Statische- en dynamische biometrie als onderdeel van sterke cliëntauthenticatie onder PSD2

mr. drs. J.A. Jans en mr. L.J.J. van den Ende[1]

Met de implementatie van de herziene Richtlijn Betaaldiensten (hierna: PSD2) worden de vereisten voor het authenticatieproces van betaalopdrachten aangescherpt. Daarnaast dienen betaaldienstverleners onder het PSD2 regime in bepaalde situaties zogenaamde sterke cliëntauthenticatie toe te passen. Sterke cliëntauthenticatie is een procedure waarbij de betaaldienstverlener gebruik maakt van twee of meer elementen die worden aangemerkt als: (i) kennis; (ii) bezit; en (iii) inherente eigenschap. In deze bijdrage bespreken Jans en Van den Ende het gebruik van biometrische systemen, zoals vingerafdrukscans, voor de invulling van het element 'inherente eigenschap' als onderdeel van sterke cliëntauthenticatie. De auteurs bespreken onder meer op welke wijze biometrische systemen kunnen worden gebruikt voor het authenticeren van betaalopdrachten en de voornaamste risico's waar betaaldienstverleners zich rekenschap van dienen te geven bij de toepassing van biometrische systemen als onderdeel van sterke cliëntauthenticatie.

Volgens de auteurs kunnen statische biometrische systemen een goede invulling zijn van het element inherente eigenschap als onderdeel van de sterke cliëntauthenticatie. Hoewel dynamische biometrische systemen hiervoor minder geschikt lijken, bieden deze systemen volgens de auteurs wel een waardevol instrument in de strijd tegen identiteitsfraude indien deze worden gebruikt in aanvulling op de sterke cliëntauthenticatie.

1. Inleiding

Als een betaaldienstgebruiker[2] een betaalopdracht wil initiëren of toegang verzoekt tot zijn betaalrekening, moet de betaaldienstverlener controleren of de betaaldienstgebruiker hiertoe bevoegd is. Voor de invulling van dit zogenaamde authenticatievereiste zijn betaaldienstverleners voortdurend op zoek naar nieuwe technieken en mogelijkheden die het gebruiksgemak van het authenticatieproces kunnen verhogen zonder daarbij afbreuk te doen aan de veiligheid van het betaalproduct. Hierbij lijkt in toenemende mate een rol te zijn weggelegd voor het gebruik van biometrische systemen. Dit zijn systemen waarbij gebruik wordt gemaakt van lichaams- en/of gedragseigenschappen van de betaaldienstgebruiker, zoals diens vingerafdruk. Het gebruik van biometrische systemen als onderdeel van het authenticatieproces is de afgelopen jaren mede in een stroomversnelling geraakt doordat steeds meer smartphones standaard zijn uitgerust met sensoren die biometrische gegevens kunnen uitlezen. Deze functionaliteit maakt het mogelijk dat betaaldienstgebruikers via hun telefoon toegang krijgen tot betaalproducten, zoals een betaalapp. Betaalproducten die gebruik maken van vingerafdruksensoren in smartphones voor de authenticatie van betaalopdrachten zijn onder meer Apple Pay en Samsung Pay. Met Selfie Pay biedt MasterCard een betaalproduct aan waarbij met behulp van de smartphone camera authenticatie plaatsvindt op basis van gezichtsherkenning.

Met de implementatie van de herziene Richtlijn Betaaldiensten[3] (hierna: PSD2) in januari 2018 worden de vereisten voor het authenticatieproces verder aangescherpt. Daarnaast dienen betaaldienstverleners onder het PSD2 regime in bepaalde situaties zogenaamde sterke cliëntauthenticatie toe te passen (hierover meer in paragraaf 2).[4] Aangezien de

