Notitie elektronisch Informed Consent (eIC) bij gezondheidsonderzoek. *een eerste verkenning met aandachtspunten voor verdere implementatie*

Aan: COREON (Federa)
Door: Evert-Ben van Veen (eindredactie), met medewerking van Marjolein Timmers en Marie-José Bonthuis (IT's Privacy) bij eerdere versies.
Datum: 03-02-2019
versie: 2.2 eindversie.

Literatuur bijgewerkt tot medio januari 2019.

Samenvatting

- Deze notitie is een eerste verkenning van elektronisch informed consent (eIC) en verder elektronisch contact met de deelnemers aan gezondheidsonderzoek.
- De notitie gaat niet in op de vraag wanneer toestemming nodig is en welke informatie in dat kader gegeven moet worden. De vraag is wat er *verandert* of kan veranderen ten opzichte van analoge communicatie indien de communicatie met de (beoogde) deelnemer geheel of voornamelijk elektronisch plaatsvindt.
- eIC kan bij de geschikte doelgroep vele voordelen bieden voor zowel onderzoekers als (potentiële) deelnemers.
- eIC kan formeel nog niet worden ingezet voor onderzoek dat onder de wet mensgebonden onderzoek (WMO) valt.[1]
- Bij gebreke aan een laagdrempelig, veilig en algemeen toegepast elektronisch identificatiemiddel (eID) kunnen de voordelen van eIC momenteel ook buiten de WMO niet over de volle breedte worden gerealiseerd.
- In lijn met het voorafgaande. Hoewel wel duidelijkheid bestaat over welk niveau van beveiliging in welke situatie (bijvoorbeeld al of niet bijzondere persoonsgegevens) noodzakelijk zou moeten zijn, is momenteel veel minder duidelijk hoe dit kan worden bereikt.
- Bij het niveau van beveiliging van het eID en het gebruik daarvan gaat het om 3 begrippen: identificatie (is de persoon aan wie een eID is uitgereikt inderdaad deze persoon), authenticatie (betreft het gebruik van een eID inderdaad die persoon) en autorisatie (mag die persoon de desbetreffende elektronische handelingen verrichten).

[1] In diens brief naar aanleiding van het evaluatierapport van de WMO (Kamerstukken 29963, nr. 19) heeft de minister van VWS gesteld dat hij naar verwachting in 2019 met een voorstel zal komen waarmee het elektronisch verlenen van toestemming aan een WMO onderzoek mogelijk moet worden. Indien dat het geval is (zulke verwachtingen blijken wel eens wat optimistisch) zal daar uiteraard bij niet WMO onderzoek op kunnen worden aangesloten.

- Daarbij kan men afwegingen maken. De voornaamste elementen die in dat kader voor gezondheidsonderzoek van belang zijn: de bescherming van de vertrouwelijkheid van de gegevens van de deelnemer via eIC en een daarmee verbonden eID bij de communicatie met de onderzoekers en de validiteit van de gegevens ten behoeve van het onderzoek. Iemand kan volkomen vertrouwelijk gegevens in het kader van het onderzoek opgeven maar helemaal niet de beoogde deelnemer zijn.
- Deze notitie geeft daartoe een aantal voorlopige uitgangspunten in een veld dat sterk in beweging is. De voorlopige uitgangspunten zijn in paragraaf 1 opgenomen. De achtergrond van deze en de huidige discussie omtrent eID of beter eID's en de elektronische handtekening wordt in de volgende paragrafen van deze notitie geschetst. Lezing van de achtergrond is van belang om de uitgangspunten in de context van de complexe discussie te kunnen plaatsen.
- De eindrapporteur is er zich er van bewust dat de uitgangspunten thans nog betrekkelijk vaag zijn. Dat is inherent aan de huidige stand van de discussie en het ontbreken van gerapporteerde 'use cases' bij gezondheidsonderzoek waarop kon worden teruggevallen. Uitwerking van de uitgangspunten zal in samenwerking met experts in digitale beveiliging moeten plaatsvinden.
- Drie andere begrippen die bij elektronische gegevensverwerking in het algemeen van belang zijn, blijven bij de uitgangspunten grotendeels buiten beschouwing, namelijk integriteit (blijven de gegevens bij diverse bewerkingen wel dezelfde of kan worden aangetoond welke bewerkingen tot welke aanpassingen hebben geleid[2]), beschikbaarheid[3], gegevensbeveiliging en cyber security. Dat zijn de randvoorwaarden, die altijd gelden ook als niet geheel of voornamelijk van eIC gebruik zou worden gemaakt. Bij eIC worden zij wel extra pregnant.
- Overigens bevat deze notitie twee aanbevelingen. Deze zijn:
    - Het gezondheidsonderzoek zou zich kunnen mengen in de discussie omtrent de eID middelen bij het wetsontwerp digitale overheid. Het is namelijk de vraag of het gezondheidsonderzoek kan aansluiten bij de overheids eID middelen die worden aangewezen voor de communicatie met de overheid en semi-overheid (waartoe ook de gezondheidszorg wordt gerekend). Dan zou een ander eID moeten worden gebruikt waarbij het de vraag is of dat wel algemeen wordt toegepast;
    - De mogelijkheden van een eID voor onderzoek dat breed door alle onderzoeksgroepen kan worden ingezet, moeten nu al worden onderzocht,

