Digitale handtekeningen en archiefdocumenten

Filip Boudrez
Expertisecentrum DAVID vzw
Antwerpen, 2005

0. INHOUD

1. INLEIDING

Digitale documenten hebben het voordeel dat ze herbruikbaar zijn. Ze kunnen snel aangepast worden of op basis van een bestaand document kan snel een nieuw document worden samengesteld. Dit digitaal voordeel is meteen ook een kwetsbaar punt want aanpassingen of wijzigingen zijn niet altijd waarneembaar. Hierdoor wordt de betrouwbaarheid van digitale documenten in vraag gesteld.

Het zoeken naar methoden om de betrouwbaarheid van digitale documenten te waarborgen is het onderzoeksonderwerp van verschillende vakdomeinen. Momenteel is één van de meest gesuggereerde oplossingen het digitaal ondertekenen van digitale documenten. Meer bepaald het gebruik van asymmetrische cryptografie en de digitale handtekening wordt als authenticiteits- en integriteitsbewijs voor digitale documenten naar voor geschoven. Deze techniek zou ook bruikbaar zijn om de betrouwbaarheid van digitale archiefdocumenten te verzekeren[1].

Het gebruik van de digitale handtekening en vooral de archivering van digitaal ondertekende documenten houdt de internationale archiefwereld al een tijd bezig. Archivarissen worden immers niet alleen geconfronteerd met de archivering van digitaal ondertekende documenten, er gingen ook stemmen op om de technologie van de geavanceerde digitale handtekening te gebruiken om de authenticiteit en integriteit van alle digitale archiefdocumenten te verzekeren. Dit laatste zou betekenen dat de archivaris of de archiefvormer alle digitale archiefdocumenten in het archief zou moeten tekenen. De integriteit van de digitale archiefdocumenten zou kunnen gecontroleerd worden door verificatie van de handtekening van de archivaris of de archiefvormer. De Victorian Electronic Records Strategy (VERS) archiveringsstrategie is hier wellicht het bekendste voorbeeld van[2].

Algauw werd echter duidelijk dat het archiveren van digitaal ondertekende documenten een aantal vragen en moeilijkheden doet rijzen. Deze bijdrage wil een overzicht bieden van de

---

1 D. Pinkas, *Long term preservation of signed documents,* op: *e-Archiving for posterity*, Leuven, 26 juni 2003.

2 http://vers3.imagineering.net.au

archiveringskwesties die digitaal ondertekende documenten met zich meebrengen[3]. Eerst wordt bij wijze van introductie de geavanceerde digitale handtekening kort voorgesteld. In het tweede deel worden een aantal problemen besproken die zich stellen bij het gebruik van de digitale handtekening als authenticiteits- en integriteitsbewijs voor digitale documenten in het algemeen. Hierbij wordt in het bijzonder ook onderzocht of het zin heeft dat de archivaris alle digitale archiefdocumenten in zijn/haar beheer digitaal zou ondertekenen. De problematiek inzake de (middel)lange termijnarchivering van digitaal ondertekende documenten komt in het derde deel aan bod. Na een overzicht van de knelpunten voor lange termijnvalidatie (4.1) worden een aantal mogelijke oplossingen besproken (4.2).

In deze bijdrage worden de begrippen authenticiteit en integriteit gehanteerd zoals ze door het InterPARES-project werden gedefinieerd[4]. Authentiek en integer zijn de eerste kenmerken van een betrouwbaar archiefdocument. Een archiefdocument is authentiek als het is, wat het beweerd te zijn en als het gecreëerd of verzonden is door de persoon die beweert het verzonden te hebben. Authentieke archiefdocumenten zijn vrij van ongeoorloofde aanpassingen of manipulaties. Een integer document is volledig en onveranderd. Dit betekent niet dat archiefdocumenten geen wijzigingen mogen ondergaan, maar wel dat archiefdocumenten beschermd worden tegen onrechtmatige veranderingen en dat heel duidelijk wordt gedefinieerd wie welke wijzigingen of annotaties na de vastlegging mag aanbrengen.

Integriteit betekent dus niet dat archiefdocumenten identiek hetzelfde hoeven te zijn als bij creatie of ontvangst. Een archiefdocument is integer wanneer zijn functie en finaliteit niet werd gewijzigd. De essentiële eigenschappen of componenten van een archiefdocument mogen niet gewijzigd worden. De incidentele eigenschappen of componenten daarentegen mogen wel gewijzigd worden of mogen zelfs verloren gaan. Deze visie gaat uit van de premisse dat originele digitale archiefdocumenten gedoemd zijn om te verdwijnen ten gevolge van de technologische veroudering en dat wijzigingen en/of verlies bijgevolg onvermijdelijk zijn. Wat we wel kunnen archiveren zijn de mogelijkheid tot reconstructie en archiefdocumenten “as close to the original as possible”.

2. DE GEAVANCEERDE DIGITALE HANDTEKENING

De technologie van de geavanceerde digitale handtekening maakt gebruik van een asymmetrisch sleutelpaar: de private sleutel en de publieke sleutel. De private sleutel dient om een digitale handtekening te genereren en/of om geëncrypteerde informatie te decrypteren. De private sleutel dient geheim te blijven, terwijl de publieke sleutel wordt gepubliceerd. De publieke sleutel wordt gebruikt voor het controleren van een digitale handtekening en/of om confidentiële informatie geëncrypteerd te versturen. De private en publieke sleutel zijn niet van elkaar af te leiden. Dit sleutelpaar wordt in de regel verstrekt door een certificatie autoriteit, die de identiteit van de aanvrager verifieert en registreert[5], maar kan ook door de gebruiker zelf worden aangemaakt[6].

Het ondertekenen van een digitaal document met een geavanceerde digitale handtekening verloopt in twee stappen. Het computerbestand dat het document bevat, wordt eerst gehashed. Dit is het

3 Met dank aan Hannelore Dekeyser en Inge Schoups voor de suggesties en opmerkingen.

4 INTERPARES AUTHENTICITY TASK FORCE, *Requirements for assessing and maintaining the authenticity of electronic records*, in: InterPARES, *The long-term preservation of authentic electronic records: findings of the InterPARES project*, 2002, p.2-3.

5 De werking van PKI en digitale handtekeningen wordt uitgebreid beschreven in: P. VAN EECKE,Naar een juridische status voor de elektronische handtekening : een rol voor de handtekening in de informatiemaatschappij?,diss. doct. rechtsgeleerdheid, Leuven, 2004, p. 328 e.v.; S. VAN DEN EYNDE en J. DUMORTIER, *De rol van de digitale handtekening bij de archivering van elektronische documenten*, Leuven,[zonder datum] (http://www.antwerpen.be/david/website/teksten/DAVIDbijdragen/Digitale_handtekening.pdf); S. HUYDECOPER en S. VAN DER HOF, *De handtekening: van geschreven naar elektronisch*, in: *Archiefbeheer in de praktijk*, 42, 1565; http://www.digitalehandtekening.be.

