Augustus 2017
Robin Oostrum

iDIN

Drempels en succesfactoren van bancair authenticatiemiddel

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 iDIN.

*iDIN is een branchebreed (en –overstijgend) inzetbaar authenticatiemiddel. Banken hebben iDIN (**id**entificeren en **in**loggen) ontwikkeld in het verlengde van iDEAL. Klanten gebruiken de vertrouwde omgeving van hun eigen bank om veilig in te loggen bij overheidsinstanties, verzekeringsmaatschappijen en webwinkels. Aanbieders van online diensten krijgen 100% zekerheid over de identiteit van de klant.*

De inmiddels afgeronde pilotfase wijst op een hoge acceptatiegraad voor zowel consumenten als aanbieders van online diensten.

- iDIN is het authenticatiemiddel van Nederlandse banken en werkt op dezelfde manier als iDEAL
- Vertrouwd voor zowel consument als aanbieder van online diensten
- Aanbieders van online diensten krijgen betrouwbare persoonsgegevens van inloggende consument
- Aansluiten is eenvoudig via een identiteitsmakelaar
- Grootste uitdaging is koppeling aan interne klantenbestand
- Aansluiting op aankomende Wet GDI staat succesvolle uitrol nog in de weg

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
De Betaalvereniging Nederland heeft iDIN ontwikkeld als breed inzetbaar authenticatiemiddel. Zoals iDIN het op haar website[i] zelf formuleert: “iDIN is een nieuwe dienst van de banken waarmee consumenten zich bij andere organisaties online kunnen identificeren, met de veilige en vertrouwde inlogmiddelen van hun eigen bank.”

Alle belangrijke Nederlandse consumentenbanken doen mee aan iDIN: ABN Amro, ING, Rabobank, de Volksbank, ASN Bank, RegioBank en Triodos Bank. Sinds 2016 lopen er iDIN-pilots met onder andere de Belastingdienst, Florius, Interbank, ONVZ Zorgverzekeraar, Verloning.nl en GoCredible. Inmiddels is de pilotfase afgerond en is iDIN breder beschikbaar. Zie het kader op pagina 5 voor aanbieders van online diensten waar iDIN te gebruiken is.

Online identificeren (authenticeren) wordt steeds belangrijker. Consumenten willen veilig gebruik kunnen maken van online diensten. Aanbieders willen volledige zekerheid over de identiteiten van hun gebruikers. Inmiddels bestaan verschillende initiatieven voor branchebrede authenticatie. De vraag is nu: welke van deze initiatieven leveren daadwerkelijk een bijdrage? Hoe reëel is een overstap vanuit de huidige situatie? Wat zijn de voor- en nadelen?

Opzet paper
Deze whitepaper geeft inzicht in iDIN: wat is iDIN, hoe werkt het, hoe sluit mijn organisatie zich erbij aan en wat zijn de belangrijkste voor- en nadelen. We onderzoeken de succesfactoren en drempels van iDIN. Dit geeft inzicht in de mogelijkheden van iDIN 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’.

Wat is iDIN?

Hoe werkt het?
iDIN werkt hetzelfde als iDEAL, maar zonder betaling. Via iDIN kan de consument inloggen met zijn/haar bestaande inlogmiddelen voor iDEAL (bankpas, TAN-codes, etc.). Eenmalige online acceptatie van de iDIN-gebruiksvoorwaarden volstaat. Net als iDEAL werkt iDIN op alle mobiele apparaten met een internetverbinding en een webbrowser. Figuur 1 geeft schematisch het inlogproces weer.

Inlogvoorbeeld Belastingdienst
Op de website van de Belastingdienst is het nu mogelijk om naast het bekende DigiD via iDIN of Idensys in te loggen. Na het kiezen voor iDIN komt de klant terecht in een keuzescherm. De klant selecteert zijn eigen bank en klikt op ‘Ga verder’. Analoog aan een internetbetaling via iDEAL leidt het de klant nu om naar de omgeving van de bank zelf. De klant authenticeert zichzelf bij de bank zoals hij dat gewend is. Bijvoorbeeld met een gebruikersnaam, wachtwoord en een digipas of met een TAN-code. Na succesvolle validatie door de bank leidt iDIN de klant terug naar de omgeving van de Belastingdienst en is hij/zij ingelogd.

