De toegang tot betaalrekeningen onder PSD2

Mr. P.T.J. Wolters & prof. dr. B.P.F. Jacobs, datum 19-03-2018

Datum
19-03-2018

Auteur
Mr. P.T.J. Wolters & prof. dr. B.P.F. Jacobs[1]

Folio weergave
Download gedrukte versie (PDF)

Vakgebied(en)
Ondernemingsrecht / Algemeen

Het ‘recht op toegang’ in de Richtlijn Betalingsdiensten 2 (‘PSD2’) geeft betalingsdienstaanbieders toegang tot de betaalrekeningen van de gebruikers. Het recht creëert verschillende risico’s met betrekking tot de beveiliging van betaalrekeningen en de bescherming van persoonsgegevens. Deze bijdrage analyseert deze risico’s. Zij besteedt hierbij in het bijzonder aandacht aan de technische reguleringsnormen die zijn vastgesteld door de Europese Commissie in de vorm van een gedelegeerde verordening, na voorbereiding door de Europese Bankenautoriteit.
De risico’s voor de bescherming van de persoonsgegevens ontstaan in het bijzonder doordat het begrip ‘rekeninginformatiedienst’ zo breed en vaag geformuleerd is dat het een grote variatie aan diensten kan omvatten. Deze keuze faciliteert innovatie en mededinging op de markt voor betalingsdiensten. Zij leidt er echter ook toe dat de beperkingen aan het recht op toegang op verschillende manieren zijn te omzeilen.
Deze ordening van de belangen blijkt ook ten aanzien van de beveiliging van de betaalrekening. De PSD2 stelt dienstaanbieders in staat om gebruik te maken van het door de bank aangeboden authenticatieproces. De gedelegeerde verordening bepaalt echter niet duidelijk hoe het proces verder dient te worden afgehandeld. De vrijheid om dit proces in te richten heeft de prioriteit over het belang om authenticatie zo sterk mogelijk te maken.
Dezelfde conclusie geldt met betrekking tot de mogelijkheid van betalingsdienstaanbieders om een eigen authenticatieproces te gebruiken. De normen eisen niet dat de bank in staat wordt gesteld om dit proces te controleren. Hoewel de PSD2 dit niet expliciet bepaalt, lijkt de bank te moeten vertrouwen op de betalingsdienstaanbieder. Iedere dienstaanbieder wordt hierdoor een potentiële bron van risico’s.
De richtlijn en de gedelegeerde verordening bevatten verschillende waarborgen voor de bescherming van de gebruiker. Uiteindelijk is de beveiliging van de rekening en de bescherming van persoonsgegevens in het stelsel van de PSD2 echter ondergeschikt aan de ontwikkeling van de markt voor betalingsdiensten.

1. Inleiding

De ‘Richtlijn Betalingsdiensten 2’ of ‘PSD2’[2] heeft verschillende doelstellingen. Sinds de vaststelling van de ‘Richtlijn Betalingsdiensten 1’[3] hebben zich significante technische ontwikkelingen voorgedaan. Daarnaast is de markt voor betaaldiensten gegroeid en vernieuwd. De PSD2 is bedoeld om het Europese juridische kader aan te passen aan deze ontwikkelingen.[4] Zij beoogt hierdoor bij te dragen aan rechtszekerheid, harmonisatie, mededinging en de ontwikkeling van een geïntegreerde markt. Tegelijkertijd garandeert zij, volgens haar overwegingen, een hoog niveau van consumentenbescherming en een beperking van de risico’s op fraude.[5]

De PSD2 reguleert twee nieuwe betalingsdiensten: ‘betalingsinitiatiediensten’ en ‘rekeninginformatiediensten’.[6] Zij faciliteert deze diensten in het bijzonder doordat banken worden verplicht om de ‘betalingsinitiatiedienstaanbieders’ en ‘rekeninginformatiedienstaanbieders’ (hierna gezamenlijk ‘dienstaanbieders’) kosteloos toegang te verlenen tot de betaalrekeningen van de gebruikers. De introductie van dit ‘recht op toegang’ heeft grote gevolgen voor de dienstaanbieders, gebruikers en banken (§ 2). De precieze vormgeving van dit recht is afhankelijk van de technische reguleringsnormen (§ 3). Zij is bovendien van groot belang voor de beveiliging van de betaalrekening en de bescherming van de persoonsgegevens van de gebruikers (§ 4). Deze bijdrage geeft een overzicht van de risico’s die bij de verschillende vormen van toegang ontstaan. Zij beantwoordt de volgende onderzoeksvraag: *In hoeverre creëert het recht op toegang van de betalingsinitiatie- en rekeninginformatiedienstaanbiederseen balans tussen de bescherming van de gebruiker en de ontwikkeling van de markt voor betalingsdiensten?* Een analyse van de PSD2 laat zien dat een adequate balans ontbreekt. De bescherming van de gebruiker is uiteindelijk ondergeschikt aan de ontwikkeling van de markt voor betalingsdiensten (§ 5).

2. Het recht van toegang in het stelsel van de PSD2

Het stelsel van de PSD2 en het recht op toegang zijn gebaseerd op een afweging tussen verschillende belangen. '*Fintech*' bedrijven ontwikkelen nieuwe financiële diensten, waaronder nieuwe manieren om te betalen en rekeninginformatie in te zien. De dienstaanbieders kunnen deze diensten echter niet aanbieden als de banken niet meewerken. Deze banken controleren immers de toegang tot de bij hen gehouden betaalrekeningen. Zij zijn hierdoor in staat om de concurrentie op de markt voor betalingsdiensten te beperken.

De richtlijn beperkt deze mogelijkheid door de uitvoering van betalingsdiensten juridisch te faciliteren. Zij doet dit in het bijzonder door de dienstaanbieders recht te geven op toegang tot de 'betaalrekeningen' van de 'betalingsdienstgebruikers'.[7] De precieze inhoud van dit 'recht op toegang' hangt af van de aangeboden dienst. Wij werken dit in de volgende subparagrafen uit.

De (potentiële) gebruikers profiteren van dit recht op toegang doordat het hun in staat stelt om de diensten te gebruiken. De toegang leidt echter ook tot verschillende fraude- en privacyrisico's. Hij zou bijvoorbeeld kunnen worden misbruikt om de rekening te plunderen. De privacy van de gebruikers wordt bovendien aangetast doordat nieuwe dienstaanbieders inzicht krijgen in hun financiële gegevens. Deze gegevens kunnen onder andere worden misbruikt voor chantage, ongeoorloofde prijsdiscriminatie en door de informatie door te verkopen.

Het is voor de gebruikers van belang om deze risico's tot een minimum te beperken. De richtlijn doet dit onder andere door te bepalen dat alleen partijen met een vergunning gebruik kunnen maken van het recht op toegang.[8] Dienstaanbieders die alleen rekeninginformatiediensten aanbieden, zijn op grond van artikel 33 PSD2 vrijgesteld van een groot deel van de vereisten voor een vergunning. Zij hoeven slechts een registeraanvraag in te dienen.[9]

Voor de banken, of 'rekeninghoudende betalingsdienstaanbieders',[10] brengt de PSD2 voornamelijk nadelen met zich. Ze zijn verplicht om de dienstaanbieders kosteloos toegang te verlenen tot de bij hen gehouden betaalrekeningen. Het uitvoeren van deze verplichting brengt kosten met zich. De banken moeten immers een extra systeem dat de uitoefening van het recht op toegang mogelijk maakt inrichten, onderhouden en beveiligen.[11]

De banken krijgen daarnaast te maken met nieuwe concurrentie. Vóór de PSD2 waren zij, in ieder geval juridisch (§ 4.2), de enige die bij het aanbieden van betalingsdiensten toegang hadden tot de bij hen gehouden betaalrekeningen. De richtlijn neemt dit competitieve voordeel weg. Dit heeft niet alleen invloed op de markt voor betalingsinitiatiediensten en rekeninginformatiediensten. De omstandigheid dat gebruikers minder direct contact hebben met de banken, zorgt er ook voor dat deze banken minder goed in staat zijn om andere producten aan hun gebruikers aan te bieden.[12]

De banken kunnen ook van deze verandering profiteren. Ze kunnen immers zelf ook toegang krijgen tot de rekeningen bij andere banken.[13] Het is echter niet waarschijnlijk dat deze mogelijkheden voor hen opwegen tegen de toegenomen concurrentie. Deze concurrentie zal immers niet alleen uit de hoek van andere banken komen, maar naar verwachting ook van technologiereuzen zoals Facebook, Apple, Amazon, Microsoft en Google.[14]

2.1 Betalingsinitiatiedienst

Artikel 4 lid 15 van de PSD2 definieert een betalingsinitiatiedienst als "een dienst voor het initiëren van een betalingsopdracht, op verzoek van de betalingsdienstgebruiker, met betrekking tot een betaalrekening die bij een andere betalingsdienstaanbieder wordt aangehouden". Het gaat hier bijvoorbeeld om iDEAL in Nederland, Sofort in Duitsland en Trustly in Zweden.

Deze dienst is bijvoorbeeld van belang voor de betaling van online afgenomen diensten. Hij geeft de begunstigde, zoals een webshop, direct de zekerheid dat de betaling succesvol is verzonden.[15] De betalingsinitiatiedienst kan daarnaast de invoering van een betalingsopdracht vergemakkelijken, bijvoorbeeld door het bedrag en de gegevens van de begunstigde en de gebruiker in te vullen. Het is ten slotte mogelijk om de authenticatie te versnellen. Een telefoon kan bijvoorbeeld een proces met een combinatie van een pinpas, pincode en fysieke kaartlezer vervangen door authenticatie aan de hand van een op de telefoon gegenereerde code, een vingerafdruk of gezichtsherkenning (§ 4.4).

