Toegang van derden tot rekeningen en sterke cliëntauthenticatie

PSD2 – risico's voor banken

11 maart 2020

Sanne Fransen

PSD 2 is de nieuwe Europese richtlijn met een herziene systematiek voor betalingen van consumenten en bedrijven aan leveranciers. Deze richtlijn zet de huidige betalingssystematiek op zijn kop. In het bijzonder verandert de rol van de traditionele banken om ruimte te maken voor nieuwe intermediairs in het betalingsverkeer. Als voorbeeld van de consequenties voor banken schetst dit artikel de risico's die PSD 2 voor ze meebrengt op twee technische terreinen: de authenticatie van klanten die betalingen of gerelateerde activiteiten doen en de uitwisseling van betaalinformatie tussen klant, bank en leverancier. Deze risico's zijn direct relevant voor IT-auditors die actief zijn in de financiële sector. Het doel van dit artikel is om inzicht te geven in deze risico's.

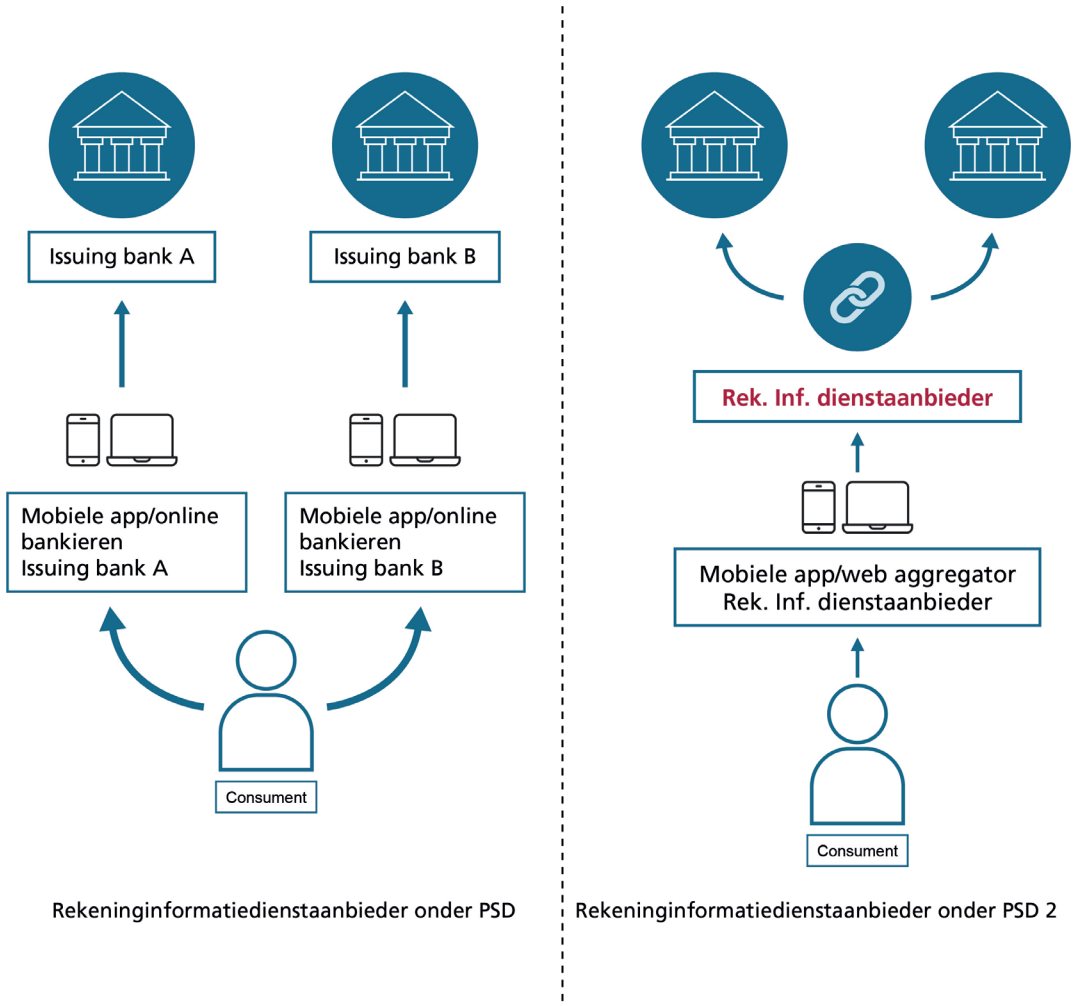
De belangrijkste drijfveren achter de introductie van de tweede *Payment Services Directive* (PSD 2) van de EU zijn de exponentiële groei van het aantal internet- en mobiele betalingen en de snel evoluerende Europese Fintech-sector. Sinds 19 februari 2019 heeft Nederland als laatste Europese land PSD 2 officieel omgezet in nationale wetgeving. PSD 2 wordt ondersteund door zes richtlijnen en vijf technische reguleringsnormen (*Regulatory Technical Standards* – RTS). Een daarvan is de RTS rondom sterke cliëntauthenticatie en gemeenschappelijke, veilige open communicatiestandaarden. Met de komst van PSD 2 verandert de traditionele betalingssytematiek. Banken zijn niet langer verantwoordelijk voor de gehele waardeketen van betalingen, wat tot verminderde controle kan leiden. Door de toetreding van nieuwe spelers tot de betalingsmarkt krijgen fraudeurs wellicht nieuwe kansen. Dit artikel schetst de risico's op het gebied van sterke cliëntauthenticatie (*Strong Customer authentication* – SCA) en toegang van derden tot rekeningen (*Third-Party Access to Accounts* – XS2A)[1].

