Visie Betaalvereniging Nederland

T.b.v. rondetafelgesprek herziene richtlijn betaaldiensten (PSD2)

De Betaalvereniging onderschrijft de doelstellingen van PSD2 volledig: meer innovatie, meer concurrentie en meer veiligheid in het betalingsverkeer. Wij willen een constructieve bijdrage leveren aan het rondetafelgesprek door via dit paper onze visie en enkele punten van zorg te delen.

1. **Voorkom verdere vertraging van de PSD2-implementatie in de Nederlandse wetgeving**.

   Meer vertraging leidt tot langere onduidelijkheid in de markt, en bovendien duurt het langer voordat nieuwe, innovatieve betaaldiensten op grond van de PSD2 in Nederland kunnen worden aangeboden. Ook staat de Nederlandse concurrentiepositie ten opzichte van de rest van de Europese Unie als vestigingsplaats voor nieuwe innovatie betaaldienstverleners op het spel.

2. **Het beeld dat PSD2 de privacy van de consument te grabbel gooit, verdient nuancering**.

   Vanuit wettelijk oogpunt is de privacybescherming van consumenten onder de PSD2 afdoende geregeld. Als een consument geen uitdrukkelijk toestemming aan derde partijen geeft voor toegang tot (informatie van) zijn betaalrekening, verandert er niets aan de huidige situatie. De vraag is echter wel of de consument zich altijd voldoende realiseert, waarvoor hij precies toestemming geeft. In dat kader is het publieke debat over privacybescherming in relatie tot de PSD2 een goede gelegenheid om deze bewustwording bij consumenten verder te vergroten.

3. **'Dedicated' open (API) interfaces zijn de beste garantie voor veilige en betrouwbare communicatie via de bancaire infrastructuur tussen derde partijen en klanten.**

   API's zijn veilig, waarborgen de privacy en zijn toekomstvast

   Banken zijn onder PSD2 verplicht om een 'digitale toegangspoort' voor derde partijen beschikbaar te stellen om hen toegang te bieden tot de bij die banken aangehouden betaalrekeningen. Via speciaal voor dat doel ingerichte ('dedicated') open Application Programming Interfaces (API's) kunnen banken deze derde partijen op een juiste, betrouwbare en veilige wijze toegang bieden tot de bij hen aangehouden betaalrekeningen, en precies die toegang geven, en precies die gegevens delen als waarvoor de rekeninghouder toestemming heeft gegeven. Dit is in beginsel ook de visie van de Europese Commissie.

   Een terugvaloptie via screen scraping levert ons inziens risico's op

   De eind deze maand door de Europese Commissie aan het Parlement en de Raad te leggen secundaire wetgeving (de technische reguleringsnormen (RTS) over sterke cliëntauthenticatie en gemeenschappelijke en beveiligde communicatienormen), schrijven voor dat banken die een API aan derde partijen beschikbaar stellen, ook een terugvaloptie (fall-back) via de reguliere klantinterface aan moeten bieden in geval de API tijdelijk uit de lucht is of niet naar behoren werkt. Aan zo'n terugvaloptie kleven een aantal belangrijke nadelen:

   - De derde partij krijgt in principe onbeperkte toegang tot alle gegevens van de rekeninghouder.
   - Consumenten zullen wennen aan het met derde partijen delen van de veiligheidscodes die zij van hun bank hebben ontvangen. Dat kan de privacy van klanten op het spel zetten en maakt hen kwetsbaar(der) voor online fraude en misbruik.

Naar wij hebben vernomen bieden de aankomende RTS banken gelukkig de mogelijkheid om – onder strikte voorwaarden – door de nationale toezichthouder te worden vrijgesteld voor de verplichting om de terugvaloptie aan te bieden. Dat vinden wij een belangrijke en waardevolle toevoeging aan de concept-RTS zoals die in mei van dit jaar door de Europese Commissie waren voorgesteld. Daarom adviseren wij de Tweede Kamer om, via het Europees Parlement, de door de Europese Commissie eind deze maand in te dienen RTS te steunen.

Op de volgende pagina's lichten wij bovenstaande punten meer in detail toe.

Amsterdam, 13 november 2017,

Mr. G. Boudewijn, adjunct-directeur Betaalvereniging Nederland.