De betalingsinitiatiedienstaanbieder kan zijn dienst alleen verlenen als de bank de via de dienst verzonden betalingsopdrachten uitvoert. Het is daarnaast noodzakelijk dat bank de opdracht 'begrijpt' en, in het licht van de vereisten van de PSD2, de herkomst (authenticiteit) ervan kan vaststellen. De dienst kan bijvoorbeeld niet functioneren als de bank het bedrag interpreteert als het rekeningnummer van de begunstigde. De dienstaanbieder moet daarom toegang hebben tot een interface die het mogelijk maakt om betalingsopdrachten te versturen (§ 4.1).

Artikel 66 van de PSD2 reguleert het recht op toegang van de betalingsinitiatiedienstaanbieder. Lid 1 formuleert de vrijheid om gebruik te maken van een betalingsinitiatiedienst als een recht van de gebruiker. De bank is op grond van lid 2 verplicht om dit recht te waarborgen door de met instemming van de gebruiker verzonden betalingsopdrachten uit te voeren. Lid 4

werkt deze plicht nader uit. De bank moet de dienstaanbieder onmiddellijk na ontvangst van de betalingsopdracht informatie verstrekken over de initiëring en uitvoering van de transactie en de via de dienst verzonden opdrachten hetzelfde behandelen als betalingsopdrachten die direct door de gebruiker zijn verstuurd. De vervulling van deze plichten mag op grond van lid 5 niet afhangen van het bestaan van een contractuele relatie tussen de bank en de betalingsinitiatiedienstaanbieder. Deze dienstaanbieder hoeft de bank dan ook niet voor de toegang te betalen.[16]
Lid 3 stelt verschillende grenzen aan dit recht op toegang. De betalingsinitiatiedienstaanbieder dient zich op grond van sub d ten overstaan van de bank te identificeren. Hij mag de verkregen informatie volgens sub c alleen verstrekken aan de begunstigde. Op grond van sub f kan hij bovendien alleen gegevens opvragen die nodig zijn voor het verstrekken van de dienst. Hij dient daarnaast op grond van sub e geen 'gevoelige betalingsgegevens' op te slaan. Hieronder vallen 'persoonlijke beveiligingsgegevens' en andere gegevens waarmee fraude kan worden gepleegd.[17] De dienstaanbieder mag de gegevens op grond van sub g ten slotte niet gebruiken voor andere doelstellingen dan de uitvoering van de door de gebruiker gevraagde betalingsinitiatiedienst.

2.2 Rekeninginformatiedienst

Artikel 4 lid 16 van de PSD2 definieert de rekeninginformatiedienst als "een onlinedienst voor het verstrekken van geconsolideerde informatie over een of meer betaalrekeningen die de betalingsdienstgebruiker bij een andere betalingsdienstaanbieder of bij meer dan één betalingsdienstaanbieder aanhoudt". Onder deze definitie kunnen verschillende diensten vallen.

De PSD2 gaat uit van een dienst die de gebruiker in staat stelt om verschillende rekeningen via één systeem te raadplegen.[18] Andere diensten zijn echter niet expliciet uitgesloten. Een rekeninginformatiedienst kan bijvoorbeeld ook de categorisering van de verschillende transacties of de analyse van de inkomsten- en uitgavenstromen omvatten.[19] Hij kan daarnaast bestaan uit de verstrekking van rekeninginformatie aan een derde, zoals een financieel adviseur of een bedrijf dat gepersonaliseerde advertenties verzorgt.[20]

De rekeninginformatiedienstaanbieder kan zijn diensten alleen verrichten als hij toegang heeft tot de informatie over de betaalrekeningen. Artikel 67 van de PSD2 reguleert deze toegang. Het recht is grotendeels op dezelfde manier vormgegeven als het recht van de betalingsinitiatiedienstaanbieder. Ook de beperkingen zijn vergelijkbaar. De ruime definitie van het begrip 'rekeninginformatiedienst' doet echter afbreuk aan deze beperkingen.

Allereerst bepaalt artikel 67 lid 2 sub f PSD2 dat de dienstaanbieder de via het recht op toegang verkregen gegevens niet mag gebruiken voor andere doelstellingen dan de uitvoering van de door de gebruiker uitdrukkelijk gevraagde rekeninginformatiedienst. Het is bijvoorbeeld niet toegestaan om de met het recht op toegang geraadpleegde gegevens te gebruiken voor het aanbieden van andere producten of diensten. Deze beperking kan echter worden omzeild door te bepalen dat het doen van persoonlijke aanbiedingen op basis van de rekeninginformatie onderdeel uitmaakt van de dienst.[21] Zij kan daarnaast worden ontweken door vast te leggen dat de dienst bestaat uit de verstrekking van informatie aan een derde. De rekeninginformatiedienst kan bovendien worden geïncorporeerd in een meeromvattende relatie. Hij kan bijvoorbeeld een onderdeel zijn van een hypotheekaanvraag bij een kredietverstrekker. In dit geval verstrekt de rekeninginformatiedienstaanbieder de gegevens aan de kredietverstrekker zodat deze een persoonlijk aanbod kan doen aan de gebruiker.

Sub f maakt daarnaast niet duidelijk of de rekeninginformatiedienstaanbieder de gegevens voor andere doelstellingen mag gebruiken als hij hier een aparte verwerkingsgrondslag, zoals de aanvullende toestemming van de gebruiker, voor heeft. Het verbod op verdere verwerkingen geldt volgens sub f 'overeenkomstig de voorschriften inzake gegevensbescherming'. Deze toevoeging suggereert dat het gebruik voor andere doelstellingen mogelijk wel is toegestaan als dit geschiedt in overeenstemming met het gegevensbeschermingsrecht.[22] Het artikel verschilt hiermee van artikel 66 lid 3 sub g PSD2. Het verbod om de gegevens voor andere doeleinden te gebruiken is voor de betalingsinitiatiedienstaanbieder niet op deze wijze geclausuleerd. Daar lijkt het niet mogelijk om het verbod door middel van aanvullende toestemming te omzeilen.

De richtlijn maakt bovendien niet duidelijk welke gegevens onder het recht op toegang vallen.[23] De rekeninginformatiedienstaanbieder dient in beginsel toegang te krijgen tot dezelfde gegevens als de gebruiker van de door de bank aangeboden online-banking omgeving.[24] Hij mag op grond van sub e echter geen gevoelige betalingsgegevens opvragen. Verder bepaalt artikel 67 lid 2 sub d PSD2 slechts dat de dienstaanbieder alleen toegang heeft tot de 'aangewezen betalingsrekeningen en de betrokken betalingstransacties'. De toegang dient daarnaast te worden beperkt tot de informatie die noodzakelijk is voor het uitvoeren van de dienst.[25] Welke informatie nodig is, hangt echter af van de aangeboden dienst. De dienstaanbieder kan deze beperking daarom omzeilen door de rekeninginformatiedienst ruim te formuleren.

De rekeninginformatie over de gebruiker kan ook betrekking hebben op 'derden'. Dit speelt bijvoorbeeld als de gebruiker geld heeft overgemaakt naar (of ontvangen van) een andere natuurlijke persoon. De rekeninginformatiedienstaanbieder die toegang heeft tot deze gegevens weet in dit geval niet alleen dat de gebruiker geld heeft overgemaakt (of ontvangen), maar ook dat de derde geld heeft ontvangen (of overgemaakt). De derde heeft hier echter, anders dan de gebruiker, geen

toestemming voor gegeven. Verschillende auteurs besteden aandacht aan de vraag of een rekeninginformatiedienstaanbieder ook toegang mag hebben tot deze '*silent party data*'.[26]

Het krijgen of verlenen van toegang tot een rekening is een verwerking van persoonsgegevens.[27] Als de dienstaanbieder ook toegang krijgt tot de persoonsgegevens van derden, worden ook deze gegevens verwerkt. De bank en de rekeninginformatiedienstaanbieder moeten hiervoor voldoen aan een van de gronden van artikel 6 lid 1 Algemene Verordening Gegevensbescherming ('AVG').[28] De grondslag van de bank is helder. Zij heeft, na implementatie van de PSD2, een wettelijke verplichting om toegang te verlenen.[29]

De grondslag van de rekeninginformatiedienstaanbieder is minder duidelijk. Hij zou slechts kunnen bestaan uit de behartiging van gerechtvaardigde belangen in de zin van artikel 6 lid 1 sub f van de AVG. De belangen van de aanbieder en de gebruiker van de dienst moeten hierbij worden afgewogen tegen de belangen van de *silent party*. Deze afweging is afhankelijk van de inhoud van de dienst.

Als de dienst bestaat uit het verschaffen van een overzicht van de rekeningen en transacties aan de gebruiker, is de afweging in de kern hetzelfde als in het geval dat de gebruiker de rekeninginformatie inziet in de door de bank aangeboden online-omgeving. Ook in deze situatie heeft de derde immers geen toestemming gegeven voor de verwerking. Toch lijken de in noot 26 genoemde auteurs in dit geval niet te twijfelen aan de rechtmatigheid. Het bezwaar tegen het verschaffen van *silent party data* lijkt bij vergelijkbare rekeninginformatiediensten voornamelijk te zijn gebaseerd op de gedachte dat de dienstaanbieders minder betrouwbaar zijn dan banken.[30] Hoewel dit risico realistisch is, strookt het niet met de uitgangspunten van de PSD2. De richtlijn gaat er nu juist vanuit dat rekeninginformatiedienstaanbieders, als zij voldoen aan bepaalde voorwaarden, wel met de gegevens kunnen worden vertrouwd.

