Juli 2017
Robin Oostrum

Het belang van branche-brede authenticatie

Veranderingen in de wetgeving en nieuwe (informatie)technologieën gaan snel en hebben grote invloed. Niet alleen op de digitale dienstverlening, maar in het bijzonder op de positie van de consument. Bijna iedere aanbieder van online diensten heeft nu een inlogvoorziening voor consumenten in gebruik, die alleen geschikt is voor de eigen online dienstverlening. Hier is winst te behalen.

In deze whitepaper gaat SIVI in op de voordelen van een branchebrede aanpak van authenticatie en identificatie. We willen hiermee de noodzaak van een branchebreed authenticatiemiddel onderstrepen en de bewustwording van de mogelijkheden vergroten. We hoeven niet opnieuw het wiel uit te vinden. Maar alleen als de hele branche meedoet, kunnen we het potentieel van branchebrede authenticatie maximaal benutten.

- Betrouwbare authenticatie is noodzakelijk voor consumenten én aanbieders van online diensten
- Bijna iedere aanbieder van online diensten heeft nu een eigen, achterhaalde inlogvoorziening in gebruik
- Branchebrede authenticatie biedt (meer) veiligheid, betrouwbaarheid, klantvriendelijkheid, efficiëntie, kostenbesparing en dienstverbetering
- Aansluiten gaat eenvoudig via een identiteitsmakelaar

Inhoud

SIVI digitale toekomst verzekerd van standaarden

De waarde van vernieuwing

SIVI ontwikkelt en beheert standaarden voor digitaal zakendoen in de verzekeringsbranche. Onafhankelijk en deskundig. SIVI analyseert trends, onderzoekt de impact van nieuwe technologieën en inspireert alle ketenpartners om samen nieuwe stappen te zetten. Met de ambitie om digitaal verkeer voor de sector en de consument te laten werken. De consument, die steeds hogere eisen stelt aan gemak, zekerheid en veiligheid. En die ‘vertrouwen’ tegenwoordig met hoofdletters schrijft. Het succesvol bedienen van de digitale consument vraagt om de eenduidigheid van standaarden en de inspiratie van nieuwe mogelijkheden.

SIVI, standaard verandering

Introductie

Context
Authenticatie is noodzakelijk voor betrouwbare online dienstverlening. Noodzakelijk voor zowel de consument als de aanbieder van online diensten. De consument wil veilig gebruik maken van online diensten, de aanbieder wil volledige zekerheid over de identiteit van zijn gebruikers.

Bijna elke dienstverlener in de financiële sector heeft op dit moment een eigen inlogvoorziening. Deze is alleen geschikt voor de eigen online dienstverlening. Technologische ontwikkelingen en nieuwe wetgeving gaan snel (zie ook Figuur 2). Het is tijd voor een nieuwe, branchebrede oplossing voor authenticatie.

Die oplossing hoeft de branche niet zelf te bedenken. Initiatieven rond branchebrede authenticatiesystemen ontwikkelen zich snel, in binnen en buitenland. In Nederland zet de overheid in op afsprakenstelsel Idensys als alternatief voor het doorontwikkelde DigiD, de bankwereld komt met iDIN. Ook in Scandinavië, Duitsland en het Verenigd Koninkrijk zien we veelbelovende initiatieven (zie onderstaand kader).

Opzet paper
In deze whitepaper gaat SIVI in op de noodzaak van een branchebreed[i] authenticatiemiddel. Eerst bespreken we kort (de definitie van) authenticatie en identiteiten in het algemeen. Ook het belang van betrouwbare middelen voor zowel consumenten als aanbieders van online diensten komt aan bod. Vervolgens nemen we de huidige situatie onder de loep en bespreken we de voordelen van branchebrede authenticatie. Tot slot volgt de migratie naar een branchebreed authenticatiemiddel en de belangrijkste drempels.

Authenticatie en online identiteiten

Definitie
Authenticatie is het proces dat nagaat of een consument daadwerkelijk is wie hij/zij beweert te zijn. Dat wil zeggen: daadwerkelijk de identiteit bezit die hij/zij opgeeft. Deze vastgestelde identiteit bepaalt of de betreffende consument gerechtigd is om een bepaalde handeling te verrichten of een service af te nemen; deze volgende stap noemen we autorisatie.