Over Betaalvereniging Nederland

De Betaalvereniging organiseert de collectieve taken in het nationale betalingsverkeer voor haar leden. Leden zijn aanbieders van betaaldiensten op de Nederlandse markt: banken, betaalinstellingen en elektronischgeldinstellingen. Zij hebben bij ons hun gemeenschappelijke taken op het gebied van infrastructuur, standaarden en gezamenlijke productkenmerken belegd.

Wij streven naar een optimaal effectief, veilig, betrouwbaar en maatschappelijk efficiënt betalingsverkeer, waarbij innovatie een belangrijk onderdeel is. Wij verrichten hiertoe diensten die voor de leden van gezamenlijk belang zijn en voeren de regie over deze collectieve taken. Bij ons werk vervullen wij, in lijn met onze kernwaarden, een gedreven, relevante en verbindende rol. De Betaalvereniging betrekt vertegenwoordigers van eindgebruikers, onder meer van ondernemers en consumenten, actief bij haar werkzaamheden.

Namens het collectief van onze leden zijn wij zichtbaar betrokken en aanspreekbaar, en nemen wij waar nodig onze maatschappelijke verantwoordelijkheid. Daarnaast staan wij open voor, en stimuleren wij, de dialoog met andere relevante betrokkenen in het betalingsverkeer. Zo geven wij invulling aan het maatschappelijke karakter van het betalingsverkeer.

Nadere toelichting van onze kernpunten

De PSD2 is een feit, hoewel de implementatie ervan in de Nederlandse wetgeving nog even op zich laat wachten en een aantal meer technische zaken op dit moment nog niet helemaal helder is. De PSD2 is een stap voorwaarts naar nieuwe en innovatieve betaaldiensten, een efficiënter én veiliger Europees betaallandschap met meer keuze voor consumenten en zakelijke partijen.

Ten behoeve van het rondetafelgesprek over de PSD2 met de vaste commissie voor Financiën op 15 november aanstaande, wil de Betaalvereniging met onderstaande visie een constructieve bijdrage leveren aan de discussie. Onze visie is als volgt samen te vatten:

1. Voorkom verdere vertraging van de PSD2-implementatie in de Nederlandse wetgeving;
2. Het beeld dat PSD2 de privacy van de consument te grabbel gooit, verdient nuancering;
3. Dedicated open (API) interfaces zijn de beste garantie voor veilige en betrouwbare communicatie via de bancaire infrastructuur tussen derde partijen en klanten.

1. Voorkom verdere vertraging van de PSD2-implementatie in de Nederlandse wetgeving

Het PSD2-implementatieproces in onze nationale wetgeving loopt circa een half jaar vertraging[1] op. In plaats van de uiterste datum die de PSD2 voorschrijft, 13 januari 2018, zal de PSD2 naar verwachting medio juni 2018 in de Nederlandse wetgeving zijn geïmplementeerd. Verdere vertraging, bijvoorbeeld vanwege een langdurig privacy-debat, waarbij ook de aankomende Algemene Verordening Gegevensbescherming (AVG) in de volle breedte wordt betrokken, is volgens ons niet in het belang van de Nederlandse consument en van betaaldienstverleners. Vanuit wettelijk oogpunt is de privacybescherming van consumenten onder de PSD2 (en de AVG) afdoende geregeld (zie ons tweede punt hieronder).

Hoe langer de PSD2-implementatie in de Nederlandse wetgeving op zich laat wachten, des te langer de onduidelijkheid in de markt aanhoudt en des te langer het duurt voor nieuwe, innovatieve betaaldiensten ook in Nederland kunnen worden aangeboden. Daarnaast staat de Nederlandse concurrentiepositie ten opzichte van de rest van de Europese Unie op het spel. Nieuwe innovatieve ondernemingen kunnen immers, zolang de PSD2 nog niet in onze nationale wetgeving is geïmplementeerd, in Nederland geen vergunning (voor betaalinitiatiedienstverlening) of registratie (voor rekeninginformatiedienstverlening) aanvragen. Zij zullen dan mogelijk Nederland de rug toekeren en zich elders in de Unie – waar de PSD2 al wel in de nationale wetgeving is geïmplementeerd – vestigen, en aldaar een vergunning of registratie aanvragen.

