PRIVACYCARE

JURIDISCH ADVIES EN BEGELEIDING

PBLQ

# Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg

Mei 2016

**Inhoudsopgave**

## Managementsamenvatting

**De onderzoeksvraag** van het ministerie van VWS is tweeledig en luidt:

1. Welk betrouwbaarheidsniveau is minimaal noodzakelijk voor patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg en kwalificeert als ‘passend’ in de zin van de Wet bescherming persoonsgegevens?
2. Is er een onderscheid tussen het elektronisch inzien van medische gegevens en het elektronisch muteren van medische gegevens door de patiënt?

Gevraagd is om in het onderzoek aan te sluiten op de weergave van het betrouwbaarheidsniveau bij de op dit moment gebruikelijke classificatie met in ieder geval een verwijzing naar STORK (1 tot en met 4) en de eIDAS-classificatie (laag, substantieel en hoog).

Als wij in het algemeen spreken over niveau substantieel of hoog dan verwijst dat naar de niveaus uit de eIDAS normering en naar STORK 3 en 4. Wat betreft STORK en eIDAS is een directe relatie niet te leggen, omdat de betrouwbaarheidsniveaus van STORK niet in eIDAS zijn overgenomen. Wel is er een parallel tussen de normen en de gedeelde terminologie. Ook STORK noemt de niveaus 3 en 4 respectievelijk 'substantieel' en 'hoog'. De STORK niveau's zijn concreter beschreven dan eIDAS als praktische implementatiestandaard. De eIDAS verordening schept een abstract kader voor Europese toepassing waarbij de betrouwbaarheidsniveau's technologieneutraal ingericht moeten kunnen worden. In de uitvoeringsverordening 2015/1502 heeft de Europese Commissie de minimale specificaties en procedures vastgesteld die vereist zijn bij de verschillende betrouwbaarheidsniveau's in eIDAS. De uitwerking van eIDAS zal in de komende tijd verder vorm moeten krijgen in eventuele nadere regels door de Europese Commissie en/of normering en standaardisering.

**Usecases VWS**

**A. Een patiënt controleert zijn inschrijvingsgegevens bij een zorgaanbieder (NAW gegevens die geen betrekking hebben op zijn gezondheid).**

We onderscheiden twee scenario’s vanwege de vraagstelling:
1) Inschrijfgegevens die - ook in combinatie met de gegevens van de zorgaanbieder - niets zeggen over de gezondheidssituatie van de patiënt en waarbij ook geen inzage is in het BSN.
2) Inschrijfgegevens inclusief het BSN en inzicht in het specialisme van de zorgaanbieder.
De gegevens vallen in alle gevallen wel onder het medisch beroepsgeheim van de zorgverlener.
Conclusie: In scenario 1 wordt minimaal betrouwbaarheidsniveau substantieel (en STORK 3) en in scenario 2 niveau hoog (en STORK 4) passend geacht.

**B. Een patiënt wijzigt zijn inschrijvingsgegevens bij een zorgaanbieder (NAW gegevens die geen betrekking hebben op zijn gezondheid).**

Ook in deze usecase bepaalt het verschil in de soort te wijzigen gegevens, zoals deze bij usecase A zijn onderscheiden in scenario 1 en 2, alsmede de koppeling daarvan aan het zorgdossier, het verlangde betrouwbaarheidsniveau. Wij verwachten daarvoor hetzelfde niveau als bij usecase A.
Conclusie: In scenario 1 wordt minimaal niveau substantieel (en STORK 3) en in scenario 2 niveau hoog (en STORK 4) passend geacht.

**C. Een patiënt maakt/wijzigt een afspraak met de zorgverlener (bijvoorbeeld voor het spreekuur of een onderzoek).**
In aansluiting op usecase A1 zou het enkele feit van een afspraak met een algemene zorgaanbieder, zoals een huisarts of tandarts geen gezondheidsgegevens hoeven te bevatten. De afspraakgegevens vallen wel onder het beroepsgeheim van de arts.
Conclusie: In een situatie vergelijkbaar met het scenario onder A.1 is niveau substantieel (en STORK 3) passend en in een situatie vergelijkbaar met scenario A.2 is betrouwbaarheidsniveau hoog (en STORK 4) passend, afhankelijk van de soort te wijzigen gegevens.

**D. Een patiënt raadpleegt zijn medisch dossier bij de hulpverlener (bijvoorbeeld zijn huisartsdossier, laboratoriumuitslagen, beeldverslagen of medicatie).**
In deze casus is het (gehele) medisch dossier zichtbaar en is er dus geen twijfel over de vraag of er sprake is van gezondheidsgegevens, inzage in het BSN en toepasselijkheid van het medisch beroepsgeheim.
Conclusie: betrouwbaarheidsniveau hoog (eIDAS), dan wel STORK 4 wordt passend geacht.

**E. Een patiënt maakt aanvullingen op zijn medisch dossier (bijvoorbeeld door het toevoegen van resultaten van zelfmetingen van parameters zoals bloedsuikerspiegel, bloeddruk, gewicht).**
Het muteren van het medisch dossier brengt meer risico's met zich mee dan alleen inzage.
Conclusie: Betrouwbaarheidsniveau hoog eIDAS / STORK 4 wordt passend geacht.

**F. Een patiënt vraagt een herhaalrecept aan**
De manier waarop de mogelijkheid wordt geboden maakt verschil in of de verwerking bij de zorgaanbieder begint of bij de patiënt. Het gaat om een het verwerken van een beperkte hoeveelheid gezondheidsgegevens.
Er is geen twijfel over de vraag of er sprake is van het verwerken van gezondheidsgegevens, verwerken/inzien van het BSN en toepasselijkheid van het medisch beroepsgeheim op de gegevens die verwerkt worden.
Conclusie: Betrouwbaarheidsniveau hoog eIDAS / STORK 4 wordt passend geacht.

**In algemene zin luiden de antwoorden op de bovenvermelde onderzoeksvraag** als volgt:

Ad 1.
Op grond van het regime voor het verwerken van gezondheidsgegevens in de Wbp en de aanstaande Algemene Verordening Gegevensbescherming, het medisch beroepsgeheim en de ISO- en NEN-normen met de patiëntauthenticatie-vereisten op grond van de Wet BSN in de zorg is naar verwachting in bepaalde gevallen eIDAS-betrouwbaarheidsniveau substantieel en in bepaalde gevallen niveau hoog (ofwel STORK 3 of 4) passend.

Ad 2.
Hoewel bij het elektronisch inzien van medische gegevens en het elektronisch muteren van medische gegevens door de patiënt in beide gevallen sprake is van verwerking van gezondheidsgegevens, het BSN en het verwerken van gegevens waarop het medisch beroepsgeheim van toepassing is, is het niettemin mogelijk dat het risico van de verwerking anders is bij inzien en muteren. Het is mogelijk om te stellen dat inzage veelal omgeven is

door minder risico's dan muteren bij dezelfde soorten gegevens. Dit leidt niet perse tot een verschil in vereist betrouwbaarheidsniveau.

**Algemene conclusie:**
Op grond van het normatieve kader en in de uitwerking van de usecases wordt in bepaalde gevallen niveau substantieel eIDAS (en STORK 3) en in bepaalde gevallen niveau hoog eIDAS (en STORK 4) passend geacht voor patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg zoals in de usecases beschreven. Het gaat om 'passend' in de zin van de Wet bescherming persoonsgegevens en de aankomende Algemene Verordening Gegevensbescherming. Uit uitspraken en richtsnoeren van de Autoriteit Persoonsgegevens volgt dat bij patiënt-authenticatie in communicatie met en onder verantwoordelijkheid van de zorgaanbieder in beginsel uitgegaan dient te worden van een 'hoog betrouwbaarheids niveau'. In bepaalde gevallen, namelijk als het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust, geeft de AP aan dat het 'hoogste' betrouwbaarheidsniveau verlangd wordt.

Het onderzoek is gericht op de casus die door VWS zijn voorgelegd. Toegang tot medische gegevens die niet onder verantwoordelijkheid van een arts of hulpverlener worden verwerkt (bijvoorbeeld in het zelf gestarte PGD van de patiënt waarbij het medisch beroepsgeheim niet aan de orde is) is niet meegenomen in het onderzoek.

Patiëntauthenticatie op betrouwbaarheidsniveau STORK niveau 4 is voor de patiënt op dit moment (nog) niet breed beschikbaar. Dat zal naar alle waarschijnlijkheid ook gezegd kunnen worden van niveau hoog eIDAS, aangezien dit het hoogste niveau van authenticatie betreft en gelet op de minimale eisen die daaraan worden gesteld in de uitvoeringsverordening (EU) 2015/1502.

Op dit moment worden er al pilots gedaan, onder andere in de zorg, waarbij waarschijnlijk niveau STORK 3/ substantieel wordt behaald. Daarbij worden in enkele pilots (iDIN) de mogelijkheden om het hoogste betrouwbaarheidsniveau te bereiken onderzocht. Ook zullen er een aantal pilots op niveau hoog gaan starten, waaronder in de zorg.

Het is aan te bevelen dat de overheid zo spoedig mogelijk het initiatief neemt om authenticatiemiddelen op niveau hoog breed beschikbaar te krijgen, publiek en/of privaat.

# H.1 Het onderzoek

### § 1.1 Inleiding

Het ministerie van VWS heeft PrivacyCare gevraagd onderzoek te doen naar het vereiste betrouwbaarheidsniveau van patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg. De vraag welk betrouwbaarheidsniveau ten minste nodig is speelt een belangrijke rol bij het goed inrichten van elektronische toepassingen in de zorg. Door de hoge toevlucht van de ontwikkelingen op dat vlak is de vraag zeer actueel. Er bestaan veel verschillende visies over wat noodzakelijk is in verband met de goede beveiliging van gegevensverwerking. Van belang is op te merken dat een goede beveiliging een veel breder veld aan vraagstukken en eisen inhoudt dan enkel het betrouwbaarheidsniveau voor online toegang.
Het ministerie heeft in de onderzoeksvraagstelling een specifiek aantal casus beschreven waarvoor zij deze vraag graag onderzocht wil hebben.

### §1.2 Vraagstelling onderzoek

De onderzoeksvraag is tweeledig en luidt:
Welk betrouwbaarheidsniveau is minimaal noodzakelijk voor patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg en kwalificeert als ‘passend’ in de zin van de Wet bescherming persoonsgegevens (Wbp)?

Het ministerie wil daarbij weten of er een onderscheid is tussen het elektronisch inzien van medische gegevens en het elektronisch muteren van medische gegevens door de patiënt.
In het onderzoek dient voor de weergave van het betrouwbaarheidsniveau te worden aangesloten bij de op dit moment gebruikelijke classificatie, waarbij het ministerie vraagt in ieder geval te verwijzen naar STORK (1 tot en met 4) en de eIDAS-classificatie (laag, substantieel en hoog).

Mogelijke casus (use cases) waar VWS vanuit gaat zijn:
**A.** Een patiënt controleert zijn inschrijvingsgegevens bij een zorgaanbieder (NAW gegevens die geen betrekking hebben op zijn gezondheid).
**B.** Een patiënt wijzigt zijn inschrijvingsgegevens bij een zorgaanbieder (NAW gegevens die geen betrekking hebben op zijn gezondheid).
**C.** Een patiënt maakt/wijzigt een afspraak met de zorgverlener (bijvoorbeeld voor het spreekuur of een onderzoek).
**D.** Een patiënt raadpleegt zijn medisch dossier (bijvoorbeeld zijn huisartsdossier, laboratoriumuitslagen, beeldverslagen of medicatie).
**E.** Een patiënt maakt aanvullingen op zijn medisch dossier (bijvoorbeeld door het toevoegen van resultaten van zelfmetingen van parameters zoals bloedsuikerspiegel, bloeddruk, gewicht).
**F.** Een patiënt vraagt een herhaalrecept aan.

### §1.3 Uitvoering

Het onderzoek is uitgevoerd binnen de in het verzoek gestelde kaders, met uitbreiding van voor beantwoording van de vragen volgens de onderzoekers tenminste relevante aspecten. Zijdelings relevante aspecten, kaders en normen zijn niet in het onderzoek betrokken in verband met de beperkte scope.

Het onderzoek is uitgevoerd in samenwerking tussen PrivacyCare en PBLQ, door mr. Jacqueline Krabben en mr. drs. Theo Hooghiemstra.

## H.2 Kader voor het onderzoek

### §2.1 Inleiding

Elektronische identificatie is een proces waarbij persoonsidentificatiegegevens in elektronische vorm worden gebruikt. Met die gegevens wordt een persoon uniek aangeduid. (artikel 3, onderdeel 1, van de eIDAS verordening, nr. 910/2014[1]).
Bij elektronische identificatie kan gebruik worden gemaakt van elektronische identificatiemiddelen (artikel 3, onderdeel 2, van de verordening).

Het gebruik van persoonsidentificatiegegevens kan met kennis die geheim blijft voor anderen, bijvoorbeeld een zelfgekozen wachtwoord of pincode. Het kan ook met een middel in combinatie met (wisselende) gegevens, bijvoorbeeld voortkomend uit een nummercalculator, token of mobiele telefoon. Tenslotte kan het gebruik van de persoonsidentificatiegegevens fysiek gebonden zijn, aan biometrische kenmerken, zoals een vingerafdruk, stemherkenning of irisscan. Een combinatie van methoden leidt tot meer veiligheid en minder kans op identiteitsfraude. Dit wordt meer-factorauthenticatie genoemd. De kans dat een derde over meerdere geheime en persoonsgebonden factoren beschikt is kleiner dan bij gebruik van een enkelvoudige methode. Voorwaarde daarvoor is het zorgvuldig gebruik en bewaren van geheime gegevens en bijbehorende middelen.

De functie van het gebruik van elektronische identificatiemiddelen is dat een persoon elektronisch duidelijk kan maken aan een ander wie hij is en dat hij het echt is. Het is gericht op het creëren van gewaarborgd vertrouwen bij een ander. Dit gebeurt doordat het gebruik van een elektronisch identificatiemiddel via een elektronisch proces leidt tot een bevestiging van de echtheid van een aan een ander opgegeven of kenbaar gemaakte identiteit. Die elektronische bevestiging van echtheid die de vertrouwende partij ontvangt, is in veel situaties afkomstig van een derde partij die de identiteit op echtheid heeft gecontroleerd en vastgelegd. Het proces dat bevestiging mogelijk maakt, heeft een specifieke naam: authenticatie (artikel 3, onderdeel 5, van de verordening).
De betrouwbaarheid van elektronische identificatiemiddelen kan verschillend zijn. Dit hangt af van de betrouwbaarheid van de keten die op het elektronisch identificatiemiddel is gericht. Bij deze keten kunnen meerdere partijen betrokken zijn. De betrouwbaarheid van het middel wordt bepaald door onder meer 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.

In dit onderzoek gaat het om patientauthenticatie bij elektronische gegevensverwerking. Hoe veiliger het authenticatiemechanisme is, hoe hoger het betrouwbaarheidsniveau van de authenticatie. Betrouwbaarheidsniveaus hebben betrekking op authenticatiemiddelen. De risico's die een bepaalde online dienst met zich meebrengt bepalen op welk niveau

[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 en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257)

maatregelen genomen moeten worden. De middelen waarmee gebruikers zich bij de dienst bekend maken, zijn een belangrijk aspect daarvan. Bij een breed gebruik van een authenticatiemiddel, neemt het het belang van betrouwbaarheidsniveaus toe, om te bepalen welke groepen van middelen geschikt zijn voor welke diensten.[2] Daarvoor wordt onder andere de ISO 29115 en de in het Europese STORK programma opgestelde criteria gehanteerd. Dit onderzoek gaat echter niet om de vraag welke eisen of middelen bij welk betrouwbaarheidsniveau passen. In dit onderzoek gaat het erom zoveel mogelijk helder te maken welk betrouwbaarheidsniveau in aangegeven toepassingen noodzakelijk is voor patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg en kwalificeert als 'passend' in de zin van de Wet bescherming persoonsgegevens (Wbp).

Aangezien een passende beveiliging steeds een (wettelijke) verantwoordelijkheid van de verantwoordelijke voor gegevensverwerking is, zal deze steeds na risicoanalyse een beslissing moeten nemen over onder andere de betrouwbaarheid van de authenticatie. Het onderzoek dient niet ter vervanging daarvan, maar heeft een beschouwend, adviserend en richtinggevend karakter.

## §2.2 Wet en normen

Bij gegevensverwerking van persoonsgegevens is het van belang deze steeds met betrekking tot de juiste persoon te verwerken. Hoe meer consequenties er aan de gegevensverwerking verbonden (kunnen) zijn hoe belangrijker dat wordt. Bij het verwerken van gevoelige informatie over iemand speelt dat een rol. En als er een geheimhoudingsplicht op de gegevens rust, is dat een extra reden om te willen voorkomen dat onbevoegden kennis kunnen nemen van de gegevens. Degene op wie de geheimhouding rust, wil dan met grote zekerheid weten wie hij toestaat gegevens te verwerken. En de wet verlangt dit ook.

Er zijn verschillende betrouwbaarheidsniveaus te onderscheiden bij authenticatie.
Om een gestructureerde aanpak mogelijk te maken zijn deze niveaus op verschillende plekken uitgewerkt in normen. Dat gebeurt in wettelijke en niet wettelijke normen. Omdat ook de niet wettelijke normen tot standaard zijn geworden, zijn ze relevant voor het onderzoek. In dit hoofdstuk wordt het (toetsings)kader uiteen gezet en de relevantie van de onderdelen besproken.