1. Beide auteurs zijn advocaat bij Linklaters te Amsterdam.
2. Hoewel in Richtlijn 2007/64/EG wordt gesproken over betalingsdienstgebruiker hanteren wij de terminologie zoals gehanteerd in de Wet op het financieel toezicht en het Burgerlijk Wetboek (hierna: BW).
3. Richtlijn nr. 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.
4. PSD2 wordt geïmplementeerd middels de Implementatiewet herziene richtlijn betaaldiensten (hierna: Implementatiewet PSD2). Ten tijde van het schrijven

verwachtingen omtrent de toepassingsmogelijkheden van biometrische systemen in het betalingsverkeer hooggespannen zijn, wijst de European Banking Authority (hierna: EBA) in haar finale rapport over de invulling van het sterke cliëntauthenticatievereiste onder PSD2 (hierna: Finale Rapport RTS) expliciet op de mogelijkheid van de toepassing van biometrische systemen.[5] Naast EBA lijkt ook de Europese consument klaar te zijn voor het gebruik van biometrische systemen voor de authenticatie van betaalopdrachten. In 2016 heeft Visa een onderzoek uitgevoerd naar de mate waarin Europese consumenten een rol zien weggelegd voor biometrie als onderdeel van het authenticatieproces in het betalingsverkeer. Uit dit onderzoek blijkt dat consumenten zich net zo comfortabel voelen bij vingerafdrukauthenticatie als bij authenticatie op basis van een pincode.[6]

Hoewel er een breed draagvlak lijkt te bestaan voor de toepassing van biometrische systemen als onderdeel van het authenticatieproces, vinden er eveneens discussies plaats over de risico's die verbonden zijn aan het gebruik van dergelijke systemen. In deze bijdrage wordt nader ingegaan op de mogelijkheden van het gebruik van statische- en dynamische biometrische systemen als onderdeel van het sterke cliëntauthenticatievereiste en de privacy- en frauderisico's die kleven aan de toepassing hiervan.

2. Van authenticatie naar sterke cliëntauthenticatie

Met de implementatie van de Richtlijn Betaaldiensten[7] (hierna: PSD) in 2009, is het begrip authenticeren verankerd in het BW.[8] De huidige definitie van 'authenticeren' spreekt uitsluitend over het verifiëren van het gebruik van een betaalinstrument[9] en de gepersonaliseerde veiligheidskenmerken en niet over het verifiëren van de identiteit van de betaaldienstgebruiker.[10] In het kader van het authenticatieproces onder het huidige regime wordt bijvoorbeeld gecontroleerd of de opgegeven pincode overeenkomt met de door de betaaldienstverlener aan de betaaldienstgebruiker verstrekte pincode. De huidige authenticatie is derhalve niet gericht op de verificatie van de identiteit van de betaaldienstgebruiker en lijkt daardoor meer een autorisatieproces van het gebruikte betaalinstrument dan een authenticatieproces.

Voor het authenticatieproces wordt bij veel betaalproducten gebruik gemaakt van een combinatie van een betaalkaart en een pincode. Bij een aantal betaalproducten, zoals internetbankieren, wordt vaak nog een extra toegangscode gevraagd die bijvoorbeeld met behulp van een aparte random reader kan worden verkregen. Het gebruik van zo'n extra code verhoogt de veiligheid van het gebruik van het betaalproduct, maar beperkt tegelijkertijd het gebruiksgemak.[11]

Met de implementatie van PSD2 zal de definitie van 'authenticeren' in het BW worden uitgebreid. Volgens PSD2 is 'authenticeren' een procedure waarmee een betaaldienstverlener de identiteit van een betaaldienstgebruiker dan wel de validiteit van het gebruik van een specifiek betaalinstrument kan verifiëren.[12] Bovendien introduceert PSD2 een verplichting voor betaaldienstverleners om als voorwaarde voor bepaalde typen handelingen de betaaldienstgebruiker een verscherpt authenticatieproces te laten doorlopen. Dit proces wordt 'sterke cliëntauthenticatie' genoemd en is een procedure waarbij de betaaldienstverlener gebruik maakt van twee of meer elementen die worden aangemerkt als: (i) kennis (iets wat alleen de betaaldienstgebruiker weet, bijvoorbeeld een wacht-

van dit artikel was uitsluitend het consultatiedocument van de Implementatiewet PSD2 beschikbaar.

