tenslotte kan de informatie ook zonder fysische verplaatsing onder de verantwoordelijkheid van de archiefinstelling komen te staan. De informatie blijft dan op server van de archiefvormende organisatie staan, maar krijgt dan de status ‘gearchiveerd’ mee.

Het is van belang om in te zien dat de overdracht, net zoals in de papieren wereld, slechts een juridische kwestie is betreffende de verantwoordelijkheid voor het archiefstuk. Een fysische verplaatsing van het archiefstuk is niet nodig om van een overdracht te spreken. Bij papieren archiefstukken is dit echter meestal wel het geval²⁵, tenzij ze bijvoorbeeld bij de archiefvormende instantie worden gelaten omwille van plaatsgebrek in de archiefbewaarplaats.

Ten aanzien van digitale archiefstukken zal de loutere overdracht van beheer en verantwoordelijkheid zonder enige fysische verplaatsing in de toekomst veel vaker voorkomen dan een overdracht die wel gepaard gaat met een fysische overdracht.²⁶ In de beginfase van de omschakeling van papieren naar digitale archieven, waarin we ons nu volop bevinden, zal de overdrachtsprocedure nog heel nauw samenhangen met de klassieke, papieren procedures. Dit heeft te maken met het feit dat oplossingen voor problemen vaak geformuleerd worden vanuit paradigma's, van waaruit we naar de wereld kijken. Vernieuwingen worden vaak bekeken vanuit het oude, heersende paradigma.²⁷ Voor de

²⁴ COPPENS, H., *Archiefbeheer in gemeenten en O.C.M.W.'s*, Brussel, Algemeen Rijksarchief, 1997, 190. Bij sommige archiefinstellingen bestaat er de tendens om, in samenspraak met de archiefvormer, reeds vóór de overdracht toezicht uit te oefenen op de ordening en de staat van de archiefstukken.

²⁵ COPPENS, H., *o.c.*, 188.

²⁶ Het archief van de toekomst wordt in de literatuur voorgesteld als een netwerk van geordende databanken (o.a. HEDSTROM, M., 'Electronic Archives: Integrity and Access in the Network Environment', *American Archivist*, Vol. 58, Summer 1995, 313. De enige verplaatsing waarvan er in een dergelijke omgeving nog sprake kan zijn, is een verplaatsing in *cyberspace*.

²⁷ Volgens KUHN is een paradigma een theoretisch geheel waarover brede overeenstemming bestaat binnen een bepaald onderzoeksdomein, en dat als voorbeeld dient voor de 'normale wetenschapper' op het terrein. Wanneer het heersende paradigma aan het wankelen wordt gebracht door de komst van vernieuwingen, ontstaat er een crisis binnen de discipline en barst er een strijd los tussen de oudere vertegenwoordigers van de discipline en de nieuwkomers. Deze nieuwe generatie zal het nieuwe paradigma geleidelijk in zich opnemen en de problemen waarmee de discipline te kampen

archiefwereld betekent dit dat men wil blijven vasthangen aan de klassieke archiveringsstrategieën, die echter niet bruikbaar zijn in de digitale wereld. Pas wanneer de digitale revolutie volledig wordt begrepen en de consequenties ervan voor de archiefwereld onder ogen worden gezien, kunnen de voordelen van de digitalisering ten volle spelen.

Het zich inleven in deze nieuwe situatie gebeurt echter steeds geleidelijk. Dit heeft te maken met het feit dat het papieren paradigma de archivariissen in de beginfase van de omschakeling nog steeds in haar ban zal hebben en houden. Een voorbeeld van het feit dat het digitale paradigma slechts moeizaam ingang vindt, is te vinden in het concept van de huidige tekstverwerkers, zoals MS Word. Hoewel de bedoeling van veel gebruikers erin bestaat om een onwijzigbaar elektronisch document te creëren als eindproduct, dat kan uitgewisseld worden via telecommunicatienetwerken, zijn de tekstverwerkers van vandaag nog steeds opgevat als hulpmiddel om een papieren document te genereren. We kunnen dit vergelijken met de vroegere typemachine, die werd ingezet om een onwijzigbaar eindproduct te maken. Immers, de meeste tekstverwerkingsprogramma's hebben als resultaat een document waarvan de structuur en de lay-out worden weergegeven op het scherm. Wanneer deze elementen worden aangebracht met een tekstverwerker, hebben zij echter geen enkele betekenis ten aanzien van het elektronisch document. De onwijzigbaarheid wordt pas bereikt wanneer het resultaat wordt uitgeprint op een papieren drager.²⁸ Merk ook op dat de huidige PC's uiterlijk gezien veel weg hebben van de klassieke typemachine, waarbij het resultaat onmiddellijk zichtbaar is op het scherm als de elektronische versie van het papieren document.

Eens de archivariissen begrijpen waar het bij het digitaliseringsproces werkelijk om gaat, en zij de knop in hun hersenen hebben omgedraaid, zal de archivering van digitale gegevensdragers stilaan verdwijnen. Een archiefinstelling met kasten vol CD-ROMs, die door de archiefvormer werden overgedragen, zal een zeldzaamheid worden. Zoals hierboven reeds werd aangehaald, moet men afstappen van het archiveren van gegevensdragers, vermits gegevensdrager en informatie niet meer samenvallen. Gegevensdragers zijn slechts tijdelijke hulpmiddelen om de digitale informatie vast te houden. Alleen in een netwerkomgeving kunnen de voordelen van digitalisering, zoals het wegvallen van de belemmeringen van plaats en tijd, ten volle benut worden. Het uitgangspunt bij digitale archivering moet zijn dat op termijn alle informatie op hetzelfde moment en overal ter wereld voor iedereen beschikbaar moet kunnen zijn.²⁹ Informatieleveranciers, en met name ook de archivaris moeten vanuit dit standpunt leren denken en handelen.

krijgt, oplossen vanuit dit nieuwe paradigma. De komst van de digitalisering heeft een crisis doen ontstaan binnen de archiefdiscipline. Archiveringsstrategieën zullen vanuit dit nieuwe digitale paradigma moet geformuleerd worden.

KUHN, Th. S., *De structuur van wetenschappelijke revoluties*, Boom Meppel, 1987, 4e druk.

<http://home.tvd.be/cr27486/Kuhn.html>

²⁸ Om een volwaardig elektronisch document te creëren, moet er een conversie gebeuren naar een formaat dat elementen zoals structuur en lay-out wel kan vasthouden, zoals PDF. PDF (*Portable Document Format*) is een bestandsformaat dat het 'beeld' van het elektronisch document vastlegt, alsof er foto van zou worden genomen, en dat toelaat om deze 'electronic image' uit te wisselen en af te drukken, onafhankelijk van de PC of de printer die gebruikt wordt.

<http://www.adobe.com/products/acrobat/adobe.pdf.html>

²⁹ HOFMAN, H., 'De digitale archivaris: een nieuwe wereld. De invloed van informatietechnologie op het archiefvlak', *l.c.*, 214; BAAK, P. en KOENEN, K., 'Het geheugen als actieve kracht. De archief functie binnen de digitale overheid', *Programma Digitale Duurzaamheid*, Den Haag, 1999, 15.

Bijgevolg zal na de beginfase van digitale archivering, de overdracht best gebeuren, hetzij via telecommunicatienetwerken, hetzij via het toekennen van de status ‘gearchiveerd’. Wanneer het archiefsysteem voor de opslag van de informatie gebruik maakt van een andere server dan die van de archiefvormende organisatie, zal er een transfer moeten plaatsvinden tussen deze twee servers. Deze situatie kunnen we vergelijken met de archiefinstelling als aparte fysische entiteit, los van de archiefvormende organisatie. Er moet dan ‘ruimte’ overbrugd worden bij de overdracht. In het geval van twee (of meer) aparte servers (die in principe naast elkaar kunnen staan), ligt de te overbruggen ruimte tussen de verschillende onderdelen van het netwerk. Dit heeft niets te maken met geografische ruimte. In het andere geval is er zelfs geen fysische verplaatsing van de informatie, zelfs niet via een netwerk. De archivaris zal met behulp van PKI deze status kunnen toekennen. Hij zal eventueel wel informatie moeten toevoegen om van een volwaardig te archiveren informatiepakket te kunnen spreken.

Deze twee nieuwe manieren om een archiefstuk over te dragen, gelden natuurlijk alleen voor digitale archiefstukken. Het feit dat het element ‘plaats’ irrelevant worden in de digitale wereld, moeten we daarom toch enigszins relativiseren. Papier zal immers altijd blijven bestaan als drager van informatie en de digitaal uitgebouwde archieffunctie moet ook de niet-digitale omgeving blijven erkennen en ondersteunen. Men zit ook opgescheept met de papieren erfenis uit het verleden die permanent moet gearchiveerd blijven. Daarom argumenteerden we hierboven dat archiefinstellingen zullen georganiseerd blijven volgens twee modellen. Het archief als een verzameling van gearchiveerde informatie op een andere plaats dan binnen de archiefvormende organisatie, zal behouden blijven, hoewel een louter digitaal archief perfect kan functioneren onafhankelijk van elke geografische ligging.

De overdracht via een telecommunicatienetwerk of het toekennen van de status ‘gearchiveerd’ moet zo snel mogelijk na de juridische overdracht gebeuren. Het digitale karakter van de archieven dwingt de archivaris immers om op zeer korte termijn maatregelen te kunnen nemen en bijgevolg moet ook het feitelijk beheer over de archiefstukken bij hem berusten.

De wijzen van overdracht zullen in het digitale kader grondig veranderen. De archiefinstelling moet daarom voldoende uitgerust zijn om de digitale archiefstukken te kunnen ontvangen. Aanvankelijk zal zij digitale gegevensdragers in ontvangst nemen op een wijze die grotendeels dezelfde is als de in ontvangst name van papieren archiefstukken nl. het fysiek in handen nemen door de archiefinstelling. Wanneer de (voordelen van de) digitalisering volledig zullen zijn doorgedrongen, gebeurt de overdracht via telecommunicatienetwerken of door toekenning van de status ‘gearchiveerd’. Hierbij moet steeds voor ogen worden gehouden dat er, net zoals in de papieren wereld, een onderscheid bestaat tussen een overdracht in fysische zin en een overdracht in juridische zin. Enkel het toekennen van het feitelijke archiefbeheer aan de archiefinstelling, kan leiden tot de creatie van een te archiveren informatiepakket.

Taak 2: Kwaliteitsbewaking bij de overdracht

Hoewel ze in het OAIS-model na de ontvangst van het overgedragen informatiepakket wordt behandeld, moet deze taak de eigenlijke juridische overdracht voorafgaan. De juridische overdracht mag enkel plaatsgrijpen als de archiefstukken aan alle voorwaarden voldoen die noodzakelijk zijn om bewaring op lange termijn te kunnen waarborgen.

GOEDE, GEORDEDE EN TOEGANKELIJKE STAAT

In de klassieke archiefterminologie vinden we steeds weer de bewoordingen dat de archiefstukken ‘in goede, geordende en toegankelijke staat’ moeten overgedragen worden. ‘Geordende staat’ betekent dat de archiefstukken zodanig zijn geordend dat zij binnen een redelijke termijn kunnen worden teruggevonden. Met ‘goede staat’ wordt het geheel van materiële condities aangegeven waaraan de gegevensdrager en de daarop vastgelegde informatie moeten voldoen om raadpleging nu en in de toekomst te garanderen. ‘Toegankelijke staat’ heeft dan weer te maken met een goede ontsluiting naar de klanten toe.

