Rapport

Betaalvereniging Nederland

Robuustheid Betalingsverkeer – Verbeteracties en Resultaten Update 2015-2018

Update van het rapport aan het MOB uit 2015 met betrekking tot de bancaire diensten Pinnen, Internetbankieren, Mobiel bankieren en iDEAL

24 september 2018 | Versie 1.0 | Definitief

Inhoud

1. Inleiding en Samenvatting

1.1 Inleiding

In oktober 2015 heeft Betaalvereniging Nederland het rapport uitgebracht “Robuustheid Betalingsverkeer – Verbeteracties en Resultaten 2013-2015”. In dit rapport worden de belangrijkste ontwikkelingen en maatregelingen beschreven, die de robuustheid van het Nederlandse betalingsverkeer, en dan in het bijzonder van de bancaire producten Pinnen, iDEAL en Internetbankieren/Mobiel bankieren moeten optimaliseren.
Dit rapport is positief besproken in de najaarsvergadering 2015 van het MOB. Ook werd gesteld, dat het MOB de beschikbaarheid van deze bancaire betaaldiensten zal blijven monitoren. Tevens was daar afgesproken, dat het rapport, indien daar behoefte aan bestond, na enige jaren zou worden geactualiseerd.
Onderhavig rapport is deze actualisatie, die de ontwikkelingen sinds 2015 beschrijft. Directe aanleiding waren meerdere DDoS-aanvallen op enkele Nederlandse banken in januari en mei 2018. Ook DNB heeft zich geuit in de discussie die ontstond n.a.v. genoemde DDoS-aanvallen[1].
Dit rapport is bedoeld voor alle stakeholders van het MOB, en het geeft aan, dat de focus van de banken en de Betaalvereniging permanent gericht is op het (verder) optimaliseren van de kwaliteit van bovengenoemde bancaire diensten. Hierbij moet echter benadrukt worden, dat andere stakeholders van de betaalproducten, zoals de winkeliers/ondernemers en de webshops, ook een eigen verantwoordelijkheid hebben om het deel van de onderliggende betaalketens waarop zij directe invloed kunnen uitoefenen, te optimaliseren.

1.2 Samenvatting

Pinnen:
Pinnen is het belangrijkste betaalproduct op de winkellocatie, zowel gemeten naar aantal transacties als naar het hiermee afgerekende geldbedrag. Het is dus van cruciaal belang voor alle stakeholders dat dit betaalproduct robuust, betrouwbaar en maximaal beschikbaar is. Het is dan ook een verantwoordelijkheid van alle stakeholders, om zodanige maatregelen te nemen dat aan deze wensen/eisen kan worden voldaan. In de periode 2015-2017 zijn veel acties ondernomen om deze doelen te realiseren.
Geconstateerd is, dat er twee kritische delen in de pinketen zijn: het winkeldomein (met daarin de betaalautomaat, het kassasysteem, de interne vaste bekabeling, het evt. Wifinetwerk, de router c.q. het access point naar de buitenwereld), en de netwerkdienst (tussen het access point en de transactieverwerker). Deze twee delen bepalen goeddeels de uiteindelijke beschikbaarheid van de pinketen. Het is de verantwoordelijkheid van de winkelier/ondernemer om de twee kritische delen van de pinketen goed in te richten, maar andere stakeholders, zoals de Betaalvereniging, kunnen hem hierbij verregaand faciliteren.
Acties 2015-2018 betreffende het winkeldomein:

- Tezamen met Detailhandel Nederland en DNB, heeft de Betaalvereniging afspraken gemaakt met koepelorganisaties van installateurs van alarmeringsapparatuur, om problemen te

[1] Zie: https://nos.nl/artikel/2214177-derde-ddos-storing-abn-amro-binnen-24-uur-ook-ing-getroffen.html. Klaas Knot, president van De Nederlandsche Bank (DNB) zegt in het tv-programma Buitenhof dat cyberaanvallen zoals die op ABN AMRO voor banken tegenwoordig aan de orde van de dag zijn. 'Dat is de realiteit anno 2018', zegt Knot, die spreekt van een 'serieuze zaak'.

voorkomen, wanneer in de winkel zowel pin- als alarmeringsapparatuur wordt geplaatst. Deze afspraken worden jaarlijks geëvalueerd.
- Detailhandel Nederland en de Betaalvereniging hebben een rapport opgesteld, dat aandachtspunten benoemt wanneer een winkelier/ondernemer een Wifinetwerk in zijn winkel installeert. Dit document wordt op verschillende plaatsen gepubliceerd, en zal ook nog worden "vertaald" in voor de doelgroep bevattelijke taal zodat het nog meer attentie zal krijgen van deze doelgroep van Detailhandel Nederland.

Acties 2015-2018 betreffende netwerkdiensten:

- Tezamen met datacomproviders heeft de Betaalvereniging (verder) gewerkt aan het verbeteren van netwerkdiensten, het introduceren van dubbele datacomoplossingen, het rapporteren van gerealiseerde beschikbaarheden van de gecertificeerde netwerkdiensten en het verbeteren van communicatie naar betrokkenen bij datacomverstoringen.

Het totaal van verbeteracties 2012-2017 heeft tot een stijging in de beschikbaarheid van de pinbetaalketen geleid, tot 99,88% in 2017. De verbeteracties hebben in deze periode ook geleid tot een duidelijke afname van het aantal grotere verstoringen in de pinketen.

Internetbankieren en Mobiel bankieren:

Het gebruik van de bancaire diensten Internetbankieren en Mobiel bankieren groeit snel. Ook nemen de door de banken aangeboden functionaliteiten binnen deze diensten toe, wat het beheer van IB en MB complexer maakt. Desondanks laten transparant gepubliceerde beschikbaarheidscijfers zien, dat de beschikbaarheid van IB en MB in de periode 2014-2017 groeide naar globaal 99,75%. De DDoS-aanvallen van begin 2018 zorgden voor een tijdelijke neergang. DDoS-aanvallen zijn een *fact of life*, maar de banken hebben inmiddels een aantal mitigerende middelen ontwikkeld om de gevolgen van DDoS-aanvallen snel en effectief te kunnen minimaliseren. Een permanente focus van de banken en de Betaalvereniging blijft echter noodzakelijk, vooral vanwege de externe dreigingen, die zich ook blijven ontwikkelen.
De *online* beschikbaarheid van IB en MB is voor zes banken op een aparte website middels een dashboard te raadplegen[2].Sinds begin 2015 worden maandelijks per bank de *historische* beschikbaarheidscijfers gepubliceerd op de website van de Betaalvereniging[3].

iDEAL:

Net als IB en MB is de betaaldienst iDEAL gevoelig voor DDoS-aanvallen. Dat hangt samen met het feit, dat deze diensten benaderbaar moeten zijn vanaf iedere willekeurige internetaansluiting. Daarnaast kunnen IB. MB en iDEAL elkaar negatief beïnvloeden, doordat ze, zeker in het verleden, gebruik maken van gedeeltelijk dezelfde infrastructuren. Verbeteracties van de banken m.b.t. iDEAL hebben dan ook vooral betrekking op deze twee factoren.

- DDoS-aanvallen zijn een *fact of life*. Geen enkele individuele partij kan alleen voldoende mitigerende maatregelen treffen om het risico volledig uit te sluiten. Samenwerking tussen diverse stakeholders, zowel in het publieke als in het private domein is noodzakelijk. De banken en de Betaalvereniging hebben hiertoe ook veel acties ondernomen, die langzamerhand vruchten beginnen af te werpen. Een permanente focus van de banken en de Betaalvereniging blijft echter noodzakelijk, vooral vanwege de externe dreigingen, die zich ook blijven ontwikkelen.
- De ontvlechting van de infrastructuren van IB, MB en iDEAL is in 2016 goeddeels voltooid. Dat heeft een positief effect gehad op de beschikbaarheden van alle drie de diensten in de periode 2014-2016.

[2] Zie: https://beschikbaarheid.betaalvereniging.nl/
[3] Zie: https://www.betaalvereniging.nl/betaalproducten-en-diensten/beschikbaarheid-internet-en-mobiel-bankieren/

De *online* beschikbaarheid van iDEAL is op een aparte website middels een dashboard te raadplegen[4]. De *historische* beschikbaarheidscijfers worden op de website van Currence gepubliceerd[5]. Te zien is, dat in 2014 de beschikbaarheden van iDEAL nog te wensen overlieten. Daarna trad een sterke verbetering op. Begin 2018 is de impact te zien van de DDoS-aanvallen. De laatste paar maanden is de beschikbaarheid van iDEAL weer boven 99,76%. Dat is in overeenstemming met de eisen, zoals vastgelegd in de *Rules & Regulations* van Currence, maar continue aandacht en verbeteringsacties blijven noodzakelijk.

In de volgende hoofdstukken worden de verbeteracties beschreven, die gerealiseerd zijn in de periode 2015-2018 van achtereenvolgens de bancaire producten Pinnen, Internet- en Mobielbankieren en iDEAL. Daarbij komen steeds de acties aan de orde, die tot de feitelijke verhogingen van de beschikbaarheden hebben geleid, alsook de verbeteringen in het communicatietraject bij mogelijk toch optredende verstoringen.
In zes INFOBOXEN worden specifieke deelonderwerpen nader beschreven en gevisualiseerd.

[4] Zie: https://beschikbaarheid.ideal.nl/
[5] Zie: https://www.ideal.nl/ontvangen/kerncijfers/ideal-beschikbaarheid/

2. Pinnen: stabiel ecosysteem

2.1 *Umwelt* van het betaalproduct Pinnen

Voordat ingegaan wordt op de activiteiten die de banken en de Betaalvereniging hebben ondernomen om de betrouwbaarheid van het betaalproduct Pinnen te vergroten, lijkt het ons zinvol om een korte schets te geven van ontwikkelingen die zich recentelijk hebben voorgedaan en in de nabije toekomst voor zullen doen bij de toonbank, de Point of Sale (PoS). De PoS is de plek (veelal de winkel) waar de consument zijn betaaltransactie verricht.
Belangrijke ontwikkelingen die relevant zijn voor de betrouwbaarheid van Pinnen zijn:

1. Meer met elkaar concurrerende partijen en oplossingen in ketenrollen, zowel binnen als buiten het gecertificeerde ecosysteem van de Betaalvereniging;
2. Meer verschillende ketens (giraal-gebaseerd naast de cards-keten, bijvoorbeeld ten behoeve van Instant Payments);
3. Meer diversiteit in betaalhandelingen aan de toonbank (als gevolg van diversiteit in betaaloplossingen);
4. Meer verschillen tussen retailers in termen van betaalmogelijkheden die worden geaccepteerd.

Bovengenoemde ontwikkelingen hebben, in het licht van betrouwbaarheid van de verschillende betaalproducten aan de toonbank, voor de consument en de winkelier/ondernemer de volgende impact:

A. Meer versnippering, onduidelijkheid en ruis. Dat vertaalt zich in meer behoefte aan overzicht en onafhankelijk kwaliteitsoordeel;
B. Minder impact bij verstoring van één specifieke keten; bij meer diversiteit kan de focus verschuiven van beschikbaarheid per keten naar beschikbaarheid aan de toonbank, over verschillende betaaloplossingen heen. Dit is van belang voor zowel de klant- als de winkelierperceptie.

Hieronder volgt een korte beschrijving en uitwerking van de ontwikkelingen.

