
Aspecten van het digitaal communiceren: de elektronische handtekening en de archiefwet

Prof. mr. dr. M.A.B. Chao-Duivis

17 december 2009



INHOUDSOPGAVE

| | |
|--|-----------|
| VOORWOORD | 3 |
| I. De elektronische handtekening en VISI | 4 |
| 1. Wat is VISI? | 4 |
| 2. Beveiliging in VISI | 5 |
| 3. De elektronische handtekening functie en techniek | 7 |
| 4. De elektronische handtekening en de Wet Elektronische Handtekeningen | 10 |
| 5. Verschillende juridische aspecten van de elektronische handtekening | 13 |
| 6. Conclusie: de vergelijking VISI werkwijze en de wettelijke regeling van de elektronische handtekening | 16 |
| II. De Archiefwet en VISI | 19 |
| 1. Inleiding | 19 |
| 2. Achtergrond: hoofdlijnen van de Archiefwet | 19 |
| 3. De praktijk | 27 |
| 4. VISI 'archivering' | 27 |
| 5. Concluderend | 29 |
| III. Bijlage | 30 |

Voorwoord

Het werken met behulp van digitale middelen is een niet meer weg te denken fenomeen in de dagelijkse praktijk. Deze nieuwe methoden en technieken vereisen dat juridisch doordacht dient te worden of er nieuwe juridische regels in het leven geroepen dienen te worden dan wel dat bestaande juridische kaders en begrippen aanpassing/vertaling behoeven. Dit heeft geleid tot een nieuwe discipline, die niet eens makkelijk in één naam te vangen is en ik gemakshalve aanduid als electronica en recht.¹ De kennis, die gegenereerd is door deze activiteiten, begint langzaam maar zeker door te sijpelen naar o.a. de werkvloer van het bouwrecht. Ik schreef al eerder over de juridische implicaties van het werken met BIM² en wijd thans opnieuw een artikel aan juridisch aspecten van de virtuele wereld. De vragen zijn ditmaal aangeleverd door CROW en betreffen twee aspecten van het werken met VISI.³ De vragen betreffen de elektronische handtekening en de verhouding van het werken met VISI en de Archiefwet. Ik zet in par. 2 uiteen wat VISI is, in par. 3 ga ik in op de elektronische handtekening en in par. 4 op de verhouding met de Archiefwet. Beide paragrafen worden afgesloten met concluderende opmerkingen.

Bij het totstandkomen van dit rapport zijn de volgende personen zeer behulpzaam geweest:

M. Maas van Gobar

T. Kramer van het Stadsarchief van de gemeente Amsterdam

F. Rosdorf van het Ingenieursbureau van de gemeente Amsterdam

B. Cortenraad van de gemeente 's-Hertogenbosch

¹ Deze benaming dekt activiteiten van de verschillende instituten, die inmiddels zijn opgericht en die zich bezighouden met alle aspecten van elektronica/digitale wereld en recht, de verschillende tijdschriften die er zijn etc.

² Zie TBR 2009, aflevering

³ Zie nader over VISI de website van CROW en met name het VISI Handboek, een fundament voor digitale samenwerking, 2003, een uitgave van CROW (hierna te noemen: VISI Handboek).

I. De elektronische handtekening en VISI

1. Wat is VISI?

VISI is een stelsel van afspraken over communicatie en informatieoverdracht in bouwprojecten. Het begin van de ontwikkeling van VISI dateert uit 1998.⁴ Binnen VISI zijn communicatieafspraken vastgelegd in een structuur die het VISI-raamwerk wordt genoemd.⁵

VISI is een communicatiestandaard die door de Nederlandse bouw is ontwikkeld en door contractpartijen wordt gebruikt om (digitale) communicatie gestructureerd te laten verlopen. Het beheer van de VISI-standaard is ondergebracht bij het CROW en de standaard wordt op het moment in honderden bouwprojecten toegepast. Deelnemers ervaren onder andere meerwaarde in VISI als hulpmiddel voor contractbeheersing, duidelijkheid in communicatie en een automatische dossieropbouw.

VISI betreft als het ware de managementkant van het werken met een deel van BIM. VISI is uitdrukkelijk geen software: benadrukt wordt nogmaals dat het gaat om afspraken; afspraken die wel de elektronische wijze van communiceren betreffen, welke communicatie wel weer afhankelijk is van software. Deze software is voorzover deze gebruikt wordt ten behoeve van VISI overigens wel gecertificeerd door CROW. Om het plastisch voor te stellen: vergelijken we VISI met het werken in een bibliotheek vol met boeken, dan wil men weten hoe de boeken in de kast fysiek geordend moeten worden: welke afstand moet tussen ieder boek of tussen de planken etc. in acht genomen worden. Welke boeken er komen te staan, is geen onderwerp van VISI. Welnu: die afspraken zijn vergelijkbaar met wat VISI is: een stelsel van afspraken niet betreffende de uitkomst van een specifieke bouwopdracht (een weg, een hoog gebouw etc.), maar betreffende de vraag: hoe communiceren de personen betrokken bij het project met elkaar. En om nogmaals van hetzelfde voorbeeld gebruik te maken: hoe de kast gemaakt moet worden, is ook geen onderwerp van VISI, dat is de taak van de software leverancier. Deze software leverancier wordt door een onafhankelijke partij (TNO) in opdracht van CROW gecertificeerd, waarmee een bepaalde kwaliteitsgarantie vast staat. Vergelijk ook dit met de aanwijzingen die aan de boekenkast maker worden gegeven: de boeken vallen uit de kast vallen als de planken scheef liggen; de VISI afspraken komen niet goed over, als de drager van de informatie niet goed is, om dat te borgen wordt de werkwijze van de fabrikant gecertificeerd.

In VISI wordt gewerkt met vaste begrippen. Voorbeelden van deze begrippen zijn: rol (aan een rol zijn verantwoordelijkheden en taken toebedeeld)⁶; transactie (een bindende afspraak tussen rollen)⁷; transactieschema (in dit schema worden de naam, een beschrijving en het resultaat van

⁴ VISI Handboek, p. 3, Woord vooraf.

⁵ Ibid., p. 9.

⁶ Ibid., p. 9.

⁷ Ibid., p. 10.

een transactie gemeld; dit schema bevat tevens de berichten die worden verstuurd)⁸; Door een berichten te versturen komt een transactie in een bepaalde transactietoestand (bijvoorbeeld verzocht, melding gereed of aanvaard/einde)⁹; berichten bevatten standaard een aantal gegevenselementen (voorbeelden: berichtomschrijving, transactieomschrijving, naam verzender, organisatie verzender, rolomschrijving verzender, naam ontvanger, organisatie ontvanger, rolomschrijving ontvanger, startdatum transactie, verzenddatum bericht, leesdatum bericht)¹⁰ deze kunnen worden aangevuld met transactie specifieke gegevenselementen en tot slot de bijlage (vergelijkbaar met de bekende 'attachment' bij email maar wel voorzien van een specificatie, waarbij gebruik wordt gemaakt van een aantal gegevenselementen zoals de naam van het document etc.). Ten behoeve van de verschillende contractmodellen die er zijn, is door CROW in 2007 in samenwerking met de Bouw Informatie Raad een Documentatie VISI Raamwerk UAV en een VISI Raamwerk UAV-GC gepubliceerd. In deze publicaties is de VISI methode als het ware geconcretiseerd voor deze beide modellen. Zo treft men bij de UAV versie onder Scope een opsomming van de sub-transacties in het VISI-raamwerk opgenomen die de formele communicatie tussen 'opdrachtgever' en 'opdrachtnemer' regelen: leveren werk, leveren deelwerk, aanleveren en beoordelen termijnstaten, technische afhandeling van afwijkingen etc. En in het equivalent voor de UAV-GC wordt onder Uitgangspunten bij punt 7 opgemerkt: 'Streven is om all formele communicatie uit de UAVgc volledig af te dekken. Uitzonderingen hierop zijn aanvraag van vergunningen, arbitrageprocedures, besluitvorming om te komen tot een betalingsregeling en besluitvorming om te komen tot opdrachtverlening.'

2. Beveiliging in VISI

Het VISI traject leidt er toe dat communicatie voor een groot deel verloopt via dit elektronische middel. Het elektronische middel is VISI-compatible software met een VISI-certificaat dat wordt uitgegeven door CROW. Voor alle duidelijkheid nog maar even: VISI zelf is geen elektronisch middel, maar een set van afspraken hoe elektronisch te communiceren.

Dat doet de vraag rijzen: hoe zeker te stellen dat niet zomaar willekeurige personen communiceren in dat systeem/hoe zeker te weten dat alleen gecommuniceerd wordt door de daartoe bevoegde personen. De VISI-organisatie heeft daartoe een communicatieprotocol ontwikkeld. Navraag bij CROW over dit - technische - aspect levert het volgende antwoord op de vraag hoe dat werkt:

'Wanneer wordt gestart met communicatie dient een aantal zaken te worden ingesteld: in zowel het systeem van de Opdrachtgever als de Opdrachtnemer wordt het verstrekte¹¹ VISI-raamwerk ingelezen. In een zogenaamd projectspecifiek bericht

⁸ Ibid., p. 13.

⁹ Ibid., p. 13.

¹⁰ Ibid., p. 16.

