ATTRIBUUT-GEBASEERDE ELEKTRONISCHE HANDTEKENINGEN EN DE EIDAS-VERORDENING

W.Y. Hu, F.M.J. Van den Broek, B.P.F. Jacobs & P.T.J. Wolters[1]

1. Inleiding

Handtekeningen zijn onmisbaar op juridisch vlak, bijvoorbeeld voor het tot stand brengen van een akte[2] of het aangaan van een non-concurrentiebeding.[3] Dergelijke handtekeningen worden vaak in traditionele vorm gezet, de zogenoemde 'natte' handtekening. Handtekeningen kunnen daarnaast ook in elektronisch vorm geschieden.[4] Door de Covid-19 crisis moesten veel zaken noodgedwongen online plaatsvinden en is het gebruik van elektronische handtekeningen sterk toegenomen.[5]

In het recht is een (elektronische) handtekening in de eerste plaats een middel om in te stemmen met een overeenkomst of de inhoud van een document.[6] Deze beschrijving is bij elektronische handtekeningen, net zo min als bij natte handtekeningen, niet beperkt tot handtekeningen die

---

1 W.Y. (Yong Yong) Hu is als promovenda verbonden aan het Onderzoekscentrum Onderneming & Recht en de iHub van de Radboud Universiteit. F.M.J. (Fabian) van den Broek is universitair docent bij de Open Universiteit van Nederland en gastonderzoeker aan de Radboud Universiteit en de iHub. B.P.F. (Bart) Jacobs is hoogleraar beveiliging, privacy en identiteit bij de iHub van de Radboud Universiteit. P.T.J. (Pieter) Wolters is universitair hoofddocent burgerlijk recht en onderzoeker bij het Onderzoekcentrum Onderneming & Recht en de iHub van de Radboud Universiteit.

2 Zie art. 156 lid 1 Rv waarin is bepaald dat een akte ondertekend dient te worden.

3 Art. 7:653 lid 1 BW; HR 28 maart 2008, ECLI:NL:HR:2008BC0384, r.o. 3.4, *NJ* 2008/503 (*Philips/Oostendorp*); HR 3 maart 2017, ECLI:NL:HR:2017:364, r.o. 3.4.2, *NJ* 2017/126. Een handtekening wordt niet door de wet voorgeschreven, maar wordt door de Hoge Raad genoemd als wijze om aan het schriftelijkheidsvereiste te voldoen.

4 Verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU* 2014, L 257/73).

5 W. Heck, 'Lockdown geeft digitale handtekening rugwind', *NRC.nl* 16 april 2020; R. Betlem, 'Virus geeft digitalisering van banken een boost', *FD.nl* 4 mei 2020.

6 Zie voor een beschrijving van (elektronische) handtekeningen ook T.F.E. Tjong Tjin Tai, 'art. 3:15a BW, aant. 4.2', in: J. Hijma (red.), *Groene Serie Vermogensrecht*, Deventer: Wolters Kluwer (online, bijgewerkt op 24 januari 2019).

voldoen aan bepaalde beveiligingseisen. Het juridische begrip elektronische handtekening moet echter worden onderscheiden van het restrictieve (technische) begrip '*digitale* handtekening'. Identiteitsmanagement beschouwt een digitale handtekening als een cryptografische constructie die een bericht in elektronische vorm bindt aan de ondertekenaar. Deze cryptografische verbinding geschiedt in de regel met certificaatgebaseerde digitale handtekeningen (*Certificate Based Signatures*, 'CBS'), waarbij een ondertekend bericht met behulp van een *public-key certificate* wordt gekoppeld aan een individueel herleidbare ondertekenaar.[7] Dergelijke handtekeningen zijn echter inflexibel. Het certificaat geeft altijd precies dezelfde (volledige) informatie over de ondertekenaar, zelfs als deze informatie niet noodzakelijk is. Het is bijvoorbeeld niet altijd vereist (of voldoende) dat een ondertekenaar is terug te leiden naar een individu. In sommige situaties is het vooral van belang dat hij een bepaald attribuut bezit, zoals een vereiste minimale (of maximale) leeftijd of de bevoegdheid om een bedrijf te vertegenwoordigen. In een dergelijk geval kan ook gebruik worden gemaakt van attribuut-gebaseerde digitale handtekeningen (*Attribute Based Signatures*, 'ABS'), waarbij er een koppeling wordt gemaakt tussen de digitale handtekening en een of meer specifieke attributen (persoonlijke kenmerken).

Op Europees niveau geeft de eIDAS-verordening het juridisch kader voor elektronische handtekeningen.[8] Dit kader ziet zowel op 'gewone' elektronische handtekeningen, als op 'geavanceerde' of 'gekwalificeerde' elektronische handtekeningen met cryptografische waarborgen. Deze verordening gaat, in het bijzonder met betrekking tot de gekwalificeerde elektronische handtekeningen in beginsel uit van CBS. Het is dan ook de vraag in hoeverre ABS verenigbaar zijn met het stelsel van de eIDAS-verordening. Deze vraag is in het bijzonder van belang in het licht van de herziening van de eIDAS-verordening door de Europese Commissie.[9] Deze herziening is een geschikt moment om ABS en andere alternatieve vormen van digitale handtekeningen beter te faciliteren. Zij wordt dan ook

7 C. Adams & S. Lloyd, *Understanding public-key infrastructure: concepts, standards, and deployment considerations*, New Riders Pub. 1999, p. 17-18.

8 Verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*PbEU* 2014, L 257/73). Zie nader §3.1.

9 Europese Commissie, *eIDAS Open Public Consultation*, 24 juli 2020 – 2 oktober 2020, ec.europa.eu/digital-single-market/en/news/eidas-open-public-consultation. De publieke consultatie over de eIDAS-verordening is op 2 oktober 2020 gesloten.

expliciet genoemd bij de *Inception Impact Assessment* en in het voorstel van de Europese Commissie omtrent een nieuwe Europese digitale identiteit.[10]

Dit artikel zet allereerst uiteen wat vanuit technisch oogpunt wordt verstaan onder digitale handtekeningen (§2). Daarbij gaan wij in op de algemene eigenschappen van een digitale handtekening, de kenmerken van ABS en de verschillen met CBS. Paragraaf 3 gaat vervolgens in op wat volgens het recht, en in het bijzonder volgens de eIDAS-verordening, wordt verstaan onder een (elektronische) handtekening. Aan de hand van verschillende use cases brengen wij de voordelen en grenzen van het gebruik van ABS in kaart (§4). Aan de hand van deze use cases analyseren wij of en hoe (niet-identificerende) ABS in de eIDAS-verordening passen (§5). Wij sluiten af met een conclusie (§6).

2. Digitale handtekeningen vanuit technisch perspectief

2.1 Identiteit vanuit een technisch perspectief

Identity Management ('IdM') is een subgebied van computerbeveiliging dat zich bezig houdt met het systematische beheer van digitale identiteiten.[11] Het ziet onder andere op authenticatie, *tracking* en *auditing*, privacy en gegevensbescherming en *life cycle management* (creëren, onderhouden en verwijderen van elektronische identiteiten).[12] Drie basisbegrippen binnen IdM zijn identificatie, authenticatie en autorisatie.[13] Identificatie gaat over het vertellen wie je bent, bijvoorbeeld door een persoonsnaam, inlognaam of bankrekeningnummer op te geven. Bij authenticatie gaat het erom te bewijzen wie (of wat) je bent. Technieken voor authenticatie zijn onder andere wachtwoorden (iets wat je weet), keycards (iets wat je hebt) of biometrie (iets wat je bent). Tweefactor-authenticatie vereist twee van deze drie factoren. De sterkte van de authenticatie is van belang voor de

10 Europese Commissie, *Proposal for a European Digital Identity (EUid) and Revision of the eIDAS Regulation. Inception Impact Assessment*, Ares(2020)3899583, p. 3-6; Europese Commissie, Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) betreffende het instellen van een kader voor een Europese digitale identiteit, COM(2021)281 def.

