ITDS

IRMA

Powered by SIDN

IDENTITEITSBEHEER OPLOSSEN MET SELF-SOVEREIGN IDENTITY.

Lees deze whitepaper als je wilt weten hoe eID-innovatie de inlogdrempels voor verzekeringsproducten wegneemt.

#GETREADY

WAAROM JE DEZE WHITEPAPER MOET LEZEN.

Vraag je je wel eens af waarom de servicedesk telkens al je persoonsgegevens moet uitvragen om te valideren of jij bent wie je zegt dat je bent? Of dat je voor verschillende verzekeringsproducten verschillende accounts moet aanmaken, dan weer moet inloggen met DigiD, dan weer met een gebruikersnaam en wachtwoord? Kan dat niet makkelijker? Ja dat kan.

Is het je opgevallen dat vernieuwende verzekeringsproducten vaak onderdeel uitmaken van verschillende diensten die naadloos aansluiten op de levensstijl en behoeften van klanten? Daar heb je identity-oplossingen voor nodig die complementaire diensten in één klantreis kunnen ontsluiten - en die tegelijkertijd de privacy van de klant waarborgen en voldoen aan hoge security-eisen. Welke identity-middelen kunnen daaraan voldoen?

Een nieuwe generatie identity-middelen biedt hiervoor de oplossing. Deze zijn gebouwd op het principe van Self Sovereign Identity (SSI). Deze oplossingen beleggen de controle over persoonsgegevens bij de klant zelf en dat uitgangspunt zorgt voor veel interessante voordelen voor online dienstverleners, in het bijzonder in de financiele sector. In deze paper richten we ons niet op de techniek, maar op de innovaties die deze nieuwe generatie eID-middelen realiseert.

Dit whitepaper bespreekt eerst de uitdagingen:

- De drempels in de klantreis
- De stijgende kosten voor security en privacy compliance

En de dan de oplossingen voor:

- Een optimale klantreis
- Verlaagde security en privacy-risico's

Wil je weten hoe innovatie en privacybescherming hand in hand gaan? Lees dan verder.

'WAAROM MOET IK VOOR ELKE VERZEKERING WEER EEN APART ACCOUNT EN INLOGMIDDEL GEBRUIKEN, IK BEN NOG STEEDS DEZELFDE PERSOON?'

Zomaar een scenario: met een ID-app op je telefoon log je in op de klantomgeving van je verzekeringsagent. Je wilt een claim indienen bij je zorgverzekering. Je scant een QR-code op de website van de agent en je ID-app vraagt toestemming om het delen van een set persoonsgegevens, waaronder je burgerservicenummer. Je gaat akkoord en je bent ingelogd. Na het indienen van je claim krijg je een aanbod van je adviseur voor een inboedelverzekering in combinatie met een Philips Hue Woonveiligpakket. Je leest de voorwaarden en klikt op akkoord. Je scant een QR-code, maar ditmaal deel je alleen je NAW-gegevens; niet je BSN. Je inboedelverzekering is afgesloten. Vervolgens klik je op 'Claim nu je woonveiligpakket'. Het beeld toont weer een QR-code. Je scant de code en de ID-app op je telefoon toont welke gegevens de leverancier van het pakket nodig heeft; je naam en adres. Je drukt op akkoord en je krijgt een bevestiging te zien dat het pakket morgen wordt vezonden.

Deze hele klantreis heb je razendsnel doorlopen met 1 inlogmiddel, in plaats van DigiD, misschien iDIN en een account bij een retailpartij. Je weet ook precies met wie je welke gegevens gedeeld hebt. Op dit moment is zo'n integrale 'seamless' klantreis al mogelijk; met Self Sovereign Identity-oplossingen.

VEEL ID-OPLOSSINGEN ZORGEN VOOR EEN HOBBELIGE KLANTREIS

In onze digitale 24-uurs economie verwachten klanten op ieder moment van de dag zaken te kunnen doen. Bovendien willen ze daarbij zo min mogelijk drempels op hun pad vinden.