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

1. **Authenticatie** van de consument: persoon X is inderdaad persoon X.
2. **Attributen** van de consument: de aanbieder van online diensten kan bij de bank van de consument gegevens opvragen. Het gaat om NAW-gegevens, geslacht, geboortedatum en de leeftijdsverificatie of de gebruiker minstens 18 jaar oud is. De bank heeft deze attributen in een eerder stadium gevalideerd (face-to-face met paspoort of id-kaart), wat ze zeer betrouwbaar maakt. Daarnaast kunnen ook het e-mailadres en telefoonnummer worden opgevraagd. De consument moet voor het delen van gegevens altijd nadrukkelijk toestemming geven tijdens het iDIN-proces.
3. **BIN** of **Bank Identificatie Nummer**: code die uniek is voor iedere combinatie tussen consument, bank van de consument en aanbieder van online diensten. Dit nummer blijft over alle authenticaties gelijk, zolang de consument voor iDIN-authenticaties van dezelfde bank gebruik blijft maken. Zo kan de aanbieder van online diensten de consument uniek identificeren.

Privacy
De aanbieder van online diensten krijgt géén inzage in de financiële gegevens van de consument. iDIN deelt alleen de in de vorige paragraaf genoemde attributen en nooit saldo- of betaalgegevens. De consument moet bovendien altijd nadrukkelijk toestemming geven voor het gebruik van deze attributen.

Implementatie

Aansluiten

Een aanbieder van online diensten kan op twee manieren aansluiten op iDIN:

1. bij één van de deelnemende banken;
2. via een identiteitsmakelaar (de Digital Identity Service Provider of DISP in iDIN-terminologie).

Via een deelnemende bank

In de eerste mogelijkheid sluit de aanbieder van online diensten een contract af met zijn bank, en regelt een routingdienst de technische implementatie[ii]. De aanbieder van online diensten zorgt zelf dat iDIN blijft werken. Het faciliteren van een helpdesk en het afhandelen van klachten moet hij daarbij zelf verzorgen. Het ligt daarom meer voor de hand om voor aansluiting via een identiteitsmakelaar te kiezen. Deze neemt de aanbieder van online diensten een groot deel van genoemde zorgen uit handen.