11 B.P.F. Jacobs, 'Attributen in plaats van identiteiten', *IT-Auditor* 2013, afl. 1, p. 29; OECD, *Digital Identity Management. Enabling Innovation and Trust in the internet Economy*, 2011, p. 143,oecd.org/sti/interneteconomy/49338380.pdf.

12 ISO/IEC 24760-1, Information Technology-security techniques – a framework for Identity Management – part I: terminology and concepts, 2011.

13 Jacobs 2013, p. 29-35.

betrouwbaarheidsniveaus die kunnen worden geboden.[14] Autorisatie gaat over wat je mag doen, als je eenmaal bent geauthentiseerd. Voorbeelden van autorisatie zijn bijvoorbeeld dat alleen personen boven de 18 jaar alcohol kunnen kopen[15] en enkel studenten korting krijgen bij het kopen van studieboeken.[16]

IdM definieert een identiteit als een attribuut – of een verzameling attributen – dat een persoon op unieke wijze identificeert binnen een bepaalde context, voor een bepaalde periode en met een zekere mate van betrouwbaarheid.[17] Het is echter ook mogelijk om niet de identificatie maar de attributen centraal te stellen. Een identiteit bestaat in deze benadering uit een verzameling van alle attributen die op een bepaald moment van toepassing zijn. Verschillende delen van deze identiteit kunnen in verschillende situaties worden onthuld door alleen die attributen te delen die in die specifieke situatie relevant zijn. Dergelijke op attributen gebaseerde benaderingen worden steeds prominenter in IdM. Niet alleen omdat ze veel flexibiliteit bieden, maar ook omdat ze privacyvriendelijk zijn. Zij beperken de verspreiding van informatie over iemands identiteit tot de situaties waarin dit noodzakelijk of gewenst is en zorgen hiermee voor dataminimalisatie en contextuele integriteit.[18]

2.2 Attribuut

Een attribuut is persoonlijke informatie die een kenmerk van een individu beschrijft.[19] Voorbeelden zijn geslacht, leeftijdsgrenzen (ofwel exact, "21 jaar", ofwel in relatie tot een limiet, zoals "ouder dan 18"), e-mail- of woonadres en persoonlijke nummers. Een '*identifier*' is een attribuut dat unieke identificatie mogelijk maakt.[20] Het gaat dan bijvoorbeeld om attributen zoals een paspoortnummer, socialezekerheidsnummer, e-mailadres of mobiele telefoonnummer. Een (volledige) naam is vaak alleen in combinatie met andere attributen (zoals een adres of geboortedatum)

14 In art. 8 eIDAS-verordening zijn de verschillende betrouwbaarheidsniveau 's voor elektronische identificatiemiddelen vastgelegd.
15 Art. 20 Drank- en Horecawet.
16 Art. 13 sub b Wet op de vaste boekenprijs.
17 E. Bertino & K. Takashashi, *Identity Management: Concepts, Technologies, and Systems*, Norwood: ARTECH HOUSE 2011, p. 11-12, 21.
18 Zie over dataminimalisatie §5. Zie over contextuele integriteit H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford: Stanford University Press 2010, p. 3-4.
19 Bertino & Takashashi 2011, p. 22.
20 Bertino & Takashashi 2011, p. 21.

uniek identificerend. Het is immers mogelijk dat ook anderen dezelfde naam hebben. Andere attributen, zoals geslacht of nationaliteit, zijn niet uniek identificerend. Attributen kunnen zowel voor persoonlijke als voor professionele doeleinden worden gebruikt. Vooral in een professionele context zijn attributen van belang om rollen binnen een organisatie uit te drukken. Zo kan een medische registratie een attribuut vormen dat kan worden gebruikt om aan te tonen dat iemand een arts (of ander medisch personeel) is. Binnen organisaties worden autorisaties vaak gekoppeld aan rollen: een persoon kan bijvoorbeeld enkel medicijnen voorschrijven en deze toevoegen aan het dossier van een patiënt als hij kan aantonen dat hij een behandelend arts is.

Een voorbeeld van een IdM-systeem op basis van attributen is IRMA. IRMA is een portemonnee-app die door gebruikers kan worden gevuld met persoonlijke attributen uit betrouwbare bronnen.[21] Dit proces wordt nader beschreven in paragraaf 2.4. De persoonlijke attributen worden beveiligd opgeslagen in de IRMA app op het persoonlijke toestel (telefoon of tablet) en voor toegang is een eigen PIN vereist. De gebruiker kan deze attributen vervolgens tonen, bijvoorbeeld om een handtekening te zetten (§2.4) of om gebruik te maken van bepaalde diensten. In dit proces krijgt de ontvanger de attributen van de gebruiker en wordt cryptografisch afgedwongen dat deze zijn uitgegeven door vertrouwde instanties en dat deze sinds de uitgave niet zijn verlopen of gewijzigd. Een gebruiker die alcohol wil kopen, kan bijvoorbeeld zijn attribuut "ouder dan 18 jaar" tonen ter bevestiging.

IRMA wordt in dit artikel als voorbeeld gebruikt. Sommige auteurs (Jacobs, Van den Broek) zijn betrokken bij het ontwerp en de ontwikkeling van IRMA.[22] Soortgelijke op attributen gebaseerde kenmerken komen ook voor in andere zelf-soevereine identiteitsprojecten, zoals Sovrin.[23] De term zelf-soevereine identiteit (Self-Sovereign Identity, SSI) omschrijft de

21 'Waar gaat IRMA eigenlijk over?',privacybydesign.foundation/irma-uitleg/#onderwerp.

22 IRMA, zie irma.app, wordt beheerd door de onafhankelijke stichting Privacy By Design, zieprivacybydesign.foundation/en/; het is een non-profit spin-off van de Radboud Universiteit. Een aantal van de auteurs van dit artikel zijn betrokken bij IRMA, maar zonder financiële belangen.

23 Zie hierover White paper Sovrin Foundation, Sovrin: a protocol and token for self-sovereign identity and decentralized trust, January 2018, sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf.

digitale beweging waarin een individu zelf zo veel mogelijk controle heeft over zijn of haar identiteit.[24]

2.3 *Algemene eigenschappen digitale handtekening*

Een digitale handtekening is een cryptografische constructie die een bericht in elektronische vorm aan een ondertekenaar bindt. Zij is een aparte bijlage ('add-on') bij het bericht. Een ondertekend bericht bestaat hiermee uit de combinatie van het bericht en deze bijlage.

De ondertekening geschiedt in de regel met behulp van asymmetrische cryptografie. Allereerst wordt er een unieke code ('hash-waarde') gegenereerd op basis van de inhoud van het bericht. De ondertekenaar ondertekent deze hash-waarde vervolgens met behulp van input die alleen van de ondertekenaar kan komen (de zogenoemde *private key*). Eenieder kan vervolgens de digitale handtekening cryptografisch controleren met behulp van de (aan de private key gekoppelde) *public key* van de ondertekenaar. Deze controle maakt duidelijk of de handtekening werkelijk door de ondertekenaar bij het ondertekende bericht is geplaatst.

Een geldige digitale handtekening geeft drie zekerheden. Zij waarborgt in de eerste plaats de integriteit. Elke wijziging in het bericht die na de ondertekening wordt aangebracht, maakt de handtekening ongeldig. Ten tweede is de authenticiteit gewaarborgd. Alleen de ondertekenaar kan het document ondertekenen. Een digitale handtekening zorgt ten slotte voor onweerlegbaarheid.[25] De controle van de handtekening kan zonder de medewerking van de ondertekenaar plaatsvinden. De ondertekenaar kan de ondertekening hierdoor niet ontkennen.