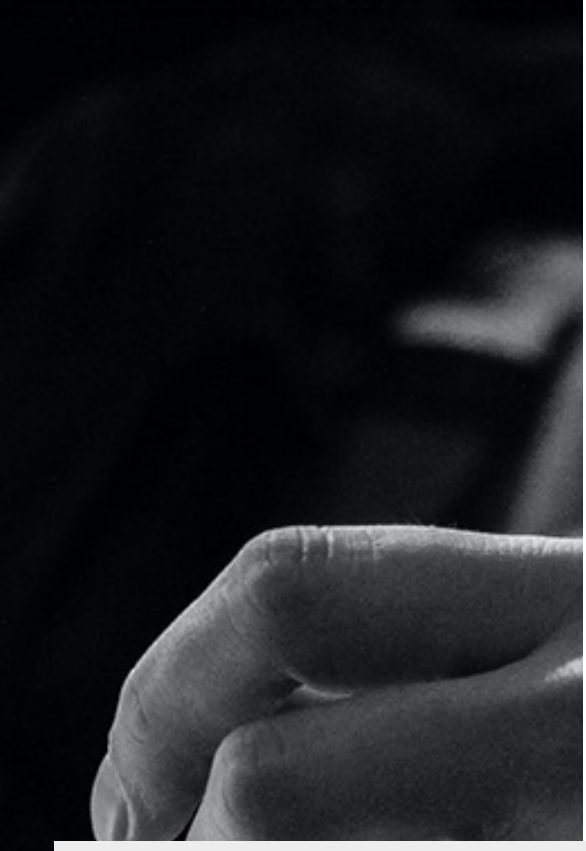
De praktijk is vaak anders. Om een paar voorbeelden te noemen:

- De aanvraagprocedure voor veel producten vergt veel identificatie-handelingen. Dat kost tijd, is frustrerend en foutgevoelig en leidt tot uitval.
- De klant moet voor elk product (bijvoorbeeld Zorg, Leven of Schade) opnieuw inloggen. Ook al zit je hiervoor bij dezelfde verzekeraar, er is geen uniforme ervaring.
- Bij telefonisch contact moet een klant wederom vragen beantwoorden om zich te identificeren.
- De klant moet met regelmaat gevoelige documenten zoals een paspoort scannen en verzenden.

Big Tech sterk in vernieuwende proposities en naadloze klantreizen

Big Tech treedt ook langzaam toe tot de verzekeringsmarkt. Nu wordt hun penetratiesnelheid beperkt door toetredingskaders die per land verschillen, maar de eerste productlanceringen zijn een feit.[1] En ze blinken uit met nieuwe verzekeringsproducten in combinatie met non-insurance diensten, gebruiksgemak en naadloze onboarding processen. Volgens het World InsurTech Report 2020 van Capgemini en Efma is de bereidheid van polishouders om een verzekering bij Big Techs af te sluiten inmiddels gestegen van 17% in 2016 naar 36% in januari 2020 tot 44% in april 2020.

Om de concurrentie aan te gaan is het dus noodzakelijk dat verzekeraars zichzelf onderscheiden met complete verzekeringsproposities en non-insurance services die voor Big Tech voorlopig onbereikbaar blijven. In combinatie met een klantreis die de verwachtingen overtreft, levert dat een sterke concurrentiepositie op.



Trend: Ecosystemen

Want klanten hebben steeds meer behoefte aan complete verzekerings-diensten die in combinatie met non-insurance producten naadloos aansluiten op hun levenstijl. Non-insurance diensten, zoals een stappenteller bij je zorgverzekering, of een homesecuritypakket bij je inboedelverzekering, bepalen de keuze voor een verzekeraar zelfs in 62% van de gevallen. [2]

Service-ecosystemen, waarvan verzekeringsproducten slechts één onderdeel uitmaken, worden een steeds grotere trend. PwC voorspelt ecosystemen rondom thema's als 'home', 'smart mobility' en 'vitality'.[3] Als verzekeraar kun je services aanbieden binnen zo'n ecosysteem of er zelf een bouwen.

Om dit mogelijk te maken heb je een universeel toepasbaar inlogmiddel nodig dat een hele waardeketen kan ontsluiten, zonder dat een klant bij zich elke stap opnieuw moet identificeren en gegevens moet delen. De meeste identity-middelen bieden hiervoor geen oplossing; DigiD, iDIN en social login's zijn vanwege hun verschillende autorisatie- en veiligheidsniveaus, slechts voor een beperkte set aan producten toepasbaar.

EEN SERVICE-ECOSYSTEEM DAT BESTAAT UIT VERSCHILLENDE DIENSTEN EN AANBIEDERS VRAAGT OM EEN UNIVERSEEL eID-MIDDEL DAT DE HELE WAARDEKETEN KAN ONTSLUITEN.