¹¹ Daarmee wordt bedoeld:

worden personen aan rollen gekoppeld, IP-adressen/URL's van de servers van beide systemen ingesteld (hierdoor is aan de ene kant duidelijk naar welk systeem de berichten dienen te worden gestuurd en of de binnenkomende berichten ook daadwerkelijk van het systeem van de projectpartner vandaan komen). Dit projectspecifieke bericht wordt ook in beide systemen ingeladen. De Opdrachtnemer wil nu een contractwijziging via VISI voorleggen aan de Opdrachtgever. In het contract zijn de gemachtigde personen, van beide partijen, die formeel met elkaar communiceren vastgelegd. Deze personen zijn via het projectspecifieke bericht verbonden aan de rol met deze verantwoordelijkheid. De gemachtigde van de Opdrachtnemer kan nu met een login en paswoord inloggen op het eigen VISI-compatible systeem (deze systemen maken over het algemeen gebruik van HTTPS een secure protocol met versleuteling die ook door banken wordt gebruikt). Vervolgens kan de gemachtigde van de Opdrachtnemer alleen kiezen uit de transacties die aan de rol verbonden zijn die hij/zij vervult in het VISI-raamwerk. In dit geval wordt gekozen voor de transactie "Indienen wijziging bij Opdrachtgever", aangezien een transactie tussen rollen plaatsvindt, is direct duidelijk naar welke persoon in welke rol bij de Opdrachtgever deze transactie wordt opgestart. In deze transactie bestaat maar één enkel start bericht met de naam "Indiening wijziging". Het bericht wordt ingevuld en aangezien de wijziging uitgebreid is uitgewerkt in een document, voegt de Gemachtigde van de Opdrachtgever een .pdf (dit formaat is in het contract afgesproken) bij van het document. Als het document wordt bijgevoegd, dienen nog een aantal meta-gegevens te worden meegegeven, zoals versie, naam, documentdatum etc.. Het bericht is nu klaar voor verzending. Door op versturen te klikken wordt het bericht opgeslagen in het eigen systeem en verzonden naar het systeem van de Opdrachtgever. Tijdens het versturen wordt een aantal checks gedaan, zoals: is het systeem van de andere partij online; voldoet het bericht aan het schema zoals in het raamwerk vastgesteld; is het bericht in goede orde ontvangen door het systeem van de andere partij. Door deze laatste check is er altijd zekerheid dat het bericht en het bijbehorende document door de andere partij is ontvangen, zo niet dan wordt het bericht als niet verzonden beschouwd (bij e-mail is dit niet het geval). Nadat berichten zijn verzonden en ontvangen zijn deze berichten niet meer aanpasbaar. De Gemachtigde van de Opdrachtgever heeft nu het VISI bericht ontvangen in zijn/haar eigen systeem. Waar uiteraard op ingelogd dient te worden met login en wachtwoord. De gemachtigde van de opdrachtgever beoordeelt de wijziging en maakt het oordeel kenbaar. Dit wordt gedaan door het bericht te beantwoorden. Aangezien de transactie en de berichten in het raamwerk zijn gedefinieerd, is er een tweetal berichten dat verzonden kan worden, namelijk: honorering wijziging en weigering wijziging. De namen van de berichten zelf geven al heel expliciet het oordeel weer. Het bericht met het oordeel is verzonden en de transactie is hiermee afgerond. Kortom: na verzenden van een bericht wordt zeker gesteld dat beide partijen het bericht hebben. Berichten en gekoppelde documenten kunnen niet uit een VISI-compatible systeem verwijderd

worden. Het bericht en het document zijn dus onlosmakelijk met elkaar verbonden. Beide partijen beschikken over dezelfde berichten en documenten die verzonden zijn (er is zelfs nog een mogelijkheid om ook nog een derde systeem bij bijvoorbeeld een notaris te zetten waar ook alle verzonden berichten terechtkomen, dit is in praktijk overigens nog nooit gedaan). Er vindt controle plaats of het bericht ook van het juiste ip adres afkomstig is en volgens het juiste raamwerk is verzonden. Alleen personen die aan een bepaalde rol verbonden zijn kunnen transacties starten die aan de rol verbonden zijn. Er moet ingelogd worden met login en paswoord op de VISI systemen.’

De vraag is nu of deze manier van werken voldoende is om te kwalificeren als elektronische handtekening. In de volgende paragraaf een paar woorden over wat een elektronische handtekening is.

3. De elektronische handtekening functie en techniek

Met een handtekening wordt in de literatuur¹² gewoonlijk verstaan lettertekens, gesteld in het handschrift van de ondertekenaar, die de persoon die de verklaring aflegt beogen te individualiseren. Functies die door een handtekening worden vervuld zijn: identificatie, toerekening van het in een geschrift gestelde aan de ondertekenaar (de ondertekenaar geeft daarmee aan dat hij de inhoud voor waar aanneemt); de inhoud geeft de wilsverklaring van de ondertekende persoon weer; door middel van ondertekening kan de echtheid van een document worden aangenomen, anders gezegd: de ondertekenaar heeft met zijn handtekening authenticiteit aan het geschrift verleend.¹³ Enkele lettertekens, een vingerafdruk en ook de elektronische handtekening worden door deze klassieke definitie niet gedekt, hoezeer ook met de laatste twee methoden individualisatie respectievelijk authenticiteit kan worden gewaarborgd.¹⁴ De Wet elektronische handtekeningen heeft hier verandering in gebracht.

Wat is een elektronische handtekening? Alvorens op deze vraag nader in te gaan, dient een onderscheid gemaakt te worden tussen drie soorten elektronische handtekeningen:

- a) een gewone handtekening kan een e-mailbericht zijn waarin persoonsgegevens staan of een ingescande handtekening. Uiteraard moet deze handtekening voldoen aan art. 3:15a, vierde lid BW, oftewel de elektronische handtekening moet bestaan uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die gegevens worden gebruikt als middel voor authenticatie. Aan deze

¹² H. Franken, H.W.K. Kasperen, A.H. de Wild, Recht en computer, Kluwer, Deventer, 2004, p. 204.

¹³ Ibid. p. 204/205.

¹⁴ Ibid.

handtekening is niet het vermoeden van art. 3:15a lid 2 aanhef BW verbonden als aan de nu te noemen elektronische handtekeningen.¹⁵

- b) De geavanceerde handtekening bestaat uit gegevens over de ondertekenaar en een certificaat van een certificaatdienstverlener. Aan de geavanceerde handtekening worden een aantal vereisten gesteld bovenop de eisen die aan een gewone elektronische handtekening worden gesteld (hierna wordt verwezen naar de eisen genoemd in art. 3:15a BW, die hieronder uitgebreid aan de orde komen).¹⁶
- c) De gekwalificeerde elektronische handtekening: deze derde soort wordt ook vaak onder die sub b geschoven, in welk geval er maar sprake is van 2 soorten elektronische handtekeningen, maar indien hij apart wordt genoemd, wordt het onderscheid gevormd door het feit dat de handtekening vervaardigd is met een certificaat afkomstig van een bij de OPTA ingeschreven Certificatiedienstverlener.

In het hierna volgende zal het steeds om de omschrijving sub b gaan, begrepen in de meest uitgebreide betekenis.

De term elektronische handtekening is een verzamelbegrip, waaronder veel verschillende technieken vallen, variërend van het gebruik van een PIN-code tot biometrische technieken en digitale handtekeningen, gebaseerd op encryptie¹⁷. De hiervoor genoemde functies van de 'klassieke' handtekening kunnen ook door de elektronische worden vervuld afhankelijk van de gebruikte techniek. In de literatuur¹⁸ wordt aangenomen dat de digitale handtekening op basis van encryptie het dichtst bij de klassieke handtekening komt. Versterking hiervan is mogelijk door gebruikmaking van de diensten van een Certification Authority of Trusted Third Party (CA of TTP¹⁹) en eventueel door ondersteuning met biometrische kenmerken voor identificatie.²⁰

Het is nodig nog iets meer over de technische kant van deze zaak op te merken. In hoeverre worden de functies van de handtekening vervuld door de elektronische handtekening?²¹ De echtheid (integriteit en authenticiteit) van een bericht zijn bij uitstek te waarborgen door een digitale handtekeningstechniek. In de Memorie van Toelichting²² op het in 2003 ingevoerde

¹⁵ <http://www.e-overheid.nl/thema/juridisch/handtekeningen/handtekeningen.xml>.

¹⁶ Ibid.

¹⁷ Franken et.al. p. XIII geven van 'encryptie' de volgende omschrijving: 'Techniek (met meerdere varianten) om met behulp van een algoritme gegevens te versleutelen (versleutelen) teneinde geheim berichtenverkeer mogelijk te maken.' Een 'algoritme', aldus dezelfde auteurs op p. XI, is 'Nauwkeurig gedefinieerde procedure om bij een bepaalde gegevensinvoer een gesteld resultaat te verkrijgen door een eindig aantal bewerkingen'.

¹⁸ Franken et. al. p. 205/206.

¹⁹ Een TTP wordt door Franken et. al. p. XVIII gedefinieerd als: 'Een onafhankelijke, onpartijdige organisatie die met behulp van bedrijfsmatige en technische beveiligingsinstrumenten kan bijdragen aan het vertrouwen ten aanzien van elektronische transacties. Een TTP verschaft technisch en juridisch betrouwbare methoden om een elektronische transactie mogelijk te maken en uit te voeren, daaromtrent bewijs te leveren en geschillen te beslechten.' Het is een soort tussenpersoon, die de garantie voor de identiteit geeft, zo zou men het ook kunnen zeggen.

²⁰ Voor een uiteenzetting van de technische kant van de zaak, zie het genoemde boek van Franken, p. 206 e.v.

²¹ Ontleend aan Franken et. al. p. 208 e.v., alwaar een uitgebreidere uiteenzetting wordt gegeven.

²² TK, 2000/01, 27.743, nr. 3, p. 2.

artikel 3:15a BW betreffende de elektronische handtekening wordt duidelijk aangegeven hoe dit technisch in zijn werk gaat²³:

‘De ondertekenaar versleutelt het te verzenden bericht met de private sleutel. Dit levert een bericht op dat bestaat uit een reeks getallen, welke reeks pas leesbaar wordt na ontcijfering. Voor deze ontcijfering moet de publieke sleutel²⁴ worden gebruikt. De sleutels zijn zo aan elkaar verbonden dat een bericht dat met de private sleutel is versleuteld, slechts met de publieke sleutel kan worden ontcijferd. Maar omgekeerd is het met kennis van de publieke sleutel praktisch niet mogelijk om een versleuteld bericht te maken. Daardoor is het ook niet mogelijk dat een derde het versleutelde bericht zonder bezit van de private sleutel kan wijzigen: dat zou immers vereisen dat de derde de versleutelde reeks getallen zodanig weet te wijzigen dat deze na toepassing van de publieke sleutel weer een zinvolle, doch gewijzigde tekst oplevert. De gekozen techniek is evenwel zodanig dat een wijziging in de versleutelde tekst ook een groot deel van de tekst radicaal wijzigt, en het praktisch niet mogelijk een zinnige wijziging aan te brengen met louter proberen. Een voorbeeld van een dergelijke techniek is het zogenaamde RSA-algoritme. Het gevolg van deze eigenschappen is dat de ontvanger met het versleutelde bericht er op kan vertrouwen dat 1. het bericht is verzonden door iemand die de beschikking heeft over de private sleutel (de ondertekenaar), 2. dat het bericht in exact deze vorm is verzonden door de ondertekenaar.’

De ontsleuteling van de handtekening kan dus alleen gebeuren met behulp van een passende sleutel en doordat wijzigingen in berichten direct zichtbaar worden, kan worden geverifieerd of het bericht is verzonden door de verzender of dat het na tekening nog is gewijzigd. De wilsuiting en toerekening kunnen ook aan de elektronische handtekening worden toegeschreven: het bericht wordt gecodeerd nadat het als geheel is opgemaakt, door middel van het uitvoeren van deze handeling kan de ‘ondertekenaar’ uiting geven aan zijn wil en kan het ondertekende aan hem worden toegerekend. Dit is anders dan bij het gebruik van een pin-code, die wel uniek is, maar veeleer wordt gebruikt als toegangscode en niet als verificatiemiddel.