2.1.1 Toename risico's op versnippering, onduidelijkheid en ruis; groeiende behoefte aan ketenregisseur

A. Er treden nieuwe, relatief onbekende partijen tot de pinbetaalketen toe, deels buiten het gecertificeerde en bewaakte ecosysteem

Op dit moment ervaren zowel winkelier/ondernemer als consument een duidelijke herkenbaarheid van het betaalproduct Pinnen. De bankpas en de betaalautomaat zijn eenvoudig herkenbare devices. De handelingen die door de consument uitgevoerd moeten worden voor een betaling zijn verregaand gestandaardiseerd, evenals de schermteksten en meldingen die een consument bij een betaling kan tegenkomen. Er is daardoor een minimale kans op verwarring. Tot voor kort was de onderliggende infrastructuur van het betaalproduct Pinnen overzichtelijk, en waren er ook heldere afspraken over het melden van storingen of geplande werkzaamheden door ketenpartijen. Wanneer een ketenpartij (terminalleverancier, gecertificeerde datacomleverancier, processor, bank, …) een storing in zijn domein heeft, wordt daarvan verplicht melding gemaakt in het notificatiesysteem CONNECT. Dit notificatiesysteem staat onder beheer bij de Betaalvereniging, en die draagt dan ook zorg voor de communicatie rondom verstoringen naar de markt. Op deze wijze werden ook winkeliers/ondernemers snel geïnformeerd over zich voordoende problemen. Voor het optimaal functioneren van dit proces is het noodzakelijk dat alle ketenpartijen participeren in CONNECT, en dat de Betaalvereniging contacten onderhoudt met al die ketenpartijen. Door marktontwikkelingen

wordt het zicht van de Betaalvereniging op de integrale betaalketen minder. Er treden nieuwe partijen toe tot de pinbetaalketen, waar de Betaalvereniging niet altijd weet van heeft (en vice versa) en die problemen (ook) niet melden in CONNECT, bijvoorbeeld omdat ze naast onbekendheid ook niet altijd het nut ervan inzien[6].
Kortom, de rol van ketenregisseur wordt steeds belangrijker in dit werkveld. Er ontstaat een sterke en groeiende behoefte aan een partij, zoals de Betaalvereniging, die deze centrale regierol invult.[7]

B. Nieuwe betaalproducten: standaardisatie voor consument en winkelier/ondernemer wordt minder
Door het beschikbaar komen van nieuwe betaalproducten zal die duidelijke herkenbaarheid aan de toonbank minder worden. Consumenten kunnen bv. te maken krijgen met *devices* die niet door de Betaalvereniging zijn beoordeeld en dus ook niet terug te vinden zijn op de website van de Betaalvereniging. Nieuwe non-cards betaalmethoden gebaseerd op bijvoorbeeld Instant Payments, QR-codes of betaalapps van nieuwe spelers zorgen voor een verdere divergentie in betaalhandelingen en mogelijke uitzonderingssituaties aan de toonbank. Dit kan onduidelijkheid geven aan de zijde van de consument. Vooral in uitzonderingssituaties raakt ook de winkelier betrokken bij de onduidelijkheid. De versnippering van betaalproducten zal ook van de winkelier/ondernemer een grotere flexibiliteit eisen en voortdurende opleiding/training/voorlichting van kassapersoneel in betaalmethoden en hun mogelijkheden. Een recent voorbeeld van (voorgenomen) gezamenlijke voorlichting in dit kader is artikel 75 van de PSD2 waarin gesteld wordt dat het bedrag van pre-autorisatie vooraf expliciet aan de consument moet worden getoond. Heldere voorlichting helpt hier dit communicatieprobleem voor alle partijen adequaat op te lossen.
De diversificatie van nieuwe betaalmogelijkheden leidt aldus tot meer ruimte voor verwarring, misverstanden en wellicht fraudemogelijkheden. Hier ligt een rol voor zowel banken, partijen die nieuwe betaaldiensten leveren (zoals Klarna, OK, Payconiq, PayPal, …), toonbankinstellingen als andere stakeholders van het MOB om hun achterbannen voor te lichten over de verschillende vormen van (nieuwe) betaalproducten. Zorgvuldige voorlichting, bij voorkeur gezamenlijk door betrokken marktpartijen, helpt om de betrouwbaarheid van de diverse betaalproducten, ook in hun onderlinge samenhang, op peil te houden. Omdat het hierbij vaak om onderling concurrerende partijen gaat, bestaat ook hier een sterke behoefte aan een ketenregisseur. Een rol die door de Betaalvereniging, als onafhankelijke en deskundige partij, ingevuld kan worden.
Overigens kiezen ondernemers en consumenten zelf voor nieuwe betaalproducten. Consumenten zullen nieuwe betaalproducten alleen gebruiken, wanneer ze die begrijpen, in die zin, dat ze snappen hoe ze een product moeten gebruiken.[8] Hetzelfde geldt voor ondernemers die nieuwe betaaldiensten aanbieden; zij hebben hier een verantwoordelijkheid naar de consument om die hierover goed voor te lichten. Wanneer zij hun verantwoordelijkheid goed invullen, zal de onduidelijkheid in de praktijk meevallen.

2.1.2 Toename betrouwbaarheid door verschillende PoS-alternatieven

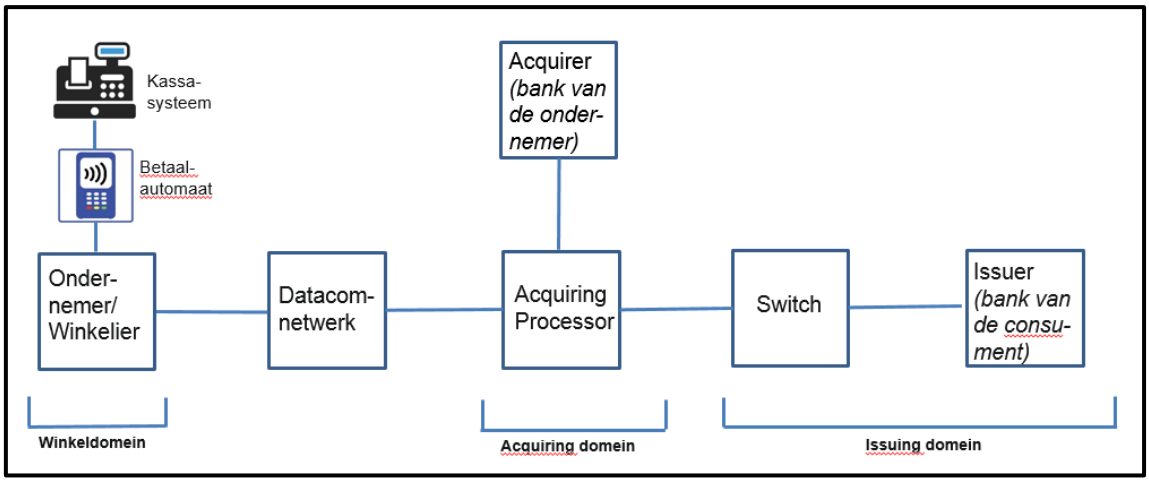
Op de toonbank bij de winkelier/ondernemer stond tot voor kort altijd een door de Betaalvereniging gecertificeerde betaalautomaat. Met behulp van de bankpas en evt. een pincode krijgt de consument hiermee toegang tot de pinbetaalinfrastructuur, wat noodzakelijk is om een pinbetaling te kunnen

[6] Verdere uitwerking van CONNECT: zie paragraaf 2.5.4.
[7] Het is hierbij zinvol om de term “regisseur” toe te lichten en af te bakenen. De regisseur zal niet zelf een operationele rol spelen bij het afwikkelen van betalingsverkeer. Zijn grootste toegevoegde waarde ligt in het hebben van een overzicht van alle operationele partijen, het organiseren van stakeholder bijeenkomsten, waarin alle stakeholders hun inbreng kunnen leveren, het bij elkaar brengen van de verschillende operationele partijen, het zorgen voor een centrale communicatie. Kortom: de regisseur begrijpt de dynamiek van de stakeholders en het werkveld, overziet deze collectiviteit en neemt het voortouw bij evt. verbeteracties, vernieuwingen, communicatie etc.
[8] Hoe een product precies werkt en wat de voor- en nadelen en risico’s zijn begrijpen consumenten vaak niet en interesseert ze (helaas) vaak ook niet. Totdat het mis gaat en ze bij de aanbieder komen klagen. Hier zit duidelijk een link met communicatie en voorlichting over producten.

doen. Voor de ondernemer was er eenduidige informatie beschikbaar over de rol van de ondernemer, bijvoorbeeld in het kiezen van de juiste apparatuur en telecomverbinding, voor het maximaliseren van de betrouwbaarheid van de betaalinfrastructuur. Daarnaast werd aan de toonbank typisch ook contant geld geaccepteerd, nagenoeg zonder tijdkritische betrouwbaarheidsrisico's, maar met voorraadbeperkingen aan zowel de kant van de consument als bij de acceptant.
In de nabije toekomst zullen ook andere betaaloplossingen beschikbaar komen, die in staat zijn online toonbankbetalingen af te wikkelen. Te denken valt aan Instant Payments al dan niet in combinatie met een QR-code. Daarbij kunnen de diverse elektronische alternatieven in voorkomende gevallen fungeren als elkaars back-up voorziening. Wanneer de ene oplossing niet beschikbaar is, kan een andere oplossing wellicht gebruikt worden. Dit komt de beschikbaarheid van betalen in het algemeen ten goede.
Hierbij zijn enkele kanttekeningen te plaatsen:
Ondernemers kunnen overwegen om niet alle verschillende betaaloplossingen te accepteren.
Ook kunnen de onderliggende betaalinfrastructuren van verschillende betaaloplossingen gemeenschappelijke schakels bevatten. Denk hierbij bv. aan telecomnetwerken. Bij een verstoring in het telecomnetwerk kunnen verschillende, schijnbaar van elkaar onafhankelijke, betaaloplossingen getroffen worden.
Tot slot moet hier genoemd worden, dat zowel klant als winkelier/ondernemer over diverse *devices* dient te beschikken om toegang te krijgen tot de diverse betaaloplossingen.
Samengevat kan geconstateerd worden, dat de diversificatie van toonbankbetaalproducten de betrouwbaarheid in elk geval niet schaadt, en in specifieke gevallen laat toenemen. Consumenten en winkeliers kunnen er in de toekomst eerder op vertrouwen dat een toonbankbetaling, hetzij linksom, hetzij rechtsom, zal slagen. Voor een consument is de beschikbaarheid van relevante *devices* (betaalkaart, smartphone) belangrijk; voor de winkelier/ondernemer geldt dat ook, en daar zal ook de kostenfactor een rol spelen. De ondernemer zal een goede keuze moeten maken welke betaalproducten hij wil aanbieden. Daarbij moet een afweging worden gemaakt tussen hogere kosten voor sommige betaalproducten en klantverlies en omzetderving.

2.2 De betaalketen voor pinnen

Het geheel van onderliggende systemen die gebruikt worden om in een winkel pinbetalingen af te wikkelen wordt de pinbetaalinfrastructuur of de pinbetaalketen genoemd. Die bestaat uit de betaalautomaat bij de winkelier op de toonbank, de verbinding binnen de winkel tussen betaalautomaat en het koppelpunt (het access point) met een datacomnetwerk (ethernet-bekabeling in geval van een vaste betaalautomaat; draadloze Wifi-koppeling of mobiele netwerkkoppeling in geval van mobiele betaalautomaat); het datacomnetwerk dat het access point koppelt aan een computersysteem dat de betalingen verwerkt en een zogenaamde switch met daarachter de verschillende banknetwerken waarin de autorisatie van de betaling plaatsvindt. Elk van deze bovengenoemde elementen moet beschikbaar zijn om tot een succesvolle transactie te kunnen komen. Vanzelfsprekend is het streven van de banken en de Betaalvereniging dan ook steeds gericht op een nagenoeg altijd beschikbare pinketen, zodat de behoefte aan (al dan niet elektronische) alternatieven minimaal kan zijn.



Figuur 1: Pinketen (functioneel)

2.3 Banken en transactieverwerkers vallen onder toezicht DNB

De functionele combinatie Acquiring Processor/Switch (zie figuur 1) valt voor wat betreft de dominante transactieverwerker equensWorldline direct onder het toezicht van De Nederlandsche Bank DNB. In de Wet Financieel Toezicht (*Regeling DNB afwikkelondernemingen* van 24 april 2014) wordt equensWorldline beschouwd als een zgn. Afwikkelonderneming, die een beschikbaarheid moeten hebben van 99,88% in het zgn. hogevraagtijdvak (06:00 uur – 00:30 uur)[9]. De feitelijke beschikbaarheid ligt duidelijk hoger (> 99,99%).
Daarnaast vallen de banken die Pinnen aanbieden aan hun klanten, onder de *Regeling Oversight goede werking betalingsverkeer* (van 21 december 2015). In deze *ROgwb* zijn eisen opgenomen t.a.v. beschikbaarheden, de maximale storingsopheffingstijden en de plicht om gerealiseerde beschikbaarheden van het bancaire deel van de pinketen (zie figuur 1) publiekelijk te rapporteren. DNB houdt toezicht op de naleving van de *ROgwb* door de individuele banken. Uit deze publieke rapportages blijkt, dat dit deel van de pinketen in het hogevraagtijdvak een beschikbaarheid kent van nagenoeg 100% (> 99,99%).

2.4 Twee kritische delen van de pinketen: het winkeldomein en de netwerkdienst

Vastgesteld is, dat de beschikbaarheid van de betaalketen goeddeels bepaald wordt door de kwaliteit van de datacomverbinding tussen het access point van een ondernemer (het winkeldomein) en de verwerker van de transacties (acquiring domein). Dit is sterk afhankelijk van het type datacomverbinding (de netwerkdienst) van de ondernemer.
Een ander belangrijk element dat de end-to-end beschikbaarheid van het betaalproduct bepaalt, is het deel van de pinketen dat zich in het winkeldomein bevindt. Daaronder valt de interne winkelbekabeling (ethernet danwel Wifi of een mobiel-netwerkkoppeling).

