Augustus 2017
Robin Oostrum

Idensys

Drempels en succesfactoren van afsprakenstelsel vanuit overheid

Op dit moment heeft bijna iedere financieel dienstverlener een eigen inlogvoorziening voor zijn klanten in gebruik. Deze is alleen geschikt voor de eigen online dienstverlening. Veel winst is te behalen met een branchebrede aanpak van authenticatie en identificatie. Deze whitepaper bespreekt de succesfactoren en drempels van Idensys.

Idensys maakt branchebreed (en –overstijgend) inzetbare authenticatiemiddelen mogelijk. Idensys is een afsprakenstelsel op initiatief van de overheid, in samenwerking met marktpartijen. Idensys is dus geen inlogmiddel op zich. Met op Idensys gebaseerde authenticatiemiddelen kunnen gebruikers veilig inloggen bij overheidsdiensten, maar ook bij private instanties als verzekeringsmaatschappijen en webwinkels. Aanbieders van online diensten krijgen dankzij de hogere betrouwbaarheidsniveaus meer zekerheid over de identiteit van de klant.

De eerste pilots wijzen inmiddels op een redelijke acceptatiegraad voor zowel consumenten als aanbieders van online diensten.

- Idensys is een afsprakenstelsel van de Nederlandse overheid; (private) partijen mogen zélf authenticatiemiddelen aanbieden die hieraan voldoen
- Met deze authenticatiemiddelen kunnen consumenten inloggen bij zowel publieke als private aanbieders van online diensten
- Dit leidt tot verschillende soorten middelen, variërend van inlogcodes via apps tot sms-verificatie en selfie-checks
- Aansluiten op Idensys is eenvoudig via een identiteitsmakelaar
- Uitdagingen bestaan vooralsnog vooral rond het BSN-koppelregister en koppeling aan interne klantenbestand

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

Ruim 13 miljoen Nederlanders maken gebruik van DigiD, waarmee ze bij meer dan 600 organisaties online overheidszaken kunnen regelen[i]. Maar de overheid ziet in[ii] dat DigiD “niet meer veilig genoeg” is voor alle toepassingen en werkt aan een toekomstbestendige oplossing.

Naast de doorontwikkeling van DigiD – de lage betrouwbaarheidsniveaus worden geschrapt – kiest de overheid daarbij voor een *multimiddelenstrategie.* Daarin is naast (het publieke) DigiD ook ruimte voor private inlogmiddelen, met hogere betrouwbaarheidsniveaus: zie het kader op pagina 3. Aanvankelijk ontwikkeld onder de noemer eID-stelsel heeft dit project nu de naam Idensys. Of, in de eigen woorden van de website van Idensys[iii]: “Met Idensys kun je je veilig en eenvoudig online identificeren. Het grote gemak is dat je met één middel bij meerdere instanties kunt inloggen.”

Afsprakenstelsel Elektronische Toegangsdiensten

Het Ministerie van Economische Zaken ontwikkelde Idensys met een *publiek-private governance* als uitgangspunt. Dat wil zeggen dat inspraak, beheer en bestuur geregeld zijn op basis van een samenwerking tussen overheid, bedrijfsleven en consumenten. Concrete afspraken over beheer, ontwikkeling, functionaliteiten, beveiliging en privacy zijn vastgelegd in het Afsprakenstelsel Elektronische Toegangsdiensten.

Meer info: https://afsprakenstelsel.etoegang.nl/

Opzet paper

Deze whitepaper geeft inzicht in Idensys: wat is Idensys, hoe sluit mijn organisatie zich erbij aan en wat zijn de belangrijkste voor- en nadelen? We onderzoeken de succesfactoren en drempels van Idensys. Dit geeft inzicht in de mogelijkheden van Idensys in het perspectief van branchebrede authenticatie.

Relevante publicaties

In deze whitepaper veronderstellen we een zekere basiskennis met betrekking tot authenticatie. Voor meer informatie over authenticatie, online identiteiten en het belang van een branchebrede oplossing verwijzen we naar de whitepaper die SIVI eerder publiceerde onder de titel ‘Het belang van branchebrede authenticatie’. Ook verscheen van SIVI een paper over de drempels en succesfactoren van iDIN, het door de banken ontwikkelde authenticatiemiddel. Beide papers zijn hier te vinden.

