“Het nieuwe eID-stelsel; een introductie voor de zorgsector ”

Betere gezondheid
door betere informatie

Nictiz

Datum
22 Mei 2017

Auteurs
Merik Seven
Melissa Obermann-Gasseling
Piet Hein Minnecré

Toelichting

In deze whitepaper over eID in de zorg wordt het nieuwe eID-stelsel voor de gezondheidssector geïntroduceerd. De komende jaren wordt gewerkt aan een brede implementatie van nieuwe eID voorzieningen ten behoeve van de elektronische toegangscontrole van de patiënt, professional en/of mantelzorger. In dit document wordt onder andere geschetst hoe het nieuwe eID-stelsel werkt, wat het betekent voor de patiënt en zorgverlener, hoe het implementatietraject en de – termijn eruit gaan zien en wat nog de belangrijkste aandachtspunten zijn. De komende jaren zal de online dienstverlening in de zorg verder toenemen. Dit stelt hogere eisen aan de betrouwbaarheid van het digitale legitimatieproces. Met dit document hopen we tegemoet te komen aan de behoefte aan meer informatie en duidelijkheid over eID in de zorg zodat de organisaties en professionals zich hierop op tijd kunnen gaan voorbereiden.

Inhoud

1. Inleiding

In dit rapport schetsen we een eerste beeld van wat de komst van het nieuwe eID-stelsel betekent voor de zorg. Daarbij kijken we specifiek naar wat deze nieuwe manier van identificatie en authenticatie zal betekenen voor de patiënt en zorgverlener. Dat doen we onder meer op basis van de ervaringen die zijn opgedaan in een aantal eID-pilots die onder leiding van Nictiz in 2016 in de zorg zijn uitgevoerd.

We beseffen ons dat het beeld (nog) niet compleet is. Deels is het nieuwe eID-stelsel nog in ontwikkeling. Zo wordt nog gewerkt aan de Wet Generieke Digitale Infrastructuur (Wet GDI) waarin de nieuwe digitale inlogmethodes worden beschreven. Maar ook de exacte werking van de middelen, de benodigde koppelvlakken tussen partijen, de inrichting van het toezicht, de financiering van het geheel, zijn nog onderwerp van verdere uitwerking. Totdat het nieuwe eID-stelsel breed (naar verwachting begin 2019) beschikbaar komt zal de zorgsector fungeren als 'voorloper' en kwartiermaker.

Dit stuk moet dan ook vooral gelezen worden als een eerste kennismaking met de nieuwe vorm van elektronische identificatie. Een nieuwe ontwikkeling die snel op de zorgsector af komt, die grote voordelen kan bieden voor de zorg, maar die ook de nodige aandacht vergt om een succesvolle implementatie en uitrol te bewerkstelligen.

2. Voor wie is dit rapport bedoeld?

Dit rapport is geschreven met de informatiemanager in de zorg in het achterhoofd. Tegelijkertijd is het voor een bredere doelgroep interessant. In hoofdstuk drie schetsen we de ontwikkelingen op het gebied van onlinedienstverlening en hoe deze betrouwbare identificatie en authenticatie steeds noodzakelijker maken. In hoofdstuk vier introduceren we het nieuwe eID-stelsel om vervolgens in hoofdstuk vijf in te gaan op de ervaringen uit de pilots in de zorg. Hoofdstuk zes gaat in op de voordelen en andere gevolgen van het stelsel voor de patiënt en de zorgverlener. Tot slot concluderen we en beschrijven we kort een aantal aandachtspunten voor de succesvolle implementatie van het stelsel in het zorgveld.

3. De zorg vraagt dringend om betrouwbare authenticatie

Een video-afspraak met een arts, een horloge dat de hartslag bijhoudt, digitale portalen waar patiënten hun gezondheidsdossier kunnen raadplegen. Zomaar een aantal voorbeelden van de digitalisering in de zorg. Deze ontwikkelingen stellen stevige eisen aan de veiligheid van gegevens en de privacy van de burger/patiënt.

3.1 Het toenemen van onlinedienstverlening

De komende jaren neemt het aanbod van onlinedienstverlening in de zorg (eHealth) naar verwachting verder toe. Mede door nieuwe wet- en regelgeving krijgen patiënten steeds meer toegang tot en regie over hun eigen medische informatie. En door het gebruik van (gezondheid)apps en medische apparatuur krijgen zorgprofessionals te maken met de groei van digitale medische informatie die door de patiënt zelf wordt gegenereerd en aangeboden, zoals bijvoorbeeld bloeddrukgegevens.

De Rijksoverheid stimuleert de ontwikkeling om meer digitale zorg aan te bieden en heeft onder andere drie concrete doelen voor 2020 gesteld[1]:

- Ten minste 80% van de chronisch zieken heeft direct toegang tot zijn eigen medische gegevens. En ten minste 40% van de overige Nederlanders.
- In 2019 kan 75% van de chronisch zieken en kwetsbare ouderen zelfstandig metingen doen en de resultaten delen met hun zorgverlener. Denk aan metingen van de bloeddruk of het cholesterolgehalte.
- Mensen die thuis zorg en ondersteuning ontvangen, kunnen in 2019 als zij dat willen via een beeldscherm 24 uur per dag met een zorgverlener communiceren.

Om deze doelen te bereiken werken overheid en zorgsector samen in een aantal programma's om de digitalisering in de zorg te versnellen. Voorbeelden zijn het programma MedMij - waarin gewerkt wordt aan een set van afspraken voor digitale persoonlijke gezondheidsomgevingen - en het Versnellingsprogramma Informatie-uitwisseling Patiënt en Professional (VIPP). Daarnaast zijn er ook veel initiatieven in het zorgveld die aan bredere adoptie en implementatie van eHealth werken.

Tegelijkertijd wordt het gebruik van eHealth gestimuleerd door nieuwe wet- en regelgeving. In de Wet cliëntenrechten zorg wordt geregeld dat binnen drie jaar de patiënt zorgverleners specifieke toestemming moet geven voor het elektronisch uitwisselen van zijn dossier. Daarnaast krijgt de patiënt het recht om zijn dossier elektronisch in te kijken of er een afschrift van te ontvangen. Tot slot kunnen patiënten raadplegen wie hun dossier heeft bekeken.

Bovenstaande ontwikkelingen geven de komende jaren een stevige impuls aan het gebruik van onlinedienstverlening in de zorg. Deze trend is overigens breder dan alleen de zorg. In bijna alle sectoren en domeinen neemt het gebruik van onlinedienstverlening toe. Wel typisch voor de zorg is de wijze waarop de patiënt centraal wordt gesteld door hem/haar meer regie over eigen gegevens te geven. Die ontwikkeling is in andere sectoren vaak nog wat onderbelicht.

[1] https://www.rijksoverheid.nl/onderwerpen/e-health/inhoud/overheid-stimuleert-e-health

3.2 Het belang van veiligheid en privacy in de zorg

De opslag en uitwisseling van gegevens brengt altijd risico's met zich mee, zoals het verlies van de gegevens of de onrechtmatige toegang tot die gegevens door derden. In de zorg kan de schade hiervan groter zijn dan in andere sectoren omdat het veelal gaat om de verwerking van zeer persoonlijke en privacygevoelige gegevens. Uit recent onderzoek blijkt bijvoorbeeld dat 33% van de ziekenhuiswebsites onvoldoende is beveiligd[2]. Daarnaast is er de afgelopen jaren een toename van identiteitsfraude zichtbaar[3]. In beide gevallen bestaat het risico dat hierdoor gevoelige gegevens op straat komen te liggen. Deze situatie staat op gespannen voet met wet- en regelgeving. Sinds mei 2016 is de nieuwe algemene verordening gegevensbescherming (AVG)[4] van toepassing. Deze nieuwe Europese privacywetgeving is vanaf 2018 verplicht en biedt een stevige wettelijke bescherming voor het veilig gebruik van onder andere eHealth.

3.3 Het betrouwbaar vaststellen van de identiteit

Betrouwbare authenticatie is een van de belangrijkste schakels in de totale beveiliging en bescherming van de informatievoorziening. Wie digitaal zaken wil doen moet erop kunnen vertrouwen met een bepaalde mate van zekerheid dat diegene met wie hij zakendoet ook daadwerkelijk degene is die hij zegt te zijn. Dat geldt zowel voor de dienstverlener als voor de patiënt.