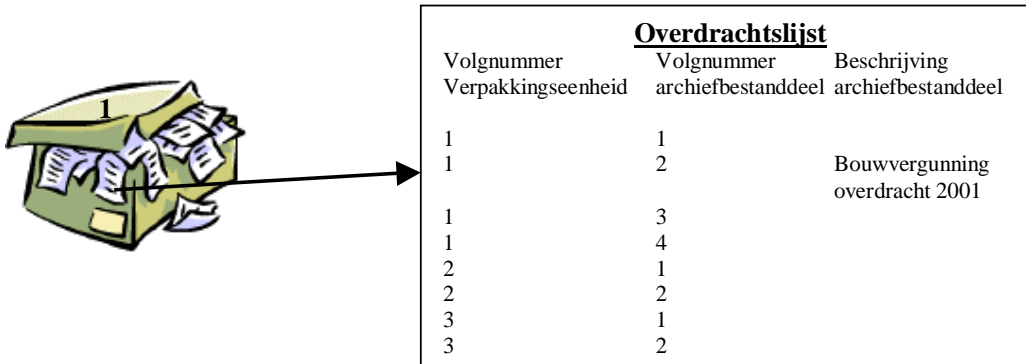
Binnen de archiefwereld zijn er allerlei technieken ontwikkeld om een archief in een **geordende en toegankelijke toestand** te brengen en te houden. Het opmaken van een goed ordeningsplan is hierbij een belangrijke stap in de goede richting. Dit is een plan, opgemaakt door de archiefvormende organisatie, met als doel het rangschikken van archiefstukken en archiefbestanden binnen een archief overeenkomstig een bepaald systeem.³⁰ Deze techniek is gebaseerd op een systematische weergave van de opdrachten van een organisatie, de daaruit voortvloeiende taken, handelingen en activiteiten die nodig zijn om die taken te realiseren, met daarbij telkens een opsomming van de archiefstukken die gevormd of ontvangen worden ter ondersteuning van die handelingen. Aan de hand van dit plan kan iedere medewerker van de organisatie aangeven waar de door hem afgehandelde stukken moeten terecht komen.

Om de overdracht en de plaatsing in het statisch archief vlot te kunnen laten verlopen, maakt de archiefvormer een overdrachtslijst op. Dit is een soort checklist met een gedetailleerde beschrijving van de overgedragen archieven, waarvan de indeling overeenstemt met de indeling van het ordeningsplan. Naar aanleiding van de overdracht, wordt er op iedere verpakkingseenheid (bijv. op de archiefdoos) een volgnummer aangebracht. Aan ieder archiefbestanddeel binnen een verpakkingseenheid, wordt er bovendien nog eens een intern volgnummer toegekend. Deze volgnummers komen ook voor op de overdrachtslijst bij de vermelding van de corresponderende overgedragen archiefbestanddelen. Op die manier kan de archivaris nagaan welke stukken precies worden overgedragen. Zo krijgt hij ook een zicht op de ordening die door de archiefvormer werd aangebracht.

Het opmaken van een overdrachtslijst, gebaseerd op het ordeningsplan, en gecombineerd met het aanbrengen van volgnummers op de fysieke stukken, wordt in de papieren archieven gevolgd om de orde en toegankelijkheid, aangebracht door de archiefvormer, te kunnen handhaven. Overeenkomstig het structuurbeginsel moet de archiefinstelling deze orde immers

³⁰ COPPENS, H., *o.c.*, 71.

mee overnemen in het statisch archief.³¹ De reden hiervoor is gelegen in het feit dat archiefstukken tot stand komen in het kader van werkprocessen en dat zij in die ontstaanscontext ook best worden bewaard. Wanneer archiefstukken bijvoorbeeld chronologisch geordend zijn, mag de archivaris ze in het statische archief niet alfabetisch gaan ordenen. Dan zouden immers alle toegangen verloren gaan. Enkel wanneer de ordening door de archiefvormende organisatie niet op een afdoende wijze werd doorgevoerd, kan de archivaris een archiefschema³² voorstellen.



De vraag rijst of deze procedure kan of moet gehandhaafd blijven voor digitale archiefstukken. De koppeling van de fysieke stukken aan de logische ordening met behulp van de volgnummers, is een typisch papieren werkwijze die er op gericht is om het werk van de archivaris te verlichten in een omgeving met tastbare archiefstukken. Op die manier is hij niet verplicht om alle archiefdozen te openen met de bedoeling om te controleren om welke archiefstukken het gaat. De archiefdozen zullen immers de archiefinstelling niet binnenkomen volgens de logische orde die de archiefvormer had aangebracht.

Tijdens de overgangsfase, waarin nog digitale gegevensdragers zullen overgedragen en gearchiveerd worden³³, blijft deze procedure nog steeds nuttig. De archiefstukken zullen in zekere zin nog tastbaar zijn en de dragers zelf moeten gemarkeerd worden met een volgnummer, dat eveneens in een papieren overdrachtslijst moet terug te vinden zijn. Wanneer een gegevensdrager slechts één archiefbestanddeel bevat, kan volstaan worden met het markeren van deze dragers. Komen er echter meerdere archiefbestanddelen per gegevensdrager in de vorm van verschillende bestanden, dan moeten deze bestanden eveneens op een identificeerbare wijze gemarkeerd worden.

³¹ Archiefstermenlexicon voor Nederland en Vlaanderen
<http://www.kvan.nl>

³² Wat een ordeningsplan is voor de archiefvorming in de dynamische fase, is het archiefschema voor de ordening van het archief in de statische fase.

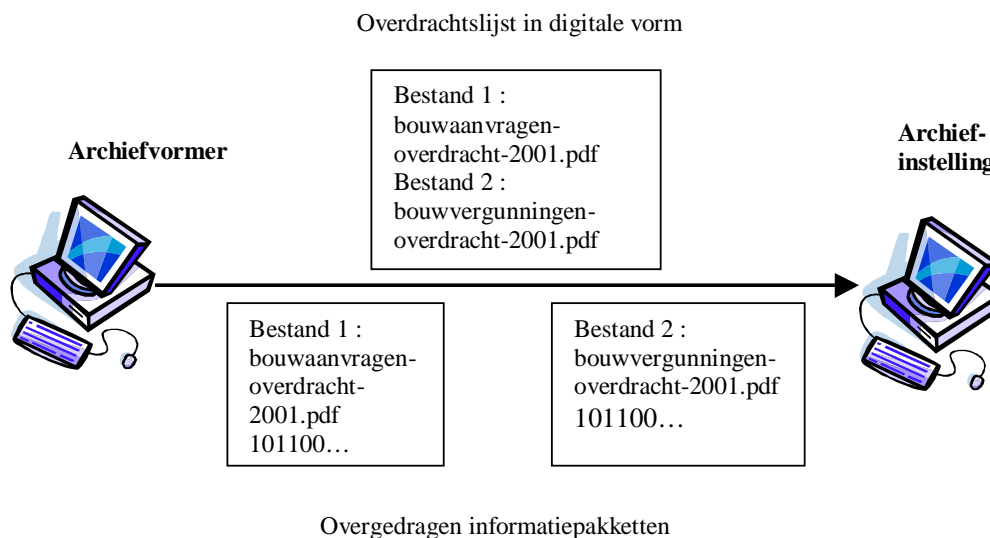
³³ Cf. supra



Overdrachtslijst		
Volgnummer Verpakkingseenheid	Volgnummer archiefbestanddeel	Beschrijving archiefbestanddeel
1	1	Bouwvergunning CDRom 1 : BT- overdracht-2001.pdf
1	2	
1	3	
1	4	
2	1	
2	2	

Van zodra echter de overdracht zal gebeuren via een telecommunicatienetwerk, kunnen de stukken niet meer fysisch gemarkeerd worden. Het probleem blijft nochtans hetzelfde. Het zal niet volstaan om de archiefstukken in een willekeurige volgorde en zonder bijkomende informatie door te sturen naar de archiefinstelling. De archivaris zal er immers geen idee van hebben welk bestand welk archiefstuk bevat, ook al krijgt hij een overdrachtslijst (in digitale vorm) doorgestuurd met daarin de beschrijving van alle overgedragen stukken. Hij zal dan verplicht zijn om alle bestanden één na één te openen en te identificeren.

Opdat de archivaris dus de geordende en toegankelijke staat van de digitale archiefstukken zou kunnen nagaan en beoordelen, is het van belang dat zij met de logische ordening in verband kunnen worden gebracht. Iedere kleinste verpakkingseenheid op digitaal vlak, zijnde het informatiepakket, moet bijgevolg identificeerbaar gemaakt worden voor de archivaris. Dit kan bijvoorbeeld gebeuren door ieder informatiepakket te voorzien van een duidelijke en uniforme naamgeving die overeenkomt met de naamgeving in de overdrachtslijst.



Hierbij is het nodig op te merken dat een digitaal archief tijdens de beginfase waarschijnlijk meer herorderingswerk van de archivaris zal vragen dan thans in de papieren archieven het

geval is. Archiefvormers gebruiken nu meer en meer de ordenings- en toegankelijkheidssystemen die de informatietechnologie ter beschikking stelt. Het beheer van de digitale archiefachtige functies binnen de bedrijfsprocessen gebeurt echter meestal niet volgens archivistische principes.³⁴ Opslag van digitale bestanden gebeurt vaak op de eigen harde schijf, die alleen voor de gebruiker toegankelijk is en waar dus niemand het bestaan van kan nagaan. Bovendien vinden we vaak vele verschillende versies terug, waarvan de status onbekend is. Daarbij komt nog dat de gebruiker zelf de bestanden niet meer terugvindt door de onoverzichtelijke en onlogische wijze waarop de bestanden geordend zijn. In het beste geval wordt de informatie per dienst of departement op een schijf bijgehouden, waarop ieder een eigen privé-archief onderhoudt. Vaak gebeurt er zelfs helemaal geen registratie, laat staan een opslag, van informatie met een hoge archiefwaarde. Denken we maar aan e-mails. De klassieke brievenbus, waarvan de inhoud routinematig geregistreerd wordt, moet meer en meer plaats maken voor de *mailbox*. E-mails kunnen op een eenvoudige en onopvallende wijze door de geadresseerde op eigen initiatief vernietigd worden. Registratie ervan is in heel wat organisaties totaal afwezig.³⁵

Meer nog dan vroeger het geval was, is het daarom van het grootste belang dat de archivaris de keuze en het beleid inzake het digitale ordenings- en toegankelijkheidsproces bij de archiefvormers ondersteunt en begeleidt.

Wat de goede, materiële staat van de drager betreft, moet de controle door de archivaris bij de overdracht eveneens vanuit een totaal andere invalshoek bekeken worden. Deze voorwaarde heeft alles te maken met de leesbaarheid van de informatie. Voor papieren archiefstukken kan het volstaan dat de papieren drager waarop de informatie is vastgelegd, in een goede conditie worden gebracht en gehouden door de archiefvormende instantie. Het is dan vooral een kwestie om het papier in een stofvrije omgeving met de juiste omgevingstemperatuur en vochtigheidsgraad weg te bergen.