6 Bijv. Pretty Good Privacy, OpenPGP, GnuPG

herleiden van een computerbestand tot een unieke code op basis van een algoritme. Dit levert een hashwaarde op, die vervolgens in de tweede stap wordt geëncrypteerd met de private sleutel van de verzender. Het resultaat van die bewerking is de digitale handtekening die als een afzonderlijk computerbestand wordt opgeslagen. De verzender stuurt het digitale document samen met de digitale handtekening naar de ontvanger. Het digitale document zelf kan ook met de publieke sleutel van de ontvanger versleuteld worden, maar dit is niet noodzakelijk. De ontvanger valideert de geldigheid van het document door met de publieke sleutel van de verzender de digitale handtekening te decrypteren. Na decryptie komt de hashwaarde van het digitale document tevoorschijn zodat de ontvanger na het herberekenen van de hashwaarde van het document de mee gestuurde en de pas berekende hashwaarde kan vergelijken.

Een geavanceerde digitale handtekening heeft in theorie drie functies:

- authenticatie: de digitale handtekening werd met de private sleutel van de afzender gecreëerd
- integriteit: bewijs dat het document na ondertekening niet meer werd gewijzigd
- 'non-repudiation': de ondertekenaar kan niet ontkennen het document te hebben verzonden of ondertekend.

Op zichzelf genomen zegt een digitale handtekening niets over de ware identiteit van de afzender, aangezien het in wezen enkel om een unieke code gaat. Voor de verificatie van een digitale handtekening moet de link tussen de afzender en zijn publieke sleutel blijken uit een een digitaal certificaat. Net als het sleutelpaar, kan het digitaal certificaat door de afzender zelf gemaakt worden of door een (geautoriseerde) tussenpersoon. Een digitaal certificaat van een certificatie autoriteit levert een hogere mate van betrouwbaarheid, want digitale certificaten zijn maar zo betrouwbaar als de persoon of de instantie die het aflevert. Wanneer de geavanceerde digitale handtekening gerealiseerd wordt op basis van een gekwalificeerd certificaat[7] spreekt de wetgever van een gekwalificeerde digitale handtekening. Certificatie autoriteiten leveren bij elk sleutelpaar een digitaal certificaat af dat de publieke sleutel bevat en informatie over de identiteit van sleuteleigenaar, de operationele periode, het serienummur van het certificaat en de naam van de certificatie autoriteit. De digitale certificaten hebben een beperkte geldigheidstermijn, maar kunnen ook voor het verstrijken van deze termijn ingetrokken worden. De eigenaar van de sleutel kan de intrekking van het certificaat vragen indien de private sleutel verloren gaat of gestolen wordt. Om de betrouwbaarheid van de certificaten aan te tonen worden de digitale certifcaten zelf ondertekend met de private sleutel van de certificatie autoriteit. De certificaten van de certificatie autoriteit worden geverifieerd met de publieke sleutel van de certificatie autoriteit. Hiervoor is een root certificaat dat een certificatie autoriteit met een sleutelpaar verbindt, vereist. Voor de verificatie van een digitale handtekening is dus een hele validatieketting of 'validation chain' nodig. Enkel het document en de digitale handtekening archiveren volstaat niet als men een digitaal document met een digitale handtekening in de toekomst valideren.

3. DIGITALE HANDTEKENINGEN ALS AUTHENTICITEITS- EN INTEGRITEITSBEWIJS

Digitale handtekeningen worden algemeen voorgesteld als authenticiteits- en integriteitsbewijs voor digitale bestanden. Maar digitale archiefdocumenten zijn meer dan louter digitale bestanden of documenten[8]. Het is dan ook de vraag of digitale handtekeningen de authenticiteit en integriteit van

[7] De wetgever formuleerde een aantal vereisten voor een gekwalificeerd certificaat, waar onder de uitreiking door een erkende certificatiedienstverlener die de identiteit van de ondertekenaar garandeert.

[8] Voor het onderscheid tussen computerbestand, digitaal document en digitaal archiefdocument, zie: F. BOUDREZ, *A. Inleiding. 2. Digitaal archiefdocument*, in: F. BOUDREZ en H. DEKEYSER, *Digitaal archiefbeheer in de praktijk. Een handboek,* Antwerpen-Leuven, 2004.

digitale archiefdocumenten kunnen aantonen en indien ja, of ze volstaan als enig authenticiteits- en integriteitsbewijs.

3.1 Digitale handtekeningen zijn zegels

De Belgische wetgever geeft voor een aantal types documenten een digitale handtekening dezelfde juridische waarde als een handgeschreven handtekening. In archiefliteratuur wordt toch op een praktisch verschil in het persoonsgebonden karakter van beide handtekeningen gewezen. In het geval van een digitale handtekening kan iedereen die in het bezit is van de private sleutel een document ondertekenen. Een digitale handtekening wordt dan ook veel vergeleken met een digitaal zegel[9]. De digitale handtekening toont aan dat iemand die in het bezit was van de private sleutel het document ondertekende. De digitale handtekening bewijst niet automatisch dat persoon X het document ondertekende, maar wel dat het document werd getekend door iemand die toegang heeft tot de private sleutel van persoon X[10].

De garantie dat het document effectief was ondertekend door de persoon wiens private sleutel werd gebruikt, is afhankelijk van de beveiliging van de private sleutel. In het PKI-model zijn eindgebruikers verantwoordelijk voor het beheren van hun private sleutels. Aangezien private sleutels digitaal worden bewaard en de courante computerbesturingssystemen niet altijd even veilig zijn, is dit geen evidentie. Net zoals zegels zijn digitale handtekeningen afzonderlijke objecten die gestolen of gekopieerd kunnen worden[11]. De waarde van de digitale ondertekening is bijgevolg afhankelijk van de procedure waarin de digitale handtekening wordt gebruikt, de associatie private sleutel en eigenaar, en van de veilige bewaring van de private sleutel[12].

De wetgever is zich terdege bewust van dit probleem. In de wetgeving is dan ook een aansprakelijkheidsregeling opgenomen in geval van verlies of diefstal. De eigenaar van de sleutel is verantwoordelijk voor elk gebruik van zijn private sleutel tot op het moment dat hij het bijhorend digitaal certificaat laat intrekken.

3.2 De authenticatie is niet afhankelijk van de documentidentiteit

Het valideren van digitale documenten door middel van een digitale handtekening komt overeen met authenticatie of het aantonen van de authenticiteit. Een digitale handtekening controleert de geldigheid

---

9 INTERPARES, *The InterPARES Glossary*, 2001, p. 3; J. CURRALL, *Digital Signatures: not a solution, but simply a link in the process chain*, Glasgow, 2002, p.3 (http://eprints.lib.gla.ac.uk/documents/disk0/00/00/00/39); VERS, *Using digital signatures for authentication*, *VERS Version 1, Specification 3,* 1999.