Wat is Idensys?

Meerdere betrouwbaarheidsniveaus

Inloggen met een Idensys-middel[iv] is vergelijkbaar met inloggen via DigiD. Net als bij DigiD is er onderscheid tussen verschillende betrouwbaarheidsniveaus (zie kader op pagina 3). Voor inloggen op een laag betrouwbaarheidsniveau zijn de registratie- en verificatieprocedures minder uitgebreid dan op hogere niveaus. Bij een hoger niveau vinden er tijdens het aanvraagproces meer checks plaats om de identiteit van de consument vast te stellen. Bijvoorbeeld door een face-to-face-check met een identiteitsbewijs. Anderzijds zit de betrouwbaarheid in het type inlogmiddel. De hogere niveaus vereisen daarom altijd tweefactorauthenticatie: naast gebruikersnaam en wachtwoord ook een extra stap als inlogcode of sms. De precieze eisen hangen af van de betreffende authenticatiedienst. Figuur 1 geeft schematisch het inlogproces weer.

Inlogvoorbeeld Belastingdienst

Op de website van de Belastingdienst loopt een pilot waardoor het nu ook mogelijk is om – naast het bekende DigiD – via iDIN of Idensys in te loggen. Na het kiezen voor Idensys komt de consument terecht in een keuzescherm waar ook het vereiste betrouwbaarheidsniveau (niveau 3 in het voorbeeld van de Belastingdienst) staat vermeld. De consument selecteert de authenticatiedienst van zijn voorkeur, bijvoorbeeld KPN. Hij klikt op ‘Verder’ en krijgt een inlogscherm te zien waar hij zijn gebruikersnaam en wachtwoord invoert, die hij in een eerder stadium bij KPN heeft aangemaakt. Hij klikt op ‘Verder gaan’ en krijgt nu, bij een juiste combinatie van gebruikersnaam en wachtwoord, een sms toegestuurd. Hij vult de sms-code in en klikt op ‘Verder gaan’, waarna hij succesvol geauthenticeerd is en ingelogd terugkeert naar de omgeving van de Belastingdienst.

Geen toepassing maar afsprakenstelsel

Daarin zit ook meteen een belangrijk verschil met DigiD. Idensys is namelijk niet één toepassing of authenticatiemiddel, maar een afsprakenstelsel. Elke erkende[v] private partij kan vervolgens authenticatiemiddelen ontwikkelen die hieraan voldoen. De consument kiest bij Idensys zelf een inlogmethode: bijvoorbeeld met mobiele app, met wachtwoord + sms of via gezichtsherkenning op een smartphone. Ook aanbieders van online diensten hebben de vrijheid om zelf een

identiteitsmakelaar te kiezen. De consument maakt een account aan bij de authenticatiedienst van zijn/haar voorkeur en logt hier voortaan mee in, onder de noemer van Idensys. Zie voor meer informatie over het afsprakenstelsel ook het kader over het Afsprakenstelsel Elektronische Toegangsdiensten hierboven, en Figuur 2 voor de rolverdeling binnen het netwerk.

Geen bestaande middelen

Omdat Idensys geen gebruik maakt van al bestaande middelen, dient de gebruiker eerst een middel te kiezen en zich eenmalig te registreren. Voor het aanmaken van een Idensys-account moet de gebruiker zich identificeren met een vertrouwd bestaand middel zoals een paspoort in combinatie met bankrekening. Het verifiëren van een bankrekening kan bijvoorbeeld door middel van 1-cent-transacties via iDEAL.

Wat krijgt de aanbieder van online diensten via Idensys van de consument?