---

[2] Daartoe dienen de zogenaamde ALCOA beginselen: attributable, legible, contemporanous, orginal, accurate. Zie oa. http://www.ofnisystems.com/growing-need-for-good-data-and-record-management/ ALOCA is een strikt vereiste voor digitale gegevensverwerking bij clinical trials.

[3] Bij beschikbaarheid moet niet alleen worden gedacht of de onderzoeksgegevens beschikbaar zijn maar ook of informatie voor potentiële deelnemers beschikbaar is. In dat verband moet ook worden gedacht aan de 'web content accessibility guidelines'(WCAG). De vertaling van deze beginselen in een EU norm (EN 301 549) wordt in de toekomst verplicht over overheids- en semi-overheidssites.

aansluitend op bestaande initiatieven, zoals bijvoorbeeld IRMA. Met een dergelijk eID zou op korte termijn al betrouwbaarheidsniveau ‘substantieel’ kunnen worden bereikt.

1. Uitgangspunten voor eIC en de communicatie met de deelnemer (voorlopig)

1. Bij eIC zal de onderzoeker afwegingen kunnen maken. Een eenmalige anonieme enquête is wat anders dan een cohort waarbij de deelnemers langdurig worden gevolgd. Er is ook een relevant verschil tussen het uitnodigen van potentiële deelnemers waar niet melding wordt gemaakt van een bepaalde aandoening waarom ze worden uitgenodigd en van personen waarin in het bericht expliciet wel bijzondere persoonsgegevens worden vermeld of waar bijzondere persoonsgegevens uit kunnen worden afgeleid.
2. De volgende factoren spelen bij die afweging een rol, in relatie tot de gevoeligheid van de gegevens:
    a. De bescherming van de identiteit van de (potentiële) deelnemer;
    b. De bescherming van de gegevens van de deelnemer;
    c. De bewijsbaarheid van de toestemming;
    d. De integriteit van het onderzoek en de in dit verband op elektronische wijze verkregen gegevens. Met name of de beoogde deelnemer wel de werkelijke deelnemer is of degene die de vragen invult. Overigens geldt dit ook voor per post gezonden vragenlijsten, dus hier zit niet het werkelijke verschil tussen eIC en de analoge methode.
3. Dit tegen de achtergrond van een keten in de informatievoorziening aan de (beoogde) deelnemer, zijnde:
    - Uitnodigen;
    - Uitleg over onderzoek;
    - Toestemming verkrijgen;
    - Vervolg informatie over het verloop van het onderzoek;
    - Feed-back omtrent de resultaten op individueel niveau dan wel inzage in de op de deelnemer betrekking hebbende onderzoeksgegevens (zelf opgegeven of eventueel verrijkt met uitslagen van analyses);
    - Vervolg uitnodigingen voor nieuwe vragen of deelstudies.