2.4 *Onderscheid tussen ABS en CBS*

De algemene beschrijving in paragraaf 2.3 is zowel van toepassing op CBS als op ABS. Er bestaan echter ook enkele verschillen. Deze verschillen zien in het bijzonder op de inhoud en herkomst van de private en publieke sleutels.

24 C. Allen, *The Path to Self-Sovereign Identity*, 2016, lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html.

25 Nederlandse Overheid Referentie Architectuur, NORA 3.0 Principes voor samenwerking en dienstverlening, noraonline.nl/wiki/Onweerlegbaarheid.

Bij CBS gebruikt de ondertekenaar een persoonlijke unieke private sleutel. De koppeling tussen de digitale handtekening en de ondertekenaar wordt bevestigd door middel van een meegestuurd public-key-certificaat. In dit certificaat bevestigt de certificaatautoriteit (CA) dat het voor de handtekening gebruikte sleutelpaar van de ondertekenaar is. Dit certificaat stelt de vertrouwende partij in staat om de authenticiteit van de digitale handtekening bij het bericht controleren.[26]

Voor de controle op de betrouwbaarheid van een CBS is het bericht, de digitale handtekening en het public-key-certificaat van de ondertekenaar vereist (Figuur 1). Elke digitale handtekening van dezelfde ondertekenaar is gekoppeld aan hetzelfde certificaat met dezelfde openbare sleutel. Daardoor zijn alle CBS van een ondertekenaar koppelbaar.

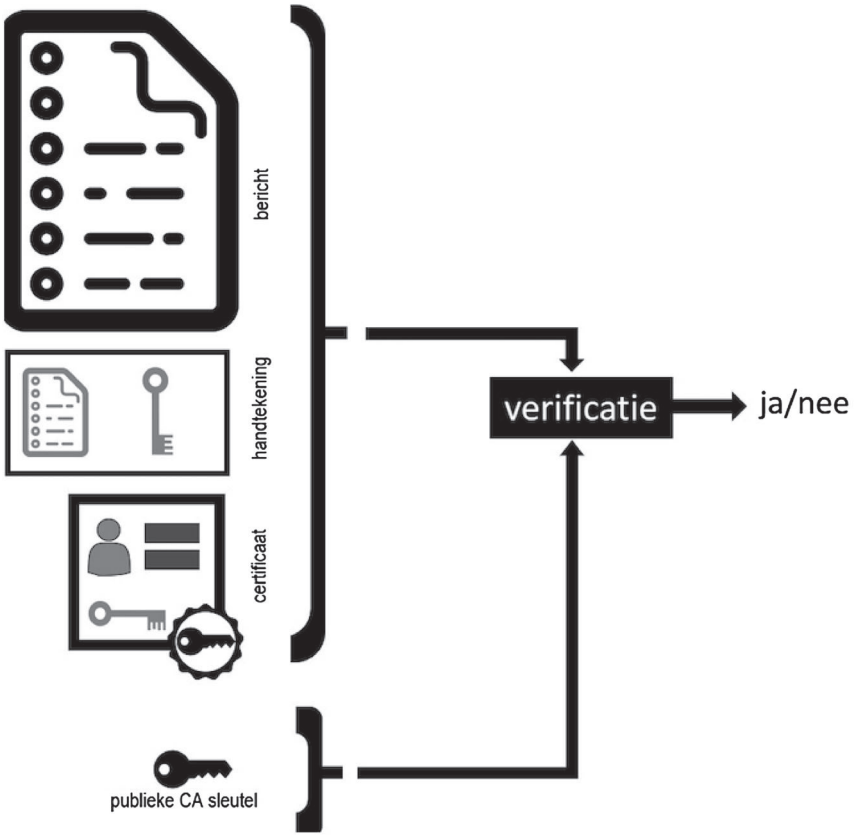
Het aanvraag- en verificatieproces van een ABS werkt als volgt: allereerst meldt de gebruiker (ondertekenaar) zich bij de *issuer* en vraagt om een bepaald attribuut (de registratiefase). Een werkgever kan bijvoorbeeld werknemersnummers uitgeven als attribuut, terwijl een nationale burgerregistratie de woonplaats en het (eventuele) burgeridentificatienummer als attribuut kan uitgeven. De issuer controleert vervolgens de identiteit van de gebruiker. Indien de identificatie en authenticatie van de gebruiker succesvol is verlopen, zal de issuer het attribuut ondertekenen en verstrekken aan de gebruiker (de verstrekkingsfase).[27] De gebruiker kan vervolgens een of meerdere attributen gebruiken om een digitale handtekening te zetten. De handtekening kan vervolgens worden geverifieerd met behulp van de public key *van de issuer(s)* van de gebruikte attribu(u)t(en) (Figuur 2).[28] Daarbij dient te worden opgemerkt dat hoewel de technische rol van een *issuer* vergelijkbaar is met die van een CA, de verstrekte informatie verschillend is. Een certificaat is verbonden aan één gebruiker, terwijl een attribuut betrekking kan hebben op meerdere gebruikers. ABS zijn hierdoor niet noodzakelijkerwijs koppelbaar aan een individuele

26 Zie over de verificatie van de CA ook P.T.J. Wolters & T. Salemink, 'Cybersecurity en de online oprichting van een BV', *WPNR* 2020, afl. 7286, p. 427-428.

27 OECD, 'Digital Identity Management. Enabling Innovation and Trust in the internet Economy', 2011, oecd.org/sti/interneteconomy/49338380.pdf, p. 146-148.

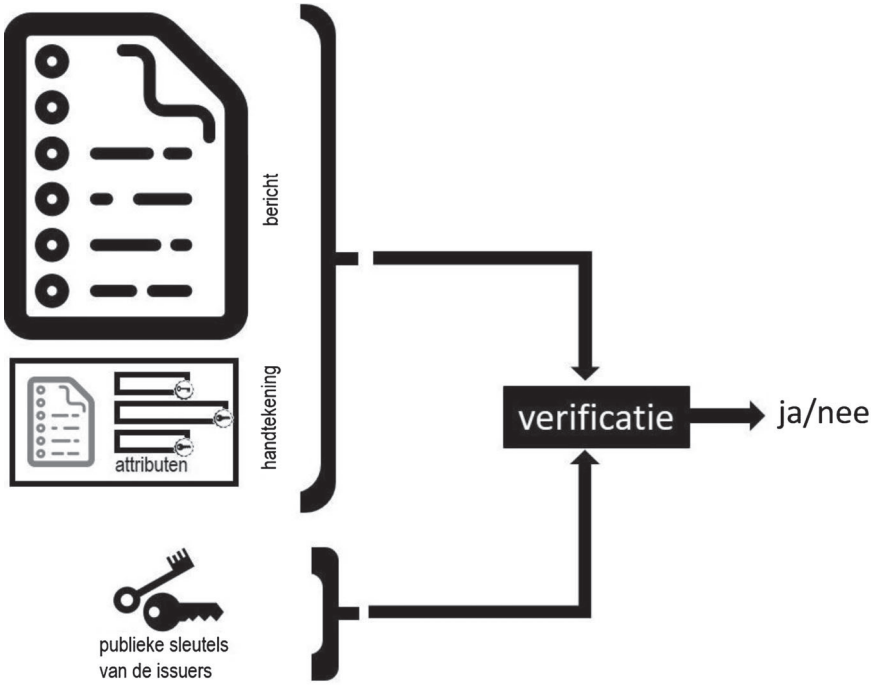
28 B. Hampiholi, G. Alpár, F. van den Broek & B. Jacobs, 'Towards Practical Attribute-Based Signatures', In: R.S. Chakraborty e.a., *Proceedings of the Fifth International Conference on Security, Privacy, and Applied Cryptography Engineering* (SPACE 2015), Jaipur, India, Springer LNCS 9354, 2015, p. 310-328.

gebruiker. Bovendien zijn ABS die met dezelfde attributen zijn gecreëerd ook niet noodzakelijk koppelbaar *aan elkaar*.[29]



Figuur 1. CBS-verificatie – Een bericht dat is ondertekend door een CBS kan worden geverifieerd met het sleutelpaar van de ondertekenaar en het certificaat van de CA.