PSD 2 heeft bij veel banken geleid tot omvangrijke investeringen. Navraag leert dat sommige banken, vooral de wat kleinere, PSD 2 puur als een compliance-issue beschouwen, terwijl de Nederlandse grootbanken zich ook richten op de concurrentievoordelen bij meebewegen in de sterk veranderende wereld van betalingen.

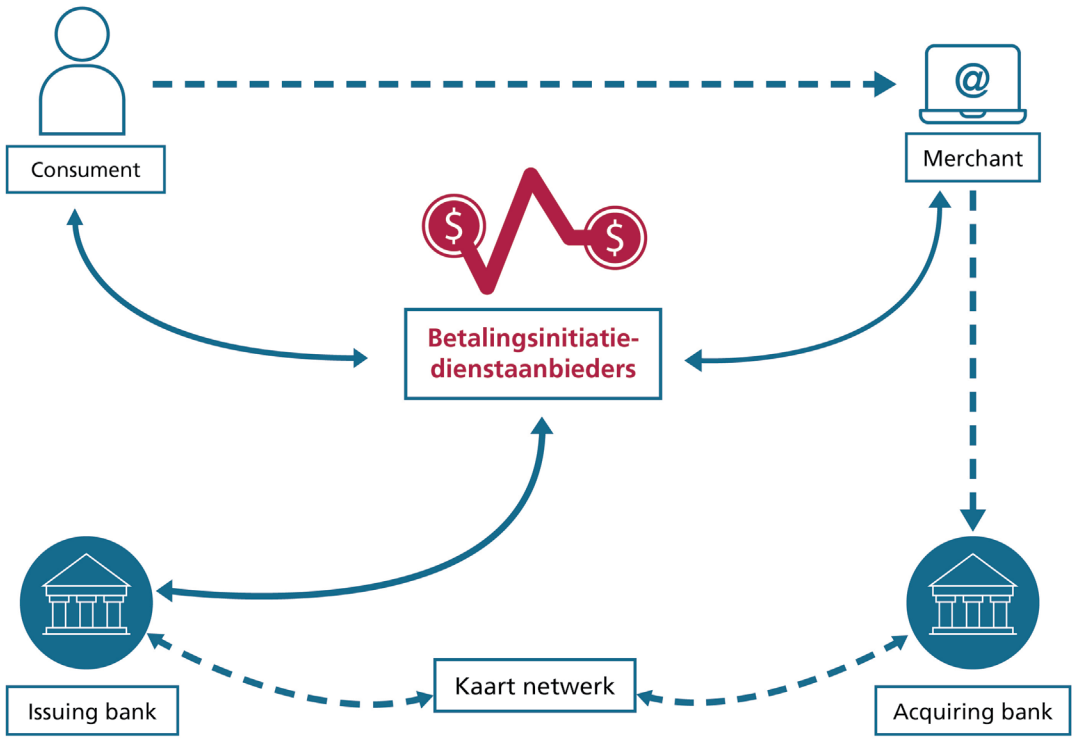
PSD2 – een geharmoniseerd landschap voor betalingsverkeer

