Whitepaper

Zo benut je als verzekeraar de kracht van de nieuwe generatie eID-middelen

IRMA
Powered by SIDN

Inhoudsopgave

Klik op een van de hoofdstukken om direct naar de bijbehorende pagina te gaan.

Inleiding

Vraag jij je weleens af waarom medewerkers van de servicedesk telkens alle persoonsgegevens uitvragen om de identiteit van je klant te bevestigen? Waarom je klanten meerdere accounts moeten aanmaken? Of waarom ze voor elk onderdeel op een andere manier (de ene keer DigiD, dan weer met een gebruikersnaam en wachtwoord) moeten inloggen? Kan dat niet makkelijker? Gelukkig wel.

Een nieuwe generatie eID-middelen is namelijk gebouwd op het principe van Self-Sovereign Identity (SSI). De belofte en kern van deze oplossing? De gebruiker zelf de regie geven over zijn of haar persoonsgegevens. Het resultaat is een win-winsituatie: meer gebruiksgemak voor je klanten en voordelen op het gebied van kosten en beheer voor verzekeraars en financiële dienstverleners.

De beperkingen van traditionele eID-oplossingen

In onze 24 uurseconomie willen klanten elk moment van de dag zaken kunnen doen met een verzekeraar. Een polis inzien op het gewenste moment? In de avond op hun gemak een declaratie afhandelen? Het moet snel en gemakkelijk kunnen, zonder digitale drempels.

Helaas ziet de praktijk er vaak anders uit. De aanvraagprocedure voor een betrekkelijk eenvoudig verzekeringsproduct vereist bijvoorbeeld een hele rits identificatiehandelingen. Of de klant moet voor elk product (levensverzekering, reisverzekering, inboedelverzekering) opnieuw inloggen, ondanks dat hij alle verzekeringen afneemt bij dezelfde verzekeraar. Het komt ook voor dat klanten bij elk telefonisch of mailcontact weer dezelfde ID-gegevens moeten opdreunen of aan de lopende band privacygevoelige documenten zoals paspoorten en ID-kaarten moeten scannen of verzenden.

Veranderende behoeften

Met het toetreden van 'big tech' tot de verzekeringsmarkt, veranderen ook de eisen die klanten stellen aan verzekeraars. Denk bijvoorbeeld aan zogenoemde non-insuranceproducten die een aanvulling vormen op verzekeringen en naadloos aansluiten op de levensstijl van een klant. Een stappenteller bij je zorgverzekering of een veiligheidspakket bij de inboedelverzekering: het zijn zomaar een paar voorbeelden.

We gaan steeds meer toe naar zogenoemde 'service-ecosystemen' rondom thema's als slimme mobiliteit of de woonomgeving van een klant. Tegelijkertijd is er maatschappijbreed sprake van een sterkere nadruk op privacybescherming en compliance met digitale veiligheidsstandaarden. Berichten over datalekken en steeds gehaaidere cybercriminelen voeden de behoefte aan veiligere en robuustere eID-middelen en -processen. Dit geldt voor bedrijven, overheden en individuele burgers. Het voldoen aan beveiligingsstandaarden en allerlei wet- en regelgeving rondom klantendata en financiële informatie brengt hoge kosten met zich mee. Forbes meldt bijvoorbeeld dat in 2018 alleen al Britse bedrijven meer dan 1,1 miljard euro uitgaven aan de voorbereiding op de invoering van de AVG. Logisch, want strengere privacyregels hebben ook de hoogte van boetes voor ondeugdelijk databeheer flink de hoogte ingejaagd.

Een ander aandachtspunt is de consistentie van data. Weet je als verzekeraar zeker dat er niet verschillende versies van datasets door je omgeving zwerven? Kloppen de bankgegevens van je klant nog wel? Zijn eventuele adreswijzigingen of veranderde verzekeringsstatussen in alle systemen geactualiseerd? Heel handig als je dit allemaal weet zonder dat je klanten lastig moet vallen met een reeks telefoontjes en e-mails waarin ze hun ID-informatie voor de zoveelste keer moeten herkauwen.

De oplossing: SSI

De nieuwste generatie SSI-middelen houdt rekening met alle aspecten die we hierboven hebben besproken. SSI stelt de gebruiker in staat om alle relevante attributen op te halen bij de betreffende uitgever. Een BSN-nummer bij de gemeente. Of een rijbewijs bij het CBR. Allemaal geen probleem.

Vervolgens kan de klant al die informatie zelf opslaan en beheren in zijn persoonlijke eID-wallet. Heb je als verzekeraar of financiële instelling een bepaald attribuut nodig van de digitale identiteit van een klant? Dan kan de gebruiker die tonen zonder eerst een uitgebreid verificatieproces te doorlopen. De klant hoeft niet allerlei informatie op te lepelen die irrelevant is voor een bepaalde aanvraag of dienst. Hij heeft bovendien de volledige controle over zijn geverifieerde persoonsgegevens. Hij beheert de informatie zelf en kan attributen individueel uitlezen en doelspecifiek ter beschikking stellen aan online-dienstverleners.