[9] Zie Artikel 12 lid 3 van deze Regeling: Een afwikkelonderneming die verzoeken doorzendt of goedkeurt waarborgt een minimale beschikbaarheid van haar kritische systemen van 99,88% gemeten op kwartaalbasis gedurende het hogevraagtijdvak en 98,5% daarbuiten. Hiertoe stelt zij zelf een beschikbaarheidsnorm op die boven de beschikbaarheidsnorm tijdens het hogevraagtijdvak ligt en die past bij het aantal door haar afgewikkelde transacties, teneinde het risico te mitigeren dat de afwikkelonderneming de minimale beschikbaarheid niet bereikt in een gegeven kwartaal.

Bij beide elementen, dus de kwaliteit van de netwerkdienst en de kwaliteit van het netwerk op de eigen winkellocatie, heeft de ondernemer een belangrijke eigen verantwoordelijkheid. Hij koopt immers zèlf een netwerkdienst in bij een datacomprovider, met een bijbehorende SLA. En hij geeft zèlf opdracht aan de installatie en het onderhoud van zijn eigen winkelnetwerk. Om de ondernemer hierbij te helpen, zodat die tot een goede keuze kan komen, kunnen de banken en de Betaalvereniging vergaand faciliteren. Maar dat ontslaat de ondernemer niet van de eindverantwoordelijkheid die hij hierin heeft.

2.5 Acties van de Betaalvereniging betreffende netwerkdiensten

In het datacomdeel van de betaalketen blijkt nog steeds een lichte verbetering mogelijk. Verbetering is mogelijk op een drietal punten:

1. Een beter zicht op de kwaliteit van netwerkdiensten;
2. Meer transparantie voor winkeliers over kwaliteitsniveaus van verschillende netwerkdiensten;
3. Een betere communicatie van datacomleveranciers bij dienstverstoringen.

Op elk van bovengenoemde verbeterpunten is in de periode 2015-2018 progressie geboekt, die hieronder nader wordt beschreven.

2.5.1. Een beter zicht op kwaliteit van netwerkdiensten

Zoals eerder beschreven, wordt de beschikbaarheid van de betaalketen goeddeels bepaald door de beschikbaarheid van de netwerkdienst tussen het access point op de winkellocatie en de acquiring processor. De overige elementen van de keten kennen een zeer hoge beschikbaarheid (>99,99%). Omdat bekend is dat het datacomdeel van de pinbetaalketen een zwakke schakel vormt, certificeert de Betaalvereniging netwerkdiensten. Wanneer een netwerkdienst aan objectieve kwaliteitseisen voldoet, kan de netwerkdienst worden gecertificeerd, en wordt een overeenkomst met de datacomleverancier afgesloten.
De *Overeenkomsten Datacomleverancier*, die de Betaalvereniging met gecertificeerde datacomleveranciers heeft afgesloten, geven voldoende stuurmiddelen om de kwaliteit van de geleverde netwerkdiensten door de sector te verbeteren. Zo stuurt de Betaalvereniging strak op het opleveren van kwalitatief goede maandrapportages, waaruit moet blijken, dat de geleverde netwerkdiensten permanent aan de certificeringseisen blijven voldoen. Wanneer de maandrapportages niet opgeleverd worden, of indien deze van onvoldoende inhoudelijke kwaliteit zijn, of indien uit de maandrapportage blijkt, dat het minimaal vereiste kwaliteitsniveau voor netwerkcertificeringen niet gehaald wordt, kan in het uiterste geval het netwerkcertificaat worden ingetrokken. Op deze wijze geeft de Betaalvereniging het toezicht op de met individuele datacomleveranciers afgesproken regels strak gestalte.

2.5.2. Transparantie verschillende kwaliteitsniveaus netwerkdiensten

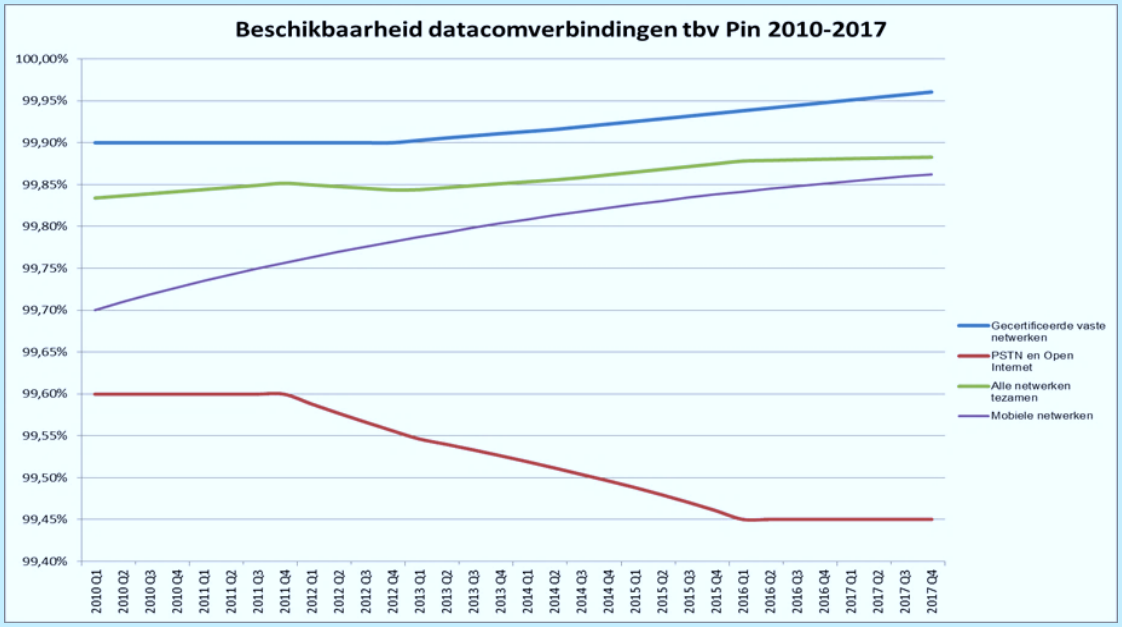
We kennen twee categorieën netwerkdiensten, namelijk door de Betaalvereniging gecertificeerde netwerkdiensten, en niet-gecertificeerde (vaak open internet) netwerkdiensten. In de regelgeving van de *global brands* of de Betaalvereniging bestaat geen verplichting, dat een netwerkdienst die gebruikt wordt voor het transporteren van data van betaaltransacties, gecertificeerd moet zijn. Toch is momenteel ongeveer 85%-90% van alle betaalautomaten gekoppeld aan een door de Betaalvereniging gecertificeerd netwerk (mobiel en vast tezamen).

Een netwerkdienst die door de Betaalvereniging is gecertificeerd, heeft een gegarandeerde beschikbaarheid op de winkellocatie van minimaal 99,6%. Uit kwaliteits-rapportages blijkt echter, dat veel gecertificeerde netwerkdiensten in de praktijk een hogere beschikbaarheid kennen. De Betaalvereniging publiceert sinds december 2012 de verschillende gecertificeerde netwerkdiensten, met daarbij verschillende gegarandeerde beschikbaarheidspercentages, op haar website[10]. Daarmee wordt voor ondernemers transparant gemaakt wat de verschillen in kwaliteit zijn tussen de verschillende netwerkdiensten, zodat zij een geïnformeerde keuze kunnen maken.
Binnen de categorie gecertificeerde netwerkdiensten bestaan ook significante kwaliteitsverschillen. Die verschillen worden bepaald door bv. de beschikbaarheid van de serviceorganisatie of de mogelijkheid om een mobiele back up netwerkdienst te leveren in geval van storing op de primaire aansluiting. Over het serviceniveau van een netwerkdienst worden afspraken in de vorm van een SLA gemaakt tussen de netwerkleverancier en de klant, in dit geval de winkelier/ondernemer.
Verschillende koepelorganisaties en ook de Stichting Bevorderen Efficiënt Betalen (SBEB) gebruiken de informatie op de website actief om hun achterban te wijzen op de verschillende kwaliteiten van de gecertificeerde netwerkdiensten[11]. Daarbij wordt ook expliciet gewezen op het belang van het gebruik van gecertificeerde netwerkdiensten. Ondernemers kunnen op deze wijze een bewustere afweging maken bij de keuze van een datacomleverancier. Geconstateerd wordt dat 85%-90% van de ondernemers kiezen voor een gecertificeerde netwerkdienst met een hoge beschikbaarheid, wat dan weer leidt tot een hoge beschikbaarheid van de hele pinbetaalketen. De 10%-15% die kiest voor een niet-gecertificeerde netwerkdienst bevindt zich vooral in het onderste MKB-segment. Daar speelt waarschijnlijk het kostenelement een belangrijke rol. Zij nemen hierbij, al dan niet bewust, een risico met betrekking tot beschikbaarheid en veiligheid.
Ook aan de vraagzijde is op initiatief van de SBEB een belangrijke stap gezet in het verbeteren van de beschikbaarheid van de betaalketen, door het stimuleren bij ondernemers van het gebruik van zogenaamde dubbele datacomoplossingen. Dit houdt in, dat ondernemers worden gestimuleerd om hun betaalautomaat niet aan één netwerk, maar aan twee verschillende netwerken te koppelen, waardoor de relatieve zwakte van dit deel van de betaalketen goeddeels ondervangen wordt.

[10] Zie: http://www.betaalvereniging.nl/kaartbetalingen/datacommunicatie/
[11] Zie: https://www.checkout.nl/bericht/pinstoring-voorkomeny-check-de-tips EN https://www.betaalvereniging.nl/betaalproducten-en-diensten/pinnen/datacommunicatie/

INFOBOX 1: Beschikbaarheid datacomdiensten

In de figuur hieronder wordt de ontwikkeling van de beschikbaarheid van datacomdiensten voor het betalingsverkeer geschetst.



Toelichting:

De grafiek geeft de ontwikkeling van de beschikbaarheden van het datacomnetwerk (de netwerkdienst), zoals dat zich bevindt tussen het access point van de winkelier/ondernemer en de transactieverwerker. Zoals in de hoofdtekst vermeld is, bepaalt dit deel van de pinketen goeddeels de uiteindelijke beschikbaarheid van het betaalproduct Pinnen.

- De blauwe (bovenste) lijn geeft de ontwikkeling aan van de beschikbaarheid van door de Betaalvereniging gecertificeerde netwerkdiensten. Op basis van maandrapportages bleek, dat die beschikbaarheid in de periode 2010-2012 stabiel op 99,9% lag. Op uitnodiging van de Betaalvereniging begonnen datacomleveranciers daarna ook hoogwaardiger netwerkdiensten te ontwikkelen, met een hogere beschikbaarheid. Door deze ontwikkeling groeide de beschikbaarheid eind 2017 naar 99,96%.
- De paarse lijn geeft de ontwikkeling aan van de beschikbaarheid van mobiele netwerken. Hierin is in de periode 2011-2017 een duidelijke evolutie te zien van 99,70% (2011) naar 99,86% (2017). Dit is volledig toe te schrijven aan de migratie van 2G (GSM) naar 3G (UMTS) en 4G (LTE). Beide laatste mobiele netwerken zijn duidelijk robuuster, met een hogere dekking, een grote bandbreedte en een hogere beschikbaarheid.
- De rode (onderste) lijn geeft de ontwikkeling aan van de beschikbaarheid van het “ouderwetse” telefonienetwerk en het open internet. Door de uitfasering van het stabiele (beschikbaarheid 99,6%) maar trage telefonienetwerk vanaf eind 2011 door KPN, kiest een deel van de winkeliers/ondernemers voor het snelle, maar duidelijk minder beschikbare open internet (beschikbaarheid 99,45%). Dit verklaart de daling van de rode lijn vanaf 2011. Sinds eind 2015 zijn er geen betaalautomaten meer aangesloten op het telefonienetwerk.
- De groene lijn geeft het gewogen gemiddelde weer van de blauwe (76%), paarse (10%) en rode (14%) lijn. Het overall gemiddelde groeide in de periode 2011-2017 van 99,83% naar 99,88%. Hoewel dit misschien een kleine groei lijkt, betekent dit wel, dat de onbeschikbaarheid is afgenomen van 0,17% naar 0,12%. Dat is een forse afname.