Zoals gezegd zal men in het archief van de toekomst immers weinig of geen externe dragers meer archiveren. In een digitale omgeving wordt de leesbaarheid dan ook beïnvloed door andere factoren dan de conditie van de drager. De archivaris moet er zich bij de overdracht van vergewissen dat de archiefvormer alle nodige metadata mee overdraagt die nodig zijn voor de leesbaarheid van de informatie. Hierboven maakten we een onderscheid tussen de leesbaarheid op korte termijn, ook wel de presentbaarheid genoemd, en de leesbaarheid op lange termijn. Gegevens omtrent de leesbaarheid op korte termijn moeten steeds voorhanden zijn bij de overdracht van digitale archiefstukken. Dit is eigen aan het feit dat de data waaruit digitale informatie bestaat, nl. bits, niet leesbaar zijn voor de mens.³⁶ Het gaat om de hierboven beschreven voorstellingsinformatie omtrent de leesapparatuur van de drager, omtrent het gebruikte bestandssysteem (bijv. NTFS), omtrent het bestandsformaat (bijv. .doc) en omtrent de applicatiesoftware (bijv. MS Word).

³⁴ BAAK, P. en KOENEN, K., *l.c.*, 20.

³⁵ SCHNEIDER, D., 'E-mail – Just Another Record. A systems approach to incorporate e-mails into a records management environment', *E-doc Magazine*, March/April 2000, 33.

³⁶ Cf. *supra*.

De leesbaarheid op lange termijn komt in het gedrang wanneer er een tijdsperiode is verstreken die zo lang heeft geduurd dat er bezorgdheid is ontstaan over de impact van de veranderende technologie op de middelen die de leesbaarheid op korte termijn garanderen. De impact bestaat erin dat deze middelen (hardware, bestandssysteem, bestandsformaat en/of applicatiesoftware), die aangewend werden bij de aanmaak van het digitale archiefstuk, verouderd zijn door de snelle evoluties in het informaticaveld en bijgevolg niet meer ondersteund worden. De digitale informatie zal dus na verloop van een dergelijke tijdsperiode niet meer kunnen gelezen worden bij gebrek aan de oorspronkelijke hardware, het oorspronkelijke bestandssysteem en/of de oorspronkelijke applicatiesoftware. Ook het oorspronkelijke bestandsformaat zal dan niet meer herkend worden door de nieuwe informaticaomgeving.

Om digitale informatie toch leesbaar te houden op lange termijn, worden er grosso modo drie pistes aangereikt, waarvan het afdrukken van de informatie op papier en het mee archiveren van de technologie (nl. de oorspronkelijke hardware, het oorspronkelijke bestandssysteem (als deel van een besturingssysteem) en de oorspronkelijke applicatiesoftware) de minst aangewezen oplossingen zijn.³⁷ De migratie- en de emulatiestrategie lijken op dit moment de enige bruikbare opties te zijn. Zonder in te gaan op de details van beide strategieën en op de kwestie wanneer welke strategie best gevolgd wordt³⁸, moet hier benadrukt worden dat de migratie of de emulatie, die eventueel werd uitgevoerd voor de overdracht aan de archiefinstelling, goed moet gedocumenteerd worden en dat deze documentatie mee moet overgedragen worden aan de archiefinstelling als metadata. Deze informatie is immers nodig om de ‘goede staat’ van de digitale informatie op het moment van de overdracht te controleren. Want indien de leesbaarheid van de overgedragen informatie niet gegarandeerd is op het moment van de overdracht, zal deze zeker naar de toekomst toe niet kunnen gewaarborgd worden door de archivaris. De archivaris moet dus nagaan of de emulatie(s) en/of migratie(s) op een correcte wijze zijn gebeurd en of alle metadata voorhanden zijn om de historie van deze bewerkingen te kunnen begrijpen. Wanneer er niet tijdig werd ingegrepen om de leesbaarheid op lange termijn te garanderen, dan moet de archiefvormer dit melden bij de overdracht, zodat de archivaris nog kan trachten dit te verhelpen.³⁹

De archiefvormer kan natuurlijk enkel de metadata overdragen die betrekking hebben op de leesbaarheid op lange termijn op het moment van de overdracht. Dit wil zeggen dat enkel informatie kan gegeven worden over de bewerkingen die werden uitgevoerd door de archiefvormer. Wat er verder met de digitale informatie zal gebeuren om de leesbaarheid te garanderen, is een zaak van de archiefinstelling. **Hoewel de archiefinstelling pas het beheer over de digitale archiefstukken krijgt bij de (juridische) overdracht, is het toch aangewezen dat de archivaris de leesbaarheid op lange termijn van deze archiefstukken**

³⁷ BOUDREZ, F., *De archivering van digitale archiefbescheiden: beheersinventaris, informatielagen en beslissingsmodel als uitgangspunt*, Antwerpen, Stadsarchief, 2001, 7.

³⁸ Zie hiervoor: BOUDREZ, F., *o.c.*, 7 e.v.

³⁹ COPPENS, H., *o.c.*, 131. Cf. de meldingsplicht van zichtbare schade, zoals schimmels en door vocht aangetast papier, in hoofde van de overdrager. Deze schade kan de leesbaarheid op lange termijn eveneens in het gedrang brengen indien zij niet wordt verholpen. Net zoals de archivaris voor het herstel van de schade aan papieren archieven soms een beroep moet doen op professionele restaurateurs, zal de ‘digitale’ archivaris soms een beroep moeten doen op computerspecialisten om de nodige emulatie- of migratie-inhaalbeweging te laten uitvoeren.

met een hoge archiefwaarde opvolgt van bij het ontstaan van deze stukken en, indien nodig, richtlijnen geeft over de te volgen strategieën.⁴⁰ De informaticadienst van een organisatie heeft immers niet altijd oog voor de problematiek van permanente bewaring.

VALIDATIE VAN DE OVERDRACHT

Naast de controle van het zich bevinden in goede, geordende en toegankelijke staat, komt daar in de digitale wereld nog een aspect bij nl. de validatie van de overdracht zelf. Hiermee bedoelen we dat de archivaris moet nagaan of de informatie die hij aangeboden krijgt voor archivering, niet gewijzigd is tijdens de overdracht (= **integriteit van de informatie**). Bovendien moet hij er zeker van zijn dat diegene die de informatie aanbiedt, ook werkelijk de persoon of de organisatie is die over de te archiveren informatie beschikt, en niet iemand die zich voordoeft als zijnde de bevoegde persoon of organisatie (= **identificatie van de overdrager**).

Het spreekt voor zich dat de archivaris ook in de papieren wereld geen archiefstukken zal aanvaarden als hij merkt dat ze niet afkomstig zijn van de archiefvormende dienst of instelling. Hij heeft dan immers goede redenen om aan te nemen dat de archiefstukken zelf niet authentiek zijn. In een papieren omgeving dringt deze problematiek zich echter niet in dezelfde mate op zoals in de digitale wereld, en hij wordt dan ook niet behandeld in de klassieke werken over archivering en archiefbeheer. Met de overdracht van papieren archiefstukken gaat er immers steeds een fysisch contact gepaard tussen de (verantwoordelijke van de) archiefvormende organisatie en de archivaris (of één van zijn medewerkers), meestal doordat de archiefinstelling de fysieke stukken ophaalt in de gebouwen de archiefvormende organisatie. Op die manier vindt de identificatie van de overdrager onbewust plaats. De archivaris zal er zich echter nooit bewust vragen over stellen.

In een digitale omgeving is deze controle soms wel vereist, afhankelijk van manier waarop de overdracht van de digitale informatie gebeurt. Worden er voorlopig nog digitale dragers overgedragen en gearhiveerd, dan dient er een fysisch contact plaats te vinden en is er geen probleem. Wanneer de digitale informatie echter via een telecommunicatienetwerk naar de archiefinstelling wordt gestuurd, dan is er geen fysisch contact mogelijk. Diegene die zich aanbiedt met de informatie, kan dan in principe eender wie zijn. De geëigende manier om zich op Internet of in een ander netwerk kenbaar te maken aan zijn communicatiepartner, is met behulp van zijn digitale handtekening. Wanneer de informatie op de locale server van de archiefvormende organisatie blijft staan voor de archivering, gebeurt er zelfs geen virtuele verplaatsing tussen de verschillende onderdelen van een netwerk door een overdrager die

⁴⁰ Bijvoorbeeld het formaat waarin een document best wordt aangemaakt, de termijn waarbinnen voor dat formaat aan migratie moet gedacht worden, aanbevelingen betreffende het gebruik van zo ruim mogelijk ondersteunde applicatiesoftware... Dit kan vergeleken worden met de taak van de archivaris in de papieren wereld om te wijzen op de geringe houdbaarheid van bepaalde papiersoorten, om het gebruik van bepaald verpakkingsmateriaal aan te bevelen (zo heeft het Algemeen Rijksarchief mappen en archiefdozen laten ontwikkelen die beantwoorden aan de voorwaarden voor langdurige bewaring)...

moet geïdentificeerd worden. Het is dan de server zelf die moet geïdentificeerd worden als toebehorend aan de archiefvormende organisatie. Ook hiervoor kan PKI een oplossing bieden.

Ter gelegenheid van de overdracht van digitale informatie moet ook de integriteit van deze informatie gecontroleerd worden. Bij papieren archiefstukken is het onmogelijk dat de data tijdens de overdracht wijzigen, vermits het papier en de verpakking integriteitsbeschermend werken. Dankzij het papier is de inhoud op een stabiele wijze vastgelegd. De verpakking fungeert als een soort enveloppe, waardoor de inhoud beschermd is tegen invloeden van buitenaf.

Op digitaal niveau doet het probleem zich enkel voor wanneer de informatie voor de overdracht op een digitale gegevensdrager wordt geplaatst en wanneer er een telecommunicatienetwerk wordt gebruikt. Voor de digitale versie van het Antwerpse kiezersregister van de verkiezingen van 8 oktober 2000 werd de eerste piste gekozen.⁴¹ Vóór de overdracht stond het kiezersregister in zijn origineel formaat op de mainframecomputer van de dienst burgerzaken. Naar aanleiding van de archivering werden alle bestanden op CD-rom geplaatst en zo overgedragen aan het stadsarchief. In dit scenario wordt er een kopie gemaakt op een andere drager om de overdracht te kunnen doen. Dit kan tot integriteitsverlies leiden wanneer er een fout gebeurt bij het kopiëren. Vermits de archiefvormer deze kopie maakt, is het aan hem om een integriteitscheck uit te voeren vóór de overdracht. Het is de archiefvormer die verantwoordelijk is voor de inhoud van wat hij overdraagt.

In het andere scenario moet er een soort enveloppe gecreëerd worden, zodat de digitale informatie tijdens de transfer niet kan gewijzigd worden. PKI kan hier opnieuw een oplossing bieden. Het is hierbij aan te bevelen dat de archiefvormer de digitale archiefstukken niet onmiddellijk verwijdert van de harde schijf van zijn computer. Het nadeel van een digitale transfer is immers het feit dat het wel mogelijk is dat de inhoud wijzigt tijdens de korte periode van de transfer. Wanneer de archivaris dit vaststelt, moet de overdracht opnieuw gebeuren.

