Self Sovereign Identity

Meer regie over eigen patiëntengegevens

Whitepaper

SIDN IRMAconnect

Inhoud

1 Waarom je deze whitepaper moet lezen

De opmars van e-health maakt de discussie over de veiligheid van patiëntengegevens actueler dan ooit. De privacy van gebruikers moet gewaarborgd blijven, waarbij het gaat om diverse beveiligingslagen:

- Via welke partij worden gegevens gedeeld?
- Waar worden deze data opgeslagen?
- Wie heeft er toegang tot deze gegevens?
- Hoe zorgen we ervoor dat de juiste personen (denk aan thuiszorg-medewerkers of mantelzorgers) op het juiste moment ook toegang kunnen krijgen tot informatie van de patiënt?

Sleutelbegrip bij het veilig omgaan met patiëntendata is authenticatie, het vaststellen dat een gebruiker van een digitale dienst is wie hij zegt te zijn. Daarom gaan we in deze whitepaper in op de volgende vragen:

- Tegen welke obstakels lopen verzekeraars, zorgverleners en patiënten nu nog aan als het gaat om authenticatie?
- Hoe gaat de nieuwe Wet digitale overheid hiermee om?
- Wat is het Self Sovereign Identity-concept en welke beloften biedt dit voor de zorg?

2 Dit zijn de uitdagingen rond digitale authenticatie

Het verlenen van zorg is altijd gekoppeld aan een persoon. Een juiste authenticatie is cruciaal: is dit de persoon die van deze zorg gebruik mag maken? Daarnaast moet voorkomen worden dat de verkeerde persoon of instantie toegang krijgt tot iemands medische gegevens.

Als het gaat om zorg op afstand, wordt nu nog vooral DigiD als authenticatie gebruikt. Die oplossing is echter verouderd en storingsgevoelig. Maar er zijn nog meer obstakels die authenticatie momenteel opwerpt.

Patiënt moet steeds opnieuw gegevens delen
Zo is het gevoel van bureaucratie een bron van frustratie voor zorgcliënten, wat niet los is te zien van authenticatie. Bij elke nieuwe zorginstantie moeten dezelfde gegevens doorgegeven worden, want een uitwisseling van data tussen de instellingen is vaak niet mogelijk omdat er met verschillende systemen wordt gewerkt.

Een deel van het probleem is dat niet alle zorgpartijen en -oplossingen toegang hebben tot DigiD. Dit is voorbehouden aan overheden en organisaties die een overheidstaak uitvoeren en daarbij het burgerservicenummer (BSN) in hun administratie mogen gebruiken, bijvoorbeeld een ziekenhuis of een zorgverzekeraar.

Deze spelregel lijkt het succes van innovatieve oplossingen te beperken. Een voorbeeld hiervan was Constamed, een online dienst waarmee consumenten via internet – voor minder urgente vragen – terecht konden bij alle aangesloten huisartsen. Hierdoor werd de beschikbaarheid van huisartsen optimaal benut.

Aanvankelijk konden bezoekers via DigiD inloggen, maar toen bleek dat ze in de praktijk vragen konden stellen aan een willekeurige huisarts die niet beschikte over hun BSN-nummer, moest Constamed het systeem wijzigen. Bezoekers konden voortaan alleen bij hun eigen huisarts terecht. Hierdoor werd de meerwaarde van Constamed tenietgedaan.

Omslachtig proces voor zaakwaarnemer
Is het huidige stelsel voor de patiënt zelf al omslachtig, ingewikkelder is het aanvragen en declareren van zorg door zaakwaarnemers. Elke keer opnieuw moet namelijk een machtiging worden afgegeven. Ook hier loopt DigiD tegen zijn grenzen aan, omdat het tegenwoordig verplicht is om hierbij met 2-factor-authenticatie in te loggen en dit meestal via de telefoon van de cliënt gaat. En juist deze persoon is iemand die zoveel mogelijk moet worden ontlast. Ook bij de zorgwaarnemer, vaak een partner of familielid, dragen al deze handelingen bij aan de stress.

Bovenstaande struikelblokken laten maar één conclusie toe: niet alleen is DigiD aan vervanging toe, ook is er behoefte aan nieuwe authenticatie-modellen om goede elektronische dienstverlening mogelijk te maken.

