WHITEPAPER

April 2020

eIDAS EN DE ZORGSECTOR

Een beknopte inleidende tekst rond eIDAS, toegespitst op de zorgsector, met name de onderdelen e-identificatie en e-handtekening.

Beer Franken, april 2020

INHOUD

eIDAS is wetgeving die weliswaar al vanaf 2016 van kracht is, maar desondanks grote onbekendheid geniet. In eIDAS worden verschillende elektronische zekerheden, zoals e-handtekeningen en e-identificatie, vastgelegd.[1] Binnen de zorgsector zijn e-identificatie en e-handtekening van groot belang en dit neemt alleen maar toe. In deze whitepaper wordt een eerste inleiding in de werking en het gebruik van zekerheden als e-identificatie en e-handtekening gegeven, zoals die door eIDAS is voorgeschreven.

Deze tekst is samengesteld door Beer Franken,[2] zelfstandig adviseur op de gebieden gegevensbescherming en informatiebeveiliging, voormalig FG en CISO bij het AMC, lid van de normcommissies 303006 (Informatievoorziening in de zorg), 381027 (Informatiebeveiliging, cyber security en privacy) en 381038 (Cloud computing and distributed platforms). Ook leverde hij inhoudelijke bijdragen bij de totstandkoming/herziening van de normen NEN 7510 (Informatiebeveiliging in de zorg), NEN 7512 (Vertrouwensbasis voor gegevensuitwisseling, NEN 7513 (Logging toegang patiëntdossiers), NEN 7524 (Pseudonimisatiedienstverlening) en NTA 7516 (Veilige e-mail en chat) en normontwerp NEN 7521 (Decentrale toestemmingsverlening).

1 eIDAS behandelt ook e-zegels, e-tijdstempels, e-documenten, e-aangetekende bezorgingsdiensten en e-certificatiediensten voor websiteauthenticatie, maar daar wordt in deze tekst niet verder ingegaan.

2 Bereikbaar via beer.franken@piasau.nl en 06 5534 7977.

eIDAS EN DE ZORGSECTOR

Een beknopte inleidende tekst rond eIDAS, toegespitst op de zorgsector, met name de onderdelen e-identificatie en e-handtekening

Beer Franken, april 2020

INLEIDING

In deze tekst wordt ingegaan op de eisen voor gebruik van e-identificatie en e-handtekeningen binnen de zorgsector. Deze vloeit voort uit EU-regelgeving, bekend onder de naam eIDAS. De betreffende wetgeving is niet makkelijk toegankelijk. Deze tekst probeert daar een handreiking voor te bieden.

1.1 Identificatie (en authenticatie)

Identificeren wordt vaak in samenhang met authentiseren genoemd. Identificeren is het 'claimen' van een bepaalde identiteit ('ik ben Jan'), terwijl je met authentiseren daarvoor het bewijs levert ('kijk maar in m'n paspoort'). Omdat deze begrippen zo dicht tegen elkaar aanliggen, wordt ook vaak één van de begrippen voor beide bedoeld.

In deze tekst spreken we verder uitsluitend over identificeren, terwijl we vaak ook authentiseren bedoelen. Een enkele keer wordt authentiseren aangehaald als we heel specifiek authentiseren (het leveren van bewijs) bedoelen.
In de fysieke wereld is identificeren een ingeburgerd proces. Als je bijvoorbeeld naar buiten gaat of een bankrekening opent, moet je je kunnen identificeren. Maar in de online-wereld is identificeren een lappendeken. Dan kun je weer aanmelden met een gebruikersnaam en wachtwoord, daar moet het met aanvullend met een sms-code op de mobiele telefoon, ergens anders kan het met een Facebook- of Google-account etc. Alle oplossingen hebben duidelijke beperkingen ten opzichte van identificeren in de fysieke wereld.

De EU richt zich op het vrije verkeer van personen, goederen, diensten en kapitaal en constateert dat een versnipperde aanpak van online identificatie (of e-identificatie) het vrije verkeer belemmert. Lidstaten willen voorkomen dat één van hen belemmeringen gaat opwerpen voor het vrije verkeer van de andere. Bijvoorbeeld door lokale invulling te verlangen.

1.2 De handtekening

De handtekening kennen we allemaal en vanaf het moment dat we zo'n beetje een potlood konden vasthouden hebben we 'm ook allemaal geoefend.
In de wet is verrassend weinig vastgelegd over de handtekening. Wel wordt regelmatig in een wet aangehaald dat ergens een handtekening moet worden geplaatst (bijvoorbeeld voor een paspoort), maar nergens worden eisen aan de handtekening gesteld. Ook algemene gebruiksregels ontbreken in de wet. In het gewoonterecht betekent een handtekening veelal dat je ergens mee akkoord bent. En dat je zo'n akkoord kunt ontkennen door erbij 'voor gezien' te vermelden of door geen handtekening te zetten.