29 Deze eigenschap is het resultaat van een geavanceerde (asymmetrische) cryptografische techniek. Zie M. Hansen, P. Berlich, J. Camenisch, S. Clauß, A. Pfitzmann & M. Waidner, 'Privacy-enhancing identity management', *Information Security Technical Report* (9) 2004, afl. 1, p. 35-44; M. Veeningen, B. de Weger & N. Zannone, 'Data minimisation in communication protocols: a formal analysis framework and application to identity management', *International Journal of Information Security* (13) 2014, p. 529-569.



Figuur 2. ABS-verificatie -- Een bericht dat is ondertekend door een ABS kan worden geverifieerd met de gebruikte attributen en de public key van de issuer(s).

3. Elektronische handtekening onder de eIDAS-verordening

In de voorgaande paragraaf hebben we elektronische handtekeningen vanuit een technisch perspectief besproken. Handtekeningen spelen echter ook een grote rol in het recht. Wettelijke regels over handtekeningen zijn in de eerste plaats gebaseerd op het nationale recht. Daarom verschillen de wettelijke eisen, functies en gevolgen van handtekeningen per rechtssysteem. Desalniettemin is het mogelijk om enkele gemeenschappelijke kenmerken vast te stellen aan de hand van internationale instrumenten zoals de eIDAS-verordening en de UNCITRAL-modelwet inzake elektronische handtekeningen.[30]

30 UNCITRAL, *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*, New York: United Nations 2002.

In deze paragraaf gebruiken wij in de eerste plaats de eIDAS-verordening om het concept van een handtekening in algemene zin te beschrijven. Het is echter belangrijk op te merken dat deze verordening niet alle aspecten van alle vormen van handtekeningen bestrijkt. Zij schept een kader voor de erkenning van elektronische handtekeningen (zie ook §4), maar verbiedt de lidstaten niet om ook in andere situaties juridische consequenties te verbinden aan (andere soorten) handtekeningen.

3.1 Juridische definitie en functies elektronische handtekening

In art. 3 lid 10 eIDAS-verordening wordt een 'elektronische handtekening' gedefinieerd als "gegevens in elektronische vorm die aan andere gegevens in elektronische vorm zijn gehecht of logischerwijze daarmee zijn verbonden en die door de ondertekenaar worden gebruikt om te ondertekenen". 'Geavanceerde' en 'gekwalificeerde' elektronische handtekeningen bieden extra zekerheid over deze associatie, maar houden geen fundamenteel andere definitie in.[31]

De relatie tussen de handtekening en de natuurlijke persoon die de handtekening gebruikt, de 'ondertekenaar'[32], is onder de eIDAS-verordening een belangrijk kenmerk van elektronische handtekeningen. Volgens art. 26 eIDAS-verordening moeten geavanceerde en gekwalificeerde elektronische handtekeningen[33] op unieke wijze aan de ondertekenaar zijn verbonden en in staat zijn hem te identificeren. Een echte naam is echter niet vereist. De eIDAS-verordening erkent ook elektronische handtekeningen die gebruik maken van pseudoniemen.[34]

Hoewel de eis van identificeerbaarheid niet expliciet wordt opgelegd aan 'gewone' elektronische handtekeningen,[35] lijkt de eIDAS-verordening ervan uit te gaan dat handtekeningen kunnen worden gebruikt om de ondertekenaar te identificeren. Dit vermoeden is gebaseerd op de primaire functie van een handtekening. Eerst en vooral wordt een handtekening gebruikt om de identiteit van de ondertekenaar te bevestigen en te

31 Vergelijk art. 3 lid 11 en 12 eIDAS-verordening.
32 Art. 3 lid 9 eIDAS-verordening.
33 Zie art. 3 lid 11 en 12 eIDAS-verordening.
34 Zie bijvoorbeeld art. 3 lid 14, 5 lid 2, 32 lid 1 onder e en Bijlage I onder c eIDAS-verordening.
35 Art. 3 lid 10 eIDAS-verordening verklaart slechts dat de handtekening is 'gebruikt' door de ondertekenaar en bepaalt niets over het doel van de ondertekening.

bewijzen.[36] Om die reden wordt deze identificeerbaarheid ook vereist door verschillende rechtsstelsels en de UNCITRAL-modelwet inzake elektronische handtekeningen.[37]

Handtekeningen hebben ook andere juridische functies.[38] Deze omvatten onder meer beveiligingswaarborgen. Een handtekening kan leiden tot integriteit en onweerlegbaarheid[39] en bewijs leveren voor deze waarborgen. Bovendien kunnen handtekeningen op andere manieren juridisch relevant zijn. Ze kunnen worden gebruikt om een juridische intentie uit te drukken, om iemand anders te vertegenwoordigen, een contract aan te gaan of een andere rechtshandeling te verrichten. Bovendien kunnen ze duidelijk maken dat het ondertekende document het origineel of een waarheidsgetrouwe kopie van het origineel is. Ten slotte kan het recht een verplichting opleggen om een document te ondertekenen om de ondertekenaar te beschermen. Door het plaatsen van een handtekening wordt de ondertekenaar gewaarschuwd dat hij op het punt staat een juridisch relevante handeling te verrichten.

3.2 CBSs en ABSs in de eIDAS-verordening

De Europese Commissie heeft de eIDAS-verordening technologie-neutraal willen formuleren, zodat door middel van verschillende technologieën

36 Bijvoorbeeld Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 December 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (*PbEU* 2000, L 13/12, overweging 21; overweging 22 en art. 25 lid 1 eIDAS-verordening); K. Rihaczek, 'Digital Signature Surrogates for Open EDI', *The EDI Law Review* 1995, afl. 4, p. 231; C. Reed, 'What is a Signature', *JILT* 2000, afl. 3, §3.1 en 3.1.3; S. Mason, *Electronic Signatures in Law*, Londen: Institute of Advanced Legal Studies 2016, p. 1-2 en 9; S. van Balen & M. Voulon, 'De elektronische handtekening. Tekent de ondertekenaar zelf?', *Ars Aequi* 2020, afl. 12, p. 1164; Tjong Tjin Tai, in: *GS Vermogensrecht*, art. 3:15a, aant. 4.1 (online, bijgewerkt op 24 januari 2019).

37 Zie bijvoorbeeld UNCITRAL 2001, p. 1, 19; HR 5 oktober 2012, ECLI:NL:HR:2012:BV6698, *NJ* 2012/570; A. Galtung, *Paperless systems and EDI. A survey of Norwegian law* (Complex 4/91), Oslo: Tano 1991, p. 38; S. Huydecoper & R.E. van Esch, 'Geschriften en handtekeningen: een achterhaald concept?', in: *ITeR-rapport* 7, Alphen aan den Rijn: Samsom BedrijfsInformatie 1997, p. 134-140; R.E. van Esch, *Electronic Data Interchange (EDI) en het vermogensrecht* (diss. Nijmegen), Deventer: W.E.J. Tjeenk Willink 1999, p. 125-128; M. Voulon, *Automatisch contracteren* (diss. Leiden), Leiden: University Press 2010, p. 241-286.

38 Over deze en andere functies van handtekeningen, zie bijvoorbeeld Rihaczek 1995, p. 230-231; Reed 2000, §3.1.3, 3.2; Van Esch 1999, p. 129-130; UNCITRAL 2001, p. 1 en 19-20; Mason 2016, p. 10-11. Van Balen & Voulon 2020, p. 1164.