Gelukkig is ook de overheid zich hiervan bewust. Reden voor de invoering van een nieuw authenticatiestelsel, zowel voor de zorg als andere (semi-) overheidsorganisaties. Dit gebeurt door middel van de Wet digitale overheid, die momenteel bij de Eerste Kamer ligt.

IoT en security
Nieuwe Internet of Things-toepassingen vragen om stevige garanties op het gebied van veiligheid. Als waardes zoals glucose of bloeddruk worden gemonitord en gedeeld met een behandelaar, mogen deze gegevens natuurlijk niet in verkeerde handen vallen.

3 Onze visie op de Wet digitale overheid

Op het moment dat we deze whitepaper schrijven, is nog niet duidelijk wat de concrete uitwerking wordt van de Wet digitale overheid (WDO). De wet zelf is echter al door de Tweede Kamer, wat betekent dat de wettekst verder niet meer wordt gewijzigd.

Wat staat er precies in de WDO?
De wet wil het mogelijk maken dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. Daaronder vallen onder meer ziekenhuizen en zorgverzekeraars, maar ook op andere zorgverleners zal de wet impact hebben.

Wat bedoelt de WDO met veilig en betrouwbaar inloggen?
Het gaat erom dat burgers elektronische identificatiemiddelen (eID) krijgen met een hogere mate van betrouwbaarheid dan het huidige DigiD. Deze authenticatiemiddelen moeten publieke dienstverleners meer zekerheid geven over iemands identiteit.

De grote vernieuwing is dat ook het gebruik van private inlogmiddelen wordt toegestaan om namens gebruikers het BSN te verwerken. Dit recht is nu nog voorbehouden aan DigiD. De vraag is nu welke keuzes er door de Nederlandse overheid worden gemaakt over welke partijen onder welke voorwaarden authenticatietoepassingen mogen aanbieden. Dit leidt tot vragen als: hoe worden gegevens opgeslagen (centraal of decentraal) en wat voor organisatie zit er achter het initiatief (bijvoorbeeld een stichting of commercieel bedrijf)?

Waarom past Self Sovereign Identity in de visie van de WDO?
Een mogelijkheid om invulling te geven aan de wet, bieden de zogenoemde Self Sovereign Identity-toepassingen (SSI). Dat zijn decentrale oplossingen waarbij de gebruiker bij officiële uitgevers waarheden en gegevens over zichzelf ophaalt en elders gebruikt om zichzelf kenbaar te maken. In zo'n model is er helemaal geen sprake van centrale databases die kunnen lekken.
Bovendien zijn SSI-oplossingen zodanig opgezet dat alleen datgene wat nodig is wordt gedeeld. Alleen die stukjes data (attributen) worden gedeeld die nodig zijn om toegang te krijgen tot de diensten waarvan de patiënt gebruik wil maken. Hij heeft op die manier regie op zijn eigen gegevens.

Laten we de voordelen van SSI eens nader bekijken:

1. Alle risico's ten aanzien van veiligheid, transparantie en de kans op oneigenlijk gebruik van persoonlijke data en gedragsinformatie worden geminimaliseerd. Een 'lek' beperkt zich tenslotte tot een persoon (account) en raakt geen hele database. Een groot aantal gebruikers compromitteren kost kwaadwillenden dus heel wat meer moeite.
2. SSI past het best bij de ontwerpprincipes van privacy-by-design. Bij het bouwen van een toepassing wordt er dan naar gestreefd al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen. Privacy-by-design voorkomt centrale honeypots voor hackers en kwaadwillenden. En het voorkomt het onverkwikkelijke risico op oneigenlijke data-exploitatie omdat in de software waarborgen zijn ingebouwd die dit voorkomen.
3. Wanneer SSI-oplossingen open-source zijn, komt dat ten goede aan de veiligheid. De code is dan door iedereen in te zien, waardoor zwakke plekken snel worden opgespoord en geheime achterdeurtjes min of meer onmogelijk zijn. Het kiezen voor open-source is overigens helemaal in lijn met de nieuwe wet.

3

4. Dan zijn er nog de economische afwegingen. Door SSI in te zetten kun je eenmalig een uitgifte doen vanuit een bron of een register, waarna gebruikers de aan hen verstrekte informatie hergebruiken zolang deze informatie geldig is. Hierdoor nemen de kosten per transactie significant af, wat natuurlijk bevorderlijk is voor het gebruik van middelen.