Als wij in het algemeen spreken over niveau substantieel of hoog dan verwijst dat naar de niveaus uit de eIDAS normering en naar STORK 3 en 4. Wat betreft STORK en eIDAS is een directe relatie niet te leggen, omdat de betrouwbaarheidsniveaus van STORK niet in eIDAS zijn overgenomen. Ook STORK noemt de beide niveaus 3 en 4 respectievelijk 'substantieel' en 'hoog', toch is een één op één vergelijking niet mogelijk. De STORK niveau's zijn concreter beschreven dan eIDAS als praktische implementatiestandaard. De eIDAS verordening schept een abstract kader voor Europese toepassing waarbij de betrouwbaarheidsniveau's technologieneutraal ingericht moeten kunnen worden. In de uitvoeringsverordening 2015/1502 heeft de Europese Commissie de minimale specificaties en procedures vastgesteld die vereist zijn bij de verschillende betrouwbaarheidsniveau's in eIDAS. De

[2] M. Stoelinga, eIDAS Verordening, Een Europees Kader voor betrouwbaarheidsniveaus van online diensten, InformatieBeveligings Magazine, maart 2016, p. 15-19.

uitwerking van eIDAS zal in de komende tijd verder vorm moeten krijgen in eventuele nadere regels door de Europese Commissie en/of normering en standaardisering.
In ETD / eID -verband (zie volgende paragraaf) wordt gewerkt aan een nadere concretisering van de eIDAS norm, zodat eraan getoetst kan worden.

Na een weergave van de context van ETD/eID worden in de navolgende paragrafen verschillende toepasselijke normen uiteengezet voordat STORK en eIDAS inhoudelijk aan bod komen.

### §2.3 Context eID / ETD

eID staat voor elektronische Identiteiten. De Tweede Kamer heeft eind 2015 gevraagd om de verantwoordelijkheid voor de toegang met eID middelen tot het BSN domein bij de minister van BZK te beleggen. De minister ontwikkelt toelatingseisen en een certificeringsprocedure. Wanneer partijen aan de eisen voldoen, zullen ze tot het BSN domein worden toegelaten. Deze eisen zullen worden vastgelegd in of bij de Wet Generieke Digitale Infrastructuur.

ETD staat voor Elektronische Toegangsdiensten. eID en ETD worden op dit moment en in dit advies door elkaar heen gebruikt. Het eID/ ETD-stelsel bestaat uit Idensys (voor burgers) en eHerkenning (voor bedrijven). Op dit moment geldt voor het ETD-stelsel een publiek-private governance. Als gevolg van de politieke besluitvorming eind 2015 zal dit veranderen voor wat betreft de toelating van eID-middelen tot het publieke domein.

Idensys is ontwikkeld als standaard voor online identificatie en uitwisseling van persoonlijke informatie. Idensys bouwt voort op de infrastructuur van eHerkenning. Die toepassing wordt door koppeling met het BSN-koppelregister, ook beschikbaar gemaakt voor burgers en patiënten. Op dit moment worden pilots uitgevoerd door Idensys, door een aantal banken (onder de naam iDIN) en door BZK. De pilots zijn beschreven in hoofdstuk 3.

De discussie over elektronische identiteiten voor burgers en bedrijven is in Nederland erg actueel. DigiD is beschikbaar op een niveau laag eIDAS en STORK 2( gebruikersnaam en wachtwoord) en op STORK 2+ (gebruikersnaam en wachtwoord met SMS authenticatie). eIDAS betrouwbaarheidsniveau's substantieel en hoog (dan wel STORK 3 en 4) worden nu nog niet geboden. De behoefte aan een betrouwbaarder gebruiksvriendelijk middel is sterk aanwezig.
Het kabinet heeft gekozen voor een afsprakenstelsel waarbinnen ruimte is voor zowel publieke als private authenticatiemiddelen, zodat er meerdere middelen op alle betrouwbaarheidsniveaus beschikbaar kunnen komen voor burgers en bedrijven.

Dit onderzoek gaat niet dieper in op het ETD / eID stelsel, behalve waar dat voor de context van het gestelde en onderbouwing van belang is.

### §2.4 Verwerken van persoonsgegevens: de Wbp en de Algemene Verordening Gegevensbescherming

Bescherming van persoonsgegevens is onderdeel van het recht op privéleven (artikel 8 EVRM) en is verder als grondrecht erkend in artikel 16 VWEU en in artikel 10 Grondwet.

Authenticatie speelt een rol bij het verwerken van persoonsgegevens. De wet vereist dat het verwerken van persoonsgegevens goed beveiligd plaatsvindt. Authenticatie op het juiste betrouwbaarheidsniveau is daarmee een eis van passende beveiliging. Deze eis is vastgelegd in artikel 13 Wbp. Deze wet stelt de algemene eisen aan het verwerken van persoonsgegevens.

Op 15 december 2015 hebben de lidstaten van de EU overeenstemming bereikt over de voorlopige tekst van de Algemene Verordening Gegevensbescherming (AVG).[3] De verwachting is dat de AVG in het voorjaar van 2016 onder Nederlands voorzitterschap definitief wordt vastgesteld en in juli van kracht wordt. Deze zal dan 2 jaar later ( juli 2018) daadwerkelijk in werking treden in verband met overgangsrecht. Het is dan de belangrijkste wetgeving op het gebied van de bescherming van persoonsgegevens in de EU. De verordening vervangt de Wbp. De komende twee jaar dient hierop te worden voorbereid.

Het voorstel voor de AVG omvat aangescherpte regels voor bescherming van (bijzondere) persoonsgegevens en hoge boetes voor niet naleving daarvan. Een verschil met de huidige Nederlandse privacywetgeving uit de Wbp is dat de verplichtingen in de AVG op veel punten gedetailleerder zijn uitgewerkt. Daarbij komt ook aan de orde op welke wijze aan de norm moet zijn voldaan. Er wordt een accent gelegd op accountability. Dat betekent dat organisaties die persoonsgegevens verwerken, verplicht worden hun verwerkingsprocessen te beschrijven en zodanig in te richten dat ze in staat zijn aan te tonen dat ze voldoen aan de wet.

Naast het algemene vereiste dat iedere organisatie moet zorgdragen voor een adequate beveiliging verplicht de AVG organisaties om “privacy impact assessments” te verrichten, om “privacy by design” toe te passen en dit alles vast te leggen. Daarnaast zullen organisaties veel meer aandacht moeten gaan besteden aan de wijze van informeren van betrokkenen over de verwerking van hun persoonsgegevens. Ook om te voldoen aan het inzage- en correctierecht zal een organisatie processen moeten inrichten.

In de AVG staat een verplichting aan de lidstaten tot het vaststellen van nadere regels binnen de grenzen van de verordening bij de verwerking van gegevens betreffende de gezondheid.

In het navolgende hanteren we de Wbp, als geldend recht.

### §2.5 De Wbp

Voor het goede begrip van dit rapport zullen we de kern van de Wbp en de begrippen toelichten. De Wbp is van toepassing voor zover het gaat om het verwerken van persoonsgegevens. Een persoonsgegeven is ‘elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’. Daarbij gaat het ook om gegevens die in hun onderlinge samenhang of op zich, indirect tot een persoon te herleiden zijn. Het 'verwerken' omvat elke handeling met betrekking tot de persoonsgegevens, zoals het inzien, opslaan en

[3] Voorstel, algemene verordening gegevensbescherming, politiek akkoord, Brussel 28 januari 2016, 5455/16, Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

delen van de gegevens. Degene wiens persoonsgegevens worden verwerkt is de 'betrokkene' in de zin van de Wbp.

*Verantwoordelijke en bewerker*
De normen van de Wbp richten zich grotendeels tot de 'verantwoordelijke' voor de gegevensverwerking. Dit is volgens de Wbp 'degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt'. De partij die de gegevens van betrokkenen voor door hem vastgestelde doelstellingen vastlegt en bepaalt hoe de verwerking plaatsvindt, is verantwoordelijke voor die gegevensverwerking. Dat kunnen ook meerdere partijen samen zijn. Wanneer een partij de gegevens vastlegt in opdracht en voor doelstellingen van een ander treedt zij op als 'bewerker' van de gegevens in de zin van de Wbp. Dit is bijvoorbeeld aan de orde bij hosting van een database door een derde dienstverlener, die niet zelf medeverantwoordelijke is.

Niet alleen is de verantwoordelijke degene die de verplichtingen uit de Wbp moet opvolgen, ook is hij het aanspreekpunt voor betrokkenen met betrekking tot de gegevensverwerking en het uitoefenen van zijn rechten. Hij is ook degene die zorgt voor een passende beveiliging en aldus verantwoordelijk is voor een passende authenticatie bij elektronische gegevensverwerking.

*Grondslag*
De Wbp vereist een grondslag voor de gegevensverwerking op grond van artikel 8 Wbp. Daarin wordt aangegeven voor welke doeleinden persoonsgegevens verwerkt mogen worden. De verantwoordelijke dient de doeleinden vast te stellen.

Als daarbij ook 'bijzondere' gegevens worden verwerkt zoals bedoeld in artikel 16 Wbp, is een grondslag uit artikel 8 Wbp alleen niet voldoende. Dan is daarnaast een ontheffing nodig zoals opgenomen in de artikelen 17 t/m 23 Wbp. Het gaat bijvoorbeeld om strafrechtelijke gegevens of gezondheidsgegevens. Als deze gegevens in combinatie met 'gewone' gegevens worden verwerkt dan is altijd een ontheffing benodigd voor die verwerking. Bij patientauthenticatie zal het verwerken van bijzondere gegevens bijna altijd aan de orde zijn. Een grondslag voor het verwerken van patientgegevens kan bijvoorbeeld zijn een wettelijke verplichting, de goede uitvoering van de behandelingsovereenkomst of toestemming van een patient.

*Gezondheidsgegevens*
Onder gezondheidsgegevens worden blijkens de Memorie van Toelichting bij de Wbp alle gegevens bedoeld die de geestelijke of lichamelijke gezondheid van een persoon betreffen.[4] Een afspraak in de agenda bij de longarts wordt ook als een gezondheidsgegeven beschouwd.

De Wbp geeft een ontheffing voor het verwerken van 'gegevens betreffende de gezondheid' aan hulpverleners en instellingen wanneer dat noodzakelijk is voor de goede zorgverlening aan de betrokkene (artikel 21 lid 1 onder a Wbp). Ook kan de ontheffing voortvloeien uit de uitdrukkelijke toestemming van de betrokkene (artikel 23 Wbp). Uitdrukkelijke toestemming dient aan bepaalde voorwaarden te voldoen om een geldige ontheffing en grondslag te bieden.

[4] Tweede Kamer 1997-1998, 25892, nr. 3, p. 108-109.

Gegevens betreffende de gezondheid mogen alleen worden verwerkt door personen op wie een geheimhoudingsplicht rust, dan wel aan wie deze contractueel is opgelegd. Ook de verantwoordelijke zelf is op grond van wet gehouden tot geheimhouding, behoudens het geval de wet hem tot mededeling van bepaalde gegevens verplicht.

Ook andere bijzondere gegevens kunnen worden verwerkt door hulpverleners en instellingen als dat in aanvulling op de gezondheidsgegevens noodzakelijk is voor de goede behandeling of verzorging van betrokkenen. (artikel 21 lid 3 Wbp)

*Verder verwerken van gegevens*
De Wbp regelt in artikel 9 dat verzamelde gegevens niet verder mogen worden verwerkt voor andere doeleinden die niet verenigbaar zijn met het doeleinde van verkrijging. Daarboven geldt op grond van artikel 9 lid 4 Wbp dat een verwerking achterwege moet blijven wanneer een geheimhoudingsplicht aan het (verder) verwerken in de weg staat. Dat kan aan de orde zijn bij vertrouwelijke gegevens die onder toepassing van een geheimhoudingsplicht worden verwerkt. Deze bepaling correspondeert met het medisch beroepsgeheim van zorgverleners zoals uit de WGBO (7:457 BW) volgt. Een vergelijkbare bepaling is opgenomen in de Jeugdwet. In dit onderzoek wordt dat onderscheid verder niet gemaakt. Verder geldt voor BIG-geregistreerde professionals artikel 88 van de Wet BIG. Op grond van dit artikel is eenieder die zorg verleent op het gebied van de individuele gezondheidszorg verplicht tot geheimhouding van datgene wat hem in de uitvoering van het beroep is toevertrouwd. Het maken van een afspraak valt daarmee ook onder de geheimhoudingsplicht.

*Persoonsnummers*
Artikel 24 Wbp beperkt het gebruik van wettelijke persoonsnummers. Het artikel stelt dat een nummer ter identificatie van een persoon dat bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts wordt gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald.

Dit is onder andere van toepassing op het verwerken van het burgerservicenummer (BSN) van personen. De regels zijn vastgelegd in Wet algemene bepalingen BSN (Wabb) en de Wet gebruik burgerservicenummer in de zorg (Wbsn-z). Het gebruik van het BSN is, conform artikel 4 van de Wbsn-z, verplicht in elektronische uitwisseling van patientgegevens om correcte identificatie van patienten te waarborgen. Van belang is ook de nieuwe Wet gebruik BSN in de jeugdzorg (Wbsn-jz). Deze regelt het verplichte gebruik van het BSN door jeugdhulpaanbieders en gecertificeerde instellingen. In dit onderzoek is jeugdhulp niet betrokken in de vraagstelling.

Behalve bij het eerste contact met de cliënt, dient op grond van artikel 6 en volgende Wbsn-z de zorgaanbieder de identiteit en het burgerservicenummer ook vast te stellen wanneer dat redelijkerwijs nodig is om zich ervan te kunnen vergewissen dat het burgerservicenummer betrekking heeft op de persoon wiens gegevens verwerkt worden.

Bij inzage in het medisch dossier of bij inzage in de inschrijfgegevens, krijgt de patient ook inzage in het BSN, zodat steeds het BSN verwerkt wordt in relatie tot gegevensverwerking ten behoeve van de patient. Dit is van belang omdat de wet eisen stelt aan de beveiliging en betrouwbaarheid van het verwerken van het BSN. Hoewel de memorie van toelichting bij de

Wbsn-z niet ingaat op de toegang van patienten tot de eigen persoonsgegevens staat hierin wel dat identificatie essentieel is voor de zorgverlening zelf en dat bij de verwerking van medische persoonsgegevens boven elke twijfel verheven moet zijn op welke persoon de in dat kader te verwerken persoonsgegevens betrekking hebben.[5]

Ten behoeve van de verwerking van persoonsgegevens in de zorg, waarbij het burgerservicenummer wordt gebruikt, heeft het Nederlands Normalisatie Instituut een standaard ontwikkeld: de NEN 7510.

In artikel 2 Regeling gebruik burgerservicenummer in de zorg[6] is bepaald dat de NEN 7510 en de uitwerkingen daarvan in de NEN 7511 en de NEN 7512 tot het geldende recht behoren. Op grond van dit artikel moet de verwerking van het BSN door zorgaanbieders voldoen aan deze NEN normen.

Zie over de NEN-normen verder §2.7.

*Beveiligingseisen*
Op grond van artikel 13 Wbp dient de verantwoordelijke passende technische en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. 'Passend' betekent in dit verband dat de beveiliging in overeenstemming is met het risico van de gegevensverwerking (in verband met onder andere de aard van de gegevens en het gebruik) de stand van de techniek en de kosten van de tenuitvoerlegging. Het begrip 'passend' duidt op proportionaliteit tussen de beveiligingsmaatregelen en de te beschermen gegevens. Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze wordt gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekent, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er is geen verplichting om steeds de allerzwaarste beveiliging te nemen. Daarom duidt ook het feit dat inbreuken zijn gemaakt op het beveiligingsniveau niet noodzakelijkerwijs op nalatigheid in de beveiliging. Er moet sprake zijn van een adequate beveiliging.[7]

Er kunnen geen algemene uitspraken worden gedaan over wat als een 'passende beveiligingsmaatregel' kan worden beschouwd. Dit criterium moet in het licht van de concrete omstandigheden worden ingevuld en is voor een deel dynamisch. Het vereiste niveau van bescherming is hoger naarmate er meer maatregelen voorhanden zijn om dat niveau te waarborgen. "In het algemeen kan worden gesteld dat indien met naar verhouding geringe extra kosten meer beveiliging kan worden bewerkstelligd deze als 'passend' moeten worden beschouwd, terwijl kosten die disproportioneel zijn aan de extra beveiliging die daardoor zou worden verkregen, niet worden vereist. Met zich ontwikkelende techniek zal periodiek een nieuwe afweging moeten worden gemaakt", stelt de wetgever vast.[8]

Technische en organisatorische maatregelen dienen cumulatief te worden getroffen. Software is een belangrijk instrument tot beveiliging.