    Aan deze stappen gaat selectie van de beoogde deelnemer vooraf. Dat valt niet onder de communicatie met de beoogde deelnemer en daarmee buiten deze notitie. Het spreekt vanzelf dat bij een eenmalig onderzoek het laatste punt geen rol speelt en het één na laatste punt meestal ook veel minder.
4. Voor uitnodigen van in beginsel gezonde vrijwilligers behoeven geen speciale voorzorgsmaatregelen te worden genomen. Dat kan via een email, gesteld dat men het mail adres zou hebben. Een email is ongeschikt als daaruit zou blijken dat de deelnemer een bepaalde aandoening heeft of daarvoor is behandeld. Een sms zou hiervoor wel geschikt kunnen zijn.
5. Attenderen op berichten, zoals uitnodigen, moet worden onderscheiden van de inhoud van wat men wil meedelen. Via het bericht kan men naar een site worden verwezen waar men kan inloggen.[4]

[4] Vergelijk een mail dat men een nieuw bericht heeft op 'Mijn Overheid'.

6. De algemene informatie op een site over een onderzoek zoals vraagstelling, waarom, welke deelnemers, hoe lang, de nieuwe ontwikkelingen etc. en privacyverklaring zijn openbaar. Daarvoor gelden geen bijzondere voorwaarden anders dan de algemene in verband met cybersecurity.[5] Maar bij de uitnodiging om kennis te nemen van nieuwe ontwikkelingen zal men zoals gezien moeten oppassen. Bevat de mail niet indirect bijzondere persoonsgegevens? Dat geldt ook voor vervolgmails over het verloop van het onderzoek. Ook hiervoor is een sms of een veilige app veel geschikter.
7. Als vervolgens na kennisname van de site het toestemmingsproces wordt doorlopen (waarbij drempels kunnen worden ingebouwd) moet op een of andere manier een 'matching' kunnen plaatsvinden tussen de uitnodiging en het toestemmingsproces. Idealiter doet de deelnemer dat via een eID. Maar dat eID is er voorzover bekend nog niet. Bij een anonieme enquête is dat een probleem voor de integriteit van het onderzoek (is de invullende deelnemer wel de beoogde deelnemer, op basis van de selectiecriteria) maar niet voor de vertrouwelijkheid van de gegevens van de deelnemer.[6] Voor een anonieme enquête heeft men in verband met de vertrouwelijkheid van de deelnemers, geen eID nodig. Voor een anonieme enquête geldt dat na voldoende uitleg klikken op doorgaan om in te vullen als voldoende toestemming geldt.
8. Voor de andere gevallen hangt het er van af. Bij een niet anoniem onderzoek[7] dient de toestemming tot de gegevensverwerking aantoonbaar te zijn en te worden bewaard.[8] Dat betekent dat de deelnemer zich op één of andere manier bekend moet maken of via de inlogmiddelen bekend moet zijn.
9. Die inlogmiddelen kunnen ook worden verstrekt indien de (beoogde) deelnemer bij de start van het onderzoek fysiek contact heeft met de onderzoekers of wie voor hen rekruteert, zoals een zorgaanbieder. Dan is slechts een deel van het proces via elektronische middelen. De identificatie vindt plaats bij de site waar wordt uitgenodigd. Via de aldus verstrekte inlogmiddelen zou de deelnemer op een beveiligde site toestemming kunnen geven en bijvoorbeeld diens mobiele nummer kunnen opgeven. Bij het vervolg van de communicatie moet men wel met het overigens hier gestelde rekening worden gehouden.
10. Indien de elektronische uitnodiging voor het onderzoek geen bijzondere persoonsgegevens vermeldt waarom de potentiële deelnemer wordt

---

[5] Het bezoek aan de site moet vertrouwelijk blijven, dus zonder tracking cookies etc.

[6] Uiteraard binnen de grenzen van de hier verder niet behandelde gegevensbeveiliging en cybersecurity in het algemeen, zoals het voorkomen dat de deelnemer 'op de digitale snelweg wordt afgeluisterd'.

[7] Voor de goede orde: als niet anoniem geldt ook een onderscheid bij dezelfde verwerkingsverantwoordelijke tussen contactgegevens en onderzoeksgegevens, gescheiden door een administratienummer.