2.5.3. Gecertificeerde netwerkdiensten en DDoS-aanvallen

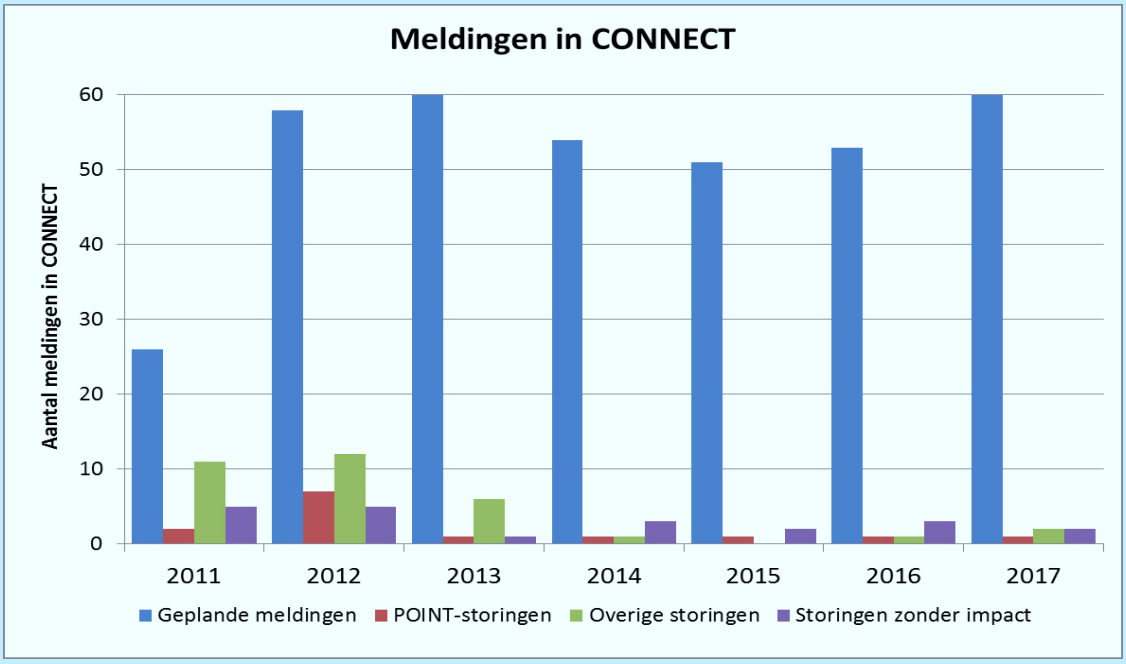
Een belangrijke certificeringseis voor netwerkdiensten, is de eis, dat niet ongeautoriseerd toegang tot het netwerk tussen access point in het winkeldomein en transactieverwerker kan worden gekregen. Uitsluitend gesloten netwerken, of zgn. virtuele privé netwerken (VPN's) kunnen worden gecertificeerd. Deze gecertificeerde netwerkdiensten staan logisch dan ook helemaal los van het internet, en staan dus ook niet bloot aan de risico's die koppelingen met internet met zich mee kunnen brengen. Een belangrijk risico vormen DDoS-aanvallen. Omdat 85%-90% van de betaalautomaten gekoppeld is aan een gecertificeerd netwerk, zijn deze automaten nagenoeg ongevoelig voor DDoS-aanvallen. Maar omdat de transactieverwerker 10%-15% pintransacties vanuit het internet verwerkt, moet deze transactieverwerker wel aanvullende maatregelen nemen, om zichzelf te beschermen tegen DDoS-aanvallen. Die maatregelen bestaan uit het inrichten van een DMZ (Demilitarized Zone), in combinatie met Intrusion Detection Systemen (IDS). Hier worden dus kosten in het ecosysteem gemaakt die een direct gevolg zijn van de keuze van de ondernemer om een goedkope, niet-gecertificeerde datacomverbinding te gebruiken. Desondanks komt het sporadisch voor, dat zich een succesvolle aanval voordoet op dit koppelpunt met het open internet van de transactieverwerker. Dit zijn de zgn. POINT-storingen (zie INFOBOX 2). Daarvan hebben dan dus uitsluitend winkeliers/ondernemers die hun betaalautomaat aan het internet hebben gekoppeld last. Dit is een specifiek risico van het gebruik van open internet. En het is zodoende een extra argument, naast het kostenaspect bij de transactieverwerker, om het gebruik van gecertificeerde netwerkdiensten te stimuleren.

2.5.4. Verbeteren Communicatie bij datacomverstoringen

Wanneer zich een verstoring in de betaalketen voordoet, is het van belang dat alle relevante *stakeholders* (zowel banken, betaaltautomaatleveranciers en transactieverwerkers, alsook retailorganisaties) hierover zo snel mogelijk geïnformeerd worden.
Om de communicatie naar marktpartijen bij verstoringen in de betaalketen te verbeteren is al in 2009 het meld- en registratiesysteem CONNECT ontwikkeld. De Betaalvereniging heeft de participatie in CONNECT voor gecertificeerde datacomleveranciers *verplicht* gesteld. Op deze wijze wordt de veelgehoorde klacht rondom de gebrekkige communicatie van datacomleveranciers bij dienstverstoringen ondervangen. Dat heeft een positief effect in de duur van een verstoring, maar ook in de subjectieve perceptie van marktpartijen van de gevolgen van de verstoring. Snelle en zorgvuldige communicatie bij verstoringen kan veel ongenoegen wegnemen.
Omdat KPN een grote, dominante datacomleverancier is op de zakelijke markt, zijn met KPN aparte afspraken gemaakt over het meldingen van storingen. Daartoe heeft de Betaalvereniging een 24/7 ingang bij het Business Service Desk BSD van KPN in Zoetermeer. Met het BSD vinden ook jaarlijks evaluatiegesprekken plaats. Daar worden de zich voorgedane verstoringen besproken, de bestaande procedures doorgelicht, de melddrempels voor CONNECT evt. geactualiseerd en eventuele wijzingen in de port folio van KPN besproken.
Door het promoten van het gebruik van CONNECT is het aantal actieve gebruikers ervan de afgelopen jaren fors gegroeid. Momenteel kent CONNECT 44 participanten[12] (dat zijn partijen, die zelf een storing in CONNECT kunnen plaatsen) en 49 retailers, die middels CONNECT worden geïnformeerd over zich mogelijk voordoende verstoringen. Met Detailhandel Nederland is een aparte afspraak gemaakt, om die direct te informeren in geval van grotere verstoringen. Totaal kent CONNECT meer dan 400 gebruikers. Hieronder wordt een overzicht gegeven van de aantallen meldingen die in CONNECT zijn geplaatst, met een onderscheid naar aard van die melding.

[12] Zie: https://www.betaalvereniging.nl/wp-content/uploads/CONNECT_lijst_deelnemers.pdf

INFOBOX 2: Ontwikkelingen Meldingen CONNECT



Toelichting:

De grafiek geeft de ontwikkelingen vanaf 2011 van het aantal door deelnemende partijen geplaatste notificaties in CONNECT, uitgesplitst over verschillende categorieën. De verschillende categorieën zijn:

Geplande meldingen: Activiteiten die door een participant enkele dagen van te voren in CONNECT worden gezet en normaliter niet tot een onderbreking van de pin-dienst leiden. Deze categorie meldingen is verreweg de grootste.

POINT storingen = PinnenOverINTernet. Hierbij maakt de winkelier/ondernemer geen gebruik van een door de Betaalvereniging gecertificeerde datacomverbinding, maar maakt hij gebruik van het open internet. Vanwege het hogere risicoprofiel, komen POINT-transacties bij de transactieverwerker binnen op een aparte gateway. Ongeveer 13% van de betaaltransacties wordt getransporteerd door het open internet. Het Kleinbedrijf is daarbij oververtegenwoordigd. Het jaarlijkse aantal POINT-storingen ligt de laatste jaren stabiel op één.

Overige storingen: Dit is de categorie meldingen die feitelijke storingen aanduiden. Te zien is, dat het aantal *Overige storingen* tussen 2011 en 2013 is sterk afgenomen van 11 naar 2, en vanaf 2014 stabiel op een zeer laag niveau ligt.[13]

Storingen zonder impact: Dit betreft meldingen die weliswaar ongepland zijn, maar, die vanwege bv. redundantie, niet leiden tot storingen die voor de winkelier/ondernemer merkbaar zijn.

[13] In de figuur zijn de aantallen van 2018 vanzelfsprekend niet opgenomen. Tot nu toe (17 augustus 2018) hebben zich 2 kleinere POINT-storingen voorgedaan (<5% van de transacties geraakt), en 1 grote storing. Die laatste vond plaats op 12 juli, van 19:00 uur tot 20:30 uur. Het netwerk (de switch) van MasterCard was in die periode volledig buiten bedrijf, waardoor ca. 60% van de transacties mislukte. De *root cause* analyse van MC gaf aan, dat de oorzaak lag in het verkeerd uploaden van een nieuwe software release. MC heeft excuses aangeboden (zie: https://www.telegraaf.nl/nieuws/2296073/mastercard-pinproblemen-opgelost) en ook direct toegezegd de noodzakelijke verbeteringen in te zullen voeren. Voor de woordvoering in Nederland heeft MC NL de Betaalvereniging bedankt. Toevalligerwijs vond iets eerder, op 1 juni, een storing bij Visa plaats. Omdat Visa voor debetkaartbetalingen een relatief klein marktaandeel heeft in Nederland, is de impact van deze storing klein geweest. Internationaal was de impact wel groot.

2.6 Acties betreffende het winkeldomein

Zoals in paragraaf 2.4 verwoord is, vormt de inrichting van het winkeldomein een belangrijke factor voor de stabiliteit en de beschikbaarheid van de end-to-end pinketen. Afgelopen paar jaar hebben de relevante stakeholders op twee deelaspecten verbeteracties ondernomen.

2.6.1 Verstoringen in Pinketen als gevolg van koppelen van alarmeringsapparatuur

Onder regie van de Betaalvereniging zijn in 2014 afspraken gemaakt met koepelorganisaties van de alarmeringswereld. De afspraken hadden tot doel uitval van betaalautomaten door ondeugdelijke installering van alarminstallaties bij winkeliers/ondernemers te voorkomen.
De gemaakte afspraken betreffen:

1. Betere voorlichting, voor zowel alarminstallatiebedrijven als winkeliers/ondernemers;
2. Betere installatierichtlijnen voor installateurs van alarminstallatiebedrijven;
3. Structureel platform voor overleg tussen alarmeringsbranche en betaalwereld.

Ad 1) Voorlichtingsmateriaal is ontwikkeld, dat door de koepelorganisaties ook actief wordt uitgedragen naar de betrokken achterbannen.
Ad 2) In nauw overleg met enkele grotere datacomproviders zijn installatievoorschriften ontwikkeld, die voor de hele branche van alarminstallatiebedrijven beschikbaar zijn gesteld. De installatiebedrijven hebben ook toegezegd gebruik van deze richtlijnen te gaan voorschrijven.
Ad 3) Om voortgang van de afspraken en eventuele nieuwe gemeenschappelijke issues te bespreken, organiseren deelnemers aan de werkgroep een jaarlijkse evaluatiebijeenkomst.

Tijdens de eerste evaluatiebijeenkomst eind 2015, hebben participanten geconstateerd dat goede voortgang is geboekt bij het uitvoeren van alle gemaakte afspraken. De participanten hebben dan ook uitgesproken vertrouwen te hebben in de effectiviteit van de gemaakte afspraken. Dit beeld is eind 2016 en eind 2017 bij de evaluatie door betrokkenen opnieuw bevestigd.

2.6.2 Wifi in de retailomgeving

Een belangrijke ontwikkeling van de laatste jaren in het winkeldomein is de grootschalige implementatie van Wifinetwerken. Deze draadloze netwerken geven de ondernemer veel mogelijkheden om zijn eigen bedrijfsprocessen te ondersteunen, maar ook om de consument te faciliteren en om betaalverkeer via de Wifinetwerken af te wikkelen. Zowel aan de fysieke en virtuele toonbank is continuïteit van het betalingsverkeer van essentieel belang. Geconstateerd werd, dat retailondernemers soms weinig kennis hebben van kansen en mogelijkheden van Wifinetwerken, maar ook van zwakheden en bedreigingen ervan. Dat is aanleiding geweest voor de werkgroep WEE van het MOB om, op verzoek van Detailhandel Nederland, een rapport op te stellen met betrekking tot het gebruik van Wifinetwerken voor betalingsverkeer. Het rapport is positief besproken in de voorjaarsvergadering 2018 van het MOB en zal worden gebruikt voor voorlichting aan de winkeliers/ondernemers. Het rapport zal worden gepubliceerd op o.a. de website van DNB, Detailhandel Nederland en de Betaalvereniging. Daarnaast zal het rapport zeer binnenkort herschreven worden in voor de doelgroep bevattelijke taal, zodat het nog meer attentie zal krijgen van deze doelgroep van Detailhandel Nederland.