39 §2.3. Zie ook art. 26 onder c en d eIDAS-verordening.

kan worden voldaan aan de beveiligingsvereisten.[40] De in paragraaf 3.1 genoemde beveiligingsvereisten van een elektronische handtekening kunnen dan ook zowel door CBS als door ABS worden vervuld. Beide vormen van handtekeningen kunnen leiden tot de noodzakelijke integriteit en onweerlegbaarheid (§2.3). Ook de andere functies kunnen zowel door CBS als door ABS worden vervuld. Zij zijn bijvoorbeeld beide geschikt om de wil van de ondertekenaar uit te drukken of om de ondertekenaar erop te attenderen dat hij een juridisch relevante handeling gaat verrichten.

Alleen het vereiste van identificeerbaarheid kan in sommige situaties tot complicaties leiden. Een attribuut daarentegen is niet altijd koppelbaar aan een individuele persoon (§2.2). Hetzelfde geldt voor een ABS die alleen op deze niet-identificerende attributen is gebaseerd (§2.4). Een dergelijke ABS kwalificeert dan ook niet als een elektronische handtekening in de zin van de eIDAS-verordening. Dit probleem bestaat echter niet bij ABS die wel (mede) zijn gebaseerd op een uniek identificerend attribuut.

De eIDAS-verordening vereist bovendien niet dat de handtekening is gekoppeld aan de echte naam van de ondertekenaar. Zij laat ook elektronische handtekeningen toe die gebruik maken van pseudoniemen.[41] Het is hierdoor ook mogelijk om gebruik te maken van gepseudonimiseerde ABS. Hiervoor kan gebruik worden gemaakt van een attribuut dat wel uniek is, maar niet leidt tot de identificeerbaarheid van de ondertekenaar.[42] Hiermee is overigens niet gezegd dat pseudoniemen ook altijd voldoende zijn voor alle rechtshandelingen waarvoor een handtekening is vereist. Art. 5 lid 2 eIDAS-verordening bepaalt dat de gevolgen van pseudoniemen door het nationale recht worden geregeld.

De technologie-neutrale benadering van de eIDAS-verordening is echter niet consequent doorgevoerd. De eIDAS-verordening schrijft dwingend voor dat een gekwalificeerde elektronische handtekening gebaseerd dient te zijn op een gekwalificeerd certificaat voor elektronische handtekeningen.[43] Hierdoor kunnen dus alleen CBS voldoen aan de eisen aan gekwa-

40 Overweging 16 eIDAS-verordening.
41 Art. 3 lid 15, 5, 32 lid 1 onder e, Bijlage I onder c en bijlage IV onder c eIDAS-verordening.
42 Het kan hierbij bijvoorbeeld gaan om een e-mailadres met een alias of een speciaal voor dit doel uitgegeven 'pseudoniem attribuut', bijvoorbeeld in de vorm van een uniek nummer.
43 Art. 3 lid 12 en 15 en 28 en Bijlage I eIDAS-verordening.

lificeerde elektronische handtekeningen. ABS maken immers *geen* gebruik van certificaten (§2.4).

Identificerende (of gepseudonimiseerde) ABS kunnen echter wel voldoen aan alle in art. 26 eIDAS-verordening genoemde vereisten voor geavanceerde elektronische handtekeningen. ABS die gebaseerd zijn op uniek identificerende attributen zijn op unieke wijze verbonden aan de ondertekenaar (sub a) en maken het mogelijk om de ondertekenaar te identificeren (sub b). Zij zorgen bovendien voor de vereiste authenticiteit (sub c) en integriteit (sub d) (§2.3).

3.3 De juridische gevolgen van een elektronische handtekening

De rechtsgevolgen van een elektronische handtekening worden zowel door de eIDAS-verordening als door het nationale recht bepaald.[44] Allereerst formuleert art. 25 lid 1 eIDAS-verordening een non-discriminatieregel. Het rechtsgevolg van een elektronische handtekening en de toelaatbaarheid ervan als bewijsmiddel mogen door de lidstaten niet worden ontkend louter op grond van het feit dat de handtekening elektronisch is of niet voldoet aan de eisen voor gekwalificeerde elektronische handtekeningen. Het nationale recht mag dus niet bepalen dat ABS, zeker als ze zijn voorzien van de benodigde beveiligingswaarborgen, geen enkele waarde hebben.

Hiermee is echter niet bepaald dat een (gewone of geavanceerde) elektronische handtekening ook echt in alle opzichten dient te gelden als een natte handtekening. Art. 25 lid 2 eIDAS-verordening bepaalt slechts dat *gekwalificeerde* elektronische handtekeningen hetzelfde rechtsgevolg hebben als een handgeschreven handtekening. Lid 3 bepaalt bovendien dat handtekeningen die zijn gebaseerd op een in een lidstaat afgegeven gekwalificeerd certificaat, in alle lidstaten als een gekwalificeerde elektronische handtekening moeten worden erkend.

Lidstaten hoeven geavanceerde elektronische handtekeningen dus niet, en zeker niet in alle gevallen, te beschouwen als een 'echte' handtekening. In Nederland bepaalt art 3:15a BW dat gewone en geavanceerde elektronische handtekeningen ook dezelfde rechtsgevolgen hebben als een handgeschreven handtekening indien zij voldoende betrouwbaar zijn, gelet op het doel waarvoor de handtekening wordt gebruikt.

44 Zie over deze gevolgen ook Van Balen & Voulon 2020, p. 1166.

Dit zou moeten beteken dat een handtekening die voldoet aan de vereisten van een geavanceerde elektronische handtekening in de regel voldoende zou moeten zijn. Een complicatie is hierbij echter dat het voor leken eigenlijk niet mogelijk is om te controleren of geavanceerde handtekeningen werkelijk aan deze vereisten voldoen.[45] Bovendien kunnen andere EU-lidstaten andere vereisten stellen. Met andere woorden: om er zeker van te zijn dat een elektronische handtekening in heel Europa 'als handtekening' wordt geaccepteerd, dien je een gekwalificeerde elektronische handtekening te gebruiken.

4. Use cases

In de voorgaande paragraaf hebben we elektronische handtekeningen vanuit een technisch perspectief en juridisch perspectief geïntroduceerd. Ons doel in deze paragraaf is om het gebruik van ABS te illustreren aan de hand van een reeks use cases met verschillende attributen. Het gaat hierbij in beginsel steeds om een arts die een professionele (recept)verklaring digitaal heeft ondertekend met behulp van een ABS en een vertrouwende partij, in de meeste gevallen een apotheek, die wil weten of deze (elektronische) handtekening voldoende betrouwbaar is.

De Geneesmiddelenwet vereist een (recept)verklaring die door een arts of andere beroepsbeoefenaar is ondertekend en waarin zijn of haar naam en werkadres is opgenomen.[46] Verschillende aspecten van het (getekende) bericht zijn van belang:

(1) de integriteit, zodat bijvoorbeeld de juiste geneesmiddelen worden besteld en geleverd;
(2) het feit dat de verklaring is ondertekend door een bevoegde arts;
(3) de identiteit van de arts, zodat hij of zij verantwoordelijk kan worden gehouden in het geval van een medische fout.

In de use cases gaan we ervan uit dat het eerste aspect, de integriteit van het bericht, is gewaarborgd. We zullen ons focussen op het tweede en derde aspect. In de verschillende onderstaande scenario's hanteren we het uitgangspunt dat alle attributen op de juiste wijze zijn uitgegeven en

45 Zie in deze zin V. van Kampen, 'De elektronische handtekening in het ondernemingsrecht', *TOP* 2020, afl. 4, p. 24-25.

46 Art. 1 lid 1 sub s en sub pp en art. 61 lid 9 Geneesmiddelenwet; art. 36 lid 1 Wet op de beroepen in de individuele gezondheidszorg (Wet BIG).

geldig zijn op de relevante momenten. We negeren bijvoorbeeld de geldigheidsduur van de attributen.