[8] Een elektronische handetekening is hiervoor niet nodig. Voldoende is dat de toestemming aantoonbaar is.

uitgenodigd, zou dat kunnen via methoden die ook bij webwinkels gebruikelijk zijn. Ook als de persoon die toestemming geeft niet de beoogde deelnemer zou zijn, heeft die ander, niet beoogde deelnemer, wel toestemming gegeven. Uitsluitend een d probleem uit de opsomming onder 2 dus.

11. Indien die uitnodiging (per sms dus indien uitsluitend elektronisch) wel juist vanwege bijzondere persoonsgegevens wordt gedaan, moet het heen en weer verkeer via het internet voor het verkrijgen van de NAW gegevens niet als onvoldoende veilig worden beschouwd. Na het bezoeken van de site met uitleg zou dan kunnen worden gedacht aan een knop waarop men stelt in beginsel deel te willen nemen waarna een nieuwe sms volgt met een inlog.
12. Een en ander geldt ook voor follow-up vragenlijsten.
13. Indien men feed-back zou willen geven over de zelf ingevulde gegevens zal dat bij gezondheidsonderzoek steeds bijzondere persoonsgegevens betreffen. Dat kan nooit via zenden per email. In een elektronische omgeving moet de deelnemer die zelf ophalen. Dan gelden strikte voorwaarden waaraan ook het gewone DigiD momenteel niet voldoet (los van het punt dan het gezondheidsonderzoek dat niet kan gebruiken). Tenminste zal twee factor authenticatie (wat men weet, zoals een wachtwoord) en wat men heeft (zoals een inlogcode via de smartphone) moeten worden gebruikt. De authenticatie zal steeds de daadwerkelijke deelnemer moeten betreffen, niet de beoogde.
14. Om de beoogde deelnemer met de daadwerkelijke deelnemer te laten samenvallen, is bij de huidige mogelijkheden een moment van fysiek contact met deze (potentiële) deelnemer nodig (de identificatie) waarbij de authenticatiemiddelen kunnen worden verstrekt waar deelnemer en onderzoeker in het vervolg gebruik van kunnen maken.

2. Inleiding

Het veld (leden van COREON) heeft behoefte aan duidelijkheid over de mogelijkheden om op elektronische wijze het informeren en toestemming geven voor deelnamen aan gezondheidsonderzoek te organiseren . Een logische behoefte in het licht van de snel ontwikkelende samenleving waarin steeds meer communicatie elektronisch gaat. De overheid communiceert voornamelijk via een persoonlijke website (MijnOverheid) en zorginstellingen investeren in elektronische ontsluiting van patiëntgegevens in 'portals' zoals via het Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional (VIPP). Deze Notitie beoogt in die behoefte te voorzien

De centrale vraagstelling is als volgt: **Wat *verandert* er (of kan er veranderen) ten opzichte van papieren communicatie indien het hele of grotendeels het hele proces van informeren, toestemming geven, vragen invullen (bij langdurige cohorten) elektronisch verloopt.**

Daartoe wordt in deze Notitie met name ingegaan op de ontwikkelingen rond elektronische identificatie en authenticatie. In paragraaf 1 zijn de uitgangspunten geschetst bij de huidige mogelijkheden in de verschillende fases van het onderzoek. Hieronder volgt een uitleg van deze ontwikkelingen.

3. De (vele) voordelen van eIC

De voordelen zijn onder andere dat de communicatie met de deelnemers voor de onderzoekers directer verloopt. Er kan betere, vaak ook meer op de (potentiële) deelnemer toegesneden informatie worden aangeboden, zowel voorafgaand als gedurende de deelname. De informatie kan gelaagd worden aangeboden. Hoewel nog steeds moet worden voldaan aan de algemene voorwaarden voor gerichte en uitdrukkelijke toestemming, indien aan de orde, kan de drempel voor deelname worden verlaagd doordat men gegevens online invult.

De communicatie, met name bij het uitnodigen van deelnemers, kan gemakkelijker worden vormgegeven, aansluitend op een kanaal waar de deelnemer toch al aanwezig is. Gedurende het onderzoek kan makkelijker met de deelnemers worden gecommuniceerd.