5. Op 23 februari 2017 publiceerde EBA het finale rapport '*Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)*'. EBA heeft gekozen voor *principle-based* in plaats van *rule-based* voorwaarden voor de invulling van het sterke cliëntauthenticatievereiste om geen concessies te hoeven doen aan de doelstellingen veiligheid en innovatie. De bevoegdheid tot het opstellen van nadere regels vloeit voort uit art. 98 PSD2 en art. 10 van Verordening (EU) nr. 1093/2010.
6. Visa, 'Visa Biometric Authentication study', Research findings, 2016, p. 5.
7. Richtlijn nr. 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 (*PbEG* 2007 L 319/1).
8. Art. 7:514(a) BW definieert authenticeren als het 'volgen van een procedure die de betaaldienstverlener in staat stelt het gebruik van het betaalinstrument te verifiëren, met inbegrip van de gepersonaliseerde veiligheidskenmerken'.
9. Onder het begrip 'betaalinstrument' wordt blijkens art. 7:514(g) BW een 'gepersonaliseerd instrument of gepersonaliseerde instrumenten of het geheel van procedures, overeengekomen tussen de betaaldienstgebruiker en de betaaldienstverlener, waarvan de betaaldienstgebruiker gebruik maakt om een betaalopdracht te initiëren' verstaan.
10. Het is relevant op te merken dat uit art. 59(2) PSD volgt dat het feit dat het gebruik van een betaalinstrument door de betaaldienstverlener is geregistreerd op zichzelf niet noodzakelijkerwijze afdoende bewijs biedt dat de betalingstransactie door de betaler is toegestaan indien een betaler ontkent een uitgevoerde betalingstransactie te hebben toegestaan.
11. Om het gebruiksgemak bij kleine betalingen te verhogen, kunnen met betaalkaarten die een NFC chip hebben *low-value* betalingen worden geïnitieerd zonder enige vorm van cliëntauthenticatie. De houder van de betaalkaart hoeft deze alleen maar binnen het bereik van de sensor te houden om de betaalopdracht te initiëren. Om de gevolgen van misbruik te beperken is er een limiet ingesteld op het bedrag dat op dagelijkse basis met een dergelijke pas kan worden betaald.
12. Art. 4(29) PSD2 en het voorgestelde art. 7:514(a) BW in het concept van de Implementatiewet PSD2.

woord of een pincode); (ii) bezit (iets wat alleen de betaaldienstgebruiker heeft, bijvoorbeeld een betaalpas); en (iii) inherente eigenschap (iets wat de betaaldienstgebruiker is, bijvoorbeeld biometrische eigenschappen).[13] Deze factoren dienen onderling onafhankelijk te zijn. Met andere woorden, het falen van één element mag geen afbreuk doen aan de betrouwbaarheid van het andere element.

2.1. Wanneer is sterke cliëntauthenticatie vereist?

Wanneer de Implementatiewet PSD2 in 2018 inwerking treedt, dienen betaaldienstverleners sterke cliëntauthenticatie toe te passen indien een betaler: (i) online toegang verzoekt tot zijn betaalrekening; (ii) een elektronische betalingstransactie[14] initieert;[15] of (iii) via een communicatiemiddel op afstand een handeling uitvoert die een risico op betalingsfraude of andere vormen van misbruik met zich mee kan brengen.[16] Sterke cliëntauthenticatie wordt ook verplicht als een betaaldienstgebruiker gebruik gaat maken van de diensten van een betalingsinitiatiedienstverlener of een rekeninginformatiedienstverlener nadat PSD2 is geïmplementeerd in de Nederlandse wetgeving. Bovendien moeten betaaldienstverleners bij elektronische betalingstransacties die op afstand worden geïnitieerd, bijvoorbeeld via internet, sterke cliëntauthenticatie gebruiken waaraan een extra element wordt toegevoegd. Dit extra element bestaat eruit dat de authenticatiecode voor een betalingstransactie op dynamische wijze aan het specifieke bedrag en een specifieke betalingsbegunstigde wordt verbonden.[17] Dynamische verbondenheid wordt bewerkstelligd doordat een unieke authenticatiecode wordt gegenereerd op basis van de gegevens van de betalingsbegunstigde en het concrete bedrag dat aan die begunstigde wordt overgeboekt. Op deze wijze wordt voorkomen dat fraudeurs met behulp van een onderschepte authenticatiecode een frauduleuze betalingstransactie naar een andere betaalrekening kunnen initiëren.