VERKLARING VAN OVERDRACHT

In het OAIS-model moet er een bevestiging van de ontvangst volgen op de ontvangst van het overgedragen informatiepakket. Dit is nodig opdat op onbetwistbare wijze kan vastgesteld worden dat de beheersverantwoordelijkheid vanaf een bepaald moment bij de archiefinstelling berust. In de papieren wereld gebeurt dit aan de hand van een verklaring van overdracht. Wanneer de archivaris vaststelt dat de kwaliteit van de archiefstukken gegarandeerd is bij de overdracht, wordt er een verklaring van overdracht opgemaakt. Deze verklaring is een overeenkomst tussen de archiefvormer en de archiefinstelling, waarmee de archiefvormer het beheer over bepaalde archiefstukken overdraagt aan de archiefinstelling en deze laatste verklaart ze op een bepaalde datum in ontvangst te hebben genomen. De beide betrokken partijen bekrachtigen de overeenkomst met hun handtekening.⁴² Deze overeenkomst wordt

⁴¹ Deze keuze is ingegeven door het feit dat in de meeste administraties op dit moment nog geen PKI is uitgebouwd, waardoor een digitale overdracht nog niet voldoende beveiligd kan verlopen.

⁴² COPPENS, H., *o.c.*, 192.

opgemaakt in twee exemplaren en wordt bewaard in het overdrachtdossier, waarin de overdracht omstandig is gedocumenteerd.

Worden er digitale dragers overgedragen, dan wordt de verklaring op papier mee overgedragen met de dragers. Wanneer de overdracht via een telecommunicatienetwerk plaatsvindt, spreekt het voor zich dat ook de verklaring van overdracht digitaal zal opgemaakt en uitgewisseld worden. PKI kan hier gebruikt worden om een elektronische handtekening te creëren. Bovendien kan door het gebruik van PKI komen vast te staan dat de archivaris de overgedragen informatie wel degelijk heeft ontvangen. In de papieren wereld zijn er hierover nog nooit discussies ontstaan, maar naar aanleiding van een digitale overdracht zouden deze discussies wel eens kunnen ontstaan. Stel dat de archiefvormer de informatie na de overdracht verwijderd van de harde schijf, en achteraf blijkt dat de archiefinstelling deze nooit heeft ontvangen. Om dit te vermijden stuurt de archivaris samen met de door hem elektronisch ondertekende verklaring van overdracht, het geheel van overgedragen informatiepakketten samen met de daarvoor berekende digitale handtekening naar de archiefvormer. Op die manier weet de archiefvormer zeker dat de archiefinstelling de overgedragen informatiepakketten heeft ontvangen, en kan hij ze uit het eigen documentatiebeheerssysteem verwijderen. De digitale handtekening wordt immers berekend op basis van de overgedragen informatiepakketten. De teruggestuurde informatiepakketten en digitale handtekening moet de archiefvormer na deze controle trouwens ook niet bewaren; de archivering zou het eigen documentatiebeheerssysteem dan alleen maar belasten in plaats van ontlasten.

Men zou kunnen aanvoeren dat de overdrager, ter vervanging van een elektronische verklaring van overdracht, bij het verzenden van digitale informatie de ontvangstfunctie zou kunnen instellen, waardoor hij een bericht zal ontvangen wanneer de informatie toekomt, waarin bevestigd wordt dat de geadresseerde de informatie ontvangen heeft.⁴³ Voor een overdracht naar aanleiding van archivering is deze werkwijze echter onbruikbaar, vermits het niet de ontvangst op zich is die moet vastgelegd worden, maar wel de bevestiging door de archivaris dat de stukken kwalitatief in orde waren bij de overdracht en dat hij ze in die staat in ontvangst heeft genomen. De archivaris moet zich dus na een grondige controle een oordeel vormen of hij de overgedragen stukken in de toestand waarin ze zich bevinden, kan en wil ontvangen. Deze beslissing kan niet door een automatisch *reply-system* worden genomen.

Indien de stukken op de locale server blijven staan, dan zal de (datum van de) overdracht ook juridisch moeten vastgelegd worden, ook al vindt er geen fysieke overdracht plaats. Vermits er geen fysiek contact plaatsvindt tussen de overdrager en de archivaris, is de meest praktische oplossing dat deze overeenkomst elektronisch wordt afgesloten en ondertekend.

Een belangrijk onderdeel van de verklaring van overdracht, is **de vermelding van de datum** waarop de stukken zijn overgedragen. Is de overeenkomst in elektronische vorm afgesloten, dan zijn er theoretisch gezien twee mogelijkheden om een datum in dit elektronisch bericht op te nemen. De datum kan door de partijen vastgesteld worden en gewoon deel uitmaken van de tekst van de overeenkomst, zoals in de papieren wereld steeds het geval is. Elektronische berichten kunnen ook een datum verkrijgen doordat een derde partij deze datum vaststelt, de

⁴³ De meeste e-mailprogramma's zijn met deze functie uitgerust.

‘Time-Stamping Authority’ (TSA) genoemd.⁴⁴ De procedure van het verkrijgen van een ‘time-stamp’ ziet er als volgt uit: de computer van de archiefvormer berekent een hashing-code voor de elektronisch aangemaakte verklaring van overdracht. Deze hashing-code wordt dan op een beveiligde manier over het Internet naar de TSA gezonden, die de datum en eventueel het tijdstip van het ‘time-stampen’ eraan toevoegt⁴⁵, en vervolgens dat geheel ‘ondertekent’ met zijn private sleutel. Het resultaat noemt men de ‘time-stamp’ en wordt teruggestuurd naar de archiefvormer. De ‘time-stamp’ wordt aan de verklaring van overdracht toegevoegd en wordt mee elektronisch ondertekend. Indien men later de datum van de overdracht wil bewijzen, dan weet men aan de hand van de overeenstemmende hashing-codes (de hashing-code berekend op basis van de originele tekst en de ontsleutelde ‘time-stamp’) dat de datum werd toegevoegd aan de inhoud die achter de hashing-codes schuil gaat, of met andere woorden, dat het wel degelijk gaat om de datum van de verklaring van overdracht.

‘Time-stamping’ is een manier om de datum van een overeenkomst die op elektronische wijze werd gesloten, op een onbetwistbare wijze vast te leggen. Deze techniek is gebaseerd op de idee dat de getijdstempelde informatie moet bestaan hebben ten laatste op het moment dat de ‘time-stamp’ tot stand komt. Dit is logisch, vermits de ‘time-stamp’ berekend wordt op basis van de inhoud van de getijdstempelde informatie. De TSA doet dus in feite niets anders dan het vaststellen van een feit, nl. het bestaan van bepaalde elektronische informatie, en het toevoegen van de datum van deze vaststelling aan deze elektronische informatie. Met behulp van de techniek van ‘time-stamping’ kan dan ook enkel elektronische informatie een datum verkrijgen.

De datum die voorkomt in een verklaring van overdracht, is echter de datum waarop de overdracht heeft plaatsgevonden.⁴⁶ Het gaat dus om de datum van een gebeurtenis die moet vastgelegd worden, niet om de datum van een feit. In een elektronische archiefomgeving bestaat er slechts één overdrachtsscenario waarbij de gebeurtenis van de overdracht blijkt uit het bestaan van elektronische informatie nl. het geval waarbij de te archiveren archiefstukken op de server van de archiefvormer blijven staan. De versleutelde toestand van de archiefstukken (met de publieke sleutel van de archivaris), wijst er op dat de stukken een gearchieveerde status hebben. Bijgevolg kan voor dit scenario de datum van de overdracht via de techniek van ‘time-stamping’ worden vastgelegd. De archivaris stuurt de hashing-code van de versleutelde archiefstukken naar de TAS, die de time-stamp berekent voor deze elektronische informatie. Deze time-stamp wordt teruggezonden naar de archivaris en toegevoegd aan de elektronische verklaring van overdracht, die dan elektronisch wordt ondertekend. De ‘time-stamp’ bewijst dat de versleutelde en dus ontoegankelijke archiefstukken bestonden op het tijdstip die zit vervat in de ‘time-stamp’, en bijgevolg dat de archiefstukken op dat tijdstip overgedragen waren.

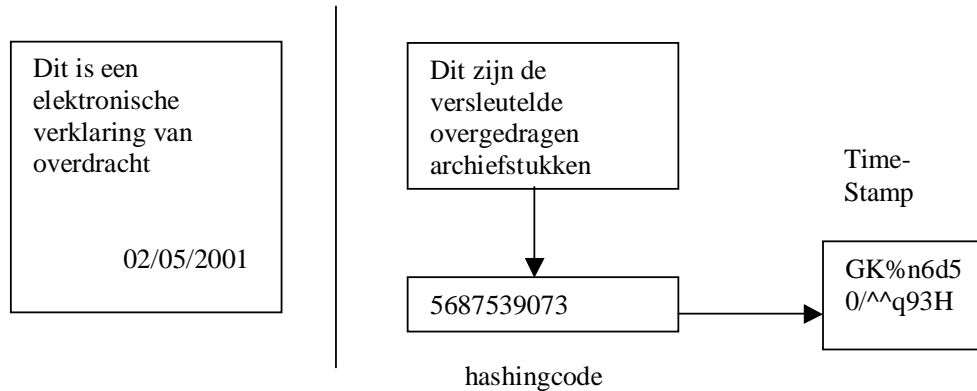
⁴⁴ Op dit moment zijn er al heel wat TSAs operatief op het Internet.

Zie: <http://www.cryptomathic.com/products/timeink.html> ,
<http://www.wisekey.com/swissetime/index.htm>

⁴⁵ Bepaalde technieken zorgen ervoor dat de TSA steeds de correcte datum en tijd toevoegt aan de hashing-code.

⁴⁶ COPPENS, H., o.c., 193: “Het ondergetekende dienst- of instellingshoofd verklaart *op een bepaalde datum* de in de specificatie opgenomen bescheiden *te hebben overgedragen* aan de archiefbeheerder, die deze in ontvangst heeft genomen.” De datum slaat niet op de verklaring, maar op de overdracht.

Time-stamping kan niet gebruikt worden om de datum van de overdracht in de overeenkomst vast te leggen, wanneer de overdracht gebeurt door het overleggen van gegevensdragers of via een telecommunicatienetwerk. In deze gevallen kan de overdracht immers niet afgeleid worden uit een geheel van elektronische gegevens. De datum van de overdracht moet dan in de overeenkomst zelf worden opgenomen door de partijen bij de overdracht.



Taak 3: Generatie van het te archiveren informatiepakket

Vervolgens moet de archivaris op basis van het overgedragen informatiepakket het te archiveren informatiepakket samenstellen. De kans is zeer klein dat het overgedragen informatiepakket zonder meer kan gearchiveerd worden. Dit type informatiepakket heeft immers niet alle kwaliteiten die nodig zijn voor de bewaring op lange termijn van het inhoudelijke informatie-object dat het bevat. Dit mag blijken uit de volgende situaties die zich kunnen voordoen. Het is dan aan de archivaris om dit informatiepakket zodanig te transformeren dat het deze kwaliteiten wel bezit.

Vooreerst is het erg waarschijnlijk dat de archivaris de overgedragen informatiepakketten moet opsplitsen of moet samenvoegen alvorens hij tot archivering kan overgaan. Het is bijvoorbeeld mogelijk dat een overgedragen informatiepakket moet opgesplitst worden in twee delen om een onderscheid te maken tussen de informatie die openbaar is en de informatie die gesloten moet blijven. Anderzijds is het ook mogelijk dat de archivaris verschillende overgedragen informatiepakketten samenvoegt omdat bijv. de voorstellingsinformatie steeds dezelfde is. Na een samenvoeging of een splitsing zal eventueel ook de pakketinformatie en pakketbeschrijving moeten aangepast worden.