De afweging kan anders uitvallen bij diensten waarbij de rekeninginformatie bestemd is om ook te worden verstrekt aan een ander. Dit speelt bijvoorbeeld als de dienst bestaat uit het doorlichten van de financiële situatie van de gebruiker ten behoeve van een ander, zoals een kredietverstrekker. Dit gebeurt nu ook al: financiers vragen voor de verstrekking van een hypotheeklening bijvoorbeeld om een rekeningafschrift. Het veelvuldig gebruik van rekeninginformatiediensten stelt partijen echter in staat om dergelijke persoonsgegevens van derden op veel grotere schaal te verwerken dan voorheen het geval is. Dit leidt tot een grotere aantasting van de belangen van een grotere groep derden.

2.3 Het recht op toegang en de bescherming van de betalingsdienstgebruiker

De richtlijn streeft bij de regulering van de toegang tot betaalrekeningen naar een balans tussen de verschillende belangen. Tegenover het uitgebreide recht op toegang van de dienstaanbieders staan verschillende waarborgen.

De bescherming ziet allereerst op de beveiliging van de betalingsdiensten. Een bank kan het recht op toegang op grond van artikel 68 lid 5 van de PSD2 aan een dienstaanbieder ontzeggen om objectieve en op voldoende aanwijzingen gebaseerde redenen in verband met niet-toegestane of frauduleuze toegang. Alle dienstaanbieders moeten daarnaast op grond van artikel 95 van de PSD2 passende maatregelen nemen om de beveiligingsrisico's te beperken. Zij zijn op grond van artikel 96 verplicht om grote beveiligingsincidenten te melden aan de bevoegde autoriteit en de gebruikers.[31] De dienstaanbieders dienen daarnaast op grond van artikel 97 sterke, tweefactoren, cliëntauthenticatie te gebruiken.[32] Ze moeten ten slotte op een beveiligde manier met de bank communiceren.[33]

De waarborgen zien ook op de bescherming van persoonsgegevens. De in Richtlijn 95/46/EG (Gegevensbescherming) opgenomen waarborgen met betrekking tot de bescherming van persoonsgegevens gelden volgens overweging 89 ook bij betalingsdiensten. Dit is ten aanzien van betalingsinitiatiedienstaanbieders vastgelegd in artikel 94 lid 1 van de PSD2. Deze verwijzingen gelden op grond van artikel 94 van de AVG vanaf 25 mei 2018 als referenties aan de verordening.

Daarnaast bepaalt artikel 94 lid 2 van de PSD2 dat dienstaanbieders alleen met uitdrukkelijke toestemming van de gebruiker toegang krijgen tot persoonsgegevens die noodzakelijk zijn voor het aanbieden van hun betalingsdiensten. De PSD2 is hiermee strenger dan de AVG.[34] Artikel 6 lid 1 AVG bepaalt immers dat de verwerking van persoonsgegevens onder andere rechtmatig is als de betrokkene hier toestemming voor heeft gegeven (sub a) *of* dit noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (sub b). Artikel 94 lid 2 PSD2 eist dat aan beide voorwaarden is voldaan.

De in de PSD2 opgenomen waarborgen met betrekking tot de bescherming van persoonsgegevens zijn in het geval van rekeninginformatiediensten minder streng. Dit komt onder andere omdat deze dienst, in vergelijking met de betalingsinitiatiedienst, veel minder duidelijk is gedefinieerd (§ 2.2). Daarnaast is artikel 94 van de PSD2 op grond van artikel 33 lid 2 PSD2 niet van toepassing op rekeninginformatiedienstaanbieders die geen andere betalingsdiensten aanbieden. Hieruit volgt overigens niet dat deze dienstaanbieders zijn vrijgesteld van het gegevensbeschermingsrecht. De AVG is immers, ook zonder uitdrukkelijke bepaling in de PSD2, van toepassing op alle bedrijven die persoonsgegevens verwerken.[35] De vrijstelling heeft slechts betrekking op de bijzondere in artikel 94 PSD2 opgenomen regels.

Het ontbreken van bijzondere privacywaarborgen met betrekking tot rekeninginformatiediensten is problematisch. Het recht

op toegang maakt het mogelijk om eenvoudig en op grote schaal rekeninginformatie van gebruikers en derden te verwerken (§ 2.2). Ook de huidige praktijk van lange, ingewikkelde toestemmingsverklaringen die door gebruikers niet of nauwelijks gelezen worden, zal met de PSD2 niet plotseling veranderen. De beantwoording van de vraag of en in hoeverre dit is toegestaan, wordt overgelaten aan de AVG. Deze kwestie leent zich daarom voor richtsnoeren van toezichthouders, zeker als het gebruik van de diensten een grote vlucht neemt.

3. De technische reguleringsnormen

De Europese Bankautoriteit ('EBA') speelt een belangrijke rol bij de uitwerking van de verplichtingen op grond van de artikelen 95, 96 en 97 van de PSD2. De EBA dient de verplichtingen van de artikelen 95 en 96 uit te werken in 'richtsnoeren' in de zin van artikel 16 van de 'Europese Bankautoriteit Verordening'.[36] Zij is daarnaast op grond van artikel 98 verplicht om 'technische reguleringsnormen' in de zin van artikel 10 van de Europese Bankautoriteit Verordening op te stellen met betrekking tot sterke cliënt authenticatie en beveiligde communicatie. De precieze vormgeving van het recht op toegang en zijn beveiliging is mede afhankelijk van deze normen. Uiteindelijk is de Europese Commissie bevoegd om de technische reguleringsnormen vast te stellen. Zij heeft de normen op 27 november 2017 bekendgemaakt.[37] De technische reguleringsnormen zijn opgenomen in een gedelegeerde verordening ('GV') en zullen op grond van artikel 38 lid 2 GV vanaf 14 september 2019 van toepassing zijn. Voor het overige dient de PSD2, inclusief het recht op toegang, echter al op 13 januari 2018 te zijn geïmplementeerd. Deze datum is in Nederland niet gehaald.[38]

Bestaande dienstaanbieders mogen hun activiteiten in de periode tussen de implementatie van de PSD2 en het van kracht worden van de GV blijven uitoefenen. Zij mogen gebruikmaken van het recht op toegang, maar zijn op grond van artikel 115 lid 4 van de PSD2 niet gebonden aan de in de artikelen 65, 66, 67 en 97 bedoelde beveiligingsmaatregelen.[39] Zij zijn slechts gebonden aan de algemenere beveiligingsverplichtingen, zoals de verplichtingen om risicobeperkende maatregelen te treffen en om de verwerkte persoonsgegevens te beveiligen.[40]

4. De vormgeving van het recht op toegang in gedelegeerde verordening

In deze paragraaf bespreken wij de invloed van de GV op de vormgeving van het recht op toegang. Wij gaan achtereenvolgens in op het verschil tussen een toegewijde interface en een aangepaste gebruikersinterface (§ 4.1), het verbod op '*screen scraping'* (§ 4.2), de rol van het authenticatieproces van de bank (§ 4.3), de mogelijkheden van de betalingsdienstaanbieder om een eigen authenticatieproces te gebruiken (de § 4.4 en § 4.5) en de respectievelijke rollen van identificatie, authenticatie en dynamische koppelingen (§ 4.6). Wij gaan hierbij steeds in op de beveiligingsrisico's die bij deze vormen van toegang ontstaan.

4.1 Een toegewijde interface of een aangepaste gebruikersinterface

Een bank die haar gebruikers online toegang tot hun rekeningen geeft, is op grond van artikel 30 lid 1 GV verplicht om een interface aan te bieden die dienstaanbieders in staat stelt om toegang te krijgen tot de betaalrekening. De bank mag hierbij op grond van artikel 31 GV kiezen tussen het aanbieden van een aparte, toegewijde '*dedicated'* interface voor dienstaanbieders en het beschikbaar maken van de gebruikersinterface.