2.7 Pinketen heeft voldoende capaciteit om voorziene groei op te vangen

Als één van de acties voortvloeiend uit de *Nadere Overeenkomst II* (de in september 2014 gemaakte afspraken tussen koepels van ondernemers en banken) heeft de Betaalvereniging in juni 2015 een risicoanalyse opgesteld voor het betaalproduct pinnen. Daarin zijn alle elementen van de pinketen geanalyseerd op mogelijke kwetsbaarheden en capaciteitsknelpunten. Dit in het perspectief van de afspraken die gemaakt zijn in de *Nadere Overeenkomst II*, om het aantal pintransacties tussen 2015 en ultimo 2018 fors te laten groeien. Het gebruik van het betaalproduct Pinnen is gegroeid van 3,226 miljard transacties in 2015 naar 3,843 miljard transacties in 2017. Dat is een groei met bijna 20%.
De overall-conclusie van de risicoanalyse was, dat er geen wezenlijke zwakheden in de pinketen zijn en dat de voorziene groei, indien die goed gemonitord wordt, zonder problemen opgevangen kan worden. De risicoanalyse, die in 2015 voor het eerst is uitgevoerd, is jaarlijks geactualiseerd, waarbij deze conclusie steeds bevestigd werd.

2.8 Resultaten verbeteracties: beschikbaarheid Pinnen neemt toe tot 99,88%

De belangrijkste verbeteringen hebben zich afgespeeld in het domein van de winkelier/ondernemer, nl. in de winkel zèlf en in de netwerkdienst tussen winkel en transactieverwerker. Het totaal van verbeteracties heeft in de periode 2012-2017 tot meetbare verbeteringen geleid in de beschikbaarheid van de pinbetaalketen. Dit is gevisualiseerd in INFOBOX 1. Na een aanvankelijke stabilisering in de periode 2010-2012, is daarna een groei zichtbaar. Die wordt vooral veroorzaakt door een groei in het gebruik van hoogwaardige netwerkdiensten (gecertificeerde dubbele datacom, gecertificeerde mobiele back up) door de winkelier/ondernemer.
De diverse verbeteracties hebben in de periode 2012-2017 ook geleid tot een duidelijke afname van het aantal grotere verstoringen in de pinketen. Zie daarvoor INFOBOX 2.
Ondanks de bereikte resultaten blijven alle stakeholders in de pinketen continue gefocust op verdere verbetermogelijkheden van deze betaaldienst.

3. Internetbankieren (IB) en Mobiel Bankieren (MB): hoge beschikbaarheden

3.1 Verschillende factoren bepalen beschikbaarheid IB en MB

3.1.1 IB en MB: Algemeen

De beschikbaarheid van de bancaire diensten IB en MB wordt door meerdere factoren bepaald. Naast elementen als gebruikte bandbreedte, capaciteit van firewalls en andere bancaire systemen, zijn dat ten eerste de soms complexe onderlinge verwevenheid van de betaalketens van IB, MB en iDEAL. Om deze onderlinge afhankelijkheden te verminderen moest deze verwevenheid van betaalketens afgebouwd worden en moest meer redundantie in de betaalketens gebouwd worden. Op deze punten zijn in de periode 2013-2015 belangrijke stappen gezet. Dat had als resultaat, dat de beschikbaarheid van IB en MB van de meeste banken gedurende de hele periode 2014-2017 boven de 99,5% lag. Dit punt van onderlinge verwevenheid van betaalketens, wordt in het hoofdstuk van iDEAL, paragraaf 4.3, nader uitgewerkt.
De tweede factor is de potentiële gevoeligheid van IB en MB voor DDoS-aanvallen.

3.2 DDoS-aanvallen

3.2.1 IB en MB: het risico van DDoS-aanvallen

Als belangrijke dreiging voor verminderde beschikbaarheid van deze bancaire producten wordt het risico van DDoS-aanvallen op bancaire systemen gezien. Bij een DDoS-aanval worden de access gateways (de technische ingangen) van het aangevallen object geblokkeerd door het massaal aanbieden van datacomverkeer.
De consument die gebruik maakt van deze bancaire diensten zal in het algemeen via het open internet zijn opdrachten verstrekken aan zijn bank. Dit is dus wezenlijk anders dan de situatie bij Pinnen, waar het overgrote deel van de betaaltransacties via door de Betaalvereniging gecertificeerde netwerkdiensten tussen de winkellocatie en de transactieverwerker wordt getransporteerd. De gecertificeerde netwerkdiensten zijn logisch afgescheiden van het open internet. Zoals bekend, vormen de koppelvlakken met het open internet verreweg de grootste risicofactor wat betreft DDoS-aanvallen.
DDoS-aanvallen hebben zich in 2013 enkele malen voorgedaan. Na een periode van relatieve rust, werden de banken in januari en mei 2018 opnieuw getroffen door grootschalige DDoS-aanvallen.

3.2.2 De DDoS-aanvallen van januari en mei 2018 en hun impact op de beschikbaarheid

De websites van verschillende Nederlandse banken zijn van 27 tot en met 30 januari en op 27 mei 2018 regelmatig vanuit talloze locaties - via ‘botnets’, ofwel netwerken van geïnfecteerde computers - bestookt met zeer grote hoeveelheden data. Ook andere websites, zoals die van de Belastingdienst, werden in diezelfde periode getroffen. Door deze DDoS-aanvallen raakten de webservers van de betreffende banken overbelast en werden hun websites tijdelijk trager en moeilijk of zelfs niet meer bereikbaar. Als gevolg daarvan kampten de banken en hun klanten met tijdelijke verstoringen in de bereikbaarheid van internetbankieren, mobiele bankapps en betalen via iDEAL.
De DDoS-aanvallen in januari waren omvangrijker en complexer dan eerdere DDoS-aanvallen op de banken. Bij deze DDoS-aanvallen pasten de aanvaller(s) een nieuwe *modus operandi* toe. Daarbij

werden niet alleen de zogeheten mijnbank- en iDEAL-omgevingen van de bank aangevallen, maar óók alle publieke IP-adressen van de bank tegelijkertijd of één voor één. De aanval hield daarbij rekening met wat er met het aanvalsdataverkeer werd gedaan. Zodra de betreffende server van de bank - via zogeheten scrubbing services of 'wasstraten' - het ongewenste, massale data-aanbod afkomstig van de DDoS-aanval kon scheiden van het bonafide dataverkeer van klanten, waardoor de webserver niet meer 'verstopt' raakte, stopte de aanval. Vervolgens werd een andere aanvalsmethode gekozen of werd de aanval verzwaard in bandbreedte.
De aanvallen van 27 mei waren weer anders van karakter. Dit waren zgn. applicatieve aanvallen. Hierbij wordt de server van de bank op applicatief niveau aangevallen. Het mitigeren van deze aanvallen is minder eenvoudig en kan niet met de bestaande scrubbing-diensten. Om deze applicatieve aanvallen af te vangen worden nieuwe middelen ontwikkeld.
De getroffen banken hebben aangifte gedaan bij het High Tech Crime Team van de Nederlandse politie. Ook werken de banken nauw samen met het Nationaal Cyber Security Centrum (NCSC). Het onderzoek naar aanleiding van deze aangifte is complex en loopt nog.

3.2.3 Mogelijke maatregelen tegen DDoS-aanvallen

Belangrijke maatregelen om de impact van een DDoS-aanval te minimaliseren zijn het vergroten van de capaciteit in het verwerken van dataverkeer in combinatie met het plaatsen van filters, die ongewenst, massaal data-aanbod afkomstig van de DDoS-aanval scheiden van het bonafide dataverkeer, waardoor de webservers niet 'verstopt' raken.
Een andere maatregel die het risico op DDoS-aanvallen kan minimaliseren betreft het inrichten van afgeschermde, beveiligde omgevingen binnen het internet. Een dergelijke afgeschermde omgeving is alleen toegankelijk voor expliciet geautoriseerd dataverkeer. Op deze wijze kunnen verschillende, logisch-gescheiden, omgevingen gecreëerd worden, waarvan er dan één ingericht wordt voor de bancaire sector.

3.3 DDoS-aanvallen: de genomen en te nemen maatregelen

3.3.1 Samenwerking met stakeholders

Volledige onaantastbaarheid voor toekomstige DDoS-aanvallen is een utopie. Incidenteel optredende verstoringen vanwege 'succesvolle' DDoS-aanvallen zijn op voorhand helaas niet volledig uit te sluiten. Internetcriminaliteit is een constante wapenwedloop tussen aanvallers en verdedigers. Met die realiteit is het zaak om de robuustheid van voor de maatschappij vitale digitale diensten en de achterliggende systemen zodanig in te richten, dat mocht zich ondanks alle genomen beschermende maatregelen toch een verstoring voordoen, deze zo kort mogelijk duurt en zo weinig mogelijk nadelige gevolgen heeft.
Naast het continu verbeteren van hun verdedigingstechnieken, werken de banken in hun strijd tegen DDoS-aanvallen nauw samen met gespecialiseerde cybersecuritybedrijven, maar ook met de autoriteiten (waaronder DNB, de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het daaronder vallende Nationaal Cyber Security Centrum (NCSC)). De NCTV en het NCSC vallen onder verantwoordelijkheid van het ministerie van Justitie en Veiligheid. De door de Betaalvereniging aangestelde bankenliaison heeft gedurende de recente DDoS-aanvallen bijgedragen aan een continue informatie-uitwisseling tussen de banken onderling en met het NCSC. Mede hierdoor werd de nieuwe DDoS-aanvalsmethode snel gedeeld, wat eraan heeft bijgedragen dat de verstoringen sneller konden worden opgelost en uiteindelijk geheel konden worden voorkomen.

Daags na de ‘succesvolle’ DDoS-aanvallen van 29 januari 2018 gaf de NCTV aan dat de aanvallen ernstig waren, maar niet kritiek. Voorts merkt de NCTV op dat de aanvallen steeds geavanceerder worden, maar dat de banken goed in staat blijken om de aanvallen in relatief korte tijd af te slaan. In dat kader vond de NCTV dat de banken de situatie goed en professioneel hebben opgepakt. De NCTV stipte het belang aan dat aanvallen als deze laten zien dat we moeten blijven investeren in digitale veiligheid.
Aanvullend op bovenstaande: de Nederlandse banken en de Betaalvereniging zijn actief betrokken bij het publiek-private project *"No More DDoS".* Betrokkenheid omvat samenwerking met politieonderzoekers door informatie uit te wisselen, bewijsmateriaal te verzamelen, contactlijsten op te stellen, manieren te ontwikkelen voor minder tijdrovende manieren om verslagen over aanvallen in te dienen, enzovoort. De bankenliaison van de Betaalvereniging, die zorgt voor de optimale samenwerking tussen de relevante publieke en private stakeholders, maakt deel uit van de projectorganisatie. In de loop van 2018 worden concrete resultaten verwacht van dit project, dat in eerste instantie tot doel heeft het aantal succesvolle DDoS-aanvallen te reduceren.

3.3.2 Technische maatregelen

De banken maken momenteel gebruik van door externe partijen geleverde scrubbing-diensten als onderdeel van hun DDoS-mitigatiestrategie. Niet al deze partners bieden hetzelfde type diensten, kwaliteitsniveau en capaciteitsniveau. Banken en de Betaalvereniging onderzoeken momenteel de verschillende opties om de kwaliteit en de capaciteit van de geleverde scrubbing-diensten te verhogen. Daarbij wordt ook gekeken naar de onafhankelijkheid van elkaar van de verschillende aanbieders. Het gaat om internationale aanbieders, maar ook nationale initiatieven zoals de Nationale Wasstraat (NaWas).
Geen enkele branche kan zelfstandig en autonoom de risico’s op DDoS-aanvallen mitigeren. Ook de banken en andere slachtoffers zullen zich niet individueel kunnen verdedigen tegen de nieuwste state-of-the-art DDoS-aanvallen (bijvoorbeeld applicatieve aanvallen). Daarvoor is intersectorale samenwerking nodig tussen de publieke en de private sector. Daarom onderzoekt de Betaalvereniging in samenwerking met de banken andere initiatieven, zoals binnen de *Dutch Continuity Board.* Dit is een samenwerkingsverband tussen verschillende Nederlandse ISP’s, beheerders van internetexchanges en ook het NCSC, de banken en de Betaalvereniging.
Het gaat erom de Nederlandse vitale infrastructuur voor te bereiden op aanvallen die te groot zijn om te mitigeren met de "normale" mitigatiemiddelen. Dit zal in de nabije toekomst een realistisch scenario zijn. Andere maatregelen moeten dan worden genomen om complete netwerken te blokkeren (waar het DDoS-verkeer vandaan komt). De 'firewall voor Nederland'-oplossing ligt zowel in technologie (met behulp van internetproviders en internetexchanges) als in governance (die er op stuurt op het uitvoeren van dit soort maatregelen).
Het NCSC brengt vertegenwoordigers van betrokken partijen uit verschillende sectoren van de vitale infrastructuur samen - evenals onafhankelijke academici - om samen te werken aan nationale oplossingen voor dit soort aanvallen. Bij het bestrijden van DDoS-aanvallen zijn de grote internetproviders, als zijnde de transporteurs van de DDoS-aanvallen, maar zelf ook slachtoffer zijnde van die aanvallen, nadrukkelijk betrokken.
In de *Dutch Continuity Board* participeren veel partijen, met verschillende belangen, en dat maakt het managen van dit initiatief complex. Maar alle partijen zijn wel doordrongen van het grotere belang, zodat de samenwerking in constructieve sfeer gebeurt.
Het inrichten van technische oplossingen is technisch niet complex. Maar omdat afspraken gemaakt moeten worden met meerdere datacomleveranciers, beheerders van internetexchanges en banken, kan de uitvoering wel complex zijn. Wanneer het domein niet goed collectief wordt ingeregeld, ontstaan nieuwe afbreukrisico’s.