3. Biometrische systemen en het betalingsverkeer

3.1. Wat is een biometrisch systeem?

Biometrische eigenschappen zijn de lichaams- en/of gedragseigenschappen van een natuurlijk persoon. Een biometrisch systeem is een systeem dat biometrische eigenschappen verwerkt voor identificatie- of verificatiedoeleinden. Biometrische systemen kunnen worden onderscheiden in systemen die fysieke eigenschappen herkennen, zoals een vingerafdruk, iris, of gezicht (zogenaamde statische biometrie) en systemen die een gedragspatroon analyseren, zoals iemands stem, handtekening[18] of toetsenborddynamiek[19] (zogenaamde dynamische biometrie). Hoewel PSD2 zelf niet refereert aan het gebruik van biometrische systemen als een van de elementen van sterke cliëntauthenticatie, wordt de rol van biometrie voor de invulling van dit vereiste onder PSD2 erkend door EBA.[20]

3.2. Statische biometrische systemen als onderdeel van sterke cliëntauthenticatie

De meer traditionele authenticatiemethoden (bijvoorbeeld door middel van een wachtwoord of

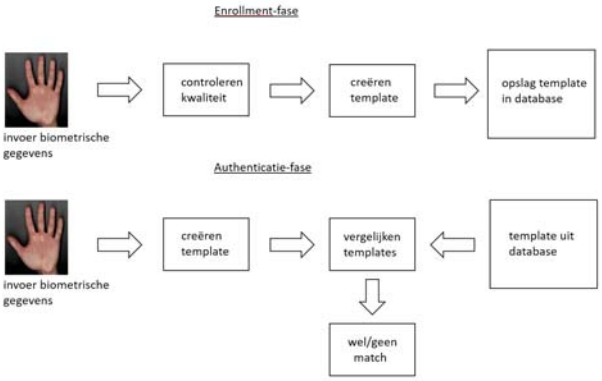
13. Art. 4(30) PSD2. In dit kader merken wij op dat EBA in haar discussion paper van 8 december 2015 '*Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2)*' de vraag heeft voorgelegd of de eIDAS Verordening (Verordening (EU) Nr. 910/2014) een mogelijke oplossing zou kunnen bieden om sterke cliëntauthenticatie te faciliteren. Daarnaast heeft de Europese Commissie in het groenboek over financiele retail diensten van 10 december 2015 (COM(2015) 630 final) erkend dat elektronische identificatie van betaaldienstgebruikers onder de eIDAS Verordening mogelijkerwijs door betaaldienstverleners kan worden gebruikt om invulling te geven aan het authenticatievereiste. Met de Betaalvereniging Nederland, de European Payments Council en de European Banking Federation zijn wij echter van mening dat de eIDAS Verordening met name relevant kan zijn bij de identificatie van nieuwe cliënten, maar dat de mogelijkheden die de eIDAS Verordening biedt minder relevant zijn voor de invulling van het sterke cliëntauthenticatie vereiste. Ook EBA noemt de eIDAS verordening niet meer in haar Finale Rapport RTS, terwijl zij in de Consultatieversie van het Finale Rapport RTS nog opmerkte dat het onder de voorgestelde RTS mogelijk zou moeten zijn om een sterke cliëntauthenticatiemethode te hanteren die is gebaseerd op de diensten van een openbaar stelsel voor elektronische identificatie onder de eIDAS Verordening.
14. Het begrip elektronische betalingstransactie omvat overmakingen en kaartbetalingen.
15. Bij betalingstransacties die door de begunstigde worden geïnitieerd (zoals incasso's) hoeft geen sterke clientauthenticatie te worden toegepast. Sterke cliëntauthenticatie geldt echter wel voor incasso's waarbij de betaler zijn instemming heeft gegeven middels een elektronische machtiging, aangezien dit heeft te gelden als het via een communicatiemiddel op afstand uitvoeren van een handeling die een risico op betalingsfraude of andere vormen van misbruik met zich mee kan brengen.
16. In het Finale Rapport RTS heeft EBA de mogelijkheid opgenomen voor betaaldienstverleners om bij bepaalde transacties een eigen risicoafweging te maken voor het al dan niet toepassen van sterke cliëntauthenticatie.
17. Art. 97(2) PSD2.
18. Bij handtekeninganalyse wordt een analyse van een handschriftsample gemaakt waarbij wordt gekeken naar bijvoorbeeld de vorm en de druk die is gebruikt bij het zetten van de handtekening.
19. Bij de analyse van toetsenborddynamiek wordt gekeken naar de manier en het ritme van typen op een toetsenbord.
20. In overweging (6) van het Finale Rapport RTS spreekt EBA uitdrukkelijk over biometrische sensoren.

