VERBOND VAN VERZEKERAARS

8 juni 2021

Verzekeraars en digitale identiteit: hoe doorbreken we de impasse?

Advies vanuit de Commissie Digitalisering en SIVI aan het Verbondsbestuur

Samenvatting

Het belang van digitale authenticatie neemt nog altijd toe. Toch is er in Nederland nog geen breed geaccepteerd digitaal authenticatiemiddel dat zowel binnen als buiten het BSN domein bruikbaar is. Het Verbond pleit wel voor het doorontwikkelen van DigiD, zodat het ook buiten het BSN domein ingezet kan worden, maar voorlopig is dit nog niet toegestaan. Het ontwikkelen van een eigen sectoraal middel is ooit overwogen, maar niet haalbaar gebleken: klanten loggen te weinig in bij verzekeraars om dit vlot te trekken. Het is voorts niet raadzaam om op één middel te focussen: het risico van leveranciersafhankelijkheid is te groot en ook zorgt dit voor een single point of failure. Daarom raadt de Commissie Digitalisering de sector aan te kiezen voor een stelsel, waarbij ook voor het niet-BSN domein aangesloten wordt op het publieke stelsel dat de Wet Digitale Overheid over enkele jaren realiseert. Wij gaan er van uit dat eIDAS[1] niveau 'substantieel' de default wordt en een hoger of lager niveau de uitzondering zal zijn.

Nederland is sterk digitaal, maar vertrouwt voor identificatie op 'kopietje paspoort'

De Nederlandse samenleving en economie zijn in hoge mate gedigitaliseerd. De Corona-crisis heeft die digitalisering alleen nog maar verder geholpen, maar ook laten zien dat hele sectoren, waaronder de verzekeringsmarkt, zonder gevolgen voor hun productie konden overschakelen naar 100% thuiswerken. Dat komt natuurlijk doordat de Nederlandse dienstensector sterk ontwikkeld is, maar ook door de bijbehorende goede digitale infrastructuur in Nederland. In schril contrast hiermee vragen veel verzekeraars hun klanten ter identificatie nog regelmatig om een kopie van hun paspoort (of rijbewijs etc.) op te sturen.

Digitale identificatie is in Nederland nog altijd niet goed geregeld. Reden hiervoor is dat de overheid met DigiD wel voor overheidsdienstverleners (het BSN-domein) een inlogmiddel heeft verzorgd, maar het niet verstandig acht om in te grijpen in de private markt op het punt van identificatie. DigiD is wel bruikbaar voor pensioen- en zorgverzekeraars, omdat zij binnen het BSN domein opereren, maar niet voor andere schade- en levensverzekeraars, waardoor klanten voor sommige verzekeringsproducten wel met DigiD kunnen inloggen, maar niet voor andere. Dat is buitengewoon onhandig voor verzekeraars.

Vanwege het gebrek aan overheidsingrijpen buiten het BSN domein, zien we in de private markt verschillende middelen in omloop, waardoor de consument in verwarring raakt en door de bomen het bos niet meer ziet. Dit is menig sector een doorn in het oog. Probleem is dat geen enkele sector voor zich in staat lijkt de consument te bewegen tot adoptie (door de consument) van een sectoraal middel. Verzekeraars zouden graag voor alle producten DigiD gebruiken, maar vooralsnog mag dat niet. De verzekeringssector heeft wel eens overwogen om zelf een digitaal inlogmiddel te ontwikkelen, maar als we zien hoe zelden een klant inlogt bij een

[1] eIDAS: een Europese richtlijn voor Electronic IDentification, Authentication and trust Services

verzekeraar, dan is niet voorstelbaar dat het verzekeraars zou lukken om zoiets van de grond te krijgen.

iDIN

De banken gooien inmiddels hoge ogen met iDIN. Miljoenen Nederlanders beschikken over een inlogmiddel van hun bank. Dat middel is veilig en dankzij IDIN is het nu ook bruikbaar voor niet-bancair inloggen. iDIN functioneert op eIDAS-niveau ‘substantieel’. iDIN wordt inmiddels veel gebruikt in de private sector, ook door grote verzekeraars. iDIN is daarmee een mooi en kansrijk middel. Als iDIN onder de WDO toegelaten wordt als ‘erkend middel’ zal toepassing van iDIN in het overheidsdomein een extra impuls geven aan het gebruik.

Wat moet strategie verzekeringssector zijn?

Wat zou de strategie van de verzekeringssector moeten zijn, waar het gaat om digitale identiteiten? Ten eerste is duidelijk dat de sector inzake DigiD tegen enkele problemen aanloopt. Die problemen adresseerden we voorjaar 2021 in een position paper over DigiD, waarin gepleit wordt voor de ontwikkeling van DigiD zonder BSN. Stel nu dat de overheid DigiD zonder BSN zou ontwikkelen, dan is dat plezierig voor verzekeraars, maar vraag is of klanten altijd met DigiD zullen willen inloggen bij een verzekeraar. Voorts is het de vraag of de sector afhankelijk wil zijn van alleen DigiD (single point of failure). De overheid wil dat in ieder geval niet en probeert met de Wet Digitale Overheid om naast DigiD minstens één extra inlogmiddel te bewerkstelligen, zodat er bij uitval van DigiD altijd een alternatief is om in te loggen bij overheidsdienstverleners. iDIN maakt in deze kans, maar zal vermoedelijk niet het enige toegelaten/erkende middel worden.

De Wet Digitale Overheid (WDO) als kans!