De richtlijn is door de Europese Commissie geïntroduceerd om haar voorganger (PSD) te moderniseren en rekening te houden met nieuwe soorten betalingsdiensten die nog niet waren gereguleerd. Door deze nieuwe diensten onder het toepassingsgebied van PSD 2 te brengen, zullen transparantie, innovatie en veiligheid van het betalingsverkeer aanzienlijk toenemen. PSD 2 biedt een wettelijk kader om consumenten beter te beschermen en tegelijkertijd de Europese betalingsmarkt verder te openen, met het doel de concurrentie te bevorderen en innovatie te faciliteren. PSD 2 verbetert tevens de samenwerking en informatie-uitwisseling tussen financiële autoriteiten en vereist verbeterde beveiligingsmaatregelen voor alle betalingsdienstaanbieders. [EURO15]

PSD 2 introduceert vereisten voor twee typen nieuwe spelers in de markt van het betalingsverkeer: aanbieders van rekeninginformatie en aanbieders van betalingsinitiatiediensten. [EURO15-2] Onder PSD 2 kan een rekeninginformatiedienstaanbieder een geconsolideerd overzicht bieden van alle betaalrekeningen van een klant op een online platform, zelfs als die accounts bij meerdere banken lopen. Betalingsinitiatiedienstaanbieders fungeren als link tussen de bankrekening van de betaler en het bankplatform van de verkoper, de *merchant*. Zij kunnen namens een gebruiker een betaling uitvoeren, bijvoorbeeld bij het kopen van een artikel in een webwinkel. In dat geval kan de klant de betalingsinitiatiedienstaanbieder toestemming geven om toegang te krijgen tot zijn/haar betaalrekening bij een andere betalingsdienstaanbieder, zoals een bank. Alle spelers moeten voldoen aan de voor hen relevante vereisten van de PSD 2. [LAMME17] Een voorbeeld hiervan is betalen via iDEAL op Marktplaats. Verkopers kunnen hierbij betaalverzoeken via iDEAL initiëren en daarmee de financiële afhandeling van een verkoop via de website in eigen hand nemen. Deze dienst wordt aangeboden door een derde partij. Met behulp van deze partij kan een verkoper een betaalverzoek aanmaken. De koper ontvangt vervolgens dit verzoek en wordt met het ingaan op het verzoek direct naar zijn eigen online bankomgeving geleid. De betaling via zijn betaalrekening wordt in die omgeving direct afgehandeld. De derde partij controleert hierbij de identiteit van de verkoper en slaat diens gegevens en IBAN-nummer op. [HAME17]



Figuur 1: De rekeninginformatiedienstaanbieder onder PSD en PSD2



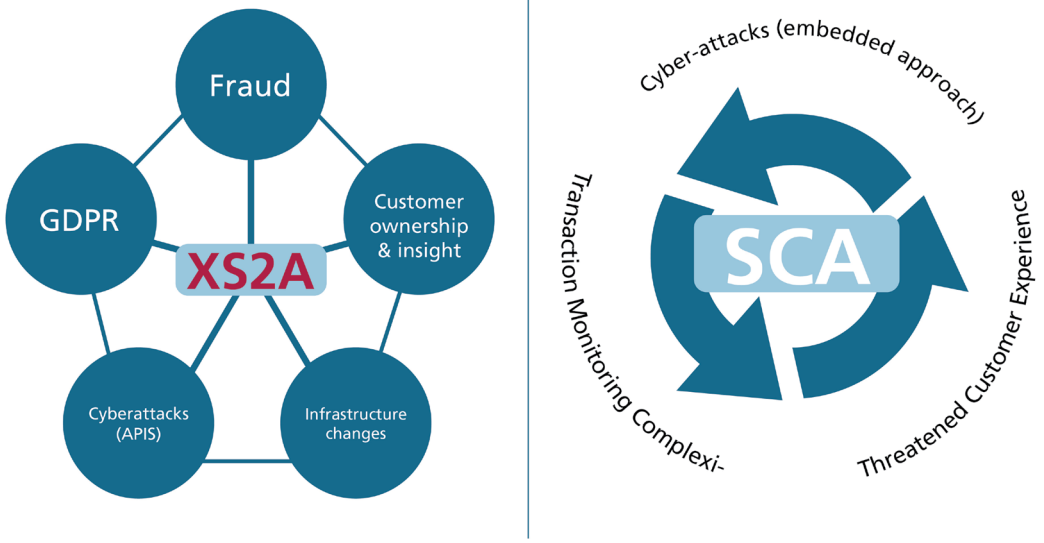
Figuur 2: Betalingsinitiatiedienstaanbieders onder PSD 2