4.1 Use case I: alleen (volledige) naam als attribuut

In de eerste situatie ondertekent de arts een (recept)verklaring met alleen een (volledige) naam als attribuut. Een dergelijke ABS kwalificeert in ieder geval als een 'gewone' elektronische handtekening onder de eIDAS-verordening. De aspecten 2 en 3 zijn echter niet gegarandeerd. Er kunnen meer personen zijn met dezelfde naam. Een enkele ondertekening met een naam maakt niet duidelijk welke van deze personen heeft ondertekend (aspect 3) en of deze ondertekenaar de bevoegdheid heeft tot het uitschrijven van recepten (aspect 2). Een enkele naam als attribuut kan dus niet, of ten minste niet in alle situaties, leiden tot een geavanceerde elektronische handtekening, omdat zij niet op unieke wijze aan de ondertekenaar is verbonden.[47] Zij lijkt om deze redenen onvoldoende betrouwbaar voor het gebruikte doel en kan niet worden gelijkgesteld met een handgeschreven handtekening (§3.3).

4.2 Use case II: twee attributen – naam en registratienummer

In het tweede geval ondertekent de arts de verklaring met twee attributen: zijn/haar (volledige) naam en (unieke) registratienummer, afkomstig uit het nationale register van beroepsbeoefenaren in de gezondheidszorg (BIG-register). Als de relevante onderdelen van dit register openbaar toegankelijk zijn, kan de betrouwbaarheid gegarandeerd worden. De vertrouwende partij kan de elektronische handtekening valideren door in het register op te zoeken of het registratienummer op de ondertekende verklaring gekoppeld is aan de juiste medische rol (aspect 2). Aspect 3 is bovendien gegarandeerd als het medische registratienummer is gekoppeld aan een unieke identificatie van persoonlijke gegevens zoals adres, telefoonnummer en geboortedatum. Zolang ook aan de andere eisen van de eIDAS-verordening wordt voldaan, kan deze handtekening worden beschouwd als een geavanceerde elektronische handtekening. Een ABS gebruikt echter geen certificaten, de handtekening kan daarom niet kwalificeren als een gekwalificeerde elektronische handtekening.

47 Art. 26 onder a eIDAS-verordening.

4.3 *Use case III: vier attributen – naam, werkadres, registratienummer en medische specialisatie*

In de derde situatie ondertekent de arts met vier attributen: de (volledige) naam, het werkadres, het registratienummer en de medische specialisatie. De medische specialisatie en het werkadres maken een controle in het landelijke register van zorgverleners overbodig. De bevoegdheid van de arts blijkt immers uit de medische specialisatie en het vereiste werkadres is als apart attribuut toegevoegd. Deze versie kan van grote praktische waarde zijn, omdat de controle van aspect 2 direct kan worden uitgevoerd, als onderdeel van de automatische verwerking van recepten en zonder de medewerking van andere partijen zoals het nationale register van beroepsbeoefenaren in de gezondheidszorg. De praktische waarde van deze variant ligt in het feit dat de betrouwbaarheidscontrole direct uitgevoerd kan worden en geautomatiseerde verwerking van recepten niet wordt gehinderd. Deze situatie is bovendien privacyvriendelijk. Doordat het niet noodzakelijk is om de bevoegdheid van de arts bij het register te controleren, krijgt het register geen inzage in het feit dat de arts een recept heeft voorgeschreven dat door de vertrouwende apotheek wordt uitgegeven.

4.4 *Use case IV: geslacht en leeftijd als attributen*

Naast de vier attributen in de derde variant, kan de arts ook zijn of haar geslacht en leeftijd gebruiken voor de elektronische handtekening. Het opnemen van het geslacht en leeftijd is in dit geval echter onnodig. Voor het controleren van de bevoegdheid en identiteit van de arts voor het uitschrijven van een (recept)verklaring is het geslacht en de leeftijd van de ondertekenaar niet relevant. De verwerking daarvan is in strijd met het beginsel van dataminimalisatie van art. 5 lid 1 onder c AVG.[48]

Dit betekent echter niet dat het geslacht en de leeftijd nooit van belang kunnen zijn. In sommige situaties is het kenbaar maken van het geslacht en/of de leeftijd wel relevant. Voorbeelden zijn activiteiten die de arts in privé onderneemt, zoals het online afsluiten van overeenkomsten,[49] het

48 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (*PbEU* 2016, L 119/1).

49 Zie ook art. 1:233 en 3:32 lid 2 BW, een overeenkomst die is gesloten door een minderjarige is vernietigbaar. Daarnaast bepaalt art. 8 lid 1 AVG dat de verwerking van persoonsgegevens in verband met een aanbod van diensten van de informatiemaatschappij aan een kind slechts rechtmatig is als het kind ten minste 16 jaar is.

bezoeken van online gok- en pornowebsites waarbij voor bezoekers een minimumleeftijd van 18 jaar geldt of het deelnemen aan sportevenementen waarbij geslachtsverificatie van belang kan zijn.

Een apart leeftijdsattribuut stelt de gebruiker van ABS daarom in staat om zijn leeftijd alleen te delen in de gevallen waarin dit echt nodig is. Het gebruik van ABS bevordert hiermee dataminimalisatie. Dit voorbeeld laat bovendien zien dat CBS door hun inflexibiliteit niet altijd een gelijkwaardig alternatief vormen. Het gebruik van CBS betekent dat altijd dezelfde, in het certificaat opgenomen, informatie wordt gedeeld met een vertrouwende partij. Een ondertekenaar kan er dus niet voor kiezen om zijn in het certificaat genoemde leeftijd niet te delen.[50] Tegelijkertijd is het weglaten van de leeftijd ook niet ideaal. De leeftijd kan in andere situaties immers wel van belang zijn.

4.5 Use case V: een niet-identificerend attribuut

Voorts kan de arts een (recept)verklaring ook met één enkel niet-identificerend attribuut ondertekenen. Door met de medische specialisatie te ondertekenen, bewijst de ondertekenaar dat hij of zij bevoegd is om geneesmiddelen voor te schrijven (aspect 2). Het biedt echter geen waarborgen met betrekking tot aspect 3, aangezien de arts niet identificeerbaar is. Dit is volgens de Nederlandse Geneesmiddelenwet echter niet toegestaan (zie §4). Het is bovendien geen handtekening onder de eIDAS-verordening. Een degelijke ABS is namelijk niet op unieke wijze aan de ondertekenaar verbonden en is dus niet identificerend.

Toch kan een dergelijke ABS een belangrijke rol spelen in situaties waarin het juist van belang is om de identiteit van de ondertekenaar geheim te houden. Zij is van belang als de precieze identiteit van de ondertekenaar niet van belang is, maar een bepaalde bevoegdheid van de ondertekenaar wel. Door gebruik te maken van het leeftijdsattribuut kan de bezoeker van een pornowebsite bijvoorbeeld bewijzen dat hij of zij ouder is dan 18 jaar, zonder zijn of haar identiteit prijs te geven.[51] Een pornowebsite

50 In Bijlage I eIDAS-verordening staat welke informatie een gekwalificeerd certificaat dient te bevatten. Vergelijk daarnaast art. 24 lid 1 en 28 lid 3 en overweging 54 eIDAS-verordening. Een certificaat kan geverifieerde aanvullende attributen bevatten zoals een leeftijd of een medische specialisatie.

51 Vergelijk het gebruik van een leeftijdsattribuut bij gokwebsites. De Nederlandse wetgever heeft echter nadere eisen opgesteld voor de identificatie en authenticatie van spelers om gokverslaving tegen te gaan. Zie art. 31k lid 2 en lid 5 sub a Wet op de kansspelen en art. 4.11 en 4.16 Besluit kansspelen op afstand.

zou elektronische handtekeningen kunnen gebruiken om de leeftijd van de bezoekers te controleren (§4.4).[52] Het is echter evident dat veel bezoekers niet geneigd zijn hun naam en andere persoonsgegevens te onthullen. Bovendien is dit niet nodig. Zolang de bezoeker betrouwbaar bewijs kan leveren dat hij of zij de vereiste leeftijd heeft bereikt, is het verwerken van meer gegevens niet nodig. Dit bewijs zou kunnen worden geleverd door een attribuut met een leeftijdskenmerk (bijvoorbeeld: 'ouder dan 18 jaar') te gebruiken om het verzoek om toegang tot het pornografisch materiaal te ondertekenen.