Voor de deelnemers kan een voordeel zijn dat ook voor hen de communicatie makkelijker wordt, dat informatie meer aansluit op de eigen beleving (bijvoorbeeld door een animatie), dat - wanneer aan de orde - de drempel voor toestemming kan worden gecontroleerd (bijvoorbeeld door enkele toetsvragen voordat men verder kan) en dat men makkelijk inzage kan krijgen in de zelf ingevoerde of opgegeven gegevens. Al gelden voor dat laatste wel strenge veiligheidsnormen, zie hierna.

De deelnemer kan makkelijker zijn rechten uitoefenen als de identiteit gelijk bij het beroep op de rechten elektronisch kan worden geverifieerd.

4. Geen principiële bezwaren tegen eIC, wel praktisch en beperkingen in verband met doelgroep

Er zijn geen principiële argumenten tegen eIC bij gezondheidsonderzoek (buiten de WMO waar specifieke wettelijk eisen gelden). Het mag, mits veilig georganiseerd. Behoudens de voorwaarden voor gegevensveiligheid zijn er ook zijn geen principiële nadelen van eIC. Over die gegevensveiligheid *specifiek* voor eIC[9] gaan de volgende paragrafen.

Naast hetgeen daar wordt behandeld, kan de praktische inrichting van de portals, de elektronische vormgeving van het informatiemateriaal met 'leuke dingen' als animaties, extra kosten met zich meebrengen. De inrichting om werkelijk van de voordelen gebruik te kunnen maken, naast de website die elk cohort inmiddels wel heeft, zal soms meer kosten met zich mee kunnen brengen dan een folder.

Dat geldt ook voor het gebruik van elektronische handtekeningen en eID's.

Tot slot. Bij bepaalde groepen (ouderen, zwakke sociaal economische positie) moet er rekening mee worden gehouden dat deze niet via eIC kunnen worden bereikt. eIC werkt uitsluitend bij de digitaal vaardigen. Bij jongeren zal een praktisch probleem kunnen zijn dat email adressen en mobiele telefoonnummers nogal eens plegen te wijzigen.

Bij gebruik van een algemeen aanvaard eID zal dit laatste probleem veel minder spelen maar ook dan zal men er rekening mee moeten houden dat marginale groepen, die daarover niet beschikken, niet kunnen worden bereikt.

5. De discussie over 'e-identities' en de elektronische handtekening.

Algemeen

Al geruime tijd geldt in Nederland dat documenten elektronisch kunnen worden ondertekend, de elektronische handtekening. Daarnaast is er een nog lopende discussie over 'e-identities' waarmee iemand zich bekend kan maken bij een website en daar zaken kan regelen.

Hoewel de elektronische handtekening en 'e-identity' (eID) aan elkaar verwant zijn en beide zijn gebaseerd op dezelfde EU Verordening 910/2014[10], moeten zij in de uitwerking wel worden onderscheiden.

---

[9] Zoals opgemerkt in paragraaf 2, cybersecurity in het algemeen is geen onderwerp van deze Notitie

[10] Voluit: Europese Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, naar de Engelse term ingeburgerd als de eIDAS Regulation of Verordening. De Verordening is gefaseerd in

De elektronische handtekening betekent niet meer dan dat de persoon die ondertekent met de inhoud van een bepaald document instemt. Een eID betekent dat een bepaald persoon een hele reeks van handelingen kan verrichten bij alle webservices die dat eID herkennen. Het eID is daarmee een veel breder instrument.

Niveaus van veiligheid

Voornoemde eIDAS Verordening onderscheidt drie niveaus van veiligheid van e-identificatiemiddelen of dat nu het eID is of de elektronische handtekening, namelijk laag, substantieel en hoog. Daaraan vooraf gaat nog niveau 0. Een gewone email heeft niveau 0 ofwel geen beveiliging.

De eIDAS Verordening onderscheidt de volgende factoren die de betrouwbaarheid van een elektronisch middel bepalen namelijk:

- Kwaliteit identificatie natuurlijke persoon;
- Kwaliteit van de procedure waarin het middel wordt uitgereikt;
- Kwaliteitseisen aan de organisatie die het middel uitgeeft en alle overige betrokken organisaties;
- Beveiligingskenmerken van het authenticatiemechanisme.