De vergelijking van een digitale handtekening met een zegel loopt op een aantal punten mank. Zo is een zegel van iemand voor elk document hetzelfde, terwijl een digitale handtekening afhankelijk is van de inhoud (bitstream) van een document. Verschillende documenten kunnen hetzelfde zegel hebben, maar niet dezelfde digitale handtekening. Een zegel is ook rechtstreeks geassocieerd met een rechtspersoon. Bij een digitale handtekening is een rechtspersoon gelinkt aan een private sleutel. Tenslotte is een zegel gebaseerd op visuele verificatie en een digitale handtekening op onzichtbare verificatie. De aanwezigheid van een digitale handtekening kan wel visueel worden waargenomen, maar de eigenlijke verificatie is niet zichtbaar.

10 H. MACNEIL, *Trusting records. Legal, historical and diplomatic perspectives*, Dordrecht, 2000, p. 108.

11 S. HUYDECOPER en S. VAN DER HOF, *De handtekening: van geschreven naar elektronisch*, in: *Archiefbeheer in de praktijk*, 42, 1565.

12 H. MACNEIL, *Trusting records. Legal, historical, and Diplomatic perspectives*, Dordrecht, 2000; J. CURRALL, *Digital Signatures: not a solution, but simply a link in the process chain*, Glasgow, 2002, p.2 (http://eprints.lib.gla.ac.uk/documents/disk0/00/00/00/39).

Veel voorkomende oplossingen voor de opslag van private sleutels zijn smartcards, USBKeys of netwerkomgevingen. In dit laatste geval is de beveiliging meestal afhankelijk van de gebruikelijke gebruikersnaam/paswoord-controle.

van een document op basis van de bitstreams (fysieke vorm) en houdt hierbij geen enkele rekening met de identiteit van het document (intellectuele vorm).

De authenticiteit van een document is gerelateerd aan zijn integriteit en identiteit. In functie van de identiteit van een digitaal document wordt zijn authenticiteit onderzocht. Met andere woorden, de authenticiteit van een digitaal document hangt af van hoe een document wordt voorgesteld of geïdentificeerd. Een vervalst document dat als zodanig wordt gepresenteerd, is authentiek terwijl een vervalst document dat als “echt” wordt voorgesteld niet authentiek is.

De authenticiteit van een document kan pas aangetoond worden als de identiteit van het document is vastgelegd. In de identiteit worden de unieke kenmerken en het onderscheidend karakter van een digitaal document geregistreerd zodat het verschil met andere archiefdocumenten duidelijk wordt. Het bepalen van de mate van authenticiteit kan niet zonder dat de essentiële kenmerken van een archiefdocument op een betekenisvolle wijze zijn geregistreerd en geïdentificeerd. De identiteit van een document kan niet met een digitale handtekening worden vastgelegd. Binnen het PKI-model wordt het vastleggen van de identiteit ook op geen enkele wijze afgedwongen.

De identiteit van een document wordt doorgaans geregistreerd in de metadata van het document. Bestandsnamen, documentprofielen, attributen (auteursnaam, datum, plaats), classificatiecodes, situering binnen werkprocessen, enz. zijn de geijkte methoden om digitale documenten te identificeren. Ook de identiteit van digitale documenten dient tegen ongeoorloofde manipulaties beschermd te worden. Tenzij de identificerende metadata in het document zelf ingekapseld worden, controleert de digitale handtekening de identificatie van het document niet.

Voor de authenticatie van digitale documenten houden digitale handtekeningen op geen enkele wijze rekening met de identiteit van het archiefdocument. De authenticatie afhankelijk maken van de bitstreams waaruit computerbestanden bestaan, gaat ook voorbij aan de vaststelling dat hetzelfde archiefdocument verschillende bitrepresentaties kan hebben. In het concept van een digitale handtekening wordt een digitaal archiefdocument louter als een digitaal object beschouwd, terwijl hetzelfde archiefdocument als verschillende digitale objecten kan worden vastgelegd. Een e-mail met archiefwaarde kan voor archivering in diverse bestandsformaten worden opgeslagen (platte tekst, XML, PDF, TIFF, HTML). Al naargelang het bestandsformaat waarin een digitaal document wordt opgeslagen, verschillen de onderliggende bitstreams van elkaar. Een digitaal archiefdocument kan niet zomaar vereenzelvigd worden met één bitstream of één bitrepresentatie.

Het falen van de authenticatie hoeft niet noodzakelijk te betekenen dat het voorliggende document niet meer betrouwbaar is. De authenticatie met een digitale handtekening zal al mislukken van zodra 1 bit van het computerbestand gewijzigd is. Dit houdt niet automatisch in dat het document niet meer authentiek en/of integer is. De fysieke integriteit (de bits) kan gecompromiteerd zijn, maar de inhoud kan nog steeds intact zijn. Mogelijke wijzigingen in de bits en bytes die geen authenticiteitsverlies met zich meebrengen zijn bijvoorbeeld de inkapseling van metadata of fouten in de bitopslag. Om een aantal metadata onlosmakelijk met het document te verbinden, worden ze soms opgenomen in hetzelfde computerbestand als het document. Het 'omvallen van bits' gebeurt meer dan we ons bewust zijn. RAID-opslagsystemen zijn hier speciaal op voorzien en in bepaalde formaten wordt volop foutencontrole en foutenverbetering toegepast.

3.3 Digitale handtekeningen bewijzen de integriteit van bitstreams

Een geavanceerde digitale handtekening is een versleutelde hashwaarde van een computerbestand. Met de validatiefunctie van een digitale handtekening kan aangetoond worden dat de bits van een computerbestand na transmissie nog dezelfde zijn als bij ondertekening. Elke wijziging na ondertekening zal in een ongeldig document resulteren. De validatiefunctie geeft aan of een document tijdens zijn transmissie werd gewijzigd en/of het document na ondertekening nog werd gewijzigd.

Digitale handtekeningen beschermen archiefdocumenten niet tegen onrechtmatige wijzigingen of manipulaties.

De validatiefunctie van digitale handtekeningen is volledig gebaseerd op de bitstreams waaruit een computerbestand bestaat. De bitstreams kunnen wijzigen terwijl de inhoud of het archiefdocument identiek gebleven is. Met een digitale handtekening worden de bits van een computerbestand en niet de inhoud van een archiefdocument getekend. Digitale archiefdocumenten kunnen niet zomaar met één bitrepresentatie geïdentificeerd worden (één-op-één relatie). In de plaats daarvan is er een één-op-veel relatie tussen digitale archiefdocumenten en bitrepresentaties (zie 3.2).