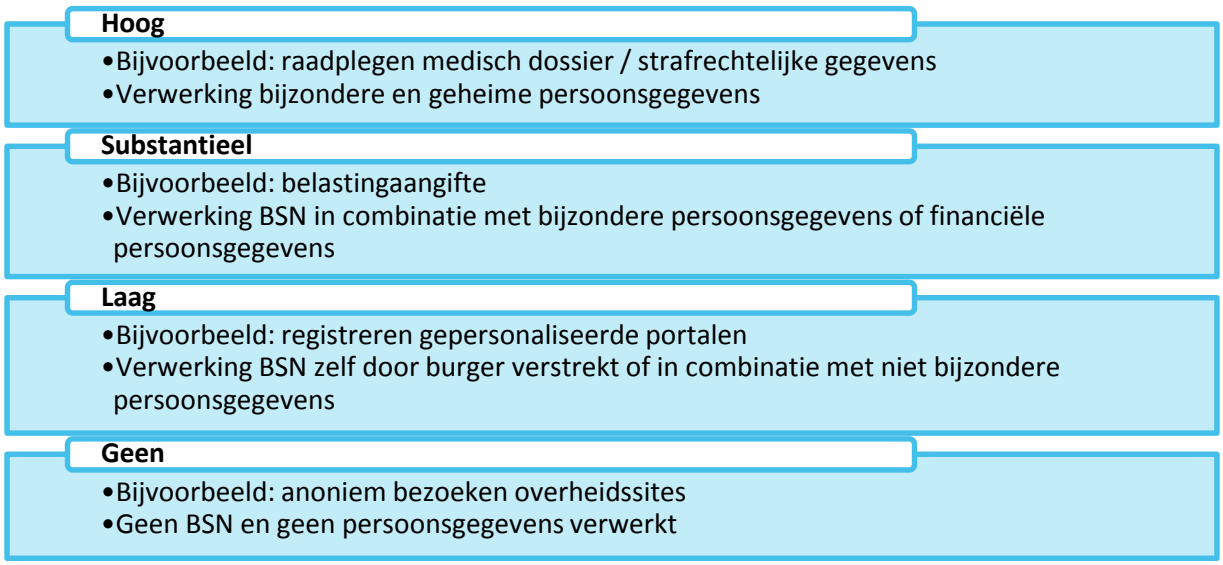
De mate van zekerheid (het zogenaamde betrouwbaarheidsniveau) waarmee de digitale identiteit van een patiënt zou moeten worden vastgesteld hangt sterk af van de aangeboden onlinedienst en het risico op misbruik. Om helderheid te verschaffen ten aanzien van de verschillende niveaus van betrouwbaarheid zijn binnen Europa afspraken gemaakt. In de Europese Verordening elektronische identiteiten en vertrouwensdiensten (eIDAS)[5] wordt onderscheid gemaakt tussen drie niveaus van betrouwbaarheid: 'laag', 'substantieel' en 'hoog'.

Om te bepalen of een dienst voor een bepaald niveau in aanmerking komt, wordt vooral gekeken naar de volgende criteria:

- De aard van de (persoons)gegevens die verwerkt worden.
- De wijze waarop gegevens verwerkt worden.
- De rechtsgevolgen van het gebruik van de digitale dienst.
- Het eventueel wijzigen van basisregistratiegegevens als gevolg van de digitale dienst.
- Het economisch en publieke belang van de digitale dienst.

Het Forum Standaardisatie heeft in november 2016 een nieuwe versie gepubliceerd van de 'Handreiking betrouwbaarheidsniveaus voor digitale dienstverlening'[6]. In figuur 1 Betrouwbaarheidsniveaus staan de verschillende niveaus met enkele voorbeelden van digitale diensten en soort gegevens beschreven.

[2] http://nos.nl/artikel/2151664-ziekenhuizen-beveiligen-hun-sites-niet-goed.html
[3] http://nos.nl/artikel/2144777-toename-identiteitsfraude-is-door-schaamte-topje-van-ijsberg.html
[4] http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&rid=1
[5] http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32014R0910&from=EN
[6] https://www.forumstandaardisatie.nl/sites/bfs/files/atoms/files/Handreiking_Betrouwbaarheidsniveaus_2016.pdf



Figuur 1. Betrouwbaarheidsniveaus

Het verschil in de niveaus zit onder meer in de technische kwaliteit van de inlogmiddelen en de manier waarop ze worden uitgegeven. Het verschil in gebruik tussen de verschillende niveaus is vooral merkbaar op het moment dat de gebruiker meer nodig heeft dan alleen een gebruikersnaam en wachtwoord om in te loggen, bijvoorbeeld een token, pas of telefoon. Er wordt dan gesproken over tweefactor-authenticatie omdat gebruik wordt gemaakt van twee vormen van authenticatie. De gebruiker moet immers zowel het wachtwoord (of de pincode) kennen en moet in het bezit zijn van een token, een pas of een ander fysiek middel. In de praktijk wordt tweefactor-authenticatie op alle betrouwbaarheidsniveaus gebruikt en is er dus beperkt onderscheid in het gebruiksgemak tussen de niveaus. Zo is het gebruik van middelen op het hoogste niveau in de praktijk goed vergelijkbaar met de huidige DigiD met sms-authenticatie, met online bankieren, of met overige tweefactor-authenticatiemethodes[7].

3.4 De zorg stelt hoge eisen aan de betrouwbaarheid

In de zorgsector zijn de huidige inlogmethoden vaak nog gebaseerd op eenvoudige combinaties van gebruikersnaam en wachtwoord die overeenkomen met het betrouwbaarheidsniveau 'laag'[8]. In mei 2016 is door PrivacyCare en PBLQ[9] onderzoek gedaan op basis van een aantal concrete beschrijvingen van voorbeelden van de uitwisseling van gegevens in de zorg tussen patiënten en zorgverleners. Op basis van de uitwerking van die voorbeelden en met toepassing van de Wet Bescherming Persoonsgegevens en overige relevante kaders komen de onderzoekers tot de conclusie dat voor authenticatie minimaal niveau eIDAS 'substantieel' noodzakelijk is. Daar waar het gaat om de uitwisseling van gegevens waarop het medisch beroepsgeheim van de zorgverlener rust is het hoogste betrouwbaarheidsniveau (eIDAS Hoog) nodig. Het digitaal tonen of ophalen van een medisch dossier bij zorgverlener vraagt om de hoogste betrouwbaarheid van de aanvrager/gebruiker. Dit geldt zowel voor de patiënt en mantelzorger (gemachtigde) als voor de zorgprofessional.

[7] Bij Tweefactor identificatie wordt gebruik gemaakt van twee van authenticatiemiddelen. Te denken valt aan het gebruik van een token met een Pincode, of een pincode met een sms bericht. Gebruikers (en dus ook kwaadwillenden) moeten over beide beschikken om zich te kunnen .authentiseren.

[8] Zie onder meer het onderzoek van Nictiz "Patiëntportalen op ziekenhuiswebsites" (juni 2016) waarin gekeken wordt naar het gebruik van authenticatiemiddelen bij portalen in de zorg. https://www.nictiz.nl/publicaties/infographics/patientportalen-ziekenhuiswebsites

[9] Zie het 'Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg', Mei 2016, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2016/12/01/onderzoek-naar-de-beveiliging-van-patientgegevens/onderzoek-naar-de-beveiliging-van-patientgegevens.pdf

4 Een nieuw stelsel voor identificatie en authenticatie

Om het betrouwbaarheidsniveau van online identificatie en authenticatie te verhogen werkt de overheid aan een set van afspraken voor elektronische identificatie en authenticatie (het zogenaamde eID-stelsel) voor het BSN-domein.

4.1 Meerdere aanbieders onder één regime

Het nieuwe eID-stelsel bestaat uit een nieuw wettelijk regime (de Wet GDI) voor digitaal inloggen en betrouwbaar identificeren van burgers/patiënten in het BSN-domein. Onder het stelsel komen meerdere inlogmiddelen beschikbaar. Alle middelen moeten daarbij voldoen aan het nieuwe wettelijk kader en de afspraken die daaronder vallen. Zo wordt getoetst of alle partijen die betrokken zijn bij het authenticatieproces voldoen aan een zogenaamde Uniforme Set van Eisen (de USvE) en wordt gewerkt aan een uitgebreid toezichtregime om de afspraken te borgen.