Het gaat dus steeds om een combinatie van al deze factoren waarbij de zwakste schakel bepalend is voor het betrouwbaarheidsniveau. Het DigiD scoort laag op de identificatie en daarom is het betrouwbaarheidsniveau van het DigiD in het algemeen laag, ook bij DigiD met sms.

In bijlage 1 is het eIDAS schema weergegeven. Meer informatie, ook over aanvullende eIDAS voorwaarden in de Handreiking Betrouwbaarheidsniveaus voor digitale dienstverlening van het Forum Standaardisatie.[11]

Het Forum geeft een overzicht van de niveaus van betrouwbaarheid die in een bepaalde situatie van overheidsdienstverlening noodzakelijk zijn.

---

werking getreden. Voor de elektronische handtekening (vertrouwensdiensten) op 1-6-2016 en voor het Europese e-ID op 29-9-2018.

[11] https://www.forumstandaardisatie.nl/sites/bfs/files/atoms/files/Betrouwbaarheidsniveaus_voor_digitale_dienstverlening_v4.PDF

Diensten	Niveau authenticatie
• Anoniem bezoeken overheidswebsites • Gemeentelijke lokale diensten (zoals meldingen over de openbare ruimte of aanvragen afvalcontainers) • Inzien WOZ-waardering[11]	Geen eisen
• Registreren gepersonaliseerde portalen • Kapvergunning • Evenementvergunning • Omgevingsvergunning particulieren • Aangifte lichte delicten (zoals een gestolen fiets)	Laag
• Aangifte overlijden (door een begrafenisondernemer) • Melding voorgenomen huwelijk of geregistreerd partnerschap (door partners) • Aangifte geboorte (door ouder) • Vergunningaanvraag seksbedrijven • Vooringevulde aangifte belastingdienst • Belastingaangifte ondernemingen • Aanvraag subsidie • Aanvraag financiële toeslagen • Aangifte ernstige delicten (zoals mishandeling of huiselijk geweld)	Substantieel
• Raadplegen medisch dossier • Raadplegen beslissingen bestuursorgaan met (medische) gegevens • Raadplegen strafrechtelijke gegevens • Aanvraag screening voor een derde	Hoog

De eID discussie in Nederland

Om aan de eIDAS Verordening te voldoen zal de overheid een eID met betrouwbaarheidsniveau hoog moeten uitgeven. Hoog is noodzakelijk om volgens eIDAS ook bij overheidsdiensten in andere lidstaten te kunnen inloggen. Zoals gezien voldoet het huidige DigiD niet aan hoog.[12]

In het NICTIZ programma voor eID in de zorg wordt voor inloggen op de patiëntgegevens ook niveau hoog vereist.[13] Dat is nu voor de inlog op patiëntenportalen nog niet het geval.

Naast het door de overheid te ontwikkelen DigiD-plus (dat dus betrouwbaarheidsniveau hoog zou moeten bieden), is al een aantal andere aanbieders van digitale identiteiten actief zoals Idensys en iDIN van de banken.[14] Deze hebben nu betrouwbaarheidsniveau substantieel. In Nijmegen wordt IRMA ontwikkeld, een app waarbij in geval van authenticatie niet meer persoonsgegevens worden onthuld dan de betrokkene zelf wenst vrij te geven[15]. Omdat nu bij de app, naar het lijkt, geen controle op de identiteit van de betrokkene plaatsvindt, is het betrouwbaarheidsniveau daarvan vooralsnog laag.

---

[12] Er vindt geen controle op de identiteit plaats bij het aanvragen van een DigiD. Voor het DigiD plus denkt men aan chip in paspoort of rijbewijs die dan ingelezen kan worden bij de authenticatie. Zie de sectie over het wetsontwerp digitale overheid.

[13] https://www.nictiz.nl/programmas/eid-in-de-zorg/ voor de veilighiedsniveaus specifiek: https://www.nictiz.nl/wp-content/uploads/2017/05/Het-nieuwe-eID-stelsel-een-introductie-voor-de-zorgsector.pdf

[14] https://www.digitaleoverheid.nl/archief/identificatie-en-authenticatie/

[15] https://privacybydesign.foundation/irma/

Via een eID zou men uiteraard toestemming voor deelname aan gezondheidsonderzoek kunnen geven en zou de verdere communicatie kunnen plaatsvinden. Maar daartoe moet dat eID wel zijn ingeburgerd en dat is nu juist het probleem.