²³ Ontleend aan De Groene Serie Privaatrecht, Vermogensrecht, Titel 1. Algemene Bepalingen, afdeling 1A, aantekening 13.

²⁴ Een publieke sleutel wordt op Wikipedia als volgt gedefinieerd: Een publieke sleutel (Engels: public key) is een onderdeel van een bepaald type cryptografische versleuteling en wel de asymmetrische cryptografie. Bij deze wijze van informatiever sleuteling, zijn er twee verschillende sleutels die bij elkaar horen: één voor versleutelen en één voor ontcijferen van informatie. Een voorbeeld van een algoritme dat dit gebruikt is RSA. Voorbeelden van programma's die dit (kunnen) gebruiken, zijn ssh en Pretty Good Privacy applicaties. Groot voordeel van twee verschillende sleutels is, dat nu één sleutel kan worden bekend gemaakt (publiek), zodat iedereen deze sleutel kan gebruiken om de data te bewerken. Vaak wordt dit gebruikt om nu informatie te versleutelen, waarna de nu beveiligde informatie verstuurd kan worden naar de eigenaar van de sleutel.

Alleen deze eigenaar heeft naast de publieke sleutel ook zijn geheime sleutel die alleen gebruikt kan worden om versleutelde informatie weer naar leesbare tekst om te zetten. Kern van het principe is dat iedereen informatie met een publieke sleutel kan beveiligen op een manier dat alleen de eigenaar van de geheime sleutel de informatie kan ontcijferen. Dit garandeert het geheim blijven van het bericht. Alleen de geadresseerde kan het bericht ontsleutelen met zijn geheime sleutel. Omgekeerd kan de eigenaar van een geheime sleutel een bericht versleutelen en dat aan iedereen sturen. De ontvangers kunnen nu met zijn publieke sleutel het bericht ontcijferen en de informatie lezen. Omdat de informatie met juist die publieke sleutel was te ontcijferen, weten de ontvangers zeker dat het bericht van de eigenaar van de geheime sleutel afkomstig is. Hij is immers de enige die de geheime sleutel kent en hij kan dan ook niet ontkennen de bron van het bericht te zijn. Dit wordt in de literatuur [non-repudiation] genoemd.

De identificatie-functie van de handtekening vereist nog wat aandacht: immers een digitale handtekening is en wordt, zeker in de zakelijke sfeer, vaak door meer personen te gebruiken. Het is dan ook niet altijd zeker wie de handeling verrichtte. Wil men hierover absolute zekerheid dan is het nodig gebruik te maken van biometrische kenmerken. Het gebruik van een CA²⁵ lost dit probleem ook niet helemaal op. Wel worden bij deze certificatie de publieke sleutel als in gebruik bij een bepaalde persoon, eventueel met een bepaalde hoedanigheid en bevoegdheid gecertificeerd, maar in concrete situaties zal nooit met zekerheid gegarandeerd kunnen worden dat de handtekeninggebruiker zeker is degenen die hij pretendeert te zijn. Is de handtekeningcode ook bij de ontvangende partij bekend, dan is niet onweerlegbaar aan te tonen dat een bericht van de verzender en niet van de ontvangende partij afkomstig is. Wil men dit voorkomen dan zijn aanvullende maatregelen nodig, waarmee de verzender van het bericht kan worden vastgesteld. De eerder genoemde Trusted Third Party kan hier goede diensten bewijzen, aldus nog steeds Franken.

4. De elektronische handtekening en de Wet Elektronische Handtekeningen

Gezien het belang van het elektronisch verkeer is er op Europees niveau regelgeving ontstaan: de Richtlijn betreffende een gemeenschappelijk kader voor elektronische handtekeningen²⁶. Deze Richtlijn is geïmplementeerd door middel van de Wet Elektronische Handtekeningen, die per 21 mei 2003 in werking trad. De Wet is opgenomen in Boek 3 van het BW in de nieuwe Afdeling 1A. Elektronisch vermogensrechtelijk rechtsverkeer. Van belang voor deze beschouwing zijn met name de volgende bepalingen:

Artikel 15a

1. Een elektronische handtekening heeft dezelfde rechtsgevolgen als een handgeschreven handtekening, indien de methode die daarbij is gebruikt voor authenticatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval.
2. Een in lid 1 bedoelde methode wordt vermoed voldoende betrouwbaar te zijn, indien een elektronische handtekening voldoet aan de volgende eisen:
 - a. zij is op unieke wijze aan de ondertekenaar verbonden;
 - b. zij maakt het mogelijk de ondertekenaar te identificeren;
 - c. zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en

²⁵ In zijn bespreking van M.H.M. Schellekens, *Electronic signatures. Authentication technology from a legal perspective*, 2004, geeft R. van Esch in *Themis*, 2005, p. 113, weer wat Schellekens opmerkt over het in de CA te stellen vertrouwen: Degene die een ondertekende verklaring ontvangt, moet er op kunnen vertrouwen dat de CA de identiteit van de houder van de publieke sleutel correct heeft vastgesteld, adequaat beveiligde systemen hanteert, gekwalificeerd personeel in dienst heeft, juiste procedures heeft ingevoerd voor de herroeping van de publieke sleutel door de houder etc.

²⁶ Richtlijn 1999/93/EG, PbEG L 13/12.

d. zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
e. zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss, van de Telecommunicatiewet²⁷; en

f. zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel vv, van de Telecommunicatiewet.

3. Een in lid 1 bedoelde methode kan niet als onvoldoende betrouwbaar worden aangemerkt op de enkele grond dat deze:

- niet is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss, van de Telecommunicatiewet;
- niet is gebaseerd op een door een certificatie­dienst­ver­lener als bedoeld in artikel 18.16, eerste lid, Telecommunicatiewet afgegeven certificaat; of
- niet met een veilig middel voor het aanmaken van elektronische handtekeningen is aangemaakt als bedoeld in artikel 1.1, onderdeel vv, van de Telecommunicatiewet.

4. Onder elektronische handtekening wordt een handtekening verstaan die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie.

5. Onder ondertekenaar wordt degene verstaan die een middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel uu, van de Telecommunicatiewet gebruikt.

6. Tussen partijen kan van lid 2 en 3 worden afgeweken.

Hoe de eisen gesteld in artikel 3:15 lid 2 BW te verstaan? Van belang is om te beginnen het bepaalde in sub e: 'zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss, van de Telecommunicatiewet'. Dit laatste artikel omschrijft certificaat als volgt: 'een elektronische bevestiging die gegevens voor het verifiëren van een elektronische handtekening met een bepaalde persoon verbindt en de identiteit van die persoon bevestigt'. Hiermee heeft men nog slechts een hulpdefinitie in handen²⁸. Nodig is nog te weten wat met gekwalificeerd wordt bedoeld, zie daarvoor art. 1.1 sub ss van de Telecommunicatiewet: 'een certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid, en is afgegeven door een certificatie­dienst­ver­lener²⁹ die voldoet aan de eisen, gesteld krachtens artikel 18.15,

²⁷ Hierna ook: Tw.

²⁸ Groene Kluwer, aantekening 14.

²⁹ Op dit moment zijn er zes certificatie­dienst­ver­leners bij de OPTA geregistreerd. Buiten deze geregistreerde certificaat­dienst­ver­leners zijn er niet geregistreerde. In het Consultatiedocument van de OPTA uit 2003, Consultatiedocument "Registratie van certificatie­dienst­ver­leners die gekwalificeerde certificaten aanbieden of afgeven aan het publiek met betrekking tot elektronische handtekeningen" wordt onder nummer 3 opgemerkt over deze dienst­ver­leners: 'Centraal in de wetgeving (en ook in de markt) van elektronische handtekeningen staan de certificatie­dienst­ver­leners. Deze partijen worden ook wel Trusted Third Parties (TTP's) of Certificate Service Providers (CSP's) genoemd. Deze partijen geven gekwalificeerde (dit betekent dat ze voldoen aan de wettelijke vereisten) certificaten uit die bij elektronische handtekeningen worden gevoegd. Met behulp van deze certificaten kunnen partijen die op deze elektronische handtekeningen willen vertrouwen de geldigheid van de elektronische handtekening verifiëren. Bij deze verificatie staat de certificatie­dienst­ver­lener garant dat de handtekening is gezet door de persoon welke in het certificaat is genoemd en dat het ondertekende bericht authentiek is. Hiermee kunnen partijen bijvoorbeeld veilig zakelijke transacties via het internet doen.'

eerste lid'. Een zodanig certificaat, aldus de Groene Kluwer t.a.p., voldoet derhalve aan twee groepen eisen: technische eisen, als bedoeld in art. 18.15 lid 2 Tw, en organisatorische eisen, te weten dat zij slechts door bepaalde organisaties mogen worden afgegeven: de certificatie­dienstverleners. Zij dienen er zorg voor te dragen dat een gekwalificeerd certificaat uniek is, waarmee is voldaan aan eis (a) van art. 15a lid 2 BW.³⁰

Gezien het feit dat de technische vereisten (weergegeven in noot 24) de naam van de ondertekenaar of een als zodanig geïdentificeerd pseudoniem verlangen, volgt dat hiermee voldaan is aan de eis gesteld in art. 3:15a lid 2 onder b (identificatiemogelijkheid van de ondertekenaar).

Omdat het om een gekwalificeerd certificaat moet gaan, is ook duidelijk dat indien daar sprake van is, dat voldaan is aan de eis onder e. Immers op grond van art. 18.15 lid 3 Tw en art. 2 onder g Besluit elektronische handtekeningen, rust op de certificatie­dienstverlener de taak feitelijk te verifiëren dat de ondertekenaar (houder van het gekwalificeerde certificaat, waarover zo meer) inderdaad de identiteit heeft die wordt vermeld in het certificaat. Met het voldoen aan het vereiste onder e is ook voldaan aan de vereisten onder a (op unieke wijze met de ondertekenaar verbonden) en onder b (zij maakt het mogelijk de ondertekenaar te identificeren).

Het vereiste sub f luidt: 'zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel vv, van de Telecommunicatiewet'. Wat is een middel voor het aanmaken van elektronische handtekeningen en wat is een veilig middel? Art. 1.1 sub uu Tw definieert een middel voor het maken van een elektronische handtekening als volgt: "geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het aanmaken van elektronische handtekeningen te implementeren'. In art. 18.17 lid 1 staat wat een veilig middel is: "een middel voor het aanmaken van elektronische handtekeningen dat voldoet aan de eisen gesteld krachtens artikel 18.17, eerste lid.' Is voldaan aan deze omschrijvingen dan is daarmee voldaan aan het bepaalde sub f van art. 15a lid 2.