Verder spreekt het natuurlijk voor zich dat de archivaris sowieso bepaalde informatie zal moeten toevoegen, omdat de archiefvormer er niet over beschikt. De authenticiteitsgaranderen informatie is hiervan het meest typerende voorbeeld. Het is de

archivaris die de digitale handtekening moet toevoegen aan de te archiveren informatie, die wordt berekend op basis van het inhoudelijke informatieobject. Het is immers deze informatie waarop de bewaring in de eerste plaats gericht is en die moet beveiligd worden. Het is essentieel dat enkel de archivaris deze informatie kan toevoegen. Ook welke semantische informatie er precies moet toegevoegd worden, zal de archivaris vaak zelf moeten inschatten, omdat de archiefvormer hiervoor helemaal niet gevoelig is. Denk aan de hierboven genoemde voorbeelden van de documenten in verschillende talen of de gebruikte codes. Er moeten in ieder geval duidelijke afspraken gemaakt worden over de aard van de informatie die de archivaris verwacht dat de archiefvormer mee overdraagt en het formaat waarin deze informatie moet staan. Maar het ligt in de lijn van de verwachting dat deze archivistische richtlijnen niet volledig zullen worden nageleefd, zeker niet tijdens de beginfase van digitale archivering van de stukken van een archiefvormer. De verantwoordelijkheid ligt dan opnieuw bij de archivaris. Het is bijvoorbeeld helemaal niet ondenkbaar dat de archiefvormer niet vertrouwd is met formaten die gericht zijn op het aanbrengen van semantische structuur in elektronische informatie en die erg geschikt zijn voor de bewaring van deze informatie op lange termijn, zoals XML.

Tenslotte is het ook mogelijk dat de interpretatieve informatie vervat zit in het inhoudelijke informatieobject en dat de archivaris deze informatie zelf moet extraheren uit het overgedragen informatiepakket. Deze informatie moet echter op een meer gestructureerde manier opgeslagen worden, omdat deze gegevens een belangrijke bron zijn om de archiefstukken toegankelijk te maken.

Het is aan te bevelen dat de afspraken die gemaakt worden tussen de archiefvormer en de archiefinstelling erop gericht zijn om het overgedragen informatiepakket zoveel mogelijk te laten aansluiten bij het te archiveren informatiepakket dat eruit moet voortvloeien. Iedere toevoeging of wijziging die de archivaris aanbrengt bij de transformatie van overgedragen naar te archiveren informatiepakket moet gedocumenteerd worden in de corresponderende metadata (voorstellingsinformatie bij wijziging van formaat, toevoegen van de authenticiteitsgaranderende informatie...)

Taak 4: generatie van pakketbeschrijvingsinformatie

Nog voor de eigenlijke archivering, is het nodig dat de archivaris de pakketbeschrijvingsinformatie samenstelt. Deze informatie omvat alle gegevens die nodig zijn om de klant toe te laten om gearchiveerde informatie die voor hem mogelijk van nut is, te vinden, te analyseren en op te vragen. Het is de taak van de archivaris om deze elementen te identificeren en te extraheren uit het te archiveren informatiepakket of eventueel uit andere bronnen. Er zal hierbij veel aandacht uitgaan naar de openbaarheid van de archiefstukken. De pakketbeschrijvingsinformatie moet ook de unieke coördinaten bevatten van het te archiveren informatiepakket in het archiefsysteem.

Deze informatie moet geïdentificeerd en afgezonderd worden opdat zij kan opgenomen worden in de *tools* die toegang verlenen tot de archiefstukken.

2. Opslag

Taak 1: archivering voor permanente bewaring

Als duidelijk is geworden welke informatie er precies allemaal moet gearchiveerd worden, is het te archiveren informatiepakket klaar om definitief ondergebracht te worden in het archiefsysteem. Hier moet de archivaris beslissen voor welke wijze van opslag er best gekozen wordt voor het betreffende te archiveren informatiepakket. Er zijn twee opties:

- Ofwel wordt het informatiepakket in een online netwerkomgeving bewaard, wat raadpleging van overal ter wereld op ieder moment mogelijk maakt. Op die manier kunnen er ook gemakkelijk verbanden worden gelegd tussen verschillende informatiepakketten. De informatie staat dan op de harde schijf van een PC of op de daarvoor voorbehouden serverruimte.
- Ofwel is de drager waarop het informatiepakket bewaard wordt, niet online toegankelijk. Het gaat dan bijv. om CD-ROMs of diskettes die in een archiefkast bewaard worden. Het nadeel van deze laatste werkwijze is dat de raadpleging van de stukken steeds ter plaatse moet gebeuren. Op termijn is het de bedoeling dat alle stukken in een netwerkomgeving gearchiveerd worden. Het beleid van de archiefinstelling op dit vlak en een tijdschema waarbinnen de evolutie naar een netwerkomgeving dient plaats te vinden, moet worden vastgelegd in het archiefbeleid.

De keuze voor de wijze van archivering is niet noodzakelijk afhankelijk van de wijze van overdracht. Worden er door de archiefvormer digitale gegevensdragers overgedragen ter archivering, dan kan de archivaris alsnog beslissen om het informatiepakket naar een netwerkomgeving over te zetten wanneer dit meer verantwoord is voor bijv. de raadpleging. Er moet in ieder geval voor opgelet worden dat bij iedere transfer binnen het archiefsysteem de authenticiteit gewaarborgd blijft. Dit kan problemen opleveren wanneer de digitale handtekening berekend werd op het te archiveren informatiepakket, maar wanneer dit pakket voor de archivering naar een andere omgeving getransporteerd wordt, waardoor de bitreeks van de gehandtekte informatie wijzigt. De waarde van de digitale handtekening gaat dan volledig verloren. **De overdracht en de wijze van archivering worden in ieder geval best zo veel mogelijk op elkaar afgestemd.**

Bij opslag in een digitaal archief krijgt het risico voor vermenging een totaal andere betekenis. In de papieren wereld betekent dit dat archiefstukken fysisch terecht komen in archiefbestanden waar ze niet thuis horen. Er is het principe van eenheid van archiefbestand ingegeven door het bestemmingsbeginsel: ieder archiefstuk maakt deel uit van het archiefbestand van een organisatie waarvoor het naar zijn aard bestemd is en indien het is opgemaakt of ontvangen als onderdeel van het werkproces van de organisatie. In een digitale omgeving betekent dit dat een archiefbestand van een organisatie of van een persoon als een afzonderlijke entiteit moet terug te vinden zijn, maar de opslag zelf kan gebeuren op hetzelfde medium als een ander archiefbestand. Het is de software van het archiefsysteem die bepaalt in welke volgorde de op te slagen informatie op de drager zal staan. Deze problematiek heeft te maken met de kwestie van de toegang tot de archiefstukken.

Taak 2: Migratie / Emulatie

Wanneer de informatie definitief in het archief is opgeslagen, zal de archivaris stappen moeten ondernemen om de informatie leesbaar te houden op lange termijn. De archivaris mag echter niet wachten om maatregelen te nemen tot het moment waarop de impact van de veranderende technologie op de middelen die de leesbaarheid op korte termijn garanderen, voelbaar wordt. Van zodra het informaticapakket gearhiveerd is, dient de archiefinstelling een studie te voeren over de te nemen maatregelen en het tijdstip waarop deze best genomen worden, rekening houdend met de te voorspellen technologische evoluties, met de aard van de gearhiveerde informatie, afgewogen aan de hand van de inventaris van de digitale informatie bij de archiefvormer aanwezig, en met de historie van de reeds uitgevoerde bewerkingen, hetzij door de archiefvormer, hetzij door de archivaris. Een bijzonder aandachtspunt is de vraag of de digitale handtekening een migratie / emulatie al dan niet overleeft.

In het OAIS-model wordt er gekozen voor een migratie-strategie, zonder echt te verantwoorden waarom. De typologie van de digitale overheidsdocumenten voor de Stad Antwerpen heeft echter uitgewezen dat er niet één beste oplossing is voor alle gevallen.⁴⁷ Beiden zullen hun diensten bewijzen, en soms zullen ze misschien samen moeten toegepast worden voor dezelfde informatie. De beschrijving in het OAIS-model van de soorten migratie die kunnen voorkomen, is wel interessant met het oog op het beantwoorden van de vraag in welke gevallen een digitale handtekening de migratie-operatie niet overleeft. Migraties kunnen ingedeeld worden naargelang de risico's op informatieverlies die de bewerking heeft voor het informatiepakket.

- Vooreerst is er wat OAIS '*Refreshment*' noemt. Deze vorm van migratie komt erop neer dat er geen enkele bit wijzigt aan het gearhiveerde informatiepakket. Een voorbeeld kan zijn dat het gearhiveerde informatiepakket op een punt is gekomen dat het aantal 'bit errors' onverantwoord is geworden en dat er dus kopie moet gemaakt worden op een andere drager. Wanneer de equivalentie van deze kopie vast te staan (waarvoor de hashingtechniek kan gebruikt worden), kan zij de oorspronkelijk gearhiveerde versie vervangen. De digitale handtekening kan dan zonder meer gekopieerd worden, vermits de bitreeks van het inhoudelijke informatieobject hetzelfde is gebleven.
- '*Replication*' is een variant van 'Refreshments'. Bij 'Replication' is er de complicatie dat er wijzigingen moeten aangebracht worden aan de informatie die nodig is om het informatiepakket te kunnen terugvinden in het archiefsysteem. Dit is bijv. het geval wanneer de gemaakte kopie op een zelfde soort drager wordt geplaatst, maar die bijv. meer opslagcapaciteit heeft dan de oude drager.
- '*Repackaging*' betekent dat de migratie leidt tot wijzigingen in de pakketinformatie. Het typevoorbeeld is hier het overzetten naar een ander soort drager, die een andere bestandsstructuur heeft. De verschillende onderdelen van het informatiepakket die op de nieuwe drager staan, zullen dan op een andere manier moeten afgebakend en

⁴⁷ BOUDREZ, F., Typologie van digitale overheidsdocumenten, Antwerpen, Stadsarchief, 2001, 11.

geïdentificeerd moeten worden als samenhoerend. De bitreeks van het inhoudelijke informatieobject wijzigt echter niet, zodat de digitale handtekening zonder problemen kan behouden blijven.

- ‘*Transformation*’ tenslotte houdt in dat de bitreeks van het inhoudelijke informatieobject gewijzigd wordt, ‘getransformeerd’ wordt. Deze vorm van migratie zal zich voordoen bij de omzetting naar een ander formaat. Wanneer bijvoorbeeld ASCII-code (8 bits) wordt omgezet in Unicode (16 bits), dan wordt in de nieuwe versie één karakter voorgesteld door meer bits dan oorspronkelijk. De corresponderende voorstellingsinformatie moet dan ook mee aangepast worden. De oorspronkelijke digitale handtekening gaat echter verloren en er moet een nieuwe ‘verzegeling’ plaatsvinden na migratie. Het behoud van authenticiteit en integriteit van het nieuwe informatiepakket moet door de archivaris gegarandeerd worden, zodat de klanten erop kunnen vertrouwen dat het inhoudelijk nog steeds om dezelfde informatie gaat, ook al is er van de oorspronkelijke bitreeks totaal geen sprake meer.