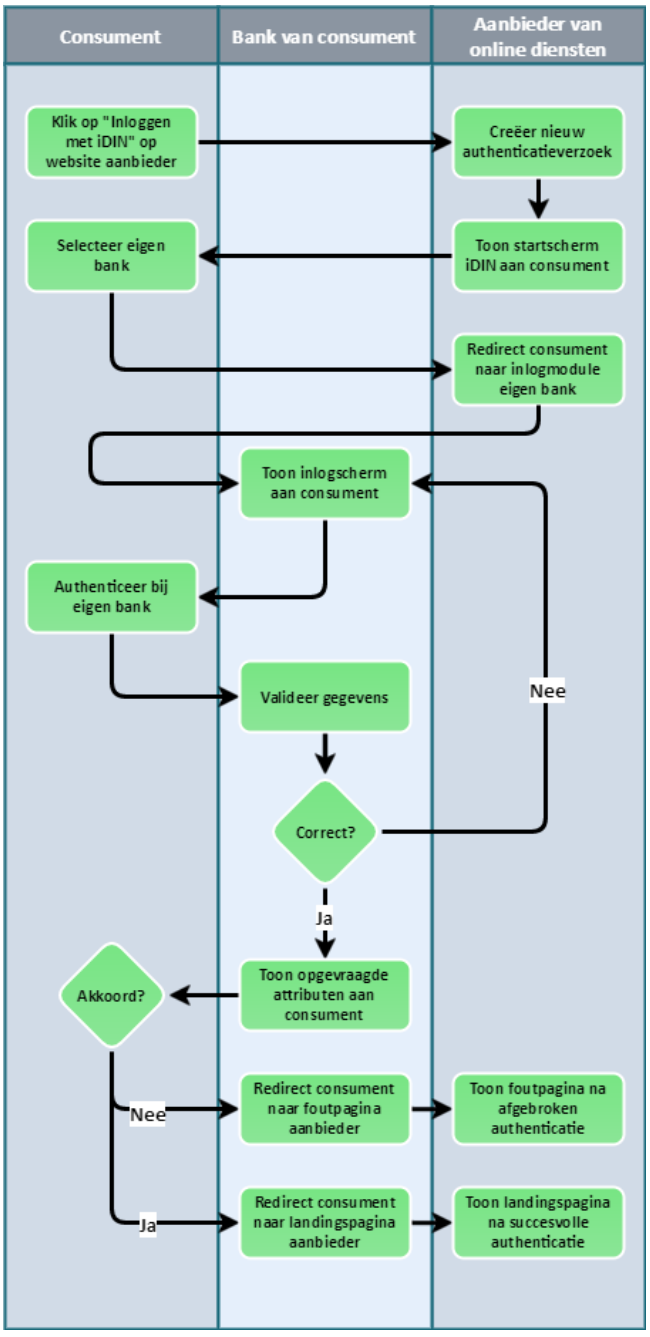
Via een identiteitsmakelaar

Aansluiten via een identiteitsmakelaar – een Digital Identity Service Provider (DISP) – gaat eenvoudig. De aanbieder van online diensten sluit een contract af met een beschikbare DISP. Op iDIN.nl/identiteitdienstverleners staat een actueel overzicht. De DISP implementeert een module op de website van de aanbieder van online diensten. Hierin kan de consument kiezen tussen meerdere inlogmodules, waaronder iDIN. Zie ook Figuur 2.

DISP's bieden de volgende voordelen voor de aanbieder van online diensten:

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

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



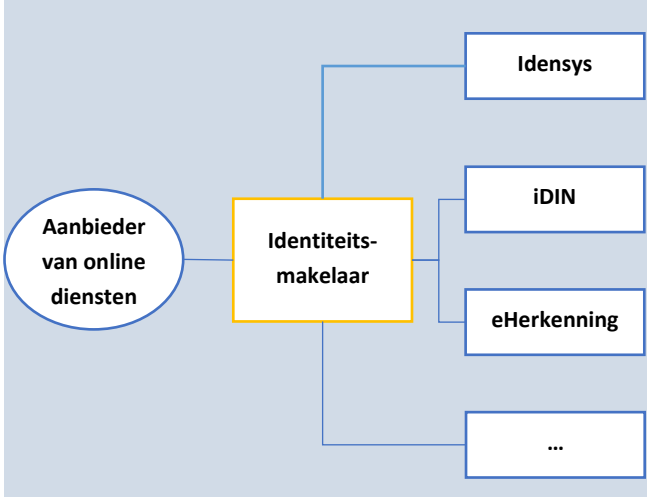
Figuur 1: Gesimplificeerde flowchart van het authenticatieproces in iDIN.

Koppelen huidig systeem aan iDIN

Voor beide manieren van aansluiten moet een aanbieder van online diensten een koppeling maken tussen iDIN en het eigen klantenbestand. Voorheen logde iemand in met gebruikersnaam en wachtwoord, maar iDIN levert andere gegevens. Toch moet ook een met iDIN 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 iDIN, moet de aanbieder van online diensten een *match* maken tussen binnenkomende attributen (NAW, leeftijd, geslacht en dergelijke) en intern bekende gegevens. Dit matchen hoeft maar éénmalig. Als een inloggende iDIN-gebruiker gekoppeld is aan de interne database, slaat het systeem het meegeleverde

Bank Identificatie Nummer (BIN) op. Dit BIN is uniek voor de link tussen consument en aanbieder van online diensten. iDIN maakt het nummer aan bij de eerste authenticatie. Het blijft daarna gelijk over meerdere authenticaties – zolang de consument voor iDIN van dezelfde bank gebruik blijft maken.



Figuur 2: Een identiteitsmakelaar sluit de aanbieder van online diensten aan op meerdere authenticatiemiddelen, waaronder iDIN.

Kosten en resources

Geen aansluitkosten

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

Resources

Aansluiten op iDIN 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 iDIN’.
2. De **technische realisatie** van de overstap op iDIN. Denk aan het aanroepen van iDIN, alternatieven als iDIN niet beschikbaar is, 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 iDIN 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 waarin klanten meerdere profielen hebben. Voor anderen is het belangrijker dat de website functioneert, en/of dat er voldoende maatregelen zijn getroffen wanneer inloggen via iDIN niet mogelijk is. Deze partijen zullen vooral resources kwijt zijn aan de technische kant (punt 2).