Van belang in zake de veiligheid is voorts van belang art. 5 Besluit elektronische handtekeningen:

³⁰ De technische eisen zijn nader uitgewerkt in art. 3 Besluit elektronische handtekeningen 'Certificaten als bedoeld in artikel 18.15, tweede lid, van de wet bevatten ten minste:

- a. de vermelding dat het certificaat als gekwalificeerd certificaat wordt afgegeven;
- b. de identificatie en het land van vestiging van de afgevende certificatie­dienstverlener;
- c. de naam van de ondertekenaar of een als zodanig geïdentificeerd pseudoniem;
- d. ruimte voor een specifiek attribuut van de ondertekenaar, dat indien nodig, afhankelijk van het doel van het gekwalificeerde certificaat, wordt vermeld;
- e. gegevens voor het verifiëren van de handtekening die overeenstemmen met de gegevens voor het aanmaken van de handtekening die onder controle van de ondertekenaar staan;
- f. vermelding van het tijdstippen van het begin en van het einde van de geldigheidsduur van het gekwalificeerde certificaat;
- g. de identiteitscode van het gekwalificeerde certificaat;
- h. de elektronische handtekening van de afgevende certificatie­dienstverlener die voldoet aan de criteria van artikel 15a, tweede lid, onderdeel a tot en met d, van Boek 3 van het Burgerlijk Wetboek;
- i. eventuele beperkingen betreffende het gebruik van het gekwalificeerde certificaat, en
- j. eventuele grenzen met betrekking tot de waarde van de transacties waarvoor het gekwalificeerde certificaat kan worden gebruikt.'

'Een veilig middel voor het aanmaken van elektronische handtekeningen voldoet aan de volgende eisen:

- a. het waarborgt dat de gegevens voor het aanmaken van elektronische handtekeningen in de praktijk slechts eenmaal kunnen voorkomen en de vertrouwelijkheid daarvan redelijkerwijs gegarandeerd is;
- b. het waarborgt met redelijke zekerheid dat de gegevens voor het aanmaken van elektronische handtekeningen niet kunnen worden afgeleid en dat de elektronische handtekening beschermd is tegen vervalsing met de op het tijdstip van het afgeven van de verklaring beschikbare technieken;
- c. het waarborgt dat de gegevens voor het aanmaken van elektronische handtekeningen door de legitieme ondertekenaar op betrouwbare wijze kunnen worden beschermd tegen gebruik door anderen;
- d. het laat de te ondertekenen gegevens ongewijzigd en belet niet dat die gegevens vóór de ondertekening aan de ondertekenaar worden voorgelegd.'

Wordt aan de eisen a, b en d van dit artikel voldaan, dan is daarmee tevens voldaan aan de eisen gesteld in art. 15a lid 2 onder a en d.

Daarmee resteert nog alleen de eis onder c van art. 15a lid 2: 'zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden'. De Groene Kluwer aantekening 17 verwijst hiervoor naar de Memorie van Toelichting³¹: 'Om deze private sleutel onder zijn uitsluitende controle te kunnen houden zijn er diverse (combinaties van) mogelijkheden. Alvorens een private sleutel te kunnen gebruiken voor het zetten van een handtekening kan er kennis (bijvoorbeeld een pincode), bezit (gebruikmaking van bijvoorbeeld een smartcard waar de private sleutel op staat) of een lichaamskenmerk van de ondertekenaar (bijvoorbeeld een vingerafdruk) worden geëist.'

5. Verschillende juridische aspecten van de elektronische handtekening

Bewijskracht

Wat betekent het juridisch dat een elektronische handtekening voldoet aan al deze vereisten?

³¹ TK, 2000/01, 27743, nr. 3. p. 2.

Art. 15a lid 2 zegt: alsdan wordt vermoed dat de in lid 1 bedoelde methode voor authenticatie voldoende betrouwbaar is. Wanneer de wet van een vermoeden spreekt, is dit vermoeden weerlegbaar door tegenbewijs.³²

Wat is rechtens indien een elektronische handtekening niet met alle waarborgen als in lid 2 van art. 15a beschreven tot stand komt? Wordt hij dan niet vermoed betrouwbaar te zijn? Nee, art. 15a lid 3 staat aan de weg van die gevolgtrekking: in dat geval kan de elektronische handtekening niet als onvoldoende betrouwbaar worden aangemerkt. Wordt de rechter met een dergelijke elektronische handtekening geconfronteerd dan zal dit vooral consequenties hebben voor de bewijslastverdeling en/of voor zijn motiveringsplicht. Zie wat de Minister over deze bewijsrechtelijke kwestie antwoordde in de Eerste Kamer³³:

'Zowel de erkenning van rechtsgevolgen die aan gewone en gekwalificeerde certificaten wordt toegekend, als de rechtsbescherming van een partij die op een van deze certificaten vertrouwt, is in beginsel gelijk. Er is sprake van gelijkheid 'in beginsel' omdat een gekwalificeerd certificaat met meer wettelijke waarborgen is omkleed, hetgeen onder omstandigheden de doorslag kan geven, bijvoorbeeld bij de waardering door de rechter van het certificaat als bewijsmateriaal. Bij de waardering van het bewijsmateriaal geldt voor de waarde die aan de elektronische handtekening wordt toegekend een ondergrens. Zo mag de rechter ingevolge artikel 3:15a lid 3 van het Burgerlijk Wetboek bijvoorbeeld niet op de enkele grond dat geen sprake is van een gekwalificeerd certificaat een methode van authenticatie als onvoldoende betrouwbaar bestempelen. Deze ondergrens in acht nemend, is de rechter echter vrij om, uiteraard op basis van omstandigheden van het concrete geval, een hoge of een lage bewijswaarde aan een elektronische handtekening toe te kennen. Een elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat heeft daarbij het voordeel dat aan bepaalde wettelijke eisen moet zijn voldaan waarbij ook is voorgeschreven welke gegevens gedurende een bepaalde periode bewaard moeten blijven. De rechter kan derhalve bijvoorbeeld op eenvoudige wijze nagaan of de identiteit van de gebruiker van de elektronische handtekening op voldoende wijze is gecontroleerd aan de hand van de in artikel 1 van de Wet op de identificatieplicht aangewezen documenten. Hiermee is zeker niet uitgesloten dat een dergelijke controle even goed zal zijn uit te voeren bij elektronische handtekeningen die niet of op een gewoon certificaat zijn gebaseerd. De voorwaarden hiervoor zijn echter niet wettelijk geregeld maar aan partijen zelf overgelaten.'

³² TK 27743, nr. 3, p. 16.

³³ EK 2002.03, 27743, nr. 35, p. 4.

In de juridische literatuur³⁴ bestaat onenigheid over de vraag naar de bewijskracht van elektronische bestanden. Het voert te ver daarop in te gaan, wel zij opgemerkt dat er inmiddels een wetsvoorstel aanhangig is, waarin de invoering wordt voorgesteld van een nieuw art. 156 Burgerlijke Rechtsvordering (BRv), dat de bewijsrechtelijke positie van de elektronische onderhandse akte nader regelt.³⁵

In algemene zin is voorts in dit kader nog van belang, dat volgens de hoofdregel van het bewijsrecht, de bewijslast ligt op degene die iets stelt. Stelt iemand dus, dat een elektronisch (of ander) document waarin bijvoorbeeld een bestelling wordt gedaan, niet van hem afkomstig is, dan rust het bewijs van die stelling op hem. Stel nu dat het gaat om een elektronische handtekening die voldoet aan de wettelijke eisen en degene om wiens handtekening het gaat, stelt dat hij de ondertekenaar is terwijl een ander dat niet wil accepteren, dan rust de bewijslast volgens de hoofdregel op de ondertekenaar. Deze kan echter gebruik maken van het bewijsvermoeden dat de wet hem geeft: hij kan volstaan met te wijzen naar de wettelijke regeling van art. 3:15a BW. De last om dit vermoeden te ontcrachten rust nu op de andere partij. Stel nu dat de elektronische handtekening die ter discussie staat niet helemaal voldoet aan de wettelijke eisen, dan gaat het bewijsvoordeel niet op en herleeft dan wel is op de gewone wijze de hoofdregel van het bewijsrecht van toepassing; zie daartoe artikel 150 Burgerlijke Rechtsvordering;

De partij die zich beroept op rechtsgevolgen van door haar gestelde feiten of rechten, draagt de bewijslast van die feiten of rechten, tenzij uit enige bijzondere regel of uit de eisen van redelijkheid en billijkheid een andere verdeling van de bewijslast voortvloeit.

Eenvoudig gezegd: wie iets stelt, moet dat bewijzen.

Misbruik van de elektronische handtekening

³⁴ Zie het overzicht in de Groene Kluwer, aantekening 22 bij Titel 1, algemene bepalingen.

³⁵ Het voorstel van art. 157a BRv luidt als volgt: 1. Onderhandse akten kunnen op een andere wijze dan bij geschrift worden opgemaakt op zodanige wijze dat het degene ten behoeve van wie de akte bewijs oplevert, in staat stelt om de inhoud van de akte op te slaan op een wijze die deze inhoud toegankelijk maakt voor toekomstig gebruik gedurende een periode die is afgestemd op het doel waarvoor de akte bestemd is te dienen, en die een ongewijzigde reproductie van de inhoud van de akte mogelijk maakt. 2. Aan een wettelijke verplichting tot het verschaffen van een onderhandse akte kan alleen op een andere wijze dan bij geschrift worden voldaan met uitdrukkelijk instemming van degene aan wie de akte moet worden verschaft. Een instemming ziet, zolang zij niet is herroepen, eveneens op het verschaffen van een gewijzigde onderhandse akte. 3. Aan een wettelijke verplichting tot het verschaffen van een onderhandse akte wordt geacht niet te zijn voldaan zolang de ontvangst van die akte door degene aan wie de akte moet worden verschaft niet aan degene op wie die verplichting rust, is bevestigd. 4. Indien de wet het opmaken van een onderhandse akte voorschrijft, kan daaraan niet op een andere wijze dan bij geschrift worden voldaan in geval van: – onderhandse akten betreffende overeenkomsten waarbij persoonlijke of zakelijke zekerheden worden verstrekt door personen die niet handelen in de uitoefening van een beroep of bedrijf; en – onderhandse akte die onder het familierecht of het erfrecht vallen.

Wat is rechtens als een handtekening onbevoegd wordt gebruikt? Uitgangspunt is het arrest van de Hoge Raad van 19 november 1993, NJ 1994, 622, waar overwogen wordt:

'De vraag wie van partijen, bij gebreke van een contractuele regeling op dit punt, het risico van misbruik van een overeengekomen code behoort te dragen, dient te worden beantwoord aan de hand van de concrete omstandigheden van het geval, waarbij in het bijzonder van belang is aan wie valt toe te rekenen dat de code ter kennis van de onbevoegde is gekomen.'