De nieuwe middelen worden binnen het eID-stelsel verzorgd door verschillende eID-aanbieders. Naast de overheid zelf (DigiD) zal ook de overheid in samenwerking met private partijen nieuwe eID-middelen gaan aanbieden (Idensys). Tevens kunnen de digitale inlogmiddelen van de banken gebruikt worden (iDIN).

Figuur 2. Overzicht eID-stelsel, aanbieders en middelen

Bovenstaande figuur geeft een overzicht van de verschillende middelen die momenteel in aanmerking komen voor erkenning. De burger krijgt met het nieuwe stelsel op termijn dus een breed aanbod aan eID-middelen beschikbaar. De eID-middelen die door de overheid worden aangeboden zijn alleen toepasbaar in het BSN-domein. Zowel iDIN als Idensys zijn ook bruikbaar in het private domein. Daarbij is Idensys onder de naam eHerkenning ook inzetbaar voor eID bij bedrijven.

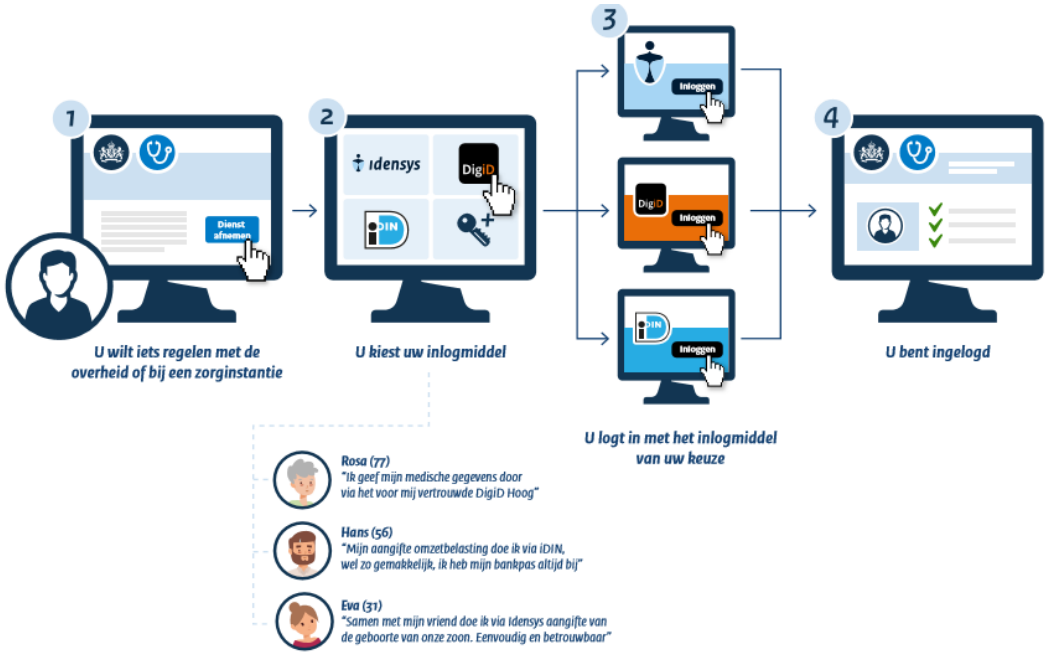
Idensys en DigiD zijn straks waarschijnlijk ook inzetbaar bij overheidsdiensten in andere landen binnen Europa. Dit wordt geregeld in de nieuwe eIDAS wetgeving. Beide eID-aanbieders en middelen zullen dan wel officieel genotificeerd moeten worden via de daarvoor aangewezen procedure door de Europese

Commissie. Tevens kan een Europese burger met een genotificeerd eID-middel uit een ander land toegang krijgen tot publieke onlinedienstverlening binnen Nederland.

Tot slot maakt het stelsel het mogelijk dat in de toekomst nog nieuwe middelen en leveranciers tot het stelsel toetreden.

4.2 Hoe werkt het in de praktijk

Onderstaande figuur geeft kort het proces weer dat de burger of patiënt moet doorlopen om in te loggen bij zijn dienst- of zorgverlener.



Figuur 3. Inlogproces

In de praktijk werkt het gebruik van de middelen op ongeveer dezelfde manier als online bankieren, het gebruik van iDeal, of het huidige DigiD met sms. De gebruiker kiest op de website van de dienstverlener voor inloggen. Hij krijgt de keuze voorgeschoteld welk middel hij daarvoor wil hanteren. Daarna gebruikt hij zijn middel om in te loggen en wordt hij – ingelogd en wel – terugverwezen naar de website van de dienstverlener. Deze procedure is voor het gebruik van alle middelen gelijk.

De nieuwe eID-middelen zelf zijn wel verschillend in gebruik. Zo zijn er middelen die voor het bepalen van de identiteit gebruik maken van de identiteitskaart van de burger in combinatie met zijn/haar mobiele telefoon met een geïntegreerde NFC-chip. Ook zijn er middelen beschikbaar die gebruik maken van een app op de mobiele telefoon in combinatie met een pincode of biometrische gegevens van de burger. Meer gangbare middelen waarbij de identiteit van de burger wordt vastgesteld op basis van inlognaam en wachtwoord in combinatie met sms-verificatie zijn ook beschikbaar in het nieuwe eID-stelsel.

Afhankelijk van de behoefte van de burger, wat vindt hij/zij prettig in het gebruik, kiest de burger een eID-middel dat bij hem/haar past. Voorwaarde bij gebruik is dat het middel aan het juiste niveau van betrouwbaarheid voldoet voor de te gebruiken onlinedienstverlening.

4.3 Onder de motorkap

Bovenstaand proces is voor de gebruiker relatief eenvoudig te doorlopen. Onder de motorkap is het beeld complexer. Zo is er een flink aantal maatregelen getroffen om te voldoen aan de eisen ten aanzien van privacy en veiligheid van de burger. Zo is het identificatie- en authenticatieproces opgezet op basis van tweefactor-authenticatie. Om ervoor te zorgen dat betrokken partijen alleen over persoonsgerelateerde informatie kunnen beschikken wanneer dat echt noodzakelijk is, worden aan de identiteit gerelateerde gegevens versleuteld. Daarnaast wordt gebruik gemaakt van versleutelde verbindingen voor het transport van de gegevens.

Voor de (zorg)dienstverlener betekent het ontsluiten van de middelen dat hij zelf moet aansluiten op een zogenaamde ontsluitende dienst. Deze dienst zorgt voor de verbinding met verschillende middelen. De ontsluitende dienst leidt de gebruiker voor het authenticatieproces naar de authenticatiedienst van het middel dat de gebruiker heeft gekozen. De authenticatiediensten authentiseren de gebruiker met behulp van diens middel en geven - al dan niet met behulp van het zogenaamde BSN-Koppelregister - een versleutelde identiteit terug. Alleen publieke dienstverleners kunnen de versleutelde identiteit omzetten in een BSN. Een publieke dienstverlener die geen BSN mag ontvangen krijgt in plaats van een versleutelde identiteit een versleuteld pseudoniem.

4.4 De planning

De komende jaren zal stapsgewijs het nieuwe eID-stelsel ingevoerd gaan worden. De zorgsector heeft hierin een voortrekkersrol. In 2016 zijn een aantal eID-pilots uitgevoerd, ook binnen de zorg. De komende jaren worden de nieuwe inlogmiddelen en het gebruik ervan gefaseerd ingevoerd. Zo worden in 2017 (fase 0) verdere beproevingen met de DigiD- en Idensys-middelen gepland. In 2018 (fase 1) start de eerste uitrol met zogenaamde voorlopers en worden de middelen in samenhang beproeft. Partijen die dan meedoen, moeten alle middelen van het stelsel aanvaarden als middel voor identificatie en authenticatie.

Het doel van de overheid is om op termijn het gebruik van de middelen (via de Wet GDI, die naar verwachting op 1 januari 2019 in werking treedt) wettelijk verplicht te stellen (fase 2) voor aanbieders van digitale diensten binnen het BSN-domein. De oude (DigiD) voorzieningen op niveau ‘laag’ worden dan afgebouwd.