Huidige situatie
Bijna iedere financieel dienstverlener heeft nu een eigen online dienstverlening met een eigen authenticatievoorziening. Het belangrijke registratieproces vindt nu meestal plaats bij de financieel dienstverlener zelf. Dit gebeurt als een bestaande of nieuwe klant een verzekeringsproduct afneemt of een bestaande klant toegang wil tot een mijnomgeving.

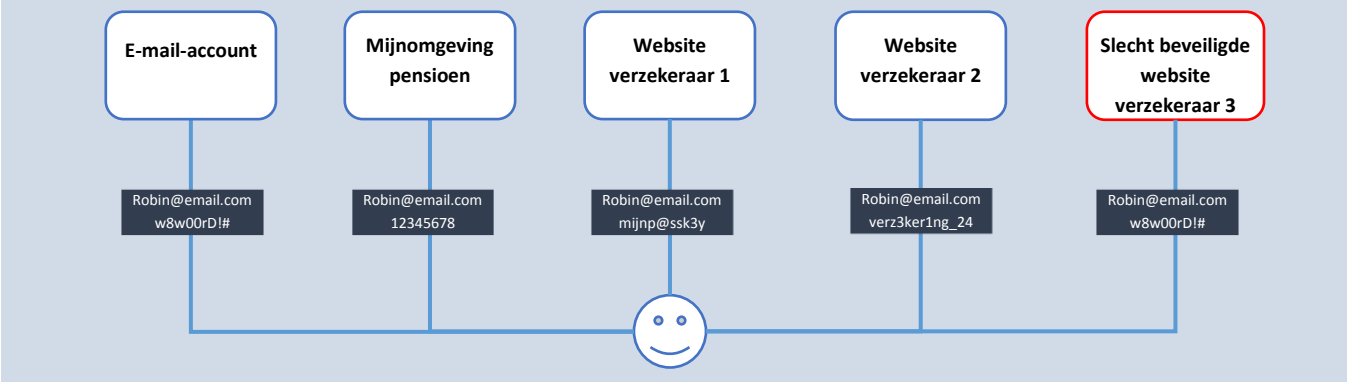
Bij de registratie levert de klant verschillende identificerende gegevens aan zoals een polisnummer bij de verzekeraar. De dienstverlener valideert deze gegevens waarna de consument een nieuw authenticatiemiddel ontvangt. Meestal ontvangt de consument per post of e-mail een wachtwoord, waarmee hij/zij in combinatie met een gebruikersnaam kan inloggen in de digitale omgeving. Een consument beschikt in de praktijk over een veelheid aan inlogaccounts (zie Figuur 1).

Voorbeelden branchebrede authenticatie
Meerdere initiatieven voor branchebrede authenticatie ontplooien zich de laatste jaren in binnen- en buitenland. In Nederland hadden we al eHerkenning en DigiD. Nu zien we een sterke ontwikkeling naar moderne, multi-inzetbare middelen als **Idensys** en **iDIN**. Sinds begin 2016 lopen pilots rondom deze middelen met publieke en private aanbieders van online diensten binnen en buiten de branche.

In het buitenland zien we een zelfde trend. Enkele varianten in nationale identiteitsoplossingen:

- publiek-private samenwerkingen (**BankID** in Noorwegen en Zweden);
- op bestaande **ID-kaarten** gebaseerde inlogmethodes (Duitsland, Estland);
- volledig van de grond af opgebouwde systemen (het Britse **GOV.UK Verify**).

Overigens zijn niet al deze middelen inzetbaar buiten het BSN-domein en toepasbaar in de verzekeringsbranche: zo is GOV.UK Verify alleen te gebruiken bij overheidsdiensten.



Figuur 1: Veelheid aan inlogaccounts consumenten

Belang aanbieder

Een webwinkel wil geen boek opsturen naar iemand die daar niet voor heeft betaald, een verzekeraar wil geen polis van klant X tonen aan klant Y. De aanbieder van online diensten wil dus 100% zekerheid dat achter consument X die bij hem inlogt, ook daadwerkelijk de natuurlijke persoon X zit.

Daar is betrouwbare authenticatie voor nodig in twee stappen: het eenmalige registratieproces (het aanmaken van een account) en de inlogfase. In beide stappen is verificatie van de identiteit van de consument noodzakelijk:

1. Het **registratieproces** controleert of de gegevens in het nieuw aangemaakte account X overeenkomen met de persoonsgegevens van persoon X; dit gaat bijvoorbeeld met een fysieke paspoortcontrole.
2. Heeft persoon X inmiddels een account, dan stelt het systeem in de **inlogfase** vast dat het echt weer persoon X is die doet alsof hij persoon X is; dit gaat met inlogmiddelen als gebruikersnaam/wachtwoord, bankkaarten enzovoort.