De Autoriteit Persoonsgegevens(AP), voorheen CBP, toezichthouder op de Wbp, heeft in de

[5] Tweede Kamer. Vergaderjaar 2005-2006, 30 380, nr. 3.
[6] Ministeriele regeling van de minister van VWS van 26 mei 2008, nr. MEVA/ICT-2838255
[7] Tweede Kamer, Vergaderjaar 1997-1998, 25 892, nr. 3, p.99
[8] Tweede Kamer, Vergaderjaar 1999-2000, 25 892, nr 92c, p.15

Richtsnoeren Beveiliging van persoonsgegevens de eisen omtrent beveiliging nader uitgewerkt.[9]

De beveiligingsverplichting richt zich in de eerste plaats tot de verantwoordelijke. De verantwoordelijke moet in kaart brengen welk risico gemoeid is met de gegevensverwerkingen. Uit de Richtsnoeren Beveiliging van persoonsgegevens volgt dat het inrichten van een Plan Do Check Act (PDCA) cyclus in de organisatie daarvoor nodig is. Het verwerken van gezondheidsgegevens brengt bijzondere risico's met zich mee, mede in verband met de vertrouwelijkheid van de gegevens. De open norm van artikel 13 Wbp kan op passende wijze worden ingevuld, door te voldoen aan de bestaande (Nederlandse en internationale) normen voor informatiebeveiliging. Er zal daarnaast moeten worden afgewogen welke aanvullende maatregelen eventueel nodig zijn in verband met de bijzonderheden en risico's van de verwerking.

De methode of het middel van toegang waarmee de gebruiker - in dit onderzoek de patiënt- toegang krijgt vormt de authenticatie. Evenals identificatie van belang voor de beveiliging.

Onderdeel van beveiliging is ook het regelen van de (omvang van de) toegang tot gegevens (autorisaties) voor gerechtvaardigde gebruikers. Er dient een autorisatieprotocol te worden vastgesteld afhankelijk van de noodzaak bepaalde gegevens te verwerken, in overeenstemming met de grondslag voor de verwerking.

*Rechten van betrokkenen*
Een betrokkene heeft het recht inzage en een overzicht te verkrijgen van de verwerking van zijn persoonsgegevens van de verantwoordelijke. Ook heeft hij het recht op correctie, aanvulling, afscherming of verwijdering van gegevens wanneer deze feitelijk onjuist zijn of zonder rechtsgrond verwerkt worden. De bijzondere wetgeving geeft aanvullende rechten aan betrokkenen en patiënten. Zo heeft de betrokkene in beginsel recht op vernietiging van het dossier dat op grond van de WGBO door de zorg- of hulpverlener is vastgelegd. Dit geldt ook voor de jeugdige, wanneer de hulpverlening onder de Jeugdwet valt. Dit onderscheid wordt in het onderzoek verder niet gemaakt. Uitgegaan wordt van de patiënt zoals bedoeld in de WGBO.

## §2.6 Wet op de geneeskundige behandelingsovereenkomst en wetsvoorstel Cliëntenrechten elektronische verwerking persoonsgegevens

De WGBO is van toepassing op het verwerken van gegevens door de zorgverlener die hij in het kader van de behandeling van de patiënt heeft verkregen. Die wet verplicht hem de noodzakelijke gegevens vast te leggen in zijn dossier over de patiënt. Wanneer de zorgverlener gegevens over de patiënt wil delen heeft hij te maken met het beroepsgeheim dat in de WGBO verankerd is.[10] Aan anderen dan de patiënt verstrekt de zorgverlener alleen gegevens omtrent de patiënt met zijn toestemming. Die toestemming is niet nodig als het gaat om rechtstreeks bij de behandelingsovereenkomst betrokkenen en de betreffende informatie noodzakelijk is voor de behandeling. De patiënt heeft recht op inzage in de vastgelegde gegevens.

[9]Richtsnoeren, Beveiliging van persoonsgegevens, College Bescherming Persoonsgegevens, februari 2013
[10] Het medisch beroepsgeheim vloeit voor zorgverleners ook voort uit artikel 88 Wet BIG. In de WGBO is het beroepsgeheim in verband met de behandelingsovereenkomst nader uitgewerkt.

Bij het gebruik van patiëntenportalen en ehealthtoepassingen speelt de vraag of de WGBO steeds van toepassing is. Nagegaan moet worden voor welke functies het portaal of de toepassing gebruikt wordt. In alle gevallen dat het portaal gebruikt wordt voor communicatie tussen patiënt en zorgverlener of patiënt en zorgaanbieder in het kader van de behandeling van de patiënt is de WGBO van toepassing. De relevante gegevens worden opgeslagen in het dossier van de zorgaanbieder. Sommige gegevens zijn bedoeld voor de patiëntenadministratie. Al deze gegevens van de patiënt vallen onder de WGBO en de geheimhoudingsplicht van de zorgverlener en de zorgaanbieder[11]. Niet alleen de gegevens die daadwerkelijk in het dossier worden vastgelegd vallen onder de geheimhoudingsplicht. Deze plicht geldt ook voor informatie over de patiënt die ter kennis van de zorgverlener is gekomen bij de behandeling, welke niet in het dossier wordt opgenomen.[12]

Voor het bepalen van (het niveau van) patiëntauthenticatie is het van belang of er sprake is van persoonsgegevens waarop de medische geheimhoudingsplicht van toepassing is.

*Wetsvoorstel Cliëntenrechten bij elektronische verwerking van gegevens*
In haar brief bij de behandeling van het wetsvoorstel 'Cliëntenrechten elektronische verwerking persoonsgegevens' in de Eerste Kamer van 22 december 2015 schreef de minister dat zorgaanbieders op dit moment nog geen adequate invulling kunnen geven aan het recht op elektronische inzage en elektronisch afschrift. Belangrijk is volgens haar dat de burger beschikt over veilige authenticatiemiddelen op voldoende hoog betrouwbaarheidsniveau waarmee hij zijn gegevens in kan zien en opslaan. Daarom laat zij de bepalingen ten aanzien van elektronische inzage en elektronisch afschrift niet eerder in werking treden dan drie jaar na inwerkingtreding van het wetsvoorstel. Zij gaat ervan uit dat op dat moment een authenticatiemiddel op hoog niveau beschikbaar is voor veilige elektronische inzage en afschrift. Het wetsvoorstel zal mogelijk dit jaar aangenomen worden, maar ligt nog bij de Eerste Kamer ter beoordeling.[13]

## §2.7 Afdeling 2.3 Awb

Het elektronisch verkeer tussen bestuursorgaan en burger wordt in algemene zin gereguleerd door Afdeling 2.3 van de Awb ("Wet elektronisch bestuurlijk verkeer"). Artikel 2:13 Awb bepaalt dat in het verkeer tussen burgers en bestuursorganen een bericht elektronisch kan worden verzonden, mits de bepalingen van afdeling 2.3 Awb in acht worden genomen. "Verzending" is hier bedoeld in de "ruimste zin van het woord": hieronder wordt "iedere vorm van elektronische gegevensuitwisseling met een ander" verstaan. Ook het plaatsen van een stuk op een website wordt hieronder bijvoorbeeld begrepen.

[11] Beiden 'hulpverlener' in de zin van de WGBO.
[12] Artikel 88 Wet BIG is ook van toepassing.
[13] Het wetsvoorstel "Wijziging van de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens)", dat de mogelijkheid van elektronische inzage van de patiënt in de toekomst verplicht stelt (EK 33.509, A) is op 1 juli 2014 aangenomen door de Tweede Kamer. De Eerste Kamercommissie voor VWS heeft op 22 december 2015 de nadere memorie van antwoord (EK 33.509, J) ontvangen. De commissie heeft op 5 april 2016 een gesprek met een aantal deskundigen (tweede consultatie).

Gezien deze ruime uitleg van "verzending" wordt aangenomen dat Afdeling 2.3 Awb van toepassing is op bijvoorbeeld DigiD. Het belang van de Awb is in dit onderzoek gering, nu het in beginsel niet om overheidscommunicatie gaat.

## §2.8 NEN en ISO normen voor informatiebeveiliging

ISO/NEN 27001 en 27002, samen de Code voor informatiebeveiliging, is de algemene norm voor de invulling van informatiebeveiliging. Voor gegevensbeveiliging in de zorg en patiëntenauthenticatie zijn de NEN 7510 en NEN 7512 aanvullend van belang. Daarnaast is er in ontwerp de NEN 7521 over toegang tot patiëntgegevens. Dit ontwerp moet nog worden geïmplementeerd en zal mogelijk als Nederlands Technische Afspraak (NTA) worden vastgesteld.

*NEN 7510 en NEN 7512*
De NEN normen voor informatiebeveiliging in de zorg zijn ook richtinggevend voor de uitwerking van het identiteits management.[14] Deze NEN-normen zijn opgenomen in de 'Regeling gebruik burgerservicenummer in de zorg' als invulling van het vereiste van 'passende technische en organisatorische beveiligingsmaatregelen in de zin van artikel 13 Wbp, en (op grond van de wet) van toepassing op gegevensverwerking waarbij het BSN wordt verwerkt.[15] De keuze van authenticatiemiddelen moet passend zijn gelet op de risico's, de stand der techniek en de kosten.

De NEN 7510:2011 is de norm voor het organiseren en borgen van informatiebeveiliging in de zorg[16]. De norm richt zich op alle kleine en grote organisaties die hiermee te maken hebben. NEN 7510 is een algemene norm. Wat betreft patiëntauthenticatie werken de NEN 7512, NEN 7513 en NEN/NTA-ontwerp 7521 deze norm verder uit. De NEN 7510 geeft aanwijzingen over het organisatorisch en technisch inrichten van informatiebeveiliging in een zorginstelling. Het managementsysteem voor informatiebeveiliging en de risicoanalyse van informatiebeveiliging hebben een centrale plaats in de norm.

De Inspectie voor de Gezondheidszorg (IGZ) en in het verleden het CBP hebben aangegeven de NEN normen te hanteren bij het toetsen van de vraag of zorginstellingen de juiste maatregelen treffen voor invoering en handhaving van adequate informatiebeveiliging.

Ook de Autoriteit Persoonsgegevens (AP) hanteert de NEN 7510 e.v. als uitgangspunt voor toetsen van passende beveiliging in de zorg, in het bijzonder ook voor toegangsbeveiliging.

Wat betreft patiëntauthenticatie benadrukt de NEN 7510:2011 dat elke gebruiker over een unieke identificatiecode dient te beschikken (gebruikers-ID) voor persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen. Informatiesystemen, die patiëntgegevens verwerken, behoren volgens de NEN 7510 authenticatie toe te passen op basis van ten minste twee afzonderlijke kenmerken. Deze beheersmaatregel is van toepassing op alle typen gebruikers (waaronder technisch ondersteunend personeel, operators, netwerkbeheerders, systeemprogrammeurs

[14] NEN 7510 Informatiebeveiliging in de zorg en NEN 7512 Vertrouwensbasis voor gegevensuitwisseling. De norm NEN 7521 gaat over Toegang tot en uitwisselen van patiëntgegevens.

[16] Deze norm vervangt wat eerder de NEN 7510:2004 en de NEN 7511 was.

en databasebeheerders). De NEN 7510 stelt dat daar waar krachtige authenticatie en verificatie van de identiteit nodig zijn, andere authenticatiemethoden dan wachtwoorden, zoals cryptografische hulpmiddelen, smartcards, 'tokens' of biometrische hulpmiddelen gebruikt moeten worden.

Objecten zoals geheugen-'tokens' of 'smartcards' die gebruikers in hun bezit hebben, kunnen voor identificatie en authenticatie worden gebruikt. Ook biometrische authenticatietechnologieën, die gebruikmaken van unieke kenmerken of eigenschappen van een individu, kunnen worden gebruikt om de identiteit van de persoon te bewijzen. Een combinatie van technologieën en mechanismen, die veilig zijn verbonden, zal leiden tot meer betrouwbare authenticatie.

De NEN 7512 bevat een aanvulling voor een vertrouwensbasis voor gegevensuitwisseling in de zorg. In de NEN 7512 wordt de voor de gegevensuitwisseling vereiste zekerheid gekoppeld aan risicoklasse.

Als authenticatiemiddel kan gebruik worden gemaakt van *kennis* waarover de entiteit moet beschikken, van een fysiek authenticatiemiddel dat deze in *bezit* moet hebben, van een uniek *kenmerk* van de gebruiker of van een combinatie van deze authenticatiefactoren. De volgende authenticatiemiddelen worden onderscheiden: 1) Geheime kennis (wachtwoord, pincode); Fysiek kenmerk (biometrie; Fysiek bezit (token); Toetsbare verklaring (digitaal certificaat).

Benadrukt dient te worden dat de beveiliging van de toegang voor patënten tot hun medische gegevens niet alleen betrekking heeft op de authenticatie van de patiënt, maar als een continu managementproces waarbij risico's worden geinventariseerd, beleid en plannen worden opgesteld, maatregelen worden geimplementeerd en de effectiviteit van de genomen maatregelen wordt geevalueerd waarvanaf het proces opnieuw begint.

*De NEN 7521*
Onduidelijk is nog of de 7521 een norm wordt of een NTA (Nederlands Technisch Afspraak), dat een lagere status kent dan de norm. Het is nog in ontwikkeling. De ontwerp NEN-norm (of NTA) 7521 gaat over toegang tot patientgegevens. Bij patiëntauthenticatie moet volgens het ontwerp (7521) de identiteit herleidbaar zijn tot een individu en diens identiteit moet met zekerheid worden geauthentiseerd overeenkomstig de eisen die gelden voor STORK QAA niveau 4.[17]

*PKI-certificaten*
Een certificaat is een computerbestand dat fungeert als een digitaal paspoort en wordt gebruikt binnen de Public key infrastructure (PKI).

De eisen die in de gezondheidszorg gelden voor PKI-certificaten (tenminste vereist bij STORK QAA niveau 4) zijn beschreven in NEN-ISO 17090-1 (deel 1, 2 en 3).

*ISO/IEC 29115:2013*
Volgens overweging 3 bij de Uitvoeringsverordening van eIDAS[18] is de ISO /IEC 29115 de

[17] Ontwerp NTA 7521: versie augustus 2015, p.15
[18] Uitvoeringsverordening (EU) 2015/1502 van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen.

belangrijkste internationale norm op het gebied van betrouwbaarheidsniveaus voor internationale identificatiemiddelen. Bij het vaststellen van de minimale technische specificaties, normen en procedures van deze uitvoeringsverordening is daarom rekening gehouden met de ISO/IEC 29115. Het afsprakenstelsel ETD/ eID neemt de ISO/IEC 29915 op dit moment als uitgangspunt in afwachting van de nadere invulling van eIDAS. Hieronder lichten wij de ISO/IEC 29115 uit voordat we eIDAS gaan behandelen. Hoewel eIDAS rekening houdt met de ISO /IEC 29115 en als belangrijkste internationale norm erkent, dient volgens de uitvoeringsverordening (zie eisen in bijlage A) niet te worden verwezen naar de specifieke inhoud van deze internationale norm, omdat eIDAS hiervan inhoudelijk verschilt wat betreft de vereisten voor het bewijs en de verificatie van de identiteit, alsmede wat betreft de wijze waarop de verschillen tussen de identeitsregelingen van de lidstaten en de bestaande EU-instrumenten op dat gebied in aanmerking worden genomen. Voordat we bij eIDAS aankomen behandelen we nu eerst de ISO/IEC 29115:2013.

De Levels of Assurance (LoA, ook wel “betrouwbaarheidsniveaus”) van de ISO/IEC 29115:2013 geven aan op welk niveau de identiteit van gebruikers is vastgesteld. Een LoA wordt doorgegeven aan een dienstverlener, zodat deze de informatie mee kan nemen in risicoafwegingen tijdens het verlenen van de dienst. De hoogte van het
LoA wordt bepaald door:
• de kwaliteit van de processen waarmee de identiteit geverifieerd en uitgeleverd wordt,
• en de technieken waarmee de authenticatie plaatsvindt (het “authenticatiemiddel”).

ISO 29115 deelt, net als de nog in dit rapport te behandelen STORK, de betrouwbaarheid van een identiteit op in vier niveaus. Onderstaande niveau beschrijving komt uit ISO 29115:

| | |
|---|---|
| 1 – Laag: | Weinig/geen vertrouwen in geclaimde of verzekerde identiteit |
| 2 – Medium | Enig vertrouwen in de geclaimd of verzekerde identiteit |
| 3 – Hoog | Veel vertrouwen in de geclaimde of verzekerde identiteit |
| 4 – Zeer hoog | Zeer veel vertrouwen in de geclaimd of verzekerde identiteit |

Een betrouwbaarheidsniveau (LoA) is hierbij gelijk aan het registratieproces plus het middel.