Het eID landschap is momenteel sterk in beweging en knopen zijn nog niet doorgehakt. De kosten spelen ook mee in de discussie: voor de overheid met betrekking tot de infrastructuur, voor de diensten die van een eID inlog gebruik maken (en dat zal ook voor de zorg gaan spelen)[16],[17] en voor de burger met betrekking tot de aanschaf van het middel. Waarschijnlijk worden meerdere eID middelen voor overheidsdoelen en de zorg toegelaten. Voor particuliere doelen staat de keuze vrij maar is niet zeker dat het overheids eID mag worden gebruikt. Tegelijk moet een 'digitale sleutelbos' worden voorkomen. Zie hierna de bespreking van het wetsontwerp digitale overheid.

Het wetsontwerp digitale overheid[18]

De wet die de door de overheid erkende eID's moet regelen is na een lange aanloop op 19 juni 2018 bij de TK ingediend.

In essentie en voorzover hier relevant regelt het wetsontwerp (in de wet zelf of via nog te verschijnen uitvoeringsmaatregelen):

a. Welk eID met betrouwbaarheid hoog door de overheid zal worden uitgegeven;
b. Welke overheid, semi-overheid en andere private organisaties dit eID mogen en dan ook moeten gebruiken in de zin van accepteren;
c. Hoe private eID middelen kunnen erkend met een zelfde betrouwbaarheidsniveau;
d. Welke andere organisaties dan onder b. eventueel kunnen worden aangewezen die het overheids eID ook mogen gebruiken.

Bij het overheids eID met betrouwbaarheid substantieel of hoog wordt gedacht aan een koppeling met rijbewijs of identiteitsbewijs waarvoor dan een aanpassing in de chip in die documenten zou moeten plaatsvinden.

De private organisaties onder b. zijn degenen die het BSN moeten gebruiken voor hun dienstverlening zoals zorgverzekeraars en pensioenfondsen.

Bij c is sprake van een 'kan' bepaling. Er staat dus niet in het wetsontwerp dat indien een dergelijk privaat eID middel aan bepaalde voorwaarden voldoet, de minister dit moet toelaten. Daarover heeft de TK in het verslag vragen gesteld.

---

[16] https://vng.nl/onderwerpenindex/dienstverlening-en-informatiebeleid/nieuws/mijnoverheid-en-digid-mogelijk-geen-factuur-in-2018 .

[17] https://www.volkskrant.nl/economie/digid-gaat-geld-vragen-aan-gebruikers-dat-gaat-pensioenfondsen-2-miljoen-euro-extra-kosten~b8528cc3/ Overigens blijkt de regering de in deze en de vorige noot genoemde problemen te onderkennen, zie Kamerstuk 26643, nr. 590, p. 4/5.

[18] Kamerstukken 34972

Voor gezondheidsonderzoek kan d. van groot belang zijn. Idealiter zijn er enkele algemeen gebruikte eID middelen. Voor betrouwbaarheid hoog raakt mogelijk echter uitsluitend het overheids eID breed ingeburgerd. Hoog is nodig om iemand toegang te kunnen geven tot diens bijzondere persoonsgegevens en dus van diens rechten op grond van de AVG gebruik te kunnen laten maken.

Indien het gezondheidsonderzoek van dit algemeen ingeburgerd overheids eID geen gebruik zou mogen maken, bestaat de kans dat de voordelen van eIC niet over de volle breedte worden bereikt.

De elektronische handtekening

Net als de gewone handtekening is deze is bedoeld om aan te tonen dat degene wiens naam onder het document staat met de inhoud van het daar verklaarde instemt. In niet elektronische situaties heeft die persoon zich meestal eerst geïdentificeerd of anders mag je daarop vertrouwen. Er is in ieder geval een 'natte' handtekening.

In het elektronisch berichtenverkeer is dat minder zeker. Een gescande handtekening kan makkelijk in een ander document worden geplakt waar de persoon van de gescande handtekening geen weet van heeft.