Als de bank kiest voor het beschikbaar maken van de gebruikersinterface, krijgen de dienstaanbieders toegang tot de omgeving die ook wordt gebruikt door de gebruiker. Dit betekent echter niet dat de bank de gebruikersinterface zomaar open kan stellen. De interface dient de dienstaanbieders op grond van artikel 30 lid 1 GV in staat te stellen om zichzelf te identificeren, informatie op te vragen over de aangewezen rekeningen en de betrokken transacties en betalingen te initiëren. Hij hoeft of mag de dienstaanbieders echter geen onbeperkte toegang te verlenen. Ook als de bank kiest voor het aanbieden van een gebruikersinterface, moet zij deze interface daarom aanpassen.[41]

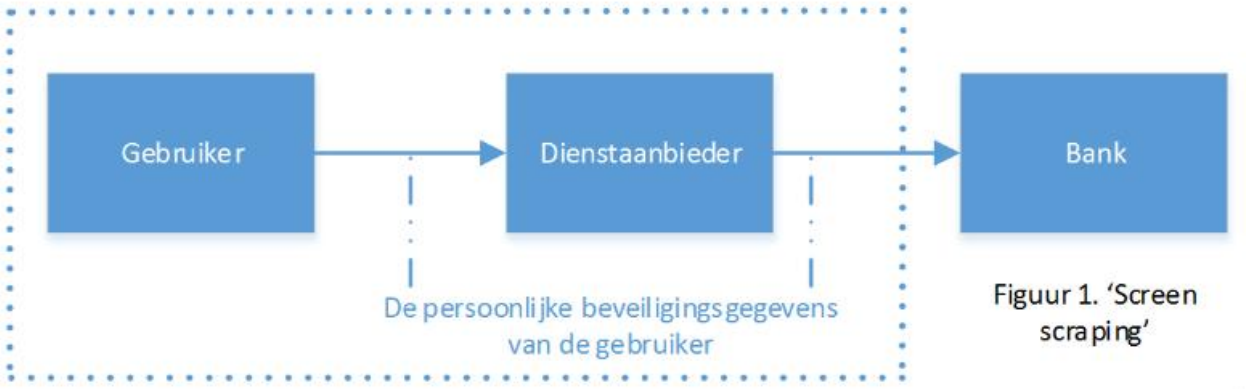
4.2 Het verbod op 'screen scraping' en de vereisten aan een toegewijde interface

De dienstaanbieders bevinden zich ten opzichte van de bank in een afhankelijke positie. Zij kunnen hun diensten niet in overeenstemming met de PSD2 uitvoeren als de bank geen goed functionerende interface inricht. Dit geeft de bank de mogelijkheid om de door de PSD2 nagestreefde ontwikkeling van een markt voor betalingsdiensten te dwarsbomen. Artikel 30 GV bevat verschillende waarborgen om dit tegen te gaan.

Een toegewijde interface creëert aanvullende mogelijkheden om het aanbieden van betalingsdiensten te beperken. De bank kan dit onder andere doen door niet alle noodzakelijke gegevens via deze interface beschikbaar te maken. De mededinging wordt daarnaast beperkt als de toegewijde interface slechter functioneert dan de gebruikersinterface, bijvoorbeeld omdat hij traag of onregelmatig beschikbaar is.[42]

De al dan niet terechte vrees voor het gebruik van deze belemmerende mogelijkheden heeft de totstandkoming van de GV

beïnvloed. Zij heeft in het bijzonder invloed gehad op de discussie over het verbod op '*screen scraping*'. Bij deze vorm van toegang heeft de dienstaanbieder toegang tot de rekening van de gebruiker zonder dat hij zich bij de bank identificeert. In plaats daarvan gebruikt de dienstaanbieder de persoonlijke beveiligingsgegevens van de gebruiker om 'als de gebruiker' toegang te krijgen.[43] De gebruiker dient hiervoor zijn beveiligingsgegevens, waaronder mogelijk zijn pincode, aan de dienstaanbieder te overhandigen. Verschillende bestaande dienstaanbieders, zoals Sofort in Duitsland, maken op dit moment gebruik van deze techniek.[44] Figuur 1 geeft een overzicht van toegang door middel van *screen scraping*.



Figuur 1. 'Screen scraping'

Hoewel de bank maatregelen kan nemen om *screen scraping* te ontdekken, weet zij doordat de dienstaanbieder zich in strijd met de artikelen 66 lid 3 sub d en 67 lid 2 sub c PSD2 niet identificeert in beginsel niet dat zij met een ander dan de gebruiker te maken heeft. De dienstaanbieder krijgt hierdoor onbeperkte toegang tot de online-banking omgeving. Hij krijgt dus ook toegang tot gevoelige betalingsgegevens en informatie die niet nodig is voor het verlenen van de dienst. Een dienstaanbieder die enkel een overzicht van het beschikbare banksaldo aanbiedt, kan op deze wijze bijvoorbeeld toch inzicht krijgen in alle transacties. Om deze redenen verbiedt de EBA *screen scraping* in haar ontwerp voor de technische reguleringsnormen.[45]

De betalingsdienstaanbieders hebben sterk gelobbyd tegen dit verbod. Zij stellen dat zij, in het geval dat de toegewijde interface niet goed functioneert, ook op deze manier toegang moeten kunnen krijgen. De Europese Commissie deelt deze mening. Artikel 33 lid 4 GV bevat daarom een *'fallback option'*. Dienstaanbieders krijgen toegang tot de gebruikersinterface als de toegewijde interface vijf achtereenvolgende verzoeken om informatie niet binnen dertig seconden beantwoordt. Zij blijven op grond van lid 5 sub b gebonden aan de verplichtingen van de artikelen 66 lid 3 en 67 lid 2 van de PSD2. De dienstaanbieders zijn in het bijzonder nog steeds verplicht om zich te identificeren. De banken moeten deze identificatie mogelijk maken.

De nationale toezichthouders kunnen de banken op grond van artikel 33 lid 6 GV vrijstellen van de verplichting om een *fallback option* te onderhouden als hun interface voor betalingsdienstaanbieders voldoet aan de eisen van de GV en gedurende ten minste drie maanden goed functioneert. Deze uitzondering stelt de banken in staat om de kosten van de *fallback option* te besparen.[46] Zij kunnen hierdoor bovendien de privacy van hun klanten versterken. Als een bank vrijstelling heeft gekregen, mag de betalingsdienstaanbieder na de overgangsperiode (§ 3) in geen geval gebruikmaken van *screen scraping*.

4.3 Het authenticatieproces van de bank

De door de bank aangeboden interface dient de dienstaanbieders in staat te stellen om gebruik te maken van de authenticatieprocessen die de bank aan de gebruiker aanbiedt.[47] Deze mogelijkheid maakt het gemakkelijker om de diensten aan te bieden. De dienstaanbieders hoeven immers geen eigen authenticatie te ontwikkelen. In plaats daarvan geven zij de bank, naast de betalingsopdracht of het verzoek om informatie, de instructie om het authenticatieproces te starten. De reguleringsnormen maken niet duidelijk hoe het proces verder moet worden afgehandeld.

De interface dient op grond van artikel 30 lid 2 sub b GV communicatiesessies tussen de bank, de dienstaanbieder en de gebruiker op te starten en te onderhouden. Het bestaan van een communicatiesessie tussen de bank en de gebruiker suggereert dat het authenticatieproces buiten de dienstaanbieder om kan worden afgehandeld. In plaats daarvan verwijst de dienstaanbieder de gebruiker voor de authenticatie door naar de website van de bank.

Ook in overige zin dient te worden aangenomen dat de dienstaanbieders zo min mogelijk toegang dienen te hebben tot de persoonlijke beveiligingsgegevens met betrekking tot de betaalrekening. Een rekeninginformatiedienstaanbieder mag geen gevoelige betalingsgegevens, waaronder persoonlijke beveiligingsgegevens, opvragen. Een betalingsinitiatiedienstaanbieder mag ze niet opslaan (§ 2.1 en § 2.2). De dienstaanbieders dienen bovendien op grond van

artikel 5 lid 1 sub g van de PSD2 bij de vergunningsaanvraag aan te geven welke procedures zij gebruiken om de toegang tot gevoelige betalingsgegevens te beperken.

Deze wijze van afhandeling beperkt de beveiligingsrisico's tot een minimum.[48] De dienstaanbieders verwerken de persoonlijke beveiligingsgegevens op geen enkele manier. Zij kunnen dan ook geen misbruik maken van deze gegevens. Daarnaast is het voor kwaadwillende derden niet mogelijk om de persoonlijke beveiligingsgegevens bij de dienstaanbieder te stelen of onderscheppen.

Deze beveiligingsvoordelen bestaan niet als het authenticatieproces geheel of gedeeltelijk via de dienstaanbieders wordt afgehandeld. Deze mogelijkheid werkt bovendien fraude in de hand. In Nederland hebben de banken hun klanten jarenlang in campagnes ervoor gewaarschuwd om geen inloginformatie aan derden te geven en bij afwijkingen van de reguliere interactie direct contact op te nemen met hun eigen bank. Deze waarschuwingen kunnen onder de PSD2 niet meer worden gegeven als de afhandeling van het authenticatieproces via de dienstaanbieder is toegestaan. Kwaadwillenden krijgen hierdoor de mogelijkheid om gebruikers te bewegen tot de afgifte van hun beveiligingsgegevens door zich voor te doen als een legitieme dienstaanbieder.