*De proces-indeling conform ISO 29115*
De registratiefase bepaalt de eisen die gesteld worden wanneer een dienstafnemer wil aansluiten, bijvoorbeeld op het stelsel van Elektronische Toegangsdiensten / eID en daartoe authenticatiemiddelen aanvraagt. Het betreft de waarborgen in het proces van registratie van de gebruiker tot en met de uitgifte van een authenticatiemiddel aan deze gebruiker. Tevens volgt het betrouwbaarheidsniveau uit de mate waarin de kwaliteit van de processen en onderliggende mechanismen zijn vastgesteld bij de partij die het authenticatiemiddel uitgeeft: aan te duiden als "de kwaliteit van de organisatie". De elementen die in deze categorie beoordeeld worden zijn:

- Identificatieprocedure bij middelenuitgifte
- Proces van middelenuitgifte
- Partij die het authenticatiemiddel uitgeeft

De elektronische authenticatiefase betreft het technisch deel van de betrouwbaarheidsniveaus. Het gaat daarbij om het authenticatiemiddel zelf én de wijze

waarop het tijdens het gebruik functioneert. De elementen die in deze categorie beoordeeld worden zijn:

- Type en robuustheid van het authenticatiemiddel
- Zekerheid van het authenticatiemechanisme

De maatregelen die zijn getroffen om het authenticatiemechanisme op afstand c.q. via internet ("zekerheid van het authenticatiemechanisme") betrouwbaar te laten functioneren worden beoordeeld op de bescherming tegen identiteitsdiefstal. Dit betreft:

1. Raden (guessing): dreiging dat een geheim gegeven (cryptografische sleutel, PIN, etc.) in de communicatie wordt geraden.
2. Afluisteren (eavesdropping): dreiging dat informatie in de communicatie wordt afgeluisterd ten behoeve van analyse en vervolgaanvallen.
3. Overnemen van een sessie (hijacking): dreiging dat een geauthenticeerde communicatiesessie wordt overgenomen door een aanvaller.
4. Naspelen (replay): dreiging dat toegang verkregen wordt tot gevoelige informatie door eerder verzonden berichten opnieuw te versturen of te vertragen.
5. Man-in-the-middle: dreiging waarbij de aanvaller onafhankelijke verbindingen maakt met beide communicatiepartners en berichten aanpast en/of invoegt

Praktische handvatten voor het inschalen van concrete diensten naar betrouwbaarheidsniveaus worden niet gegeven door deze standaarden. De handreiking van het Bureau Forum Standaardisatie[19] is een voorbeeld voor het inschalen van diensten voor burger-naar-overheid. Hetzelfde geldt voor bijvoorbeeld de website van eHerkenning[20]. Op die website wordt het raadplegen van zeer gevoelige informatie, zoals een medisch dossier, ingedeeld in niveau 4 (zeer hoog) van de ISO 29115.

## §2.9 STORK

STORK is naast de ISO 29115/ 113 een van de belangrijkste standaarden voor indeling van betrouwbaarheidsniveaus voor authenticatie.
De betrouwbaarheid van ETD/eID - middelen is niet alleen afhankelijk van de beveiliging van het middel zelf, maar ook van het uitgifteproces. In STORK - een Europees project voor de interoperabiliteit van ETD's / eID's over de grenzen heen - zijn er net als bij ISO 29115 vier betrouwbaarheidsniveaus, de zogenaamde Quality Authentication Assurance (QAA) niveaus. Deze werken we verderop in de tekst uit. Het gaat dan om middelen die uitgegeven zijn met een fysieke controle van de persoon en zijn of haar identiteitsbewijs en een robuust ETD/eID-middel. In Nederland zijn in het personendomein nog geen middelen op hoog niveau beschikbaar. Technologisch is het wel mogelijk.

Voor de indeling van de niveaus wordt gekeken naar zowel de organisatorische als technische factoren. Bij organisatorische factoren wordt gekeken naar de identificatieprocedure, het afgifteproces van identeitstokens en de kwaliteit van de certificerende autoriteit. Bij de technische aspecten wordt onder andere gekeken naar het

[19] Forum Standaardisatie, Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten (versie 3), september 2014

[20] https://www.eherkenning.nl/aansluiten-op-eherkenning/betrouwbaarheidsniveaus/bepalen-van-juiste-niveau/voorbeelden-van-diensten/

type en de robuustheid van de identiteitstoken en de kwaliteit van het mechanisme dat gebruik wordt voor gebruikersauthenticatie. Elk van de factoren wordt gescoord en de zwakst scorende factor bepaalt het niveau van het authenticatiemiddel.
Het Forum Standaardisatie gebruikt STORK op dit moment als belangrijkste basis voor de uitwerking van vereiste betrouwbaarheidsniveaus bij overheidcommunicatie. In de vervolgversie van de handreiking betrouwbaarheidsniveaus neemt het forum eIDAS als uitgangspunt met STORK daarnaast. Wij betrekken in ons rapport beide standaarden, zoals ook door het ministerie verzocht.
Het STORK raamwerk gaat net als de ISO 29115:2013 uit van vier niveaus van betrouwbaarheid.
De vier niveaus die STORK definieert, zijn:

*STORK QAA niveau 1*
Dit niveau biedt het laagste niveau van zekerheid. Dat betekent: geen of minimale zekerheid ten aanzien van de geclaimde identiteit van de gebruiker.
Bij het registratieproces ter verkrijging van het authenticatiemiddel worden identificerende kenmerken zonder nadere verificatie overgenomen. Een voorbeeld is een proces waarin de aanvrager van het middel een email ontvangt van de uitgever met daarin een hyperlink die de aanvrager slecht hoeft aan te klikken om het middel in gebruik te nemen. De enige zekerheid is dat het e¬mail adres van de aanvrager bestaat op het moment van de aanvraag en dat een verder ongeïdentificeerde aanvrager in staat is te reageren op naar dat adres. verzonden e¬mailberichten. De hyperlink in dit voorbeeld leidt naar een algemeen document met hooguit openbare persoonsgegevens.

*STORK QAA niveau 2*
Op dit niveau vindt bij het registratieproces ter verkrijging van het authenticatiemiddel verificatie plaats van de door de gebruiker geclaimde identiteit. Dit gebeurt door controle op basis van een door een Staat afgegeven document (bijvoorbeeld een kopie van een paspoort of rijbewijs) of registratie (bijvoorbeeld de BRP. Er is echter geen sprake van fysieke verschijning in het registratieproces, een middel met ‘1 factor authenticatie’ volstaat. Onder een ‘factor’ wordt in dit kader verstaan een bewijsmiddel voor een geclaimde identiteit, bijvoorbeeld een username/password combinatie, of een door een vertrouwde partij toegezonden unieke code. DigiD is een voorbeeld van een middel met 1 factor authenticatie.

*STORK QAA niveau 3*
Dit niveau vereist striktere methoden voor de verificatie van de geclaimde identiteit van de gebruiker. Deze moeten een hoge mate van zekerheid bieden. Middelenuitgevers moeten verder onder overheidstoezicht staan. Als type middel is ‘2 factor authenticatie’ vereist. Voorbeelden daarvan zijn ‘soft’ certificaten of ‘one time password’ tokens. De RDW gebruikt bijvoorbeeld 2 factor authenticatie bij communicatie met bedrijven uit de voertuigenbranche die in die hoedanigheid bepaalde RDW gegevens mogen inzien. Ook de online bankapplicaties waarvoor de bankklanten een token nodig hebben zitten op dit niveau.

*STORK QAA niveau 4*
Dit niveau vereist tenminste eenmaal fysiek verschijnen van de gebruiker in het registratieproces en het voldoen aan alle eisen van de nationale wetgeving van het

desbetreffende land aangaande uitgifte van gekwalificeerde certificaten als bedoeld in Annex II van Richtlijn 1999/93/EG betreffende elektronische handtekeningen. Voor Nederland betreft dat de eisen van artikel 1.1, onderdeel ss, van de Telecommunicatiewet. Tevens moet de middelenuitgever voldoen aan Annex I van diezelfde richtlijn. In Nederland is dat artikel geïmplementeerd in artikel 18:16, eerste lid, van de Telecommunicatiewet. Overheidspartijen of bijvoorbeeld notarissen die documenten elektronisch willen aanleveren bij het Kadaster, kunnen dat doen via een speciale applicatie. Dit systeem vereist gebruik van een token, een gewaarmerkt certificaat èn een digitale handtekening.

## §2.10 eIDAS[21]

De eiDAS-verordening van het Europees Parlement en de Raad van 23 juli 2014 wordt per 1 juli dit jaar van kracht. Deze verordening gaat over de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en leidt tot een wettelijk kader voor betrouwbaarheidsniveaus.[22] De verordening regelt daartoe het grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de Europese Unie.
Om het stelsel in 2018 over de grens bruikbaar te laten zijn, zal Nederland -waarschijnlijk in 2017- zijn eigen ETD stelsel notificeren bij de Europese Commissie. Een lidstaat bepaalt zelf (of en) wanneer hij zijn stelsel wil notificeren. Notificatie is echter een voorwaarde om Nederlandse authenticatiemiddelen in andere EU lidstaten te kunnen gebruiken.[23]
Nederland moet het in september 2018 mogelijk maken dat met genotificeerde middelen uit andere EU lidstaten diensten afgenomen kunnen worden bij Nederlandse publieke instellingen en overheden.

eIDAS kent drie niveau's: laag, substantieel en hoog. Deze zijn nader uitgewerkt in een uitvoeringsverordening. [24] Voor het vaststellen van de specificaties en procedures die in deze uitvoeringshandeling zijn opgenomen, is rekening gehouden met de internationale norm ISO/IEC 29115, de internationale norm op het gebied van betrouwbaarheidsniveaus voor elektronische identificatiemiddelen. eIDAS verschilt inhoudelijk van die internationale norm, met name wat betreft de vereisten voor het bewijs en de verificatie van de identiteit, alsmede wat betreft de wijze waarop de verschillen tussen de identiteitsregelingen van de lidstaten en de bestaande EU-instrumenten op dat gebied in aanmerking worden genomen.

De verordening geeft aan welke resultaten met bepaalde controles bereikt moeten worden. Hoe die resultaten bereikt moeten worden wordt niet genoemd en vraagt om nadere uitwerking (in normering en lagere wetgeving).

---

[21] 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 (PbEU 2014, L 257)
[22] Naast betrouwbaarheidsniveaus biedt de eIDAS verordening een vernieuwd stelsel voor elektronische handtekeningen in de bredere context van 'vertrouwensdiensten'.
[23] Wij zijn ons ervan bewust dat we spreektaal en terminologie uit de Verordening door elkaar gebruiken. Waar we het gemakshalve hebben over authenticeren kan in de meeste gevallen ook gelezen worden 'electronisch identificeren'. Feitelijk is authenticatie onderdeel van de elektronische identificatie. De onderzoeksvraag richt zich op het betrouwbaarheidsniveau van de patiënt authenticatie, waardoor we ook de vaak gebruikte term authenticatiemiddel gebruiken. Dit middel wordt gebruikt voor elektronische identificatie, maar dus tegelijkertijd voor 'authenticatie' in dat proces. De eisen aan electronische identificatie zijn ruimer dan het authenticatiemiddel zelf.
[24] Uitvoeringsverordening (EU) 2015/1502 van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen.

In eerdere fase werden voor het afsprakenstelsel eHerkenning en in het ontwerp voor Idensys de betrouwbaarheidsniveaus van de in het Europese STORK programma opgestelde criteria gebruikt. [25] Idensys werkt eraan om de eisen in het Normenkader Betrouwbaarheidsniveaus (ETD-stelsel) in overeenstemming te brengen met de eisen die de Europese eIDAS verordening en de Uitvoeringsverordening stellen. Die overeenstemming is noodzakelijk om het stelsel te notificeren bij de Europese Commissie.

De eIDAS verordening dient op grond van overweging 11 van de verordening te worden toegepast in volledige overeenstemming met de beginselen inzake de bescherming van persoonsgegevens overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad. Daarmee zijn de hiervoor behandelde Wbp en de eIDAS verordening met elkaar verbonden.

Volgens overweging 16 van de eIDAS verordening dient het betrouwbaarheidsniveau de mate van vertrouwen weer te geven die in een elektronisch identificatiemiddel kan worden gesteld voor het vaststellen van de identiteit van een persoon, en moet zodoende zekerheid geven dat de persoon die beweert een bepaalde identiteit te hebben ook daadwerkelijk degene is aan wie deze identiteit is toegekend.[26] Diverse technische definities en beschrijvingen van betrouwbaarheidsniveaus danken hun bestaan aan grootschalige proefprojecten, standaardisering en internationale activiteiten. In het bijzonder refereren Proefproject STORK en ISO 29115 aan, onder meer, de niveaus 2, 3 en 4, met welke niveaus ten zeerste rekening moet worden gehouden bij het vaststellen van minimale technische vereisten, standaarden en procedures voor de betrouwbaarheidsniveaus laag, substantieel en hoog in de zin van deze verordening, terwijl gezorgd moet worden voor een consequente toepassing van deze verordening, met name wat betreft betrouwbaarheidniveau hoog voor het bewijzen van de identiteit voor het afgeven van gekwalificeerde certificaten. De vereisten moeten technologieneutraal zijn. Het moet mogelijk zijn aan de noodzakelijke veiligheidsvereisten te voldoen door middel van verschillende technologieën.

Dit laatste is ook de reden dat de Verordening niet concreet kan zijn op de manier zoals bijvoorbeeld STORK dat is. Bepaalde minimumvereisten kunnen worden benoemd, zonder dat al een keuze wordt gemaakt voor maatregelen die bij een betrouwbaarheidsniveau horen. De minimale vereisten dienen te worden vastgesteld om uniforme interpretatie te waarborgen. In de Uitvoeringsverordening (EU) 2015/1502 zijn de basis specificaties en procedures opgenomen, die concreet zullen moeten worden ingevuld.
Van belang voor het onderzoek is dat op basis van de eIDAS verordening, zowel als de uitvoeringsverordening, geen uitspraken kunnen worden gedaan over welk betrouwbaarheidsniveau bij bepaalde typen verwerking tenminste noodzakelijk moet worden geacht. De keuze in Europa om Verordeningen op te stellen voor privacywetgeving, elektronische identiteiten en elektronische handtekeningen is gericht op een sterke positie van Europa in de digitale wereld en de toenemende aandacht voor digitale fraude en de discussies over privacy. Deze ontwikkelingen vragen om hoge betrouwbaarheidsniveaus.

[25] STORK Secure idenTities acrOss boRders linKed. Zie document D2.3 – Quality authenticator scheme, paragraaf 2.3 en 2.4., te vinden op www.eid-stork.eu, onder STORK materials, deliverables approved/public.
[26] Het betrouwbaarheidsniveau hangt af van de mate van vertrouwen die elektronische identificatiemiddelen bieden voor de opgegeven of beweerde identiteit van een persoon, rekening houdend met processen (bijvoorbeeld het bewijzen van de identiteit,verificatie, en authenticatie), beheersactiviteiten (bijvoorbeeld de entiteit die elektronische identificatiemiddelen uitgeeft en de procedure voor uitgifte van dergelijke middelen) en geïmplementeerde technische beheersmaatregelen.

Niveau laag eIDAS laten we verder buiten beschouwing, omdat het voor de zorg en dit onderzoek niet relevant is. Niveau substantieel heeft vele aanvullende voorwaarden ten opzichte van niveau laag, zoals een twee authenticatiefactoren van verschillende soort plus een aanvraagproces waarbij een identiteitsdocument vereist is. De uitvoeringsrichtlijn geeft aan dat tonen van een identiteitsdocument mogelijk is, maar laat ook de mogelijkheid voor online-technologie zoals bijvoorbeeld bij Remote Document Authenticatie (RDA) technologie. Niveau Hoog kent in de Uitvoeringsverordening aanvullende voorwaarden die verschillend ingevuld kunnen worden. Op dit moment zijn er in Nederland nog geen authenticatiemiddelen op het niveau hoog voor patiënten breed beschikbaar.

### §2.11 Forum Standaardisatie

Het Forum Standaardisatie[27] heeft een Handreiking betrouwbaarheidsniveaus´s bij gebruik van overheidsdiensten opgesteld in opdracht van het College Standaardisatie overheidscommunicatie.[28] De handreiking geeft invulling aan betrouwbaarheidsniveaus op basis van de nationale geldende (wettelijke) regels en in aansluiting op het Europese STORK kader voor (grensoverschrijdend) gebruik van e-diensten. De handreiking van het forum heeft op dit moment zijn derde versie. De vierde versie waarin ook het eIDAS normenstelsel is meegenomen, is in de maak.

Zoals de naam van de handreiking duidelijk maakt gaat het daarin om authenticatie bij gebruik van overheidsdiensten. In de vraagstelling in dit onderzoek en de daarin genoemde use cases gaat het niet om het gebruik van overheidsdiensten, maar veeleer om het gebruik van private diensten. De uitwerking door het forum is derhalve niet zomaar toepasbaar in het onderzoek. Toch is een deel van de informatie in de Handreiking en het classificatiemodel daarin zeker van nut voor de beoordeling in dit onderzoek in verband met de overeenkomsten die te onderkennen zijn tussen bepaalde overheidsdiensten en de hier bedoelde private diensten evenals de overeenkomsten in relevante criteria.