Wanneer een consument succesvol inlogt via Idensys, krijgt de aanbieder van online diensten twee soorten informatie en een uniek identificatiemiddel:

1. **Authenticatie** van de consument: persoon X is inderdaad persoon X.
2. Een **pseudoniem** van de consument: code die uniek is voor iedere combinatie tussen consument, authenticatiedienst en aanbieder van online diensten. Dit pseudoniem[vi] blijft over alle authenticaties gelijk, zolang de consument voor Idensys-authenticaties van dezelfde authenticatiedienst gebruik blijft maken. Zo kan de aanbieder van online diensten de consument uniek identificeren. Aanbieders van online diensten die daartoe gerechtigd zijn, ontvangen het **BSN** in plaats van een pseudoniem.
3. **Attributen** van de consument: de aanbieder van online diensten kan van de consument gegevens opvragen via Idensys. Het gaat daarbij om voorletter(s), achternaam, woonadres, leeftijdsindicatie (“minstens 18 jaar?”), geboortedatum en/of geslacht. De overheid heeft deze attributen in een eerder stadium gevalideerd, wat ze zeer betrouwbaar maakt. De consument moet voor het delen van deze gegevens altijd nadrukkelijk toestemming geven tijdens het inlogproces via Idensys.

Betrouwbaarheidsniveaus

Idensys maakt onderscheid tussen vier betrouwbaarheidsniveaus, oplopend van 2 (laag) tot 4 (hoog). Bij diensten in het publieke domein (de overheid, maar ook zorg- en pensioenverzekeraars) kan alleen worden ingelogd op niveau 3 of 4: de gebruiker moet daarin meerdere stappen ondernemen om zich te authenticeren. Bij bepaalde commerciële organisaties, zoals webwinkels, is het mogelijk om al vanaf niveau 2+ in te loggen.

Een overzicht van de verschillende betrouwbaarheidsniveaus en bijbehorende authenticatie- en registratie-eisen:

Niveau	Registratie	Authenticatie
2	online + post	gn + ww
2+	online + post	gn + ww + sms/app
3	online	gn + ww + sms/app
4	face-to-face	pki-smartcard

(gn = gebruikersnaam, ww = wachtwoord, pki = public key-certificaat)

eIDAS

Aanbieders van online diensten bepalen zelf het minimale betrouwbaarheidsniveau, afhankelijk van de risico’s. Overheidsinstanties moeten daarbij voldoen aan de Europese eIDAS-verordening. Idensys voldoet hieraan. Met andere woorden: aansluiten via Idensys leidt direct tot compliance met de eIDAS-verordening. De betrouwbaarheidsniveaus van Idensys matchen als volgt met die van het eIDAS-framework:

Idensys	eIDAS
2	laag
2+	laag
3	substantieel
4	hoog

Meer informatie over eIDAS op de website van Idensys: https://www.idensys.nl/idensys-voor-organisaties/eidas/

Merk op dat Idensys-middelen alleen het BSN aanleveren als de aanbieder van online diensten bevoegd is deze te verwerken. Zie het kader op pagina 6 voor hoe Idensys dit voor rechthebbende partijen oplost via het BSN-koppelregister.

Implementatie

Aansluiten

Een aanbieder van online diensten kan aansluiten op Idensys via een identiteitsmakelaar (de “herkenningsmakelaar” in Idensys-terminologie). Aanbieders van online diensten kunnen niet rechtstreeks bij een afzonderlijke authenticatiedienst aansluiten. Overigens zijn de meeste authenticatiediensten ook identiteitsmakelaar en vice versa.

Aansluiten bij zo'n makelaar gaat eenvoudig. De aanbieder van online diensten sluit een contract af met een beschikbare aanbieder van Idensys (op https://www.idensys.nl/idensys-voor-organisaties/direct-aansluiten/ staat een actueel overzicht van erkende identiteitsmakelaars). De identiteitsmakelaar zorgt voor de koppeling met alle authenticatiemiddelen van Idensys, en implementeert een module op de website van de aanbieder van online diensten. Hierin kan de consument kiezen tussen alle inlogmiddelen van Idensys.