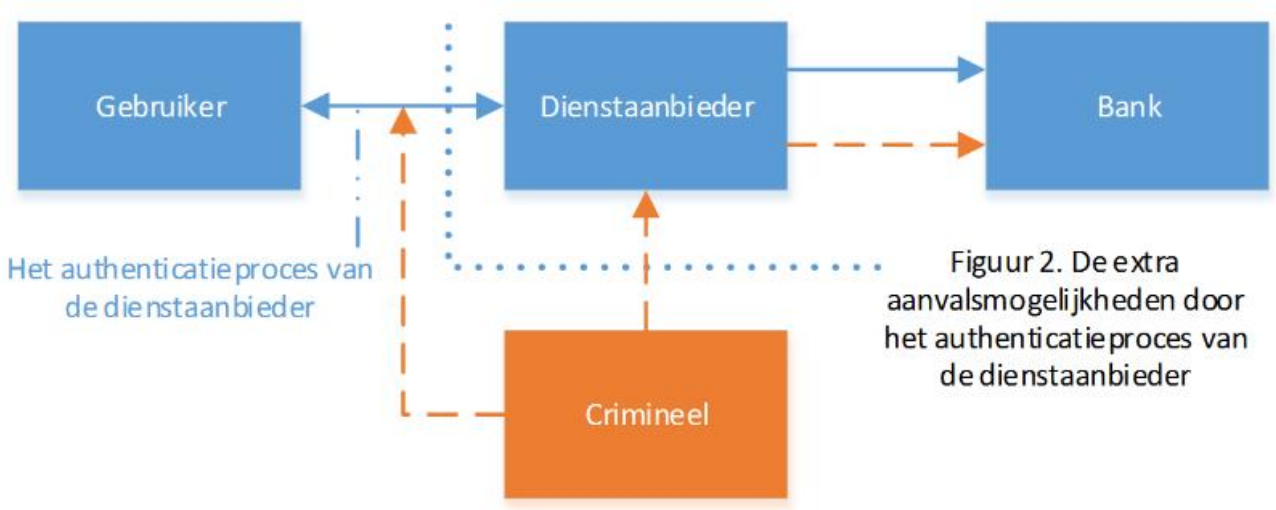
Verschillende bepalingen suggereren echter dat de afhandeling via de dienstaanbieder toch is toegestaan. De artikelen 66 lid 3 sub b en 67 lid 2 sub b van de PSD2 bepalen dat de dienstaanbieders ervoor moeten zorgen dat de persoonlijke beveiligingsgegevens niet beschikbaar zijn voor andere partijen, met uitzondering van de uitgever van deze gegevens. Artikel 30 lid 2 sub c GV stelt daarnaast dat de vertrouwelijkheid en integriteit van de door of via de dienstaanbieder verzonden persoonlijke beveiligingsgegevens door de interface dienen te worden verzekerd. De dienstaanbieders moeten ten slotte op grond van artikel 35 lid 5 GV ervoor zorgen dat hun medewerkers de door hen gecommuniceerde beveiligingsgegevens op geen enkel moment kunnen lezen. Zij zijn verplicht om een verlies van vertrouwelijkheid dat onder hun verantwoordelijkheid ontstaat, te melden aan de gebruiker en de uitgever van deze gegevens. Deze bepalingen illustreren dat de dienstaanbieders wel degelijk een rol kunnen spelen bij de authenticatie met behulp van beveiligingsgegevens die door de bank zijn uitgegeven.[49]

4.4 Een eigen authenticatieproces

De dienstaanbieders dienen sterke cliëntauthenticatie toe te passen (§ 2.3). Zij hebben het *recht* om hierbij gebruik te maken van het authenticatieproces van de bank (§ 4.3). De richtlijn en de GV bepalen echter niet dat de aanbieders ook *verplicht* zijn om dit proces aan te wenden. De ontwikkeling van gebruiksvriendelijkere manieren om te betalen is een van de doelstellingen van de PSD2. Snellere en gemakkelijkere authenticatieprocessen dragen hieraan bij.[50]

De door de dienstaanbieder aangeboden authenticatie dient te voldoen aan de PSD2 en GV. Zij is gebonden aan dezelfde beveiligingsvereisten als het authenticatieproces van de bank. Toch leidt het gebruik van alternatieve processen tot extra risico's. Als alleen de authenticatie van de bank mag worden gebruikt, kunnen criminelen slechts toegang krijgen tot de rekeninginformatie en geldmiddelen als zij dit authenticatieproces omzeilen of kraken. De alternatieve authenticatiemogelijkheden van de dienstaanbieders leiden tot een vermenigvuldiging van de mogelijke aanvalsmogelijkheden. Zelfs als deze authenticatieprocessen in beginsel even adequaat beveiligd zijn, vergroten zij de kans dat een crimineel profiteert van een fout van de ontwikkelaar of gebruiker van het proces.

Dit speelt in het bijzonder omdat de bank zonder het gebruik van haar authenticatiesysteem niet in staat is om te beoordelen of de gebruiker van de betalingsdienst dezelfde persoon is als de rechthebbende van de rekening. Zij kan dan ook niet controleren of de rechthebbende werkelijk instemt met de uitvoering van de betalingsinitiatie- of rekeninginformatiedienst.[51] Zij moet vertrouwen op de dienstaanbieder. De dienstaanbieder is immers slechts verplicht om een beperkte hoeveelheid informatie, zoals de naam en het rekeningnummer van de gebruiker, aan de bank te verschaffen.[52] In theorie kan hierdoor iedere dienstaanbieder toegang krijgen tot een betaalrekening, ook als hij in werkelijkheid geen contractuele relatie heeft met de beweerde gebruiker. Ook (buitenlandse) inlichtingendiensten en criminelen kunnen, los van het authenticatieproces, toegang tot een rekening krijgen door in te breken bij een willekeurige dienstaanbieder. De mogelijkheid om een eigen authenticatieproces te gebruiken, leidt daarom tot een vermenigvuldiging van de aanvalsmogelijkheden. Figuur 2 geeft de extra risico's weer.



Figuur 2. De extra aanvalsmogelijkheden door het authenticatieproces van de dienstaanbieder

4.5 Eenmalige autorisatie met behulp van het authenticatieproces van de bank

De extra risico's kunnen worden verkleind door te vereisen dat een gebruiker ten minste een keer, of een keer per jaar, het authenticatieproces van de bank gebruikt om een dienstaanbieder te autoriseren. Hoewel deze maatregel de extra aanvalsmogelijkheden niet geheel wegneemt, beperkt hij de risico's tot de geautoriseerde aanbieders.

Artikel 95 lid 1 van de PSD2 verplicht de dienstaanbieders om de risico's te beperken die voortvloeien uit de door hen aangeboden diensten. [53] De eis dat de gebruiker de dienstaanbieder bij de bank autoriseert, draagt bij aan haar vervulling. Het gebruik van het authenticatieproces van de dienstaanbieder maakt bovendien op zichzelf niet duidelijk of de gebruiker ook de rechthebbende van de bankrekening is.[54] Een dienstaanbieder die een vingerafdruk voor de authenticatie gebruikt, weet bijvoorbeeld niet of de afdruk ook werkelijk bij de rechthebbende van de rekening hoort. Een bank die haar authenticatieproces niet baseert op een vingerafdruk, kan dit ook niet controleren. De dienstaanbieder dient de identiteit van de gebruiker en de rechthebbende daarom op enige manier aan elkaar te koppelen. Hoewel de PSD2 niet voorschrijft dat hij hiervoor het proces van de bank gebruikt, is de eenmalige autorisatie met behulp van het authenticatieproces van de bank een veilige en gebruiksvriendelijke manier om deze koppeling te bewerkstelligen.[55]

Hiermee is echter niet gezegd dat de bank het recht op toegang mag of moet opschorten totdat de dienstaanbieder door de gebruiker is geautoriseerd. Hoewel een dergelijke bevoegdheid of plicht niet expliciet uit de richtlijn volgt,[56] bieden verschillende bepalingen een mogelijke grondslag. Allereerst bepaalt artikel 68 lid 5 van de PSD2 dat de bank het recht op toegang kan ontzeggen om objectieve en op voldoende aanwijzingen gebaseerde redenen in verband met niet-toegestane of frauduleuze toegang (§ 2.3). Daarnaast kan artikel 95 PSD2 ook hier van belang zijn. Hoewel de risico's in de eerste plaats aan de betalingsinitiatie- en rekeninginformatiedienst zijn verbonden, kan het misbruik slechts plaatsvinden als de aanvaller ook echt toegang krijgt tot de betaalrekening. Het risico is daarom ook verbonden aan het aanbieden van een betaalrekening. Bovendien verplicht artikel 2 GV betalingsdienstaanbieders, waaronder banken, om transactie monitorende mechanismen te implementeren om ongeautoriseerde of frauduleuze betalingen te ontdekken. De bank zou op grond van deze artikelen kunnen eisen dat de gebruiker eenmalig haar authenticatieproces gebruikt om de dienstaanbieder te autoriseren. Deze eis is in ieder geval gerechtvaardigd als ook aanvullende omstandigheden op een risico op fraude wijzen.[57]

Artikel 68 van de PSD2 stelt de dienstaanbieder en gebruiker daarnaast in staat om beperkingen in het contract vast te leggen. Lid 1 bepaalt dat als de instemming wordt gegeven via een specifiek 'betaalinstrument',[58] zoals een betalingsinitiatiedienst, de dienstaanbieder en de gebruiker uitgavenlimieten kunnen overeenkomen. Hoewel dit niet expliciet uit het artikel blijkt, kan ook een bank, als betalingsdienstaanbieder, deze beperkingen met haar klanten overeenkomen. Als dergelijke ongeclausuleerde contractuele betalingslimieten zijn toegestaan, zou het contract bovendien ook moeten kunnen bepalen dat de beperkingen alleen gelden als het authenticatieproces van de bank niet is gebruikt of als de dienstaanbieder niet bij de bank is geautoriseerd. Lid 2 stelt de dienstaanbieder en gebruiker daarnaast in staat om in de 'raamovereenkomst'[59] af te spreken dat het gebruik van een betaalinstrument kan worden geblokkeerd om objectief gerechtvaardigde redenen die verband houden met een vermoeden van niet-toegestaan of frauduleus gebruik van het instrument.