De WDO gaat in het BSN-domein zorgen voor een aantal ‘erkende authenticatiemiddelen’. Binnen dat BSN-domein zullen partijen verplicht zijn om alle erkende middelen te ontsluiten. Dus in het geval dat naast DigiD nog drie middelen erkend worden, dan zullen collectieve pensioenverzekeraars en zorgverzekeraars vier middelen moeten ontsluiten. Dat mag vervelend zijn in bepaalde opzichten, het biedt ook kansen. Het ligt namelijk voor de hand dat niet alle overheden en andere WDO-plichtigen zelf koppelingen gaan leggen met alle authenticatieproviders van erkende middelen. Digital Identity Service Providers (DISP’s) zullen zich opwerpen, om de koppeling te verzorgen met alle middelen in één keer, vergelijkbaar met een Payment Service Provider die voor een webwinkel alle online betaalmethoden ondersteunt. Het zou voor een klant vreemd zijn om voor hun pensioen- en zorgverzekering via zo’n DISP te kunnen kiezen uit een viertal inlogmiddelen, terwijl zij voor hun schade- of levensverzekering die mogelijkheid niet krijgen. Vraag is ook of het zo veel meer kost om de WDO-inlogmiddelen naast de pensioen- en zorgportalen ook voor de andere producten te ontsluiten.

Kijkend naar de stand van zaken, kan gesteld worden dat de ontwikkelingen weliswaar niet snel (genoeg) gaan, maar wel de goede kant op bewegen:

Vraag vanuit perspectief consument	**Ontwikkeling**
Breed inzetbaar middel	Onder WDO komen meerdere authenticatiemiddelen beschikbaar die inzetbaar zijn in private en publieke domein.
Veilig middel, niveau eIDAS substantieel	iDIN is beschikbaar en wordt door grote verzekeraars al toegepast.
Gebruiksvriendelijk	Authenticatiemiddelen zijn gemakkelijk te gebruiken. In toenemende mate komen privacyvriendelijke authenticatiemiddelen beschikbaar.
Twee of meer authenticatiemiddelen	Onder WDO komen meerdere authenticatiemiddelen beschikbaar die inzetbaar zijn in private en publieke domein.

Vraag vanuit perspectief financiële dienstverlener	Ontwikkeling
Breed inzetbaar middel	Onder WDO komen meerdere authenticatiemiddelen beschikbaar die inzetbaar zijn in private en publieke domein. Mogelijk is straks sprake van een geïntegreerd burger- en bedrijfs- en organisatiemiddel. De verzekeringssector loopt hier met de adoptie van eHerkenning voorop.
Veilig middel, eIDAS substantieel	Onder WDO komen meerdere authenticatiemiddelen beschikbaar die inzetbaar zijn in private en publieke domein.
Acceptabele voorspelbare kosten	Bij toenemend hoog volume in gebruik en marktwerking – en dat is de trend – worden kosten lager en zijn deze zonder meer voorspelbaar.
Gebruiksgemak	Authenticatiemiddelen zijn gemakkelijk te gebruiken. In toenemende mate komen privacyvriendelijke authenticatiemiddelen beschikbaar.
Functionaliteit	Doordat authenticatiemiddelen onder de WDO worden toegelaten, ontstaat er gezonde druk op de functionaliteit.

Advies aan Verbondsbestuur

Het advies is dat het Verbond van Verzekeraars haar leden er toe beweegt om de private inlogmiddelen die erkend worden onder de Wet Digitale Overheid ook buiten het BSN domein te gaan ondersteunen. Consumenten krijgen dan met gebruikersvriendelijke en veilige middelen toegang tot zowel overheden als tot hun gegevens bij verzekeraars. Via een Digital Identity Service Provider zijn genoemde middelen eenvoudig te ontsluiten.

eIDAS substantieel als default

We adviseren eIDAS niveau ‘substantieel’ als default te hanteren, omdat dat ook de norm wordt voor inloggen bij de overheid en het de norm is voor inloggen bij de banken. Bij eIDAS niveau substantieel dient een controle plaats te vinden van de opgegeven identiteitsgegevens aan de hand van een fysiek identiteitsbewijs. Dat is een zware controle voor een simple risk schadeverzekering, maar als consumenten middelen aanschaffen op niveau laag, dan kunnen zij daarmee niet inloggen bij diensten op niveau substantieel. Daarom is het beter om uit te gaan van middelen die een substantiële mate van vertrouwen in iemands opgegeven of beweerde identiteit bieden en die breed inzetbaar zijn. Dat voorkomt verwarring aan de kant van consumenten en is goed uit te leggen in termen van beveiliging. Denkbaar is dat voor sommige processen een hoger niveau wenselijk zal zijn. Sowieso zal het voor een klant die zich wil identificeren voor een simple risk schadeverzekering mogelijk moeten blijven om dat op een lager eIDAS niveau te doen. Wij gaan er van uit dat eIDAS niveau ‘substantieel’ de default wordt en een hoger of lager niveau de uitzondering zal zijn.

Gekwalificeerd ondertekenen en hergebruik van authenticatie

Door te koppelen met de aanbieders van private middelen (erkend onder de WDO) komen ook additionele diensten als digitaal ondertekenen en machtigen binnen handbereik. Dat is echter een vervolg op deze fase.

Kosten

Over de kosten van deze koers is op dit moment nog niet veel te zeggen. Voor de consument zijn de kosten nihil of beperkt. Voor dienstverleners zal het sterk afhangen van het aantal keren dat ingelogd wordt.