Productsheet iDIN

Voor Acceptanten

Versie 2.0

10-8-2018

Deze productsheet is bedoeld ter informatie voor u als Acceptant. In deze productsheet vindt u onder andere 1. een uitleg over de verschillende partijen die in het proces van iDIN-gebruik deelnemen, 2. een flowchart waarin de rolverdeling / het proces duidelijk wordt, 3. informatie over de gegevens die kunnen worden verwerkt bij het gebruik van iDIN, 4. een toelichting op de betrouwbaarheid, veiligheid, privacy en kwaliteit van de data bij het gebruik van iDIN en 5. extra informatie over de beschikbaarheid, bewaartermijnen en andere documentatie.

Inhoudsopgave

1 De verschillende rollen

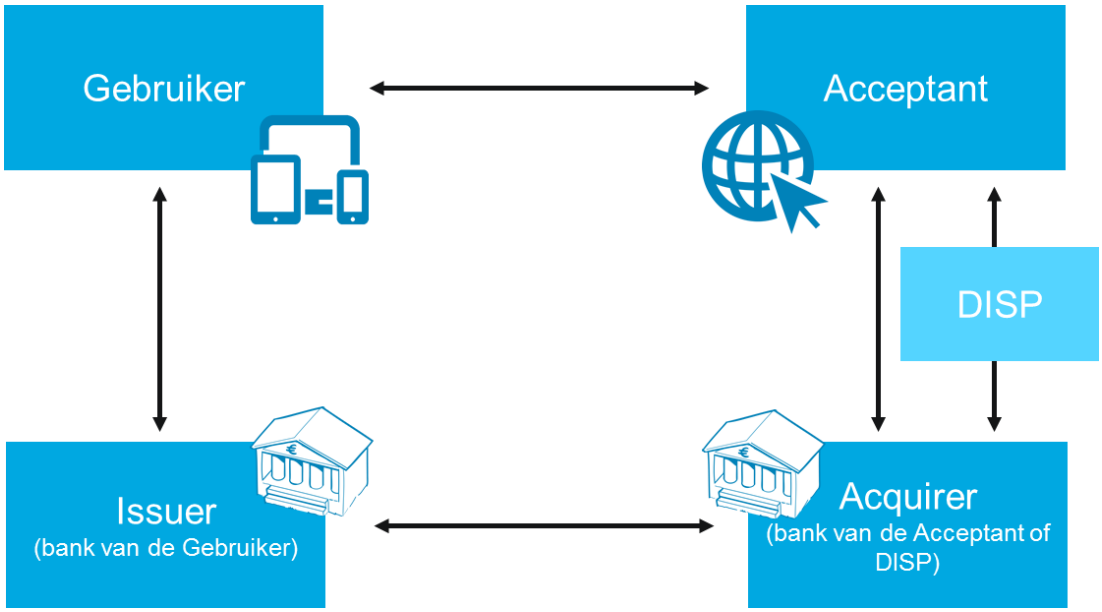
De verschillende rollen	
Rol	**Uitleg**
Acceptant	Een bedrijf/dienst/instelling die een gemakkelijke en veilige online identificatiemethode wil gebruiken en de Gebruiker (klant) meer keuze wil geven bij het inloggen en dit kan doen door iDIN als (extra) online identificatiedienst aan te bieden op zijn/haar website.
Acquirer	Een partij die een Licentieovereenkomst voor iDIN met Currence (iDIN B.V.) heeft afgesloten en contracten afsluit met Acceptanten en DISP's voor iDIN.
Dataverwerker	Een partij die alleen (on)versleutelde iDIN gebruikers data ontvangt en daarna verder levert aan de Acceptant of alleen klantgegevens beheert in opdracht van de Acceptant. Deze partij heeft geen formele rol binnen iDIN.
DISP - Digital Identity Service Provider	Een partij die een Certificaatovereenkomst voor iDIN met Currence heeft afgesloten. De DISP maakt afspraken met haar Acceptanten aangaande iDIN en sluit zelf iDIN-contracten met haar Acceptanten.
Gebruiker	Een natuurlijk persoon met toegang tot het online kanaal van zijn Issuer voorzien van de juiste autorisaties. Zijn/haar gegevens worden vastgelegd door zijn/haar bank, de Issuer.
Issuer	Een partij die een Licentieovereenkomst met Currence heeft afgesloten. Het is de consumentenbank van de Gebruiker.