Ieder migratieproces, hoe klein de risico’s op informatieverlies ook zijn, zal steeds uitvoerig moeten gedocumenteerd worden in de interpretatieve informatie.

Taak 3: Maken van veiligheidskopieën van gearcheeerd informatiepakket

Telkens wanneer het informatiepakket opnieuw wordt vastgelegd voor permanente bewaring (bijv. na een migratie), dient er een veiligheidskopie gemaakt te worden. Dit sluit aan bij wat reeds eerder werd gezegd in het rapport ‘Digitale archivering: juridische stand van zaken. Deel 1’ omtrent de vormvereiste die oplegt dat er meerdere exemplaren moeten bewaard worden. Ondanks het feit dat een digitale drager een bedreiging kan vormen voor de informatie, omdat een digitale drager veel van de kwaliteiten moet prijsgeven die aan papier kunnen toegeschreven worden, waardoor vooral de te bewaren informatie zelf moet beschermd worden, eerder dan de drager⁴⁸, is er bij elektronische informatie hoe dan ook sprake van een drager die de informatie vasthoudt. De enige oplossing om deze drager te beschermen tegen externe invloeden, bestaat erin om de informatie in meerdere exemplaren te bewaren.⁴⁹

Teneinde in geval van vernietiging, beschadiging of onbruikbaarheid van de drager volledig te kunnen terugvallen op de veiligheidskopie, moet niet alleen van het inhoudelijke informatieobject een kopie worden gemaakt, maar van het hele informatiepakket zoals het werd klaargemaakt voor archivering in het archiefsysteem. Het maken van deze kopie mag in geen geval uitgesteld worden. Beide exemplaren moeten idealiter tegelijkertijd gearcheeerd worden. Bovendien moet erover gewaakt worden dat de veiligheidskopie eveneens het origineel bevat. Het woord ‘*veiligheidskopie*’ is hier dus eigenlijk niet op zijn plaats. Beter is

⁴⁸ De drager alleen volstaat niet meer om de integriteit en de duurzame beschikbaarheid van de inhoud te garanderen.

⁴⁹ VAN DEN EYNDE, S., *Digitale archivering: een juridische stand van zaken. Deel 1*, Leuven, ICRI, 2001, 58.

te spreken over ‘het tweede exemplaar’. [Vraag: moet het tweede exemplaar dezelfde bitreeks hebben om te kunnen checken of het gaat om een origineel aan de hand van de hashing-techniek?]

Het reserve-exemplaar moet in ieder geval op een fysiek gescheiden medium geplaatst worden, die ruimtelijk gezien ook gescheiden zijn. Dit kan gebeuren door het informatiepakket op een verplaatsbare drager te zetten, die op een andere plaats bewaard wordt. De informatie kan ook over een telecommunicatienetwerk gestuurd worden, waardoor er elders een tweede exemplaar ontstaat.

Taak 4: ontoegankelijk maken van de gearchiveerde informatiepakketten

De archivaris moet zeker kunnen zijn dat er niemand op ongeoorloofde wijze toegang kan verkrijgen tot de gearchiveerde informatiepakketten om fraude te vermijden (**ontoegankelijk maken voor derden**). Ten aanzien van papieren archiefstukken bestaan er een aantal methoden om dit te vermijden. De toegang tot het archiefdepot moet formeel worden verboden en verhinderd (bijv. door bordjes ‘verboden toegang’ en door de mogelijkheid het archiefdepot af te sluiten zodanig dat enkel de personen die over de sleutel beschikken, er toegang toe hebben). Bovendien voorzien archiefinstellingen in een registratieprocedure voor alle leeszaalbezoekers. Toegang tot de archiefstukken moet met andere woorden steeds gebeuren via de omweg van een archiefmedewerker, die de stukken uit hun beschermde archiefomgeving weghaalt en de raadpleging vervolgens op een gecontroleerde manier laat verlopen.

Voor offline toegankelijke digitale dragers kan deze procedure behouden blijven: zij worden in een gesloten archiefkast bewaard, waarvan alleen de archivaris (en zijn archiefmedewerkers) de sleutel hebben. Een netwerkomgeving daarentegen heeft precies de eigenschap dat dit door verschillende personen kan betreden worden. Het netwerk moet natuurlijk zo goed mogelijk beveiligd worden, maar men kan en zal steeds proberen in te breken in het archiefsysteem. Daarom moet de gearchiveerde informatie zelf ontoegankelijk gemaakt worden. PKI kan hiervoor aangewend worden door het inhoudelijk informatieobject te versleutelen met de publieke sleutel van de archivaris; enkel diegene die over de corresponderende private sleutel beschikt (zijnde de archivaris zelf) heeft toegang tot de inhoud.

3. Toegang en Data Management

Taak 1: Onderhoud Data Management Databank

In een digitaal archief wordt de toegang tot de opgeslagen informatie geregeld vanuit de ‘Data Management Databank’. Deze databank bevat voor ieder opgeslagen informatiepakket de pakketbeschrijvingsinformatie op een gestructureerde manier, waarin de tools die het

archiefsysteem toegankelijk maken voor de klanten de nodige informatie kunnen vinden om het gezochte informatiepakket terug te vinden. Van zodra de archivering een feit is, moet deze informatie hierin terug te vinden zijn.

Deze databank moet up-to-date gehouden worden om een efficiënte raadpleging mogelijk te maken. De pakketbeschrijving van informatiepakketten die uit het archief verwijderd worden, wegens beperkte bewaartermijn, moet eveneens verwijderd worden. Het feit dat een informatiepakket openbaar wordt, na lange tijd gesloten te zijn geweest, moet weerspiegeld worden in de pakketbeschrijving, zodat de mechanismen die het stuk effectief ter beschikking stellen, ‘weten’ dat het informatiepakket openbaar is. Na een overplaatsing naar een andere drager, is het van belang te weten of de unieke coördinaten van het informatiepakket binnen het archiefsysteem veranderd zijn enz.

Taak 2: Ontvangen van een vraag tot raadpleging

De archiefinstelling kan op verschillende wijzen geraadpleegd worden door klanten:

- De archiefinstelling kan een online dienst voorzien in de vorm van een eigen website als user interface, aan de hand waarvan de klant altijd en overal de archiefdienst kan bevragen. De klant kan een e-mail sturen naar de archiefdienst om het gezochte stuk aan te vragen.
- Het is ook mogelijk dat de klant zich ter plaatse persoonlijk aanbiedt om een stuk te raadplegen (*walk-in facility*) Hoewel het Internetgebruik in Vlaanderen de laatste maanden spectaculair gestegen is, blijft Internettoegang voor een relatief groot deel van de bevolking problematisch.⁵⁰ Het zich persoonlijk aanbieden zal dus voor heel wat mensen voorlopig de enige manier zijn om een vraag tot de archivaris te richten.

Taak 3: Samenstellen van toegankelijk gemaakt informatiepakket

In het OAIS-model is de informatie die aan de klant wordt overgelegd slechts een ‘kopie’ van het gearchiveerde informatiepakket. In de digitale wereld mag de archivaris nooit de gearchiveerde informatie als zodanig in handen geven van de klant zonder dat hij zelf ook over die informatie blijft beschikken. Naast het gearchiveerde informatiepakket en het tweede exemplaar als veiligheidskopie, moet de archivaris met andere woorden nog een kopie creëren naar aanleiding van de raadpleging. Ook in de papieren wereld wordt de vrije raadpleging van de originele stukken beperkt en wordt er steeds een vervangingskopie ter inzage gegeven als die voorhanden is. Het voordeel van de digitale wereld bestaat erin dat deze ‘kopieën’ zeer snel kunnen gemaakt worden en dat het eveneens originelen zijn, wat voor de klanten een enorme meerwaarde betekent.

In tegenstelling tot het gearchiveerde informatiepakket, dat speciaal is ontworpen voor bewaring op lange termijn, is het toegankelijk gemaakte informatiepakket zodanig samengesteld dat het beantwoordt aan de eisen van de klant en aan de

⁵⁰ Hoge Raad voor de werkgelegenheid. Synthese en aanbevelingen, februari 2001.
<http://meta.fgov.be/pdf/pd/nldf7.pdf>

openbaarheidsvoorwaarden. Stel dat de klant slechts één document wil raadplegen dat deel uitmaakt van een zeer groot informatiepakket bijv. de registers van de burgerlijke stand van een tienjarige periode. De archivaris zal de gevraagde informatie dan moeten afzonderen en overmaken aan de klant. De raadplegingskopie is dus niet noodzakelijk een exacte kopie van het gearchiveerde informatiepakket. De informatie die ter beschikking wordt gesteld moet wel het origineel zijn. Het is bijvoorbeeld ook mogelijk dat de gevraagde informatie naar aanleiding van de privacywetgeving moet geanonimiseerd worden.

Taak 4: Ter beschikking stellen van een toegankelijk gemaakt informatiepakket

De archivaris kan op verschillende manieren het toegankelijk gemaakte informatiepakket aanbieden aan de klant. Dit zal evenwel afhankelijk zijn van de toegang van de klant tot de nieuwe telecommunicatiemiddelen en eveneens van de graad van automatisering van de archiefinstelling. Het is bijv. mogelijk dat de archiefinstelling wel de mogelijkheid voorziet om via e-mail vragen te stellen over de aanwezigheid van bepaalde stukken, of zoekfuncties online ter beschikking stelt, maar dat de raadpleging van de stukken zelf online nog niet mogelijk is.

- In een eerste fase zullen de archiefstukken nog niet online raadpleegbaar zijn, omdat ze nog op digitale dragers bewaard worden die niet toegankelijk zijn via telecommunicatiemiddelen, zoals het Internet. De archiefinstelling kan de klant dan toch een aantal diensten online aanbieden, zoals archievenoverzichten en inventarissen aan de hand waarvan de klant zijn bezoek aan de leeszaal kan voorbereiden. Deze klassieke toegangsmiddelen zijn sterk verbonden met de fysische plaatsing van het archiefstuk in het archief, wat nodig blijft voor deze wijze van opslag. De **raadpleging** dient echter **ter plaatse** te gebeuren. In de leeszaal moet de nodige apparatuur worden voorzien om de dragers te kunnen lezen.
- Bij digitale archivering is het uiteindelijk te bedoeling om alle archiefstukken in een netwerkgeving te bewaren. **Online raadpleging** wordt dan wel mogelijk, hetzij onmiddellijk voor privacy-ongevoelige stukken die sowieso voor iedereen toegankelijk zijn, hetzij doordat de archivaris het gevraagde stuk via e-mail aan de klant bezorgt. Het online opzoeken van de stukken krijgt in deze context eveneens een andere betekenis, doordat er andere toegangen kunnen gecreëerd en gebruikt worden, die niet meer aan de fysische plaatsing is gebonden. Deze toegangen zijn gebaseerd op de pakketbeschrijvingsinformatie.