In de uitspraak wordt gesproken van code, daarmee zou de elektronische handtekening gelijk gesteld kunnen worden. In de Memorie van Toelichting is door de Minister opgemerkt dat voor de risico-verdeling de contractuele verhouding met de Trusted Third Party (TTP) is. Daar wordt in de literatuur over gediscussieerd: verdedigd wordt dat de wetgever een regeling hierover zou moeten treffen, ook wordt gewezen naar de houder van de elektronische handtekening en weer anderen knopen aan bij de rechtspraak inzake vertegenwoordiging. Dit aspect is dan ook nog niet uitgekristalliseerd.

6. Conclusie: de vergelijking VISI werkwijze en de wettelijke regeling van de elektronische handtekening

De kern van de regeling van de elektronische handtekening voor zover thans van belang wordt gevormd door de vereisten geformuleerd in art. 15a lid 2 onder a tot en met f. Zoals hiervoor is opgemerkt, bepaalt lid 3 van art. 15a, dat een methode waarmee een elektronische handtekening wordt 'gezet' en die afwijkt van hetgeen beschreven is in lid 2, door die afwijking niet de aldus 'gezette' handtekening onvoldoende betrouwbaar maakt.

De vraag is dus:

- a) in hoeverre komt de VISI werkwijze overeen met het bepaalde in art. 15a lid 2 BW?
- b) Wat is de consequentie indien de VISI methode afwijkt van het bepaalde in art. 15a lid 2 BW?

Vraag a:

Ik zet hieronder achter elkaar wat de wet aan eisen stelt en wat daarvan het mogelijke equivalent in VISI is:

BW: a. zij is op unieke wijze aan de ondertekenaar verbonden.

VISI: bij twee partijen (Opdrachtgever-Opdrachtnemer) is het versterkte VISI-raamwerk gelezen. Derden kunnen niet in dit raamwerk komen(???). De

berichten worden aan IP-adressen/URL's van de servers van beide systemen ingesteld.

BW: b. zij maakt het mogelijk de ondertekenaar te identificeren.

VISI: bepaalde personen zijn gemachtigd met en voorzien van een login naam en een wachtwoord, er wordt gebruik gemaakt van een secure protocol met versleuteling die ook door banken wordt gebruikt. De gemachtigde heeft een bepaalde rol in VISI en kan alleen transacties verrichten die aan die rol gekoppeld zijn. Wanneer een bericht wordt verstuurd, wordt een aantal checks gedaan.

BW: c. zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;

VISI: ??

BW: d. zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;

VISI: nadat de berichten zijn verzonden en ontvangen is aanpassing van het bericht niet meer mogelijk.

BW: e. zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1, onderdeel ss, van de Telecommunicatiewet

VISI: heeft geen gekwalificeerd certificaat.

BW: f. zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel vv, van de Telecommunicatiewet.

VISI: heeft een dergelijk veilig middel niet.

Conclusie: VISI kan niet gelijk gesteld worden met de geavanceerde handtekening als bedoeld in art. 3:1a BW.

Dat brengt ons naar de volgende vraag:

Wat is de consequentie van deze vaststelling?

De consequentie lijkt niet zo groot te zijn. Het uitgangspunt van de wet is immers in art. 3:15a lid 3, dat ook al voldoet een elektronische handtekening niet aan de vereisten gesteld in lid 2 van dat artikel, daarmee niet gezegd kan worden dat deze handtekening niet voldoende betrouwbaar is.

De wijze waarop VISI beveiligd is, komt een heel eind in de richting van wat de wet vereist. Het is dus zeer wel denkbaar dat een rechter indien zich bewijsproblemen voordoen, de partij die zich beroept op de juistheid van de VISI elektronische handtekening het voordeel van de twijfel zal geven. Uiteraard met dien verstande dat de andere partij tegenbewijs mag leveren.

II. De Archiefwet en VISI

1. Inleiding

De Archiefwet stelt eisen aan archivering. Het werken in VISI leidt tot een vorm van archivering: voldoet deze wijze aan de Archiefwet? Dat is de vraag die in dit tweede deel van deze opdracht beantwoord zal worden. Daartoe wordt eerst uiteen gezet welke eisen de Archiefwet stelt en vervolgens hoe in VISI gearchiveerd wordt, waarna geoordeeld zal worden of beide methoden op elkaar aansluiten.

2. Achtergrond: hoofdlijnen van de Archiefwet

De Archiefwet bevat bepalingen omtrent vragen als: wie moet archiveren, hoe moet gearchiveerd worden, bepalingen omtrent vernietiging, een aanwijzing inzake het aanleggen van selectielijsten wat wel of geen archiefbescheiden zijn e.d. Deze wet wordt hier niet uit de doeken gedaan, slechts een paar punten van belang voor de verhouding met VISI zullen hier nader bekeken worden.

De belangen van de Archiefwet

Artikel 2 van het Archiefbesluit 19954 somt de verschillende belangen op waarmee bij de selectie van overheidsarchieven rekening dient te worden gehouden:

- de taak van het desbetreffende overheidsorgaan;
- de verhouding van dit overheidsorgaan tot andere overheidsorganen;
- de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed;
- en het belang van de in de archiefbescheiden voorkomende gegevens voor overheidsorganen, voor recht- en bewijszoekenden en voor historisch onderzoek.

Om in deze complexe omgeving wat duidelijkheid te verschaffen is een Commissie aan het werk gegaan die in 2007 met het rapport *Gewaardeerd Verleden*³⁶ is gekomen, waarin suggesties voor toekomstig archiveren worden gedaan, maar waar ook veel inzicht wordt geboden in de verplichtingen rond het archiveren van de verschillende overheden.

³⁶ Bouwstenen voor een nieuwe waarderingsmethodiek voor archieven, eindredactie: K.J.P.F.M. Jeurgens, A.C.V.M. Bongenaar, M.C. Windhorst

Begrip archiefbescheiden

In het rapport *Gewaardeerd Verleden* wordt op p. 17 opgemerkt dat het begrip archiefbescheiden als volgt veranderd is:

Onder archiefbescheiden werden verstaan al die bescheiden die, ongeacht hun vorm, naar hun aard bestemd zijn om te berusten onder de instelling, persoon of groep personen die deze heeft ontvangen of opgemaakt uit hoofde van zijn/haar activiteiten of vervulling van zijn/haar taken.

Recentelijk is er, onder invloed van automatisering van processen en digitalisering van de documenthuishouding, een verschuiving in de begripsbepaling opgetreden, waarbij de nadruk is komen te liggen op archief als procesgebonden informatie. Dit betekent: "informatie die door onderling samenhangende werkprocessen is gegenereerd en die zodanig door die werkprocessen is gestructureerd en vastgelegd dat ze vanuit de context van die werkprocessen kan worden bevraagd".

Wat zijn archiefbescheiden volgens de Regeling geordende en toegankelijke staat archiefbescheiden?

De Regeling geordende en toegankelijke staat archiefbescheiden geldt naar de letter alleen voor archiefbescheiden die ingevolge een selectielijst voor bewaring in aanmerking komen. Het documentair structuurplan is echter van toepassing op alle gegevens, zegt de toelichting op artikel 9. Letterlijk staat er het volgende: 'De in het eerste lid bedoelde gegevens (gegevens over de inhoud, structuur en vorm én gegevens aangaande de technische kenmerken van de informatie) zijn geen -te bewaren- archiefbescheiden in de zin van de Archiefwet 1995. Desalniettemin dienen de duurzaamheid van deze gegevens alsook de raadpleegbaarheid daarvan op dezelfde wijze als van de te bewaren archiefbescheiden te worden gewaarborgd. Het gaat immers om gegevens die juist op langere termijn noodzakelijk zijn om digitale archieven te ontsluiten.'

Conclusie: omdat ook deze informatie tijdens haar levensloop toegankelijk, vindbaar en leesbaar moet zijn, is het efficiënt om voor op termijn vernietigbare stukken hetzelfde regime te kiezen als voor de permanent te bewaren archiefbescheiden.

Keteninformatisering

In een tijd dat in de bouw het werken met Building Information Models opkomt, dient ook aan het begrip keteninformatisering aandacht te worden besteed. Ook hier wordt geciteerd uit het rapport Gewaardeerd Verleden, p. 17:

Keteninformatisering is een manier om geautomatiseerde informatieuitwisseling mogelijk te maken tussen samenwerkende, zelfstandige organisaties die als ketenpartner ieder een specifieke rol binnen samenhangende (werk)processen spelen. De ketenpartners delen informatie met elkaar, in beginsel zonder dat zij een gemeenschappelijke informatieinfrastructuur hebben, met het doel om te komen tot eenmalige opslag en meervoudig gebruik. Aangezien niet langer sprake is van een duidelijke archiefvormer die verantwoordelijk is voor het gehele proces van archiefvorming, dient een ketenverantwoordelijke aangewezen te worden. Een tweede doel van keteninformatisering is het digitaal ondersteunen van verschillende (geschakelde) dienstverleningsprocessen zodat de klant slechts één proces en daarmee een gestroomlijnde dienstverlening ervaart.

Wie zijn gehouden te archiveren?

Alle overheidsorganen zijn gehouden aan artikel 5 van de Archiefwet³⁷. Voor de lagere overheden betekent dit dat het College van B&W zorgdrager is voor de archieven van het gemeentelijk apparaat. Ook Waterschappen, Provincies en bijvoorbeeld de regionale Politieorganisaties vallen onder deze verplichting en uiteraard de Rijksoverheid.

Wat zijn bewaarcriteria?

Ook hier wordt het antwoord ontleend aan de studie Gewaardeerd Verleden, p. 47/48:

Neerslag wordt als potentieel behoudenswaardig aangemerkt wanneer de archiefvormers/ actoren:

³⁷ Artikel 51. De zorgdrager is verplicht tot het ontwerpen van selectielijsten waarin tenminste wordt aangegeven welke archiefbescheiden voor vernietiging in aanmerking komen.
2. De lijsten worden, nadat Onze minister de Raad voor cultuur, bedoeld in artikel 2a van de Wet op het specifiek cultuurbeleid, heeft gehoord, vastgesteld, voor zover het betreft:
a. archiefbescheiden van de Eerste en de Tweede Kamer der Staten-Generaal, de andere Hoge Colleges van Staat en het Kabinet van de Koning: bij koninklijk besluit, op voordracht van Onze minister, in overeenstemming met het betrokken overheidsorgaan;
b. archiefbescheiden van de ministeries: door Onze minister en Onze minister wie het mede aangaat;
c. archiefbescheiden van andere overheidsorganen: door Onze minister.
3. Een besluit tot vaststelling van een selectielijst wordt bekendgemaakt in de Staatscourant.