Rol – Algemene Verordening Gegevensbescherming (AVG)	**Rol - iDIN**
Gezamenlijke verantwoordelijkheden - De rechtspersonen die tezamen de middelen voor de verwerking van persoonsgegevens bepaalt binnen de kaders van het iDIN stelsel van afspraken. Voor iDIN zijn de Issuer en Acquirer gezamenlijk verantwoordelijke voor de veilige verwerkingen binnen het iDIN Scheme[1].	• Acquirer • Issuer
Verantwoordelijke - De rechtspersoon die het doel van en de middelen voor de verwerking van persoonsgegevens bepaalt. De Acceptant is dus zelf verantwoordelijk voor de verwerking van de persoonsgegevens die hij in het kader van de IDIN dienstverlening verkrijgt.	• Acceptant
Verwerkers - Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen. Conform de geldende afspraken binnen het iDIN scheme. Voor iDIN geldt dat: • De RSP[2] is verwerker in de zin van de AVG voor de Acquirer; • De VSP[3] is verwerker in de zin van de AVG voor de Issuer; • De DISP[4] is verwerker in de zin van de AVG voor de Acceptant;	• Dataverwerker • DISP
Betrokkene - Degene op wie de te verwerken persoonsgegevens betrekking heeft. Voor iDIN betreffen dit natuurlijke personen die gebruik maken van de iDIN-dienstverlening.	• Gebruiker

[1] Een Scheme is een stelsel van functionele, organisatorische en technische afspraken zoals nader beschreven in de R&R Online van de Producten iDEAL, iDIN en Incassomachtigen.
[2] Een Routing Service Provider biedt haar service aan voor de routering van een iDIN-bericht, geïnitieerd door een Gebruiker middels het online kanaal van zijn Issuer via de website van de Acceptant of DISP.
[3] Een Validatie Service Provider draagt zorg voor het verwerken en afhandelen van het berichtenverkeer voor (de) Issuer(s).
[4] Een DISP die alleen een contractuele relatie met de Acceptant heeft en waarbij de technische afhandeling van het iDIN berichtenverkeer direct tussen de Acquirer en Acceptant plaatsvindt, dient zich ook te laten certificeren als DISP, maar heeft niet de rol van verwerker.

2 Flowchart gebruik iDIN

Om duidelijk te maken hoe de rolverdeling en het proces van de implementatie en beheer van iDIN er uit zien, is onderstaande flowchart gemaakt. Deze flowchart is het best te lezen in combinatie met de tabel op de vorige pagina.



3 Welke gegevens kan iDIN verwerken

iDIN biedt verschillende gegevens die individueel of gecombineerd opgevraagd kunnen worden.

Uniek nummer voor inloggen

- BIN - Bank Identificatie Nummer geschikt voor herhaal-login (nummer dat wordt toegekend door de bank (Issuer) van de Gebruiker en waarmee de Gebruiker zich uniek identificeert bij de Acceptant);
- Transient_ID voor eenmalig gebruik (eenmalig nummer toegekend door de Issuer aan desbetreffend bericht).

Geverifieerde gegevens van de Gebruiker
Afkomstig van een onafhankelijke bron, het wettelijk identiteitsbewijs:

- Naam: voorletter(s), voorvoegsels, achternaam (geslachtsnaam/legal lastname);
- Leeftijdsindicatie (18 jaar of ouder) of geboortedatum;
- Geslacht.

Gegevens verstrekt aan de bank door de Gebruiker

- Achternaam die de voorkeur van de Gebruiker heeft (preferred/partner lastname)
- Woonadres: straat, huisnummer, postcode, stad;
- E-mailadres;
- Telefoonnummer.

Gebruikers kunnen ervoor kiezen om het telefoonnummer en/of emailadres niet mee te sturen of een telefoonnummer en/of emailadres naar keuze in te vullen.

iDIN bestaat uit meerdere producttypes die inzetbaar zijn in verschillende toepassingen:

- Identificeren
- Inloggen
- Leeftijd bevestigen

4 Betrouwbaarheid, kwaliteit, privacy & veiligheid

4.1 Betrouwbaarheidsniveaus

Bij het gebruik van elektronische identificatiemiddelen is het belangrijk dat dit betrouwbaar, veilig en kwalitatief goed is. Met specifieke eisen is bepaald waaraan de elektronische identificatiemiddelen van een Issuer moeten voldoen om te worden toegelaten in het iDIN-Scheme. De eisen zijn opgesteld op basis van de Europese eIDAS regulering en bestaan uit technische specificaties en procedures. Er worden verschillende eisen gesteld per niveau gerelateerd aan inschrijving, beheer van de elektronische identificatiemiddelen, authenticatie, beheer en organisatie.
Er zijn drie betrouwbaarheidsniveaus te onderscheiden, namelijk: laag, substantieel en hoog. Bij iDIN dienen Issuers minimaal een elektronisch identificatiemiddel aan te bieden aan hun Gebruikers dat voldoet aan betrouwbaarheidsniveau substantieel. Voor meer informatie wordt verwezen naar de eIDAS regulering.

Betrouwbaarheidsniveau substantieel heeft de volgende hoofdkenmerken:

- Identificatie op basis van een geldig identiteitsbewijs. De identiteit van de consument dient aan de hand van dit geldige identiteitsbewijs te worden geverifieerd.
- Er wordt gebruik gemaakt van tweefactor-authenticatie (dit betekent dat je alleen toegang krijgt met iets wat je weet (een wachtwoord of code) samen met iets wat je hebt (een pasje of token).