Of, en in welke gevallen, de bank mag eisen dat een dienstaanbieder door middel van haar authenticatie wordt geautoriseerd, blijkt niet duidelijk uit de richtlijn of de GV. De eis leidt tot een beperking van de mededinging doordat hij een barrière opwerpt voor het gebruik van betalingsinitiatie- en rekeninginformatiediensten. Deze beperking is echter, mede

gelet op de verplichtingen van de dienstaanbieder, van geringe omvang. De aanpak past daarom bij een goede afweging van de verschillende belangen. Hij draagt bij aan de doelstelling om mededinging en de ontwikkeling van een geïntegreerde markt te combineren met de beperking van fraude.

Grotere beperkingen van het recht op toegang zijn eerder in strijd met de PSD2. Het gerechtvaardigde belang van de bestrijding van fraude mag niet worden misbruikt als instrument om de concurrentie te beperken. De bank mag niet te snel aannemen dat er sprake is van objectieve en op voldoende aanwijzingen gebaseerde redenen in verband met niet-toegestane of frauduleuze toegang. Ook de contractuele beperkingen dienen niet verder te gaan dan nodig is om fraude te beperken en de klant te beschermen.

4.6 Identificatie, authenticatie en dynamische koppeling

De PSD2 en de GV gebruiken verschillende aan elkaar gerelateerde begrippen.[60] Het begrip 'identificatie' ziet op de mogelijkheid om een individuele gebruiker te identificeren. Hiervoor is bijvoorbeeld een naam of een rekeningnummer vereist. 'Authenticatie' is het proces waarmee dit individu bewijst dat hij werkelijk deze gebruiker is. Iedereen kan zich identificeren aan de hand van een naam of rekeningnummer, maar alleen de rechthebbende kan zich authentiseren met behulp van (bijvoorbeeld) de pincode. Ook authenticatie bewijst echter niet dat de gebruiker werkelijk een bepaalde opdracht heeft gegeven. Zij sluit bijvoorbeeld niet uit dat een cybercrimineel of de dienstaanbieder de begunstigde van de betalingsopdracht verandert. Een 'digitale handtekening' of 'dynamische koppeling' tussen de ondertekeningscode en de opdracht kan een dergelijke 'integriteit' wel bewerkstelligen. Zij stellen de dienstaanbieder in staat om te bewijzen dat de gebruiker een bepaalde opdracht daadwerkelijk heeft gegeven.[61] Een code die is gebaseerd op een dynamische koppeling is alleen geldig bij een specifieke opdracht. Een verandering van, bijvoorbeeld, het bedrag of de begunstigde leidt tot de ongeldigheid van de ondertekeningscode. Bij een digitale handtekening kan dit ook door derden, zoals een bank, worden gecontroleerd. Deze 'onloochenbaarheid' lijkt niet vereist te zijn bij het begrip 'dynamische koppeling'.

De begrippen 'identificatie', 'authenticatie' en 'digitale handtekening' zijn aan elkaar gerelateerd, maar geven fundamenteel verschillende garanties. Zij bewerkstelligen verschillende beveiligingsdoelen. De PSD2 en de GV schrijven zowel identificatie, authenticatie als dynamische koppeling voor. Welk proces vereist is, hangt af van de verhouding.
De dienstaanbieders zijn verplicht om zich ten overstaan van de bank te identificeren (§ 2.1, § 4.1 en § 4.2). Artikel 34 GV verplicht de dienstaanbieders om hierbij gebruik te maken van 'gekwalificeerde certificaten voor elektronische zegels' en 'gekwalificeerde certificaten voor website authenticatie' in de zin van artikel 3 lid 30 en 39 van de 'eidas-verordening'.[62] De bijlagen III en IV van de eidas-verordening geven de voorwaarden waaraan dergelijke certificaten moeten voldoen. Het certificaat moet onder andere een 'geavanceerde elektronische handtekening' van een 'gekwalificeerde verlener van vertrouwensdiensten' bevatten.[63] Het certificaat stelt de dienstaanbieders daarom niet alleen in staat om zich te identificeren. Het zorgt er ook voor dat de bank de aanbieders kan authentiseren.

De gebruiker moet het bedrag en de begunstigde bovendien kunnen zien. De dienstaanbieder is op grond van lid 2 sub b GV verplicht om maatregelen te nemen om de integriteit van de weergegeven informatie te waarborgen. Hij moet bijvoorbeeld voorkomen dat een cybercrimineel een *man-in-the-middle attack* uitvoert met behulp van malware op de mobiele telefoon of computer van de gebruiker. Bij een dergelijke aanval denkt de gebruiker dat hij een authenticatiecode voor een bepaalde transactie genereert, maar laat de cybercrimineel hem in werkelijkheid een code genereren voor een andere betalingsopdracht, bijvoorbeeld door de weergave op het scherm aan te passen.[64] De verantwoordelijkheid van de partij die de authenticatie aanbiedt, strekt zich hierdoor mede uit tot de digitale omgeving van de gebruiker. De weergegeven informatie is immers uiteindelijk afhankelijk van de hard- en software van de gebruiker.

De door de PSD2 vereiste 'authenticatie' wordt door de GV met additionele waarborgen omkleed. Van belang blijft echter dat deze verplichtingen alleen gelden in de relatie tussen de gebruiker en de partij die de authenticatie uitvoert. Zij eisen niet dat de bank in staat wordt gesteld om het authenticatieproces van de dienstaanbieders te controleren.[65] De in § 4.4 gesignaleerde risico's blijven daarom bestaan.

De GV stelt beveiligingseisen die strenger zijn dan de tekst van de PSD2 doet vermoeden. De door de richtlijn vereiste identificatie van dienstaanbieders wordt door de GV van waarborgen voorzien. De authenticatie die door de richtlijn wordt gevergd, leidt door de dynamische koppeling ook tot integriteit, maar niet tot onloochenbaarheid.

5. Synthese en conclusie

In deze bijdrage adresseren wij de volgende onderzoeksvraag: *In hoeverre creëert het recht op toegang van de betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbiederseen goede balans tussen de bescherming van de gebruiker en de ontwikkeling van de markt voor betalingsdiensten?* Een analyse van de bepalingen van de PSD2 laat zien dat de bescherming van de gebruiker uiteindelijk ondergeschikt is aan de ontwikkeling van de markt.

Dit blijkt allereerst uit de regels met betrekking tot privacy. De PSD2 begrenst het recht op toegang op verschillende

manieren. De dienstaanbieders zijn bovendien gebonden aan de AVG (§ 2.3). De ontleding van de bepalingen over rekeninginformatiediensten laten echter zien het begrip ‘rekeninginformatiedienst’ zo breed en vaag geformuleerd is dat het een grote variatie aan diensten kan omvatten. Deze keuze faciliteert innovatie en mededinging op de markt voor betalingsdiensten. Zij leidt er echter ook toe dat de beperkingen aan het recht op toegang op verschillende manieren zijn te omzeilen (§ 2.2). De richtlijn heeft bovendien geen oog voor de privacygevolgen die kunnen ontstaan door grootschalige verwerkingen van persoonsgegevens als gevolg van het veelvuldig gebruik van rekeninginformatiediensten (§ 2.3).

De regels met betrekking tot *screen scraping* leiden tot een vergelijkbare conclusie (§ 4.2). Deze vorm van toegang gaat verder dan noodzakelijk is voor de uitoefening van de betalingsdiensten. De EBA pleit daarom voor een verbod. De Europese Commissie heeft echter besloten dat het risico op een beperking van de mededinging zwaarder weegt. Zij geeft de dienstaanbieders het recht om gebruik te maken van de gebruikersinterface als de toegewijde interface niet goed functioneert. Deze toegang is omkleed met waarborgen. Deze zekerheden bestaan echter voornamelijk uit controle achteraf, nadat de aanbieder al toegang heeft gekregen. De bescherming van het belang om zonder belemmeringen betalingsdiensten aan te bieden, wordt hiermee opnieuw boven de bescherming van de gebruikers gesteld.
Ook de regels met betrekking tot authenticatie lijken de belangen van de dienstaanbieders boven de bescherming van de gebruikers te stellen. De dienstaanbieders mogen gebruikmaken van het door de bank aangeboden authenticatieproces. De GV bepaalt echter niet duidelijk hoe het proces verder dient te worden afgehandeld (§ 4.3). De vrijheid om dit proces in te richten heeft de prioriteit over het belang om authenticatie zo sterk mogelijk te maken.

Deze ordening van de belangen blijkt ook uit de mogelijkheid van betalingsdienstaanbieders om een eigen authenticatieproces te gebruiken. De PSD2 en de technische reguleringsnormen eisen niet dat de bank in staat wordt gesteld om dit proces te controleren. Hoewel de PSD2 dit niet expliciet bepaalt, lijkt de bank te moeten vertrouwen op de dienstaanbieder (§ 4.4). De normen eisen niet dat de bank in staat wordt gesteld om het authenticatieproces van de betalingsdienstaanbieders, bijvoorbeeld door middel van een digitale handtekening van de gebruiker, te controleren (§ 4.4, § 4.5 en § 4.6). Het recht op toegang leidt hierdoor tot een vermenigvuldiging van de risico’s. Een kwaadwillende kan in theorie via iedere dienstaanbieder toegang krijgen tot een rekening (§ 4.4).