Identiteitsmakelaars bieden de volgende voordelen voor de aanbieder van online diensten:

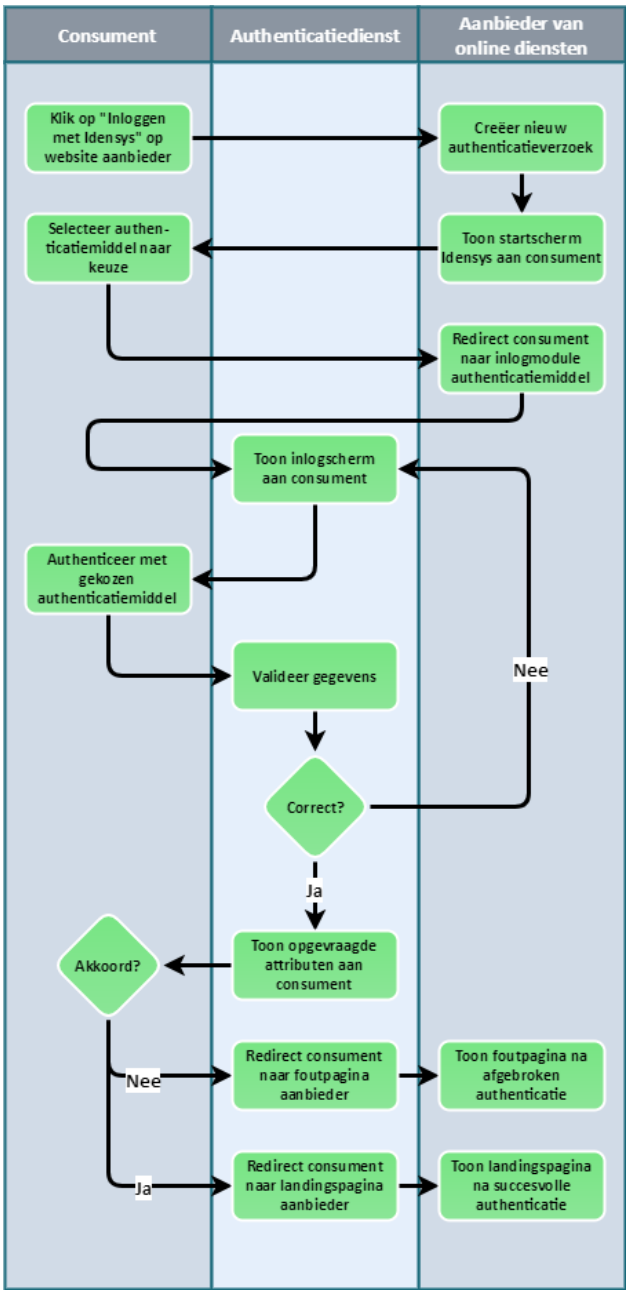
- de identiteitsmakelaar regelt foutafhandeling, helpdesk etc.;
- er is altijd een vangnet van andere inlogmiddelen in het geval dat één van de authenticatiediensten niet beschikbaar is.

Zie de whitepaper 'Het belang van branchebrede authenticatie' voor meer uitleg over identiteitsmakelaars.

Koppelen huidig systeem aan Idensys

De aanbieder van online diensten moet een koppeling maken tussen Idensys en het eigen klantenbestand. Voorheen logde iemand in met gebruikersnaam en wachtwoord, maar Idensys levert andere gegevens. Toch moet ook een met Idensys inloggende consument in zijn/haar eigen omgeving terechtkomen. Daar is een koppeling tussen de oude en nieuwe situatie voor vereist.

Wanneer een consument voor het eerst inlogt via Idensys, moet de aanbieder van online diensten een *match* maken tussen binnenkomende attributen (naam, adres, leeftijd, geslacht en dergelijke) en intern bekende gegevens. Dit matchen hoeft maar éénmalig. Als een inloggende Idensys-gebruiker gekoppeld is aan de interne database, slaat het systeem het meegeleverde pseudoniem op. Dit pseudoniem is uniek voor de link tussen consument en aanbieder van online diensten. De authenticatiedienst maakt het pseudoniem aan bij de eerste authenticatie. Het blijft daarna gelijk over meerdere authenticaties – zolang de consument voor Idensys van dezelfde authenticatiedienst gebruik blijft maken.



Figuur 1: Gesimplificeerde flowchart van het authenticatieproces in Idensys.

Kosten en resources

Aansluitkosten

De exacte voorwaarden van de identiteitsmakelaars zijn op dit moment nog niet bekend. We verwachten geen aansluitkosten voor Idensys, maar alleen een transactieprijs. Voor de aansluiting zijn wel resources nodig. Deze zetten we in de volgende paragraaf uiteen.