1. hetzij representatief zijn voor een groot aantal vergelijkbare actoren, hetzij bijzonder vanwege de uitzonderlijke of opzienbarende rol die zij gespeeld hebben;
2. een bepalende of althans invloedrijke rol hebben (gespeeld), waaronder archiefvormers die verstrekkende bevoegdheden en verantwoordelijkheden hebben (gehad) of die vernieuwend zijn (geweest);
3. in intensieve interactie met burgers werken of gewerkt hebben, en daarbij niet alleen routinematige handelingen verrichten, maar van geval tot geval afwegingen maken waaruit, door precedentwerking of jurisprudentie, nieuw of aangepast beleid kan voortvloeien;
4. structureel substantiële informatie vastleggen of vastgelegd hebben die relevant is voor kennis van segmenten van de samenleving. Te denken valt aan omvangrijke dataverzamelingen zoals CBS, CBP e.d. die opbouwen en beheren.

Hoe weet men concreet wat te archiveren?

Op grond van wederom artikel 5 van de Archiefwet is iedere zorgdrager verplicht tot het ontwerpen van een 'selectielijst', waar aangegeven wordt welke archiefbescheiden voor vernietiging in aanmerking komen. Voor de gemeenten is door de VNG het initiatief genomen om te komen tot een 'Selectielijst archiefbescheiden gemeentelijke en intergemeentelijke organen'. Uit deze publicatie, p. 9/10, citeer ik het volgende:

'In principe dienen archiefbescheiden bewaard te blijven op die plaats(en) die binnen het kader van verleende bevoegdheden, plichten en verantwoordelijkheden daarvoor in aanmerking komen. Hierbij dient in aanmerking genomen te worden de samenhang tussen de bij verschillende organisatieonderdelen voorkomende archiefbescheiden, zoals die in de fases van voorbereiding, beslissing en uitvoering ontstaan.

De bewaring geschiedt omwille van het belang van de in archiefbescheiden voorkomende gegevens voor de gemeentelijke en intergemeentelijke organen zelf, de recht- of bewijszoekende burger en het historisch onderzoek. De commissie heeft bij de samenstelling van deze lijst dit belang steeds onderkend.

In het algemeen kan gesteld worden dat archiefbescheiden die het gevoerde beleid ten aanzien van de taak kunnen karakteriseren, dienen te worden bewaard. Stukken die betrekking hebben op de dagelijkse uitvoering zullen in het algemeen niet voor bewaring in aanmerking komen, met uitzondering van bescheiden betreffende hoofdzaken van het verloop van de uitvoering. Ook bescheiden die overbodig zijn voor de kennis van de zaak en/of het vaststellen van verplichtingen hoeven niet bewaard te worden.

Dubbelen (dat wil zeggen kopieën en afschriften) van bescheiden behoeven niet gedurende de voorgeschreven termijn te worden bewaard. Zij kunnen worden vernietigd met uitzondering van de gevallen, waarin de originelen ontbreken dan wel op de dubbelen aantekeningen zijn geplaatst die niet op het origineel voorkomen, maar die

wel van belang zijn voor de afhandeling van de zaak. In dergelijke gevallen is wel sprake in de zin van archiefbescheiden in de zin van de Archiefwet 1995. Deze bescheiden moeten dus beoordeeld worden aan de hand van de criteria in de lijst vermeld. Ook zij gewezen op de specifieke voorwaarden gesteld aan dubbelen in hoofdstuk 3.7.

Burgerzaken en bevolking. Archiefbescheiden die in deze lijst afzonderlijk en in meer algemene zin worden genoemd kunnen in de gemeentelijke praktijk ook deel uitmaken van een meer specifieke categorie. In dat geval moet de bewaartermijn van die specifieke categorie aangehouden worden, als deze laatste langer is dan.

Desgewenst is steekproefsgewijze bewaring van vernietigbare archiefbescheiden mogelijk.

Deze lijst is niet limitatief. Archiefbescheiden die niet vallen onder de hoofdstukken 2 en 3 dienen te worden bewaard, totdat eventueel de selectielijst is aangepast.

De volgende categorieën archiefbescheiden, die op grond van de hoofdstukken 2 en 3 in principe voor vernietiging in aanmerking komen, dienen te worden bewaard:

- bescheiden betreffende zaken of gebeurtenissen met een voor de eigen organisatie uniek of bijzonder karakter;
- bescheiden die betrekking hebben op bijzondere tijdsomstandigheden of gebeurtenissen;
- bescheiden inzake objecten die door vorm of (vroegere) bestemming op zichzelf of voor de gemeente beeldbepalend, karakteristiek of van bijzondere aard zijn;
- bescheiden die een samenvatting zijn van gegevens, zoals bijvoorbeeld jaarverslagen, overzichten en statistieken;
- bescheiden inzake personen die op enig gebied van bijzondere betekenis (geweest) zijn;
- bescheiden die door een calamiteit verloren gegane stukken, die voor bewaring in aanmerking zouden zijn gekomen, kunnen vervangen;
- bescheiden betreffende individuele zaken die geleid hebben tot algemene regelgeving;
- bescheiden die bij daadwerkelijke vernietiging de logische samenhang van de te bewaren archiefbescheiden zouden verstoren;’.

Hoe moet digitaal gearchiveerd worden?

Om te weten welke wettelijke eisen gelden voor het digitaal archiveren dient de, als bijlage in zijn geheel opgenomen, Regeling Geordende en Toegankelijke Staat Archiefbescheiden te worden geraadpleegd. Voor een groot deel gaat het om verplichtingen die rusten op de formele zorgdrager, die aspecten blijven thans buiten beschouwing. De aandacht gaat vooral uit naar die aspecten die relevant zijn voor de ‘werkvloer’.

Van belang zijn met name de volgende aspecten.

In artikel 1 wordt onder f gedefinieerd wat digitale archiefbescheiden zijn:

digitale archiefbescheiden: archiefbescheiden die uitsluitend met behulp van besturings- of toepassingsprogrammatuur geraadpleegd kunnen worden;

In algemene zin wordt in artikel 2 over te bewaren archiefbescheiden bepaald:

De zorgdrager zorgt ervoor dat van elk van de archiefbescheiden te allen tijde kan worden vastgesteld:

- a. de inhoud, structuur en vorm bij het ontstaan, één en ander voor zover de inhoud, structuur en vorm kenbaar moesten zijn voor de uitvoering van het betreffende werkproces;
- b. op welk tijdstip en uit hoofde van welke taak of handeling het door het overheidsorgaan werd ontvangen of opgemaakt; en
- c. de samenhang met de andere door het overheidsorgaan ontvangen en opgemaakte archiefbescheiden.

De zorgdrager zorgt ervoor dat het archiefbeheerssysteem de toegankelijke staat van de archiefbescheiden waarborgt en wel zo dat, aldus artikel 4:

- a. elk van de archiefbescheiden binnen een redelijke termijn kan worden gevonden, hetzij aan de hand van een onderwerp dat in het stuk is behandeld, hetzij aan de hand van het werkproces uit hoofde waarvan het stuk is ontvangen of opgemaakt, hetzij aan de hand van de afzender, dan wel de datum en het nummer dat door de afzender aan het stuk is gegeven, hetzij aan de hand van het nummer waaronder het stuk bij het ontstaan is geregistreerd; en
- b. elk van de archiefbescheiden binnen een redelijke termijn leesbaar of waarneembaar te maken is.

En over het bewaren van digitale archiefbescheiden in het bijzonder bevat artikel 5 aanwijzingen over hoe om te gaan met wijzigingen in de besturingsprogrammatuur³⁸.

³⁸ Artikel 5.1. Indien een gereede kans bestaat dat, als gevolg van wijziging van besturingsprogrammatuur, toepassingsprogrammatuur of andere apparatuur, niet langer voldaan kan worden aan de artikelen 2, 3 en 4, zorgt de zorgdrager ervoor dat conversie dan wel migratie van digitale archiefbescheiden plaatsvindt.

2. Iedere conversie of migratie van digitale archiefbescheiden die niet geschiedt met inachtneming van de artikelen 2, 3 en 4, is een vervanging in de zin van artikel 7 van de Archiefwet 1995.

3. De zorgdrager maakt van de conversie of de migratie een verklaring op, die ten minste een specificatie van de geconverteerde of gemigreerde digitale archiefbescheiden bevat en waarin tevens is aangegeven op welke wijze en met welk resultaat getoetst is of na de conversie of migratie aan de artikelen 2, 3 en 4 is of kan worden voldaan.

Van groot belang is natuurlijk in welke standaard de gegevens opgeslagen dienen te worden. Zie daartoe artikel 6:

Digitale archiefbescheiden dienen, uiterlijk op het tijdstip van overbrenging, als bedoeld in de artikelen 12 en 13 van de Archiefwet 1995, te worden opgeslagen volgens de volgende standaarden:

- a. voor character sets: ASCII (ISO/IEC 8859-1) of Unicode (ISO/IEC 10646-1);
- b. voor tekstbestanden: Portable document format (PDF) of SGML dan wel XML vergezeld van een stylesheet (XSL, CSS) dan wel TIFF of PDF met de metadata in een XML-wrapper;
- c. voor CAD/CAM bestanden; Portable document format (PDF) en STEP (Standard for the exchange of product data) als metadata standaard (ISO 10303);
- d. voor images/beelden (bitmapped): Portable document format (PDF) en, indien gebruik gemaakt wordt van compressie: ITU T4 of ITU T6;
- e. voor databases: het oorspronkelijke opslagformaat of ASCII (flatfile, met veldscheidingstekens), vergezeld van documentatie bij voorkeur in XML-DTD over de structuur van de database, tenminste omvattende een compleet logisch datamodel met beschrijving van de entiteiten; queries dienen in de vraagtaal SQL (SQL2) te worden vastgelegd.

Artikel 8 legt een aantal zorgplichten op de zorgdrager van het archief, neerkomend op een soort administratie inzake de :

1. De zorgdrager zorgt ervoor, dat de functionele eisen ten aanzien van de inhoud, structuur en vorm, bedoeld in artikel 2, worden vastgelegd.
2. De zorgdrager zorgt voor de bewaring van de toepassingsprogrammatuur, met inbegrip van de nieuwere versies, voorzover dat nodig is om aan de artikelen 2, 3 of 4 te voldoen.
3. In voorkomende gevallen zorgt de zorgdrager ervoor dat hij beschikt over de noodzakelijke licenties met betrekking tot de in het tweede lid genoemde toepassingsprogrammatuur.