2. Het beeld dat PSD2 de privacy van de consument te grabbel gooit, verdient nuancering

In de maatschappelijke discussie ontstaat de laatste tijd soms een beeld dat de privacy van consumenten – voor zover het hun betaaldata aangaat – met de komst van de PSD2 te grabbel wordt gegooid. Privacybescherming was geen directe aanleiding voor de Europese wetgever om PSD(1) te herzien, wel het bevorderen van concurrentie en innovatie op de Europese betaalmarkt. Graag willen wij het beeld van de mogelijke negatieve privacy gevolgen van de PSD2 nuanceren. Als een consument geen uitdrukkelijke toestemming aan derde partijen geeft voor toegang tot zijn

[1] Brief 'Voortgang implementatie herziene betaaldienstenrichtlijn (PSD2)' (d.d. 22 sept. 2017) van voormalig minister Dijsselbloem van Financiën aan de Tweede Kamer.

betaalrekening, verandert er niets aan de huidige situatie. Alleen de consument en zijn bank hebben dan toegang tot de betaalrekening.

Meer specifiek stelt de PSD2 het volgende:

- Voordat een derde partij[2] toegang krijgt tot de betaalrekening van een betaaldienstgebruiker[3] om namens hem een betaling te initiëren of om informatie op te halen, moet de betaaldienstgebruiker de betreffende derde partij daarvoor eerst uitdrukkelijk toestemming geven. Dat mag niet met een simpel vinkje onderaan een lange trits van voorwaarden. Daarbij geldt dat de toestemming voor het opstarten van een betaling via een betalingsinitiatiedienstverlener alleen van toepassing is op die ene betaling. Ook is het zo dat een rekeninginformatiedienstverlener alleen die informatie op mag vragen waarvoor de betaaldienstgebruiker hem uitdrukkelijk toestemming heeft gegeven.
- Een betaaldienstgebruiker moet elke derde partij afzonderlijk toestemming geven. Hij kan niet in één keer toestemming geven aan meerdere derde partijen tegelijkertijd.
- Een betaaldienstverlener kan alleen toegang tot de persoonsgegevens van een betaaldienstgebruiker krijgen, deze verwerken en/of bewaren, voor zover noodzakelijk voor het verlenen van betaaldiensten, én uitsluitend met de uitdrukkelijke toestemming van de betaaldienstgebruiker.
- Het verlenen van betaalinitiatie- of rekeninginformatiediensten is in de PSD2 het enige doel op grond waarvan gegevensverwerking door derde partijen is toegestaan. Hiervoor moet de betaaldienstgebruiker zijn uitdrukkelijke toestemming geven en dient de derde partij te beschikken over de juiste vergunning of registratie bij zijn nationale toezichthouder.
- Een derde partij mag alleen met de aanvullende uitdrukkelijke toestemming van de betaaldienstgebruiker informatie opvragen voor andere (eigen) doeleinden of andere bedrijfsactiviteiten dan het verstrekken van de gevraagde betaalinitiatie- en/of rekeninginformatiedienst.
- Zodra de betaaldienstgebruiker zijn toestemming intrekt, mag een rekeninginformatiedienstverlener niet langer toegang hebben tot (informatie van) diens betaalrekening.

In het onlangs voor consultatie gepubliceerde ‘Implementatiebesluit herziene richtlijn betaaldiensten’ legt de Nederlandse wetgever de relatie uit tussen de PSD2 en de AVG. Het begrip “uitdrukkelijke toestemming” komt twee keer voor in de PSD2, namelijk bij het verkrijgen van toegang tot betaalrekeningen en bij het verwerken van persoonsgegevens. De betekenis die de PSD2 aan dit begrip geeft, heeft in PSD2-context voorrang ten opzichte van de betekenis in de AVG. Met betrekking tot de inhoud van het PSD2-begrip en de vormgeving daarvan is de Nederlandsche Bank (DNB) in eerste instantie de relevante nationale toezichthouder. Dit laat onverlet dat als er persoonsgegevens worden verwerkt, deze verwerking wel overeenkomstig (de overige eisen van) de AVG dient te gebeuren, waarop door de Autoriteit Persoonsgegevens wordt toegezien.