We willen de critici van SSI ook nog graag meenemen in de discussie. Doorgaans wordt deze aanpak namelijk gezien als ondermijning van bestaande verdienmodellen. Maar dat kun je ook anders zien. Want als we in de BV Nederland in staat zijn om een digitale vertrouwens-infrastructuur betrouwbaar en betaalbaar te maken, profiteert letterlijk elke digitale dienstaanbieder en overheid daarvan.

Er wordt dan namelijk flink minder geld uitgegeven aan authenticatie-kosten. Geld dat je direct kunt inzetten voor betere of goedkopere dienstverlening. In een wereld waarin we steeds meer zaken digitaal willen organiseren, kun je dat onmogelijk géén goed idee vinden.

4 De toekomst van elektronische identificatiemiddelen

In het huidige eID-landschap zijn allerhande middelen beschikbaar voor particulieren: itsme, iDIN, DigiD en veel meer. Allemaal hebben ze één ding gemeen: ze zijn óf bruikbaar in het publieke domein (zoals de zorg) óf bruikbaar in het private domein.

Door het aanstaande toelatingskader verandert dat mogelijk en krijgen burgers eindelijk middelen in handen waarmee zij in beide domeinen gemakkelijk en betrouwbaar kunnen inloggen. In de nabije toekomst zien we hopelijk een SSI waarmee de burger zowel BRP-attributen en bankattributen als zijn persoonlijke contactgegevens kan tonen.

Een mooi voorbeeld binnen het SSI-domein is IRMA, wat staat voor I Reveal My Attributes. Daarmee kunnen gebruikers op een makkelijke en veilige manier online inloggen, zichzelf kenbaar maken en toestemmingen geven. De gratis IRMA-app stelt gebruikers in staat zelf identiteitskenmerken op te halen via hun smartphone en alleen de noodzakelijke kenmerken te delen met – of te tonen aan – partijen die iets van hen willen weten. De persoonsgegevens staan alleen op de eigen smartphone en worden nergens centraal opgeslagen.

De burger bepaalt zelf met welke (combinatie van) middelen hij zichzelf kenbaar maakt, wat de acceptatie van het eID ten goede komt. Hij kan immers meer middelen tegelijk gebruiken om een verhoogd digitaal vertrouwen te realiseren.

Na het ingaan van de WDO worden toelatingseisen van authenticatiemiddelen in lagere regelgeving uitgewerkt. De makers van IRMA streven ernaar dat hun oplossing dan wordt toegelaten.

IRMA en VGZ

Zorgverzekeraar VGZ gebruikt IRMA om zaakwaarnemers declaraties in te laten dienen namens hun cliënten. Via IRMA geeft de verzekerde een machtiging aan zijn zaakwaarnemer, zodat die zorgdeclaraties kan indienen. Dat kan ook via DigiD, maar omdat het tegenwoordig verplicht is om hierbij met 2-factor-authenticatie in te loggen en dit meestal via de telefoon van de cliënt gaat, is dat eigenlijk geen werkbare mogelijkheid meer.

Overigens werken ook andere zorgpartijen met IRMA, bijvoorbeeld ChipSoft, Ivido en HINQ.

4

Hoe werkt IRMA?
Bij IRMA stelt de gebruiker uit meerdere bronnen een persoonlijk soort ‘paspoort’ samen op zijn eigen smartphone. Daarin staan persoonsgebonden attributen, zoals: naam, adres, geboortedatum, e-mailadres, mobiel telefoonnummer, BSN, BIG-registratie, IBAN, studentschap, schooldiploma’s, lidmaatschappen van allerlei clubs, kortingskaarten, leeftijdsgrenzen enzovoort.

Deze attributen worden voorzien van een digitale handtekening die de authenticiteit van die attributen waarborgt. Zo’n handtekening komt van een erkende autoriteit, bijvoorbeeld een gemeente als het om een adres gaat. Verder zijn alle attributen voorzien van een geldigheidsdatum.

Een gebruiker kan ook een selectie van de eigen attributen gebruiken om zelf een digitale handtekening te zetten. Het ligt voor de hand om je naamattribuut te gebruiken voor een handtekening, maar met IRMA kan bijvoorbeeld ook een arts ondertekenen vanuit zijn beroep. Dat wil zeggen, met de eigen medische attributen uit het nationale BIG-register voor professionals in de zorg.