Informatici beschouwen een handtekening als een non-repudiation maatregel. Met andere woorden: als er een handtekening is gezet, dan kan de tekenende partij niet meer ontkennen waarvoor hij/zij heeft getekend. En als je tekent voor ontvangst van een pakketje aan de deur, is dat ook precies wat je doet. Je kunt naderhand niet meer ontkennen dat je het pakketje hebt ontvangen.

De wereld van de elektronische handtekening (hierna: e-handtekening) is echter niet gebaseerd op gewoonterecht, maar strak gecodificeerd in wetten. En die vloeien allemaal voort uit EU-regelgeving. De reden is dat de EU zich richt op vrij verkeer van personen, goederen, diensten en kapitaal. Ook hier ligt het dus in de rede dat lidstaten willen voorkomen dat één van hen belemmeringen gaat opwerpen voor het vrije verkeer. Bijvoorbeeld door exotische eisen aan een e-handtekening te stellen.

2 eIDAS

De oorsprong van EU-regelgeving is te vinden in «Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen». Lidstaten moesten de richtlijn voor medio 2001 in eigen wetgeving implementeren. Die nationale implementaties liepen een beetje uiteen en er was inmiddels meer ervaring met e-handtekeningen opgedaan, wat leidde tot «Verordening (EU) Nr. 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». Verordening 910/2014 trad medio 2016 in werking (en richtlijn 1999/93 werd ingetrokken).

Verordening 910/2014 heeft een veelgebruikte bijnaam: eIDAS. Deze naam staat voor *electronic identification and trust services for electronic transactions*. In deze tekst wordt verder uitsluitend verwezen naar eIDAS in plaats van Verordening 910/2014.

Een verordening (en dus ook eIDAS) heeft rechtstreekse werking. Dat wil zeggen dat een verordening niet in nationale wetgeving hoeft te worden geïmplementeerd. Anders gezegd: wat in de verordening staat is de wet. Maar waar richt eIDAS zich precies op? Dat wordt duidelijk in de artikelen 1 en 2 van eIDAS (onderwerp en toepassingsgebied):

- het wederzijds erkennen van elektronische identificatiemiddelen van natuurlijke en rechtspersonen, voor zover zij door een lidstaat zijn aangemeld; [3]
- regels voor vertrouwensdiensten (voor met name elektronische transacties) in niet-gesloten stelsels (denk voor gesloten stelsels in Nederland aan het notariaat, rechtspraak etc.); en
- juridisch kader vaststellen voor elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, elektronische aangetekende bezorgingsdiensten en certificatiediensten voor websiteauthenticatie.

eIDAS legt kort gezegd regels neer voor:
- elektronische identificatie,
- vertrouwensdiensten,
- elektronische handtekeningen,
- elektronische zegels,
- elektronische tijdstempels,
- elektronische documenten,
- elektronische aangetekende bezorgingsdiensten en
- certificatiediensten voor websiteauthenticatie.

In deze tekst gaan we verder uitsluitend in op e-identificatie en e-handtekeningen.

3 Eind 2019 heeft Nederland eHerkenning aangemeld. Hiermee kunnen functionarissen van een rechtspersoon zich identificeren. DigiD (het identificatiemiddel voor natuurlijke personen) is niet aangemeld omdat het nog niet aan de eisen van eIDAS voldoet.

2.1 E-identificatie

eIDAS kent drie betrouwbaarheidsniveaus voor e-identificatie (verschillen vet weergegeven): [4]

betrouwbaarheidsniveau laag	Een e-identificatiemiddel dat een **beperkte** mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te **verkleinen**.
betrouwbaarheidsniveau substantieel	Een e-identificatiemiddel dat een **substantiële** mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te **verkleinen**.
betrouwbaarheidsniveau hoog	Een e-identificatiemiddel dat een **hogere** mate van vertrouwen in iemands opgegeven of beweerde identiteit biedt **dan een elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel**, en wordt toegekend onder verwijzing naar technische specificaties, normen en procedures die daarmee verband houden, onder meer technische controles die tot doel hebben het risico van misbruik of wijziging van identiteit te **voorkomen**.

Wanneer welk betrouwbaarheidsniveau vereist is, is slechts mondjesmaat vastgelegd in wet- en regelgeving. Wel is voor de zorgsector een uitspraak van de Autoriteit persoonsgegevens[5] (AP) van belang: bij authenticatie door een patiënt is 'minimaal niveau "substantieel" vereist' en voor toegang tot 'gegevens waarop het medisch beroepsgeheim van de hulpverlener rust, is betrouwbaarheidsniveau "hoog" vereist'.[6]

Samengevat:

- voor patiënten/cliënten geldt minimaal betrouwbaarheidsniveau substantieel; en
- voor alle (professionele) anderen geldt betrouwbaarheidsniveau hoog.

Onduidelijk is welk betrouwbaarheidsniveau zou moeten gelden voor mantelzorgers…

4 eIDAS art 8 lid 2.

5 Integraal opgenomen in de bijlage.

6 De AP gaat verder nog in op voorlopige maatregelen, maar die laten wij hier buiten beschouwing. Immers, deze tekst behandelt 'hoe het hoort'.