Door een document digitaal te ondertekenen worden geen manipulaties voorkomen. De digitale handtekening is enkel een controle, geen bescherming of waarborg. In geval van een ongeldige validatie is het niet mogelijk om met de digitale handtekening te achterhalen welke wijzigingen door wie in het document werden aangebracht na ondertekening of wat de oorspronkelijke inhoud was. Nochtans is dit een belangrijke voorwaarde voor een integriteitswaarborg voor digitale archiefdocumenten. Immers, archiefdocumenten verliezen hun integriteit niet wanneer geautoriseerde personen bepaalde aanpassingen aanbrengen of doorvoeren. Digitale handtekeningen kunnen de integriteit van digitale archiefdocumenten dus niet altijd aantonen. Ze bewijzen alleen dat een digitaal object al dan niet na ondertekening werd gewijzigd.

Manipulaties of wijzigingen kunnen met een digitale handtekening beter worden voorkomen door de verzender een document te laten encrypteren met de publieke sleutel van de ontvanger en vervolgens zijn eigen digitale handtekening aan het document toevoegen. De internationale archiefwereld wijst het archiveren van geëncrypteerde documenten echter algemeen af[13]. Encryptie druist in tegen het principe om de nodige reconstructieschakels tot een absoluut minimum te beperken. Geëncrypteerde archiefdocumenten worden bijgevolg eerst gedecrypteerd alvorens ze in het digitaal archief worden opgenomen.

3.4 Besluit

Uit bovenstaande blijkt dat vanuit archiefwetenschappelijk standpunt digitale handtekeningen geen geschikte methode zijn om de authenticiteit en integriteit van digitale archiefdocumenten aan te tonen. Op het vlak van de authenticiteit zeggen digitale handtekeningen niets over de identiteit van digitale archiefdocumenten. De authenticatieverklaring reikt niet verder dan het bewijs dat iets/iemand in het bezit van de private sleutel van de ondertenaar het document ondertekende. Met betrekking tot de integriteit bewijst een digitale handtekening enkel dat de bits van het verstuurde document intact zijn. Met digitale handtekeningen worden evenmin onrechtmatige wijzigingen of manipulaties voorkomen.

Het heeft bijgevolg maar weinig zin dat de records manager of de archivaris zelf alle digitale archiefdocumenten zou voorzien van een digitale handtekening. Het archiveren van authentieke en integere archiefdocumenten is veeleer een kwestie van de registratie van essentiële identificerende metadata, het beschrijven van archiefdocumenten en het nemen van maatregelen om de betrouwbaarheid van archiefdocumenten te garanderen (wijzigingen voorkomen, audit trail bijhouden, documenteren van de bewerkingen, enz.).

[13] The Library and Archives Canada wijst het archiveren van geëncrypteerde berichten om twee redenen af. Ten eerste heeft encryptie de functie van envelop. Enveloppen zijn geen integraal onderdeel van het archiefdocument en worden in het algemeen niet geselecteerd. Ten tweede is voor de reconstructie van geëncrypteerde archiefdocumenten de overeenstemmende decryptiesleutel nodig, wat een bijkomende reconstructieafhankelijkheid is. Bij verlies van de decryptiesleutel dient het archiefdocument als verloren beschouwd te worden (http://www.collectionscanada.ca/06/0618_e.html). The National Archives van Australië archiveert evenmin geëncrypteerde documenten. Naast het argument van de extra reconstructieafhankelijkheid wijst the National Archives hiervoor ook op het feit dat na ontvangst de encryptie geen zin meer heeft. Encryptie heeft immers als initieel doel de inhoud te beschermen tijdens de transmissie (NATIONAL ARCHIVES OF AUSTRALIA, *GDA for encrypted records created in online security processes*, mei 2004).

4. LANGE TERMIJNARCHIVERING VAN DIGITAAL ONDERTEKENDE ARCHIEFDOCUMENTEN

Vanuit archiveringsstandpunt volstaat de archivering van digitale handtekeningen niet om de authenticiteit en integriteit van digitale archiefdocumenten aan te tonen. Toch heeft de de archivaris een archiveringsoplossing voor digitaal ondertekende archiefdocumenten nodig. Archiefvormers zullen digitale handtekeningtechnieken toepassen om te voldoen aan allerlei juridische vereisten en deze documenten komen voor (middel)langetermijnarchivering in aanmerking. Vanuit (Belgisch) juridisch oogpunt is het immers belangrijk dat het origineel document met de originele digitale handtekening bewaard blijft.

4.1 Archiefkwesties

Digitale handtekeningen zijn ontworpen om onmiddellijk na de ontvangst van een document de geldigheid te controleren. De transmissie en de aansluitende verificatie is in tijd beperkt. Bepaalde digitaal ondergetekende documenten komen echter voor (middel)langetermijnarchivering in aanmerking en hun authenticiteit dient evenlang gewaarborgd te blijven. Het valideren van digitale archiefdocumenten door middel van een digitale handtekening op een tijdstip in de verre toekomst is echter geen evidentie:

- digitale handtekeningen zijn tijdsgebonden
- de bitstreams van digitale archiefdocumenten worden gemigreerd
- de validation chain moet beschikbaar blijven.

4.1.1 DIGITALE HANDTEKENINGEN ZIJN TIJDSGEBONDEN

Terwijl digitale documenten in aanmerking komen voor een (middel)lange of zelfs permanente bewaartermijn, is de techniek van de digitale handtekening ontworpen om op korte termijn de digitale documenten te valideren. Digitale handtekeningen zijn bedoeld om documenten onmiddellijk na hun ontvangst te valideren. In het PKI-model is de transmissietijd van korte duur en zeker niet gelijk aan de middellange of lange termijnopslag van digitale archiefdocumenten. De authenticatiefunctie van digitale handtekeningen heeft een korte levenscyclus. Het valideren van documenten een zekere tijd na ontvangst vormt vanwege twee redenen een probleem.

Digitale handtekeningen zijn een overwegend op technologie gebaseerde oplossing. Net zoals andere technologieën is de authenticatietechnologie onderhevig aan technologische veroudering. Het hashen van bitstreams en het encrypteren van de hashcode is afhankelijk van specifieke algoritmes en software. Beide zijn onderhevig aan technologische veroudering, maar zijn nodig voor de (her)validatie van digitale handtekeningen. Een realistische verwachting is dat met de doorbraak van quantumcomputing de huidige algoritmes naar de prullenbak zullen verwezen worden. Het is nu al duidelijk dat sleutellengtes mee moeten evolueren met de computerkracht[14]. Krachtige computers kunnen alsmaar sneller hash- en encryptiealgoritmes kraken. Zo zetten Chinese onderzoekers in 2004 de cryptografiewereld op zijn kop door aan te kondigen dat het MD5-algorime niet zo onfeilbaar is[15].