De Nederlandse regeling van de elektronische handtekening beoogt hierin te voorzien. Op grond van voornoemde EU verordening bestaan er in Nederland twee typen elektronische handtekeningen[19], namelijk de 'geavanceerde elektronische handtekening' en 'andere elektronische handtekeningen'. Bij de geavanceerde elektronische handtekening is de identiteit van de persoon door een erkende derde partij (een zogenaamde 'vertrouwensdienst') vastgesteld en verbonden aan het authenticatiemiddel waarmee de handtekening wordt geplaatst. Bij de andere elektronische handtekeningen is dat niet het geval. Dat betekent echter niet dat deze in het rechtsverkeer per definitie minder waarde hebben. Beide hebben volgens het Nederlands recht "dezelfde rechtsgevolgen als een handgeschreven handtekening, indien voor deze beide elektronische handtekeningen de methode voor ondertekening die gebruikt is voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekening is gebruikt en op alle overige omstandigheden van het geval".

Er is een aantal commerciële aanbieders van de elektronische handtekening en men heeft dus een keuze.

Maar overigens is het de vraag of het onderzoek de kant van de elektronische handtekening op zou willen. Voor de 'bewijsfunctie' in gezondheidsonderzoek is uitsluitend de uitdrukkelijke toestemming van belang. Dat zou ook via eID van niveau substantieel kunnen worden vormgegeven. Ook de 'drempelfunctie' van een handtekening kan na inloggen via

[19] Zie ook artikel 3:15 a BW zoals dat luidt na de invoering van de Wet uitvoering EU-verordening elektronische identiteiten en vertrouwensdiensten die op 28-2-2017 in werking is getreden.

een eID in een webomgeving worden bereikt, mogelijk zelfs beter, zoals eerst het invullen van een aantal vragen.

Het vervolgens downloaden van een formulier, van een e-handtekening voorzien en dan weer opladen, lijkt dan toch een omweg.

Conclusies bij deze paragraaf

Een eID met beveiliging hoog is vooralsnog niet beschikbaar. Het door de overheid te ontwikkelen DigiD-plus zal volgens het wetsontwerp digitale overheid niet voor wetenschappelijk onderzoek kunnen worden gebruikt. Tegelijk zal dit overheids eID, zo niet het enige eID met betrouwbaarheidsniveau hoog, zeer waarschijnlijk wel het meest gangbare eID met dit niveau worden.[20]

Dan is het de vraag of alle voordelen van eIC wel kunnen worden bereikt. Dat zou er voor pleiten dat ook organisaties die gezondheidsonderzoek uitvoeren dit overheids eID mogen gebruiken, ook al betreft het geen elektronische dienstverlening en is op de achtergrond bij het overheids eID het BSN actief.

COREON zou hiertoe een gesprek kunnen aangaan met de betrokken ministeries.

Er zijn nu al eID's met beveiligingsniveau substantieel. Deze zijn echter niet breed ingevoerd.[21] Een idee zou zijn om 'in te stappen' in de verdere ontwikkeling van de IRMA app (de achterliggende software is open source) speciaal voor wetenschappelijk onderzoek. Indien deze speciaal voor wetenschappelijk onderzoek kan worden ontwikkeld, speelt het probleem van de digitale sleutelbos (waar je de juiste sleutel niet vindt) mogelijk veel minder. Eventueel zou dit eID ook kunnen worden erkend met betrouwbaarheid hoog. Uiteraard gaat dit onderzoek de mogelijkheden van een bepaalde onderzoeksgroep te boven. Dit zou bijvoorbeeld via TraIT, Lygature of Surf kunnen worden opgepakt.

[20] De burger zal kosten moeten maken voor de aanschaf van het eID.

[21] Binnen de omgeving van banken is daar wel sprake van maar die middelen zijn uitsluitend binnen de eigen omgeving van de bank bruikbaar. De kosten zijn in de prijs van het product meegenomen.

Bijlage, bepalen betrouwbaarheidsniveau

Figuur 3. eIDAS geeft vier factoren om een authenticatiemiddel op te scoren. De laagste score bepaalt het uiteindelijke niveau van het authenticatiemiddel.