Kortom, een inlogmiddel voor de verzekeringsbranche moet aan de volgende eisen voldoen:

- Het middel biedt alle attributen over de gebruiker aan die relevant zijn.
- Deze attributen zijn waarheidsgetrouw op basis van gevalideerde persoonsgegevens.
- Het middel is daarmee door de hele keten inzetbaar voor een seamless ervaring.

Naast een compleet aanbod aan diensten kunnen verzekeraars zich op een ander punt goed positioneren. De roep om privacybescherming stijgt en daar heeft Big Tech een grote achterstand in te halen. Verzekeraars kunnen ook hier een onderscheidende positie innemen.

DE ROEP OM PRIVACYBESCHERMING EN DE STIJGENDE KOSTEN VAN COMPLIANCE

De zorgen van klanten over de bescherming van hun privacygevoelige gegevens groeien met de dag. Bedrijven die de mist in gingen, haalden de afgelopen jaren consequent de krantenkoppen.

Het hele complex rondom security, privacy(wetgeving) en compliance is dan ook een steeds belangrijker onderwerp geworden voor CIO's bij verzekeraars.

Steeds meer privacywetgeving

Opvallende verhalen, zoals het privacyschandaal van Cambridge Analytica en grote datalekken zoals die bij Facebook en Equifax, leiden ertoe dat klanten zich afvragen wie ze kunnen vertrouwen en hoe ze zichzelf kunnen beschermen. De uitkomsten van diverse onderzoeken[5] op dit gebied zijn overtuigend:

- Slechts 52% van de klanten heeft het gevoel dat ze bedrijven kunnen vertrouwen, en slechts 41% wereldwijd vertrouwt hun overheid.
- 85% van de klanten vindt dat bedrijven meer zouden moeten doen om hun gegevens actief te beschermen.
- 61% van de klanten zegt dat hun angst voor identiteitsdiefstal de afgelopen twee jaar is toegenomen.

75% van de klanten stelt intussen dat ze liever niet kopen bij bedrijven die het niet zo nauw lijken te nemen met de bescherming van privacygevoelige data. Ook al is het onduidelijk hoeveel van deze klanten handelen naar deze overtuiging, het is wel evident dat het vertrouwen van de klant belangrijk is voor diens loyaliteit.

Tegelijkertijd zien we dat het voldoen aan beveiligingsstandaarden en allerlei wet- en regelgeving rondom klantendata hoge kosten met zich meebrengt. Forbes meldt dat in 2018 alleen al in Groot-Brittannië meer dan 1,1 miljard euro door bedrijven werd uitgegeven aan de voorbereiding op de invoering van de GDPR (AVG).[6]

BIJNA 90% VAN DE NEDERLANDERS WIL MEER CONTROLE OVER WIE WELKE DATA OVER HEN VERZAMELT. TWEEDERDE ZEGT DAAR TOTAAL GEEN GRIP OP TE HEBBEN. 96% WIL KUNNEN KIEZEN HOEVEEL EN WELKE GEGEVENS ZE DELEN.[4]

Hogere Know Your Customer-eisen, veel controleprocessen

Dan moet je nog zorgen voor waarheidsgetrouwe, consistente klantdata. De uitdaging is dat er snel verschillende versies van klantendatasets door systemen zwerven, bijvoorbeeld doordat een klant zijn adreswijziging vergeet door te geven. De huidige standaard vergt dat één 'gouden record' wordt aangewezen als basiswaarheid. Nu is het vaak geen sinecure om dat record goed te bewaken. Hoe weet je zeker dat een adreswijziging overal goed is doorgevoerd? Kloppen bankgegevens nog wel? Vaak moet je klanten telefonisch nog allerlei controlevragen stellen en kom je er dan pas achter dan iemand bijvoorbeeld verhuisd is.