2.2 E-handtekening

eIDAS kent twee soorten e-handtekeningen en erkent impliciet een derde:[7]

gewone e-handtekening	Bijvoorbeeld de afzender van een normaal e-mailbericht. Dit kan een persoon correct aanwijzen, maar het kan ook een alias zijn of zelfs volstrekt misleidend.
geavanceerde e-handtekening	Een e-handtekening die voldoet aan de volgende eisen: - op unieke wijze aan de ondertekenaar verbonden; - maakt het mogelijk de ondertekenaar te identificeren; - komt tot stand met gegevens voor het aanmaken van e-handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken; en - op zodanige wijze aan de daarmee ondertekende gegevens verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.
gekwalificeerde e-handtekening	Een geavanceerde e-handtekening (met de daarbij geldende eisen) die: - is aangemaakt met een gekwalificeerd middel voor het aanmaken van e-handtekeningen en - gebaseerd is op een gekwalificeerd certificaat voor e-handtekeningen.

Wat de verschillende rechtsgevolgen zijn, is als volgt te beschouwen:

gewone e-handtekening	Ondertekening is 'voldoende betrouwbaar' is gelet op het doel waarvoor de elektronische handtekening is gebruikt en alle overige omstandigheden van het geval.[8]
geavanceerde e-handtekening	Tussengebied – tussen gewoon en gekwalificeerd – waarvan in verschillende wetten gebruik wordt gemaakt, zoals de Algemene wet bestuursrecht, het Burgerlijk wetboek boek 2, de Kadasterwet etc.
gekwalificeerde e-handtekening	Per definitie hetzelfde rechtsgevolg als van een handgeschreven[9] ('natte') handtekening , ook als het in een ander EU-lidstaat is ondertekend (met behulp van de betreffende middelen aldaar). Ook hiernaar kan (en wordt) in verschillende wetten verwezen.

7 eIDAS art 25, 26 en 28.

8 Art 3:15a BW. Een informatievraag naar parkeermogelijkheden bij een instelling is een duidelijk voorbeeld.

9 eIDAS art 25 lid 2.

Vanuit zorgwetten wordt niet verwezen naar een specifieke vorm van e-handtekening.[10] Wel kan een norm (bijvoorbeeld NTA 7516[11]) gebruik van een e-handtekening voorschrijven. Elke organisatie, instelling en praktijk moet dus nadenken over wanneer welke vorm van e-handtekening nodig is. Twee voorbeelden uit de praktijk:

- een e-mail met de vraag 'wat zijn de bezoektijden?' kan uitstekend worden ondertekend met een gewone e-handtekening;
- een verzoek om inzage in het medisch dossier vergt een gekwalificeerde e-handtekening.

Ook berichten met potentieel grote gevolgen (risico's) zijn duidelijke kandidaten voor de gekwalificeerde e-handtekening:

- denk bij risico's voor een patiënt zoals bij de medicatieopdracht (gezondheidsschade in geval van misplaatste zelfmedicatie);
- denk bij risico's voor een verwijzer zoals bij de verwijsbrief (fraudering in geval van vervalsing);
- denk bij risico's voor een organisatie zoals bij toestemming voor het delen van patiënt-/cliëntgegevens met derden (privacyschade als gevolg van een datalek).

10 In zorgwet- en regelgeving wordt trouwens nauwelijks naar handtekeningen (e- of anderszins) verwezen. Het woord 'handtekening' wordt aangetroffen in enkele besluiten, zoals het besluit hersendoorprotocol, het besluit donorregister, het besluit gesteriliseerde hulpmiddelen in ziekenhuizen en het besluit sterilisatiebedrijven medische hulpmiddelen.

11 NTA 7516:2019 Medische informatica - Eisen voor veilige e-mail en chatapplicaties (uitwisseling van ad-hocberichten met persoonlijke gezondheidsinformatie).

3 GEDELEGEERDE HANDELINGEN

Organisaties, instellingen en praktijken moeten nadenken over welke e-handtekening waarbij moet worden gebruikt en welke e-identificatie waarvoor nodig is. Maar gelukkig is de invulling van e-identificatie en van e-handtekeningen redelijk tot in detail uitgewerkt. Op basis van eIDAS is de Europese Commissie bevoegdheid verleend om bepaalde zogenaamde gedelegeerde handelingen vast te stellen.[12] In dat kader zijn van belang:

Verordening 2015/1502 ook bekend als UeIDAS	«Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt» en
Besluit 2015/1506	«Uitvoeringsbesluit (EU) 2015/1506 van de Commissie van 8 september 2015 tot vaststelling van specificaties betreffende formaten van geavanceerde elektronische handtekeningen en geavanceerde zegels die door openbare instanties moeten worden erkend overeenkomstig respectievelijk artikel 27, lid 5, en artikel 37, lid 5, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt»

3.1 UeIDAS

In de bijlage van UeIDAS zijn technische specificaties en procedures voor de betrouwbaarheidsniveaus laag, substantieel en hoog voor e-identificatiemiddelen middelen uitgeschreven. Het gaat hierbij om de volgende onderwerpen:

- Inschrijving
  - Aanvraag en registratie
  - Bewijs en verificatie van identiteit (natuurlijke persoon respectievelijk rechtspersoon)
  - Koppeling tussen de elektronische identificatiemiddelen van
- Beheer van elektronische identificatiemiddelen
  - Kenmerken en ontwerp van elektronische identificatiemiddelen
  - Uitgifte, uitreiking en activering
  - Schorsing, herroeping en reactivering
  - Verlenging en vervanging
- Authenticatie(mechanisme)
- Beheer en organisatie
  - Algemene bepalingen
  - Gepubliceerde mededelingen en informatie voor de gebruikers
  - Beheer van informatiebeveiliging
  - Bijhouden van de administratie
  - Faciliteiten en personeel
  - Technische controles
  - Compliance en audit

12 eIDAS art 30 lid 4.

De opsomming alleen al geeft al aan dat het inrichten van een e-identificatiedienst geen sinecure is. Maak daarom gebruik van een door de Nederlandse overheid aangemelde identificatiestelsel. Eind 2019 heeft Nederland hiervoor eHerkenning aangemeld. Hiermee kunnen functionarissen van een rechtspersoon zich identificeren.

DigiD (het identificatiemiddel voor natuurlijke personen) is niet aangemeld, omdat het nog niet aan de eisen van eIDAS voldoet. Controleer regelmatig (eens per kwartaal) of de lijst van de EU is uitgebreid[13] of volg andere berichtgeving. Een centrale website met het meest actuele overzicht van aangemelde identificatiestelsels is helaas niet beschikbaar.

3.2 Besluit 2015/1506

Besluit 2015/1506 maakt duidelijk waaraan een e-handtekening moet voldoen. Er zijn drie verschillende handtekeningen: XML-handtekening, CMS-handtekening en PDF-handtekening. In de bijlage van het besluit worden de technische specificaties voor geavanceerde e-handtekeningen belegd in een viertal standaarden:

XAdES Baseline Profile (XML)	ETSI TS 103 171 V2.1.1 (2012-03)	https://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
PAdES Baseline Profile (PDF)	ETSI TS 103 172 V2.2.2 (2013-04)	http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf
CAdES Baseline Profile (CMS)	ETSI TS 103 173 V2.2.1 (2013-04)	http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
Associated Signature Container Baseline Profile	ETSI TS 103 174 V2.2.1 (2013-06)	http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

In de baseline profiles voor XAdES, PAdES en CAdES worden conformiteitsniveaus (conformance levels) gebruikt die aangeven voor welke tijdspanne een e-handtekening kan worden gebruikt:

B biedt zekerheid dat een e-handtekening geldt op het moment dat werd getekend.
T biedt zekerheid dat een handtekening op een bepaald moment gold.
LT biedt zekerheid dat een handtekening op lange termijn kan worden gevalideerd.
LTA biedt extra zekerheid op langere termijn (archivering) door middel van time-stamping.

Let op: conformiteitsniveau LTA is uitgesloten in Besluit 2015/1506![14]

13 Zoek op internet naar “Stelsels voor elektronische identificatie aangemeld overeenkomstig artikel 9, lid 1”.

14 Besluit 2015/1506 art 1.

Een kleine leeswijzer rond AdES is op z'n plaats:

e-handtekening	object	hoe te signen	hoe signing veilig te doen (Besluit 2015/1506)
XAdES	eXtensible mark-up language (XML)	ETSI TS 101 903	ETSI TS 103 171
PAdES	Portable document format (PDF)	ETSI TS 102 778/3,4	ETSI TS 103 172
CAdES	Cryptographic message syntax (CMS)	ETSI TS 101 733	ETSI TS 103 173

Let op: met de ETSI-standaarden zitten we op het niveau van geavanceerde e-handtekeningen. Voor gekwalificeerde e-handtekeningen geldt bovendien dat die is aangemaakt met een gekwalificeerd middel voor het aanmaken van e-handtekeningen en is gebaseerd op een gekwalificeerd certificaat voor e-handtekeningen.

Waar de gekwalificeerde middelen aan moeten voldoen, is vastgelegd in bijlage II van eIDAS:

1 Gekwalificeerde middelen voor het aanmaken van e-handtekeningen waarborgen via passende technieken en procedures dat ten minste:
   a de vertrouwelijkheid van de gegevens die worden gebruikt om e-handtekeningen aan te maken redelijkerwijs gewaarborgd is;
   b de gegevens voor het aanmaken van e-handtekeningen in de praktijk slechts één keer kunnen voorkomen;
   c de gegevens voor het aanmaken van e-handtekeningen met redelijke zekerheid niet kunnen worden afgeleid en dat de e-handtekening op betrouwbare wijze beschermd is tegen vervalsing met de thans beschikbare technologie;
   d de gegevens voor het aanmaken van e-handtekeningen door de legitieme ondertekenaar op betrouwbare wijze kunnen worden beschermd tegen gebruik door anderen.
2 Gekwalificeerde middelen voor het aanmaken van e-handtekeningen laten de te ondertekenen gegevens ongewijzigd en beletten niet dat die gegevens vóór ondertekening aan de ondertekenaar worden voorgelegd.
3 Het genereren of beheren van de gegevens voor het aanmaken van e-handtekeningen namens de ondertekenaar kan alleen worden uitgevoerd door een gekwalificeerde verlener van vertrouwensdiensten.
4 Onverminderd punt 1, onder d, mogen gekwalificeerde verleners van vertrouwensdiensten die namens de ondertekenaar gegevens voor het aanmaken van e-handtekeningen beheren, de gegevens voor het aanmaken van e-handtekeningen alleen dupliceren voor back-updoeleinden, op voorwaarde dat aan de volgende eisen wordt voldaan:
   a de beveiliging van de gedupliceerde gegevensverzamelingen moet van hetzelfde niveau zijn als de beveiliging van de originele gegevensverzamelingen;
   b het aantal gedupliceerde gegevensverzamelingen mag niet hoger zijn dan het minimum dat nodig is om de continuïteit van de dienst te waarborgen.

Gekwalificeerde certificaten moeten bevatten (bijlage I van eIDAS):

a een vermelding, ten minste in een vorm die geschikt is voor automatische verwerking, dat het certificaat afgegeven is als een gekwalificeerd certificaat voor e-handtekeningen;
b een reeks gegevens die ondubbelzinnig verwijzen naar de gekwalificeerde verlener van vertrouwensdiensten die de gekwalificeerde certificaten afgeeft, met inbegrip van ten minste de lidstaat waarin de verlener is gevestigd en
   - voor een rechtspersoon: de naam en, indien van toepassing, het registratienummer zoals vermeld in de officiële registers,
   - voor een natuurlijke persoon: de naam van de persoon;
c op zijn minst de naam van de ondertekenaar of een pseudoniem; als er een pseudoniem wordt gebruikt, wordt dat duidelijk aangegeven;
d gegevens voor de validering van e-handtekeningen, die overeenkomen met de gegevens voor het aanmaken van de e-handtekening;
e informatie over begin en einde van de geldigheidsduur van het certificaat;
f de identiteitscode van het certificaat, die uniek moet zijn voor de gekwalificeerde verlener van vertrouwensdiensten;
g de geavanceerde e-handtekening of het geavanceerde e-zegel van de afgevende gekwalificeerde verlener van vertrouwensdiensten;
h de locatie waar het certificaat ter ondersteuning van de geavanceerde e-handtekening of het geavanceerde e-zegel als bedoeld onder g) gratis beschikbaar is;
i de locatie van de diensten waar informatie kan worden opgevraagd over de geldigheidsstatus van het gekwalificeerde certificaat;
j indien de gegevens voor het aanmaken van een e-handtekening die gekoppeld zijn aan de gegevens voor de validering van de e-handtekening zich bevinden in een gekwalificeerd middel voor het aanmaken van e-handtekeningen, een passende vermelding hiervan, ten minste in een vorm die geschikt is voor automatische verwerking.

Bovendien volgen uit de Telecommunicatiewet (art 18.15a – 18.15e) aanvullende eisen.

Wederom geen sinecure. Het is verstandig om gebruik te maken van door de Nederlandse overheid aangemelde aanbieders van vertrouwensdiensten. Een actuele lijst van dergelijke aanbieders wordt door de EU bijgehouden op https://webgate.ec.europa.eu/tl-browser/#/tl/NL (kijk naar aanbieders met het label ‘QCert for ESig’).

4 IMPLEMENTATIEHANDREIKING

Om aan eIDAS te kunnen voldoen, moeten drie stappen worden doorlopen: beleid opstellen, huidige situatie in kaart brengen en in overleg gaan met de leveranciers van software en diensten. Een en ander is nader toegelicht in de volgende paragrafen.

4.1 Beleid

De praktijk, organisatie, instelling moet beleid ontwikkelen, waaruit blijkt op welke plaatsen, in welke situaties en onder welke omstandigheden welke van de drie verschillende betrouwbaarheidsniveaus voor e-identificatie nodig is, respectievelijk welke soort e-handtekening nodig is.

Raadpleeg de betreffende koepelorganisatie om te bezien of er misschien een modelbeleid beschikbaar is.

4.2 Inventarisatie

De plaatsen, situaties, omstandigheden en voorwaarden moeten worden geïnventariseerd die volgens het zojuist ontwikkelde beleid moeten voldoen aan een specifiek betrouwbaarheidsniveaus voor e-identificatie dan wel een bepaalde soort e-handtekening moet gebruiken.

Leg tegelijk vast welke software of dienst daarbij wordt gebruikt, én of die software of dienst al een zeker betrouwbaarheidsniveau of bepaalde e-handtekening toepast.

4.3 Leveranciers

Aan de leveranciers van zojuist geïnventariseerde software en diensten moet duidelijk worden gemaakt dat de instelling/organisatie/praktijk wil kunnen voldoen aan geldende wetgeving en dat het daarvoor de software dan wel dienstverlening op bepaalde plaatsen moet worden aangepast, zodat wordt voldaan aan de in de eerste stap ontwikkelde beleid.