5 Pilots in de zorg

Om de werking van de middelen te toetsen en ervaringen op te doen met het gebruik zijn in 2016 in de zorg onder regie van Nictiz zes pilots met Idensys uitgevoerd. Idensys is een van de eID-aanbieders binnen het nieuwe stelsel. Er is gekozen voor Idensys omdat dit begin 2016 de enige beschikbare eID aanbieder was voor beproeving in de zorgsector. De zorgsector heeft de intentie om ook met de andere aanbieders van middelen op niveau substantieel en hoog nog eID-pilots uit te voeren.

Het doel van de eID-pilots was om te testen of de nieuwe middelen op niveau 'substantieel' en 'hoog' werken zoals beoogd wordt en om inzicht te krijgen in de implementatie van het nieuwe eID-stelsel bij patiënten en zorgaanbieders.

De pilotorganisaties in de zorg bestonden uit ICT-dienstverleners in de zorg (aanbieders van patiëntportalen) en zorgverleners met een vertegenwoordiging over de hele breedte van het zorgveld; (academische) ziekenhuizen, huisartspraktijken en fysiotherapiepraktijken. Via de zorgverleners zijn patiënten gevraagd om mee te doen met de pilots waarbij veel aandacht besteed is aan de minder digivaardigen en (chronisch zieken) ouderen[10]. In bijlage A is een uitgebreide omschrijving van de verschillende pilots en de deelnemers opgenomen.

Tijdens de pilots is getoetst of de middelen in het algemeen goed inzetbaar zijn in het zorgveld. De verschillende middelen die door de Idensys-leveranciers zijn aangeboden zijn echter niet onderling vergeleken. Daarnaast is onderzocht hoe de technische en organisatorische implementatie van het nieuwe stelsel bij de pilotorganisaties in de zorg verliep. Dit om ervaring op te doen die als input kan dienen voor de doorontwikkeling van het gebruik van het eID-stelsel in de zorg.

5.1 De opgedane ervaringen

In de pilots hebben zowel patiënten als dienstverleners positieve ervaringen opgedaan in de dagelijkse praktijk met de middelen onder het nieuwe stelsel. Opvallend in de bevindingen van het Panteia evaluatierapport is dat de meeste problemen zijn ervaren bij de eenmalige (opstart)handelingen zoals de aansluiting, de aanvraag en de uitgifte van de middelen. Het gebruik lijkt in de praktijk weinig tot geen problemen op te leveren. Daarbij moet opgemerkt worden dat een deel van de kritische bevindingen voortkomen uit het feit dat dit een pilot is, dat er bijgevolg nog weinig ervaring is bij betrokken partijen.

- Gebruikers vinden over het algemeen inloggen met de nieuwe middelen makkelijk en snel, en ervaren de middelen als veilig en betrouwbaar. Opvallend daarbij is dat patiënten aangeven in het gebruiksgemak tussen middelen op niveau 'substantieel' en 'hoog' weinig verschil te ervaren in deze pilot. De groep ouderen is over het algemeen positief over het gebruik.

- De meerwaarde van het nieuwe eID-stelsel blijkt voor burgers nog onvoldoende duidelijk. Dit blijkt onder andere uit de beperkte respons op het verzoek om mee te doen aan de eID-pilots. Slechts vijf procent van de patiënten die benaderd zijn voor deelname hebben zich aangemeld om mee te doen aan de pilots. Een effect hiervan was dat gaandeweg de pilots ook de dienstverleners gingen twijfelen over het nut en de noodzaak.

[10] Onder verwijzing naar het Panteia rapport

- Verkregen middelen worden relatief vaak gebruikt in de pilots en 74% van de gebruikers geeft aan het Idensys middel in de toekomst te willen blijven gebruiken. De voordelen die men benoemt zijn veiligheid, betrouwbaarheid, gemak en snelheid. Het meest positief zijn de gebruikers over het waarborgen van de privacy, de betrouwbaarheid en de veiligheid van het inloggen. Het algehele beeld uit de evaluatie van het gebruik is positief.

- Het aansluitproces voor zorgverleners is maatwerk, en wordt door veel partijen als 'taai' gekenschetst. Elke zorgorganisatie kent een eigen ICT-omgeving die in veel gevallen (gedeeltelijk tot geheel) bij een externe ICT-leverancier is ondergebracht. De implementatie van het koppelvlak is een intensief traject dat vraagt om nauwe afstemming tussen en inspanning van zowel de makelaar/implementatiepartij en de zorg- en/of ICT-dienstverlener.

- Het aanvraag- en uitgifteproces van de middelen werd door een deel van de patiënten als lastig ervaren. De redenen hiervoor zijn verschillend van aard maar hebben toch vooral te maken met de complexiteit, de onduidelijkheid en de lange duur van het proces van aanvraag. Meer principiële redenen, zoals privacy-gerelateerde overwegingen, spelen een minder grote rol, al is er een beperkte groep die aangeeft onvoldoende helder te hebben wat er met aangeleverde gegevens wordt gedaan.

- Voor het realiseren van de aansluiting, de aanschaf van middelen en het beheer worden kosten gemaakt. De aansluiting en aanschaf van middelen zijn eenmalige kosten. De beheerkosten zijn blijvend. Specifieke cijfers over de hoogte van de kosten voor de pilot zijn lastig in kaart te brengen. Een inschatting is dat voor de eenmalige kosten een bedrag tussen €35.000 tot €65.000 uitgegeven is, exclusief de verdere beheerkosten. Hierin zijn voornamelijk de implementatie- en organisatiekosten opgenomen. In deze pilots is niet gekeken naar de betaalbaarheid voor de patiënt en dienstverlener. De middelen zijn om niet aan de patiënten verstrekt en voor het gebruik van de middelen zijn geen kosten per transactie in rekening gebracht bij de dienstaanbieder. Er is niet getoetst hoe patiënten tegenover de kosten van de nieuwe middelen staan. Met de zorg(ICT-dienst)verleners uit de pilot is wel gesproken over de kosten van de implementatie en het gebruik van de nieuwe middelen. Zij hebben in de evaluatie aangegeven dat de onduidelijkheid over eventuele kosten en de hoogte daarvan als een belangrijk knelpunt wordt ervaren. Voor de implementatie van de nieuwe standaard zijn de dienstaanbieders financieel gestimuleerd.

6 Wat betekent het nieuwe eID-stelsel voor het zorgveld?

In deze paragraaf gaan we in op wat het nieuwe stelsel betekent voor het zorgveld. We zetten de voordelen op een rij en beschrijven wat de gevolgen voor zowel zorgverlener als patiënt zijn.

6.1 De voordelen op een rij

Veiligheid en privacy

Het invoeren van eID heeft verschillende gevolgen voor de veiligheid en privacy van de patiënt. Ten eerste betekent eID dat er een beter slot komt op de kluis waarin de gegevens van de patiënt staan. Op dit moment zijn deze gegevens in de digitale kluis vaak beveiligd met een gebruikersnaam en wachtwoord (al dan niet met sms-verificatie). Met de komst van de nieuwe standaard kan de identiteit van de patiënt met meer zekerheid worden vastgesteld. Identiteitsdiefstal “je voor doen als iemand anders” zal hierdoor moeilijker worden.

Ten tweede worden er strenge eisen gesteld aan de eID-aanbieders die inloggen via de nieuwe eID-methode mogelijk maken. Zij staan onder toezicht van de overheid en moeten zorgen voor een goede beveiliging van de inloggegevens. Voor de patiënt betekent dit dat zijn identiteitsgegevens maar ook de gegevens waar hij of zij is ingelogd goed beschermd worden. De identiteit van de burger wordt gepseudonimiseerd en de inloggegevens worden tijdens de gehele procedure versleuteld. Ook zijn de eID-middelen zo ingericht dat de eID-aanbieders niet meer gegevens kunnen gebruiken dan strikt noodzakelijk voor de authenticatie of voor fraudedetectie. Burger en patiënten krijgen wel de mogelijkheid om de logging van het gebruik van het middel in te zien. Zo kunnen ze zelf nagaan waar en wanneer het middel is gebruikt.