Waar je als online dienstverlener behoefte aan hebt, is een oplossing waarmee je golden records automatisch geverifieerd zijn en actueel blijven. Dat is hard nodig, want de managementkosten van KYC-compliance programma's stijgen al jaren en een gebrekkige KYC-experience kan er zelfs voor zorgen dat klanten vertrekken. [7]

Stijgende securityrisico's en -kosten

Tot slot is het risico op datalekken groot en security-expertise kostbaar, en als klantgegevens eenmaal op straat liggen dan zijn de gevolgkosten nog hoger. In de huidige situatie zijn klantgegevens vaak versnipperd, inconsistent en/of dubbel opgeslagen in allerlei systemen. Daardoor zijn de security-risico's veel hoger dan noodzakelijk. Immers, hoe meer gegevens je verwerkt, hoe meer datapunten er beveiligd moeten worden.

Slim voorsorteren
Identity-oplossingen hebben – naast impact op de klantreis - impact op alle hierboven genoemde compliancekaders.

Organisaties die onderscheidend willen zijn en een toekomstvaste oplossing zoeken voor alsmaar toenemende compliancelasten, gaan dus gericht op zoek naar een identity-oplossing die zowel de klantervaring verhoogt als compliancelasten verlaagt.

Het complete wensenlijstje voor een ideale identity-oplossing is dus:

- Het middel biedt alle attributen over de gebruiker aan die relevant zijn.
- Deze attributen zijn waarheidsgetrouw op basis van gevalideerde persoonsgegevens.
- Het middel is daarmee door de hele keten inzetbaar voor een seamless ervaring.
- Het biedt de klant vertrouwen.
- Het voldoet aan Nederlandse en Europese privacy-wetgeving.
- Het zorgt automatisch voor geactualiseerde, geverifieerde klantdata (KYC-compliant).
- Het voldoet aan hoge security-eisen.

Hoe ziet zo'n inlogmiddel er in de praktijk uit?

EEN INTEGRAAL INLOGMIDDEL VOOR VERZEKERAARS.

Dát is het antwoord op de vraagstukken op de voorafgaande pagina's: een identity-oplossing die overal toepasbaar is en voldoet aan de hoogste privacy- en securitystandaarden. Dan kan je een veilige, seamless experience aanbieden tussen complementaire verzekeringsdiensten.

In de verzekeringswereld worden al oplossingen gebruikt die aan deze eisen voldoen.

Self Sovereign Identity; het fundament voor een nieuwe generatie identity-oplossingen

We hebben het dan over Self Sovereign Identity-toepassingen (SSI). De naam zegt het al; het uitgangspunt van SSI-oplossingen is dat de gebruiker – de klant - zelf controle heeft over geverifieerde persoonsgegevens – attributen genaamd. Daarnaast hebben de meeste SSI-oplossingen een decentraal karakter. Er worden dus nergens grote hoeveelheden klantdata verwerkt of opgeslagen.

'IK HEB NU GEWOON ZELF EEN DIGITAAL PASPOORT WAARMEE IK INLOG. DigiD IS ONNODIG, EEN KOPIE OPSTUREN HOEFT OOK NIET. SUPERHANDIG.'

Hoe werken SSI-oplossingen?

De gebruiker kan verschillende attributen ophalen bij desbetreffende, officiële uitgevers zoals een gemeente, of het Centraal Bureau Rijvaardigheid – en slaat deze data op in een digitale wallet op zijn smartphone; denk aan een BSN, NAW-gegevens, geboortedatum en rijbewijzen. Vervolgens kan de gebruiker zich met deze attributen identificeren bij online dienstverleners. SSI-oplossingen bieden online dienstverleners aan de andere kant de mogelijkheid om verschillende attributen aan te bieden én uit te vragen als identificatiemiddel.

Stel je wilt als gebruiker met een SSI-middel inloggen bij een zorgverzekeraar. Deze vraagt om een uitgebreide set aan attributen: BSN, NAW-gegevens en een geboortedatum. Jij ziet als gebruiker precies welke attributen worden uitgevraagd en je kunt per attribuut beslissen of je deze data wilt delen. De zorgverzekeraar weet aan de andere kant dat elk attribuut dat jij deelt waarheidsgetrouw is, en gedeeld met jouw expliciete toestemming. Als je vervolgens met datzelfde middel inlogt bij een wijnhandel, dan kan de online verkoper op zijn beurt voldoen met het uitvragen van de attributen 'ouder dan 18 jaar' en 'adres', zonder dat je jouw echte naam of je geboortedatum hoeft te delen.

Wat zijn specifiek voor verzekeraars de voordelen van een SSI-oplossing?

#1 Het gebruiksgemak van de klant schiet omhoog, evenals de snelheid waarmee verzekeraars klanten kunnen onboarden.