Betrouwbare authenticatie is alleen mogelijk wanneer zowel het registratieproces als de inlogfase volledig betrouwbaar verlopen.

Belang consument

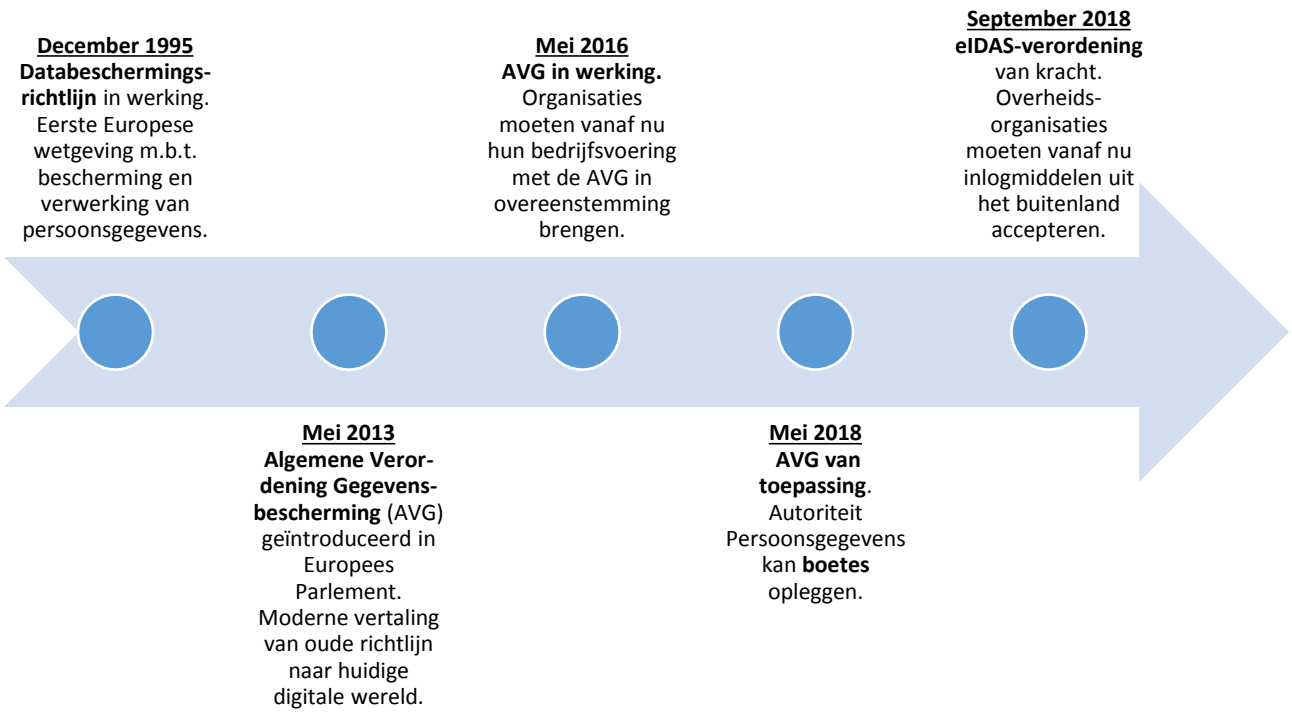
Een consument vindt vooral privacy, veiligheid en gebruiksgemak belangrijk. Steeds meer online-omgevingen (voor bijvoorbeeld verzekeringen, zorginstellingen en overheidsdiensten) maken gebruik van persoonlijke gegevens. Veilige toegang is hierbij noodzakelijk. De consument wil bijvoorbeeld niet dat de verzekeraar toegang heeft tot medische gegevens of belastingaangiftes, zonder dat hij/zij daar zelf uitdrukkelijk toestemming voor geeft.