pincode) hebben als nadeel dat ze geen onderscheid maken tussen een geautoriseerde gebruiker en een gebruiker die op frauduleuze wijze gebruik maakt van de authenticatiemiddelen van een ander. Het feit dat biometrische eigenschappen voor iedere persoon uniek zijn, maakt biometrische systemen naar onze mening bij uitstek geschikt als instrument om de identiteit van betaaldienstgebruikers mee te verifiëren. Hiermee wordt op passende wijze invulling gegeven aan het element inherente eigenschap als onderdeel van sterke cliëntauthenticatie.

De toepassing van een statisch biometrisch systeem als onderdeel van sterke cliëntauthenticatie, bijvoorbeeld een betaalproduct dat gebruik maakt van gezichtsherkenning, werkt als volgt. Alvorens de betaaldienstgebruiker het betaalproduct kan gebruiken, maakt de betaaldienstverlener een biometrische template van het gezicht van de betaaldienstgebruiker. Tijdens dit proces, dat ook wel de enrollment-fase wordt genoemd, wordt er een foto gemaakt van het gezicht van de betaaldienstgebruiker.[21] Vervolgens wordt er een aantal gezichtskenmerken[22] van deze foto op basis van een algoritme geselecteerd en verwerkt in de biometrische template.[23] Deze biometrische template fungeert als referentiemateriaal wanneer de betaaldienstgebruiker het betaalproduct gaat gebruiken. Als de betaaldienstgebruiker zich tijdens de authenticatiefase identificeert, door bijvoorbeeld met zijn smartphone een foto te maken van zijn gezicht, worden de relevante kenmerken uit deze foto vergeleken met de kenmerken zoals opgeslagen in de biometrische template.