Veel van de vereisten van PSD 2 houden verband met toegang van derden tot rekeningen en sterke cliëntauthenticatie. Zo zijn banken onder PSD 2 wettelijk verplicht om derde partijen toegang te verlenen tot de bankrekeningen van klanten die hiervoor toestemming hebben gegeven. De banken moeten dan hun waardevolle klantgegevens en processen aanbieden aan partijen zonder commerciële contracten met deze partijen af te sluiten. [EBA17] Dit geldt voor zowel financiële als niet-financiële instellingen (een voorbeeld van een dergelijke goedgekeurde vergunningsaanvraag van een niet-financiële instelling is een aanvraag van Google in Litouwen). De sector beschouwt *Application Programming Interfaces* (API's) als de beste oplossing om deze toegang op een veilige en effectieve manier technisch te regelen. [DEUT17]

Een ander belangrijk element van PSD 2 zijn de nieuwe wettelijke vereisten voor sterke cliëntauthenticatie bij betalingen op afstand (*payer-not-present*). Sterke cliëntauthenticatie is vereist wanneer klanten online toegang krijgen tot hun betaalrekening of een elektronische betalingstransactie initiëren of acties via een extern kanaal uitvoeren die een risico van betalingsfraude of ander misbruik met zich meebrengen. Om het vertrouwen in transacties via internet te vergroten is gezocht naar een balans tussen de noodzaak van verbeterde beveiligingsmaatregelen bij betalingen op afstand en de behoefte aan gebruiksvriendelijkheid en toegankelijkheid. In PSD 2 is dit gebeurd door enerzijds sterke cliëntauthenticatie verplicht te stellen en anderzijds zeven[2] vrijstellingen op te nemen. Een voorbeeld is de vrijstelling bij onbemande betaalautomaten voor vervoerbewijzen en parkeergelden. [EBA17]

Potentiële risico's voor banken

Wat zijn nu de mogelijke risico's voor banken die de introductie van PSD 2 met zich mee brengt in termen van toegang van derden tot rekeningen en sterke cliëntauthenticatie? Om te beginnen hebben banken de afgelopen jaren veel tijd en geld geïnvesteerd in de beveiliging van hun ecosysteem, maar met de komst van de nieuwe dienstaanbieders zijn zij niet langer meer verantwoordelijk voor de gehele waardeketen van betalingen. Daardoor wordt het wellicht moeilijker voor ze om alle risico's binnen de keten te herkennen. Fraudeurs kunnen zich bijvoorbeeld gaan richten op de systemen en processen (API's) van de, mogelijk zwakker beveiligde, derde partijen. Naast dit algemene risico zijn er specifieke risico's op de gebieden van toegang van derden tot rekeningen en sterke cliëntauthenticatie. De figuren 3.1 en 3.2 schetsten een framework als mogelijk startpunt voor banken om deze risico's te beheersen.



Figuur 3.1: Risico Framework toegang van derden tot rekeningen en sterke cliëntauthenticatie

Low	Medium	High
Low	Medium	Medium
Low	Low	Low

Figuur 3.2: Risico matrix gebaseerd op kans en impact

Risico's bij derdentoegang tot rekeningen

Door de introductie van PSD 2 zou het risico op fraude kunnen toenemen. Nu derde partijen kunnen fungeren als intermediair tussen klanten en banken, verliezen banken immers mogelijk de grip op die klantgegevens waar ze traditioneel op vertrouwden om fraude te detecteren. Ook kan het voor banken moeilijk zijn om de betrouwbaarheid van de klant- en transactiegegevens te beoordelen en potentiële frauduleuze derde partijen te identificeren. Tevens zal er een snelle toename zijn van nieuwe 'ingangen' voor fraudeurs, aangezien banken verplicht zijn om interfaces beschikbaar te stellen aan derde partijen die daarom verzoeken.