Voordelen

Veilig

De huidige ieder-voor-zich-systemen zorgen voor veel veiligheidsissues. Branchebrede authenticatie biedt de volgende verbeteringen:

1. Wachtwoorden worden sterker. Consumenten moeten nu gebruikersnaam-en-wachtwoord-combinaties onthouden voor alle afzonderlijke systemen (zie Figuur 1). Daarom gebruikt hij vaak eenvoudigere wachtwoorden en/of hetzelfde wachtwoord op meerdere websites. Nog waarschijnlijker is dat hij dezelfde gebruikersnaam gebruikt op een groot deel van deze websites. Een hack van het e-mailaccount is dan genoeg om toegang te krijgen tot alle wachtwoorden. Met branchebrede authenticatie hoeven consumenten nog maar één i.p.v. tientallen wachtwoorden te onthouden. Dit vergroot de kans op een sterk wachtwoord. Hoe ingewikkelder/langer het wachtwoord, hoe moeilijker dit te “raden” is door een hacker.
2. Wachtwoorden blijven eenvoudiger geheim. Het is niet langer nodig om lijsten met wachtwoorden on- en offline op te slaan. Eén wachtwoord onthouden is genoeg. Dit vermijdt een groot veiligheidsrisico.
3. Het authenticatieproces wordt veiliger. Veel huidige systemen bleken kwetsbaar (zoals DigiD) en/of gebruiken verouderde inlogmethodes. Gebruikersnaam en wachtwoord voldoen niet langer aan de hoogste veiligheidseisen. Tweefactorauthenticatie[ii] en het gebruik van beveiligde verbindingen zijn noodzakelijk. Een grote, achtenswaardige partij (bijvoorbeeld de overheid, bankenwereld of Google) zal bij branchebrede authenticatie de inlogmiddelen en systemen leveren. Dit soort partijen beschikken over kennis, geld en middelen om significant sterke security tot stand te brengen.



Figuur 2: Tijdlijn van relevante wetgeving m.b.t. verwerking persoonsgegevens

Klantvriendelijk

De "digitale sleutelbos" wordt kleiner of verdwijnt. De consument moet nu een grote hoeveelheid aan gebruikersnamen en wachtwoorden onthouden. Een branchebrede aanpak leidt tot één sleutel: één middel waarmee de consument overal kan inloggen.

In het ideale geval bevat de branchebrede authenticatie ook *single sign-on*. Dit houdt in dat de consument niet voor elke omgeving opnieuw hoeft in te loggen. Hij blijft na één authenticatie ingelogd wanneer hij van de ene website naar de andere schakelt. Dit maakt het gebruik van online diensten laagdrempeliger.

Efficiënt

Aanbieders van online diensten hoeven niet langer zelf parafernalia aan certificaten, inlogmiddelen en lijsten met vertrouwde instanties bij te houden. Met andere woorden: de overstap op branchebrede authenticatie koppelt het authenticatieproces los van de aanbieders van online diensten. Dit verhoogt de efficiëntie t.o.v. eigen authenticatiesystemen. In de offlinewereld is dit al gebruikelijk. Burgers halen hun paspoort bij de overheid en authenticeren zich hier vervolgens mee aan de kassa van de wijnhandel. De wijnhandel vertrouwt het – door een externe partij verstrekte – paspoort als geldig middel. Dit scheelt de wijnhandel geld en tijd.

Lagere kosten (op termijn)

Een externe authenticatievoorziening leidt tot kostenbesparing voor aanbieders van online diensten:

- geen beheer van online identiteiten;
- geen investeringen in gebruikersondersteuning;
- onderling verdelen van kosten voor onderzoek en doorontwikkeling;
- reductie van het aantal helpdeskverzoeken gerelateerd aan (verloren) gebruikersnamen/wachtwoorden.

De kosten voor het migreren naar een branchebreed systeem komen later in deze paper aan bod. Onderzoek wijst uit dat op termijn branchebrede authenticatie tot lagere kosten leidt dan gebruikmaken van eigen middelen.

Betrouwbaar

De betrouwbaarheid van de authenticerende consument gaat omhoog. De besproken veiligheidsvoordelen van branchebrede authenticatie leiden er ook toe dat de kans op identiteitsdiefstal, fraude en privacyschending afneemt.

Tweefactorauthenticatie maakt het lastiger voor oplichter Y om zich voor te doen als consument X. De aanbieder van online diensten kan er dan van uitgaan dat online consument X ook daadwerkelijk persoon X is en niet oplichter Y.