Aangezien de foto van het gezicht van een betaaldienstgebruiker nooit precies gelijk zal zijn aan de foto die tijdens de enrollment-fase is gemaakt, is er in de praktijk vrijwel nooit sprake van een 100% match. Daarom wordt er bij biometrische authenticatie gewerkt met een matchingspercentage dat lager is dan 100%, maar dat nog steeds voldoende hoog is om de veiligheid en betrouwbaarheid van het betaalproduct te waarborgen. Wanneer de overeenkomsten tussen de biometrische template gemaakt tijdens de authenticatiefase en de opgeslagen biometrische template groter is dan een vooraf gespecificeerde drempel, vindt er een positieve authenticatie plaats. Bij het vaststellen van de te hanteren authenticatiedrempel dient de betaaldienstverlener een balans te vinden waarbij sprake is van een acceptabele False Acceptance Rate (hierna: FAR) en een acceptabele False Rejection Rate (hierna: FRR).[24] De FAR is een maatstaf voor het risico dat onterecht een positieve authenticatie plaatsvindt. De FRR is een maatstaf voor het risico dat er ten onrechte een negatieve authenticatie plaatsvindt. Dat geen enkel biometrisch systeem een FAR en FRR haalt van 0% lijkt ook EBA te accepteren. Het Finale Rapport RTS stelt aan apparaten en software die gebruikt worden voor biometrische authenticatie slechts de eis dat deze ervoor zorgen dat er een zeer geringe kans bestaat dat een onbevoegde als betaler wordt geauthentiseerd.[25] EBA heeft daarbij geen concrete tolerantiedrempels gedefinieerd.

Onderstaande figuur geeft weer hoe een authenticatieproces werkt waarbij gebruik wordt gemaakt van statische biometrie.



3.3. Praktische bezwaren aan gebruik statisch biometrisch systeem

Er is een aantal praktische kanttekeningen te plaatsen bij het gebruik van een statisch biometrisch systeem. Hoewel het risico op een hoge FAR bij een dergelijk systeem relatief beperkt is, is het voor een betaaldienstgebruiker in geval van fraude zeer lastig te bewijzen dat er sprake is geweest van onterechte toegang.[26] Hierbij speelt mee dat er, door onder meer het gebruik van vingerafdrukken in de criminele opsporing, een breed maatschap-

21. Dit kan bijvoorbeeld met behulp van de camera op een smartphone, tablet of laptop.
22. Omdat de afstanden op een foto verschillen naar mate de foto van dichterbij of verder af wordt gemaakt, wordt er in de praktijk veelal gewerkt met verhoudingen. Bijvoorbeeld de verhouding tussen de afstand van de ogen ten opzichte van de afstand tussen de neus en lippen van de betaaldienstgebruiker.
23. Deze methode wordt bijvoorbeeld gebruikt door Atom bank. Atom bank maakt een template op basis van gezichtsherkenning en spraak zonder daarbij afbeeldingen of geluidsfragmenten op te slaan.
24. Van Velzen, Oostdijk en Wegdam,'Biometrie voor Sterke Authenticatie: een State-of-the Art scan', 14 januari 2016, p. 2.
25. Art. 8(1) Finale Rapport RTS.
26. Art. 7:527 BW bepaalt dat als de betaaldienstverlener ontkent te hebben ingestemd met een uitgevoerde betalingstransactie, of aanvoert dat een betalingstransactie niet correct is uitgevoerd, het aan de betaaldienstverlener is om bewijs te leveren dat de betalingstransactie is geauthenticeerd, deze juist is geregistreerd en geboekt en deze niet door een technische storing of enig ander falen van de door de betaaldienstverlener aangeboden diensten is beïnvloed. De betaaldienstverlener zal hier in het geval van sterke cliëntauthenticatie in beginsel aan kunnen voldoen door te bewijzen dat het betaalinstrument is gebruikt voor de overmaking en in dit kader bijvoorbeeld een vingerafdruk is ingescand die matcht met de opgeslagen template. De betaaldienstgebruiker zal in een dergelijk geval niet eenvoudig bewijs aan kunnen leveren dat de vingerafdruk hem niet toebehoort.

pelijk vertrouwen bestaat in de betrouwbaarheid van het gebruik van vingerafdrukken voor identificatiedoeleinden. Het argument dat een gebruikte vingerafdruk niet aan een betaaldienstgebruiker toebehoort die aantoonbaar dezelfde vingerafdruk heeft, zal derhalve niet snel worden gehonoreerd. Daarnaast kan het voor een betaaldienstgebruiker bijzonder lastig zijn om zijn biometrische gegevens aan te passen als deze zijn gecorrumpeerd. Hiertoe zal de software die gebruikt wordt door de betaaldienstverlener verschillende templates moeten kunnen maken van dezelfde biometrische gegevens, zodat, als een van de templates vanwege, bijvoorbeeld, fraude onbruikbaar is geworden, er een andere template gemaakt kan worden.[27]