Bij het realiseren van deze initiatieven, zoals afgeschermde internetomgevingen, werkt de Betaalvereniging nauw samen met het National Cyber Security Center (NCSC), in een vorm van publiek-private samenwerking. Op deze wijze wordt gegarandeerd, dat voorgestelde maatregelen gesynchroniseerd blijven met maatregelen die in andere marktsegmenten genomen worden.
De eerste meetbare resultaten van het initiatief van het Dutch Continuity Board worden in de loop van 2018 verwacht.

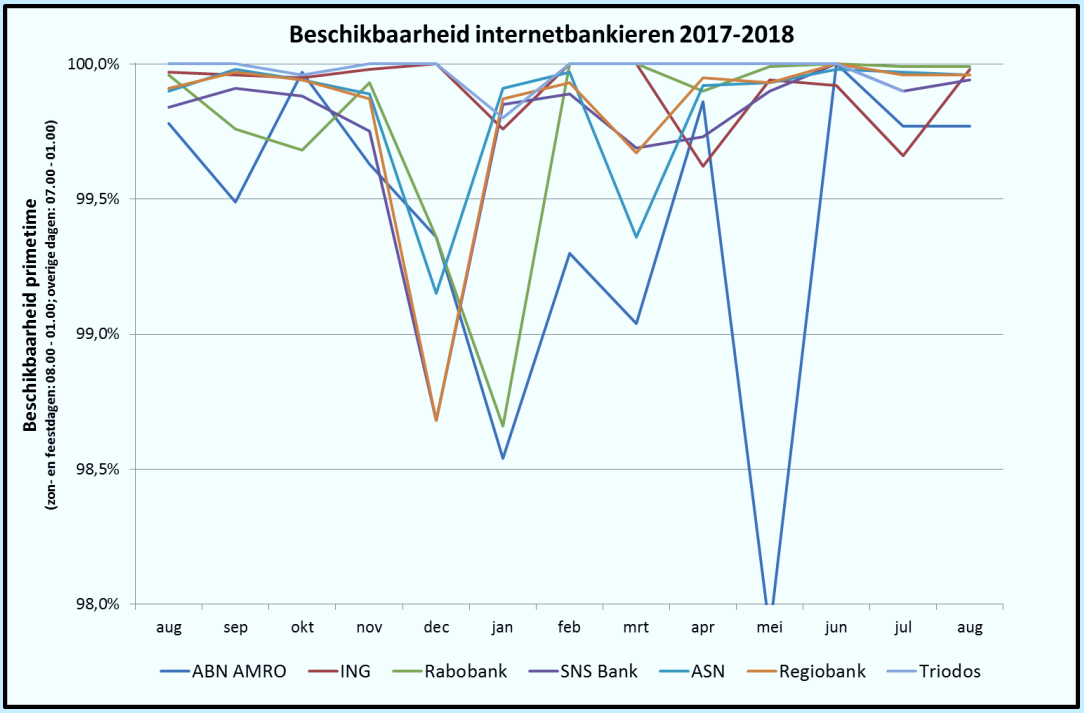
3.4 Transparantie en Communicatie: Dashboard IB en MB

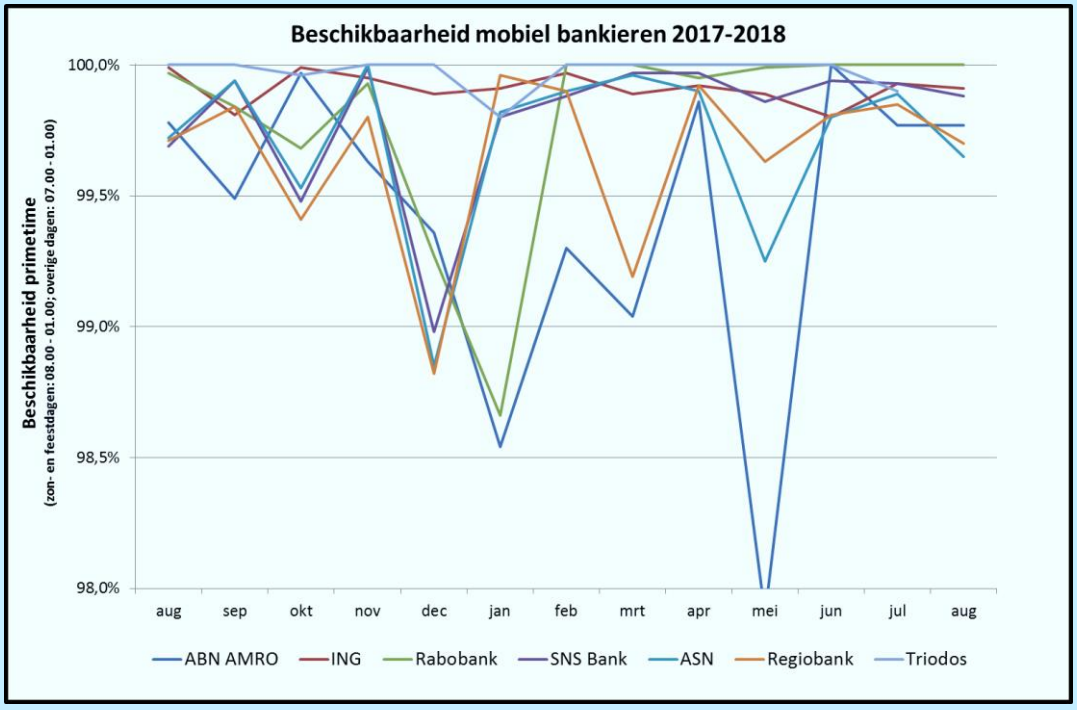
3.4.1 Historische beschikbaarheden IB en MB worden gepubliceerd

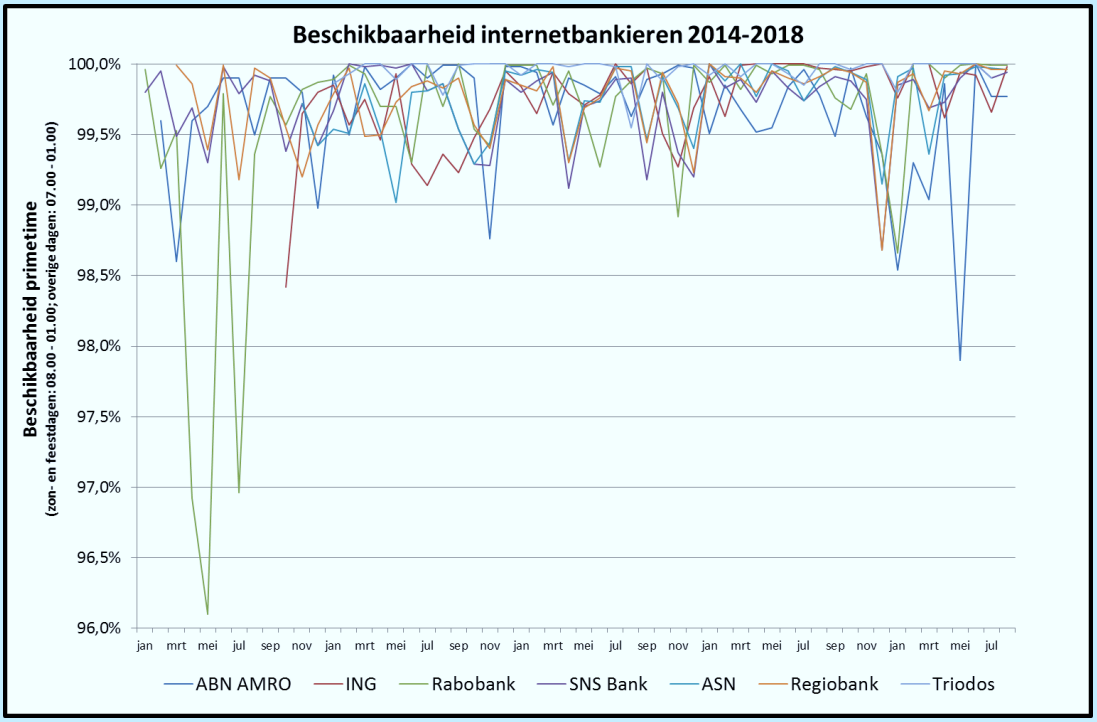
Om de markt inzicht te geven in de beschikbaarheid van de diensten IB en MB, leveren zeven banken, te weten ABN AMRO, ING, Rabobank, SNS, ASN, Regiobank en Triodos rapportages op over werkelijk behaalde beschikbaarheden. Sinds februari 2015 worden op de website van de Betaalvereniging maandelijks de gerealiseerde beschikbaarheden van de individuele banken gepubliceerd[14]. Zie hiervoor INFOBOX 3.
Zoals uit INFOBOX 3 blijkt, lag de beschikbaarheid tussen 2015 en eind 2017 permanent boven de 99%, en veelal zelfs boven 99,5%. Door de vóór 2015 genomen maatregelen zijn de grote fluctuaties van eerdere jaren tussen 2015 en eind 2017 niet meer voorgekomen. Door de DDoS-aanvallen van eind 2017/begin 2018 was de beschikbaarheid in die periode lager, zoals ook goed te zien is in de grafieken. Inmiddels zijn, door de genomen maatregelen, de beschikbaarheden weer terug op het oude niveau.

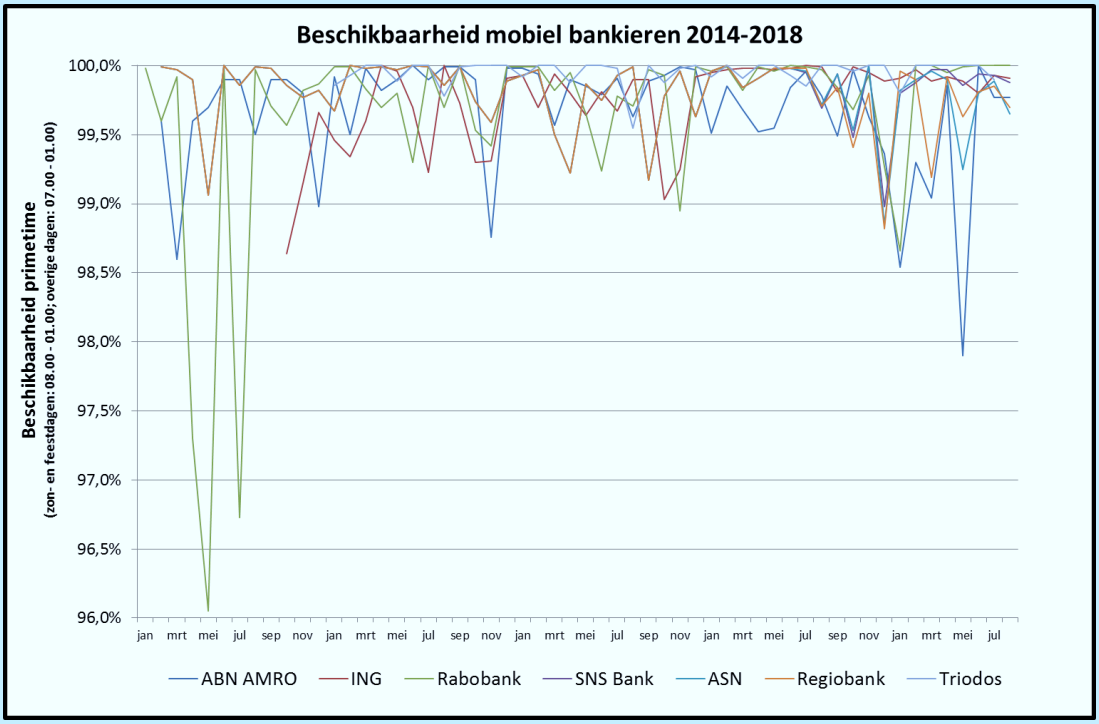
[14] Zie: https://www.betaalvereniging.nl/betaalproducten-en-diensten/beschikbaarheid-internet-en-mobiel-bankieren/