4.2 Datakwaliteit

Om hoge kwaliteit te borgen heeft iDIN bepaalde eisen gesteld aan de kwaliteit van de gegevens die Issuers verstrekken, hierbij wordt bijvoorbeeld gelet op zowel formaat als inhoud. Er wordt daarbij gekeken naar de aanwezigheid van de gegevens, of de gegevens voldoen aan het vereiste veldformaat en of de gegevens in de database van de bank overeenkomen met de gegevens op het identiteitsbewijs van de klant.

De gebruikersdoelgroep van iDIN voldoet aan de volgende randvoorwaarden[5]:

- Natuurlijke personen;
- Met toegang tot internet en/of mobielbankieren[6];
- Die Wwft-compliant (Wet ter voorkoming van witwassen en financieren van terrorisme) zijn geïdentificeerd door de bank.

De meetcriteria voor de kwaliteitsbeoordeling van gegevens en de normen voor de criteria zijn als volgt:

Meetcriteria	Uitleg	Norm
Accuraatheid	De mate waarin iDIN-datavelden overeenkomen met hetgeen er is vastgelegd in de kopie identiteitsbewijs.	95 – 99 %
Compleetheid	De mate waarin iDIN-data aanwezig is: de datavelden uit het datamodel zijn gevuld.	98 – 100 %
Correctheid	De mate waarin iDIN-data voldoet aan het vereiste veldformaat: voldoet aan de formatting rules zoals beschreven in de meest recente versie van de implementatiegids iDIN. Een attribuut moet kunnen worden geleverd conform de formatting rules.	99 %
Uniciteit	De mate waarin iDIN-data (i.c. BSN) uniek is: slechts één keer voorkomt bij een Issuer.	97 %

[5] Iedere bank kan deze verder afbakenen, op dit moment zijn bijvoorbeeld de zakelijke vertegenwoordigers zijn uitgesloten.

[6] De banken hanteren de volgende minimum leeftijdsgrenzen voor iDIN gebruikers: ABN AMRO, ASN Bank, RegioBank en SNS 18+; Rabobank en Triodos 16+; ING 12+.

4.3 Privacy & veiligheid

In het ontwerp van iDIN zijn verschillende maatregelen genomen om privacy en veiligheid te waarborgen:

- iDIN is gebaseerd op het principe van privacy by design: privacy verhogende maatregelen en dataminimalisatie.
- De Gebruiker geeft zelf opdracht aan zijn bank voor het verstrekken van de gegevens die nodig zijn om zich bij een organisatie te identificeren.
- Een organisatie mag de door een bank verstrekte persoonsgegevens opslaan, zolang de organisatie zich aan de privacywetten houdt en de gegevens alleen gebruikt voor de doeleinden die hij aan de klant bekend heeft gemaakt.
- Bank-inloggegevens worden door de Gebruiker alleen ingevoerd in de internetomgeving van zijn eigen bank en niet bij de webwinkel. Deze gegevens zijn en blijven alleen bij de klant bekend;
- De Gebruiker logt in via een beveiligde verbinding bij zijn eigen bank, zodat derden niet kunnen meekijken.
- De Gebruiker maakt gebruik van zijn bestaande, veilige bankmiddelen om in te loggen en om iDIN te gebruiken.
- Gegevens worden versleuteld verzonden naar Acceptanten.
- Online, realtime fraudedetectie is ingericht om eventuele fraudeaanvallen zo vroeg mogelijk te detecteren en deze tegen te gaan.
- Door gebruik te maken van bestaande bank-infrastructuur heeft iDIN dezelfde hoge security, fraudebestendigheid en monitoring zoals de bestaande producten internetbankieren en iDEAL.

5 Extra informatie

5.1 Beschikbaarheid

De totale openstellingstijd wordt onderscheiden in twee perioden: prime time (06.00-00.30) en non-prime time (00.30-06.00). Voor prime time geldt per periode van een kalendermaand 99,5% online realtime beschikbaarheid van de systemen en voor non-prime time 93,5% online realtime beschikbaarheid. De Acquirer of DISP dient gepland onderhoud alleen in de non-prime time periode uit te voeren.

5.2 Bewaartermijnen

Transactiegegevens die in de berichtenprotocollen worden uitgewisseld worden gedurende de wettelijk bepaalde termijnen bewaard (in (elektronische) archieven of logs). De Acquirer is verplicht de bewaartermijnen te hanteren conform de bewaartermijnen overeenkomstig wat daarover in de iDX staat vermeld, dan wel voor de periode van tenminste 13 maanden.

5.3 Extra informatie (www.idin.nl)

De volgende documentatie kan aangevraagd worden via:
https://www.idin.nl/acceptanten/documentatie-aanvragen/

- Acceptant Implementatiegids
    - Inclusief de bijlage diversiteit bij gebruikersattributen - de Acceptant dient hier rekening mee te houden bij het integreren van iDIN
- Software libraries (Java, .NET, PHP) met handleiding
- Huisstijlhandboek
- Toolkit communicatiemiddelen organisaties
- Achtergronddocumenten
- Banners
- Logo’s

Gebruikers demo: https://demo.idin.nl/
Ervaringen Acceptanten: https://www.idin.nl/acceptanten/acceptanten-aan-het-woord-video/
Animatie: https://www.idin.nl/consumenten/animatie/