---

[2] Een betaalinitiatiedienstverlener die namens de betaaldienstgebruiker (hier: de betaalrekeninghouder) een betaling op kan starten of een rekeninginformatiedienstverlener die namens de betaaldienstgebruiker betaalrekeninggegevens ophaalt.

[3] Een betaaldienstgebruiker kan zowel een consument als een zakelijke partij zijn.

Ook stelt de Nederlandse wetgever dat alleen als de betaaldienstgebruiker daarvoor zijn uitdrukkelijke toestemming geeft, een derde partij de opgehaalde betaalrekening-gerelateerde informatie mag doorleveren aan andere partijen. Denk bijvoorbeeld aan een hypotheekverstrekker die, met de uitdrukkelijke toestemming van de consument, via een rekeninginformatiedienstverlener toegang krijgt tot informatie van de betaalrekening van die consument. Op basis daarvan analyseert de hypotheekverstrekker de inkomende en uitgaande betalingen om de kredietwaardigheid van de consument vast te stellen en voor hem een op maat gesneden hypotheekofferte samen te stellen. Deze informatieverwerking door de derde partij of een eventuele andere partij aan wie de derde partij deze data doorlevert, valt buiten de reikwijdte van PSD2. De algemeen geldende Europese privacyregels, zoals de AVG, zijn dan van toepassing.

Al met al is – vanuit wettelijk oogpunt – de privacybescherming van consumenten onder de PSD2 afdoende geregeld. De vraag is echter wel of consumenten altijd voldoende beseffen, waarvoor zij nu precies uitdrukkelijke toestemming geven als zij derde partijen toegang geven tot (informatie van) hun betaalrekeningen. Meerdere partijen zullen de consument hiertoe proberen over te halen door hem (gratis) online diensten, kortingen of andere voordelen in het vooruitzicht te stellen. Zijn consumenten zich altijd bewust dat zij in die gevallen, in plaats van met geld, met hun persoonlijke data betalen? Veel online bedrijven baseren hun verdienmodel immers op handel in persoonsgegevens. Hoe meer privacy de consument prijs geeft, des te vaker hij gebruik kan (blijven) maken van gratis online diensten. Wij beschouwen het huidige publieke debat over privacybescherming in relatie tot de PSD2 als een goede gelegenheid om deze bewustwording bij consumenten te vergroten. Echter, tot meer vertraging in het PSD2-implementatieproces in de Nederlandse wetgeving zou dat, wat ons betreft, niet mogen leiden.

3. Dedicated open (API) interfaces zijn de beste garantie voor veilige en betrouwbare communicatie via de bancaire infrastructuur tussen derde partijen en klanten

De belangrijkste meer technisch-juridische secundaire wetgeving die de Europese bankenautoriteit (EBA) onder de PSD2 diende te ontwikkelen, zijn de technische reguleringsnormen (RTS) over sterke cliëntauthenticatie en gemeenschappelijke en beveiligde communicatienormen. Die normen gelden voor elektronische betalingen in het algemeen en voor de (technische) interactie tussen banken en derde partijen. De Europese Commissie stelt eind deze maand (november 2017) de definitieve RTS vast en zal deze vervolgens naar het Europees Parlement en de Raad sturen. Dat betekent dat op zijn vroegst in september 2019 de RTS effectief worden, en betaaldienstverleners aan de daarin gestelde eisen moeten voldoen. In de tussenliggende periode gelden de bestaande veiligheidsregels.

Onder PSD2 zijn banken verplicht om een ‘digitale toegangspoort’ voor derde partijen beschikbaar te stellen, om hen toegang te bieden tot de bij de banken aangehouden betaalrekeningen. Net als de Europese Commissie[4] menen wij dat open, speciaal voor dat doel ontwikkelde (‘dedicated’) interfaces – in de praktijk: Application Programming Interfaces (API’s)[5] –, de beste garantie zijn voor

[4] Zie o.a. de recente brief (d.d. 20 okt. 2017) van dhr. Valdis Dombrovskis (vicevoorzitter Europese Commissie) aan dhr. Walsh (CEO Fin Tech & Payments Association of Ireland), mevr. Beaumont (CEO Vector) en dhr. Morgan (Director of Policy & Regulation Innovate Finance).