[14] Zo raadt het National Institute of Standards and Technology (NIST) het gebruik van MD5 (Message Digest 5, 128 bits) voor digitale handtekeningen en certificaten af. Het NIST formuleerde ook de aanbeveling om SHA-1 (Secure Hash Algorithm, 160 bits) tegen 2010 te vervangen door SHA-256 en SHA-512. (B.BURR, *Implications of recent analytic results hash functions: practical implications of recent analytic results*, op: Federal PKI Technical Working Group Meeting, 23 November 2004 (http://csrc.nist.gov/pki/twg/y2004/Presentations/twg-04-14.pdf))

[15] De onderzoekers kondigden aan een zgn. 'hash collision' (twee verschillende inputs die in dezelfde hashcode resulteren) in MD5 gevonden te hebben (X. WANG e.a., *Collisions for hash functions MD4, MD5, HAVAL-128*

Ook de uitgereikte certificaten hebben een beperkte levensduur. Elk certificaat heeft een geldigheidsperiode die in tijd beperkt is. Die geldigheidsperiode kan in theorie maximaal de periode zijn waarvoor de certificatie autoriteit informatie over de publieke sleutel bijhoudt. In de praktijk is de geldigheidsperiode beperkt tot een aantal jaren of zelfs korter omwille van de veiligheid van de sleutels en de algoritmes. Digitale certificaten kunnen ook vroeger ingetrokken worden (bijv. bij diefstal van de private sleutel). De bewaartermijn van archiefdocumenten kan deze geldigheidsperiode overstijgen zodat de authenticatie door middel van de digitale handtekening een probleem vormt.

4.1.2 MIGRATIE VAN DE BITSTREAMS VAN DIGITALE ARCHIEFDOCUMENTEN

Als de authenticatie al problemen oplevert bij een niet-intacte bitstream dan zal dat zeker het geval zijn wanneer archiefdocumenten worden gemigreerd om het probleem van de technologische veroudering op te lossen.

De archiefwereld buigt zich al meer dan een decennium over de vraag hoe digitale archiefdocumenten op lange termijn leesbaar kunnen blijven. Archivarissen zijn het algemeen eens dat archivering op papier of conversie geen goede oplossingen zijn. Migratie van de archiefdocumenten en emulatie van de nodige hard- en softwareomgeving zijn de meest geciteerde digitale bewaarstrategieën.

Migratie is momenteel de meest toegepaste bewaarstrategie. De digitale documenten worden hierbij omgezet naar een geschikt archiveringsformaat. Standaardisatie van het bestandsformaat is één van de belangrijkste vereisten voor zo'n archiveringsformaat. Emulatie is vooralsnog een theoretische oplossing voor het duurzaamheidsprobleem. Het blijft niet alleen een open vraag of emulatie een realistische piste is, maar het lijkt ook weinig waarschijnlijk dat emulatie een haalbare oplossing is voor documenten in gesloten bestandsformaten zoals de populaire formaten van het MS Office-pakket. Voor het bouwen van een emulator dient men immers te beschikken over de specificatie van het formaat. In het geval van gesloten bestandsformaten is die specificatie niet beschikbaar en methoden zoals decompileren of reverse-engineering die hiervoor een (gedeeltelijke?) oplossing zouden kunnen bieden, zijn strijdig met het auteursrecht[16]. Vanwege deze reden zullen documenten in gesloten bestandsformaten in de emulatiestrategie wellicht eerst worden omgezet naar een gestandaardiseerd bestandsformaat. Vervolgens kan op basis van de beschikbare formaatspecificatie een emulator voor raadpleging worden gebouwd.

Het omzetten van de digitale documenten naar een gestandaardiseerd formaat heeft als gevolg dat de bits en bytes van het document wijzigen. De bitstreams die het bron- en doelbestand vormen, verschillen van elkaar en zullen verschillende hashcodes opleveren. Na migratie zal de digitale handtekening die werd berekend op het bronbestand niet voor de validatie van de doelbestanden kunnen gebruikt worden.

4.1.3 DE VALIDATION CHAIN MOET BESCHIKBAAR BLIJVEN

Om in de toekomst digitale handtekeningen voor de authenticatie van digitale documenten te blijven gebruiken, volstaat het niet om enkel de documenten en de digitale handtekeningen te archiveren. Voor de verificatie is een externe PKI-structuur vereist. De volledige 'validation chain' met inbegrip van digitale certificaten en root certifcaten dient beschikbaar te blijven[17].

---

and RIPEMD, augustus 2004. (http://eprint.iacr.org/2004/199.pdf).

[16] F. BOUDREZ, *B. Bewaarstrategieën*, in: F. BOUDREZ en H. DEKEYSER, *Digitaal archiefbeheer in de praktijk. Een handboek*, Antwerpen-Leuven, 2004.

[17] J. DUMORTIER en S. VAN DEN EYNDE, *Electronic signatures and trusted archival services*, in: Proceedings of the DLMForum 2002, Barcelona 6-8 May 2002, Luxembourg, 2002, p. 520-524.

Binnen het PKI-model verspreiden certificatie autoriteiten de digitale certificaten. Voor de verificatie van digitale handtekeningen dienen deze certificaten beschikbaar te blijven. Certificatie autoriteiten zijn doorgaans commerciële organisaties. Men heeft geen garanties dat digitale certicaten op lange termijn bewaard worden. Ook alle software voor het decrypteren van digitale handtekeningen en hashen van digitale documenten zou operationeel moeten blijven. Rekening houdende met de relatief korte levensduur van softwaretoepassingen is het geen evidentie dat de authenticatietechnologie beschikbaar blijft. Het herbouwen van de benodige software is op basis van gedocumenteerde algoritmes in de toekomst wellicht wel mogelijk, maar dat zal een vrij dure en complexe aangelegenheid zijn. Van zodra een essentieel onderdeel niet meer aanwezig of operationeel is, breekt de validatieketting.

Het in stand houden van zo'n externe validatiestructuur botst bovendien met het archivistische principe dat digitale archieven zo zelfvoorzienend mogelijk moeten zijn. Alle essentiële elementen van de 'validation chain' zouden bijgevolg mee gearchiveerd moeten worden in het digitaal depot. Binnen het digitaal depot zou een certificaatarchief moeten worden aangelegd. Dit certificaatarchief zou heel goed beveiligd moeten worden, zodat certificaten niet kunnen gewijzigd of toegevoegd worden. Aangezien certificaten kunnen verlopen of ingetrokken worden, is het ook belangrijk dat informatie over de status van het certificaat wordt bijgehouden (bijv. geldigheidsperiode, datum en tijdstip van documentondertekening, certificate revocation list). Het archiveren van een time-stamp is belangrijk om aan te tonen dat een document werd ondertekend met een private sleutel voor dat het digitaal certificaat is vervallen of werd ingetrokken.