Voor eigen software of diensten, die in eigen beheer worden geleverd, kan wat betreft e-handtekening een beroep worden gedaan op door de Nederlandse overheid aangemelde leveranciers van vertrouwensdiensten (die de laatste alinea van paragraaf 3.2. Voor e-identificatie moet, zolang de Nederlandse overheid nog geen identificatiestelsel voor natuurlijke personen heeft aangemeld, gebruik worden gemaakt van de richtlijn die de AP geeft in haar brief (zie bijlage) op bladzijde 4 (pagina 17 in dit document) onder het kopje ‘Wat te doen in de tussentijd?’.

REFERENTIES

Richtlijn 1999/93 (ingetrokken)	Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen	
Verordening 910/2014 (eIDAS)	Verordening (EU) Nr. 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	Zoek op internet naar “910 2014”.
Verordening 2015/1502 (UeIDAS)	Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt	Zoek op internet naar “2015 1502”.
Besluit 2015/1506	Uitvoeringsbesluit (EU) 2015/1506 van de Commissie van 8 september 2015 tot vaststelling van specificaties betreffende formaten van geavanceerde elektronische handtekeningen en geavanceerde zegels die door openbare instanties moeten worden erkend overeenkomstig respectievelijk artikel 27, lid 5, en artikel 37, lid 5, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt	Zoek op internet naar “2015 1506”.
ETSI TS 103 171	Electronic Signatures and Infrastructures (ESI); XAdES Baseline Profile	Zoek in etsi.org naar ‘standards’ en “103171”.
ETSI TS 103 172	Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile	Zoek in etsi.org naar ‘standards’ en “103172”.
ETSI TS 103 173	Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile	Zoek in etsi.org naar ‘standards’ en “103173”.
ETSI TS 103 174	Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile	Zoek in etsi.org naar ‘standards’ en “103174”.
ETSI TS 101 903	Electronic Signatures and Infrastructures (ESI);XML Advanced Electronic Signatures (XAdES)	Zoek in etsi.org naar ‘standards’ en “101903”.
ETSI TS 102 778-3	Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles	Zoek in etsi.org naar ‘standards’ en “102778”.
ETSI TS 102 778-4	Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 4: PAdES Long Term - PAdES LTV Profile	Zoek in etsi.org naar ‘standards’ en “102778”.
ETSI TS 101 733	Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)	Zoek in etsi.org naar ‘standards’ en “101733”.
Aangemelde identificatiemiddelen	Zoek op internet naar “Stelsels voor elektronische identificatie aangemeld overeenkomstig artikel 9, lid 1”.	
Aangemelde aanbieders van vertrouwensdiensten	Zie https://webgate.ec.europa.eu/tl-browser/#/tl/NL en kijk naar aanbieders met het label “QCert for ESig”.	

BIJLAGE AUTHENTICATIEVEREISTEN VOLGENS AP

AUTORITEIT
PERSOONSGEGEVENS

Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
Bezuidenhoutseweg 30, 2594 AV Den Haag
T 070 8888 500 - F 070 8888 501
autoriteitpersoonsgegevens.nl

Ministerie van Volksgezondheid, Welzijn en Sport
t.a.v. de secretaris-generaal
Directie Wetgeving en Juridische Zaken (cluster 6)
Parnassusplein 5
2511 VX DEN HAAG

Datum	Ons kenmerk	Uw brief van
4 oktober 2018	z2018-17577	26 juli 2018
	Contactpersoon	Uw kenmerk

Onderwerp
Patiëntauthenticatie

Geachte,

Bij brief van 26 juli 2018 hebt u bij de Autoriteit persoonsgegevens (AP) aandacht gevraagd voor patiëntauthenticatie bij digitale informatie-uitwisseling tussen zorgaanbieders en patiënten. In uw brief geeft u aan dat in het zorgveld opnieuw vragen zijn ontstaan over welk niveau van patiëntauthenticatie op dit moment gebruikt dient te worden voor het uitwisselen van medische gegevens tussen zorgverleners en patiënten. In reactie op uw brief bericht de AP u als volgt.

1 Algemeen

Innovatieve technologie in de gezondheidszorg is goed...

De komende jaren neemt het aanbod van onlinedienstverlening in de zorg verder toe. Doel daarvan is dat de patiënt meer toegang tot en regie over de eigen medische gegevens krijgt. De AP staat in beginsel positief tegenover deze technologische ontwikkelingen. Die kunnen namelijk bijdragen aan kwalitatief goede, veilige en doelmatige patiëntenzorg.

... mits de privacy van patiënten is gewaarborgd

Bij technologische ontwikkelingen in de zorg moet er wel rekening worden gehouden met de bescherming van persoonsgegevens van patiënten. Gegevens over gezondheid zijn per definitie privacygevoelig. Patiënten moeten erop kunnen vertrouwen dat de informatie die zij met hun arts delen geheim blijft. Daarom gelden voor de bescherming van gegevens over gezondheid extra hoge eisen.