Resources

Aansluiten op Idensys vereist resources. Deze kunnen we globaal opsplitsen in drie aandachtspunten:

1. Het **koppelen** van consumenten aan de interne klantadministratie. Zie voor meer informatie de paragraaf 'Koppelen huidig systeem aan Idensys'.

2. De **technische realisatie** van de overstap op Idensys. Denk aan het aanroepen van de authenticatiemodules, alternatieven als Idensys-middelen niet beschikbaar zijn, enzovoort.
3. Het realiseren van concrete **inlogmodules**. Dit neemt de identiteitsmakelaar grotendeels op zich. De aanbieder van online diensten moet zaken regelen als een knop op de website die naar de authenticatiedienst doorstuurt, eventuele apps aanpassen, enzovoort.

De verdeling qua belasting van deze resources is afhankelijk van het soort financieel dienstverlener. De één zal vooral tijd en geld kwijt zijn aan het koppelen (punt 1). Dit geldt bijvoorbeeld voor partijen met een grote klantendatabase. Voor anderen is het belangrijker dat de website functioneert, en/of dat er voldoende maatregelen zijn getroffen wanneer inloggen via Idensys niet mogelijk is. Deze partijen zullen vooral resources kwijt zijn aan de technische kant (punt 2).

Inlogmiddelen

Idensys maakt – in tegenstelling tot bijvoorbeeld iDIN – geen gebruik van bestaande inlogmiddelen. De kosten voor de inlogmiddelen zijn vermoedelijk inbegrepen in het contract tussen de aanbieder van online diensten en de identiteitsmakelaar, maar een precieze uitwerking hiervan ontbreekt vooralsnog.

Kosten per authenticatie

SEO Economisch Onderzoek adviseerde in een rapport[vii] uit 2015 al transactieprijzen van 2,4 en 11 eurocent op respectievelijk niveau ‘laag’ en ‘hoog’. Dit rapport dateert echter nog uit de tijd vóór er sprake was van vier betrouwbaarheidsniveaus – laat staan de naam Idensys. Verder baseert het model van SEO zich op gunstige aannames, en houdt het bijvoorbeeld geen rekening met concurrerende initiatieven als iDIN.

Een recenter rapport[viii] uit september 2016 van de Algemene Rekenkamer is minder positief. Zij stelt dat zolang een actuele integrale business case ontbreekt, de kosten en inrichting van het Idensys-stelsel onduidelijk zullen blijven.

Als inschatting kijken we naar de transactiekosten van DigiD. Die zijn, dankzij het fors toegenomen gebruik, in tien jaar tijd gedaald van €3,50 naar circa 10 cent[ix] per transactie. Het is aannemelijk dat Idensys bij ingebruikname meer deelnemers heeft dan DigiD in haar beginjaren. De kosten per authenticatie zullen straks dan ook dichter bij dat laatste bedrag liggen dan bij de aanvankelijke prijs, maar dit is afhankelijk van de makelaars.

Gebruiksgemak

Als onderdeel van de eerste pilots is er een consumentenonderzoek uitgevoerd. Daarbij gaf 91% van de 172 respondenten aan Idensys vaker te willen gebruiken en gaf 90% een positief oordeel over het gebruiksgemak van Idensys. Het oordeel over het aanvraagproces was minder positief: slechts 53% vond het aanvragen van een inlogmiddel snel verlopen, 56% beoordeelde het aanvragen als eenvoudig. Voor de waargenomen betrouwbaarheid/veiligheid van Idensys werden tijdens de pilots wel positieve resultaten behaald: 90% beschouwde Idensys als een veilige manier om in te loggen, 78% dacht dat zijn privacy met Idensys goed is gewaarborgd.
(bron: Gebruikerservaringen pilots publieke en private eID-middelen (d.d. 27-5-2016))

Waar is Idensys momenteel* te gebruiken?