Om te voorkomen dat gebruikers door verschillende oplossingen voor digitale toegang te maken krijgen met een grote digitale ‘sleutelbos’, wordt binnen de overheid gewerkt aan generiek inzetbare oplossingen.
Voorbeelden daarvan zijn DigiD, PKIoverheid en het afsprakenstelsel eTD/eID. Dit zorgt er tevens voor dat de kosten beheersbaar blijven. De vraag blijft welk middel in welke situatie dient te worden toegepast. Tegen die achtergrond is de handreiking voor authenticatie bij overheidsdiensten opgesteld door het forum.
De handreiking is bedoeld om een bijdrage te leveren aan een eenduidige bewuste bepaling van het betrouwbaarheidsniveau van elektronische overheidsdiensten. Het bevat daartoe een ‘classificatiemodel’ dat in feite een vereenvoudigde risicoanalyse is. Het classificatiemodel maakt op basis van verschillende (wettelijke) criteria een generieke

[27] Artikel 3 sub b Instellingsbesluit College en Forum Standaardisatie 2012, Stcrt, 2011, 23581.
[28] 1. Het Forum Standaardisatie adviseert op basis van onderzoek het College Standaardisatie over de digitale uitwisseling van informatie tussen overheden onderling en tussen overheid, bedrijven en burgers. Het College doet vervolgens aanbevelingen aan verschil- lende ministers over beleid op dit gebied en beheert de lijst met aanbevolen en verplichte open standaarden die voor de publieke sector van toepassing zijn. College en Forum Standaardisatie (http://www.forumstandaardisatie.nl).

koppeling mogelijk tussen (soorten) diensten en betrouwbaarheidsniveaus. Ook geeft de handreiking indicaties die tot inschaling op een hoger of lager betrouwbaarheidsniveau zouden kunnen leiden. De handreiking bevat geen vertaling van de betrouwbaarheidsniveau's naar specifieke authenticatiemiddelen.

Het classificatiemodel van het Forum geeft niet onder alle omstandigheden een juiste uitkomst. Er zijn zowel risicoverlagende als risicoverhogende factoren, waarmee door de verantwoordelijke altijd rekening gehouden dient te worden.

Forum Standaardisatie geeft voorbeelden over het betrouwbaarheidsniveau van diensten (corresponderend met STORK niveaus):

- **Betrouwbaarheidsniveau 1**

Gemeentelijke lokale diensten zoals melden gebreken in de openbare ruimte, aanvragen afvalcontainers.

- **Betrouwbaarheidsniveau 2**

Registreren voor gepersonaliseerde portalen (MijnOverheid.nl)
Gemeentelijke vergunningen (kap, evenementen e.d.)
Omgevingsvergunning particulieren
Financiële aanspraak particulieren (subsidie, uitkering, toeslag)
Verblijfsvergunning au pair
(Status)informatie in MijnOverheid.nl
Melden/registreren
Aangifte (delicten, licht)
Wijzigingen doorgeven
Belastingaangifte particulieren, geen voorinvulling gegevens over persoonlijke financiele situatie.
Naleving vergunning¬voorschriften particulieren
Inzien WOZ waardering

- **Betrouwbaarheidsniveau 3**

Belastingaangifte particulieren; ophalen of muteren vooringevulde aangifte (tonen persoonsgegevens klasse II)
Aanbestedingsdocumenten indienen
Omgevingsvergunning ondernemingen, verblijfsvergunning arbeids/kennismigranten, officiële documenten (VOG, paspoort, rijbewijs ed.)
Belastingaangifte ondernemingen
Financiële aanspraak ondernemingen (subsidie)
(Financiële) verantwoordingen (jaarrekening ed.)

- **Betrouwbaarheidsniveau 4**

Aangifte (geboorte)
Raadplegen medisch dossier
Aangifte (delicten, zwaar)
Octrooiaanvragen

# H3 Enkele authenticatie-proeftuinen in Nederland

In Hoofdstuk 2 is naar voren gebracht dat authenticatie op hoog niveau nog niet breed voorhanden is en op het hoogste niveau voor burgers nog niet breed beschikbaar. Er zijn enkele voorbeelden van pilots met 'nieuwe' authenticatiemethoden die worden beproeft, ook in de zorg. Deze worden in dit hoofdstuk beschreven. Mogelijk wordt met die methoden een betrouwbaarheidsniveau conform substantieel of hoog in de zin van de EU verordening bereikt. Een aparte studie is nodig om dit met zekerheid vast te stellen. Dit betreft niet de scope van ons onderzoek. Het is niettemin van belang om hier aan te geven dat de meest recente grotere experimenten op dit gebied mogelijk een dergelijk betrouwbaarheidniveau realiseren maar dat dit niet vast staat. In de iDIN pilot wordt onderzocht of en met welke aanvullende maatregelen mogelijk betrouwbaarheidsniveau hoog (eIDAS) gerealiseerd kan worden. (Zie ook §5.9) Hetzelfde geldt voor de pilots met Idensys.

*RDA Pilot*
Logius voert tot en met 31 december 2016 samen met de RDW ten behoeve van een onderzoek naar een veiliger en betrouwbaarder authenticatieproces met DigiD, een pilot uit met RDA. RDA is een techniek waarmee een gebruiker - na een geslaagde inlog met zijn DigiD-gebruikersnaam en wachtwoord - met behulp van een Nederlands identiteitsdocument (paspoort, identiteitskaart of rijbewijs), in combinatie met een kaartlezer, toegang krijgt tot digitale diensten in het burgerservicenummerdomein. De kaartlezer communiceert hiertoe met de contactloze chip in het reisdocument en stelt via cryptografische processen vast dat de chip authentiek en onveranderd is en toebehoort aan de persoon die inlogt. De aansluiting bij deze RDA-pilot op het huidige DigiD betekent dat alle DigiD diensten van RDA gebruik kunnen maken. Dat betreft dus overheidsdiensten, maar ook de specifieke domeinen die op dit moment al van DigiD gebruik mogen maken, zoals bepaalde organisaties in de zorg.

*Publiek middel*
Op 15 februari jl. heeft Minister van Binnenlandse Zaken Ronald Plasterk de eerste Nederlandse elektronische identiteitskaart uitgereikt in het kader van een pilot in Den Haag. Naast de pilot in Den Haag wordt in Eindhoven en Groningen in het kader van deze pilot ervaring opgedaan met het elektronisch rijbewijs.

*iDIN pilot*
De banken zijn op 8 maart 2016 gestart met de eerste pilot met iDIN onder regie van Betaalvereniging Nederland. iDIN is een nieuwe dienst van de banken waarmee consumenten zich bij andere organisaties online kunnen identificeren, met de inlogmiddelen van hun eigen bank.
Gedurende de pilotperiode kunnen consumenten met iDIN onder meer inloggen op Mijn Belastingdienst. Klanten van ING en Rabobank kunnen vanaf de start meedoen aan de pilot. Klanten van ABN AMRO, SNS en Triodos volgen in april.
iDIN wordt aangeboden naast andere inlogmethodes, zoals DigiD bij de overheid. Bezoekers kunnen zelf kiezen welke inlogmethode ze gebruiken. Het gebruik van iDIN lijkt op de manier waarop consumenten iDEAL gebruiken. Om met iDIN te kunnen inloggen op Mijn Belastingdienst moet de identificatiedienst eenmalig via internet worden geactiveerd voor

gebruik bij de overheid. Daarna kan bij volgende bezoeken aan Mijn Belastingdienst direct met iDIN worden ingelogd.
De banken zullen in de loop van 2016 ook pilots met webwinkels en verzekeringsmaatschappijen uitvoeren.

*Pilots in de zorg*
Nictiz begeleidt en faciliteert zeven (mogelijk acht) organisaties in het zorgveld bij het testen van Idensys in de praktijk.
De organisaties die deelnemen aan de testen in de zorg zijn:

- Isala Klinieken
- MijnZorgtoegang (Fysiomanager)
- Meddex
- Patient 1
- Pazio
- Pharmeon
- UMCU

Eind april 2016 starten de eerste organisaties in de zorg met het testen van Idensys. Dit betekent dat gebruikers (patiënten) gaan inloggen met een nieuw middel om zichzelf te identificeren. De test moet laten zien of alles werkt zoals bedoeld. De ervaringen uit de zorg worden samen met die van de andere deelnemers geëvalueerd. Vervolgens besluit de regering of Idensys een nieuwe manier van inloggen wordt waar iedereen gebruik van kan maken.

Gedurende het jaar 2016 worden in Nederland meerdere pilots[29] uitgevoerd, afhankelijk van verdere invulling van eIDAS in de loop van het jaar, ervaringen met de pilots en het al dan niet aansluiten op het ETD/eID-stelsel. Via het stelsel wordt de koppeling met de rest van Europa mogelijk. Na evaluatie van bovenstaande pilots gaat het kabinet een besluit nemen over de verschillende inlogmiddelen.

[29] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/12/14/rapport-start-van-de-pilots/rapport-start-van-de-pilots.pdf

## H4 Richtsnoeren beveiliging van de Autoriteit Persoonsgegevens

Het beveiligen van persoonsgegevens is een van de verplichtingen die de Wbp oplegt aan verantwoordelijken voor de verwerking van persoonsgegevens. De beveiligingsmaatregelen die de verantwoordelijke treft, zijn onderdeel van het totaal aan maatregelen dat de verantwoordelijke neemt om te voldoen aan de Wbp. De richtsnoeren gaan in op het beveiligingsaspect.

De Registratiekamer, de voorloper van het CBP, bracht in 2001 een publicatie uit over de beveiliging van persoonsgegevens (hierna: a&v 23).[30] De richtsnoeren vervangen a&v 23. In de overwegingen in de richtsnoeren komen aspecten uit de AV 23 echter wel weer naar voren, waarmee de AP bepaalde elementen daaruit meeneemt in het huidige kader. Die elementen zijn in dit onderzoek relevant en komen verderop aan bod.
In de richtsnoeren is gekozen voor een methodiek die aansluit bij de gangbare praktijk van de informatiebeveiliging en die verantwoordelijken de flexibiliteit biedt om die beveiligingsmaatregelen te treffen die in hun situatie het meest passend zijn.

Rechterlijke uitspraken kunnen naast wetswijzigingen, technische ontwikkelingen en praktijkervaringen aanleiding geven tot aanvulling of herziening van deze richtsnoeren. De AP herziet de richtsnoeren in ieder geval bij de invoering van de Algemene Verordening Gegevensbescherming, tenzij er dan een Europese handreiking wordt vastgesteld dat de richtsnoeren vervangt of overbodig maakt. De richtsnoeren houden volgens de AP al zo veel mogelijk rekening met de relevante bepalingen uit de verordening.

*Informatiebeveiliging*
Drie elementen uit het vakgebied informatiebeveiliging worden door de AP beschouwd als randvoorwaarden om tot passende beveiliging te komen zoals de wet die voorschrijft: maatregelen treffen op basis van risicoanalyse, beveiligingsstandaarden toepassen en de inbedding in een plan-do- check-act-cyclus.

De term betrouwbaarheid behelst de drie aspecten integriteit, vertrouwelijkheid en beschikbaarheid. Dat laatste is voor de beveiligingseis van artikel 13 slechts gedeeltelijk relevant: namelijk voor zover het gaat om het beveiligen tegen verlies van gegevens. Integriteit wordt in de Wbp beschermd door beveiliging tegen aantasting of onbevoegde wijziging van gegevens. Vertrouwelijkheid wordt beschermd door het vereiste van beveiliging tegen onbevoegde kennisneming of verstrekking van gegevens.

Inbedding van de plan-do-check-act-cyclus of kwaliteitscirkel in de dagelijkse praktijk van de organisatie stelt de verantwoordelijke in staat om tot een blijvend passend beveiligingsniveau te komen.

Het treffen van maatregelen op basis van een risicoanalyse stelt de verantwoordelijke in staat om die maatregelen te treffen die een passend beveiligingsniveau garanderen.

[30] G.W. van Blarkom en drs. J.J. Borking, 'Beveiliging van persoonsgegevens', Achtergrondstudiesen Verkenningen nr. 23, Registratiekamer,april 2001 (http://www.cbpweb.nl/downloads_av/av23.pdf ).

De risicoanalyse geeft aan welke risico's moeten worden afgedekt; beveiligingsstandaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de risico's af te dekken. Veel beveiligingsstandaarden bevatten ook een 'basisset' aan maatregelen die in de meeste situaties noodzakelijk zijn om tot adequate beveiliging te komen.
Beveiligingsstandaarden vormen een weerslag van de *lessons learned* die bij de beveiliging in een specifieke branche of in een specifieke technologische omgeving zijn opgedaan. Ze geven weer welke maatregelen door beveiligingsdeskundigen binnen de betreffende context in het algemeen als 'passend' worden beschouwd en, in het geval van de meer technisch gerichte standaarden, welke technologische middelen bij de beveiliging worden toegepast. Correct gebruik van actuele beveiligingsstandaarden stelt de verantwoordelijke in staat om passende maatregelen te treffen en om tot een evenwichtig en effectief geheel aan technische en organisatorische maatregelen te komen.

De Code voor Informatiebeveiliging is een technologieneutrale standaard die binnen de informatiebeveiliging breed wordt toegepast bij het formuleren en implementeren van beveiligingsmaatregelen. Voor de zorgsector is de Code voor Informatiebeveiliging nader uitgewerkt in de NEN 7510. De Code voor Informatiebeveiliging en NEN 7510 zijn beveiligingsstandaarden die door de AP worden gezien als standaarden die het hele terrein van de informatiebeveiliging binnen een organisatie afdekken. Het zijn algemene, technologie-neutrale standaarden, wat betekent dat ze niet ingaan op de maatregelen die moeten worden getroffen bij een specifiek type verwerking of bij het gebruik van een specifieke technologie.

Voor de beveiliging van webapplicaties zijn er de ict-beveiligingsrichtlijnen voor web-applicaties van het Nationaal Cyber Security Centrum (NCSC[31]) van het ministerie van Veiligheid en Justitie.

*Voldoen aan de wettelijke normen*
Wanneer zijn beveiligingsmaatregelen nu 'passend', zoals de Wbp eist? De Richtsnoeren Beveiliging van Persoonsgegevens leggen uit hoe de AP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen de beveiligingsnormen uit de Wbp toepast. De richtsnoeren vormen de verbindende schakel tussen enerzijds het juridisch domein, met daarbinnen de eisen uit de Wbp, en anderzijds het domein van de informatiebeveiliging, waarin de noodzakelijke kennis en kunde aanwezig is om daadwerkelijk aan die eisen te voldoen.
Dat betekent dat de richtsnoeren in samenhang worden gebruikt met algemeen geaccep-teerde beveiligingsstandaarden binnen de praktijk van de informatiebeveiliging, zoals de Code voor Informatiebeveiliging of de ICT-Beveiligingsrichtlijnen voor webapplicaties van het Nationaal Cyber Security Centrum.

Na het vaststellen van de betrouwbaarheidseisen treft de verantwoordelijke passende beveiligingsmaatregelen die waarborgen dat aan de betrouwbaarheidseisen wordt voldaan. "De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand

[31] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau," zo stelt het CBP (destijds) in het rapport.

De maatregelen zijn gebaseerd op een risicoanalyse en dekken de risico's zodanig af dat aan de betrouwbaarheidseisen wordt voldaan. Naarmate de vereiste betrouwbaarheid c.q. het vereiste beveiligingsniveau hoger is, treft de verantwoordelijke meer en zwaardere beveiligingsmaatregelen om de aanwezige risico's af te dekken en het vereiste beveiligingsniveau daadwerkelijk te garanderen.

De risicoanalyse geeft aan welke risico's moeten worden afgedekt; beveiligingsstandaarden geven houvast bij het daadwerkelijk treffen van passende maatregelen om de risico's af te dekken. Welke beveiligingsstandaarden voor een bepaalde verwerking relevant zijn en welke beveiligingsmaatregelen op grond van deze beveiligingsstandaarden moeten worden getroffen, moet van geval tot geval worden bepaald.

Het CBP geeft in de richtsnoeren concrete aanwijzingen over het gevraagde betrouwbaarheidsniveau bij bepaalde gegevensverwerking. Het geeft daarbij ook enkele voorbeelden uit de zorgpraktijk die we zullen gebruiken in de beoordeling.

# H5 Beoordeling van de onderzoeksvraag

*Betrouwbare digitale dienstverlening*
Voor het leveren van goede, gebruikersvriendelijke digitale diensten, maar ook voor de ontwikkeling van nieuwe diensten is vertrouwen nodig in een zorgvuldige en betrouwbare dienstverlening. Dat betekent dat er zekerheid nodig is over de identiteit van een burger, in dit onderzoek de patient, op een vergelijkbaar niveau van zekerheid over de identiteit van iemand in de off-line wereld. Er moet onder andere vastgesteld worden met wie een dienstverlener te maken heeft (identificatie) en dat de geclaimde identiteit ook daadwerkelijk bij de betreffende persoon hoort (authenticatie). Vervolgens moeten de persoonlijke gegevens bij de identiteit ook betrouwbaar zijn. Het kan van een aantal van die gegevens afhangen of iemand wel of geen recht heeft op de te leveren dienst. Daarnaast moet de persoon bevoegd zijn om de betreffende dienst af te nemen en de daarbij horende rechtshandeling uit te voeren (autorisatie).

## §5.1 Betrouwbaarheidsniveau's

In de beoordeling zullen we uitgaan van de betrouwbaarheidsniveau's zoals ze zijn aangegeven in de gangbare standaarden STORK en de eIDAS verordening en uitvoeringswetgeving. Derhalve zullen de STORK niveau's QAA 1 t/m 4 en de niveau's laag, substantieel en hoog uit de verordening gebruikt worden in de beoordeling, zoals het ministerie van VWS expliciet in haar opdracht heeft verzocht. Dit betekent overigens niet dat de de ISO/IEC 29115 daarmee minder belangrijk is dan STORK.

Als wij in het algemeen spreken over niveau substantieel of hoog dan verwijst dat naar de niveaus uit de eIDAS normering en naar STORK niveau 3 respectievelijk niveau 4.