De gebruiker met zijn ‘paspoort’ vol attributen kan vervolgens een deel van die persoonsgegevens vrijgeven aan ‘verifiers’. Die partijen – ‘controleurs’ met een Nederlandse term – kunnen met geavanceerde cryptografische technieken de authenticiteit ervan controleren en zijn daarbij niet noodzakelijkerwijs afhankelijk van derde partijen. Bij conventionele identiteitssystemen is zo’n derde partij onvoorwaardelijk nodig. Dat maakt zo’n systeem ingewikkelder en kwetsbaarder. En ook duurder.

Het belangrijkste van alles: in het hele proces heeft de gebruiker zelf de regie gehouden.

De voordelen van IRMA in het kort:
- Doordat data niet meer centraal worden opgeslagen, gaat de algemene veiligheid van patiëntengegevens omhoog.
- Door ketenoptimalisatie komt de patiënt minder hobbels tegen op zijn ‘klantreis’. Hij kiest voortaan zelf welke zorgverlener welke informatie van hem krijgt. Als hij wil, gebruikt hij dezelfde eID bovendien in communicatie met private partijen.
- Innovaties op onder meer IoT-gebied worden niet afgeremd door zwakke beveiliging.
- Doordat de scheidslijn tussen publieke en private middelen wordt doorbroken, wordt samenwerking tussen overheid en bedrijfsleven gestimuleerd.

Gemeente Amsterdam

IRMA en de Gemeente Amsterdam
Op een veilige en betrouwbare manier omgaan met gegevens en geen onnodige informatie vragen of opslaan. Dat is het uitgangspunt van de Gemeente Amsterdam wanneer het gaat om haar digitale dienstverlening.

Tegenwoordig hoeven inwoners van de gemeente niet iedere keer opnieuw formulieren in te vullen met hun postcode, telefoonnummer et cetera. Met IRMA zijn ze op het moment dat ze inloggen eigenlijk al klaar.

5 Over IRMA

IRMA is voortgekomen uit onderzoeksactiviteiten op het gebied van attribuut-gebaseerde authenticatie die sinds 2008 plaatsvinden binnen de Radboud Universiteit onder leiding van professor Bart Jacobs. In oktober 2016 is het resultaat ondergebracht bij de stichting Privacy by Design met als ambitie het IRMA-systeem grootschalig uit te rollen.

IRMA powered by SIDN is de samenwerking tussen SIDN en de stichting Privacy by Design. De samenwerking is gericht op het verder ontwikkelen van het privacyvriendelijke identiteitsplatform IRMA. We werken als beheerder van de .nl-zone al jaren aan de veiligheid en toegankelijkheid van het internet in Nederland en versterken IRMA met dezelfde zekerheden die we leveren voor ons nationale internetdomein .nl.

Een veilige en bruikbare digitale identiteit voor individuen en organisaties is in het algemeen belang. Daarom is IRMA open-source en werken we zonder winstoogmerk. Wij geloven dat IRMA de meest integere en betrouwbare oplossing is voor een publiek en privaat identificatiesysteem waarbij de privacy van de gebruiker centraal staat.

www.sidn.nl/irma-powered-by-sidn

Over IRMAconnect

Met IRMAconnect kan IRMA ook als ontzorgde verificatiedienst worden afgenomen, waarin je attributen kunt opnemen. IRMAconnect is dan de verbindende schakel tussen jouw online dienst(en), je klanten en IRMA.

Je sluit je makkelijk aan op basis van de protocollen SAML 2.0, OAuth en OpenID Connect. Hierdoor geef je jouw klanten met behulp van IRMA als inlog- en authenticatiemiddel eenvoudig toegang tot bijvoorbeeld je website of online klantportaal.

Door het betrouwbare IRMAconnect kun je garanties over jouw dienstverlening opnemen in een SLA.

www.sidn.nl/product/IRMAconnect

Colofon

Meer weten? Neem contact op met:
Bob Kronenburg, propositie developer
bob.kronenburg@sidn.nl
T +31 (0)6 31 03 14 23

Meld je aan voor onze nieuwsbrief
www.sidn.nl/nieuwsbrief

SIDN
Postbus 5022
6802 EA Arnhem
Meander 501
6825 MD Arnhem
T +31 (0)26 352 55 00
www.sidn.nl