Betere dienstverlening

Als we meer diensten kunnen digitaliseren, kan dit leiden tot betere dienstverlening aan consumenten. Denk hierbij aan gerichter klantadvies. De aanbieder van online diensten beschikt over gevalideerde gegevens van de consument. Bovendien leidt meer digitalisering tot een actueler, toegankelijker en eenvoudiger te koppelen aanbod van informatie. Een sterk, breed uitgerold authenticatiesysteem is hiervoor noodzakelijk.

Overstappen en aansluiten

Introductie

Drie belangrijke aandachtspunten bij de overstap naar / het aansluiten op branchebrede authenticatie:

1. Hoe verloopt de overstap van de huidige systemen naar één branchebreed authenticatiesysteem?
2. Welke kosten zijn daaraan verbonden?
3. Hoe voorkom je dat er een wildgroei aan authenticatiemiddelen ontstaat? Aanbieders van online diensten moeten niet met allerlei partijen afzonderlijk contracten en technische implementaties regelen.

Identiteitsmakelaars

Voor mogelijke wildgroei aan authenticatiemiddelen bestaat een oplossing: de identiteitsmakelaar. Een identiteitsmakelaar sluit de aanbieder van online diensten aan op één of meer authenticatiediensten. Hij vormt aan de kant van de consument een soort portaal tussen hem en de mogelijke inlogmiddelen. Bijkomend voordeel is een eenvoudige implementatie van nieuwe (branchebrede) authenticatiemiddelen via de identiteitsmakelaar. Bovendien zorgt de toename van het aantal identiteitsmakelaars voor concurrentie: dit zal de aansluitkosten drukken. Voorbeelden van identiteitsmakelaars zijn Signicat[iii] en het Nederlandse Digidentity[iv].

Figuur 3 geeft het gebruik van een identiteitsmakelaar weer bij branchebrede authenticatie. De consument hoeft minder inloggegevens te onthouden. Daarnaast is een slecht beveiligde website of kwaadwillende partij niet direct fataal. De consument stuurt zijn inlogmiddelen namelijk alleen naar de identiteitsmakelaar.

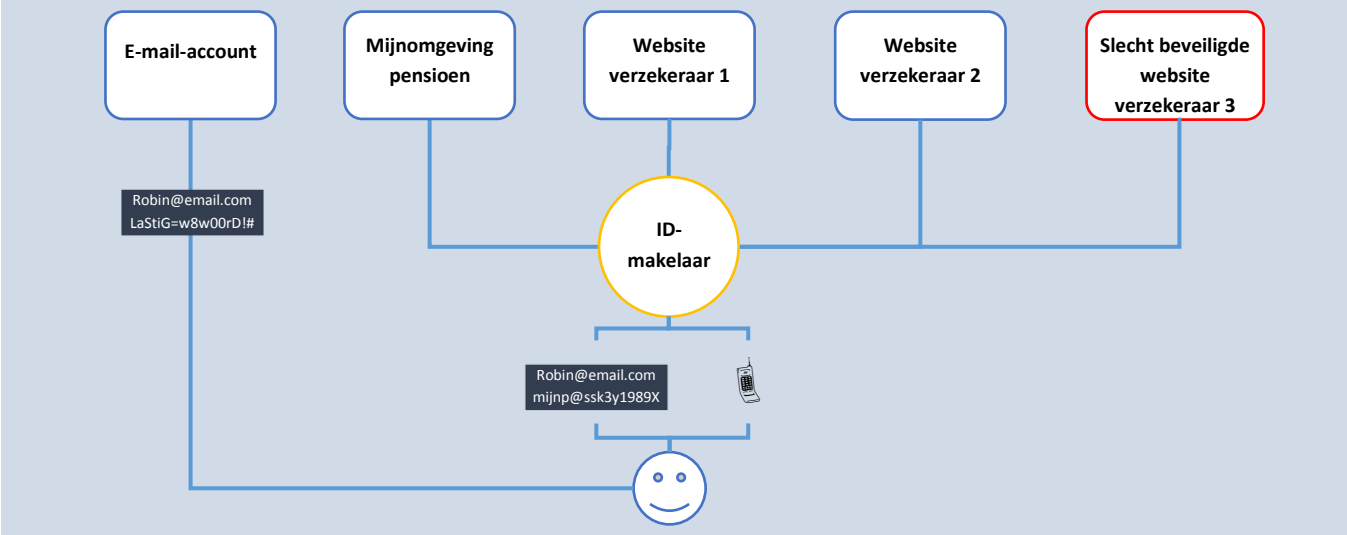
Kosten

In opdracht van de overheid stelde Ecorys een rapport[v] op met de kosten en baten van het eID-stelsel. Dit rapport richt zich specifiek op een overheidsinitiatief, maar sommige bevindingen en conclusies gelden breder. Het rapport onderscheidt vijf verschillende kostensoorten bij het invoeren van een nieuw, landelijk authenticatiestelsel. Twee kostensoorten zijn relevant voor de private aanbieder van online diensten:

1. **Investeringskosten**: eenmalige kosten voor toezicht & beheer in de authenticatiedienst en aansluitkosten voor aanbieders van online diensten.
2. **Variabele kosten gebruik**: de kosten per transactie. Deze zijn afhankelijk van het aantal authenticaties en gebruik.

Beide kostenposten zijn afhankelijk van het betreffende authenticatiemiddel. Waarschijnlijk sluit de aanbieder van online diensten een jaarcontract met een identiteitsmakelaar met daarin de vaste en variabele kosten. Dat is bijvoorbeeld ook de huidige situatie met eHerkenning[vi] (het zakelijke inlogmiddel bij overheidsdiensten). Jaarcontracten kosten tussen €5,95 en €45 afhankelijk van het betrouwbaarheidsniveau. Andere aanbieders vragen bijvoorbeeld €5 per 20 authenticatie-sms'jes.

Een ander voorbeeld is iDEAL. De meeste banken maken nog gebruik van maandabonnementen, maar tegenwoordig zijn er ook aanbieders die alleen transactiekosten rekenen. De goedkoopste aanbieder vraagt op dit moment 19 cent per iDEAL-transactie[vii]. Daarbij is de trend dat de transactiekosten dalen als meer mensen gebruikmaken van iDEAL.



Figuur 3: Branchebrede authenticatie via een identiteitsmakelaar

Koppeling bestaand systeem

Veel financieel dienstverleners hebben al een onlineplatform met een eigen authenticatiesysteem. Dit succesvol vervangen door een nieuw, branchebreed authenticatiemiddel vereist een zorgvuldige eenmalige koppeling tussen intern bekende gegevens en inloggende consumenten. Hier zijn twee opties voor:

1. Bij de authenticatie attributen mee laten sturen die de inloggende consument kunnen identificeren. Denk bijvoorbeeld aan een combinatie van volledige naam, NAW-gegevens, geslacht en geboortedatum.
2. De consument eerst in laten loggen met het oude systeem. Vervolgens authenticeert de ingelogde consument zich met behulp van het nieuwe, branchebrede authenticatiemiddel. Zo ontstaat een link tussen de intern bekende gebruiker en het nieuwe middel. Mijnverzekeringenopeenrij (zie kader op vorige pagina) gebruikt een dergelijke *nested login*. Het branchebrede authenticatiemiddel biedt extra attributen van de consument en verifieert eerder ingevulde attributen van de consument.

Conclusie

Voordelen overheersen

De overstap naar nieuwe, veilige branchebrede authenticatie levert veel voordelen op voor consumenten en aanbieders van online diensten (zie ook de samenvattende Figuur 4). Het biedt daarnaast mogelijkheden om meer diensten te digitaliseren en de dienstverlening verder te verbeteren.