[5] Een API is een set aan definities waarmee softwareprogramma's onderling kunnen communiceren. Het dient als een interface tussen verschillende softwareapplicaties waardoor de gebruikte code automatisch elkaar toegang tot informatie en/of functionaliteit geeft, zonder dat ontwikkelaars hoeven te weten hoe het andere programma exact werkt.

een veilige en betrouwbare communicatie via de bancaire infrastructuur tussen derden partijen en klanten.

Naar wij – uit onofficiële bronnen – hebben vernomen, schrijven de eind deze maand door de Europese Commissie voor te leggen RTS voor dat banken die een dedicated interface aan derde partijen beschikbaar stellen, in beginsel ook een terugvaloptie (fall-back) aan moeten bieden. Dit voor de situatie waarin de dedicated interface om wat voor reden dan ook tijdelijk uit de lucht is of niet naar behoren zou werken. De terugvaloptie moet in dat geval derde partijen via screenscraping[6] – overigens wel mét identificatie tussen bank en derde partij – via de 'reguliere' online klanteninterface van de bank toegang bieden tot de bij die bank aangehouden betaalrekeningen.

Aan bovengenoemde terugvaloptie kleven volgens ons echter een aantal belangrijke nadelen. Het biedt derde partijen onbeperkte toegang tot alle gegevens die in de beveiligde online bankomgeving van de rekeninghouder beschikbaar zijn. Denk hierbij aan betaalrekening- en spaarrekeninggegevens, maar ook aan hypotheekgegevens, roodstandlimieten en adres- en woonplaatsgegevens. Het zorgt er daarnaast voor dat rekeninghouders wennen aan het met derde partijen delen van de veiligheidscodes die zij van hun bank hebben ontvangen. Dat zet de privacy van klanten op het spel en maakt hen kwetsbaar(der) voor online fraude en misbruik. Immers, ook cybercriminelen proberen de veiligheidscodes van consumenten te verkrijgen, maar dan om er online fraude mee te plegen of anderszins misbruik van te maken.

Echter, de aankomende RTS bieden de banken zeer waarschijnlijk de mogelijkheid om – zij het onder strikte voorwaarden – door de nationaal aangewezen toezichthouder te worden vrijgesteld voor de verplichting om deze terugvaloptie aan te bieden. De voorwaarden zijn, onder meer, dat de dedicated interface voldoet aan de eisen van PSD2 en de RTS, voldoende is getest én gebruikt door derde partijen, en eventuele beschikbaarheids- en/of functionaliteitsproblemen met de dedicated interface meteen worden opgelost. Derde partijen dienen de aangeboden dedicated interface te gebruiken, maar kunnen bij eventuele storingen daarin onder voorwaarden gebruik maken van de terugvaloptie. Hierover dient de nationale toezichthouder te worden geïnformeerd, die eventueel de genoemde vrijstelling kan intrekken.

De hierboven genoemde onder strikte voorwaarden te bieden vrijstelling vinden wij een belangrijke en waardevolle toevoeging aan de concept-RTS zoals die in mei van dit jaar door de Europese Commissie waren voorgesteld. Daarom adviseren wij de Tweede Kamer om, via het Europees Parlement, de door de Europese Commissie eind deze maand in te dienen RTS te steunen.

API's zijn dé norm in de markt en worden veel gebruikt om verschillende softwareprogramma's op effectieve, efficiënte, veilige en betrouwbare wijze onderling te laten communiceren. API's kunnen voor allerlei doeleinden worden ingezet, waaronder voor het door banken op juiste, betrouwbare en veilige wijze toegang bieden aan derde partijen tot de bij hen aangehouden betaalrekeningen.

[6] Screenscraping is een computertechniek waarbij de gegevens vanaf een voor het computerbeeldscherm bedoelde webpagina worden uitgelezen en gebruikt voor invoer in een ander, achterliggend, programma. Bestaande aanbieders die reeds betaalinitiatie- en/of rekeninginformatiediensten aanbieden, werken in de regel met screenscraping-technieken.