De 3 belangrijkste voordelen van SSI voor verzekeraars

Wat zijn nu de belangrijkste voordelen die SSI-oplossingen hebben voor verzekeraars? We zetten de belangrijkste voor je op een rij.

1. Klanten op betrouwbaarheidsniveau selecteren

Met de nieuwe generatie eID-middelen kun je klanten op elk betrouwbaarheidsniveau identificeren. Zo kun je bijvoorbeeld een KYC-proces ('know your customer') doorlopen om zeker te weten dat een gebruiker gemachtigd is om een zorgverzekering af te sluiten.

Wil een klant deelnemen aan een actie voor branddekens bij een inboedelverzekering, waarvoor de aangesloten leverancier alleen een leveringsadres nodig heeft? Geen probleem. Een SSI-oplossing geeft een klant de mogelijkheid om alleen die informatie op te halen en beschikbaar te stellen. Met een SSI-middel heb je een uniforme oplossing voor alle identificatieprocessen en voldoe je automatisch aan KYC-, privacy- en securitystandaarden.

2. Veiligheid en privacy

Goede SSI-oplossingen sluiten prima aan op het principe van privacy by design. De klant heeft de volledige controle over zijn eigen persoonsgegevens, terwijl verzekeraars niet meer informatie hoeven uit te vragen dan noodzakelijk is voor het leveren van een dienst of product. Je kunt bovendien het systeem gegevens laten uitvragen. Servicemedewerkers hebben dus geen complete profielen meer van een klant als dat niet nodig is. De verificatie van gevoelige informatie vindt namelijk 'onder water' plaats.

Dit verkleint de kans op datalekken. Het decentraal opslaan van gegevens dat gepaard gaat met SSI draagt nog eens extra bij aan het verkleinen van veiligheidsrisico's. Je kunt als verzekeraar ook veel efficiëntere keuzes maken rondom de opslag van gegevens. Gebruik bijvoorbeeld alleen een attribuut als bewijs, zonder de inhoud prijs te geven of op te slaan. Denk aan het attribuut 'ouder dan 18' zonder een geboortedatum te openbaren. Door de verhoogde veiligheid en betrouwbaarheid draag je bij aan je merkwaarde.

3. Je hebt maar één ID-middel nodig

Een belangrijk voordeel van een SSI-oplossing is dat je met één middel meerdere diensten kunt ontsluiten. Dat is prettig voor de eindgebruiker/klant, maar ook voor de verzekeraar. Je kunt de klant in één reis voorzien in zijn behoeften, zonder steeds uitstapjes te hoeven maken naar verschillende middelen.

Daarbij zijn de klantgegevens ook altijd accuraat en actueel, waardoor er minder mis zal gaan in het proces. Het ontsluiten van meerdere diensten met één SSI-middel scheelt verzekeraars bovendien een hoop tijd en geld. Het beheren van klantprofielen en uitvragen van informatie gaat namelijk veel sneller en efficiënter.