- Mijn Belastingdienst
- Accountantsportaal CreAim
- Gemeenten Rotterdam, Den Haag, Drechtsteden, Eindhoven, Groningen, Hollands Kroon en Molenwaard
- Fysiomanager
- Pazio
- Stedin
- SVB
- UMCU
- Pharmeon
- CZ
- Isala Klinieken
- Meddex
- Bureau Krediet Registratie
- Zilveren Kruis

**stand van zaken d.d. 17-8-2017. Momenteel bevindt Idensys zich nog in de pilot-fase: bij sommige organisaties kun je alleen als pilotdeelnemer / op uitnodiging inloggen. Zie https://www.idensys.nl/idensys-voor-gebruikers/waar-kan-je-inloggen/ voor een up-to-date overzicht.*

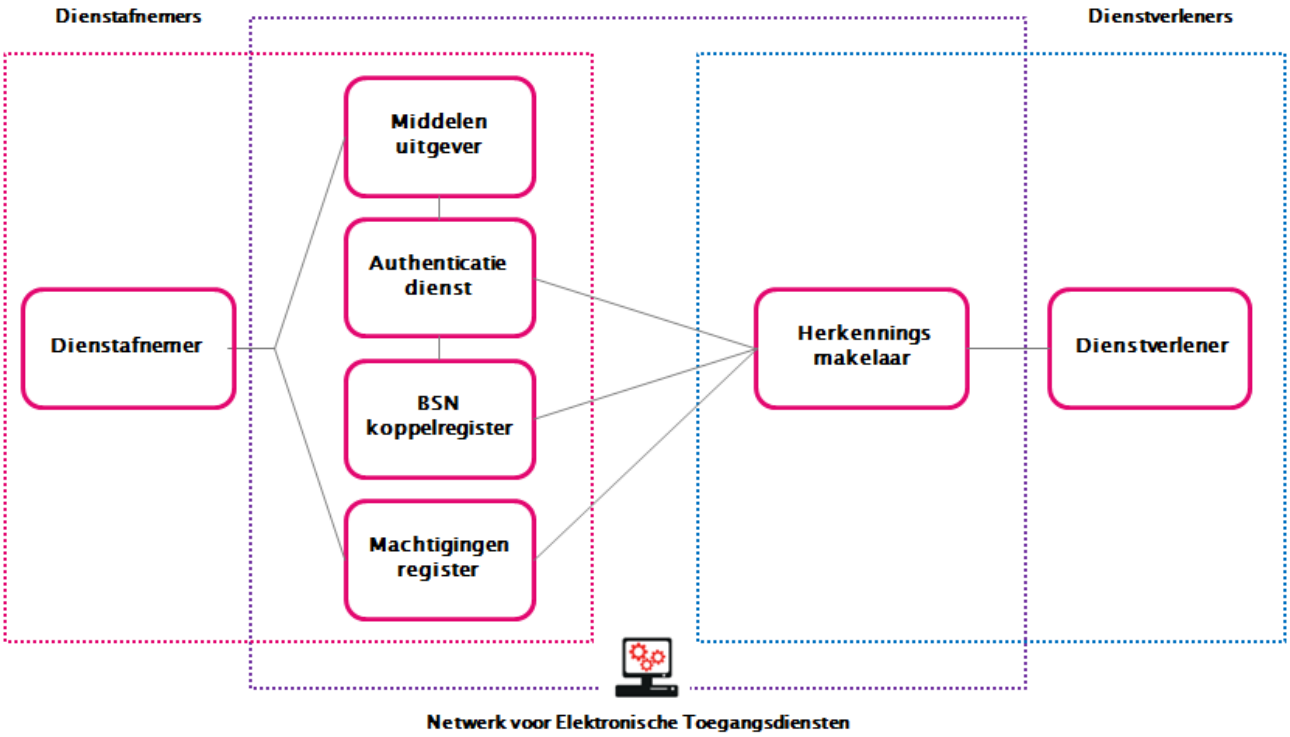
Welke authenticatiediensten bieden momenteel Idensys aan?