INFOBOX 3: Beschikbaarheid IB en MB 2014-2018






Beschikbaarheid internetbankieren 2014-2018
Beschikbaarheid primetime
(zon- en feestdagen: 08.00 - 01.00; overige dagen: 07.00 - 01.00)
100,0%
99,5%
99,0%
98,5%
98,0%
97,5%
97,0%
96,5%
96,0%
jan mrt mei jul sep nov jan mrt mei jul sep nov jan mrt mei jul sep nov jan mrt mei jul sep nov jan mrt mei jul
ABN AMRO
ING
Rabobank
SNS Bank
ASN
Regiobank
Triodos


Beschikbaarheid mobiel bankieren 2014-2018
Beschikbaarheid primetime
(zon- en feestdagen: 08.00 - 01.00; overige dagen: 07.00 - 01.00)
100,0%
99,5%
99,0%
98,5%
98,0%
97,5%
97,0%
96,5%
96,0%
jan mrt mei jul sep nov jan mrt mei jul sep nov jan mrt mei jul sep nov jan mrt mei jul sep nov jan mrt mei jul
ABN AMRO
ING
Rabobank
SNS Bank
ASN
Regiobank
Triodos

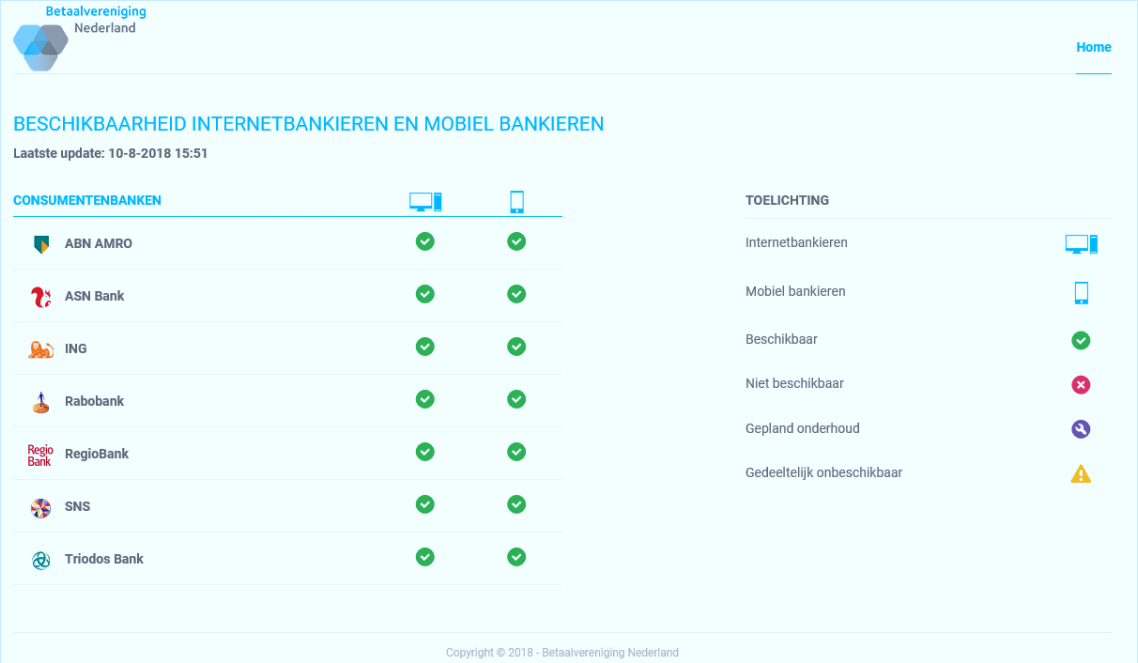
Toelichting:
Hierboven staan de grafieken van Internetbankieren (IB) en Mobiel bankieren (MB). De eerste twee grafieken geven de situatie van de laatste 13 maanden. De laatste twee grafieken geven de situatie vanaf 2014, toen de banken begonnen met het publiceren van hun beschikbaarheidscijfers.
Te zien is, dat in 2014 de beschikbaarheden van IB en MB bij enkele banken nog te wensen overlieten. Daarna trad een sterke verbetering op. In de bovenste grafiek is duidelijk de impact van de DDoS-aanvallen van januari 2018, en de nasleep daarvan. Inmiddels lijken de genomen maatregelen effect te ressorteren, en is de beweging naar boven weer ingezet. In april 2018 rapporteerden alle banken weer een beschikbaarheid hoger dan 99,8%.
De actuele grafieken zijn hier te zien: https://www.betaalvereniging.nl/betaalproducten-en-diensten/beschikbaarheid-internet-en-mobiel-bankieren/

3.4.2 Dashboard voor IB en MB van zes banken beschikbaar

De Betaalvereniging heeft in 2015 een notificatiesysteem ontwikkeld: het Online Banking Availability-systeem, OBA. Dit dashboard is geplaatst op de website van de Betaalvereniging[15]. Stakeholders en consumenten kunnen zo in één oogopslag zien of er problemen zijn met IB of MB bij de participerende banken. In INFOBOX 4 is een screen shot opgenomen van het dashboard. De banken die deelnemen aan dit notificatiesysteem kunnen in OBA storingsinformatie of geplande activiteiten plaatsen, die door stakeholders en het publiek kan worden geraadpleegd. In 2016 en 2017 hebben de banken in totaal 137 keer een melding geplaatst in dit dashboard. Dit kunnen geplande activiteiten betreffen, maar ook feitelijke, ongeplande verstoringen.

[15] Zie: https://beschikbaarheid.betaalvereniging.nl/

INFOBOX 4: Dashboard IB en MB *(screen shot)*



Toelichting:

Hierboven een *screen shot* van het dashboard van IB en MB. Op dit moment (10 augustus) waren beide diensten bij alle deelnemende banken beschikbaar.
Op dit moment worden de beschikbaarheden van zeven banken gepubliceerd op dit dashboard, te weten: ABN AMRO, ASN, ING, Rabobank, Regiobank, SNS en Triodos Bank.
Het dashboard is hier te zien: https://beschikbaarheid.betaalvereniging.nl/

3.5 Resultaten verbeteracties: beschikbaarheden IB en MB continue hoog

Het gebruik van de bancaire diensten Internetbankieren en Mobiel bankieren groeit snel. Ook nemen de door de banken aangeboden functionaliteiten binnen deze diensten toe, wat het beheer van IB en MB complexer maakt. Desondanks laten transparant gepubliceerde beschikbaarheidscijfers zien, dat de beschikbaarheid van IB en MB in de periode 2014-2017 groeide naar globaal 99,75%. De DDoS-aanvallen van begin 2018 zorgden voor een tijdelijke neergang in de beschikbaarheid. DDoS-aanvallen zijn een *fact of life*, maar de banken hebben inmiddels een aantal mitigerende middelen ontwikkeld om de gevolgen van DDoS-aanvallen snel en effectief te kunnen minimaliseren. Een permanente focus van de banken en de Betaalvereniging blijft echter noodzakelijk, vooral vanwege de externe dreigingen, die zich ook blijven ontwikkelen.

4. iDEAL: beschikbaarheid bijna op peil

4.1 iDEAL in relatie met IB en MB

Zoals in hoofdstuk 3 al aangegeven, kunnen iDEAL en IB/MB binnen zekere grenzen als elkaars alternatief gezien worden. Beide betaalmiddelen zijn middels een mobiel en middels een vast datacomnetwerk benaderbaar. In tabelvorm ziet dat er als volgt uit:

Betaalproduct → ***Datacomkanaal*** ↓	**Bankieren (reguliere overboekingen en saldo-opvragingen)**	**iDEAL**
Vaste aansluiting (PC, laptop)	Internetbankieren IB Wordt door alle relevante banken aangeboden	Vast iDEAL Wordt door alle relevante banken aangeboden
Mobiele aansluiting (smartphone, tablet)	Mobiel bankieren MB Wordt door alle relevante banken aangeboden	Mobiel iDEAL Wordt door alle relevante banken aangeboden

De tabel geeft bijvoorbeeld aan, dat een consument met zijn PC, via zijn vaste datacomaansluiting IB-transacties en iDEAL-betalingen kan verrichten. Die consument kan via de *app* op zijn smartphone ook MB-transacties en mobiel-iDEAL-betalingen doen. En die consument kan bij onbeschikbaarheid van het ene datacomnetwerk (vast of mobiel) of betaalproduct (IB/MB of iDEAL), een poging doen om met zijn andere *device* via een ander datacomnetwerk (mobiel of vast) een andere betaaltransactie (iDEAL of IB/MB) te doen. Dit mechanisme werkt optimaal, wanneer de datacomnetwerken (vast en mobiel) en de bancaire ICT-systemen voor internetbankieren en iDEAL volledig onafhankelijk van elkaar zijn ingericht. Dat is in de praktijk niet altijd het geval.
De uiteindelijke beschikbaarheid van elk van deze vier varianten wordt, naast de kwaliteit van de gebruikte datacomverbinding, vooral bepaald door de beschikbaarheid van alle relevante ICT-systemen van de betrokken banken.

4.2 iDEAL en toezicht

Alle grootbanken die iDEAL aanbieden aan hun klanten, vallen onder de *Regeling Oversight goede werking betalingsverkeer*. Hetzelfde geldt voor de banken die Pinnen aanbieden. In deze *ROgwb* zijn eisen opgenomen t.a.v. beschikbaarheden, de maximale storingsopheffingstijden en de plicht om gerealiseerde beschikbaarheden van het bancaire deel van de infrastructuur van iDEAL publiekelijk te rapporteren. DNB houdt toezicht op de naleving van de *ROgwb* door de individuele banken. In 2017 moesten de banken tijdens het hogevraagtijdvak een beschikbaarheid op kwartaalbasis realiseren van 99,64%. In 2018 en 2019 zijn die percentages resp. 99,76% en 99,88%. Zoals uit INFOBOX 5 blijkt, lukt het nog niet alle banken om dit zeer hoge ambitieniveau te realiseren.