3.4. Dynamische biometrische systemen als onderdeel van sterke cliëntauthenticatie

Indien een betaalproduct gebruik maakt van een dynamisch biometrisch systeem, worden in grote lijnen dezelfde stappen doorlopen als bij een statisch biometrisch systeem. Echter, tijdens de enrollment-fase wordt er een biometrische template van de betaaldienstgebruiker aangemaakt op basis van gedragspatronen in plaats van fysieke eigenschappen.[28] Hiervoor worden gedurende een bepaalde periode biometrische gegevens verzameld en niet, zoals bij een statische biometrisch systeem, uitsluitend op één specifiek moment. Tijdens de authenticatiefase kunnen dynamische systemen verschillend worden toegepast. Systemen die functioneren op basis van handtekeningherkenning of stemherkenning lijken geschikt om in deze fase op dezelfde wijze te worden gebruikt als statische systemen, namelijk, indien een betaaldienstgebruiker bijvoorbeeld gebruik maakt van internetbankieren, alleen bij het inloggen en het initiëren van een betaalopdracht. Op dat moment wordt de wijze waarop een handtekening wordt gezet vergeleken met de opgeslagen biometrische template. Dynamische systemen zoals typpatroonherkenning zijn geschikter om biometrische gegevens van de betaaldienstgebruiker te verifiëren gedurende de gehele periode dat hij is ingelogd. Hierbij wordt dan doorlopend het typpatroon vergeleken met de opgeslagen biometrische template. Indien op enig moment de vereiste authenticatiedrempel niet wordt gehaald, kan bij een dergelijk systeem het betaalproduct worden geblokkeerd.

Een belangrijk voordeel van dynamische biometrie ten opzichte van statische biometrie is dat dynamische biometrie de betaaldienstverlener in staat stelt om ten aanzien van betalingstransacties real-time risicoanalyses uit te voeren.[29] Dit is van belang aangezien betaaldienstverleners onder PSD2 niet verplicht zijn sterke cliëntauthenticatie toe te passen voor betalingen met een waarde tot EUR 500 die een laag risico op fraude vormen. Om vast te kunnen stellen of er voor een bepaalde categorie betalingen een laag risico op fraude geldt, heeft EBA in het Finale Rapport RTS een aantal toetselementen geïdentificeerd, waaronder: (i) of er sprake is van een abnormaal bestedingspatroon; (ii) of de betaaldienstgebruiker de betaalopdracht vanaf een abnormale locatie heeft geïnitieerd; en (iii) of de betaaldienstgebruiker een abnormaal gebruik maakt van het apparaat of de software waarmee de betaling is geïnitieerd.[30] Naar onze mening kunnen dynamische biometrische systemen in dit kader effectief door betaaldienstverleners worden ingezet om te analyseren of er sprake is van een abnormaal gebruik van het apparaat of de software door de betaaldienstgebruiker.

3.5. Praktische bezwaren gebruik dynamisch biometrisch systeem

De technologie achter dynamische biometrische systemen lijkt nog onvoldoende ontwikkeld om als separate invulling van het element inherente eigenschap voor sterke cliëntauthenticatie te kunnen worden gebruikt. Met name een gebrek aan precisie blijft een van de grootste bezwaren tegen het gebruik van dynamische biometrische systemen als separate invulling van het element inherente eigenschap voor sterke cliëntauthenticatie.[31] Authenticatie op basis van gedragsanalyse is complex aangezien menselijk gedrag varieert afhankelijk van factoren zoals de toestand en de omgeving waarin de betaaldienstgebruiker zich bevindt. Deze variatie kan leiden tot een hoge FRR waardoor er te vaak ten onrechte een negatieve authenticatie wordt vastgesteld. Dit probleem kan deels worden ondervangen door gebruik te maken van een combinatie van verschillende gedragssystemen die gezamenlijk een uniek biometrisch profiel van de betaaldienstgebruiker vormen.[32] Daarnaast kan de betrouwbaarheid van de biometrische template van de betaaldienstgebruiker bij bepaalde biometrische systemen worden verhoogd door de gegevens van de biometrische template continu te updaten en te verfijnen op basis van nieuwe informatie verkregen tijdens de authenticatiefase. Dit is bijvoorbeeld mogelijk bij het biometrische systeem typpatroonherkenning.