Een ander risico voor banken vormen de radicale technische veranderingen die nodig zijn om te voldoen aan de vereisten van de technische standaarden voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatie. Vooral bij de wat kleinere banken kunnen gebrek aan budget en mankracht leiden tot onvoldoende investering van geld en tijd. Daarnaast formuleert de richtlijn wel de technische vereisten, maar op welke wijze daaraan moet worden voldaan is minder duidelijk. Vooral in de

beginfase was het nog een open vraag welke implementatie-keuzes toezichthouders wel of niet acceptabel zouden vinden. Dit is een risico omdat het voor banken na de implementatie moeilijk of vrijwel onmogelijk is om fundamentele architectuurkeuzes uit een eerder stadium te wijzigen. [CORT17]

Nog een potentieel risico voor banken ontstaat door een mogelijke toename van cyberaanvallen door de vereiste om open *application programming interfaces* (API's) aan te bieden. Nieuwe kanalen impliceren nieuwe aanvalsmogelijkheden en moeten dus voldoende worden beveiligd, getest en gecontroleerd. Een extra risico ontstaat wanneer banken voortbouwen op traditionele (*legacy*) B2B API's, waarvan de architecturen misschien niet veilig genoeg meer zijn. [MANS16]

Daarnaast bestaat er een risico voor banken dat de Algemene Verordening Gegevensbescherming (AVG) onvoldoende in acht genomen wordt bij het verlenen van toegang tot rekeningen aan derden. Banken kunnen dit risico beheersbaar maken door de juiste toestemmingsmechanismen te implementeren. [EROG16]

Het framework onderkent tot slot het risico dat banken hun inzicht in de klant deels kwijtraken. Klantervaring en klanttevredenheid zien banken als vereisten voor succes. De toetreding van nieuwe spelers, met hun innovatieve oplossingen, kan er echter toe leiden dat het inzicht in de klant afneemt. Denk hierbij aan banken die in zekere mate het directe contact met hun klanten verliezen wanneer ze fungeren als *utility-type service* voor derde partijen. [LIGH16] Dat is overigens minder erg dan het lijkt omdat banken ook al via hun kernactiviteiten veel inzicht in hun klanten krijgen. Voorbeelden hiervan zijn *Know your Customer* (KYC), *Anti Money Laundering* (AML) en *Foreign Account Tax Compliance Act* (FATCA) activiteiten. De impact van PSD 2 hierop blijft beperkt.

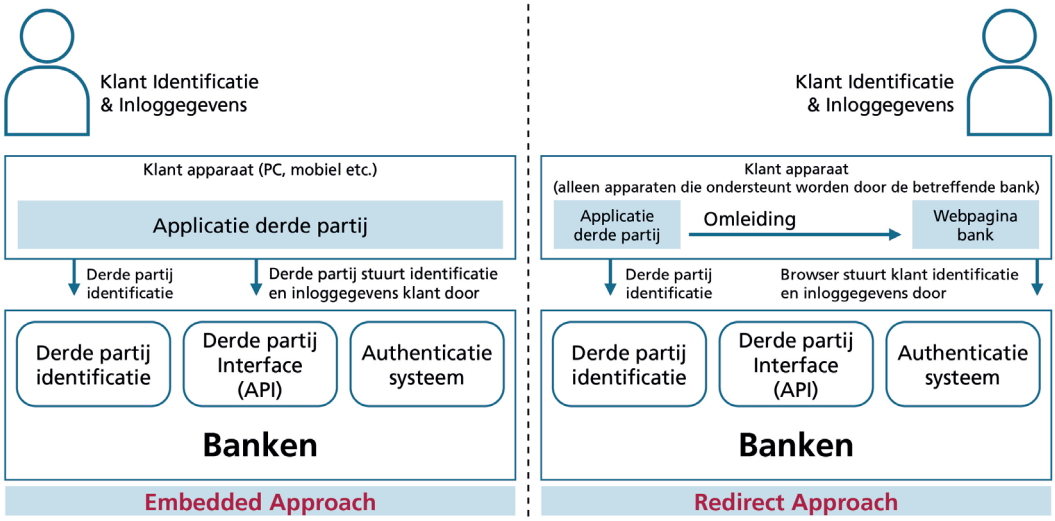
Risico's rond cliëntauthenticatie

Banken lopen om te beginnen het risico dat klanten door de sterke cliëntauthenticatie een complexere en doorbroken 'klantreis'[3] ervaren. Toch maken lang niet alle banken gebruik van de zeven vrijstellingen die de European Banking Authority (EBA) biedt om dat risico tegen te gaan. Die banken hebben verschillende redenen om dat risico te accepteren. Zo geven ze hoge prioriteit aan een veilige betalingsomgeving voor klanten. Verder wensen ze mee te bewegen in een gedigitaliseerde economie. Ten slotte schrikken ze terug voor de complexiteit en kosten van de uitvoering van de vrijstellingen. [EBA17]