Een impuls voor nieuwe dienstverlening

De eID-middelen kunnen een impuls geven aan de digitale dienstverlening van zorgverleners doordat het deze dienstverlening veiliger maakt. Zo maakt het gebruik van middelen met een hoger betrouwbaarheidsniveau het bijvoorbeeld mogelijk om medische gegevens die door een patiënt zijn verzameld betrouwbaar te verwerken. Maar ook andere processen waarvoor de burger normaliter aan de balie moet verschijnen kunnen anders ingericht worden, denk aan het inschrijven of het doen van intakes op afstand. Idealiter wordt de invoering van eID meegenomen in een bredere strategie, gericht op het leveren van nieuwe en innovatieve onlinediensten. In zo’n strategie zal ook helder moeten zijn hoe traditionele kanalen voor dienstverlening in de toekomst gepositioneerd worden, en hoe ze zich verhouden tot de nieuwe kanalen.

Betrouwbare aanlevering van gegevens door de patiënt en andere professionals

Zorgverleners die gebruik maken van digitale diensten waarin patiënten zelf informatie kunnen toevoegen of aanpassen (van adres tot bloeddrukmetingen) kunnen door gebruik van de nieuwe eID-middelen met meer zekerheid vaststellen dat deze informatie ook inderdaad van de patiënt zelf komt.

Weg met de digitale sleutelbos

eID brengt een einde aan de alsmaar langer wordende lijst van inlogcodes en wachtwoorden. De patiënt/burger krijgt de mogelijkheid om op één uniforme en gestandaardiseerde manier in te loggen. Eén sleutel die past op alle sloten die voldoen aan de eID-eisen. Deze mogelijkheid gaat minimaal gelden voor het publieke (BSN) domein. Het private domein kan echter ook (vrijwillig) de nieuwe standaard accepteren en implementeren. Daarbij kan de burger kiezen welke en hoeveel inlogmiddelen hij/zij wilt

gebruiken.

Op termijn zullen nieuwe mogelijkheden ontstaan

De verwachting is dat op termijn nieuwe diensten aan het stelsel toegevoegd worden. Zo wordt het waarschijnlijk mogelijk anderen digitaal te machtigen, en wordt gedacht aan diensten ten behoeve van leeftijdsverificatie of het zetten van een digitale handtekening. Daarnaast maakt het stelsel het mogelijk om op termijn de burger in verschillende rollen (mantelzorger, of zorgprofessional) te ondersteunen waardoor ook autorisatieregels toegepast kunnen worden. Hierdoor kunnen legio nieuwe onlinediensten of nieuwe (zorg)apps ontstaan. Zo kan bijvoorbeeld thuiszorg op afstand veilig en betrouwbaar toegelaten worden tot de leefruimte van hulpbehoevenden die minder mobiel zijn. Met de groei van het stelsel zullen dus ook de mogelijkheden voor nieuw en innovatief gebruik toenemen.

6.2 Wat betekent het voor de patiënt?

De voordelen voor de patiënt zijn evident. Het nieuwe stelsel biedt meer veiligheid, creëert een oplossing voor steeds groter wordende digitale sleutelbos. Naarmate meer dienstverleners gebruik van de middelen mogelijk maken, en de onlinediensten die ze aanbieden verder evolueren, zullen deze voordelen ook beter merkbaar worden.

Tegelijkertijd zijn er nog vragen over de kosten van de middelen. Het is nog niet helder wat de middelen zullen kosten. Burgers zijn momenteel gewend aan (voor hen) kosteloze identificatie en authenticatie. Eventuele kosten die ze moeten maken voor de aanschaf van middelen zijn dus nieuw en moeten uitgelegd worden.

De verwachting – mede op basis van de pilotervaringen - is dat het gebruik van de middelen geen onoverkoombare problemen zal opleveren. De burger logt nu al voor een groot aantal diensten binnen en buiten de zorg en buiten de overheid in met verschillende middelen, denk aan het elektronisch regelen van bankzaken, maar ook het inloggen bij emaildiensten, webwinkels, en sociale media. Het voordeel hiervan is dat de burger wel wat gewend is en dat de introductie van nieuwe middelen voor de meeste gebruikers geen al te steile leercurve met zich mee zal brengen.

De meeste burgers zijn dus wel wat gewend, maar dat geldt niet voor iedereen. Er is een groep burgers en patiënten die lastig zijn weg vindt in een steeds verder digitaliserende wereld. Dit geldt niet alleen voor het gebruik van eID maar in bredere zin voor het gehele aanbod aan digitale diensten. Uit de pilot blijkt bijvoorbeeld dat ouderen – een groep die overigens zeer goed vertegenwoordigd was in de pilots – gemiddeld 5-8% minder positief zijn over het gebruik van de nieuwe middelen. Daarbij moet in acht genomen worden dat het gaat om de groep die vrijwillig meedoet aan de pilots. In werkelijkheid zou de groep dus weleens groter kunnen zijn.

Dit beeld is overigens ook herkenbaar bij overige vormen van dienstverlening. Er is een groep minder digitaal vaardigen die meer ondersteuning nodig zal hebben dan de gemiddelde gebruiker. Zo adviseert de Nationale Ombudsman in zijn rapport over het verdwijnen van de blauwe belastingenvelop een set van maatregelen ter ondersteuning van deze groep. De ondersteuning van minder digitaal vaardigen speelt zo mogelijk in de zorg nog sterker dan bij overige vormen van digitale dienstverlening. Juist voor de zorg is laagdrempelige toegang van het grootste belang. De introductie van middelen die meer zekerheid opleveren, maar waarbij ook de perceptie bestaat dat ze meer inspanningen vergen om van dienstverlening gebruik te kunnen maken lijkt daar haaks op te staan. In de praktijk (de resultaten van de pilots) blijkt echter dat het gebruik van de nieuwe eID-middelen niet als negatief wordt ervaren ten opzichte van overige bestaande inlogmiddelen.

6.3 Wat betekent het voor de zorgverlener?

Voor zorgverleners is de impact groter dan voor patiënten. Zorgverleners moeten ervoor zorgen dat gebruik gemaakt kan worden van de nieuwe middelen bij het aanbieden van onlinedienstverlening. Daarvoor moeten ze een aantal stappen doorlopen, die we hier kort beschrijven. Daarbij is van belang te beseffen dat alhoewel de grote lijnen wel helder zijn, de meeste eisen en stappen nog onvoldoende gespecificeerd zijn om de daadwerkelijk impact in te schatten. Het voorstel voor de Wet GDI dat momenteel voorligt en waarin dit soort zaken geregeld worden, moet nog verder uitgewerkt worden in onderliggende regelgeving. De verwachting is dat het komende jaar geleidelijk meer helderheid zal ontstaan.

Het classificeren van diensten naar betrouwbaarheidsniveau

Als gevolg van de Wet GDI moeten (zorg)dienstverleners bepalen wat het minimale vereiste betrouwbaarheidsniveau is voor authenticatie bij gebruik van digitale dienstverlening. De verwachting is dat de meeste dienstverlening binnen de zorg zich op het niveau hoog dan wel substantieel zal bevinden.

Voldoen aan de acceptatieplicht

De wet verplicht dienstverleners alle erkende (publieke en private) authenticatiemiddelen te accepteren bij het verlenen van toegang tot digitale dienstverlening. Voorwaarde hierbij is dat het middel het minimale vereiste betrouwbaarheidsniveau heeft voor de betreffende digitale dienst. Bijvoorbeeld, indien het minimaal vereiste betrouwbaarheidsniveau substantieel is, dan moet een gebruiker zich ook kunnen authentiseren met een middel op betrouwbaarheidsniveau Hoog. Voor digitale diensten met een betrouwbaarheidsniveau Laag, geldt dat ook middelen op niveau Substantieel en Hoog toegestaan moeten worden.

Om de acceptatieplicht in de praktijk mogelijk te maken moeten zorgverleners een contract afsluiten met een of meer ‘ontsluitende diensten’. Deze diensten verbinden de dienstverlener met de verschillende authenticatiediensten. Momenteel is nog niet helder hoeveel ontsluitende diensten er zullen ontstaan en of zij elk alle middelen zullen afdekken. Het is dus denkbaar dat een (zorg)dienstverlener) met meerdere ontsluitende diensten moet samenwerken om alle middelen af te dekken.