Bij de raadpleging kan een onderscheid gemaakt worden tussen raadpleging door de eigen medewerkers van de archiefvormende organisatie (bijv. in een gemeente door de gemeenteambtenaren) of door derden/klanten. Aan de archiefvormer wordt in de papieren wereld vaak uitlening toegestaan van de originele stukken. Uiteindelijk is het immers de archiefvormer die eigenaar blijft van de stukken.⁵¹ De gemeentewet bepaalt evenwel ten

⁵¹ Tenzij in de uitzonderlijke gevallen van schenking of koop van archiefstukken door de archiefinstelling. Archiefstukken van overheidsorganen maken deel uit van het openbaar domein en

aanzien van gemeentearchieven dat het college van burgemeester en schepenen 'belet dat enig stuk uit de bewaarplaats weggenomen wordt'. Toch moet 'bewaarplaats' in dit voorschrift geïnterpreteerd worden als 'het geheel van de dienstgebouwen' opdat een efficiënt werkproces mogelijk blijft.⁵² De archiefvormer moet steeds over zijn eigen stukken kunnen blijven beschikken.

Uitlening van de papieren archiefstukken is niet toegelaten ten aanzien van derden. Raadpleging dient door hen steeds onder toezicht te gebeuren in de leeszaal. De originelen mogen nooit direct toegankelijk worden opgesteld, de leeszaal mag nooit betreden worden met mantels en boekentassen en er wordt slechts één archiefstuk tegelijk in lezing gegeven, dat eerst moet worden teruggegeven aan de archiefmedewerker alvorens een nieuw stuk mag geraadpleegd worden. De reden voor deze werkwijze is het feit dat archiefstukken unieke stukken zijn waar er slechts één origineel van bestaat (in sommige gevallen twee), dat ten allen tijde in de archiefinstelling moet blijven.

Bekijken we nu deze twee scenario's naargelang de wijze van archiveren. Het toegankelijk gemaakte informatiepakket is zoals gezegd slechts een bewerkte kopie van het gearchiveerde informatiepakket, maar dat tevens de gevraagde originelen bevat.

- Uitlening in een traditionele archiefcontext wil zeggen dat het enige origineel aan de klant ter beschikking wordt gesteld, waarna het terug moet keren naar zijn oorspronkelijke plaats in het archief. In een digitale omgeving is er echter niet noodzakelijk sprake van slechts één origineel. Het voordeel van digitale informatie is dat men een oneindig aantal originelen kan creëren.⁵³ Het toegankelijk gemaakte informatiepakket is slechts een bewerkte kopie van het gearchiveerde informatiepakket en de inhoud is tevens een origineel. In een digitaal archief kan en mag er geen sprake van zijn dat de archivaris ooit het enige origineel uit handen geeft.

Uitlening in de strikte betekenis van het woord bestaat dus eigenlijk niet meer in een digitale omgeving. De archiefinstelling blijft ten allen tijde over de originele informatie beschikken. De medewerkers van archiefvormende organisaties kunnen dan op verschillende wijzen in het bezit worden gesteld van de gevraagde informatie.⁵⁴

- Wanneer de archiefstukken op offline toegankelijke dragers bewaard worden, kan de archiefinstelling aparte digitale dragers voorzien die speciaal voor de medewerkers ter beschikking worden gehouden. Na de uitleenperiode moeten ze terugkeren naar de archiefinstelling. Voor stukken die niet frequent geraadpleegd worden, kan de archiefinstelling beslissen om de kopie pas te maken naar aanleiding van een concrete vraag.

zijn dus in principe onvervreemdbaar. Hun archiefbestand kan enkel aan een archiefinstelling worden overgedragen via bewaargeving.

⁵² COPPENS, H., *o.c.*, 350.

⁵³ VAN DEN EYNDE, S., *Digitale archivering: een juridische stand van zaken. Deel 1*, 58 en 65.

⁵⁴ In veel gevallen zal de archiefvormende organisatie zelf een exemplaar behouden van wat er aan het archief werd overgedragen. Toch kan een beroep op de archiefinstelling nodig zijn omdat de leesbaarheid op lange termijn van de gearchiveerde stukken gegarandeerd is.

- Is de gevraagde informatie gearchiveerd in een netwerkomgeving, dan wordt het begrip 'uitlening' nog problematischer. Niet alleen blijft de archiefinstelling gedurende de uitleenperiode in het bezit van de informatie, maar de medewerker beschikt meteen ook definitief over een eigen exemplaar wanneer de gevraagde informatie over het netwerk wordt gezonden via e-mail. Dit eigen exemplaar blijft aanwezig bij de medewerker, ook al zendt deze de gevraagde informatie na een bepaalde periode terug naar de archiefinstelling. Dit feit is op zich geen probleem omdat de archiefvormende organisatie meestal toch de eigenaar is gebleven van de archiefstukken, zolang ze maar tegelijk ook op een afdoende wijze gearchiveerd blijven door de archiefinstelling.
- Worden de stukken geraadpleegd door derden, dan geldt de regel dat de derde niet in het bezit mag gesteld worden van de stukken, niet alleen omdat het origineel in de archiefinstelling moet blijven in de best mogelijke archiefomstandigheden (dit probleem is opgelost in de digitale wereld door de mogelijkheid om meerdere originelen te creëren), maar ook omdat de derde vaak geen enkel recht heeft om de stukken bij zich te hebben. De raadpleging van het bevolkingsregister bijvoorbeeld, is onderworpen aan zeer strikte modaliteiten.⁵⁵ De terbeschikkingstelling van het gehele bevolkingsregister is uitgesloten, aangezien de wet verbiedt dat er personenlijsten uit de registers aan derden worden verstrekt.⁵⁶
- Wanneer de archiefstukken op offline toegankelijke dragers bewaard worden, dan kan de raadpleging van de kopieën hiervan enkel ter plaatse gebeuren via de in de leeszaal voorziene apparatuur. Het voordeel van de digitale wereld is dat de raadpleging zelf niet noodzakelijk meer onder toezicht van een archiefmedewerker dient te gebeuren. Er wordt immers slechts een kopie ter beschikking gesteld, die gewoon kan vervangen worden als er fraude wordt vastgesteld. De inspanning die vanwege het archief moet gebeuren om te garanderen dat de originele stukken ook nadien nog kunnen ter beschikking worden gesteld, verlegt zich dus van de periode tijdens de raadpleging, naar een moment ergens na de raadpleging (controle van de digitale handtekening), wat een aanzienlijke tijdswinst kan opleveren. Het is wel zo dat ieder geraadpleegd stuk afzonderlijk moet gecontroleerd worden.
- Hebben we te maken met een online raadpleging van de netwerkomgeving waarin de archiefstukken zich bevinden, dan krijgt de klant (zoals de medewerker van de archiefvormende organisatie: zie hierboven) definitief een eigen exemplaar ter beschikking van de gevraagde informatie, wanneer deze zou worden doorgezonden via e-mail. Deze manier van ter beschikking stellen van de gevraagde informatie moet dus zoveel mogelijk vermeden worden. Ten aanzien van derden moet er eerder gedacht worden aan een raadpleging online via de website van de archiefinstelling, waarbij de informatie op geen enkele wijze verplaatst wordt of kan gekopieerd worden. Maar dit is natuurlijk helemaal niet evident voor stukken die een individuele behandeling vragen, bijvoorbeeld omdat de openbaarheid naar iedereen toe niet

⁵⁵ Zie K.B. 16 juli 1992 betreffende het verkrijgen van informatie uit de bevolkingsregisters en uit het vreemdelingenregister (B.S. 15 augustus 1992).

⁵⁶ Art. 6 K.B. 16 juli 1992.

vaststaat.⁵⁷ Hier is e-mail het geëigende middel om te beantwoorden aan een concreet verzoek tot raadpleging.

Taak 5: Mogelijk maken van validering van de raadplegingsoperatie

In een netwerkgeving, waarbij er geen contact is tussen de klant en de archivaris, is het van belang dat de raadplegingsoperatie gevalideerd wordt, zowel door de archivaris als door de klant.

- Vooreerst moet de archivaris (of het orgaan dat beslist over de openbaarmaking) kunnen nagaan **wie** de persoon is die **zich aanbiedt**. In een aantal gevallen bepaalt de wet immers dat enkel bepaalde personen toegang krijgen tot bepaalde stukken. Nemen we het voorbeeld van het kiezersregister van 8 oktober 2000 van de stad Antwerpen, dat gearchiveerd werd in een stadsarchief.⁵⁸ Het gaat om een gearchiveerd gemeentelijk bestuursdocument, waarop de wet van 12 november 1997 betreffende de openbaarheid van bestuur in de provincies en de gemeenten van toepassing is. Deze wet bepaalt dat de inzage van een bestuursdocument op schriftelijke aanvraag dient te gebeuren. Via de website van het stadsarchief Antwerpen kan men het formulier ‘Aanvraag voor inzage van bestuursdocumenten’ downloaden, afprinten + ondertekenen en versturen naar het college of de betrokken dienst.⁵⁹

Het besluit van 25 februari 1999 van het college van burgemeester en schepenen bepaalt dat het bevolkingsregister, en afgeleide documenten zoals het kiezersregister, pas openbaar worden na honderd jaar, ingevolge de strikte regeling inzake de toegang tot het bevolkingsregister, die is ingegeven door privacyoverwegingen. Dit betekent niet dat het kiezersregister gedurende honderd jaar nooit geraadpleegd mag worden. Overeenkomstig het advies nr. 11/97 van de Commissie voor de bescherming van de persoonlijke levenssfeer betreffende de raadpleging van de bevolkingsregisters door genealogen, mag er ook voordien toegang worden verleend om wetenschappelijk onderzoek te verrichten.⁶⁰

Voor de raadpleging van een aantal documenten zal het dus van belang zijn dat de archivaris zeker weet wie zich via het Internet aanbiedt. Iemand met commerciële belangen kan zich bijv. voordoen als genealoog om zo toch een personenlijst te kunnen bemachtigen met het oog op direct marketing. PKI is een middel om identificatie in een netwerkgeving mogelijk te maken.

- Vervolgens moet de klant die een archiefstuk van op afstand raadpleegt, er zeker van kunnen zijn dat hij te maken heeft met het authentieke stuk. Een stuk is authentiek

⁵⁷ BOUDREZ, F. en VAN DEN EYNDE, S., *De digitale archivering van het kiezersregister*, 20: *Het verlenen van toegang [tot het kiezersregister] blijft echter steeds een afweging van de bevoegde overheid tot wie de archivaris zich in dat geval moet wenden.*

⁵⁸ En nemen we aan dat dit kiezersregister op het netwerk gearchiveerd werd, wat op dit moment echter nog niet het geval is.

⁵⁹ Aan de hand van PKI kan de aanvrager het aanvraagformulier elektronisch ondertekenen.

⁶⁰ Zie BOUDREZ, F. en VAN DEN EYNDE, S., *De digitale archivering van het kiezersregister*, Antwerpen – Leuven, Stadsarchief Antwerpen – ICRI, 2001, 18 e.v.

wanneer vaststaat dat het is wat het beweert te zijn, dat het 'echt, waarachtig' is. Een elektronische handtekening is één van de middelen aan de hand waarvan men zich in de digitale wereld kan vergewissen van de authenticiteit van de aangeboden informatie; Bovendien moet de integriteit van het archiefstuk kunnen nagegaan worden. Hier biedt de techniek van de digitale handtekening als verzegelingstechniek een oplossing. Deze twee middelen moeten de klant op een veilige manier kunnen bereiken. Als de publieke sleutel niet past, betekent dit niet noodzakelijk dat het stuk niet authentiek of niet integer is. Het is ook mogelijk dat er fraude werd gepleegd tijdens de transfer. Daarom moet de informatie tijdens de transfer ontoegankelijk gemaakt worden aan de hand van PKI.