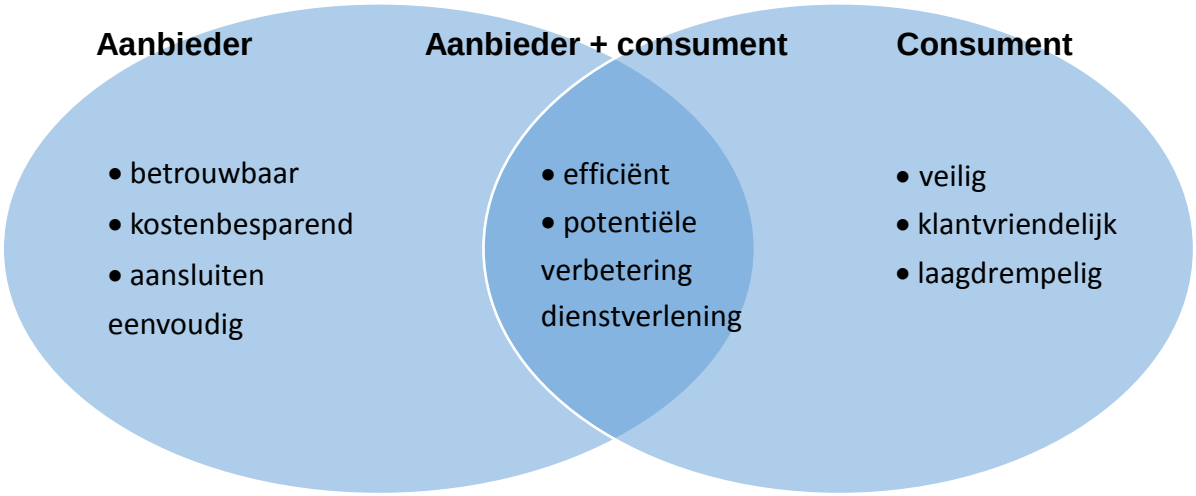
Vanzelfsprekend zijn er nieuwe kosten verbonden aan het aansluiten op een branchebreed middel. Daarentegen verdwijnen onderhouds-, beheer- en helpdeskkosten grotendeels met het uit handen geven van de directe implementatie aan een identiteitsmakelaar. Wel moeten aanbieders van online diensten gegevens koppelen voor het migreren naar een systeem met branchebrede authenticatie. Dit vereist resources en kosten, maar levert ook betrouwbaardere en potentieel uitgebreidere klantidentiteiten op.

Een belangrijke vraag die opkomt bij branchebrede authenticatie is die van een vertrouwde derde partij. Wie neemt het initiatief voor de uitgifte en het beheer van nieuwe middelen? Is er voldoende *governance* om de identiteitsmakelaars te reguleren? En hoe voorkomen we dat er privacy-hotspots ontstaan bij deze nieuwe partijen in het authenticatiestelsel? Vragen die we per geval moeten beantwoorden en los staan van branchebrede authenticatie in de brede scope van deze paper. Het overheidsinitiatief Idensys heeft andere voor- en nadelen dan het bancaire middel iDIN. Voor nu is het vooral zaak om vooruit te denken en de overstap doelbewust te gaan verkennen.

Samen optrekken

We hoeven het wiel niet opnieuw uit te vinden. De ontwikkeling van branchebreed inzetbare authenticatiemiddelen loopt voortvarend. Identiteitsmakelaars regelen de aansluiting op de middelen, maar de branche moet zich nu samen sterk maken om dergelijke aansluitingen te realiseren. Alleen als iedereen meedoet, kunnen we het potentieel van branchebrede authenticatie maximaal benutten.

SIVI maakt zich daar de komende periode sterk voor. Daarvoor gaan we met zowel leveranciers als dienstaanbieders uit de branche in gesprek om de noodzaak verder toe te lichten en de verschillende mogelijkheden inzichtelijk te maken. Met whitepapers over specifieke oplossingen als iDIN, Idensys, NotarisID en de afwegingen daartussen leveren we een concrete bijdrage aan de overstap naar een branchebreed authenticatiemiddel.



Figuur 4: Voordelen van branchebrede authenticatie voor aanbieders en consumenten

[i] 'Branchebreed' betekent bijna overal 'minstens branchebreed', omdat ook partijen buiten de verzekeringsbranche de meeste authenticatiemiddelen kunnen en zullen toepassen.
[ii] Tweefactorauthenticatie houdt in dat de consument niet alleen inlogt met iets dat hij *weet* (gebruikersnaam, wachtwoord), maar ook met iets dat hij *heeft* (smartcard, TAN-codes, mobiele app) of iets dat hij *is* (vingerafdruk, irisscan).
[iii] https://www.signicat.com/
[iv] http://digidentity.eu/nl/home/
[v] Rijksoverheid, Rapport 'Businesscase Inloggen in het BSN domein', 9 november 2016 - https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2016/11/09/rapport-businesscase-inloggen-in-het-bsn-domein/rapport-businesscase-inloggen-in-het-bsn-domein.pdf, geraadpleegd op 1-3-2017.
[vi] https://www.eherkenning.nl/inloggen-met-eherkenning/leveranciers/leveranciersoverzicht/, geraadpleegd op 1-3-2017.
[vii] Wat kost iDeal voor je webshop? Anno 2017 - https://elephantcs.nl/blog/wat-kost-ideal-voor-je-webshop/, geraadpleegd op 27-3-2017.

Voor vragen en reacties

Robin Oostrum
06-53398893
Robin.Oostrum@sivi.org