Dit voorbeeld laat opnieuw (§4.4) zien dat CBS door hun inflexibiliteit niet altijd een geschikt alternatief bieden. Zij stellen een ondertekenaar niet in staat om wel zijn leeftijd maar niet zijn naam te onthullen.

4.6 Use case VI: een pseudoniem als attribuut

Het voordeel van ABS is dat de ondertekenaar zelf kan bepalen hoeveel en welke gegevens hij of zij wil gebruiken. In de in paragraaf 4.3 beschreven variant gebruikt de arts vier attributen bij de ondertekening. Het is echter ook mogelijk om alleen het registratienummer en de medische specialisatie als attributen te gebruiken.

De medische specialisatie garandeert dat het document afkomstig is van een bevoegde arts (aspect 2). De werkelijke naam en het werkadres kunnen indien nodig onder strikte voorwaarden in een register worden opgezocht. Dit speelt bijvoorbeeld in het geval van een medische fout. Aspect 3 is hierdoor toch gewaarborgd.

Het registernummer fungeert in deze variant als een pseudoniem, waardoor de ondertekenaar niet direct identificeerbaar is. De eIDAS-verordening faciliteert dergelijke gepseudonimiseerde handtekeningen, maar laten de gevolgen van pseudoniemen over aan het nationale recht. (§3.2). Het staat de Nederlandse wetgever dus vrij om in de Geneesmiddelenwet te vereisen dat de naam en het werkadres van de arts zijn opgenomen.

Deze variant ligt dan ook niet voor de hand in het 'typische' geval van een arts die recepten voorschrijft die een patiënt bij een apotheek ophaalt. Hij

52 De vraag of de huidige, minder strenge, procedures al dan niet legaal zijn, valt buiten het bestek van deze bijdrage.

kan echter wel uitkomst bieden als het noodzakelijk is om de identiteit van de arts af te schermen om vergelding door de patiënt te voorkomen.

Het kan bijvoorbeeld wenselijk zijn om de identiteit van de beoordelend psychiater bij een gedwongen opname in een psychiatrisch ziekenhuis geheim te houden. Onder art. 16 lid 1 Wet bijzondere opnemingen in psychiatrische ziekenhuizen (Wet Bopz) werd[53] de verklaring bijvoorbeeld (elektronisch)[54] ondertekend door de geneesheer-directeur, en niet door de beoordelend psychiater.[55] Dit systeem was in de eerste plaats bedoeld om de verantwoordelijkheid (aspect 3) te verplaatsen van de beoordelend psychiater naar de geneesheer-directeur.[56] Een dergelijk handelswijze maakte het echter ook mogelijk om de naam of andere persoonlijke gegevens van de behandeld arts af te schermen.

Dit neemt natuurlijk niet weg dat het wenselijk kan zijn om de identiteit van de arts in bepaalde situaties te achterhalen. In het systeem van de Wet Bopz kon de identiteit via de geneesheer-directeur worden achterhaald. Het is echter ook mogelijk om gepseudonimiseerde ABS te gebruiken. De beoordelend psychiater kan zijn verklaring in dit geval ondertekenen met een registratienummer in een niet-openbaar register. Art. 5:8 lid 1 Wvggz bepaalt bijvoorbeeld dat de geneesheer-directeur moet zorgen voor een medische verklaring *van een psychiater.* Lid 2 bepaalt bovendien dat bij ministeriële regeling een model voor een medische verklaring kan worden vastgesteld. In het huidige model dient de psychiater naast zijn of haar naam, werkadres en e-mailadres ook zijn of haar handtekening te zetten.[57] Dit model is echter geen voorschrift, dus de psychiater zou de verklaring ook met een registratienummer in een niet-openbaar register kunnen

53 Per 1 januari 2020 is de Wet Bopz vervangen door de Wet verplichte Geestelijke Gezondheidszorg (Wvggz; *Stb.* 2018, 36) en de Wet zorg en dwang (Wzd; *Stb.* 2018, 36). Ook de Wvggz schrijft net als de Wet Bopz niet expliciet voor dat de geneesheer-directeur de verklaring moet ondertekenen. Uit de parlementaire geschiedenis blijkt niet dat nog steeds een handtekening is vereist, zie onder meer *Kamerstukken II* 2009/10, 32399, nr. 3 (MvT).

54 Het moet dan gaan om een geavanceerde of gekwalificeerde elektronische handtekening. Zie HR 14 juni 2019, ECLI:NL:HR:2019:957.

55 HR 19 april 2019, ECLI:NL:HR:2019:635.

56 HR 11 september 2015, ECLI:NL:HR:2015:2533; *Kamerstukken II* 1998/99, 26527, nr. 3 (MvT).

57 Medische verklaring ten behoeve van de voorbereiding van een Zorgmachtiging als bedoeld in art. 5:8 en 7:11 lid 4 Wvggz, dwangindezorg.nl/binaries/dwangindezorg/documenten/publicaties/implementatie/ketenproducten/producten-wvggz/5-8-en-7-11-lid-4-medische-verklaring-zm-definitief/5+8+en+7+11+lid+4+medische+verklaring+ZM+definitief.pdf. Het model is opgesteld door werkgroepen van verschillende ketenpartijen en is geen voorschrift.

ondertekenen. Een dergelijke handtekening is bovendien, ook als het registratienummer niet met de op te nemen persoon kan worden gedeeld, een betrouwbare en tegelijkertijd relatief privacyvriendelijke manier om het oordeel van de psychiater naar de geneesheer-directeur te versturen.

Een vergelijkbaar systeem kan worden gebruikt bij andere gevoelige zaken zoals de ondertoezichtstelling (OTS) van kinderen.[58] In het geval dat de ontwikkeling van de minderjarige ernstig in gevaar is, dient de Raad voor de Kinderbescherming (of het Openbaar Ministerie) een verzoek tot OTS in bij de kinderrechter.[59] Dit geschiedt in de regel na een onderzoek door een 'jeugdprofessional' met een SKJ-registratie.[60] Ook hierbij geldt dat de ondertekening met een dergelijke registratie kan worden gebruikt om te bewijzen dat het onderzoek is uitgevoerd door een bevoegde professional (aspect 2). Het register kan onder strikte voorwaarden worden gebruikt om de identiteit van deze professional te achterhalen (aspect 3).

De in deze paragraaf genoemde toepassingen zijn onder het huidige recht hypothetisch. Zij bieden echter wel een goede illustratie van de mogelijkheden van gepseudonimiseerde handtekeningen. Deze handtekeningen kunnen als CBS of als ABS worden vormgegeven. Een bijkomend voordeel van ABS is echter opnieuw de flexibiliteit. Het stelt een psychiater bijvoorbeeld in staat om zijn verklaring in het kader van de Wvggz[61] alleen te ondertekenen met zijn registratienummer en medische specialisatie en om bij het schrijven van recepten ook zijn naam en werkadres toe te voegen.

5. Synthese en conclusie

De use cases laten zien dat ABS verschillende voordelen hebben boven CBS. Deze voordelen concentreren zich in het bijzonder op twee mogelijkheden: de mogelijkheid om extra attributen toe te voegen of juist weg te laten (§4.4) en de mogelijkheid om te ondertekenen met een niet-identificerend attribuut (§4.5). Ondanks deze voordelen biedt de eIDAS-verordening

58 Art. 1:1 Jeugdwet en art. 1:255 lid 1 BW.
59 Art. 1:255 lid 2 BW.
60 Art. 1.1 Besluit van 5 november 2014 houdende regels ter uitvoering van de Jeugdwet (Besluit Jeugdwet). De Stichting Kwaliteitsregister Jeugd (SKJ) is het Nederlandse beroepsregister waarin de functie, het niveau, de vestigingsplaats, de eerste registratiedatum en de registratieperiode van jeugdprofessionals zijn opgenomen.
61 Art. 5:7 sub a Wvggz en art. 14 Wet BIG.

slechts in beperkte mate ruimte aan ABS (§3.2). Dit heeft verschillende nadelen.