Bestaande inlogmiddelen

Inlogmiddelen kosten niets bij een overstap naar iDIN – voor zowel de consument als de aanbieder van online diensten. Het grote voordeel van iDIN is namelijk: iedereen die internetbankiert heeft al inlogmiddelen. Extra wachtwoorden verzenden, smartcards maken enzovoort is dus niet nodig.

Transactiekosten

Op dit moment is de prijs bij de goedkoopste aanbieder 22 eurocent per authenticatie. De verwachting is dat die kosten dalen naarmate het gebruik van iDIN toeneemt. Dit gebeurde bij iDEAL ook: een iDEAL-authenticatie kost tegenwoordig circa 19 eurocent bij de goedkoopste aanbieder[iii].

Aandachtspunten

Alles binnen bankomgeving

De consument zit binnen het iDIN-proces in de digitale omgeving van de bank, net als bij een iDEAL-betaling. Het inlogproces van iDIN vindt dus volledig plaats buiten de omgeving van de aanbieder van online diensten. Vanaf het moment dat de consument aangeeft in te willen loggen via iDIN, zijn geen logo’s van de aanbieder van online diensten meer zichtbaar.

Dit levert een bijkomend voordeel op. De consument vertrouwt de inlogvoorziening van de bank op basis van zijn ervaring met internetbankieren. Hij is daarbij gewend het logo van zijn eigen bank te zien. Bovendien wijst onderzoek in

opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties[iv] uit dat consumenten een voorkeur hebben voor een authenticatieproces ingericht door de overheid, gemeenten of banken.

Geen aansluiting op Wet GDI

iDIN wil vooralsnog niet aansluiten op de in consultatie zijnde Wet GDI[v]. De betrokken partijen onderschrijven wel de doelen en uitgangspunten van deze wet, maar “de huidige uitwerking van de wet en uniforme set van eisen vinden ze te zwaar en ingrijpend” (zie kamerbrief[vi]). Concreet geven ze daarbij aan dat ze geen gebruik willen maken van polymorfe pseudoniemen[vii]. Zolang het stelsel Elektronische Toegangsdiensten een uniforme set van eisen oplegt, betekent dit dat men iDIN niet in het publieke domein kan inzetten. Dit houdt in: niet bij overheidsdiensten, maar ook niet bij zorg- en pensioenverzekeraars. Een mogelijke oplossing zou zijn om af te stappen van dat afsprakenstelsel, door bijvoorbeeld de DNB als toezichthouder te installeren en een verder gelijkwaardige set van eisen te formuleren voor iDIN. De Betaalvereniging kijkt ondertussen naar alternatieven voor het gebruik van polymorfe pseudoniemen.

Aanbieders van iDIN moeten zich wel conformeren aan de zogenoemde Rules & Regulations van de Betaalvereniging zelf. Ook de rol van de aanbieder van online diensten staat hierin beschreven. Dit afsprakenstelsel is niet openbaar, maar is naar alle waarschijnlijkheid analoog aan de Rules & Regulations van iDEAL.

Conclusie

Drempels en succesfactoren

Overstappen op iDIN biedt veel voordelen, zowel voor consumenten als aanbieders van online diensten. Onderzoeken wijzen steeds weer op het gebruiks- en acceptatiegemak onder consumenten. De kosten voor aanbieders van online diensten zijn te overzien. De aansluiting op het bestaande systeem waarschijnlijk ook, gezien de set persoonsgegevens die iDIN verschaft.

Problematischer voor een brede uitrol is dat iDIN zich niet wil schikken naar de in consultatie zijnde Wet GDI. Als de overheid voor het publieke domein een multi-middelenstrategie nastreeft waarin (bijvoorbeeld en onder andere) Idensys en iDIN naast elkaar bestaan, zal iDIN aan dezelfde eisen moeten voldoen als alle andere authenticatiediensten. Een gelijk speelveld is vereist.

Toch is iDIN 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.