4.2 Oplossingen voor de lange termijnarchivering

De problematiek van de lange termijnarchivering van digitaal ondertekende documenten is momenteel volop in onderzoek. Het archiveren van de digitaal ondertekende documenten en de bijhorende digitale handtekeningen is op zich geen probleem, wel de verificatie van de digitale handtekening. Opvallend is dat een aantal initiatieven wel een oplossing bieden voor de lange termijnarchivering voor de digitale handtekening en de validation chain, maar niet voor de lange termijnraadpleging van de getekende documenten zelf[18]. De uitdaging bij het archiveren van digitaal ondertekende documenten is net een passende oplossing vinden voor beide problemen samen. Pistes die hiervoor momenteel verkend worden, zijn:

- het hertekenen van documenten na migratie
- het registreren van de validatie
- de bewaring van de originele bitstream en de validation chain
- de certificering van het migratieproces

4.2.1 HERTEKENEN NA MIGRATIE

Digitale handtekeningen verliezen hun authenticatiefunctie wanneer de digitale archiefdocumenten worden omgezet naar een ander bestandsformaat. Na migratie zijn de bits van het computerbestand gewijzigd zodat elke validatie na migratie twee verschillende hashwaarden, en bijgevolg geen authenticatie, zal opleveren.

[18] Voorbeelden hiervan zijn: XML Advanced Electronic Signatures (XAdES); EESSI, *Electronic signatures and infrastructures (ESI)*; *Electronic signature formats (ETSI TS 101 733 V1.5.1 (2003-12))*, december 2003; D. LEKKAS and D. GRITZALIS, *Cumulative notarization for long-term preservation of digital signatures*, [zonder datum] (http://www.syros.aegean.gr/users/lekkas/pubs/j/2004COMPSEC.pdf)

Een oplossing voor dit probleem zou het hertekenen van de gemigreerde documenten kunnen zijn[19], maar dit botst op zowel juridische als praktische bezwaren. De oorspronkelijke ondertekenaar kan weigeren een document opnieuw te tekenen of kan in tussentijd overleden zijn. Het hertekenen van de documenten door een trusted third party zou hiervoor een oplossing kunnen zijn[20], maar is nog steeds strijdig met het wettelijk standpunt dat een document niet mag hertekend worden of dat de originele handtekening nodig is[21]. Bovendien heeft een verklaring van een trusted third party niet dezelfde status als een persoonlijke authenticatie zoals de geavanceerde digitale handtekening[22].

4.2.2 REGISTREREN VAN DE VALIDATIE

Onmiddellijk na ontvangst wordt de geldigheid van het digitaal ondertekend document door middel van de digitale handtekening gecontroleerd. Het resultaat van deze validatie wordt door de ontvanger in de metadata van het document geregistreerd. Deze metadata dient samen met het archiefdocument gearchiveerd te worden en beschermd te worden tegen onrechtmatige manipulaties of wijzigingen.

De achterliggende filosofie van deze aanpak is dat de authenticatietechnologie van een digitale handtekening een overwegende technologische oplossing is en niet aan technologische veroudering ontsnapt. Bovendien dient de volledige validation chain gearchiveerd te worden. Het alternatief wordt gezocht in de inbedding van de authenticiteit en integriteit in een procedure die wel op lange termijn overbrengbaar is en waarin verschillende technologieën elkaar kunnen opvolgen. Deze benadering sluit ook aan bij de visie dat wordt aangenomen dat documenten die binnen een werkproces worden gebruikt, authentiek zijn, ook al ondergingen ze wijzigingen[23].

Het Nationaal Archief van Finland volgt deze invalshoek en gaat ook nog een stap verder door de digitale handtekeningen niet te archiveren. Ook de Nederlandse norm voor records management applicaties (ReMaNo)[24] en het NARA voorzien deze mogelijkheid[25]. Men gaat er immers van uit dat het archiveren van digitale handtekeningen na verificatie, registratie en opname van het document en zijn metadata in een betrouwbaar digitaal depot geen nut meer heeft[26]. Bovendien worden de digitale

---

19 C. LYNCH, *Canonicalization: a fundamental tool to facilitate preservation and management of digital information*, in: *D-Lib Magazine*, september 1999, (http://www.dlib.org/dlib/september99/09lynch.html); J. CURRALL, *Digital Signatures: not a solution, but simply a link in the process chain*, Glasgow, 2002, p.9 (http://eprints.lib.gla.ac.uk/documents/disk0/00/00/00/39).

20 Een dergelijke oplossing werd gesuggereerd in de ontwerptekst US FDA E.A., *Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures: Maintenance of Electronic Records*, juli 2002, p. 21 Inmiddels werd deze tekst ingetrokken (zie hiervoor US FDA E.A., *Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application*, 2003, p. 2-3).

21 DEKEYSER, H. en DUMORTIER, J., *Juridische obstakels voor de elektronische handel op het vlak van archivering en datering*, Studie in opdracht van de FOD Economie, KMO, Middenstand en Energie, September 2004, onuitg., p. 26.

22 J. DUMORTIER en S. VAN DEN EYNDE, *Electronic signatures and trusted archival services*, in: Proceedings of the DLMForum 2002, Barcelona 6-8 May 2002, Luxembourg, 2002, p. 520-524.

23 INTERPARES AUTHENTICITY TASK FORCE, *Requirements for assessing and maintaining the authenticity of electronic records*, in: InterPARES, *The long-term preservation of authentic electronic records: findings of the InterPARES project*, 2002, p.2.

24 G.J. VAN BUSSEL, P.J. HORSMAN, H. WAALWIJK, *Softwarespecificaties voor Records Management Applicaties voor de Nederlandse Overheid*, Amsterdam, 2004, p. 78-79.(http://www.archiefschool.nl/docs/ReMANO_2004.pdf)

25 NARA, *Records Management Guidance for Agencies Implementing Electronic Signature Technologies*, Washington, oktober 2000, p. 13. Een vereiste van het NARA voor digitaal ondertekende archiefdocumenten met een permanente bewaartermijn is dat de naam van de ondertekenaar en de datum van ondertekening in leesbare vorm in het archiefdocument wordt opgenomen.
(http://www.archives.gov/records_management/policy_and_guidance/electronic_signature_technology.html)

26 R.POHJOLA, *Implications of electronic signatures - the situation in Finland*, op: *DLM-FORUM 2002*, Barcelona, 7 mei 2002.

handtekeningen onbruikbaar na migratie. De Finse aanpak is vergelijkbaar met het wegknippen van een handtekening onder een document en botst op juridische en archiefwetenschappelijke bezwaren. Vanwege juridische redenen moet de oorspronkelijke handtekening soms bewaard blijven[27]. In de diplomatiek en archiefwetenschap is een handtekening onder een document een extrinsiek element van de documentaire vorm dat meestal als “essentieel” wordt beschouwd en dus mee moet worden gearchiveerd.