De implementatie van eID vergt zorgvuldige voorbereiding

Daarnaast dient de dienstverlener de eigen infrastructuur gereed te maken voor een of meer koppelvlakken. Uit de interviews met in de pilot betrokken partijen komt het beeld naar voren dat de implementatie van eID technische complex is. Daarnaast is er geen sprake van een ‘standaard’ implementatietraject, maar eerder van maatwerktrajecten. Dat valt deels te verklaren door het feit dat zorgverleners geen standaard ICT-omgeving hebben maar ook doordat er nog verschillen zitten in de wijze waarop de middelen aan die omgevingen gekoppeld kunnen worden.

De kennis die benodigd is voor de implementatie is vaak onvoldoende binnen de eigen organisatie aanwezig. Tegelijkertijd geven de partijen aan dat het ook bij de leveranciers soms nog zoeken is. Nu is dit deels te verwachten in pilotsituaties. Geconcludeerd moet worden dat er behoefte is aan gedegen implementatieondersteuning als de uitrol van de middelen breder opgepakt wordt.

De wet stelt ook eisen aan de beveiliging van de dienstverlening

De Wet GDI bevat de grondslag om per AMvB eisen te stellen aan de werking, betrouwbaarheid en beveiliging van de toegang tot digitale dienstverlening. Het gaat er dan dat eisen worden gesteld aan

bijvoorbeeld veiligheidsplannen, risicomanagement, het uitvoeren van audits, koppelvlakspecificaties, functionele(ontwerp)normen, technische procesbeschrijvingen en testbepalingen. Daarnaast voorziet de wet in jaarlijkse audits, toezicht, en een meldplicht. Hoe dit alles precies vorm krijgt is momenteel onderwerp van de verdere uitwerking.

Het huidige DigiD wordt uitgefaseerd

Het huidige DigiD zal op termijn uitgefaseerd worden. Voor digitale diensten die authenticatie op betrouwbaarheidsniveau Laag vereisen, mag het huidige DigiD nog tot drie jaar na inwerkingtreding van de Wet GDI gebruikt worden. Op basis van de huidige planning betekent dit tot 1 januari 2022.

6.4 De kosten voor implementatie en gebruik moeten verder uitgewerkt worden

Op dit moment is nog niet helder wat de kosten voor het gebruik van het nieuwe eID-stelsel voor de dienstverlener zullen worden. Tot op heden is het uitgangspunt dat kosten voor de aanschaf van de nieuwe inlogmiddelen voor de burger/patiënt van het middel zijn. En dat de kosten voor de koppeling met de systemen die voor authenticatie zorgen, en de kosten voor het gebruik van het middel voor de dienstverlener zijn.

Aangezien voor de dienstverlener niet helder is wat de kosten zijn voor de transacties met de verschillende middelen is het ook lastig een inschatting te maken van de totale kosten. Mogelijk zullen er ook verschillende tarieven worden gehanteerd voor de verschillende eID-middelen. Deze variabele transactiekosten zullen vervolgens verwerkt moeten gaan worden in de kostprijs van de dienstverlening. Hoe dit exact moet gaan plaatsvinden en wat hier de consequenties van zijn (bijvoorbeeld voor de bedrijfsvoering of verzekeraars) is nu nog niet duidelijk.

6.5 Informatie voor en door de zorgverlener

Tot nu toe is de communicatie richting zorgverleners over de komst van deze nieuwe manieren van inloggen zeer beperkt geweest. Uit de pilots blijkt wel hoe essentieel het is om die informatievoorziening tijdig en gedegen op te zetten. Dat is niet alleen noodzakelijk om nut en noodzaak voor de zorgverlener helder te maken, maar ook om deze concreet voor te bereiden op de transitie naar de nieuwe middelen. In verdere pilots zou daarom beproefd kunnen worden aan welke informatie behoefte is, hoe die het beste vormgegeven wordt en welke kanalen het beste werken.

Tegelijkertijd heeft de zorgverlener een belangrijke rol in de informatievoorziening naar zijn patiënt. In algemene zin is het aan de zorgverlener om de patiënt in te lichten over de digitale diensten die de patiënt afneemt. Onderdeel daarvan is de wijze waarop daarbij ingelogd wordt. De verwachting is dat dit de komende jaren met de komst van meer uniforme middelen eenvoudiger zal worden. De patiënt komt de middelen immers op steeds meer plekken tegen en raakt daardoor steeds beter bekend met nieuwe middelen. Daarnaast zal vanuit de overheid aandacht besteed worden aan de introductie van middelen. Dat neemt niet weg dat veel patiënten toch hun eerste vragen zullen richten tot hun zorgverlener. Die vragen kunnen gaan over de keuze voor middelen, over het gebruik van de middelen of over mogelijke problemen bij het inloggen met de middelen. Voor veel van deze vragen zal de zorgverlener de patiënt kunnen doorverwijzen naar de helpdesk van de leverancier van de middelen.

Mits goed geïnformeerd - en daarmee goed in staat de patiënt te informeren - kunnen zorgverleners een belangrijke drijfveer zijn voor de patiënt om over te stappen op veiligere vormen van authenticatie.

7 Tot slot

Bestaande en toekomstige toepassingen voor onlinedienstverlening stellen stevige eisen aan de veiligheid van gegevens, zeker daar waar het gaat om privacygevoelige gegevens. Juist daarom is in de zorg het belang van betrouwbare online identificatie en authenticatie op het juiste niveau hoog.

De pilots met de Idensys-middelen in de zorg laten zien dat het nieuwe eID-stelsel een veilig en bruikbaar alternatief kan zijn voor de huidige minder veilige en minder betrouwbare authenticatiemethodes in het zorgveld. De pilots zijn over het algemeen succesvol verlopen. De vereiste technische aansluitingen zijn gerealiseerd en het gebruik van het middel verliep zonder noemenswaardige problemen. De ervaringen van zowel patiënten als dienstaanbieder zijn over het algemeen positief over het dagelijks gebruik.

Tegelijkertijd zijn er nog veel vragen rondom de verdere invoering, de exacte werking en kosten van het nieuwe stelsel. Bij de internetconsultatie van de Wet GDI in maart 2017 heeft NICTIZ daarom onder meer aandacht gevraagd voor de volgende onderwerpen.

- Een snelle uitwerking van de exacte termijnen voor de invoering van het eID-stelsel. Wanneer wordt het gebruik van de middelen (in de zorg) verplicht, en wanneer worden overige inlogmiddelen uitgefaseerd?
- De verdere uitwerking van de technische specificaties met daarin nadrukkelijk de wens om te komen tot één koppelvlak zodat zorgverleners niet meerdere verschillende koppelvlakken hoeven te ontsluiten Daarnaast zou het mogelijk moeten zijn om zorgverleners als groep aan te sluiten om te voorkomen dat kleine partijen buitenproportioneel hoge kosten moeten maken voor het aansluiten op het stelsel.
- De wijze waarop toezicht en handhaving binnen het stelsel worden ingericht.
- De financiering van de (eenmalige en exploitatie-) kosten. Daarbij gaat de voorkeur uit naar een eenvoudig model waarbij de kosten vooraf helder en inzichtelijk zijn voor de zorgverlener.
- De uitwerking van handvatten voor het omgaan met het gebruik van het stelsel op de grenzen van het BSN-domein. Een patiënt die gegevens opslaat in een persoonlijke gezondheidsomgeving (PGO)handelt buiten het BSN-domein, maar als hij die gegevens deelt met zijn ziekenhuisarts dan handelt hij wel degelijk binnen het BSN-domein. Hoe kan voorkomen worden dat patiënten hierdoor meerdere keren moeten inloggen?
- Handvatten voor de praktische toepassing van de niveaus ‘substantieel’ en ‘hoog’. Wat moet wanneer gebruikt worden en hoe is dit eenvoudig aan patiënten uit te leggen?

Daarnaast hebben de pilots duidelijk gemaakt dat de grootschalige introductie van het nieuwe stelsel de nodige voeten in de aarde zal hebben. De implementatie van de eID-standaard blijkt een significante inspanning te vergen van het zorgveld. Deze inspanning zit voornamelijk in de eenmalige opstart-stappen, zoals de aansluiting van de dienstverlener op de eID-standaard. Deze blijkt technisch complex en vereist vaak de nodige ondersteuning. Hoe groot de inspanning straks daadwerkelijk zal zijn, is in dit stadium nog lastig te voorspelen, mede omdat veel van de voor zorgdienstverleners belangrijke onderwerpen nog verder uitgewerkt moeten worden.