- CreAim
- KPN
- SecureIdentity
- Digidentity

(zie: https://www.idensys.nl/idensys-voor-gebruikers/waar-kan-je-inloggen/leveranciers-inlogmiddelen/)

Beschikbare documentatie (via Idensys.nl)

- Factsheet Idensys: legt in het kort Idensys uit en beschrijft beknopt de voordelen.
- Afsprakenstelsel Elektronische Toegangsdiensten (via afsprakenstelsel.etoegang.nl)



Figuur 2: onderscheid verschillende rollen binnen Idensys

Issues en aandachtspunten

BSN-koppelregister

Het koppelregister is een aparte dienst (zie Figuur 2) die ervoor zorgt dat het BSN toch als attribuut kan worden meegegeven, als daar noodzaak en toestemming voor is. Om tijd en kosten te besparen heeft de consument alleen direct contact met de authenticatiedienst. Hij/zij uploadt zijn paspoort- of id-kopie bij een authenticatiedienst, die een combinatie van BSN en benodigde attributen doorgeeft aan het BSN-koppelregister. Dit koppelregister controleert de aangeleverde informatie met die uit het Basisregister Personen. Is alles correct, dan kent het BSN-koppelregister een pseudoniem toe dat het intern koppelt aan het BSN. De authenticatiedienst ontvangt alleen dit pseudoniem en slaat daarbij het BSN niet op. Bij toekomstige authenticaties waarbij het BSN vereist is, koppelt dit koppelregister weer het pseudoniem aan het bijbehorende (versleutelde) BSN en levert deze aan de makelaar.

Bij die eerste stap zit het probleem: de (private!) authenticatiedienst verwerkt immers het BSN in dit proces. Privacy-experts[x,xi] waarschuwen daarnaast voor privacygevoelige hotspots bij zowel identiteitsmakelaar als BSN-koppelregister: allemaal rollen in het Idensys-netwerk waar grote hoeveelheden persoonsgegevens bij elkaar komen.

Betrouwbaarheidsniveaus en middelen

Zoals eerder aangegeven zijn er binnen Idensys vier verschillende betrouwbaarheidsniveaus, en mogen alle welwillende private authenticatiediensten aansluiten. Dit biedt een hoop mogelijkheden, maar ook de uitdaging om het geheel op een goede manier richting de consument te communiceren: alleen al binnen de pilotfase kent Idensys elf verschillende inlogmiddelen.

Kip-ei-probleem

Idensys wordt alleen succesvol als we het massaal gaan gebruiken. Maar we kunnen het pas gebruiken als het breed geïmplementeerd en geaccepteerd wordt. Immers: Idensys vraagt van private authenticatiediensten om in te stappen, maar aangezien die er zelf aan moeten

Burger Service Nummer

DigiD maakt gebruik van het Burger Service Nummer, maar Idensys niet. Dat komt omdat Idensys ook te gebruiken is bij private partijen. Op enkele uitzonderingen na mogen die echter geen gebruik maken van het BSN. Daarom verstrekt Idensys voor de identificatie van de consument alleen een pseudoniem en enkele persoonsgegevens (zie hoofdtekst), maar geen BSN.

Voor de partijen die wel gebruik (mogen) maken van het BSN is het BSN-koppelregister in het leven geroepen. Zie de paragraaf ‘BSN-koppelregister’ op pagina 5 voor meer informatie over het koppelregister.

verdienen zullen deze eerst zeker willen weten dat er voldoende gebruikers zijn. Dit kip-ei-probleem is typerend voor de elektronische afsprakenstelsels die de overheid de laatste jaren ontwikkelde. DigiD kan inmiddels op brede steun rekenen, maar heeft diverse tekortkomingen: aan de overheid de taak om Idensys als een geloofwaardig alternatief op/naast DigiD te presenteren.

Conclusie

Drempels en succesfactoren

Overstappen op Idensys heeft veel voordelen, zowel voor consumenten als aanbieders van online diensten. De kosten voor aanbieders van online diensten zijn te overzien. De aansluiting op het bestaande systeem ook, gezien de set persoonsgegevens die Idensys-middelen verschaffen. Daarnaast opent Idensys zowel de deur naar sterkere, veiligere authenticatiemiddelen, als naar gebruiksvriendelijkere opties als gezichtsherkenning-checks en andere biometrische inlogmethodes. Tot slot voldoet Idensys aan zowel de internationale eIDAS-verordening als de Wet GDI. Dat neemt niet weg dat Idensys enkele belangrijke aandachtspunten en issues kent, die de ingebruikname – zowel specifiek voor de verzekeringsbranche als algemeen – in de weg kunnen staan. Met name rond het BSN-koppelregister, de privacy-hotspots en de communicatie naar buiten bestaan nog uitdagingen.