SSI-oplossingen nemen veel drempels waar de klant van vandaag tegenaan loopt weg. Ze kunnen een eindeloze set aan geverifieerde persoonsgegevens opslaan als afzonderlijke attributen. Hierdoor kunnen gebruikers zich met hetzelfde middel – maar met wisselende attributen - identificeren bij verschillende diensten. Zo vervangen SSI-middelen bestaande ID-middelen die slechts een beperkte set aan data kunnen delen.

Inloggen bij een zorg- én schadeverzekering? Dat kan voortaan met hetzelfde inlogmiddel. Zo maken SSI-middelen het mogelijk om eindeloos veel diensten van verschillende dienstverleners te combineren en 'seamless journey's' te ontwikkelen die aansluiten op de bredere klantbehoefte.

#2 Je gaat automatisch efficiënt om met privacygevoelige data.

SSI-oplossingen sluiten naadloos aan op de principes van privacy-by-design en dwingen zorgvuldige omgang met persoonsgegevens af. In de eerste plaats door de klant de controle te bieden over het delen van persoonsgegevens. Dit dwingt online dienstverleners vervolgens om niet meer informatie uit te vragen dan strikt noodzakelijk. En tot slot zorgt het ervoor dat persoonsgegevens expliciet in overeenstemming met de klant worden gedeeld. Hierdoor voldoe je als online dienstverlener voor een groot deel 'automatisch' aan AVG-standaarden.

#3 Persoonsgegevens zijn als vanzelfsprekend geverifieerd

Ook het werk van de KYC-afdeling wordt stukken eenvoudiger. Bij eID's op basis van SSI deelt de klant beveiligde attributen die zijn 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 BPR-gegevens gaat. Verder zijn attributen voorzien van een geldigheidsdatum. Een klant die inlogt met een SSI-middel zorgt er zo voor dat veel routine-werkzaamheden van de KYC-afdeling al zijn gedaan. Er hoeft niets meer telefonisch geverifieerd te worden en het opsturen van een kopie-paspoort zal ook nauwelijks meer nodig zijn.

DE KLANT ZELF DE REGIE GEVEN OVER PERSOONLIJKE DATA LEVERT VEEL VOORDELEN OP.

#4 Er zijn minder zwakke schakels, geen grote data honeypots

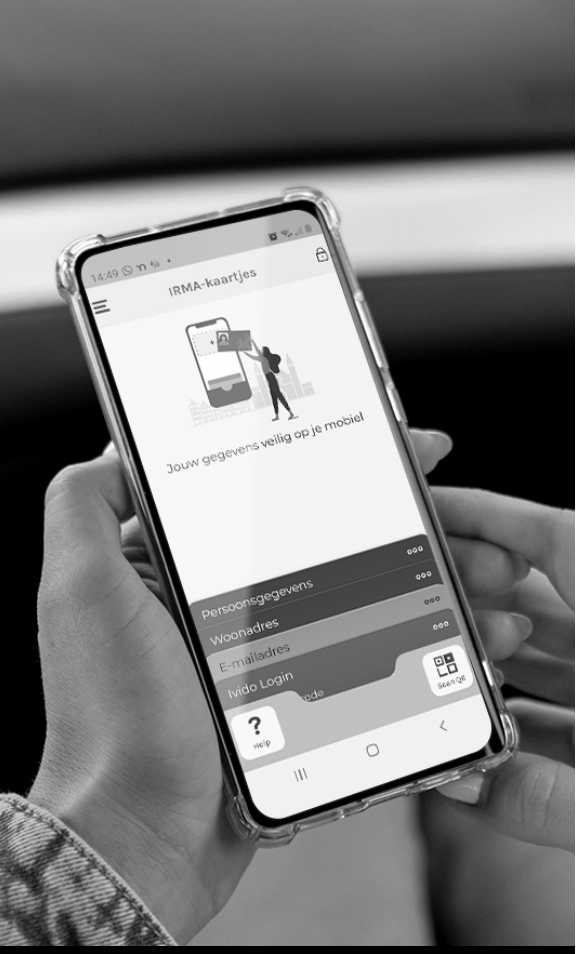
Het decentrale karakter van de meeste SSI-oplossingen zorgt ervoor dat er op minder plekken persoonsgegevens geopenbaard hoeven te worden en er minder centrale honeypots ontstaan. Als een gebruiker inlogt met een SSI-oplossing, dan hoeft een servicemedewerker bijvoorbeeld geen persoonsgegevens meer te controleren of in te zien. De verificatie vindt onder water plaats. Attributen zijn immers bijna als vanzelfsprekend geverifieerd.