De GV versterkt het niveau van de beveiliging. De normen stellen beveiligingseisen die strenger zijn dan de tekst van de PSD2 doet vermoeden (§ 4.6). Zij doen echter geen afbreuk aan de principiële keuze van de PSD2: de dienstaanbieders krijgen ruime mogelijkheden om hun diensten aan te bieden, ook als dit tot een vergroting van de risico’s leidt.
Er bestaat geen adequate balans tussen de bescherming van de gebruiker en de ontwikkeling van de markt voor betalingsdiensten. De bescherming van de gebruiker is in het stelsel van de PSD2 uiteindelijk ondergeschikt. Dit betekent niet automatisch dat de bescherming ook werkelijk tekortschiet. De beveiliging staat of valt uiteindelijk bij de betrouwbaarheid van de dienstaanbieders. Het systeem van de PSD2 gaat ervan uit dat zij, mits zij voldoen aan de vereisten voor een vergunning of registratie, kunnen worden vertrouwd. In de komende jaren zal moeten blijken of dit uitgangspunt juist is. De bescherming van de gebruikers kan bijvoorbeeld onder druk komen te staan als vergunningen, in de hele Europese Unie of in bepaalde lidstaten, te gemakkelijk worden verleend of het toezicht op de instellingen tekortschiet. Zij kan bovendien in het geding komen als de dienstaanbieders gebruik gaan maken van een grote hoeveelheid verschillende, mogelijk niet goed doordachte, alternatieve authenticatieprocessen.

Dit brengt de gevestigde banken in een lastige positie. Het doorbreken van hun juridische monopolie op de toegang tot betaalrekeningen is het voornaamste doel van de PSD2. Een maatregel om de gebruiker te beschermen tegen misbruik van het recht op toegang, zal al snel worden gezien als een ongeoorloofde beperking van de mededinging. Tegelijkertijd hebben de banken juridische verplichtingen om persoonsgegevens te beschermen en fraude te voorkomen (§ 4.5). Zij kunnen deze verplichtingen gebruiken om, in samenwerking met de dienstaanbieders en toezichthouders, de toegang van onbetrouwbare aanbieders te beperken en de ontwikkeling van betrouwbare en transparante alternatieve authenticatieprocessen en koppelingsmethoden te stimuleren. Deze mogelijkheden mogen onder de PSD2 echter in geen geval worden gebruikt om de mededinging alsnog te beperken.

Het stelsel van de PSD2 garandeert geen balans tussen de bescherming van de gebruiker en de ontwikkeling van de markt voor betalingsdiensten. Of deze balans toch ontstaat, is daarom afhankelijk van het toekomstige aanbod en gebruik van de diensten en de invulling van de normen door banken, dienstaanbieders en toezichthouders.

Voetnoten

[1]

Pieter Wolters is universitair docent burgerlijk recht en onderzoeker bij het Onderzoekcentrum Onderneming & Recht van de Radboud Universiteit. Bart Jacobs is hoogleraar computerbeveiliging bij het Institute for Computing and Information Science van de Radboud Universiteit.

[2]

Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn

2007/64/EG (*PbEU* 2015, L 337/79). Engels: *Payment Services Directive 2*.

[3]
Richtlijn 2007/64/EG van het Europees Parlement en de Raad van 13 november 2007 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG.

[4]
PSD2, overweging 3-4, 7, 11, 13, 18-19 en 27-29; Commission, *Impact assessment Accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/UE and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions* (Staff Working Document), SWD (2013) 288 final, Volume 1/2, p. 15-27; M. Cortet, T. Rijks & S. Nijland; 'PSD2: The digital transformation accelerator for banks', *Journal of Payments Strategy & Systems* 2016, afl. 1, p. 18; M. Donnelly, 'Payments in the digital market: Evaluating the contribution of Payment Services Directive II', *Computer Law & Security Review* 2016, afl. 6, p. 827-829; A.P.C. Godlieb, 'De aansprakelijkheidsverdeling tussen banken en *payment initiation service providers* onder de *Payment Services Directive II*', *FR* 2016, nr. 4, p. 134; J. den Hamer & R. Middelburg, 'Regulering van betaaldienstverlening onder PSD II – is tech eating everything?', *O&F* 2017, afl. 4, p. 6-7; J.L. Jonker & B.M. Dijkmans van Gunst, 'De getemperde belofte van PSD2/XS2A', *IR* 2017, nr. 4, p. 142; R.H.J. van Houts & D.E. Martens-Schutten, 'PSD 2: Naar een veiliger betalingsverkeer?', *TvCo* 2017, afl. 2, p. 106-108. Zie over de uitzonderingen die onder de PSD2 (blijven) bestaan ook J.Ph. Broekhuizen, 'Extensies van de betaalketen. Regulering van betaaldiensten en de PSD II', *IR* 2017, nr. 3, p. 102-103.

[5]
PSD2, overweging 5-7, 33, 66-67, 69, 75, 77, 84-85, 95 en 109. Zie over de doelstellingen van de richtlijn daarnaast Commission 2013, p. 35-37; Broekhuizen 2017, p. 98; Den Hamer & Middelburg 2017, p. 7.

[6]
PSD2, artikel 4 lid 15, 16, 18 en 19, bijlage I onder 7 en 8 en overweging 27-29.

[7]
PSD2, artikel 4 lid 10 en 12; Jonker & Dijkmans van Gunst 2017, p. 144.

[8]
PSD2, artikel 1 lid 1 sub d, 4 lid 4, 5, 11 en 37 lid 1 en overweging 34. Zie ook Den Hamer & Middelburg 2017, p. 8; Van Houts & Martens-Schutten 2017, p. 109 en 111-112; Jonker & Dijkmans van Gunst 2017, p. 143. Andere betalingsdienstaanbieders vallen onder andere vergunningsstelsels. Zie PSD2, artikel 1.

[9]
PSD2, artikel 5 lid 3 en overweging 48; Jonker & Dijkmans van Gunst 2017, p. 143.

[10]
PSD2, artikel 4 lid 17.

[11]
Zie ook Temenos, *Payment Services Directive 2 (PSD2)*, 2016, p. 5 (beschikbaar op www.temenos.com/globalassets/mi/wp/16/temenos_psd2_whitepaper_v2.pdf, laatst bezocht 10 januari 2018); B.P.F. Jacobs, 'PSD2, een Europese strategische blunder', *iBestuur.nl,* 12 september 2017.

[12]
Zie ook Temenos 2016, p. 5; Den Hamer & Middelburg 2017, p. 5.

[13]
Zie ook Temenos 2016, p. 11; Den Hamer & Middelburg 2017, p. 13.

[14]
Zie bijvoorbeeld R. Betlem, 'Natuurlijk gaat Facebook zich nestelen tussen de banken', *FD.nl* 7 december 2017; Den Hamer & Middelburg 2017, p. 5; Jacobs 2017.

[15]
PSD2, overweging 29; Godlieb 2016, p. 135. Zie ook Donnelly 2016, p. 830.

[16]
Zie ook A. van der Beek, 'FinTech en mededingingsrecht: FinTech als 'driver of competition'?', *TFR* 2017, afl. 5, p. 166; Broekhuizen 2017, p. 100-101; Financial Conduct Authority, *Payment Services and Electronic Money – Our Approach. The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011*, 2017, p. 210. Jonker en Dijkmans van Gunst (2017, p. 145-146) stellen dat het wel mogelijk is om 'objectieve, evenredigen en niet-discriminerende' contractuele voorwaarden te stellen. Zij baseren deze mogelijkheid onder andere op het ontwerp voor artikel 5:88a Wft (toegang tot betaalrekeningsdiensten) en artikel 3:17 Wft (beheerste en integere bedrijfsuitoefening). Deze interpretatie is echter in strijd met de tekst van de richtlijn. De richtlijn laat dergelijke voorwaarden wel toe bij de toegang tot betalingssystemen en betaalrekeningsdiensten. PSD2, artikel 4 lid 7, 35 en 36.

[17]
PSD2, artikel 4 lid 31 en 32; Jonker & Dijkmans van Gunst 2017, p. 146.

[18]
PSD2, overweging 28; Donnelly 2016, p. 831; Jonker & Dijkmans van Gunst 2017, p. 147.

[19]
Vergelijk ook Cortet, Rijks & Nijland 2016, p. 24; Broekhuizen 2017, p. 100; Den Hamer & Middelburg 2017, p. 12; Financial Conduct Authority 2017, p. 214.

[20]
Financial Conduct Authority 2017, p. 16; Jonker & Dijkmans van Gunst 2017, p. 147; Autoriteit Persoonsgegevens, *Vragen over PSD2*, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/financiele-instellingen (laatst bezocht 5 februari 2018).

[21]
Vergelijk Financial Conduct Authority 2017, p. 16.

[22]
Zie ook *Kamerstukken II* 2017/18, 34616, 3 (brief van minister Hoekstra).

[23]
Zie ook European Banking Federation, *Guidance for implementation of the revised Payment Services Directive. PSD2 guidance* (EBF_020819), EBF 2016, p. 25.

[24]
Commission, *Commission Delegated Regulation (EU) No …/.. of XXX supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication* C(2017) 7782 final, 2017, artikel 36 lid 1 sub a (beschikbaar op https://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf, hierna: 'Technische reguleringsnormen'); Financial Conduct Authority 2017, p. 209.

[25]
Zie ook EBA, *Opinion of the European Banking Authority on the European Commission's intention to partially endorse and amend the EBA's final draft regulatory technical standards on strong customer authentication and common and secure communication under PSD2*, EBA/OP/2017/09, 2017, p. 8 (hierna: 'EBA reactie juni 2017'); § 2.3.