4.2.3 BEWAREN VAN DE ORIGINELE BITSTREAM EN DE VALIDATION CHAIN

Een aantal initiatieven zoeken oplossingen voor het archiveren van de validation chain zodat de validatie op lange termijn mogelijk blijft. Hiervoor is het niet alleen noodzakelijk dat de originele bitstreams worden gearchiveerd, maar ook alle elementen van de public key infrastructuur die nodig zijn voor verificatie op termijn zoals de digitale handtekening, het digitaal certificaat met de publieke sleutel, metadata over het certificaat, time-stamp, tegenhandtekeningen, enz. De validation chain moet even lang als de ondertekende documenten bewaard worden en operationeel blijven. Van elke digitale handtekening dient minimaal de volgende informatie vastgelegd te worden:

- het gebruikte hashingalgoritme
- het gebruikte algoritme voor het berekenen van de digitale handtekening
- de naam van de ondertekenaar
- de gedecrypteerde digitale handtekening
- de publieke sleutel
- de status van het digitaal certificaat

EESSI (European Electronic Signature Standardisation Initiative) ontwikkelde een formaat met de naam ES-A (Archival Electronic Signature) dat als doel de verificatie van de digitale handtekening op lange termijn heeft[28]. XAdES of XML Advanced Electronic Signatures vertoont veel gelijkenissen met deze aanpak. XAdES heeft de ambitie om tot een op XML gebaseerd archiveringsformaat voor digitale handtekeningen uit te groeien. XAdES is een uitbreiding op de XMLDSIG-Recommendation en biedt diverse schema's aan voor de opslag van een digitale handtekening en alle essentiële metadata[29].

Ook de VERS-archiveringsstrategie voorziet de archivering van alle elementen van de validation chain. De digitale handtekening en alle benodigde certificaten worden ingekapseld in de archiefcontainers waarin de archiefdocumenten verpakt worden (<SignatureBlock> in VEO-objecten). De VERS VEO-archiveringscontainers kunnen zowel de originele als de gemigreerde bitstream van de archiefdocumenten bevatten. De originele digitale handtekening en alle afhankelijkheden kunnen bij de originele bitstream opgenomen worden. De gemigreerde bitstream wordt digitaal getekend door de 'notary' of het record keeping system[30]. Vanwege de lage penetratie van PKI is er momenteel nog geen enkele praktische implementatie van de VERS-archiveringsstrategie waarbij de originele digitale handtekening in het VEO-object wordt ingekapseld. In de praktijk is de VERS-archiveringsstrategie dus eerder een toepassing van het hertekenen na migratie, maar hun theoretisch model voorziet de archivering van de originele digitale handtekeningen en de validation chain.

Het toepassen van deze benadering voor de lange termijnvalidatie van digitale handtekeningen heeft een aantal praktische gevolgen. Ten eerste moet de records management applicatie van de archiefvormer bij het valideren van digitaal ondertekende documenten alle digitale certificaten en

---

[27] J. DUMORTIER EN S. VAN DEN EYNDE, *Electronic signatures and trusted archival services*, in: Proceedings of the DLMForum 2002, Barcelona 6-8 May 2002, Luxembourg, 2002, p. 520-524.

[28] ESSI, *Electronic signatures and infrastructures (ESI)*; *Electronic signature formats (ETSI TS 101 733 V1.5.1 (2003-12))*, december 2003.

[29] http://www.w3.org/TR/2003/NOTE-XAdES-20030220; A. EGGER, *Digitale Signaturen, Probleme und Lösungen bei der Archivierung*, december 2003.

[30] http://www.prov.vic.gov.au/vers/standard/advice_12/5-2.htm

bijhorende metadata mee archiveren. Deze vereiste is bijvoorbeeld opgenomen in de Model Requirements for the management of electronic records (Moreq, 10.5.7) en in ReMaNO (vereiste nr. 261). Deze oplossing gaat ten tweede uit van de archivering van de originele digitale objecten. Hoe die originele digitale objecten op lange termijn raadpleegbaar blijven, is nog niet duidelijk. Voorstanders van deze oplossing suggeren emulatie als digitale bewaarstrategie, maar het blijft vooralsnog een open vraag of emulatie een praktische of of zelfs haalbare oplossing is. Ook het beperken van deze oplossing tot archiefdocumenten in een open of geschikt archiveringsformaat waarvoor later viewers kunnen gecreëerd worden, lijkt weinig realistisch. Hetzelfde geldt voor het tekenen van archiefdocumenten in een "canonieke vorm"[31]. Men kan immers niet altijd een bepaald formaat aan een ondertekenaar opleggen. Migratie als onderdeel voor de oplossing voor langetermijnraadpleging zal zich waarschijnlijk opdringen. De VERS-archiveringsstrategie bijvoorbeeld voorziet een migratie van de archiefdocumenten naar PDF. Ten slotte dient in de toekomst ook nog een oplossing uitgewerkt te worden voor het operationeel houden van de authenticatietechnologie zelf.

4.2.4 CERTIFICERING VAN HET MIGRATIEPROCES

Een andere oplossing voor het validatieprobleem dat na migratie optreedt, zou certificering van het migratieproces kunnen zijn[32]. Hierbij worden de gemigreerde archiefdocumenten niet hertekend. Een daartoe gemachtigde trusted third party:

- verifieert voor de migratie de digitaal ondertekende documenten
- controleert het migratieproces (audit van de migratieprocedure, van de gebruikte software, van de gemigreerde archiefdocumenten)
- levert een certificaat af.

Deze benadering houdt in dat de betrouwbaarheid van de omgezette digitale archiefdocumenten niet meer wordt aangetoond door middel van een digitale handtekening, maar met een certificaat. De gemigreerde digitale archiefdocumenten moeten gevrijwaard blijven van onrechtmatige manipulaties of wijzigingen.

4.3 Besluit

De archivering van de digitale handtekening op lange termijn stelt weinig of geen problemen. Het archiveren van de validatiefunctie daarentegen vraagt wel een bijzondere aandacht. Dit spruit voort uit het feit dat digitale handtekeningen niet ontworpen zijn om digitale documenten op (middel)lange termijn te valideren. De oplossingen voor het digitale duurzaamheidsprobleem van digitale archiefdocumenten vergroten dit probleem nog.