Vanwege de decentrale infrastructuur, waarbij attributen worden opgehaald bij verschillende uitgevers die als beveiligde kaartjes worden opgeslagen in de e-wallets van gebruikers, bestaat er nergens een grote opslag van persoonsgegevens. Je kunt als online dienstverlener ook veel efficiëntere keuzes maken rondom de opslag van gegevens. Je kunt er als online dienstverlener bijvoorbeeld voor kiezen dat een gebruiker alleen een attribuut als bewijs toont zonder de inhoud prijs te geven of op te slaan; bijvoorbeeld het attribuut 'ouder dan 18', zonder een geboortedatum te openbaren.

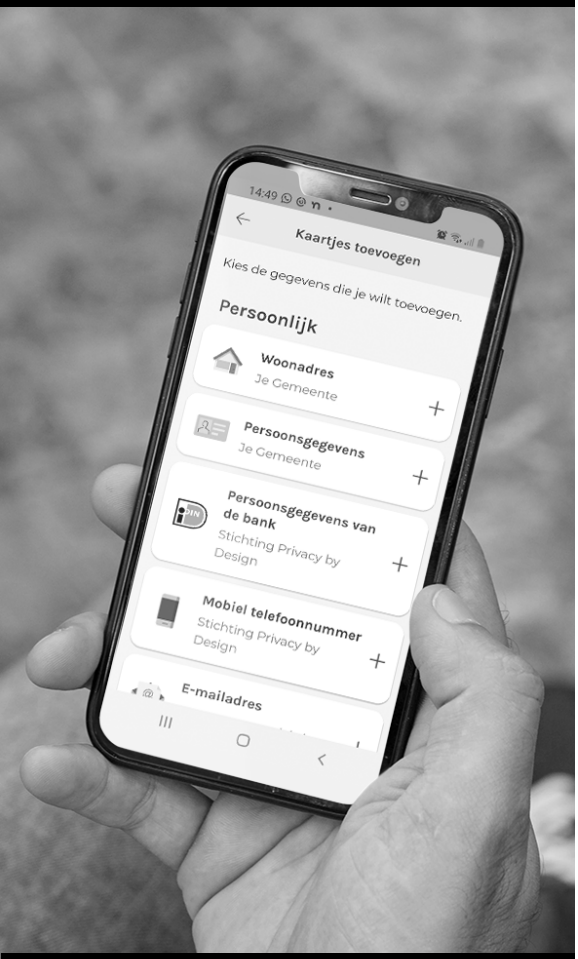
Zo worden alle risico's ten aanzien van veiligheid, transparantie en de kans op oneigenlijk gebruik van persoonlijke data geminimaliseerd.

#5 Tot slot, een SSI-oplossing draagt door haar veiligheid en betrouwbaarheid bij aan klantvertrouwen en daardoor ook aan je merkwaarde.

Met een SSI-oplossing impliceer je als organisatie dat je privacybescherming hoog in het vaandel hebt staan. Je geeft de controle over gevoelige data 'terug' aan de klant en vraagt alleen essentiële gegevens uit. Hierdoor onderscheid je je van de Big Tech concurrenten die vooral gebaat zijn bij Big Data en gebrek aan transparantie over het delen van persoonsgegevens. Op een markt waar klanten er niet meer op vertrouwen dat bedrijven naar eer en geweten met hun data omgaan, kan een SSI-oplossing dus onderscheidende waarde leveren.



SIDN verbetert continue de gebruiksvriendelijkheid van de app. Download de app en geef jouw verbetertips door!



Met IRMA sla je jouw persoonsgegevens op als kaartjes in een digitale portemonnee.

SSI in de praktijk: IRMA

Een SSI-oplossing die in Nederland al kan worden gebruikt is IRMA, wat staat voor I Reveal My Attributes. Het IRMA platform is een open source decentraal platform dat bestaat uit de IRMA-app voor eindklanten en de stack om zelf IRMA-diensten te ontwikkelen. IRMAconnect is bijvoorbeeld een applicatie die het voor online dienstverleners mogelijk maakt om gebruikers in te laten loggen met IRMA via hun bestaande Identity en Access Management provider.