Bijlage(n) -

AUTORITEIT
PERSOONSGEGEVENS

Datum
4 oktober 2018

Ons kenmerk
z2018-17577

Elektronische uitwisseling van gegevens over gezondheid tussen artsen en patiënten, zoals persoonlijke gezondheidsomgevingen en patiëntportalen, zijn pas mogelijk als gebruik wordt gemaakt van inlog- en identificatiemethoden met een passend betrouwbaarheidsniveau. De betrouwbaarheid van elektronische identificatiemiddelen wordt onder meer bepaald door de koppeling tussen persoonsidentificatiegegevens met de persoon, het uitgifteproces van een elektronisch identificatiemiddel, het beheer van het middel, de gebruikte techniek en de inrichting van het authenticatieproces.

2 Passende technische en organisatorische maatregelen

Wat zegt de AVG?

Op grond van artikel 32 AVG moeten verwerkingsverantwoordelijken en verwerkers passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Naarmate de persoonsgegevens een gevoeliger karakter hebben of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekent, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Gegevens over gezondheid zijn per definitie gevoelig, dus worden hoge eisen gesteld aan de beveiliging van die gegevens.

Wanneer is een beveiligingsmaatregel "passend"?

Er kunnen geen algemene uitspraken worden gedaan over wat een "passende" beveiligingsmaatregel is. Dat is afhankelijk van de concrete omstandigheden van het geval. Bij de uitleg van het begrip "passend" zoekt de AP aansluiting bij algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de *Code voor Informatiebeveiliging* of de *ICT-Beveiligingsrichtlijnen voor webapplicaties* van het Nationaal Cyber Security Centrum. Daarnaast zijn concrete normen voor informatiebeveiliging opgenomen in de ISO/NEN 27001 en 27002. Voor wat betreft de zorgsector (verwerking van gegevens over gezondheid) zijn deze normen uitgewerkt in NEN 7510:2017 en in aanvulling daarop NEN 7512:2015 en NEN 7513:2018. De AP ziet die normen als een beveiligingsstandaard die binnen de sector algemeen wordt geaccepteerd en die organisaties binnen de zorgsector moeten toepassen.

De eIDAS-verordening

De Europese eIDAS-verordening[1] gaat over de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt. Het leidt tot een wettelijk kader voor betrouwbaarheidsniveaus. Europese burgers en bedrijven moeten vanaf 29 september 2018 bij alle Nederlandse organisaties in de publieke sector kunnen inloggen met een door Europa erkend nationaal inlogmiddel. Om het betrouwbaarheidsniveau van online inloggen te verhogen, werkt de overheid aan een set van afspraken voor elektronische identificatie en authenticatie, het zogenaamde eID-stelsel.[2] De AP heeft dit belang met grote nadruk onderschreven.[3] Bij brief van 16 juli 2018 heeft de staatsecretaris van Binnenlandse Zaken en Ko-

[1] Verordening (EU) nr. 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.
[2] *Kamerstukken II* 2016-2017, 26 643, nr. 476.
[3] Brief van de AP aan de minister van BZK van 14 september 2016, met kenmerk z2015-00357.

AUTORITEIT
PERSOONSGEGEVENS

Datum
4 oktober 2018

Ons kenmerk
z2018-17577

ninkrijksrelaties de Tweede Kamer geïnformeerd over de voortgang van het programma eID en over de implementatie van de eIDAS-verordening.[4]

3 Toepasselijke norm voor patiëntidentificatie in de zorg

Bij haar toezichtstaken moet de AP uitgaan van de geldende wet- en regelgeving op het gebied van de bescherming van persoonsgegevens. In het verleden heeft de AP regelmatig aangegeven dat bij patiëntauthenticatie in het kader van de uitwisseling van gegevens over gezondheid in beginsel dient te worden uitgegaan van een "hoog betrouwbaarheidsniveau" en dat in gevallen waar het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust het "hoogste betrouwbaarheidsniveau" vereist is.[5] In de terminologie van de eIDAS-verordening wil dit zeggen dat bij patiëntauthenticatie minimaal niveau "substantieel" vereist is. Als het gaat om gegevens waarop het medisch beroepsgeheim van de hulpverlener rust, is betrouwbaarheidsniveau "hoog" vereist. Dit is in lijn met de conclusies van een onderzoek uit 2016, dat op verzoek van het ministerie van VWS is uitgevoerd door de advieskantoren PBLQ en Privacy-Care. De minister van VWS heeft deze conclusies destijds gedeeld met de Tweede Kamer.[6] In de brief schreef de minister dat de conclusies uit het rapport de leidraad zullen zijn bij de invulling van de eisen waaraan authenticatiemiddelen in de zorg moeten voldoen.