4. Beleid

De laatste fase doorkruist alle vorige fasen, in die zin dat er ten aanzien van elk van de fasen door de archiefinstelling een duidelijk digitaal archiefbeleid moet gevoerd worden, afhankelijk van zijn concrete noden. In plaats van een louter uitvoerende taak zal de archivaris meer en meer een beleidstaak moeten op zich nemen. Het gaat hier om het uittekenen van procedures, *policies*. Dit houdt in dat er keuzes zullen moeten gemaakt worden, waarbij de ene keuze onmiskenbaar een andere keuze beïnvloedt.

Aansluitend bij de eerste fase, kan er gezegd worden dat het digitale archiefbeleid binnen de archiefinstelling niet alleen door de archivaris moet uitgetekend worden, maar dit moet gebeuren in samenspraak met de archiefvormer, en meer bepaald met de informatieverantwoordelijken binnen de organisatie. Het archiefbeleid moet er immers toe bijdragen dat er optimaal kan voorzien worden in de informatiebehoefte van de bedrijfsprocessen, en, misschien nog belangrijker, dat de bedrijfsprocessen zodanig worden georganiseerd dat de archivering als het ware reeds kan beginnen bij de aanmaak van de informatie. Een goede wisselwerking tussen deze twee functies binnen de organisatie is van groot belang. Zo zal er moeten uitgemaakt worden hoe het overgedragen en het te archiveren informatiepakket het best op elkaar kunnen afgestemd worden, en verder welke informatie er van de archiefvormer verwacht wordt dat hij mee overdraagt. Bovendien moet ook duidelijk afgesproken worden in welke mate de archivaris technische hulp van de archiefvormer kan verwachten bij het archiefbeheer.

De archiefinstelling zal ook een beleid moeten uitstippelen ten aanzien van de wijze van opslag, die mede zal beïnvloed worden door de manier waarop de archiefstukken overgedragen worden en de manier waarop de archiefinstelling ze ter beschikking wil stellen. Dit laatste is dan weer afhankelijk van de doelgroep en de mate waarin de leden ervan toegang hebben tot de nieuwe telecommunicatiemiddelen, zoals Internet en e-mail. De evolutie van de doelgroep en de situatie op dit vlak moet de archivaris nauwgezet opvolgen, om zo een idee te krijgen over het tijdstip waarop een volledige omschakeling naar een netwerkgeving verantwoord wordt. Verder moet er ook gekeken worden naar de evoluties op technisch vlak en moeten de strategieën bepaald worden om deze evoluties het hoofd te bieden.

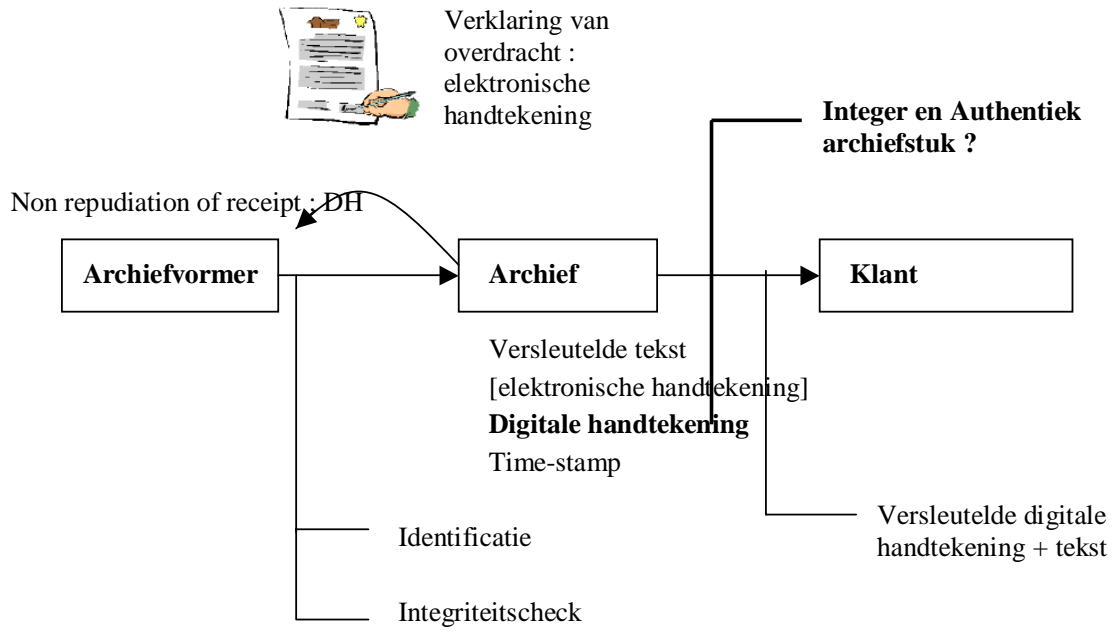
V. Besluit: De rol van PKI bij digitale archieven

PKI kan verschillende functies vervullen. Als besluit sommen we ze op en situeren we waar in het digitale archiveringsproces deze functies hun nut zullen bewijzen.

1. **Integriteit:** traditioneel wordt er onder deze functie verstaan dat aan de hand van PKI kan nagegaan worden of digitale informatie werd gewijzigd tijdens de transfer. PKI kan echter ook gebruikt worden om te integriteit te controleren van digitale informatie, die gedurende een bepaalde periode werd opgeslagen.
 - Validatie van de overdracht: bereiken de stukken de archiefinstelling zoals ze aanwezig waren bij de archiefvormer?
 - Netwerk: op alle overgedragen informatie wordt er een digitale handtekening berekend en deze wordt meegestuurd.
 - Drager: er moet een integriteitscheck gebeuren vóór de overdracht wanneer de informatie vóór de overdracht naar een andere drager wordt gekopieerd. Hiervoor kan hashing volstaan. PKI is niet vereist.
 - Toevoegen van de integriteitsgaranderende informatie: berekenen en mee opslaan van de digitale handtekening die de archivaris berekent op het moment van archivering (zowel voor het gearchiveerde exemplaar als voor de veiligheidskopie). Bij latere raadpleging van het stuk blijkt uit de digitale handtekening of de opgeslagen digitale informatie al dan niet gewijzigd werd tijdens de opslag.
2. **Authenticatie:** deze functie zorgt ervoor dat de origine van digitale informatie met zekerheid kan achterhaald worden. Maar het is opnieuw niet enkel de origine van elektronische communicatie die met PKI kan komen vast te staan. Ook de bron van een archiefstuk dat reeds jaren geleden werd opgeslagen, kan vastgesteld worden.
 - Validatie van de overdracht: wie draagt de stukken over? Dit heeft een invloed op het oordeel van de archivaris op de authenticiteit van de overgedragen stukken.
 - Netwerk: De digitale handtekening die voor integriteitsdoeleinden bij de overdracht werd meegestuurd, kan eveneens dienen om de identiteit van de overdrager te achterhalen.
 - Locale server: de server die de archivaris betreedt om de stukken te archiveren, moet met behulp van PKI geïdentificeerd worden.
 - Ondertekening van de elektronische verklaring van overdracht
 - Toevoegen van de authenticiteitsgaranderende informatie: de digitale handtekening die voor integriteitsdoeleinden bij de archivering werd berekend en opgeslagen, kan eveneens dienen om de origine van het stuk (als archiefstuk) naar aanleiding van de raadpleging op afstand vast te stellen. Wanneer de klant bij de raadpleging op afstand er zeker van kan zijn dat het stuk destijds door een echte archivaris verzegeld werd (en niet door eender

wie) en sindsdien niet meer gewijzigd is, weet hij meteen ook zeker dat het stuk een authentiek archiefstuk is, en dus niet een stuk dat niet het archief als bron heeft.

- Validering van de raadplegingsoperatie: de archivaris moet de identiteit kunnen nagaan van de persoon die zich aanbiedt op afstand.
- 3. Toegangscontrole:** PKI bewijst ook zijn nut door de toegang tot digitale informatie, een elektronisch bericht of andere digitale informatie, voor te behouden aan bepaalde personen.
- Onmiddellijk na de archivering moet de archivaris de gearchiveerde stukken in het archiefsysteem ontoegankelijk maken: versleutelen met de publieke sleutel van de archivaris en in die toestand opslaan in het archief.
 - Validering van de raadplegingsoperatie: De digitale handtekening die omwille van de authenticiteit werd toegevoegd, evenals het gevraagde stuk zelf, moet de klant op veilige wijze bereiken. Als de publieke sleutel niet past, betekent dit niet noodzakelijk dat het stuk niet authentiek is. Het is ook mogelijk dat er fraude werd gepleegd tijdens de transfer. Daarom moet de informatie tijdens de transfer ontoegankelijk gemaakt worden aan de hand van PKI.
- 4. Non Repudiation:** niet-ontkenning betekent dat de maker van digitale informatie bij gebruik van PKI niet kan ontkennen dat hij deze informatie heeft aangemaakt, of tenminste dat deze informatie van hem is uitgegaan. Voor archivering is enkel de Non Repudiation of Receipt functie van belang. Dit wil zeggen dat de geadresseerde van digitale informatie niet kan ontkennen dat hij deze digitale informatie heeft ontvangen.
- Non Repudiation of Receipt van de archiefstukken door de archivaris: de archivaris moet de digitale handtekening die hij berekent voor de ontvangen archiefstukken samen met deze archiefstukken naar de overdrager sturen.
 - Niet-ontkenning van de datum van de overdracht: berekenen van een time-stamp voor de door de archivaris versleutelde archiefstukken; Niet ontkenning van de datum van overdracht is enkel mogelijk aan de hand van PKI als de archivering gebeurt op de lokale server van de archiefvormer.



BIBLIOGRAFIE

Reference Model for an Open archival Information system (OAIS), Draft Recommendation for space data system standards, Red Book May 1999, Consultative Committee for Space Data Systems, CCSDS 650.0-R-1

Beschikbaar op <http://www.ccsds.org/documents/pdf/CCSDS-650.0-R-1.pdf>

A blueprint for Representation Information in the OAIS model, HOLDSWORTH, D., SERGEANT, D., The Cedars Project, University of Leeds

Beschikbaar op: <http://gps0.leeds.ac.uk/~ecldh/cedars/nasa2000/nasa2000.html>

ISO "Reference Model for an Open Archival Information System (OAIS)", Tutorial Slide-Presentation IEEE/GSFC Mass Storage Symposium, REICH, L., SAWYER, D., March 15, 1999.

Beschikbaar op: <http://www.loc.gov/rr/mopic/avprot/oais/OAIS/sld001.htm>

LAVOIE, B., 'Meeting the challenges of digital preservation: the OAIS reference model', OCLC Newsletter, No.243, January/February 2000, 26-30.

Beschikbaar op: <http://www2.oclc.org/oclc/pdf/news243.pdf>

Nedlib Contribution to the review of OAIS. Applying the OAIS Reference Model to the Deposit System for Electronic Publications (DSEP)

Beschikbaar op: <http://www.kb.nl/coop/nedlib/results/OAISreviewbyNEDLIB.html>

LUPOVICI, C., MASANES, J., *Metadata for long term preservation*, Nedlib, July 2000

Beschikbaar op: <http://www.kb.nl/coop/nedlib/results/preservationmetadata.pdf>

DAY, M., *Metadata for digital preservation: an update*, december 1999, Ariadne Issue 22

Beschikbaar op <http://www.ariadne.ac.uk/issue22/metadata/intro.html>