Tot slot blijkt de meerwaarde van het nieuwe eID-stelsel voor burgers en voor zorgverleners vaak nog onvoldoende duidelijk. Dat is niet heel vreemd. In algemene zin is het maatschappelijk bewustzijn over het nut en de noodzaak van betrouwbare authenticatie bij online gegevensverwerking beperkt aanwezig. Voor een succesvolle adoptie van het nieuwe stelsel zal de komende jaren flink geïnvesteerd moeten worden in communicatie richting zorgdienstverleners en patiënten over het nut en de noodzaak van de

combinatie van betrouwbare inlogmogelijkheden. Daarbij zal het besef van nut en noodzaak naar verwachting toenemen naarmate nieuwe en betekenisvolle eHealth-toepassingen zich verder ontwikkelen. Immers, wie iets waardevols in een kluis heeft zitten, zal eerder geneigd zijn te investeren in een solide slot.

Het stelsel wordt daarmee een onmisbare component in een veel bredere strategie die gericht is het op vergroten van de onlinedienstverlening in de zorg. Om dat mogelijk te maken is de komende jaren een stevige en gezamenlijke inspanning van overheid, zorgverleners, hun ICT-leveranciers, en de leveranciers van de eID-middelen nodig.

Bijlage 1. Overzicht van de pilots in de zorg

In deze bijlage geven we een overzicht van de pilots in de zorg.

- Fysiomanager – World of Health
- Isala
- Medischegegevens.nl (Meddex)
- PAZIO
- Pharmeon
- UMC Utrecht

Fysiomanager – World of Health

Soort organisatie:
Softwareleverancier voor paramedici voor administratie en EPD

Soort dienstverlening (waar in de pilot toegang via eID aan wordt verleend):
Fysiomanager heeft een portaal waar patiënten gegevens kunnen inzien en vragenlijsten kunnen invullen. Voor dit portaal is de Idensys toegangssystematiek ingebouwd.

Motivatie voor deelname aan de pilot:
Het inloggen door patiënten op het portaal moet zo veilig mogelijk, maar tevens eenvoudig zijn. Eén systematiek van inloggen voor verschillende portalen maakt dat de toegankelijkheid verhoogd. Aansluiten bij een systematiek als Idensys betekent tevens dat, na een eenmalige technische exercitie, de inlogprocedure up to date blijft.

Doel en aanpak van de pilot:
1) Inbouwen van de techniek
2) Uitrollen naar eindgebruikers (patiënten) via de praktijken
3) Verzorgen van voldoende communicatie naar de eindgebruiker via de praktijk (folder)
4) Evalueren en motiveren om respons te verhogen
5) Directe mailing vanuit de praktijken naar actuele gebruikers van het portaal

Respons:
De respons blijkt laag te zijn. Het besef om een veiliger manier van inloggen te kiezen blijkt niet hoog te zijn. Uit de mailing bleek slechts 5-10% de aanvraag van een middel te starten. Daarnaast was het proces van het verkrijgen van de middelen moeilijk voor een aantal klanten, waardoor uitval tijdens de aanvraagprocedure.
Omdat er een getrapte aansturing is (vanuit WOH naar praktijk, vanuit praktijk naar eindgebruiker) is het lastig direct te motiveren.
Toch zijn er ongeveer 60 patiënten die een middel hebben aangevraagd en ook hebben gebruikt.

Isala

Soort organisatie
Isala is één ziekenhuisorganisatie met vijf locaties in Zwolle, Meppel, Steenwijk, Kampen en Heerde. Onder het motto 'dichtbij als het kan, verder weg als het moet' waarborgen wij samen het aanbod van basis- en topzorg in Zuidwest-Drenthe en Noordwest-Overijssel.
Isala biedt meer dan basiszorg. In de loop der jaren hebben we steeds meer bijzondere, topklinische functies toegewezen gekregen. Vaak als erkenning van de kennis en vaardigheden die specialisten op eigen initiatief hadden opgebouwd. In de topklinische functies, zoals hart- en neurochirurgie en dialyse, kunnen we ons meten met academische ziekenhuizen.
Om het niveau van deze zorg zo hoog mogelijk te houden, wordt voortdurend toegepast wetenschappelijk onderzoek gedaan. De specialistische kennis die we in huis hebben, geven we door aan artsen en verpleegkundigen in opleiding. Studenten uit het MBO, HBO en van de universiteit kunnen voor opleidingsplaatsen bij ons terecht.

Dienstverlening afdeling pilot Idensys
De Trombosedienst in Isala Zwolle draagt zorg voor patiënten met trombose: ongewenste bloedstolling. Heeft u trombose, dan kan uw huisarts of specialist u naar ons doorverwijzen. Wij controleren regelmatig uw bloed en de dosering van medicijnen die uw (huis)arts heeft voorgeschreven.
De Trombosedienst van Isala is aangesloten bij de Nederlandse Federatie van Trombosediensten.

Patiënten die onder behandeling zijn bij de Trombosedienst kunnen toegang tot het Trombosezorg portaal verkrijgen door gebruik te maken Idensys

Motivatie deelname aan de pilot
Bij het ontwikkelen van een nieuw Trombosezorg portaal is nadrukkelijk gekeken naar de beveiliging van het portaal en het veilig authentiseren van patiënten en externe zorgverleners in het kader van uitgangspunten en architectuur principes t.a.v. digitale beveiliging binnen Isala van portalen en apps..

Doel en aanpak van de pilot
Bij de ingebruikname van het Trombosezorg portaal was het gestelde doel om alle (ongeveer 1000) patiënten die al gebruik maakten van het oude Trombosezorg portaal via Idensys in te laten loggen in het nieuwe portaal.
Om dit doel te bereiken zijn de patiënten per brief, per email en via een mededeling in het oude portaal geïnformeerd en opgeroepen om het beveiligingsmiddel aan te vragen. Verder is het hulp aangeboden bij het doorlopen van het aanvraagproces voor het verkrijgen van dit middel.

Respons
Ten tijde van de Live-gang van het nieuwe Trombosezorg portaal hadden ongeveer 800 patiënten beschikking over het nieuwe beveiligingsmiddel.
Gezien de leeftijd van de gebruikers van het Trombosezorg portaal werd de aanvraagprocedure van het Idensys middel als lastig gezien. Zodra de gebruikers het middel in bezit hebben, wordt het gebruik ervan om in te loggen het Trombosezorg portaal als eenvoudig aangeduid.

Toekomst
In 2017 heeft de Trombosedienst het voornemen om sterk te groeien met het aantal gebruikers in het Trombosezorg portaal.

Medischegegevens.nl (Meddex)

Soort dienstverlening
Persoonlijk gezondheidsdossier in ziekenhuis

Motivatie voor deelname aan de pilot
Vooroplopen bij nieuwe ontwikkelingen op het gebied van veilig inloggen en gebruiksgemak

Doel en aanpak pilot
Actieve gebruikers van medischegegevens.nl via een Idensys login toegang geven tot de eigen vertrouwde medischegegevens.nl omgeving.

Repsons
>150 deelnemers (plm. 8%)

PAZIO

Soort organisatie
PAZIO, onderdeel van UMC Utrecht, biedt een eHealth platform voor zorg en welzijn dat online diensten en portalen bundelt voor de zorgconsument. Zo krijgen zij via één veilige inlog toegang tot al hun online diensten.

Soort dienstverlening (waar in de pilot toegang via eID aan wordt verleend)
Voor de Idensys pilot werkte PAZIO samen met Gezondheidscentrum Oog in Al en de Leidsche Rijn Julius Gezondheidscentra (LRJG). De gezondheidscentra tellen respectievelijk ruim tienduizend en achtendertigduizend patiënten in hun bestand. Naast DigiD met SMS authenticatie zijn de patiëntportalen benaderbaar gemaakt via Idensys. De portalen bieden online diensten geïntegreerd met het huisarts informatiesysteem zoals online afspraak, econsult, herhaalrecept, dossier, Saltro labuitslagen en zelfmanagement diensten op maat. Eenmaal ingelogd kan de gebruiker in het portaal van het gezondheidscentrum zonder opnieuw in te loggen ook gebruik maken van portalen van andere aanbieders zoals bijvoorbeeld het ziekenhuis.