De afzonderlijke oplossingen voldoen niet aan de juridische en archivistische noden. Het hertekenen van archiefdocumenten na migratie dient vanuit juridisch standpunt afgewezen te worden. Het verwijderen van de digitale handtekening na validatie is doorgaans juridisch of archiefwetenschappelijk niet geoorloofd. De metadata van het validatieproces zijn vanuit administratief, juridisch en archiefstandpunt belangrijke gegevens die in relatie met het archiefdocument gearchiveerd moeten worden. Het bewaren van de originele bitstreams, de digitale handtekening en de validatiemetadata dringt zich op.

---

[31] C. LYNCH, *Canonicalization: a fundamental tool to facilitate preservation and management of digital information*, in: *D-Lib Magazine*, september 1999, (http://www.dlib.org/dlib/september99/09lynch.html); W3C, *Canonical XML version 1.0*, Recommendation, 15 maart 2001.

[32] RLG*, Trusted digital repositories: attributes and responsibilities*, Mountain View, 2002, p. 33-35.

Verder onderzoek moet uitwijzen of het volstaat om de digitale handtekening en validatiemetadata te archiveren of dat het werkelijk noodzakelijk is dat de validatiefunctie en de bijhorende software wordt gearchiveerd. Deze laatste optie is technisch de meest complexe. Beide archiveringsoplossingen kunnen ook naast elkaar worden gebruikt. Voor digitaal ondertekende archiefdocumenten met een beperkte bewaartermijn zou men de validation chain kunnen archiveren en operationeel houden, terwijl voor archiefdocumenten met een permanente bewaartermijn de validatiemetadata en een betrouwbaar archiefbeheerssysteem de rol van de digitale handtekening zouden kunnen overnemen. Het Nationaal Archief van Australië laat beide mogelijkheden open en suggereert dat een benadering wordt gekozen op basis van een risico-analyse, en niet op basis van de bewaartermijnen. Volgens het Nationaal Archief van Australië is het wel onwaarschijnlijk dat digitaal ondertekende archiefdocumenten na hun neerlegging nog met digitale handtekeningen gevalideerd kunnen worden[33].

Het ziet er dus naar uit dat een oplossing voor het archiveren van digitaal ondertekende documenten zal bestaan uit een combinatie van de resterende oplossingen zoals het archiveren van het origineel document en de validation chain enerzijds en het maken van (gecertificeerde) kopieën voor raadplegingsdoeleinden (migratie) anderzijds. De digitale bewaarstrategie van het DAVID-project houdt hier rekening mee door zowel de originele als de gemigreerde bitstream in het digitaal archief op te nemen. Of certificatie door een trusted third party nodig zal zijn, hangt af van het vertrouwen dat men stelt in de archivaris of het archiefbeheerssysteem van de archiefvormer en de archiefbeherende instelling. Externe certificatie van het migratieproces en/of van de gemigreerde archiefdocumenten kan het vertrouwen en de betrouwbaarheid alleen maar vergroten[34]. Men kan zich overigens afvragen of het beschikbaarstellen van gecertificeerde kopieën niet het hoogst haalbare is. Immers, bij digitale archivering zijn de opslagwijze en de presentatievorm niet gelijk en elke raadpleging resulteert in een nieuwe kopie. Digitale archiefdocumenten zijn eigenlijk per definitie reproducties van originelen, ook al raadpleegt men een digitaal document in zijn oorspronkelijk bestandsformaat. Een belangrijk aandachtspunt in het aantonen van de authenticiteit is het bewijzen of achterhalen van de status van de kopie ten opzichte van het origineel[35].

Ongeacht de oplossing die voor het archiveren van digitaal ondertekende documenten wordt gekozen, dient de archiefbeherende instelling te zorgen voor een archiefbeheerssysteem dat in staat is om authentieke en integere archiefdocumenten in tijd over te brengen. Immers, digitale handtekeningen voorkomen geen manipulaties of wijzigingen. Bovendien zullen de digitaal ondertekende archiefdocumenten maar een minderheid uitmaken van alle digitale archiefdocumenten die de archivaris bewaart. De authenticiteit en integriteit van de niet ondertekende digitale archiefdocumenten dient even goed gewaarborgd te worden.

5. ALGEMEEN BESLUIT

Het gebruik van een geavanceerde digitale handtekening als authenticiteits- en integriteitsbewijs voor digitale archiefdocumenten doet een aantal vragen en problemen rijzen. Die spruiten vooral voort uit het feit dat het hele concept van de digitale handtekening op een digitaal object is gebaseerd. Hierbij wordt voorbij gegaan aan het feit dat digitale archiefdocumenten veel meer zijn dan zomaar digitale

[33] NATIONAL ARCHIVES OF AUSTRALIA, *Recordkeeping and online security process: guidelines for managing commonwealth records created or received using authentication or encryption*, Canberra, 2004. (http://www.naa.gov.au/recordkeeping/er/security.html). De National Archives zelf archiveren de publieke sleutels of digitale certificaten niet, maar laten wel toe dat de archiefvormer zelf alle elementen van de validation chain bijhoudt.

[34] R. DALE, *Certification and audit*, op: *ErpaWorkshop 'Trusted digital repositories for cultural heritage'*, Rome, 17-19 november 2003.

[35] INTERPARES AUTHENTICITY TASK FORCE, *Requirements for assessing and maintaining the authenticity of electronic records*, in: INTERPARES, *The long-term preservation of authentic electronic records: findings of the InterPARES project*, 2002, p.4.

objecten of originele bitstreams. Bij het zoeken naar betrouwbaarheidswaarborgen voor digitale archiefdocumenten moet men uitgaan van het concept van het digitaal archiefdocument, en niet dat van het digitaal object. Anders is het gevaar groot dat men de archiefstatus van digitale documenten verliest of dat men maatregelen toepast die indruisen tegen het reconstructieproces dat de basis is van digitale archivering.

De maatregelen of garanties voor de betrouwbaarheid voor digitale archiefdocumenten moeten ook in tijd overbrengbaar zijn. De problemen inzake de langetermijnvalidatie van digitale handtekeningen zijn inherent aan het hele concept van de digitale handtekening. Naast de afhankelijkheid van een 'validation chain' is er ook de afhankelijkheid van technologie (raadpleging van het document, hashing, berekenen digitale handtekening, enz.). Technologie veroudert snel en mag bijgevolg niet de exclusieve basis voor het verzekeren van de betrouwbaarheid zijn. Technologische oplossingen dienen vervangbaar te zijn en in een overkoepelende beheersprocedure ingebed te worden.

Overigens mag men evenmin uit het oog verliezen dat betrouwbaarheid meer inhoudt dan authenticiteit en integriteit alleen. Ook accuraatheid en vertrouwen spelen een belangrijke rol bij het archiveren van betrouwbare archiefdocumenten. Het verzekeren van de betrouwbaarheid is een continu proces, dat start van bij de creatie of ontvangst en dat bij archivering in stand moet worden gehouden.