Tot slot wordt gewezen op artikel 9, dat een gedetailleerde regeling bevat er op gericht dat de gegevens bewaard in digitale vorm, terug te vinden zijn:

1. De zorgdrager zorgt voor het vastleggen en het bewaren van tenminste de volgende gegevens:

- a. de benaming van de toepassingsprogrammatuur waarmee de digitale archiefbescheiden zijn ontvangen en opgemaakt, inclusief het versienummer;
 - b. de beschrijving van het platform, met naam en versie van de besturingsprogrammatuur en met naam en type van de apparatuur;
 - c. de documentatie die aangeeft hoe de toepassingsprogrammatuur heeft gewerkt met inbegrip van de nieuwere versies;
 - d. een beschrijving van de opgeslagen bestanden, omfattende ten minste de volgende gegevens:
 - 1^o. de naam van het overheidsorgaan dat de digitale archiefbescheiden heeft ontvangen en opgemaakt en de benaming van het werkproces waarbinnen de digitale archiefbescheiden zijn ontvangen en opgemaakt;
 - 2^o. de benaming en omvang van elk opgeslagen bestand;
 - 3^o. een specificatie van de digitale archiefbescheiden met begin- en einddatum;
 - 4^o. de relatie met andere bestanden;
 - 5^o. het opslagformaat;
 - 6^o. in voorkomende gevallen de toegepaste compressiemethode;
 - 7^o. de datum en het tijdstip van de opslag van het bestand op de gegevensdrager;
 - 8^o. in geval van een database: de documentatie over de structuur, tenminste omfattende een compleet logisch datamodel met beschrijving van de entiteiten.
2. Op de in het eerste lid bedoelde gegevens zijn deze regeling en de Regeling duurzaamheid archiefbescheiden van overeenkomstige toepassing.

Samengevat komt het voorgaande neer op het volgende:

- Digitale archiefbescheiden moeten in een bepaalde standaard worden opgeslagen, voordat ze worden overgebracht naar een archiefbewaarplaats (Artikel 6 Regeling geordende en toegankelijke staat archiefbescheiden).
- Archiefbescheiden op CD-ROMs moeten worden overgezet op nieuwe dragers, zodra het gevaar dreigt dat de informatie verloren gaat of niet meer leesbaar zal zijn. Dit gevaar ontstaat als de materialen niet duurzaam zijn, maar ook als de bijbehorende apparatuur in onbruik raakt (Artikel 8 Regeling duurzaamheid archiefbescheiden).
- Van de digitale archiefbescheiden dienen bepaalde gegevens vast gelegd te worden, zoals de benaming van de toepassingsapparatuur; de beschrijving van het platform; een beschrijving van de werking van de toepassingsprogrammatuur; een beschrijving van de opgeslagen bestanden (Artikel 9 Regeling geordende en toegankelijke staat archiefbescheiden).
- De archiefbescheiden moeten goed toegankelijk en terug te vinden zijn.

3. De praktijk

Navraag leert dat in de praktijk de wet- en regelgeving nader vorm is gegeven in zogenaamde Bedrijfs Management Systemen, Document Management Systemen en specifieke archiveringssystemen en document registratiesystemen zoals 'Walvis'. Geconstateerd wordt dat de uitwerking van deze systemen per dienst of stadsdeel kan verschillen. Wel lijkt de indruk gerechtvaardigd, aldus de zegsliden, dat met deze systemen aan de wet- en regelgeving wordt voldaan.

In de praktijk blijkt voorts dan indien met VISI wordt gewerkt het VISI dossier leidend is: alle documenten worden daarin opgeslagen en op een enkele uitzondering na (bijvoorbeeld betreffende de de formele opdrachtverlening) ook alleen daarin. Na afloop van een project wordt van het VISI dossier een HTML export gemaakt die gezippt in het centrale gemeentelijk Documentatie Management Systeem wordt geplaatst. Dit impliceert dus dat er twee stappen gezet worden: eerst wordt in VISI gewerkt en daarna wordt alles nog eens overgezet. Het streven is er opgericht om de tweede stap overbodig te maken en wel zo dat de VISI documenten direct in het DMS terecht komen. Dit vereist echter een technische aanpassing.

4. VISI 'archivering'

Tijdens het werken in een bepaald project met VISI is de uitwisseling en vastlegging van informatie gedetailleerd geregeld. Daarnaast is ook de technische kant nauwgezet omschreven, zodat alle informatie terug te vinden is en niet dan wel vrijwel niet te manipuleren door daartoe niet bevoegde personen. Van belang is voorts dat na afloop van het project een deel van de informatie die met behulp van VISI is gegenereerd digitaal wordt opgeslagen op een dvd, die aan de betrokken 'stakeholders' ter beschikking wordt gesteld. De informatie is alsdan technisch zo opgeslagen dat wijzigingen niet meer zijn aan te brengen.

Werken met VISI betekent dat aan de eisen genoemd in de Geordende en Toegankelijke Staat Archiefbescheiden als volgt is voldaan:

Artikel 4a.: Terugvinden van de archiefbescheiden binnen een redelijke termijn kan worden gevonden:

Het werken met VISI is iets dat eindig is per project. De vraag die hier aan de orde is, is of na afloop van een project de alsdang opgeslagen informatie binnen redelijke termijn is terug te vinden. Strikt genomen heeft deze vraag geen betrekking op het werken met VISI, maar op de vraag: wat doen partijen met de in VISI tot stand gekomen informatie

nadat het project is opgeleverd, althans geëindigd. Laat men bij wijze van spreken de drager van de met VISI gegenereerde informatie in een la liggen, of wordt de informatie in een willekeurige map met een onduidelijke naam in iemands eigen pc opgeslagen, dan zal de informatie waarschijnlijk niet binnen redelijke termijn terug te vinden zijn (zo die al terug te vinden is). Maar dat probleem is niet inherent aan het werken met VISI.

b. binnen een redelijke termijn leesbaar of waarneembaar maken van archiefbescheiden:

Projecten waarbinnen gecommuniceerd is overeenkomstig VISI worden wat de communicatie betreft 'afgesloten' door middel van het vastleggen van de uitgewisselde informatie op een DVD dan wel CD, welke dragers afkomstig zijn van de leveranciers van de software. In ontwikkeling is het bewaren van deze gegevens online. Ervaringen tot nu toe, afkomstig van de gemeente Amsterdam, laten zien dat het lezen probleemloos verloopt.

Artikel 6: gebruikte standaard van VISI komt overeen met:

Vanuit de gemeente Amsterdam wordt op dit punt gereageerd met de opmerking, dat de software waarmee met VISI gewerkt kan worden (nogmaals: deze software komt van onafhankelijke daarin gespecialiseerde bedrijven) lijkt te voldoen aan de in artikel 6 gestelde eisen. Een zeker antwoord kan evenwel alleen geleverd worden door de technische specialisten op dit gebied.

Artikel 8:

lid 1: functionele eisen ten aanzien van inhoud e.d. zijn vastgelegd; lid 2: toepassingsprogrammatuur wordt bewaard; lid 3: beschikken over licenties:

Ook deze zorgplichten staan los van het werken in VISI zelf, maar hebben betrekking op verplichtingen hoe de in VISI gegenereerde en vastgelegde informatie 'software/hardware-matig' te bewaren en het bevoegd zijn van deze technische ondersteuningsmiddelen gebruik te mogen maken (licenties). Gegeven de uitgebreidheid van de informatie rond het werken met VISI wordt door schrijver dezes aangenomen dat deze punten door degenen die VISI ter beschikking stellen onder ogen zijn gezien.

Artikel 9:

1. a. Benaming toepassingsprogrammatuur:
 - b. beschrijving platform:
 - c. hoe werkte de programmatuur:

d. beschrijving van de opgeslagen bestanden, omfattende de gegevens gevraagd in deze bepaling (zie hierboven):

De aspecten die in artikel 9 aan de orde komen, zijn eveneens van zuiver technische aard. Ook hier wordt aangenomen dat vanuit de achtergrond waaruit VISI ter beschikking wordt gesteld, aandacht is geschonken aan deze feitelijke kwesties.

5. Concluderend

De wet- en regelgeving legt op de overheid bepaalde verplichtingen inzake wat te archiveren en hoe te archiveren. VISI is een communicatie middel en staat als zodanig los van deze wet- en regelgeving gelijk bijvoorbeeld via de telefoon gecommuniceerde inhoud los staat van deze verplichtingen. Het werken in een project met VISI resulteert evenwel in het opslaan van informatie, welke informatie wel binnen deze wet- en regelgeving komt wat de inhoud betreft en wat de wijze van opslaan betreft. Het opslaan van de informatie nadat een project in VISI is voltooid, dient te gebeuren overeenkomstig de regelgeving. De wijze waarop dit in VISI gebeurt komt voor zover nagegaan kon worden overeen met de eisen die technisch aan het opslaan worden gesteld. Uiteraard is het aan degenen belast met een archieftaak om daaraan feitelijk uitvoering te geven. Het feit dat in VISI gewerkt is, staat hier aan niet in de weg, sterker: helpt de bewaarder vergaand op weg.

III. Bijlage

Regeling geordende en toegankelijke staat archiefbescheiden

De Staatssecretaris van Onderwijs, Cultuur en Wetenschappen, dr. F. van der Ploeg;

Gelet op artikel 12 van het Archiefbesluit 1995,

Besluit:

§ 1. Begrippen

Artikel 1.1. In deze regeling wordt verstaan onder:

- a. archiefbeheerssysteem: een geheel van mensen, methoden, procedures, gegevensverzamelingen, opslag-, verwerkings- en communicatieapparatuur en andere middelen, bestemd tot het beheer van archiefbescheiden;
- b. archiefbescheiden: archiefbescheiden als bedoeld in artikel 12 van het Archiefbesluit 1995;
- c. bestand: een geheel van gegevens in een zelfde opslagformaat;
- d. besturingsprogrammatuur: de programmatuur die bestemd is ter besturing van een informatiesysteem;
- e. conversie: het omzetten in of het overzetten van gegevens in een ander opslagformaat;
- f. digitale archiefbescheiden: archiefbescheiden die uitsluitend met behulp van besturings- of toepassingsprogrammatuur geraadpleegd kunnen worden;
- g. documentair structuurplan: een plan waarin is vastgelegd de wijze waarop de toegankelijkheid van archiefbescheiden is georganiseerd en de wijze waarop archiefbescheiden zijn ingedeeld en gerangschikt;
- h. handeling: een complex van activiteiten ter vervulling van een taak of op grond van een bevoegdheid;
- i. migratie: het overzetten van gegevens en toepassingsprogrammatuur naar een ander platform;
- j. ontstaan: het moment dat archiefbescheiden door een overheidsorgaan worden ontvangen of opgemaakt als naar hun aard bestemd om daaronder te berusten;
- k. opslagformaat: de code volgens welke gegevens op een gegevensdrager zijn opgeslagen;
- l. platform: geheel van apparatuur en besturingsprogrammatuur waarop de toepassingsprogrammatuur werkt;
- m. structuur: het logische verband tussen de elementen van een document of van een archief;
- n. toepassingsprogrammatuur: de programmatuur die bestemd is voor de ondersteuning van de uitvoering van een werkproces;
- o. vorm: de uiterlijke verschijning waarin de structuur en opmaak zichtbaar zijn;

p. werkproces: de uitvoering van de taak of handeling uit hoofde waarvan archiefbescheiden door een overheidsorgaan worden ontvangen of opgemaakt als naar hun aard bestemd om daaronder te berusten.