Gebruiksgemak

De Betaalvereniging liet een consumentenonderzoek doen als onderdeel van de eerste pilots met iDIN. Daarbij gaf 87% van de respondenten aan iDIN vaker te willen gebruiken en gaf 85% een positief oordeel over het gebruiksgemak van iDIN. De waargenomen betrouwbaarheid/veiligheid van iDIN tijdens de pilots haalde vergelijkbare resultaten.
(bron: Gebruikerservaringen pilots publieke en private eID-middelen (27-5-2016))

iDIN is momenteel onder meer te gebruiken bij:

- Mijn Belastingdienst
- GoCredible
- Interbank
- Florius
- ASR
- Ondertekenen.nl
- ZYNYO
- ONVZ Zorgverzekeraar
- Aangetekend Mailen
- Kedin
- Mobiel.nl
- OPR Bedrijfskrediet
- OHRA
- ValidSign

* stand van zaken d.d. 3-8-2017

Beschikbare documentatie (via iDIN.nl)

- Implementatiegids voor iDIN

Dit document richt zich specifiek op organisaties die als aanbieder van online diensten aan willen sluiten op het iDIN-platform. Belangrijkste topic is het berichtenverkeer tussen deze partijen en hun bank.

- Integratiehandleiding

Engelstalige handleiding voor ontwikkelaars die iDIN implementeren met behulp van de hierna vermelde software libraries. Het bevat richtlijnen voor integratie en voorbeeldcode.

- Software libraries

Deze software libraries zijn ontwikkeld in de programmeertalen Java, PHP en .NET. Het is een hulpmiddel voor de implementatie van iDIN aan de kant van de afnemende aanbieder van online diensten.

- Huisstijlhandboek

Nederlandstalig document met richtlijnen en instructies voor het gebruik van het iDIN-logo. Het levert een zip-bestand met iDIN-logo’s (12 afbeeldingen) mee.

Gebruikte definities:

- **Authenticatie**: het proces dat nagaat 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 iDIN wil authenticeren. Binnen iDIN de acceptant genoemd.
- **Bank van consument**: de consument gebruikt de omgeving en de inlogmiddelen van zijn eigen bank om zich te authenticeren bij de aanbieder van online diensten. Binnen iDIN de issuer genoemd.
- **Inlogmiddel**: middel waarmee de consument gebruikmaakt van iDIN en iDEAL. Bijvoorbeeld een gebruikersnaam/wachtwoord-combinatie, bankpas, digipas, lijst met TAN-codes, betaal-app.
- **Identiteitsmakelaar**: derde partij die de aanbieder van online diensten aansluit op iDIN en de technische implementatie voor zijn rekening neemt. Binnen iDIN de Digital Identity Service Provider (DISP) genoemd.

---

[i] iDIN | Online identificeren via uw bank - https://www.idin.nl/, geraadpleegd op 27-3-2017.
[ii] Er is geen mogelijkheid binnen iDIN waarin de aanbieder van online diensten rechtstreeks aansluit op de bank. Er zit altijd een technische partij tussen, in de vorm van een routingdienst.
[iii] Wat kost iDeal voor je webshop? Anno 2017 - https://elephantcs.nl/blog/wat-kost-ideal-voor-je-webshop/, geraadpleegd op 27-3-2017.
[iv] Motivaction: Publieksonderzoek elektronische identiteitskaart - https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/02/09/publieksonderzoek-elektronische-identiteitskaart/z5168-motivaction-eindrapportage-publieksonderzoek-elektronische-identiteitskaart.pdf, geraadpleegd op 1-3-2017.
[v] Wet Generieke Digitale Infrastructuur: burgers en bedrijven moeten zich vanaf 2019 met een inlogmethode naar keuze kunnen identificeren bij overheids- en zorginstellingen. De Wet GDI zet de eisen aan deze inlogmethoden uiteen. - https://www.digitaleoverheid.nl/beleid/digitalisering-aanbod/inhoud/
[vi] Kamerbrief over voortgangsrapportage eID - https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2017/06/23/kamerbrief-inzake-voortgangsrapportage-programma-eid/kamerbrief-inzake-voortgangsrapportage-programma-eid.pdf, geraadpleegd op 25-6-2017.
[vii] Met polymorfe pseudoniemen kan de identiteitsmakelaar niet zien en/of bijhouden van welke aanbieders van online diensten een consument gebruikmaakt. Dit voorkomt dat de identiteitsmakelaar een gevoelige privacy-hotspot is in het authenticatieproces. Zie ook https://blog.surf.nl/privacy-surfconext-polymorfe-pseudoniemen/, geraadpleegd op 25-6-2017.

Voor vragen en reacties

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