Motivatie voor deelname aan de pilot
PAZIO houdt zich al jaren bezig met het aanbieden van online zorg via één inlog. Idensys is voor PAZIO dus een waardevol instrument om het gebruikersgemak voor de zorgconsument te vergroten. Zo is PAZIO koploper op het gebied van authenticatie in de zorg en heeft december vorig jaar ook een pilot met Idensys niveau hoog succesvol afgerond.

Doel en aanpak van de pilot
Voor Oog in Al en LRJG zijn actieve portaal gebruikers (N=1.703 en 6.285) per mail uitgenodigd. Daarnaast hebben de gezondheidscentra folders verspreid met daarin informatie over Idensys en het verzoek tot deelname aan de Idensys pilot. Gedurende de gehele pilot periode waren de portalen ook benaderbaar met DigiD met SMS authenticatie. De PAZIO helpdesk was gedurende de pilot benaderbaar voor vragen over Idensys.

Respons
In totaal hebben 163 gebruikers zich voor de pilot aangemeld middels een korte vragenlijst bij gezondheidscentrum Oog in Al waarvan 2 zich uiteindelijk hebben afgemeld en 3 niet in het bezit waren van een mobiele telefoon. De overigen (N=158) zijn door PAZIO toegewezen aan een inlogmiddel Creaim (N=60) en Digidentity (N=98).

Bij LRJG hebben 340 gebruikers zich aangemeld voor de pilot. PAZIO heeft 201 gebruikers toegewezen aan het inlogmiddel Digidentity en 139 aan het middel Creaim.

Het aantal inlogs met Idensys voor het portaal van Oog in Al en LRJG zag er gedurende pilotperiode als volgt uit:

	Oog in Al	LRJG
Juli	35	Idensys nog niet geïmplementeerd
Augustus	13	Idensys nog niet geïmplementeerd
September	141	97
Oktober	156	137
November	30	3

De PAZIO helpdesk heeft in totaal 34 meldingen ontvangen over de Idensys test.

Pharmeon

Soort organisatie
Pharmeon maakt websites, patiëntportalen en apps voor eerstelijns zorgpraktijken. Door een unieke koppeling van online diensten met zorginformatiesystemen wordt een eHealth platform voor veilige, professionele en efficiënte communicatie met patiënten gecreëerd.
Soort dienstverlening (waar in de pilot toegang via eID aan wordt verleend)
Via Idensys kunnen patiënten van deelnemende huisartspraktijken inloggen in het patiëntportaal met de volgende diensten, direct gekoppeld aan het HIS:

- Herhaalrecepten (recepten herhalen op basis van de informatie in het HIS)
- Webagenda (afspraken maken op de door de medewerker beschikbaar gestelde momenten)
- eConsult (veilig communiceren met medische gegevens)

Motivatie voor deelname aan de pilot
Pharmeon biedt een eigen authenticatiemethode voor de online diensten. Die vereist dat je aan iedereen die een account aanmaakt voor online dienstverlening, vraagt om langs te komen om zich te legitimeren. Voor de zorgverlener, maar ook voor de patiënt, kost dit eenmalig extra tijd. Patiënten hebben bij vrijwel elke zorgverlener of zorginstelling een ander account met mogelijk een andere inlognaam en wachtwoord. Met Idensys is dat probleem verholpen. Doordat patiënten één manier van inloggen hebben en daarmee bij verschillende organisaties terecht kunnen hoeven ze zich maar één keer aan te melden en te identificeren.
De zorgpraktijken hebben direct een voordeel, omdat zij de identiteit van de patiënten niet meer hoeven te controleren. Dit is immers al gedaan. Het neemt de praktijk werk uit handen en patiënten kunnen vervolgens meteen gebruik maken van de online services van de praktijk.

Doel en aanpak van de pilot
Pharmeon ondersteunt zorgverleners met complete online dienstverlening om efficiënte en veilige communicatie met patiënten mogelijk te maken. Daarom is het voor ons van belang ervaring op te doen met het gebruik van toekomstige identificatiemiddelen zoals bijvoorbeeld Idensys.
Twee huisartspraktijken nemen deel die al langer online diensten van Pharmeon aanbieden waarvoor authenticatie vereist is. De betreffende praktijken benaderden bestaande gebruikers van hun diensten via een mailing en via de website. Bereidwillige patiënten werd gevraagd een Idensys account aan te vragen en vervolgens met Idensys in te loggen bij de zorgpraktijk om gebruik te maken van de online diensten.

Respons
Bij de twee deelnemende praktijken hebben zich 125 patiënten actief aangemeld voor deelname aan de pilot waarvan een groot deel de Idensys middelen daadwerkelijk gebruikt. Bij de relatief hoge bereidheid tot deelname speelt een belangrijke rol dat het verzoek daartoe van de eigen huisarts kwam. Dat deels de dienst uiteindelijk niet in gebruik werd genomen komt o.a. door de aanvraagprocedure die complex bevonden werd door gebruikers. Men is soms angstig om gegevens te delen met makelaars die het middel uitgeven. Wie is Safran, Morpho, Creaim? Waarom moet KPN een kopie van mijn paspoort hebben?

UMC Utrecht

Soort organisatie
Universitair Medisch Centrum

Soort dienstverlening (waar in de pilot toegang via eID aan wordt verleend):
Voor al onze patiënten geven we toegang tot ons 'Patiëntenportaal' waarmee patiënten een groot deel van hun (realtime) EPD/dossier in kunnen zien.

Motivatie voor deelname aan de pilot
Het UMC Utrecht wil graag vooroplopen als ziekenhuis om zoveel mogelijk van haar patiënten toegang te geven tot hun EPD/dossier, uiteraard ook op een zo veilig mogelijke manier.
Idensys heeft een nog hoger veiligheidsniveau dan ons huidig gebruikte DiGiD-inlog met sms-verificatie. Dat was de belangrijkste reden om te participeren bij de pilot.
Daarnaast voelt het UMC Utrecht ook een maatschappelijke verantwoordelijkheid om te participeren bij deze landelijke pilot die als doelstelling heeft om de toegang van **alle** patiënten tot hun medische gegevens veiliger te maken.

Doel en aanpak van de pilot
Wij hebben patiënten geworven via ons UMC-Utrecht patiëntenpanel, en met een oproep in ons patiëntenportaal om te participeren bij de Idensys-pilot. Als extra beloning hebben we een BOL.COM bon van 10 euro in het vooruitzicht gesteld. Daarnaast hebben we binnen onze IT-organisatie collega's uitgenodigd mee te doen aan de pilot.
Ongeveer 230 personen hebben vervolgens een begin gemaakt met het aanvragen van de toegang.
We hebben vanuit het UMC Utrecht geen zicht op hoeveel gebruikers werkelijk een Idensys-middel hebben aangevraagd en hoeveel gebruikers het middel succesvol hebben ontvangen.
Ook hebben we geen exact inzicht hoe vaak het middel gebruikt wordt om in te loggen in ons patiëntenportaal.
We hebben geen eigen/UMCU evaluatie uitgevoerd, we zullen de evaluatie van Panteia gebruiken om een goed beeld te krijgen van oordeel en ervaringen van gebruikers.
Voorafgaand aan het starten van de pilot hebben we de vereiste infrastructurele componenten ingericht (of laten inrichten, we hebben hiervoor samengewerkt met bedrijf Anoigo).

Respons
In de aanmeldfase hebben we diverse reacties ontvangen over moeizame aanmeldingen. Nadien hebben we nauwelijks nog spontane reacties ontvangen. Zelf hebben we dus ook geen evaluatie uitgevoerd voor onze gebruikersgroep.

Optimale toepassing van eHealth en ICT in de zorg kan niet zonder standaardisatie. In nauwe samenwerking met zorgverleners, koepelorganisaties, standaardisatieorganisaties en industrie draagt Nictiz zorg voor de ontwikkeling en beschikbaarheid van de noodzakelijke standaarden. We doen dit door het organiseren van gemeenschappelijke ontwikkelprojecten, kennisoverdracht en kwaliteitstoetsing.

Nictiz
Postbus 19121
2500 CC Den Haag
Oude Middenweg 55
2491 AC Den Haag

T 070 - 317 34 50
@Nictiz
info@nictiz.nl