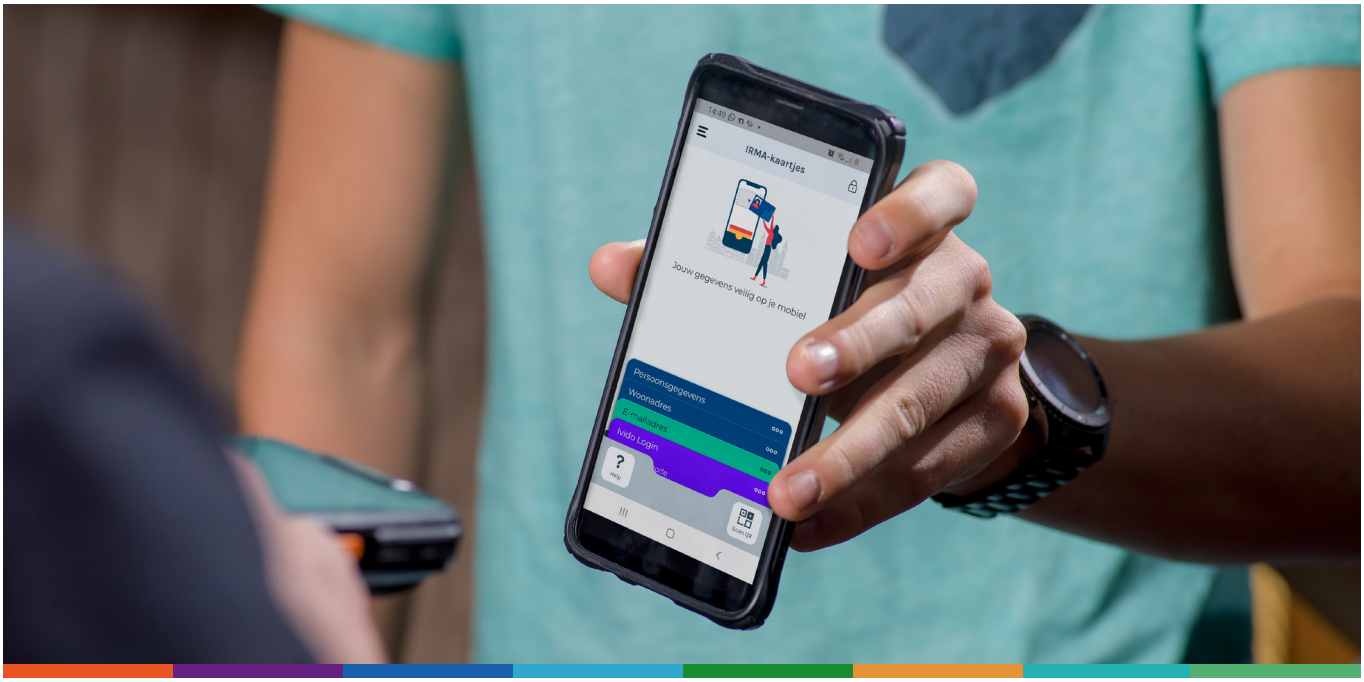
IRMA: jouw digitale paspoort

IRMA (I Reveal My Attributes) is een SSI-oplossing die je in Nederland al kunt gebruiken. Het decentrale platform is open source en bestaat uit twee hoofdcomponenten: de IRMA-app en een stack om zelf IRMA-diensten te ontwikkelen. Desgewenst kun je IRMA ook afnemen als een geheel ontzorgde dienst, via een brokerpartij of rechtstreeks van SIDN. Met de IRMA-app kunnen klanten zelf identiteitskenmerken ophalen via hun smartphone bij gemachtigde partijen als het Basisregister Persoonsgegevens, de Kamer van Koophandel of het 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 mogelijk om met IRMAconnect zelf attributen uit te geven in IRMA. Denk bijvoorbeeld aan een onderwijsinstelling die een diploma als attribuut aanbiedt, of een attribuut dat het aantal schadevrije jaren aangeeft voor een autoverzekering. IRMA is bovendien een oplossing die aansluit op de nieuwe wetgeving (WDO). In de loop van dit jaar zal bekend worden met welke authenticatiemiddelen je in de toekomst kunt inloggen bij zorgverzekeraars. Het goede nieuws: alle signalen staan voor IRMA vooralsnog op groen.

IRMA wordt op dit moment gebruikt in verschillende omgevingen, waaronder ziekenhuizen, patiëntportalen, het onderwijs en de publieke sector. 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 vervolgens zorgdeclaraties kan indienen.



Hoe helpt SIDN?

SIDN, de partij achter .nl, borgt de betrouwbaarheid van IRMA, een ID-oplossing die uitermate geschikt is voor diverse publieke diensten. Met IRMA profiteer je onder meer van de volgende diensten en voordelen:

- Gebruikers krijgen de volledige regie over hun eigen gegevens en privacy. De ID-informatie staat en blijft op hun telefoon en wordt niet beheerd door derde partijen.
- Je controleert eenvoudig een specifiek identiteitskenmerk van een gebruiker, bijvoorbeeld of iemand 18 jaar of ouder is. Het voordeel: je verwerkt als publieke organisatie geen onnodige persoonsgegevens, zoals een geboortedatum of BSN-nummer.
- Belt iemand met IRMA? Dan heeft die persoon zich al geïdentificeerd, waardoor jij geen extra controlevragen meer hoeft te stellen.
- Gebruikers kunnen al hun ID-informatie beheren en aanroepen vanuit één centrale omgeving.
- IRMA is beveiligd met de juiste cryptografische protocollen en ISO-gecertificeerd. De oplossing beantwoordt aan het principe van 'privacy by design' en wordt geregeld op veiligheid getoetst. Hiermee voldoe je als overheidsinstantie makkelijk aan alle Nederlandse regels en wetten op het gebied van privacy- en databescherming. Omdat IRMA open source is, kan bovendien iedereen de broncode bekijken.
- De plannen van de EU voor het creëren van een Europese eID-wallet zijn volledig in lijn met het IRMA-gedachtegoed.
- Inloggen bij de Nederlandse overheid kan, als de WDO van kracht wordt, alleen met inlogmiddelen die open source zijn. Vooralsnog voldoet alleen IRMA aan die eis.
- IRMA is het enige eID-middel dat in Nederland zowel publiek als privaat wordt gebruikt.

Je IRMA-server, het onderhoud en de ondersteuning: SIDN regelt het voor je en ontzorgt jou zo op alle gebieden. SIDN is bovendien onderdeel van een rijk ecosysteem dat diverse uitgevers en aanbieders herbergt. SIDN Business levert ook support voor publieke dienstverleners en verzorgt de implementatie van IRMA.

Meer informatie

Wil je meer weten over de vele mogelijkheden die IRMA biedt voor verzekeraars? Neem dan gerust contact op met SIDN. SIDN borgt de betrouwbaarheid van IRMA als gratis open source platform en levert daarbij betaalde garanties op de open source propositie, zoals een SLA met support of een SaaS-service. Je IRMA-server, het onderhoud en de ondersteuning: wij regelen het voor je en ontzorgen jou zo op alle gebieden.

Team IRMA (SIDN)
support.irma@sidn.nl
+31 (0)26 352 55 55