IRMA heeft al een rijk ecosysteem. Met de IRMA-app stelt klanten in staat om zelf identiteitskenmerken op te halen via hun smartphone bij gemachtigde partijen als het Basisregister Persoonsgegevens, Kamer van Koophandel en Centraal Bureau voor de Rijvaardigheid.

Vervolgens hoeft de klant alleen de noodzakelijke kenmerken te delen met - of te tonen aan - partijen die iets van hem willen weten. De beveiligde persoonsgegevens staan alleen op de eigen smartphone en worden nergens centraal opgeslagen.

Het IRMA-ecosysteem biedt met onder andere een geverifieerd BSN, e-mailadres en telefoonnummer een uitgebreide set aan attributen. Is er behoefte aan specifieke attributen van klanten, dan is het met IRMAconnect ook mogelijk om zelf attributen uit te geven in IRMA. Denk aan een onderwijsinstelling die een diploma als attribuut aanbiedt.

IRMA is bovendien een oplossing die in lijn ligt met nieuwe wetgeving. Naar verwachting op 1 juli 2021 treedt de Wet digitale overheid (WDO) in werking. Hiermee wil de overheid private partijen de mogelijkheid bieden om – naast DigiD - hoogwaardige identity-oplossingen te ontwikkelen waarmee gebruikers kunnen inloggen bij overheidsorganisaties en zorgverleners, waaronder zorgverzekeraars. Omdat het hier gaat om de verwerking van BSN-gegevens, moeten deze oplossingen voldoen aan strenge privacy- en security-eisen.

In de loop van 2021 wordt bekend welke authenticatiemiddelen worden toegestaan om in te loggen bij zorgverzekeraars. Ten tijde van de publicatie van deze whitepaper staan alle signalen voor IRMA op groen.

VOORBEELDCASE: 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 hierbij met 2-factor-authenticatie in te loggen en dit meestal via de telefoon van de cliënt gaat, is dat een suboptimale oplossing geworden.

Het IRMA logo kun je ook tegenkomen bij ziekenhuizen (ChipSoft), Ivido, HINQ, Gemeente Amsterdam en CIS.

‘IK KAN INLOGGEN BIJ Ivido, HINQ, GEMEENTE ADAM EN CIS.’

OVER ITDS

ITDS Business Consultants is een adviesbureau voor financiële dienstverleners. Sinds 1998 werken we voor aansprekende Nederlandse en internationale verzekeraars, banken en pensioenfondsen. Deze ervaring combineren we met diepgaande kennis van technologie, wetgeving en digital marketing. Want op dat snijvlak liggen de oplossingen die het verschil maken.

www.itds.nl

OVER IRMA EN IRMACONNECT

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.

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.

Met **IRMAconnect** kan IRMA ook als ontzorgde verificatiedienst worden afgenomen, maar kun je als online dienstverlener ook zelf attributen uitgeven. IRMAconnect is dan de verbindende schakel tussen jouw online dienst(en), je klanten en IRMA.

Partijen die met IRMA werken, zijn: VGZ, ChipSoft, Ivido, HINQ, Gemeente Amsterdam en CIS.
www.sidn.nl/product/IRMAconnect

Meer weten? Neem contact op met:

Bob Kronenburg (SIDN)
bob.kronenburg@sidn.nl
06 31 03 14 23

Maarten Breimer (ITDS)
m.breimer@itds.nl
06 15 68 75 46

Eindnoten

1. https://www.insurancebusinessmag.com/us/news/technology/amazons-entry-into-auto-insurance-holds-valuable-lessons-for-agencies-231940.aspx
2. https://www2.deloitte.com/content/campaigns/uk/insurancetrends/insurancetrends/insurancetrends.html
3. https://www.pwc.nl/nl/actueel-en-publicaties/diensten-en-sectoren/verzekeraars/verzekeraars-gebruiken-technologie-om-dienstverlening-te-verbreden.html
4. https://www.emerce.nl/nieuws/nederlander-meer-grip-persoonlijke-gegevens
5. Zie voor meer achtergronden en bronvermelding: https://www.sidn.nl/nieuws-en-blogs/2021-het-jaar-waarin-respect-voor-privacy-concurrentievoordeel-oplevert
6. https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/
7. https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html