[26]
Zie bijvoorbeeld S. Hania, 'Bankgegevens niet veilig na invoering PSD2', *Netkwesties.nl* 25 oktober 2017; Jonker & Dijkmans van Gunst 2017, p. 146-147; E. Timmer, 'PSD2 voor accountants | Bent u bereid om uw betaalgegevens te delen? En uw klant?', *Ellentimmer.wordpress.com* 20 december 2017; J.A. Voerman, 'PSD2 als katalysator voor Open Banking', *TvCo* 2017, afl. 2, p. 121; Autoriteit Persoonsgegevens, *Vragen over PSD2*, https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/financiele-instellingen (laatst bezocht 5 februari 2018).

[27]
Het 'verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen' is een verwerking in de zin van artikel 4 lid 2 AVG. De informatie over iemands financiële positie en transacties is een persoonsgegeven in de zin van artikel 4 lid 1 AVG. Zie over dit begrip ook Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN WP 136, 2007.

[28]
Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

[29]
Artikel 6 lid 1 sub c AVG. Voerman (2017, p. 121) en Timmer (2017) stellen dat toestemming (mogelijk) de enige rechtmatige grondslag is op grond van artikel 94 lid 2 van de PSD2. Dit artikel heeft echter slechts betrekking op de relatie tussen de gebruiker en dienstaanbieder. Het geeft geen bijzondere regels met betrekking tot de gegevens van derden. Het is daarnaast niet van toepassing op rekeninginformatiedienstaanbieders, § 2.3.

[30]
In deze zin bijvoorbeeld Timmer 2017.

[31]
Deze plichten gelden, ten aanzien van persoonsgegevens, ook op grond van de artikelen 32, 33 en 34 van de AVG. Zie ook PSD2, overweging 89.

[32]
Zie ook PSD2, artikel 4 lid 30; GV, artikel 4-9; Donnelly 2016, p. 837; Den Hamer & Middelburg 2017, p. 15. Zie voor uitzonderingen GV, artikel 10-21.

[33]
PSD2, artikel 66 lid 3 sub b en d en lid 4 sub a en 67 lid 2 sub b en c en lid 3 sub a. Zie ook § 4.3.

[34]
Zie ook Den Hamer & Middelburg 2017, p. 17; Van Houts & Martens-Schutten 2017, p. 111; Jonker & Dijkmans van Gunst 2017, p. 148; Voerman 2017, p. 120; § 4.2.

[35]

Vergelijk Autoriteit Persoonsgegevens, 'AP adviseert over wetsvoorstel PSD2', *Autoriteitpersoonsgegevens.nl* 24 oktober 2017. Zie over het toepassingsgebied van de verordening ook AVG, artikel 1-3.

[36]
Verordening (EU) 1093/2010 van het Europees Parlement en de Raad van 24 november 2010 tot oprichting van een Europese toezichthoudende autoriteit (Europese Bankautoriteit), tot wijziging van Besluit nr. 716/2009/EG en tot intrekking van Besluit 2009/78/EG van de Commissie (*PbEU* 2010, L 331/12). Zie over de procedure hiervoor PSD2, artikel 95 lid 3 en 96 lid 3, 4 en 5 en Europese Bankautoriteit verordening, artikel 16.

[37]
Gedelegeerde Verordening (EU) 2018/389 van de Commissie van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliënt authenticatie en gemeenschappelijke en veilige open communicatiestandaarden (*PbEU* 2018, L 69/23).

[38]
De Minister van Financiën gaat uit van een implementatie in het voorjaar van 2018. Brief van de Minister van Financiën van 22 september 2017, 2017-0000188569. Het voorstel is ingediend bij de Tweede Kamer. Het is beschikbaar op https://zoek.officielebekendmakingen.nl/behandelddossier/34813 (laatst bezocht 21 februari 2018). In deze bijdrage besteden wij geen aandacht aan de Nederlandse implementatie.

[39]
Vergelijk EBA, *Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*, EBA/RTS/2017/02, 2017, p. 4, 11-12 en 46 (hierna: 'EBA normen februari 2017'); Commission, 'Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electronic payments' (Press release), MEMO/17/4961, 27 november 2017.

[40]
PSD2, artikel 95; AVG, artikel 32.

[41]
EBA normen februari 2017, p. 110 en 113; EBA reactie juni 2017, p. 8.

[42]
Zie bijvoorbeeld EBA normen februari 2017, p. 11, 46 en 113; EBA reactie juni 2017, p. 7; Betlem & Keuning 2017, p. 5; Den Hamer & Middelburg 2017, p. 14; Weermeijer 2017.

[43]
EBA normen februari 2017, p. 4; EBA reactie juni 2017, p. 8.

[44]
Zie bijvoorbeeld 'PSD2 RTS on secure communication and screen scraping', *ThePaypers.com* 2 mei 2017.

[45]
EBA normen februari 2017, p. 4, 11, 46, 113 en 117-118; EBA reactie juni 2017, p. 8.

[46]
Zie over de nadelen van de *fallback option* uitgebreider EBA reactie juni 2017, p. 8-11; Technische reguleringsnormen, p. 4.

[47]
PSD2, overweging 30, 69 en 96; GV, artikel 30 lid 2.

[48]
Zie ook Cortet, Rijks & Nijland 2016, p. 24.

[49]
Zie ook EBA normen februari 2017, p. 118, 123 en 145-147.

[50]
Zie onder andere EBA 2015, p. 7-9, 18-19 en 27; G. Cimiotti & C.N. Dahl, 'Paying in 2025: Scenarios for payment systems in Germany in 2025', *Journal of Payment Strategy & Systems* 2016, afl. 3, p. 255-256; EBA normen februari 2017, p. 38, 41 en 117; § 2.1. Verschillende bepalingen stellen dat de instemming met een betalingsopdracht ook aan een ander dan de bank kan worden verstrekt. PSD2, artikel 76 lid 3 sub a en 80 lid 2. Vergelijk echter PSD2, artikel 64 lid 2 ("De instemming met een betalingstransactie wordt verleend in de tussen de betaler en de betalingsdienstaanbieder overeengekomen vorm. De instemming met de uitvoering van een betalingstransactie kan ook worden verleend via de begunstigde of de betalingsinitiatiedienstaanbieder"), artikel 66 lid 4 sub c en 67 lid 3 sub b (de rekeninghoudende betalingsdienstaanbieder behandelt de verzoeken en opdrachten van de betalingsinitiatie- en de rekeninginformatiedienstaanbieder niet anders); GV, artikel 36 lid 4 ("*Payment initiation service providers shall provide account servicing payment service providers with the same information requested from the payment service user when initiating the payment transaction directly*"). Het is mogelijk om te bepleiten dat 'overeengekomen vorm', '*the same information*' en 'niet anders' ook betrekking hebben op de authenticatie. Deze interpretatie sluit echter niet aan bij de doelstellingen van de PSD2.

[51]

Zie ook het voorstel voor het *Implementatiebesluit herziene richtlijn betaaldiensten*, p. 16-17 (beschikbaar op www.internetconsultatie.nl/implementatiebesluitherzienerichtlijnbetaaldiensten, laatst bezocht 10 januari 2018); Den Hamer & Middelburg 2017, p. 17; Financial Conduct Authority 2017, p. 137; Jonker & Dijkmans van Gunst 2017, p. 149.

[52]
Noot 50.

[53]
Zie ook PSD2, artikel 5 lid 1 sub e, i en j en 11 lid 4 (alleen voor betalingsinitiatiediensten); EBA, *Consultation Paper. Draft Guidelines on the security measures for operational and security risks of payment services under PSD2*, EBA/CP/2017/04, 2017, p. 8 en 21.

[54]
Vergelijk GV, artikel 24 over de associatie van de identiteit van de gebruiker en zijn persoonlijke beveiligingsgegevens.

[55]
Een andere mogelijkheid is iDIN (www.idin.nl). Deze authenticatiemethode is gebaseerd op de authenticatie van de banken. Ook 'IRMA' (https://privacybydesign.foundation/irma/) ondersteunt via iDIN een koppeling met de authenticatie van de banken. DigiD ondersteunt tweefactorenauthenticatie. Deze authenticatiemethode kan echter alleen worden gebruikt om een koppeling te bewerkstelligen als zij ook door de bank wordt ondersteund.

[56]
Noot 50. Anders: Temenos 2016, p. 14, waar deze eis wordt afgeleid uit het vereiste dat de gebruiker toestemming moet hebben gegeven aan de betalingsdienstaanbieder.

[57]
Vergelijk Financial Conduct Authority 2017, p. 211.

[58]
PSD2, artikel 4 lid 14.

[59]
Een overeenkomst die de verplichtingen en voorwaarden voor het openen van een betaalrekening weergeeft, is een raamovereenkomst. PSD2, artikel 4 lid 21.

[60]
Zie over deze begrippen ook B.P.F. Jacobs, 'Vertrouwen en authenticatie', in: S.E. Bartels e.a. (red.), *Vertrouwen in het burgerlijke recht* (Kortmann-bundel, Serie Onderneming en Recht deel 100), Deventer: Wolters Kluwer 2017, p. 239-243.

[61]
Zie ook PSD2, artikel 77.

[62]
Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.

[63]
Zie hierover eidas-verordening, artikel 3 lid 11 en 20 en 26.

[64]
Zie ook GV, artikel 25 en overweging 18. De aanbieder moet ervoor zorgen dat de persoonlijke beveiligingsgegevens, authenticatieapparaten en software op een beveiligde manier bij de gebruiker worden afgeleverd.

[65]
Vergelijk GV, overweging 4. De overweging noemt de digitale handtekening slechts als een van de mogelijkheden om een dynamische koppeling te creëren.