Een tweede risico op het gebied van sterke cliëntauthenticatie houdt verband met mechanismen voor transactie-monitoring. Een op risico's gebaseerde aanpak is cruciaal om fraude te verminderen, maar het betaalproces moet ook voldoende gebruiksvriendelijk zijn. Met het oog op dat laatste heeft de EBA de zeven vrijstellingen op sterke cliëntauthenticatie vastgesteld. Voorwaarde voor banken om van die vrijstellingen gebruik te mogen maken is dat ze transactiemonitoring hebben ingericht, wat een ingewikkeld

proces is. Zo moeten ze eerst een systeem ontwikkelen, daarna regels beschrijven en implementeren, en tot slot het ingerichte systeem verbinden met de gehele infrastructuur. Deze complexiteit kan leiden tot misverstanden, buitensporige kosten en eventuele tijdrovende herstelactiviteiten. [DNB17]

Een laatste risico is gericht op nieuwe *phishing*-mogelijkheden die ontstaan bij gebruik van de *embedded-approach*[4]. In deze aanpak is de omgeving waarin klanten hun gegevens invoeren niet die van bank maar die van de derde partij. Deze derde verzendt de ingevoerde gegevens via een API naar de bank. Doordat banken de gegevens via deze omweg ontvangen, zijn ze voor de beveiliging van het betaalproces afhankelijk van de derde partijen, terwijl ze niet te allen tijde weten of die partijen de juiste processen en protocollen hebben ingesteld. Bovendien weet de klant niet altijd of zijn gegevens wel met een geldige derde partij worden gedeeld. Deze omstandigheden vergroten de mogelijkheden voor phishing. De tegenhanger van de *embedded-approach is de redirect-approach*[5]. Deze benadering heeft over het algemeen de voorkeur van banken omdat ze hierbij kunnen steunen op hun eigen authenticatie-proces met hun eigen set aan maatregelen om phishing te voorkomen. Voor de duidelijkheid zijn deze twee benaderingen weergegeven in figuur 4.



Figuur 4: Embedded versus Redirect approach

Tot slot

Dit artikel geeft een globaal inzicht welke inherente risico's PSD 2 met zich meebrengt voor banken op de gebieden van toegang van derden tot accounts en sterke cliëntauthenticatie. Voor meer uitleg verwijs ik naar mijn afstudeerverslag. Daarin is ook meer informatie te vinden over mijn onderzoek. [FRA19]

De veranderingen in het betalingslandschap hebben niet alleen gevolgen voor banken, maar ook voor de uit te voeren IT-auditwerkzaamheden. Zo zijn bijvoorbeeld audits

nodig op de implementatie van de technische standaarden voor sterke cliëntauthenticatie en voor de gemeenschappelijke en veilige open communicatiestandaarden (artikel 3 beveiligingsmaatregelen en artikel 18 Transactierisicoanalyse). Daarnaast moet PSD 2 een plaats krijgen in de auditplanning. Denk aan onderwerpen zoals: rapporteren over fraude, rapporteren over incidenten, uitgifte e-IDAS certificaten[6], et cetera.

Deze consequenties vielen buiten de scope van mijn afstudeerreferaat en dus ook buiten het bestek van dit artikel.

Literatuur

[CORT17] Cortet, M., Jung, N., Matzner, H. & Schaefer, C. *PSD2 sparks innovation in open banking systems*. Article Deutsche Bank & Innopay, 2017. https://cib.db.com/docs_new/PSD2_Open_Banking_Ecosystems_Innopay_DB_Article_June2017.pdf, bezocht op: 15 december 2019.

[DEUT17] *Deutsche Bank. Cash management – Financial Intelligence Guide: Payment services – Leveraging PSD2 to open up transaction banking*. The Financial Times Limited (July 2017).

[DNB17] De Nederlandsche Bank. *Post-event transaction monitoring process for payment service providers*. DNB Guidance. https://www.toezicht.dnb.nl/en/binaries/51-236852.pdf, bezocht op: 15 december 2019.