Toch is Idensys een implementatie met toekomstperspectief. De branche kan hier ook zelf een bijdrage aan leveren. Denk mee in de werk- en stuurgroepen van SIVI, of sluit je aan bij lopende pilots.

Gebruikte definities:

- **Authenticatie**: het proces waarbij wordt nagegaan of een consument daadwerkelijk is wie hij beweert te zijn, dat wil zeggen: daadwerkelijk de identiteit bezit die hij opgeeft.
- **Consument**: de natuurlijke, levende persoon die zich wil authenticeren. Ook klant of gebruiker genoemd.
- **Aanbieder van online diensten**: de organisatie/service bij wie de consument zich met behulp van Idensys wil authenticeren.
- **Authenticatiedienst**: private partij die de inlogmiddelen levert en verantwoordelijk is voor het authenticeren van de consument.
- **Inlogmiddel**: middel waarmee de consument gebruikmaakt van Idensys. Bijvoorbeeld een gebruikersnaam/wachtwoord-combinatie aangevuld met sms, app, gezichtsherkenning, etc.
- **Identiteitsmakelaar**: derde partij die de aanbieder van online diensten aansluit op de beschikbare Idensys-authenticatiediensten en de technische implementatie voor zijn rekening neemt. Binnen Idensys de herkenningsmakelaar genoemd.

---

[i] Logius, 250 miljoen keer ingelogd met DigiD - https://www.logius.nl/over-logius/actueel/item/titel/250-miljoen-keer-ingelogd-met-digid/, geraadpleegd op 12 april 2017

[ii] Tweede Kamer, vergaderjaar 2016-2017, 26 643, nr. 443 - https://zoek.officielebekendmakingen.nl/kst-798314.pdf, geraadpleegd op 12 april 2017

[iii] Idensys - https://www.idensys.nl/, geraadpleegd op 3 april 2017

[iv] Waar we spreken van “inloggen met Idensys” bedoelen we feitelijk “inloggen met een authenticatiemiddel dat gebaseerd is op het afsprakenstelsel van Idensys”. Waar nodig maken we duidelijk onderscheid tussen een authenticatiemiddel en het afsprakenstelsel.

[v] Dit erkennen gebeurt door een Commissie van Deskundigen voor het toezicht op het ETD-stelsel, aangewezen door het Ministerie van Economische Zaken. Zie ook http://wetten.overheid.nl/BWBR0037833/2016-04-20

[vi] Idensys maakt gebruik van *polymorfe pseudoniemen*. Met polymorfe pseudoniemen kan de authenticatiedienst niet zien en/of bijhouden van welke aanbieders van online diensten een consument gebruikmaakt. Dit voorkomt dat de authenticatiedienst een gevoelige privacy-hotspot is in het authenticatieproces. Zie ook https://blog.surf.nl/privacy-surfconext-polymorfe-pseudoniemen/, geraadpleegd op 25-6-2017.

[vii] SEO Economisch Onderzoek, *Rekenmodel eID-stelsel*, augustus 2015 - http://www.seo.nl/uploads/media/2015-36_Rekenmodel_eID-stelsel_01.pdf

[viii] Algemene Rekenkamer, *Vernieuwing stelsel voor digitale identificatie en authenticatie (eID-stelsel)*, augustus 2016 - http://www.rekenkamer.nl/dsresource?objectid=24600&type=org

[ix] Platform Identity Management Nederland, Authenticeren voor 10 cent – http://www.pimn.nl/profiles/blogs/authenticeren-voor-10-cent (geraadpleegd 10-5-2017)

[x] Maarten Wegdam, Van eID naar GDI – de schuivende kabinetsvisie op onze digitale identiteit, 01-09-2016 – https://innovalor.nl/eid-naar-gdi-schuivende-kabinetsvisie-op-digitale-identiteit/ (geraadpleegd 16-3-2017)

[xi] Bart Jacobs, An Assessment of a Privacy Impact Assessment: Idensys under review – http://pilab.nl/about%20pi%20lab/blog/privacy%20impact%20assessement.html (geraadpleegd 16-3-2017)

Voor vragen en reacties

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