Wat betreft STORK en eIDAS is een directe relatie (mapping) niet te geven, omdat de betrouwbaarheidsniveaus van STORK niet in eIDAS zijn overgenomen. Wel is er een parallel tussen de normen en de gedeelde terminologie. Ook STORK noemt deze niveaus (STORK 3 en 4) respectievelijk 'substantieel' en 'hoog'. De niveau's in STORK zijn echter concreet beschreven, als praktische implementatiestandaard. De verordening schept daarentegen een abstract kader voor Europese toepassing, waarbij de betrouwbaarheidsniveau's technologieneutraal ingericht moeten kunnen worden. In de Uitvoeringsverordening (EU) 2015/1502 heeft de Europese Commissie de minimale specificaties en procedures vastgesteld die vereist zijn bij de verschillende betrouwbaarheidsniveau's. De uitwerking van eIDAS zal in de komende tijd verder vorm moeten krijgen in eventuele nadere regels door de Europese Commissie en/of normering en standaardisering.

Zowel STORK als de ISO/IEC 29115 zijn heel belangrijk voor elektronische identificatie. In de Uitvoeringsverordening wordt in de overwegingen expliciet verwoord dat de bijlage waarin de specificaties en procedures zijn opgenomen op de ISO/IEC 29115 is gestoeld. Er is echter ook een aantal belangrijke verschillen[32] waardoor er geen verwijzing naar specifieke inhoud van de norm bestaat. Daarnaast wordt in de overwegingen van de uitvoeringsverordening

[32] De eIDAS Verordening verschilt van de ISO/IEC 29115, met name wat betreft de vereisten voor het bewijs en de verificatie van de identiteit, alsmede op het punt van het in aanmerking nemen van verschillen tussen identiteitsregelingen van de lidstaten.

benadrukt dat bij het vaststellen van specificaties en procedures op basis van de Uitvoeringsverordening terdege rekening moet worden gehouden met STORK en de ISO/IEC 29115.[33]

Overigens stelt de Europese 'Algemene verordening persoonsgegevens' (AVG) aangescherpte voorwaarden voor (het) proces van de (on line) verwerking van (bijzondere) persoonsgegevens (in de zorg).

## §5.2 Risico analyse van de toepassingen

De onderzoeksvraag naar het betrouwbaarheidniveau van de patiënttoegang is feitelijk een analyse van de beschikbare aanwijzingen van het risico van de gegevensverwerkingen *in het algemeen*. Bijzonderheden van het concrete geval kunnen het noodzakelijke betrouwbaarheidsniveau beinvloeden.

De verantwoordelijke is degene die zorg moet dragen voor passende beveiliging en bescherming van persoonsgegevens die hij verwerkt. Het is dan ook de verantwoordelijke die moet zorgen dat een digitale toepassing waarbij aan patiënten toegang wordt gegeven tot persoonsgegevens op passende wijze beveiligd is en aldus een voldoende betrouwbaarheidsniveau van authenticatie kent. Wie de verantwoordelijke voor een bepaalde toepassing van gegevensverwerking is, bepaalt mede welk betrouwbaarheidsniveau vereist is. Zo kan er verschil zijn in toepassingen die in stand worden gehouden door overheidsinstanties, zorgaanbieders of private (commerciële) organisaties die geen zorgaanbieder zijn. Ook zouden er toepassingen van de patiënt zelf kunnen zijn. Verschillen kunnen onder andere veroorzaakt worden door de (extra) eisen die aan de overheid gesteld worden en door het al dan niet van toepassing zijn van het medisch beroepsgeheim op de betreffende gegevens en de verantwoordelijke.

In de use cases wordt niet uitgegaan van de overheid als verantwoordelijke, het gaat immers om 'patiënten' in de casus. Voor het overige zullen bovengenoemde relevante aspecten die verschil kunnen maken in de casus besproken worden.

## §5.3 Algemene uitgangspunten beoordeling use cases

Het is van belang dat de verantwoordelijke beveiligingsmaatregelen treft op basis van een risicoanalyse, waarbij hij de dreigingen inventariseert die kunnen leiden tot een beveiligingsincident, de gevolgen die het beveiligingsincident kan hebben en de kans dat deze gevolgen zich voordoen. De verantwoordelijke kiest de maatregelen zodanig dat wordt voldaan aan de vastgestelde betrouwbaarheidseisen. De risicoanalyse is een belangrijke randvoorwaarde voor "[maatregelen die], rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau [garanderen]".[34]

Het bovenstaande betekent dat de verantwoordelijke een vertaalslag moet maken van de risico's voor de betrokkene(n) naar de betrouwbaarheidseisen. Voor deze vertaalslag zijn vooral de gevolgen relevant die betrokkenen kunnen ondervinden van verlies of

[33] Zie overweging 3 en 4 van de Uitvoeringsverordening.
[34] Artikel 13 Wbp.

onrechtmatige verwerking van hun persoonsgegevens. Deze gevolgen kunnen, afhankelijk van de aard van de verwerking en van de verwerkte persoonsgegevens, onder meer bestaan uit stigmatisering of uitsluiting, schade aan de gezondheid of blootstelling aan (identiteits)fraude.

Voor het vaststellen van de betrouwbaarheidseisen zijn, vanuit de beveiliging van persoonsgegevens en het belang van de betrokkenen bezien, de risico's voor één, individuele betrokkene maatgevend. De schade die betrokkenen ondervinden van verlies of onrechtmatige verwerking van hun persoonsgegevens wordt bepaald door de aard van de gegevens en de aard van de verwerking en niet door het aantal anderen van wie de persoonsgegevens eveneens verloren zijn gegaan of onrechtmatig zijn verwerkt.[35]

Bij verwerkingen met een hoog risico voor de betrokkene(n) is over het algemeen een hoge mate van vertrouwelijkheid vereist. Afhankelijk van de aard van de verwerking geldt hetzelfde voor de integriteit en voor de beveiliging van de persoonsgegevens tegen verlies.

De beoordeling van de use cases doet niet af aan de noodzaak voor verantwoordelijken om een risicoanalyse uit te voeren. Het gaat in dit onderzoek uitsluitend om het in kaart brengen van de algemene aanwijzingen voor beoordeling van het risico en de inschaling van het benodigde betrouwbaarheidsniveau.

De vragen die bij beoordeling van een betrouwbaarheidsniveau door de verantwoordelijke steeds gesteld moeten worden zijn:

- *Is er sprake van "een passend beveiligingsniveau gelet op de risico's die [...] de aard van de te beschermen gegevens met zich meebrengt"?*

De stand van de techniek, ontwikkelingen in de maatschappij en andere factoren kunnen van invloed zijn op de gevolgen die verlies of onrechtmatige verwerking van persoonsgegevens met zich mee kunnen brengen voor de betrokkenen. Het CBP (tegenwoordig de AP) noemt in de richtsnoeren onder andere:

- Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp;

- Gegevens over de financiële of economische situatie van de betrokkene;

- (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;

Hieronder vallen bijvoorbeeld gegevens over verslaving, werkprestaties of relatieproblemen.

- Gegevens die betrekking hebben op mensen uit kwetsbare groepen;

- Gegevens die kunnen worden misbruikt voor (identiteits)fraude.

Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het burgerservicenummer (BSN).

- *Is er sprake van "een passend beveiligingsniveau gelet op de risico's die de verwerking [...] met zich*

[35] CBP, Richtsnoeren beveiliging van persoonsgegevens, 2013

*meebrengt"?*

Behalve de aard van de verwerkte gegevens, kan ook de verwerking zelf risico's met zich meebrengen voor de betrokkenen. Factoren die een rol spelen zijn onder meer:

- Hoeveelheid verwerkte persoonsgegevens per persoon;

Naarmate er per persoon meer persoonsgegevens worden verwerkt, kan verlies of onrechtmatige verwerking leiden tot een grotere inbreuk op de persoonlijke levenssfeer. Het uitlekken van een compleet medisch dossier leidt over het algemeen bijvoorbeeld tot een grotere inbreuk dan het uitlekken van een herhaalrecept.[36]

- Doel of doelen waarvoor de persoonsgegevens worden verwerkt;

Naarmate de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpender zijn, is ook de impact van verlies of onrechtmatige verwerking groter.

Als voorbeeld kan gelden het medisch ingrijpen of handelen op basis van elektronisch verwerkte gegevens waarvan de integriteit geschaad is.

### §5.4 Voorbeeldcasus en jurisprudentie AP

Zoals hierboven beschreven geven de standaarden en normen veel informatie over waar betrouwbaarheidsniveaus's aan moeten voldoen, maar weinig over welk betrouwbaarheidsniveau in een bepaald geval vereist is. Ook de wetgever is niet expliciet over welk niveau in welk geval vereist is, wel wordt steeds over een hoog niveau of het hoogste niveau gesproken als het om gezondheidsgegevens gaat. Invulling komt derhalve goeddeels tot stand in jurisprudentie. Het CBP, nu AP, heeft in de richtsnoeren een uitgesproken voorbeeld gegeven van de vereisten en ook uitspraak gedaan in onderzoek.

Het voorbeeld uit de richtsnoeren gaat over 'beveiliging van via internet toegankelijke bijzondere persoonsgegevens'. Dit slaat, zoals in de use cases onderbouwd zal worden, op alle voorgelegde casus in het onderzoek.

*"Beveiligingsonderzoekers komen erachter dat een webapplicatie die toegang geeft tot elektronische dossiers met persoonsgegevens beveiligingslekken bevat, waardoor onbevoegden toegang kunnen krijgen tot de achterliggende database. De applicatie wordt gebruikt door een groot aantal organisaties. In de applicatie worden bijzondere persoonsgegevens (medische gegevens) en het BSN verwerkt en de hoeveelheid gegevens die per persoon wordt verwerkt is in sommige gevallen aanzienlijk. Onrechtmatige toegang tot de dossiers kan voor de betrokkenen dus grote schade met zich meebrengen. Daarbij gaat het om een webapplicatie, waarbij altijd rekening moet worden gehouden met de mogelijkheid dat een hacker onrechtmatig toegang krijgt tot de verwerkte persoonsgegevens.*

*De leverancier van de applicatie besluit daarom om niet alleen de beveiligingslekken te dichten, maar ook de beveiliging van de toegang tot de dossiers met persoonsgegevens aan te scherpen door gebruik te maken van zogeheten tweefactorauthenticatie. Gebruikers kunnen in het vervolg alleen nog maar toegang krijgen tot de applicatie als ze beschikken*

[36] Het voorbeeld wordt genoemd in de CBP Richtsnoeren beveiliging van persoonsgegevens, 2013.

*over een combinatie van een wachtwoord en een fysiek herkenningsmiddel (token). Door het gebruik van tweefactorauthenticatie wordt voorkomen dat een hacker door het wachtwoord te achterhalen zich toegang verschaft tot de verwerkte persoonsgegevens."*[37]

Naar aanleiding van deze casus beschrijft het CBP in de richtsnoeren het volgende: "Bepaalde verwerkingen brengen door de combinatie van de aard van de verwerkte gegevens, de hoeveelheid gegevens die per persoon wordt verwerkt en de doelen waarvoor de persoonsgegevens worden verwerkt dusdanige risico's met zich mee dat het *hoogste beveiligingsniveau* is vereist". Verwerkingen in deze categorie zijn onder meer verwerkingen bij opsporingsdiensten met bijzondere bevoegdheden of verwerkingen waarbij de belangen van een grote groep betrokkenen zeer ernstig kunnen worden geschaad indien de verwerkingen onzorgvuldig of onbevoegd geschieden, zoals bij DNA-databanken. Daarnaast vallen ook verwerkingen waarop een bijzondere geheimhoudingsplicht van toepassing is binnen deze categorie. Deze geheimhoudingsplicht kan door de overheid zowel wettelijk als anderszins formeel zijn geregeld of door een private organisatie zijn ingevoerd voor haar medewerkers.[38]

Bij dergelijke verwerkingen wordt er al in het vroegste ontwerpstadium rekening gehouden met het vereiste beveiligingsniveau (security by design) en het vereiste niveau van gegevensbescherming (privacy by design). Privacy enhancing technologies (pet) zijn bij dergelijke verwerkingen onmisbaar aldus het CBP/AP. Bij de keuze van de beveiligingsmaatregelen is het vereiste beveiligingsniveau leidend.[39]

Passende beveiliging moet altijd worden afgemeten aan onder andere de stand van de techniek. Het feit dat een bepaalde technologie bestaat, betekent nog niet dat deze ook (al) daadwerkelijk (in de markt of van overheidswege) toegankelijk is voor een bepaalde gebruikersgroep (bijvoorbeeld de burger) tegen reële kosten.[40] Tegelijkertijd is het logisch dat gegevens die een hoog betrouwbaarheidsniveau niveau nodig hebben niet verwerkt mogen worden bij gebrek aan goede middelen voor elektronische identificatie. Passende beveiliging mag door een gebruiker steeds verwacht en verlangd worden.

De verantwoordelijke (en eindgebruiker) heeft een afweging te maken ten aanzien van de toepassing van passende beveiliging. Welke beveiliging is passend op het moment van de gegevensverwerking gelet op alle relevante factoren? Hoe moet dit specifiek worden gewogen wanneer bijvoorbeeld gedurende lange tijd een middel op niveau hoog eIDAS niet voorhanden blijkt in de gevallen waarin dat niveau het meest passend lijkt, terwijl er druk bestaat vanuit vraag of zelfs wetgeving om tot elektronische gegevensverwerking over te gaan? Dit vraagpunt dient nader ingevuld te worden. Wij wijzen er hier in elk geval op dat de richtsnoeren aangeven dat bij gebrek aan beveiliging op *passend* niveau de verwerking vooralsnog achterwege dient te blijven.

*Analyse casus*
Opvallend in dit uitgangspunt van de AP is dat men duidelijk aangeeft dat de verwerking van gezondheidsgegevens waarop een bijzondere geheimhoudingsplicht - zoals het medisch

[37] CBP heeft dit voorbeeld in de richtsnoeren op pagina 20.
[38] CBP, Richtsnoeren Beveiliging van Persoonsgegevens, p.20
[39] CBP, Richtsnoeren Beveiliging van Persoonsgegevens, p.20
[40] Redelijke kosten betekent overigens niet dat met het beschikbaar maken van een authenticatiemiddel op hoog betrouwbaarheidsniveau niet hoge kosten gepaard zullen gaan en dat dit een reden zou zijn een dergelijk middel als niet passend te beschouwen.

beroepsgeheim- van toepassing is in deze categorie valt. De categorie waarvoor *het hoogste* beveiligingsniveau noodzakelijk is bij verwerking. Het is duidelijk dat het CBP hiermee de overwegingen uit de eerdere A&V 23 studie, ten aanzien van de hoogste risicoklasse van gegevensverwerking, terug laat komen in deze richtsnoeren.

*Jurisprudentie*
Daarnaast heeft het CBP op het onderzoek toegesneden jurisprudentie gemaakt in de casus van het Flevo ziekenhuis. In de Flevo-zaak (z2005-1372) heeft het CBP (nu AP) gesteld dat de aanwezigheid van een afspraak op een polikliniek een significante correlatie met de gezondheidssituatie van de patiënt heeft. Afspraakgegevens zijn volgens de Autoriteit naar hun aard specifieker dan het enkele feit dat iemand ziek is, omdat zij, afhankelijk van de grootte van de afdeling (of polikliniek) en de breedte van de specialisatie een – min of meer nauwkeurig - beeld kunnen geven van de betreffende ziekte. Dat maakt dat het ook in dat geval gaat om gegevens betreffende de gezondheid, bijzondere gegevens dus zoals de Wbp bedoeld. Het verwerken van gezondheidsgegevens is in de Wbp en de aanstaande Algemene verordening gegevensbescherming aan strikte voorwaarden en een verbodsregime onderworpen vanwege het hoge risiconiveau.

Volgens de Autoriteit Persoonsgegevens kunnen bovendien ook niet-strikt medische zaken onder het begrip “inlichtingen over de patiënt” vallen (artikel 7:457 lid 1 Burgerlijk Wetboek (BW). Ook afspraakgegevens vallen volgens de Autoriteit onder het medisch beroepsgeheim. Dit sluit overigens aan bij de gangbare uitleg van het medisch beroepsgeheim in het gezondheidsrecht.[41] Dat betekent dat de AP in deze uitspraak via twee redeneerlijnen tot de conclusie komt dat deze gegevensverwerking in een hoge risicoklasse ingedeeld moet worden. Deze beide aspecten spelen een rol in de casus van dit onderzoek.[42]

## §5.5 Het verwerken van het BSN

Hierboven zagen we al dat het verwerken van bijzondere persoonsgegevens zoals gezondheidsgegevens en BSN extra risico meebrengt, evenals het verwerken van gegevens waarop een bijzondere geheimhoudingsplicht rust zoals het medisch beroepsgeheim. In de te beoordelen casus spelen deze drie factoren meestal allemaal mee.
In het kader is reeds ter sprake gekomen wat het verwerken van het BSN meebrengt. Een aantal bepalingen in de Wet gebruik BSN in de zorg, de regeling gebruik BSN in de zorg en de Wet Algemene Bepalingen BSN (Wabb) regelen dat het BSN als gegeven verwerkt zal worden in de toepassingen waarover we het hebben in de use cases van dit onderzoek.
Op het verwerken van het BSN gaan we hier apart in.