De inflexibiliteit van CBS is in de eerste plaats privacy-onvriendelijk en in strijd met het beginsel van dataminimalisatie uit de AVG. Dataminimalisatie betekent dat het verwerken van persoonsgegevens voor het doel toereikend en ter zake dienend moeten zijn. Daarnaast mogen er niet meer persoonsgegevens worden verwerkt dan noodzakelijk is voor specifieke doeleinden.[62] Minimaliseren van data ziet niet enkel op hetgeen noodzakelijk is voor de verwerking, maar kan ook verwijzen naar de mate van identificatie. Indien het doel van de verwerking geen verwijzing naar de identiteit van een persoon behoeft, moet de verwerkingsverantwoordelijke de persoonsgegevens anonimiseren.[63] CBS zijn in strijd met dit beginsel. Zij dwingen de ondertekenaar om altijd alle in het certificaat opgenomen attributen te tonen, ook als deze in het onderhavige geval niet van belang zijn (§4.4). CBS zijn bovendien niet volledig anoniem (§4.5). Zij kunnen weliswaar gepseudonimiseerd zijn, maar er bestaat in dat geval altijd een risico dat de ondertekenaar toch wordt geïdentificeerd.[64] Dit risico wordt nog eens versterkt doordat de verschillende gepseudonimiseerde CBS aan elkaar kunnen worden gekoppeld (§2.4). Het is dus nog steeds mogelijk om te zien dat hetzelfde pseudoniem ook op andere momenten is gebruikt. Dit maakt het dan weer makkelijker om de identiteit achter het pseudoniem te achterhalen.

De inflexibiliteit van CBS kan ook tot het tegenovergestelde resultaat leiden. Het is mogelijk dat een certificaat bepaalde attributen niet heeft opgenomen die in sommige gevallen juist wel van belang zijn (§4.4). CBS zijn in deze gevallen minder betrouwbaar dan ABS, aangezien zij geen waarborgen bieden voor het niet-opgenomen attribuut.

De nadelen van CBS kunnen in theorie worden verholpen door verschillende elektronische handtekeningen en bijbehorende certificaten te creëren. Dit is echter een tijdrovend, kostbaar en omslachtig proces, zeker bij gekwalificeerde elektronische handtekeningen die met strenge

62 Dit kan bijvoorbeeld bewerkstelligd worden door *privacy by design & default* waarbij maatregelen worden genomen om zo min mogelijk persoonsgegevens te verwerken, zie art. 25 lid 1 AVG. Een voorbeeld van een dergelijke maatregel is pseudonimisering, zie art. 4 lid 5 AVG.

63 European Data Protection Board (EDPB), Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, nr. 70.

64 Groep gegevensbescherming artikel 29, Advies 5/2014 over anonimiseringstechnieken (WP216), p. 23-26.

waarborgen zijn omkleed.[65] Elke gekwalificeerde elektronische handtekening dient namelijk gebaseerd te zijn op een gekwalificeerd certificaat, op unieke wijze aan de ondertekenaar te zijn verbonden en in staat te zijn hem te identificeren.

ABS hebben de gesignaleerde nadelen niet. De Europese wetgever kan hierdoor zowel de privacy van ondertekenaars als de betrouwbaarheid van het online rechtsverkeer vergroten door ook ABS te faciliteren. Onze analyse laat zien dat het huidige kader in het bijzonder op twee manieren tekortschiet.

De eIDAS-verordening is in de eerste plaats beperkt tot identificerende of gepseudonimiseerde elektronische handtekeningen. Zij laat geen handtekeningen toe die niet uniek-identificerend en koppelbaar zijn aan een individuele persoon (§3.2). Deze beperking is in de eerste plaats begrijpelijk. Zij vloeit immers voort uit de primaire functie van (elektronische) handtekeningen: het identificeren van de ondertekenaar (§3.1). De use-cases laten echter zien dat ook niet-identificerende handtekeningen nuttige functies kunnen vervullen in ons rechtsverkeer (§4.5).

De facilitering van niet-identificerende ABS vereist daarom dat enigszins afstand wordt genomen van de klassieke opvattingen over handtekeningen. Het begrip elektronische handtekening beweegt hiermee in de richting van de digitale handtekening van identiteitsmanagement (§1). Ook de eisen aan geavanceerde en gekwalificeerde elektronische handtekeningen dienen te worden versoepeld. In het bijzonder geldt dat de eisen van art. 26 sub a en b eIDAS-verordening alleen zouden moeten gelden voor zover de handtekening pretendeert te zijn verbonden aan een unieke ondertekenaar.

De eIDAS-verordening schiet daarnaast tekort doordat het begrip gekwalificeerde elektronische handtekening ondanks de gepretendeerde technologieneutraliteit is beperkt tot CBS (§3.2). De rechtsgevolgen van ABS blijven hierdoor onzeker (§3.3), zelfs in de gevallen dat de attributen met de grootste zorg zijn geverifieerd. Dit kan worden verholpen door de definitie van gekwalificeerde elektronische handtekening technologieneutraal te formuleren.

De betrouwbaarheid van gekwalificeerde elektronische handtekeningen vloeit immers niet zozeer voort uit het feit dat het certificaat gekwalificeerd

65 §3.2. Zie ook art. 3 lid 12 en 15, art. 28 en Bijlage I eIDAS-verordening.

is, maar uit de betrouwbaarheid van de technologie en de in het certificaat opgenomen informatie en het feit dat deze betrouwbaarheid uiteindelijk wordt geverifieerd door een gekwalificeerde aanbieder van vertrouwensdiensten.[66] Zolang de uiteindelijke handtekeningen zowel op het gebied van de techniek als met betrekking tot de opgenomen informatie (met andere woorden: de attributen) net zo betrouwbaar zijn, zouden deze gekwalificeerde aanbieders ook andere vormen van gekwalificeerde elektronische handtekeningen moeten kunnen aanbieden.

Hierbij is het overigens wel van belang om de details goed uit te werken. Dit speelt bijvoorbeeld bij ABS die zijn gebaseerd op een gekwalificeerd attribuut (zoals een medisch specialisme, uitgegeven door een gekwalificeerde instantie) en een niet-gekwalificeerd attribuut (zoals een naam, uitgegeven door een niet-gekwalificeerde instantie). De handtekening kan dan alleen met betrekking tot het specialisme als gekwalificeerd worden beschouwd. Met andere woorden: de handtekening is gekwalificeerd met betrekking tot het feit dat de ondertekenaar het medische specialisme bezit (aspect 2), maar slechts gewoon of geavanceerd met betrekking tot de naam, en dus de identiteit van de ondertekenaar (aspect 3).

In oktober 2020 is de Europese Commissie gestart met de herziening van de eIDAS-verordening. Het doel van deze herziening is om de effectiviteit van de verordening te vergroten. ABS dragen hieraan bij doordat zij meer flexibiliteit voor de ondertekenaar creëren en tevens de betrouwbaarheid van het online rechtsverkeer vergroten. Daarnaast zijn ABS privacyvriendelijk, omdat de ondertekenaar alleen relevante en noodzakelijke attributen onthult. Om deze voordelen in heel Europa te bewerkstelligen, strekt het tot aanbeveling om bij de herziening van de eIDAS-verordening tevens (niet-identificerende) ABS te faciliteren en de verordening daadwerkelijk technologie-neutraal te maken.

66 Art. 3 lid 12, 15 en 20 eIDAS-verordening.