[EBA17] European Banking Authority. *Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*.

[EROG16] Eroglu, H., Bhatia, G., Bhardwaj, A. & McFarlane, A. *PSD II & Open Banking – Security and Fraud impacts on banks*. Accenture Payments Services Research. https://www.accenture.com/_acnmedia/pdf-40/accenture-psd2-open-banking-security-fraud-impacts.pdf, bezocht op: 15 december 2019.

[EURO15] European Commission. *Payment Services, Revision of EU Legislation*. URL: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en#revision-of-eu-legislation, bezocht op: 13 november 2019.

[EURO15-2]European Commission. *Directive 2015/2366/EC of the European Parliament and of the Council on payment services in the internal market – Payment services (PSD II).*

[FRAN19] Fransen, S.C. The potential risks of the introduction of the second Payment Service Directive (PSD II). Afstudeerscriptie IT Audit, Compliance & Advisory, Vrije Universiteit, Amsterdam

[HAME17] Den Hamer, J., Middelburg R. R*egulering van betaaldienstverlening onder PSD II – is tech eating everything?* http://www.openaccessadvocate.nl/tijdschrift/ondernemingenfinanciering/2017/4/OenF_1570-1247_2017_025_004_002/fullscreen, bezocht op: 16 december 2019.

[LAMME17] Lammerts, I., Ma, D., Ploeger, N., Deutekom, B.A., van Eerten, S.J., Vink, N., … Schaap, R.B. *De tweede Europese betaaldienstenrichtlijn (PSD II) en de risico's op fraude en witwassen*. https://www.amlc.nl/wp-content/uploads/2018/02/PSD2-en-de-risicos-op-fraude-en-witwassen-definitief-1.1.pdf, bezocht op: 15 december 2019.

[LIGH16] Light, J., McFarlane, A., Barry, K. & Ruotsila, I. *Seizing the Opportunities unlocked by the EU's Revised Payment Services Directive. Accenture Payment Services Research.* https://www.accenture.com/t20160505t180127__w__/ca-fr/_acnmedia/pdf-15/psd2-seizing-opportunities-eu-payment-services-directive%20(1)%20(1).pdf, bezocht op: 15 december2019.

[MANS16] Mansfield – Devine, S. Open Banking: Opportunity & Danger. C*omputer Fraud & Security, 10: 8-13.*

Noten

1. Dit artikel is gebaseerd op mijn afstudeerscriptie voor de opleiding IT Audit, Compliance & Advisory aan de Vrije Universiteit, Amsterdam
2. Vrijstellingen: (1) Betaalrekeninginformatie (2) Contactloze betalingen in verkooppunten (3) onbemande betaalautomaten voor vervoerbewijzen en parkeergelden (4) Betrouwbare betalingsbegunstigden (5) Recurrente transacties (6) Overmakingen tussen door dezelfde natuurlijke persoon of rechtspersoon aangehouden rekeningen (7) Transacties voor kleine bedragen.
3. De klantreis (customer journey) is het pad dat een consument aflegt om uiteindelijk een bepaald product of een bepaalde dienst te doorlopen.
4. Embedded approach: volledig geautomatiseerd proces waarbij de betaling wordt geïnitieerd uit naam van de klant.
5. Redirect approach: de klant wordt omgeleid door middel van een web-interface, om sterke cliëntauthenticatie toe te passen en zo een betaling te initiëren.
6. Europese burgers en bedrijven moeten sinds september 2018 bij alle Nederlandse organisaties in de publieke sector kunnen inloggen met een door Europa erkend nationaal inlogmiddel. Dat hebben de EU-lidstaten met elkaar afgesproken in de eIDAS-verordening. Bron: https://www.eherkenning.nl/aansluiten-op-eherkenning/eidas

S.C. (Sanne) Fransen Msc | Senior Advisor Cyber Security, Data Protection & Privacy, Risk Management bij *EY Financial Services Advisory*

Sanne Fransen werkt bijna vijf jaar bij EY in het Cybersecurity Advisory Team. Veel van haar klanten zitten in de financiële sector. Sanne richt zich vooral op opdrachten binnen het privacy-domein, maar ook op het gebied van Strategy, Risk & Compliance. Juni 2019 heeft zij de postdoctorale master IT Audit, Compliance & Advisory afgerond met als afstudeeronderwerp PSD2.