Dat heeft een aantal elkaar aanvullende redenen. Er bestaat geen rechtstreekse uit de wet voortvloeiende verplichting (vooralsnog) om het BSN te verwerken in communicatie tussen zorgaanbieder en patiënt. Die verplichting is er bijvoorbeeld wel voor communicatie tussen zorgaanbieders onderling of met de verzekeraar. (artikel 9 Wet gebruik burgerservicenummer in de zorg)

[41] Zie bijvoorbeeld de wetstoelichting op artikel 88 Wet BIG en artikel 7:457 BW, alsmede Handboek Gezondheidsrecht, Deel 1 Rechten van mensen in de gezondheidszorg, H.J.J. Leenen.
[42] Opgemerkt dient te worden dat deze uitspraak dateert uit 2005 met de stand van de techniek die op dat moment beschikbaar was.

Er is echter wel een verplichting het BSN op te nemen in de eigen administratie en het te gebruiken bij gegevensverwerking in verband met de zorgverlening. (artikel 6 lid 2 Wet gebruik burgerservicenummer in de zorg) Ook is de zorgverlener verplicht het BSN te verifiëren en zich ervan te vergewissen dat het BSN wordt verwerkt in combinatie met de juiste persoon, tenzeinde ervoor te zorgen dat de gegevens die worden verwerkt in de zorg de juiste persoon betreffen.

Daarnaast heeft een patient ook recht op inzage en correctie van de verwerking van hem betreffende gegevens. Dit omvat ook het BSN dat verwerkt wordt.

Dit alles brengt met zich dat de zorgaanbieder bij online communicatie steeds het juiste BSN zal moeten verwerken bij de gegevens van een patient en maatregelen zal moeten garanderen om dat te doen, zowel bij elektronisch toepassingen die hij aanbiedt als waarvan hij gebruik wenst te maken voor verwerken van patientgegevens.

Aan het verwerken van het BSN door de zorgaanbieder zijn hoge beveiligingseisen gesteld via de NEN 7510 en de NEN 7512. Het voldoen aan deze normen is expliciet vastgelegd in artikel 2 Regeling gebruik BSN in de zorg.

Op grond van het regime voor het verwerken van gezondheidsgegevens in de Wbp en de aanstaande Algemene Verordening Gegevensbescherming, het medisch beroepsgeheim, de ISO- en NEN-normen met de patiënt authenticatie-vereisten alsmede de Wet BSN in de zorg, is in beginsel een hoog betrouwbaarheidsniveau noodzakelijk.

### §5.6 Verschil tussen muteren en inzien

In de vraagstelling wordt onderscheid gemaakt tussen het elektronisch inzien van medische gegevens en het elektronisch muteren van medische gegevens door de patiënt. Dit aspect wordt meegenomen in de beoordeling. Dit onderscheid is niet van invloed op de hierboven beschreven belangrijke aspecten, zoals het verwerken van gezondheidsgegevens, het verwerken van het BSN en/of het verwerken van gegevens waarop het medisch beroepsgeheim van toepassing is. Niettemin is het mogelijk dat het risico van de verwerking anders is bij inzien of muteren.

De integriteit van de gegevens is in dat laatste geval bijvoorbeeld makkelijker te beïnvloeden en ook de beschikbaarheid van gegevens- beide belangrijke aspecten bij beveiliging van gegevens- is in dat geval aan te tasten. Het is mogelijk om te stellen dat inzage doorgaans omgeven is door minder risico's dan muteren. Dit is echter niet altijd het geval. Bij inzage is bijvoorbeeld het risico van verlies en onrechtmatig hergebruik een belangrijk risicoaspect.

### §5.7 Enkele criteria Forum Standaardisatie

Voor wat betreft muteren van gegevens maakt het forum onderscheid tussen het muteren van gegevens uit basisregistraties en andere gegevens. Bij muteren van basisregistraties is niveau 4 STORK vereist. In onderhavig onderzoek is daarvan geen sprake, maar er is wel een parallel te trekken in risico. Wanneer een onbevoegde (zorg)inhoudelijke patientgegevens kan aanvullen of wijzigen als ware hij de patiënt, dan kan dit ernstig nadeel berokkenen aan de gezondheid van de patiënt wanneer op basis van de informatie gehandeld of geoordeeld

wordt door de zorgaanbieder. Denk bijvoorbeeld aan het aanvullen van medicatie of doseringsinformatie of het muteren van allergie informatie.

Het kunnen wijzigen van deze informatie in het domein (onder verantwoordelijkheid) van de zorgaanbieder of in communicatie met de zorgaanbieder via een door hem beschikbaar gestelde methode dient volgens ons dan ook op het hoogste betrouwbaarheidsniveau te gebeuren. Dit zou anders zijn wanneer de patiënt zelfbeheerde medische gegevens met de zorgaanbieder wenst te delen. In dat geval ligt de verantwoordelijkheid voor de juistheid daarvan bij de patient of de door hem ingeschakelde (commerciële) partij.

Daarnaast gaat het forum ervan uit dat als het publiek belang of het economisch belang hoog is, sprake is van niveau 4 STORK.

Bij het tonen van medische persoonsgegevens waarop het beroepsgeheim van toepassing is en het verwerken van het BSN door de zorgaanbieder moet op basis van de criteria door het forum onderscheiden, uitgegaan worden van niveau 4 van STORK.

## §5.8 De usecases

### A. Een patiënt controleert zijn inschrijvingsgegevens bij een zorgaanbieder (NAW gegevens die geen betrekking hebben op zijn gezondheid).

We onderscheiden twee scenario's vanwege de vraagstelling:
1) Inschrijfgegevens die - ook in combinatie met de gegevens van de zorgaanbieder - niets zeggen over de gezondheidssituatie van de patiënt en waarbij ook geen inzage is in het BSN.
2) Inschrijfgegevens inclusief het BSN en inzicht in het specialisme van de zorgaanbieder.
Risico-analyse: Volgens de Autoriteit Persoonsgegevens (AP) is in beide situaties sprake van een hoog risico, omdat afspraakgegevens onder het medisch beroepsgeheim vallen.
In scenario 1 is het, althans theoretisch, mogelijk dat er ook indirect geen inlichtingen worden gegevens over de gezondheidstand van de patient en ook niet over het BSN. Betoogd kan worden dat het dan geen gezondheidsgegevens zijn en er geen inzage is in het BSN. Evenwel vallen de gegevens altijd onder het medisch beroepsgeheim en dus geldt een hoog betrouwbaarheidsniveau volgens de AP in de Flevo-zaak en het hoogste niveau als we de richtsnoeren letterlijk nemen.[43] We denken verder dat gelet op het iets geringere risico in de eerste situatie het aannemelijk is dat een hoog betrouwbaarheidsniveau vereist is, mogelijk niet perse het hoogste. We gaan ervan uit dat betrouwbaarheid op op niveau STORK 3 en eIDAS substanieel als passend zal worden beschouwd. In situatie 2 is er aanvullend sprake van gegevens betreffende de gezondheid zoals de wetgever het bedoeld en gegevens over het persoonsnummer BSN. In dat geval is duidelijker sprake van een gegevensverwerking waarvoor AP het hoogste betrouwbaarheidsniveau van belang acht. Dit is in overeenstemming met de criteria die het forum onderscheidt. Voor het verwerken van gegevens met het BSN geldt ook wettelijk in elk geval een hoog betrouwbaarheidsniveau.
Conclusie: In scenario 1 wordt naar verwachting minimaal betrouwbaarheidsniveau substantieel eIDAS (en STORK 3) en in scenario 2 niveau hoog eIDAS (en STORK 4) passend geacht.

[43] Opgemerkt dient te worden dat de uitspraak in de Flevo-zaak plaats vond in 2005 en dat inmiddels de stand van de techniek is veranderd. De Richtsnoeren zijn echter van recente datum (2013).

**B. Een patiënt wijzigt zijn inschrijvingsgegevens bij een zorgaanbieder (NAW gegevens die geen betrekking hebben op zijn gezondheid).**

Risico-analyse: ook hier zijn twee scenario's mogelijk: 1. De gegevens over de afspraak en de zorgverlener geven geen inzicht in de gezondheidstoestand van de patient en diens BSN; 2. De gegevens over de afspraak geven wel inzicht in de gezondheidstoestand van de patiënt en diens BSN.

Volgens de AP is in beide situaties het medisch beroepsgeheim van toepassing en is in het eerste scenario geen sprake van gezondheidsgegevens en een persoonsnummer en in het tweede scenario wel.

Op basis hiervan is het risico scenario hetzelfde als hierboven in casus A, met dezelfde overwegingen. Het wijzigen van gegevens is echter omkleed met iets meer risico.

Risico-analyse: Wijzigen van gegevens door een eventuele onbevoegde die zich voor de patiënt uitgeeft geeft meer risico's dan alleen het inzien van de inschrijfgegevens (casus A). Door het wijzigen van inschrijfgegevens door onbevoegden kan persoonsverwisseling ontstaan bij de uitvoering van zorg. Dit zou echter ook door extra maatregelen voorkomen kunnen worden. De inrichting is derhalve van belang voor inschaling.

Conclusie: Afhankelijk van het soort te wijzigen gegevens en de koppeling daarvan aan het zorgdossier verwachten we net als bij usecase A dat in scenario 1 minimaal niveau substantieel eIDAS (en STORK 3) en in scenario 2 niveau hoog eIDAS (en STORK 4) passend wordt geacht.

**C. Een patiënt maakt/wijzigt een afspraak met de zorgverlener (bijvoorbeeld voor het spreekuur of een onderzoek).**

Risico-analyse: dit is een combinatie van usecase A en B, waarbij er in de praktijk doorgaans ook gezondheidsgegevens verwerkt zullen worden. Dit zou anders kunnen zijn wanneer het bijvoorbeeld uitsluitend gaat om een afspraak bij de huisarts, zonder dat bekend is waarvoor de afspraak gemaakt wordt of het type afspraak. In dat geval is wel sprake van gegevens die onder het beroepsgeheim vallen. In de overige situaties vervalt het onderscheid tussen wel medisch beroepsgeheim, maar geen gezondheidsgegevens, zoals dat bij casus A en B is beschreven.

Conclusie: In een situatie vergelijkbaar met het scenario onder A.1 zal niveau substantieel eIDAS (en STORK 3) passend zijn en in een situatie vergelijkbaar met scenario A.2 is naar verwachting betrouwbaarheidsniveau hoog (eIDAS en STORK 4) passend, afhankelijk van de soort te wijzigen gegevens.

**D. Een patiënt raadpleegt zijn medisch dossier bij de hulpverlener (bijvoorbeeld zijn huisartsdossier, laboratoriumuitslagen, beeldverslagen of medicatie).**

In deze casus is het (gehele) medisch dossier zichtbaar en is er dus geen twijfel over de vraag of er sprake is van gezondheidsgegevens, inzage in het BSN en toepasselijkheid van het medisch beroepsgeheim.

Conclusie: Betrouwbaarheidsniveau hoog eIDAS / STORK 4 wordt passend geacht.

**E. Een patiënt maakt aanvullingen op zijn medisch dossier (bijvoorbeeld door het toevoegen van resultaten van zelfmetingen van parameters zoals bloedsuikerspiegel, bloeddruk, gewicht).**

Het muteren van het medisch dossier brengt over het algemeen meer risico's met zich mee dan alleen inzage. Onder andere vanwege de denkbare gevolgen voor het gebruik van de gemuteerde gegevens voor de zorgverlening.
Conclusie: In deze gevallen wordt betrouwbaarheidsniveau hoog eIDAS / STORK 4 passend geacht.

**F. Een patiënt vraagt een herhaalrecept aan**

De manier waarop de mogelijkheid wordt geboden maakt verschil in of de verwerking bij de zorgaanbieder begint of bij de patiënt. Het gaat om het verwerken van een beperkte hoeveelheid gezondheidsgegevens.
Er is geen twijfel over de vraag of er sprake is van het verwerken van gezondheidsgegevens, verwerken/inzien van het BSN en toepasselijkheid van het medisch beroepsgeheim op de gegevens die verwerkt worden.
Conclusie: Betrouwbaarheidsniveau hoog eIDAS / STORK 4 wordt passend beschouwd.

## §5.9 De betekenis van de betrouwbaarheidsniveau's

Dit onderzoek gaat zoals hierboven duidelijk is gebleken niet om de vraag welke eisen of criteria bij welk betrouwbaarheidsniveau passen. In dit onderzoek gaat het erom zoveel mogelijk helder te maken welk betrouwbaarheidsniveau in voorgelegde toepassingen noodzakelijk is voor patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg. Het gaat er derhalve om welk betrouwbaarheidsniveau kwalificeert als 'passend' in de zin van de Wet bescherming persoonsgegevens (Wbp).

In het onderzoek kan alleen uitspraak worden gedaan over het geldende wettelijke kader en de gangbare standaarden en normen. Zoals gesteld is de invulling van de betrouwbaarheidsniveau's van eIDAS nog in ontwikkeling. De concrete praktische invulling van betrouwbaarheidsniveau's, zoals nu o.a. in de STORK niveau's, zal in de toekomst waarschijnlijk een andere betekenis en waarde krijgen. De eIDAS normering moet geschikt zijn voor brede Europese toepassing en mogelijkheden laten voor een technologie neutrale invulling. Hoe dit in de praktijk uiteindelijk precies vorm zal krijgen is nog niet te zeggen. De minimale vereiste procedures en specificaties zijn vastgelegd in de uitvoeringsverordening van eIDAS. Wat wel duidelijk is en ook uit diverse pilots blijkt is dat de invulling van maatregelen en mogelijkheden van beveiliging zo sterk in ontwikkeling zijn, dat al te statische criteria en voorwaarden weinig toekomstbestendig lijken te zijn. Deze doen bovendien weinig recht aan de kansen voor ontwikkeling van verschillende methoden voor sterke toegangbeveiliging. Gebleken is in het onderzoek dat adequate toegangsbeveiliging zich ook meer tevens kan gaan uitstrekken tot een continue monitoring van activiteit op doorlopende processen, meer dan alleen een proces aan de voorkant (bij het aanmelden) van een toepassing.

In concreto hebben de banken die bezig zijn met de ontwikkeling van iDIN aangegeven dat hun *authenticatieproces* veiliger is geworden door maatregelen die volgen op de aanvankelijke authenticatie (en de stappen die daartoe geleid hebben) en die vervolgens continue plaatsvinden op het gebied van toegangsfraudedetectie en -beheersing, het

monitoring van gebruik van toegangsmiddelen en de controle op gebruik van de toepassing. Door slimme invulling kan een 'misser' op authenticatieniveau direct gesignaleerd en verstoord worden, voorafgaand aan enige activiteit maar ook na verloop van tijd. Op deze manier kan de veiligheid van het toegangsproces verhoogd worden.[44]

Wat wij ermee willen zeggen is dat het een voorwaarde voor succes is om met een open mind te kijken naar de kansen en ontwikkelingen voor inrichting van betrouwbaarheid in toegang. Voor de toekomst zullen te concrete invullingen van eisen aan betrouwbaarheidsniveau's een beperking voor beveiliging vormen. Tegelijkertijd blijft het voor uniforme interpretatie en interoperabiliteit, toetsing en toezicht noodzakelijk om kaders voor invulling te stellen. Daartoe is in elk geval de Uitvoeringsverordening zeer belangrijk, alsmede de (verder te ontwikkelen) normen en standaarden. Er zal een balans gevonden moeten worden in toetsbaarheid enerzijds en aantoonbaarheid en accountability anderzijds. Dat betekent mogelijk bijvoorbeeld ook dat gebleken veiligheid kan meewegen in een beoordeling van het veiligheidsniveau.

Tot slot willen we, in dit verband, benadrukken dat de criteria die nu gelden voor betrouwbaarheidsniveau STORK 3 en STORK 4 als zodanig in de toekomst niet (allemaal) vereist zijn in de niveau's substantieel respectievelijk hoog van eIDAS.[45] Zo is het ook mogelijk dat een middel dat nu ontwikkeld wordt en niet het niveau van STORK 4 behaalt, wel als eIDAS hoog zou kunnen kwalificeren met een juiste combinatie van maatregelen.

[44] Dit lijkt overigens aan te sluiten op de kaders die de Uitvoeringsverordening ten aanzien van de verschillende niveau's stelt.
[45] De minimale eisen die gelden per betrouwbaarheidsniveau volgen uit de Uitvoeringsverordening (EU) 2015/1502 bij de eIDAS Verordening.

## H.6 Conclusies en aanbevelingen

Op grond van het normatieve kader en in de uitwerking van de usecases wordt in bepaalde gevallen niveau substantieel eIDAS (en STORK 3) en in bepaalde gevallen niveau hoog eIDAS (en STORK 4) passend geacht voor patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg zoals in de usecases beschreven. Dit is onze verwachting naar aanleiding van de bevindingen in het onderzoek. Passende authenticatie dient altijd te worden afgestemd op de specifieke voorgenomen verwerking en de daaraan verbonden (bijzondere) risico's. Het gaat om 'passend' in de zin van de Wet bescherming persoonsgegevens en de aankomende Algemene Verordening Gegevensbescherming. Uit uitspraken en richtsnoeren van de Autoriteit Persoonsgegevens volgt dat bij patiënt-authenticatie in communicatie met en onder verantwoordelijkheid van de zorgaanbieder in beginsel uitgegaan dient te worden van een 'hoog betrouwbaarheids niveau'. In bepaalde gevallen, namelijk als het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust, geeft de AP aan dat het 'hoogste' betrouwbaarheidsniveau verlangd wordt.