2. Met de in deze regeling genoemde technische producteisen worden gelijkgesteld technische producteisen die worden gesteld in een andere lidstaat van de Europese Unie dan wel in een staat die partij is bij de overeenkomst inzake de Europese Economische Ruimte, en die ten minste een gelijkwaardige productkwaliteit waarborgen, mits daarbij een geldig rapport wordt overgelegd, waaruit blijkt dat de producten aan die eisen voldoen en dat rapport is opgemaakt door een proevenlaboratorium dat voldoet aan NEN-EN-ISO/IEC17025.

§ 2. Te bewaren archiefbescheiden in het algemeen

Artikel 2. De zorgdrager zorgt ervoor dat van elk van de archiefbescheiden te allen tijde kan worden vastgesteld:

- a. de inhoud, structuur en vorm bij het ontstaan, één en ander voor zover de inhoud, structuur en vorm kenbaar moesten zijn voor de uitvoering van het betreffende werkproces;
- b. op welk tijdstip en uit hoofde van welke taak of handeling het door het overheidsorgaan werd ontvangen of opgemaakt; en
- c. de samenhang met de andere door het overheidsorgaan ontvangen en opgemaakte archiefbescheiden.

Artikel 3. De zorgdrager zorgt ervoor dat de onder hem ressorterende overheidsorganen beschikken over een actueel, compleet en logisch samenhangend overzicht, geordend overeenkomstig het ten tijde van de vorming van het archief daarvoor geldende documentaire structuurplan, van:

- a. de bij dat overheidsorgaan berustende archiefbescheiden; en
- b. de bestanden waarin deze bewaard worden, met daarin tenminste de in artikel 9 bedoelde gegevens, alsmede de verblijfplaats van de archiefbescheiden.

Artikel 4. De zorgdrager zorgt ervoor dat het archiefbeheerssysteem de toegankelijke staat van archiefbescheiden waarborgt, zodanig dat:

- a. elk van de archiefbescheiden binnen een redelijke termijn kan worden gevonden, hetzij aan de hand van een onderwerp dat in het stuk is behandeld, hetzij aan de hand van het werkproces uit hoofde waarvan het stuk is ontvangen of opgemaakt, hetzij aan de hand van de afzender, dan wel de datum en het nummer dat door de afzender aan het stuk is gegeven, hetzij aan de hand van het nummer waaronder het stuk bij het ontstaan is geregistreerd; en
- b. elk van de archiefbescheiden binnen een redelijke termijn leesbaar of waarneembaar te maken is.

§ 3. Te bewaren digitale archiefbescheiden in het bijzonder

Artikel 5.1. Indien een gereede kans bestaat dat, als gevolg van wijziging van besturingsprogrammatuur, toepassingsprogrammatuur of andere apparatuur, niet langer voldaan kan worden aan de artikelen 2, 3 en 4, zorgt de zorgdrager ervoor dat conversie dan wel migratie van digitale archiefbescheiden plaatsvindt.

2. Iedere conversie of migratie van digitale archiefbescheiden die niet geschiedt met inachtneming van de artikelen 2, 3 en 4, is een vervanging in de zin van artikel 7 van de Archiefwet 1995.

3. De zorgdrager maakt van de conversie of de migratie een verklaring op, die ten minste een specificatie van de geconverteerde of gemigreerde digitale archiefbescheiden bevat en waarin tevens is aangegeven op welke wijze en met welk resultaat getoetst is of na de conversie of migratie aan de artikelen 2, 3 en 4 is of kan worden voldaan.

Artikel 6. Digitale archiefbescheiden dienen, uiterlijk op het tijdstip van overbrenging, als bedoeld in de artikelen 12 en 13 van de Archiefwet 1995, te worden opgeslagen volgens de volgende standaarden:

- a. voor character sets: ASCII (ISO/IEC 8859-1) of Unicode (ISO/IEC 10646-1);
- b. voor tekstbestanden: Portable document format (PDF) of SGML dan wel XML vergezeld van een stylesheet (XSL, CSS) dan wel TIFF of PDF met de metadata in een XML-wrapper;
- c. voor CAD/CAM bestanden; Portable document format (PDF) en STEP (Standard for the exchange of product data) als metadata standaard (ISO 10303);
- d. voor images/beelden (bitmapped): Portable document format (PDF) en, indien gebruik gemaakt wordt van compressie: ITU T4 of ITU T6;
- e. voor databases: het oorspronkelijke opslagformaat of ASCII (flatfile, met veldscheidingstekens), vergezeld van documentatie bij voorkeur in XML-DTD over de structuur van de database, tenminste omvattende een compleet logisch datamodel met beschrijving van de entiteiten; queries dienen in de vraagtaal SQL (SQL2) te worden vastgelegd.

Artikel 7. De ordening en toegankelijkheid van digitale archiefbescheiden, zoals gerealiseerd door middel van toepassingsprogrammatuur, maken onverbreekelijk onderdeel uit van de archiefbescheiden waarop ze betrekking hebben.

Artikel 8.1. De zorgdrager zorgt ervoor, dat de functionele eisen ten aanzien van de inhoud, structuur en vorm, bedoeld in artikel 2, worden vastgelegd.

2. De zorgdrager zorgt voor de bewaring van de toepassingsprogrammatuur, met inbegrip van de nieuwere versies, voorzover dat nodig is om aan de artikelen 2, 3 of 4 te voldoen.

3. In voorkomende gevallen zorgt de zorgdrager ervoor dat hij beschikt over de noodzakelijke licenties met betrekking tot de in het tweede lid genoemde toepassingsprogrammatuur.

Artikel 9.1. De zorgdrager zorgt voor het vastleggen en het bewaren van tenminste de volgende gegevens:

- a. de benaming van de toepassingsprogrammatuur waarmee de digitale archiefbescheiden zijn ontvangen en opgemaakt, inclusief het versienummer;
 - b. de beschrijving van het platform, met naam en versie van de besturingsprogrammatuur en met naam en type van de apparatuur;
 - c. de documentatie die aangeeft hoe de toepassingsprogrammatuur heeft gewerkt met inbegrip van de nieuwere versies;
 - d. een beschrijving van de opgeslagen bestanden, omfattende ten minste de volgende gegevens:
 - 1^o. de naam van het overheidsorgaan dat de digitale archiefbescheiden heeft ontvangen en opgemaakt en de benaming van het werkproces waarbinnen de digitale archiefbescheiden zijn ontvangen en opgemaakt;
 - 2^o. de benaming en omvang van elk opgeslagen bestand;
 - 3^o. een specificatie van de digitale archiefbescheiden met begin- en einddatum;
 - 4^o. de relatie met andere bestanden;
 - 5^o. het opslagformaat;
 - 6^o. in voorkomende gevallen de toegepaste compressiemethode;
 - 7^o. de datum en het tijdstip van de opslag van het bestand op de gegevensdrager;
 - 8^o. in geval van een database: de documentatie over de structuur, tenminste omfattende een compleet logisch datamodel met beschrijving van de entiteiten.
- 2.Op de in het eerste lid bedoelde gegevens zijn deze regeling en de Regeling duurzaamheid archiefbescheiden van overeenkomstige toepassing.

§ 4. Overgangs- en slotbepalingen

Artikel 10.1. De artikelen 2, 4, 5, 6 en 8 zijn niet van toepassing op digitale archiefbescheiden in bestanden waaraan sedert 1 januari 1996 geen gegevens zijn toegevoegd of waarin sedert 1 januari 1996 geen gegevens zijn gewijzigd.

2. Indien een gerede kans bestaat dat als gevolg van wijziging van besturingsprogrammatuur, toepassingsapparatuur of apparatuur de in het eerste lid bedoelde archiefbescheiden niet binnen een redelijke termijn leesbaar of waarneembaar te maken zijn, zorgt de zorgdrager ervoor dat conversie dan wel migratie van die archiefbescheiden plaatsvindt met inachtneming van de standaarden, genoemd in artikel 6.

3. De zorgdrager maakt van de conversie dan wel de migratie, bedoeld in het tweede lid, een verklaring op, die ten minste een specificatie van de geconverteerde dan wel gemigreerde archiefbescheiden bevat en waarin tevens is aangegeven op welke wijze en met welk resultaat getoetst is of na de conversie of migratie de leesbaarheid of waarneembaarheid is gewaarborgd.

4. Na verkregen instemming van de Minister van Onderwijs, Cultuur en Wetenschappen dan wel, indien het archiefbescheiden betreft voor de bewaring waarvan een andere dan een rijksarchiefbewaarpplaats is aangewezen, na verkregen instemming van gedeputeerde staten,

kunnen de artikelen 2, 4, 5, 6 en 8 buiten toepassing blijven ten aanzien van sedert 1 januari 1996 ontvangen en opgemaakte digitale archiefbescheiden in bestanden waaraan sedert de datum van inwerkingtreding van deze regeling geen gegevens zijn toegevoegd of waarin sedert die datum geen gegevens zijn gewijzigd.

5. Ten aanzien van archiefbescheiden als bedoeld in het vierde lid waarop de artikelen 2, 4, 5, 6 en 8 met instemming van de Minister van Onderwijs, Cultuur en Wetenschappen dan wel van gedeputeerde staten niet van toepassing zijn, zijn het tweede en het derde lid van overeenkomstige toepassing.

6. Aan de instemming, bedoeld in het vierde lid, kunnen voorwaarden worden verbonden.

Artikel 11.1. Op andere dan de in artikel 10 bedoelde, bij de inwerkingtreding van dit besluit bestaande, digitale archiefbescheiden zijn de artikelen 2, 4, 5 en 8, eerste lid, tot 1 januari 2004 niet van toepassing.

2. Indien een gereede kans bestaat dat als gevolg van wijziging van besturingsapparatuur, toepassingsapparatuur of andere apparatuur, de in het eerste lid bedoelde archiefbescheiden niet binnen een redelijke termijn leesbaar of waarneembaar zijn, of niet langer voldaan wordt aan artikel 3, zorgt de zorgdrager ervoor dat conversie dan wel migratie van de archiefbescheiden plaatsvindt met inachtneming van de standaarden, genoemd in artikel 6.

3. Artikel 10, derde lid, is van overeenkomstige toepassing.

Artikel 12 Deze regeling treedt in werking met ingang van de tweede dag na de dagtekening van de Staatscourant waarin zij wordt geplaatst.

Artikel 13. Deze regeling wordt aangehaald als: Regeling geordende en toegankelijke staat archiefbescheiden.