4 Wat te doen zolang de vereiste betrouwbaarheidsniveaus nog niet breed beschikbaar zijn?

Probleem: nog geen brede beschikbaarheid

De AP is zich ervan bewust dat patiëntauthenticatie op betrouwbaarheidsniveaus "substantieel" en "hoog" op dit moment (nog) niet breed beschikbaar is als gebruik wordt gemaakt van DigiD. De staatssecretaris van BZK heeft in de eerder genoemde brief aan de Tweede Kamer toegezegd om in het zogenoemde BSN-domein, waarin doorgaans gebruik wordt gemaakt van DigiD, inlogmethoden met betrouwbaarheidsniveau "substantieel" en "hoog" mogelijk te maken. Daarbij zal allereerst worden gezorgd voor brede beschikbaarheid van inlogmethoden op het niveau "substantieel". De staatssecretaris acht dat van belang omdat de middelen op niveau "hoog" in de komende jaren pas geleidelijk worden ingevoerd, via het natuurlijke vervangingspatroon van de rijbewijzen en de identiteitskaarten. Volgens de staatssecretaris is *"het betrouwbaarheidsniveau "substantieel", in combinatie met publieke en één of meerdere (nog te verwerven) private authenticatiediensten, wél gereed voor bredere implementatie"*.

Uitgangspunt van de AP

Tegen deze achtergrond is het uitgangspunt van de AP als volgt. Zolang een passend betrouwbaarheidsniveau voor patiëntauthenticatie niet kan worden gerealiseerd, mag elektronische uitwisseling van gegevens over gezondheid tussen zorgaanbieders en patiënten in beginsel niet plaatsvinden. De bescherming van persoonsgegevens, waaronder gegevens over gezondheid, is dan onvoldoende gewaarborgd. Zodra binnen het eID-programma inlogmethoden met de betrouwbaarheidsniveaus "substantieel" en "hoog" breed beschikbaar komen, dient een lager betrouwbaarheidsniveau bij de verwerking van gegevens over gezondheid dus niet meer beschikbaar te worden gesteld.

[4] *Kamerstukken II* 2017-2018, 26 643, nr. 550.
[5] Zie de brief van de AP aan de NVZ Nederlandse Vereniging van Ziekenhuizen van 7 oktober 2016.
[6] Brief van 4 november 2016, *Kamerstukken II* 2016-2017, 27 529, nr. 143.

AUTORITEIT
PERSOONSGEGEVENS

Datum
4 oktober 2018

Ons kenmerk
z2018-17577

Wat te doen in de tussentijd?

Brede beschikbaarheid van betrouwbaarheidsniveaus "substantieel" en "hoog" voor alle patiënten zal nog enige tijd in beslag nemen. Het zou niet goed zijn – en ook niet in het belang van de patiënt – als zorginnovaties stilstaan totdat die betrouwbaarheidsniveaus binnen het eID-programma breed beschikbaar zijn. Daarom is het in eerste instantie van belang dat de nodige voortvarendheid wordt betracht bij de ontwikkeling en het beschikbaar maken van de benodigde betrouwbaarheidsniveaus binnen het eID-stelsel. Dat past ook bij de hiervoor aangehaalde uitgangspunten van de staatssecretaris van BZK.

Verder moet de zorgsector bezien welke mogelijkheden – eventueel buiten DigiD om – momenteel wél beschikbaar zijn om te gebruiken voor patiëntauthenticatie. Zo zijn er binnen de gezondheidszorg enkele pilots uitgevoerd, zoals het Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional (VIPP) en het MedMij-programma.[7] Het is van belang dat op basis daarvan op zo kort mogelijke termijn wordt geëvalueerd of de nieuwe middelen op niveau "substantieel" en "hoog" werken zoals beoogd. Zo wordt duidelijk op welke wijze het nieuwe eID-stelsel bij patiënten en zorgaanbieders kan worden geïmplementeerd.

In afwachting van het breder beschikbaar komen van authenticatiemethoden met een passend hoog niveau, dient authenticatie plaats te vinden met tenminste tweefactorauthenticatie (zoals DigiD in combinatie met sms). Een lagere betrouwbaarheid is in ieder geval niet aanvaardbaar. Randvoorwaarde daarbij is dat er zo nodig aanvullende maatregelen worden getroffen om openstaande risico's, die niet worden weggenomen met tweefactorauthenticatie, te mitigeren.

Tot slot: naar een toekomstbestendige manier van patiëntauthenticatie

Tot slot vraagt de AP u te bevorderen dat binnen de zorgsector wordt geïnvesteerd in een toekomstbestendige wijze van patiëntidentificatie op een passend betrouwbaarheidsniveau. Een passend beveiligingsniveau is immers mede afhankelijk van de stand van de techniek. Die techniek staat niet stil. Dat betekent dat de wijze van patiëntidentificatie technisch flexibel moet zijn, zodat snel en eenvoudig nieuwe en/of aanvullende beveiligingsmaatregelen kunnen worden getroffen wanneer de stand van de techniek dat vereist.

Hoogachtend,
de Autoriteit persoonsgegevens,
w.g.

mr. A. Wolfsen
voorzitter

[7] Zie nader "Het nieuwe eID-stelsel; een introductie voor de zorgsector", Nictiz: mei 2017.

4/4

VOOR MEER INFORMATIE

NEN

Postbus 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft

Zorg & Welzijn
Telefoon 015 2 690 318
zw@nen.nl

nen.nl