Het onderzoek is gericht op de casus die door VWS zijn voorgelegd. Zoals in het voorgaande ook tot uitdrukking is gekomen is toegang tot medische gegevens die niet onder verantwoordelijkheid van een arts of hulpverlener worden verwerkt (bijvoorbeeld in het zelf gestarte PGD van de patiënt) niet meegenomen in het onderzoek. Het criterium dat het 'medisch beroepsgeheim' op de gegevens rust, speelt in dat geval doorgaans geen rol.

Patiëntauthenticatie op betrouwbaarheidsniveau STORK niveau 4 is voor de patiënt op dit moment (nog) niet breed beschikbaar. Dat zal naar alle waarschijnlijkheid ook gezegd kunnen worden van niveau hoog eIDAS, aangezien dit het hoogste niveau van authenticatie betreft en gelet op de minimale eisen die daaraan worden gesteld in de uitvoeringsverordening (EU) 2015/1502.

Op dit moment worden er al pilots gedaan, onder andere in de zorg, waarbij waarschijnlijk niveau STORK 3/ substantieel wordt behaald. Daarbij worden in enkele pilots (iDIN) de mogelijkheden om het hoogste betrouwbaarheidsniveau te bereiken onderzocht. Ook zullen er een aantal pilots op niveau hoog gaan starten, waaronder in de zorg.

Het is aan te bevelen dat de overheid zo spoedig mogelijk het initiatief neemt om authenticatiemiddelen op niveau hoog breed beschikbaar te krijgen, publiek en/of privaat.

**Geraadpleegde documentatie**

Afsprakenstelsel Elektronische Toegangsdiensten - https://afsprakenstelsel.etoegang.nl/display/as/Startpagina

CBP, Flevo-zaak (z2005-1372)

CBP Richtsnoeren, beveiliging van persoonsgegevens, februari, 2013.

CBP, Toegang tot digitale patiëntendossiers binnen zorginstellingen, juni 2013.

https://www.eherkenning.nl/aansluiten-op-eherkenning/betrouwbaarheidsniveaus/bepalen-van-juiste-niveau/voorbeelden-van-diensten/

https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/12/14/rapport-start-van-de-pilots/rapport-start-van-de-pilots.pdf.

ISO 17090-2:2008, Medische informatica – Public Key Infrastructure (PKI) – Deel 2: Profiel van certificaat

ISO 17090-3:2008, Medische informatica – Public Key infrastructure (PKI) – Deel 3: Beleidsmanagement van certificeringinstelling

ISO 29115: 2013

Jacobs, B, Nouwt, S, de Bruijn, A, Vermeulen, O., van der Knaap, R., de Bie, C: Beveiligingseisen ten aanzien van identificatie en authenticatie voor toegang tot het EPD; PriceWaterhouseCoopers, Universiteit van Tilburg, Radboud Universiteit Nijmegen, 2 december 2008.

Forum Standaardisatie, Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten (versie 3), september 2014

Memorie van Toelichting Wbp, Tweede Kamer 1997-1998, 25892, nr. 3.

NCSC. Beveiligingsrichtlijnen voor webapplicaties, augustus 2015, https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

NEN-ISO 17090-1:2013, Medische informatica – PKI (Public Key Infrastructure) – Deel 1: Overzicht van digitale certificeringsdiensten

NEN 7510: 2011

NEN 7512: 2015 Medische informatica – Informatiebeveiliging in de zorg – Vertrouwensbasis

Ontwerp NTA 7521:2015 nl Medische Informatica – Toegang tot patientgegevens – Grondslagen voor uitwisseling

PBLQ, Internationale vergelijking eID-middelen, 2015

STORK Secure idenTities acrOss boRders linKed. Zie document D2.3 – Quality authenticator scheme, paragraaf 2.3 en 2.4., te vinden op www.eid-stork.eu, onder STORK materials, deliverables approved/public.

Tweede Kamer, Vergaderjaar 1997-1998, 25 892, nr. 3, p.99
Tweede Kamer, Vergaderjaar 1999-2000, 25 892, nr 92c, p.15
Tweede Kamer. Vergaderjaar 2005-2006, 30 380, nr. 3.
Tweede Kamer, 26643-379, Vervolgbrief pilots eID van 15 december 2015

Uitvoeringsverordening (EU) 2015/1502 van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen.

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 (PbEU 2014, L 257)

Voorstel, algemene verordening gegevensbescherming, politiek akkoord, Brussel 28 januari 2016, 5455/16, Voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Wet bescherming persoonsgegevens

Wet gebruik burgerservicenummer in de zorg.

Wet inzake de geneeskundige behandelingsovereenkomst, boek 7 BW, artikel 446 en volgende

**Bijlage A: 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**
**(Voor de EER relevante tekst)**

DE EUROPESE COMMISSIE,
Gezien het Verdrag betreffende de werking van de Europese Unie,
Gezien 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 ([1]), en met name artikel 8, lid 3,
Overwegende hetgeen volgt:

(1) In artikel 8 van Verordening (EU) nr. 910/2014 wordt bepaald dat een stelsel voor elektronische identificatie dat is aangemeld krachtens artikel 9, lid 1, de betrouwbaarheidsniveaus laag, substantieel en hoog omschrijft voor op grond van dat stelsel uitgegeven elektronische identificatiemiddelen.

(2) De minimale technische specificaties, normen en procedures dienen te worden vastgesteld om een uniforme interpretatie te waarborgen van de details van de betrouwbaarheidsniveaus en de interoperabiliteit te verzekeren wanneer de nationale betrouwbaarheidsniveaus van aangemelde stelsels voor elektronische identificatie worden gerelateerd aan de betrouwbaarheidsniveaus volgens artikel 8, zoals bepaald in artikel 12, lid 4, onder b), van Verordening (EU) nr. 910/2014.

(3) Voor het vaststellen van de specificaties en procedures die in deze uitvoeringshandeling zijn opgenomen, is rekening gehouden met de internationale norm ISO/IEC 29115, de belangrijkste internationale norm op het gebied van betrouwbaarheidsniveaus voor elektronische identificatiemiddelen. Verordening (EU) nr. 910/2014 verschilt echter inhoudelijk van die internationale norm, met name wat betreft de vereisten voor het bewijs en de verificatie van de identiteit, alsmede wat betreft de wijze waarop de verschillen tussen de identiteitsregelingen van de lidstaten en de bestaande EU-instrumenten op dat gebied in aanmerking worden genomen. In de bijlage, die weliswaar op deze internationale norm is gestoeld, dient derhalve niet te worden verwezen naar enige specifieke inhoud van ISO/IEC 29115.

(4) Deze verordening is tot stand gekomen volgens een resultaatgestuurde aanpak, omdat die het meest geschikt is; hetzelfde geldt voor de definities van termen en begrippen. Daarbij is rekening gehouden met de doelstelling van Verordening (EU) nr. 910/2014 met betrekking tot de betrouwbaarheidsniveaus voor elektronische identificatiemiddelen. Bij het vaststellen van de specificaties en procedures in deze uitvoeringshandeling moet daarom terdege rekening worden gehouden met het grootschalige proefproject STORK, inclusief de in dat verband ontwikkelde specificaties, alsmede de definities en begrippen in ISO/IEC 29115.

(5)Afhankelijk van de context waarin verificatie van een aspect van het bewijs van de identiteit moet plaatsvinden, kunnen gezaghebbende bronnen in allerlei vormen voorkomen, zoals registers, documenten, instanties en dergelijke. In de verschillende lidstaten kunnen, zelfs in vergelijkbare contexten, verschillende gezaghebbende bronnen bestaan.

(6)De vereisten voor het bewijs en de verificatie van de identiteit dienen verschillende systemen en praktijken in aanmerking te nemen, waarbij een voldoende hoog betrouwbaarheidsniveau moet worden gewaarborgd om het noodzakelijke vertrouwen tot stand te brengen. Procedures die eerder werden gebruikt voor andere doeleinden dan de afgifte van elektronische identificatiemiddelen, mogen dan ook slechts worden aanvaard indien is bevestigd dat die procedures voldoen aan de eisen die voor het overeenkomstige betrouwbaarheidsniveau zijn vastgesteld.

(7)Er wordt doorgaans gebruikgemaakt van authenticatiefactoren zoals gedeelde geheime sleutels, fysieke hulpmiddelen en fysieke attributen. Om het authenticatieproces beter te beveiligen, is het echter aan te bevelen om een groter aantal authenticatiefactoren te gebruiken, en dan met name authenticatiefactoren die tot verschillende categorieën behoren.

[…]

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

*Artikel 1*

1. Voor elektronische identificatiemiddelen die op grond van een aangemeld stelsel voor elektronische identificatie zijn uitgegeven, worden de betrouwbaarheidsniveaus laag, substantieel en hoog bepaald onder verwijzing naar de specificaties en procedures in de bijlage.

2. De specificaties en procedures in de bijlage worden gebruikt voor het bepalen van het betrouwbaarheidsniveau voor elektronische identificatiemiddelen die op grond van een aangemeld stelsel voor elektronische identificatie zijn uitgegeven, door de betrouwbaarheid en de kwaliteit te bepalen van de volgende elementen:

a)inschrijving, zoals bedoeld in punt 2.1 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder a), van Verordening (EU) nr. 910/2014;

b)beheer van elektronische identificatiemiddelen, zoals bedoeld in punt 2.2 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder b) en f), van Verordening (EU) nr. 910/2014;

c)authenticatie, zoals bedoeld in punt 2.3 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder c), van Verordening (EU) nr. 910/2014;

d)beheer en organisatie, zoals bedoeld in punt 2.4 van de bijlage bij deze verordening overeenkomstig artikel 8, lid 3, onder d) en e), van Verordening (EU) nr. 910/2014.

3. Indien het elektronische identificatiemiddel dat op grond van een aangemeld stelsel voor elektronische identificatie is uitgegeven, voldoet aan een vereiste dat voor een hoger

betrouwbaarheidsniveau is vermeld, wordt het geacht ook te voldoen aan het overeenkomstige vereiste voor een lager betrouwbaarheidsniveau.
4. Tenzij in het desbetreffende deel van de bijlage anders is aangegeven, kan een elektronisch identificatiemiddel dat op grond van een aangemeld stelsel voor elektronische identificatie is uitgegeven, slechts aan het opgegeven betrouwbaarheidsniveau voldoen indien is voldaan aan alle elementen die in de bijlage voor dat betrouwbaarheidsniveau zijn vermeld.

*Artikel 2*

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 8 september 2015.

*Voor de Commissie*

*De voorzitter*

Jean-Claude JUNCKER

---

([1]) PB L 257 van 28.8.2014, blz. 73.

---

**BIJLAGE**

**Technische specificaties en procedures voor de betrouwbaarheidsniveaus laag, substantieel en hoog betreffende op grond van een aangemeld stelsel voor elektronische identificatie uitgegeven elektronische identificatiemiddelen**

**1. Definities**

Voor de toepassing van deze bijlage wordt verstaan onder:

1. **„gezaghebbende bron”**: elke bron, ongeacht de vorm ervan, waarvan kan worden verwacht dat deze nauwkeurige gegevens, informatie of bewijsmateriaal biedt op basis waarvan een identiteit kan worden aangetoond;
2. **„authenticatiefactor”**: een factor waarvan is bevestigd dat deze gebonden is aan een persoon en die onder een van de volgende categorieën valt:

a) **„op bezit gebaseerde authenticatiefactor”**: een authenticatiefactor waarvan de betrokkene moet aantonen dat deze in zijn bezit is;

b) **„op kennis gebaseerde authenticatiefactor”**: een authenticatiefactor waarvan de betrokkene moet aantonen dat hij ervan kennis draagt;

c) **„inherente authenticatiefactor”**: een authenticatiefactor die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit;

3. **„dynamische authenticatie”**: een elektronisch proces, dat met gebruikmaking van cryptografie of een andere techniek de middelen biedt om op verzoek een elektronisch bewijs op te maken dat de betrokkene de controle heeft over of in het bezit is van de identificatiegegevens, en dat verandert telkens als authenticatie plaatsvindt tussen de betrokkene en het systeem dat diens identiteit verifieert;
4. **„beheerssysteem voor informatiebeveiliging”**: een geheel van processen en procedures die zijn ontworpen om de informatieveiligheidsrisico's tot een aanvaardbaar niveau te beperken.

**2. Technische specificaties en procedures**

Aan de hand van de in deze bijlage beschreven elementen van de technische specificaties en procedures wordt bepaald op welke wijze de vereisten en criteria van artikel 8 van Verordening (EU) nr. 910/2014 worden toegepast op elektronische identificatiemiddelen die zijn uitgegeven op grond van een stelsel voor elektronische identificatie.

**[…]**

**2.1.2. Bewijs en verificatie van identiteit (natuurlijke persoon)**

| **Betrouwbaarheidsniveau** | **Vereiste elementen** |
|---|---|
| Laag | 1. De persoon kan worden verondersteld in het bezit te zijn van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt.<br><br>2. Het bewijs kan worden verondersteld echt te zijn, dan wel volgens een gezaghebbende bron te bestaan, en het bewijs lijkt geldig te zijn.<br><br>3. Een gezaghebbende bron weet dat de opgegeven identiteit bestaat en er kan worden verondersteld dat de persoon die de identiteit opgeeft, dezelfde persoon is. |
| Substantieel | Niveau laag plus een van de onder de punten 1 tot en met 4 vermelde alternatieven.<br>1. Er is geverifieerd dat de persoon in het bezit is van bewijs dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt;<br>en<br>het bewijs is gecontroleerd op de echtheid ervan; of het bestaan ervan is volgens een gezaghebbende bron bekend en het heeft betrekking op een werkelijk bestaande persoon;<br>en<br>er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat het bewijsstuk verloren, gestolen, geschorst, ingetrokken of verlopen is.<br>Of<br><br>2. Er is een identiteitsdocument overgelegd tijdens een registratieproces in de lidstaat waar het document is afgegeven, en het document lijkt betrekking te hebben op de persoon die het heeft overgelegd;<br>en<br>er zijn maatregelen getroffen om het risico te minimaliseren dat de identiteit van de persoon niet met de opgegeven identiteit overeenstemt, rekening houdend met bijvoorbeeld het risico dat |

| | |
|---|---|
| | documenten verloren, gestolen, geschorst, ingetrokken of verlopen zijn.<br>Of<br><br>3.Indien procedures die eerder door een publieke of private entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau substantieel, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad ([1]) of een daaraan gelijkwaardige instantie.<br>Of<br><br>4.Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau substantieel of hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau substantieel of hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie. |
| Hoog | Er moet zijn voldaan aan de vereisten van punt 1 of punt 2.<br>1.Niveau substantieel plus een van de onder a) tot en met c) vermelde alternatieven.<br>a)Indien is geverifieerd dat de persoon in het bezit is van een bewijs dat voorzien is van een foto of biometrische gegevens, dat wordt erkend door de lidstaat waar de aanvraag voor het elektronische identificatiemiddel wordt gedaan, en dat de opgegeven identiteit vertegenwoordigt, wordt het bewijs gecontroleerd op geldigheid aan de hand van een gezaghebbende bron;<br>en<br>de door de aanvrager opgegeven identiteit wordt geverifieerd door vergelijking van één of meer fysieke kenmerken van de persoon met een gezaghebbende bron.<br>Of<br><br>b)Indien procedures die eerder door een publieke of private |

| | |
|---|---|
| | entiteit in dezelfde lidstaat voor een ander doel dan de uitgifte van elektronische identificatiemiddelen zijn gebruikt, voorzien in betrouwbaarheidscriteria die gelijkwaardig zijn aan die van punt 2.1.2 voor het betrouwbaarheidsniveau hoog, dan hoeft de voor de registratie verantwoordelijke entiteit die eerdere procedures niet opnieuw uit te voeren, mits de gelijkwaardigheid van de betrouwbaarheidscriteria is bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie;<br>en<br>er zijn maatregelen getroffen om aan te tonen dat de resultaten van de eerdere procedures nog steeds geldig zijn.<br>Of<br><br>c)Indien elektronische identificatiemiddelen worden uitgegeven op basis van een aangemeld geldig elektronisch identificatiemiddel met betrouwbaarheidsniveau hoog, is het, rekening houdend met het risico van een wijziging van de persoonsidentificatiegegevens, niet nodig om het proces van bewijs en verificatie van de identiteit opnieuw uit te voeren. Is het als basis dienende elektronische identificatiemiddel niet aangemeld, dan moet het betrouwbaarheidsniveau hoog worden bevestigd door een conformiteitsbeoordelingsinstantie als bedoeld in artikel 2, punt 13, van Verordening (EG) nr. 765/2008 of een daaraan gelijkwaardige instantie.<br>en<br>er zijn maatregelen getroffen om aan te tonen dat de resultaten van deze eerdere uitgifteprocedure van een aangemeld elektronisch identificatiemiddel nog steeds geldig zijn.<br>OF<br><br>2.Indien de aanvrager geen erkend identiteitsdocument met een foto of biometrische kenmerken overlegt, worden dezelfde procedures toegepast die op nationaal niveau van toepassing zijn in de lidstaat van de verantwoordelijke instantie voor de verkrijging van een dergelijk bewijsstuk met foto of biometrische kenmerken. |

[..]