4.3 Ontvlechting infrastructuren: resultaten worden zichtbaar

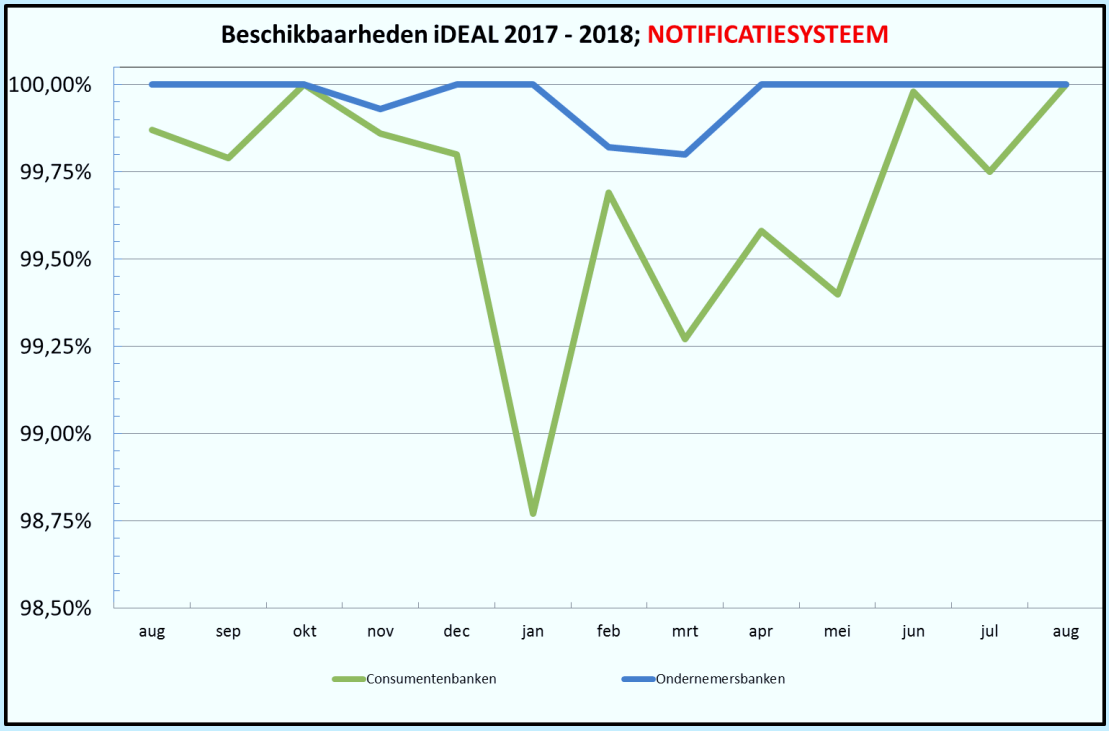
iDEAL is functioneel een onderdeel van IB/MB. Dat betekent ook, dat de onderliggende infrastructuren van iDEAL en IB/MB (ICT-systemen) onderling vervlochten kunnen zijn. Deze vervlechting kan de impact van een verstoring in één van de systemen vergroten.
Dit inzicht heeft enkele banken er reeds in 2012 en 2013 toe gebracht een scheiding door te voeren in hun systemen voor IB/MB-transacties en voor iDEAL-betalingen, waardoor iDEAL-betalingen niet meteen verstoord worden bij problemen in internetbankieren, en andersom.
De in 2014 en 2015 gerealiseerde ontvlechting van de infrastructuren van IB, MB en iDEAL heeft geleid tot een duidelijke, meetbare verbetering van de beschikbaarheid van al deze diensten in de periode 2015 tot 2017. Zie de relevante INFOBOXEN. Begin 2018 hebben de banken last gehad van de DDoS-aanvallen op hun domein. Zowel IB/MB als iDEAL hebben hier last van ondervonden. De door de banken en de Betaalvereniging ondernomen acties om de risico's van DDoS-aanvallen te mitigeren zijn uitgebreid beschreven in het vorige hoofdstuk.
Het gebruik van het betaalproduct iDEAL is gegroeid van 222,1 miljoen transacties in 2015 naar 378,1 miljoen transacties in 2017. Dat is een groei met ruim 70%. Wanneer een dienst zo snel groeit, vergt het extra aandacht van de aanbieders om de kwaliteit van de dienst op het gewenste peil te houden.
Naast de ontvlechting van de infrastructuren zijn de banken daarom ook actief om de verschillende infrastructuren robuuster te maken. Dat gebeurt bv. door (voor iDEAL) de SLA-afspraken met de transactieverwerkers te reviewen en strakker te maken en door meer redundantie en overdimensionering in de IB, MB en iDEAL- infrastructuren te realiseren. Dit betreft continue activiteiten.

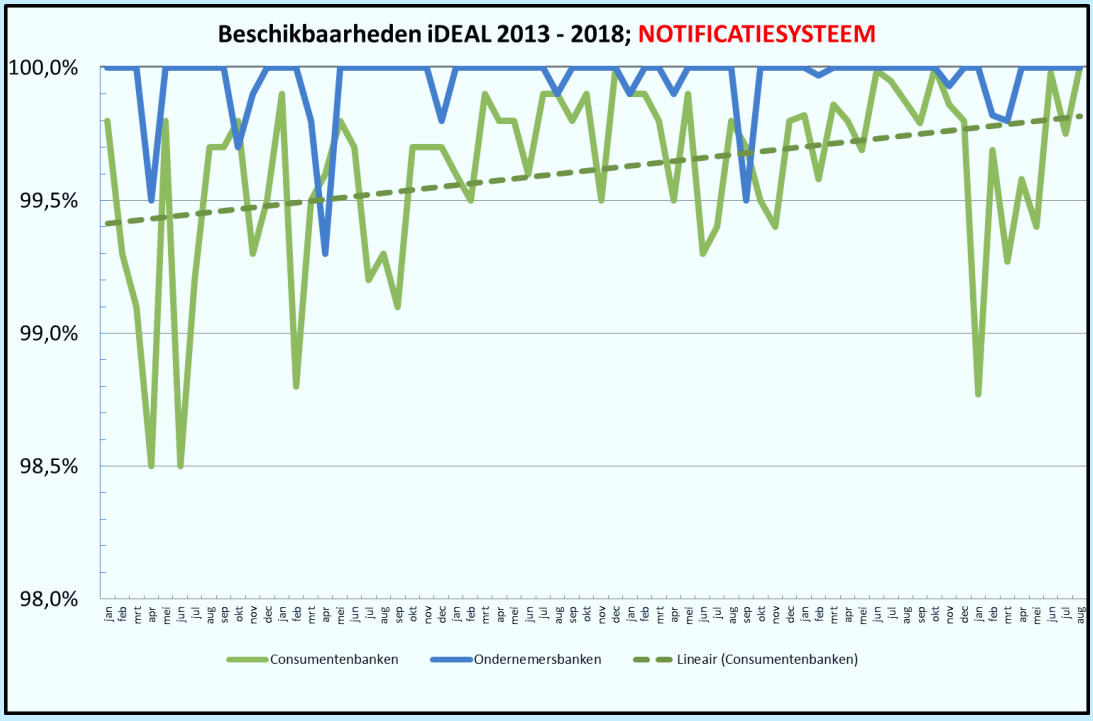
4.4 Transparantie en Communicatie

De geaggregeerde historische beschikbaarheid voor het betaalmerk iDEAL wordt gerapporteerd op de website van iDEAL.nl[16]. In een iets andere vorm geeft INFOBOX 5 de historische ontwikkeling van de beschikbaarheid weer.

[16] Zie: https://www.ideal.nl/ontvangen/kerncijfers/ideal-beschikbaarheid/

INFOBOX 5: Beschikbaarheid iDEAL 2013-2018

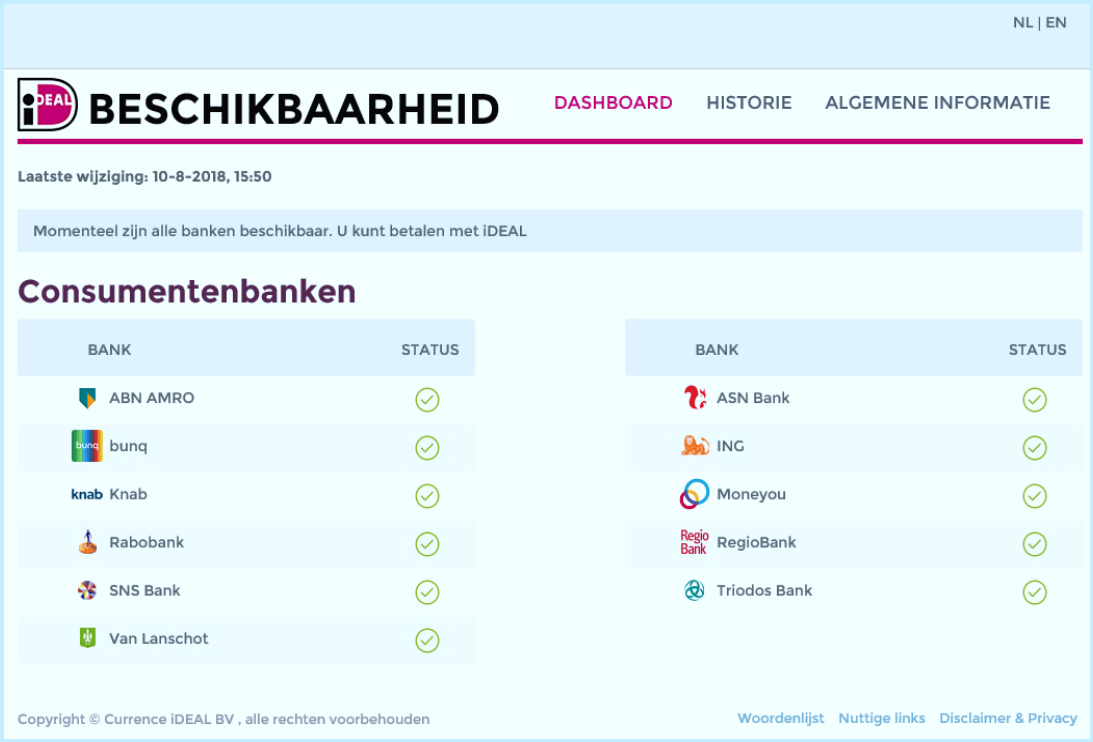




Toelichting:
De bovenste grafiek geeft de ontwikkeling van de beschikbaarheid van iDEAL van de laatste 13 maanden, terwijl de onderste grafiek de ontwikkeling vanaf 2013 weergeeft.
De groene stippellijn geeft de lineaire trendlijn. Te zien is dus, dat de trendlijn van de Consumentenbanken stijgt van 99,4% beschikbaarheid in januari 2013 tot 99,8% beschikbaarheid in april 2018. In de bovenste grafiek is duidelijk de impact van de DDoS-aanvallen van januari 2018, en de nasleep daarvan. Inmiddels lijken de genomen maatregelen effect te ressorteren, en is de beweging naar boven weer ingezet.
De Ondernemersbanken kennen het laatste jaar een beschikbaarheid van nagenoeg 100%.
De informatie van de grafieken is gebaseerd op publieke informatie. De brongegevens zijn hier te raadplegen: https://www.ideal.nl/ontvangen/kerncijfers/ideal-beschikbaarheid/

Naast het al eerder genoemde dashboard voor IB en MB, is ook een meetsysteem voor iDEAL gerealiseerd[17]. Daarop wordt zichtbaar gemaakt voor zowel ondernemers als consumenten, wat de actuele beschikbaarheid van het betaalproduct iDEAL is. Het meetsysteem is gerealiseerd op uitdrukkelijk verzoek van betrokken stakeholders en voorziet in een maximale transparantie voor wat betreft de beschikbaarheid van iDEAL bij consumentenbanken (issuers). Tevens worden historische beschikbaarheden van de individuele banken getoond. Voor een voorbeeld (screen shot) van dit dashboard: zie INFOBOX 6.

INFOBOX 6: Dashboard iDEAL (screen shot)



[17] Zie: https://beschikbaarheid.ideal.nl/

Toelichting:
Hierboven een *screen shot* van het dashboard van iDEAL. Op dit moment (10 augustus) was iDEAL bij alle tien deelnemende banken beschikbaar.
Het dashboard is hier te zien: https://beschikbaarheid.ideal.nl/

Ondanks alle genomen maatregelen, kan zich toch nog een verstoring voordoen in de iDEAL-betaalketen. Daarom is, in nauw overleg met Thuiswinkel.org, de zogenaamde Merchant Integratie Gids (MIG) ontwikkeld. De MIG dient weliswaar een breder doel, namelijk om iDEAL te integreren in de systemen van de merchant, maar zij bevat ook richtlijnen over hoe te handelen bij verstoringen en het aanbieden van alternatieve betaalproducten. Het is een levend document, dat regelmatig wordt geactualiseerd.
Daarnaast worden internetwinkeliers er altijd op gewezen, dat zij over een alternatief betaalmiddel dienen te beschikken in geval van onbeschikbaarheid van iDEAL. Mogelijke alternatieven zijn daarbij Credit Card, betaling vooraf of achteraf, of betaling onder rembours.

4.5 Resultaten van verbeteracties: beschikbaarheid iDEAL bijna op peil

Gedurende het jaar 2017 lag de beschikbaarheid van iDEAL (de issuing banken) op prime time gemiddeld op 99,83%. Dat was ruim boven de in de *Rules & Regulations* (die weer geharmoniseerd zijn met de *ROgwb)* geformuleerde eis van 99,64%. De eerste vier maanden van 2018 zakte dat percentage tot 99,33%, terwijl de eis voor 2018 op 99,76% ligt. De laatste paar maanden is de beschikbaarheid van iDEAL weer boven 99,76%. Dat is in overeenstemming met de eisen, zoals vastgelegd in de *Rules & Regulations* van Currence, maar continue aandacht en verbeteringsacties blijven noodzakelijk.
In 2019 ligt de eis op 99,88%, wat betekent, dat de betaaldienst er maximaal twee uur per kwartaal uit mag liggen gedurende het hogevraagtijdvak (06:00 uur – 00:30 uur). *De facto* betekent dat, dat DDoS-aanvallen nooit succesvol mogen zijn om deze norm te halen, zodat heel hoge eisen gesteld moeten worden aan het geheel van mitigerende maatregelen. Het mag duidelijk zijn, dat een permanente focus op dit betaalproduct noodzakelijk is om de norm, zoals vastgelegd in de *R&R*, te halen.