Ook EBA erkent dat gedragsanalyse niet als zelfstandig inherente eigenschap element kan gelden

27. Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies', 27 april 2012, p. 32.
28. Afhankelijk van het biometrisch systeem dat wordt gebruikt, is voor gedragsanalyse vaak geen nieuwe hardware vereist. Veel smartphones zijn bijvoorbeeld al uitgerust met bewegingssensoren.
29. Aimbrain, 'Biometrics and PSD2', 2016, p. 4.
30. Artt. 16(2)(b) juncto 2(4) Finale Rapport RTS.
31. Li, Xie en Bian,'SegAuth: A Segment-based Approach to Behavioral Biometric Authentication', 2016 IEEE Conference on Communications and Network Security (CNS), p. 1.
32. BehavioSec,'Behavioral Biometrics: Balancing security with usability', White Paper, p. 4.

in het kader van sterke cliëntauthenticatie, maar dat het wel een positieve bijdrage kan leveren als een aanvullend instrument voor fraudepreventie.[33] Op dit moment biedt gedragsanalyse vooral mogelijkheden als extra veiligheidsmechanisme dat op de achtergrond mogelijke risico's signaleert die veeleer te maken hebben met het gebruik van betaalproducten nadat daartoe door middel van andere authenticatietechnieken toegang is verkregen. Dynamische biometrie lijkt dan ook met name zinvol indien dit gebruikt wordt in combinatie met andere authenticatietechnieken en het gebruik hiervan gaat in feite verder dan de verplichtingen die voortvloeien uit PSD2.[34]

4. Mogelijke risico's bij het toepassen van biometrische authenticatie

Hoewel het gebruik van biometrische authenticatie leidt tot veilige en gebruiksvriendelijke betaalproducten, aangezien je bijvoorbeeld je vingerafdrukken altijd bij je hebt, bestaan er ook twijfels omtrent de wenselijkheid van het gebruik hiervan. Er zijn grofweg twee categorieën van veel gehoorde bezwaren: (i) de inbreuk op de privacy van betaaldienstgebruikers; en (ii) het gevaar van identiteitsfraude.[35]

4.1. Inbreuk op de privacy van betaaldienstgebruikers

Een veelgehoorde zorg is dat het gebruik van biometrische authenticatie zou kunnen leiden tot een inbreuk op de privacy van betaaldienstgebruikers, bijvoorbeeld doordat betaaldienstverleners meer biometrische gegevens verzamelen dan nodig is voor het authenticeren van betalingstransacties.[36] Uit een irisscan, vingerafdruk of afbeelding van het gezicht kan bijvoorbeeld informatie over de gezondheid of het ras van de betaaldienstgebruiker worden afgeleid, terwijl deze informatie niet noodzakelijk is voor het authenticatieproces bij betaaldiensten.[37] Deze gegevens zijn zeer privacygevoelig en gelden dan ook als bijzondere persoonsgegevens onder de Wet bescherming persoonsgegevens (hierna: Wbp).[38] De verwerking van bijzondere persoonsgegevens door een betaaldienstverlener is in beginsel verboden, tenzij de betaaldienstgebruiker hiertoe uitdrukkelijk toestemming heeft gegeven of indien er een wettelijke grondslag bestaat.[39] Toestemming is echter alleen geldig indien de betaaldienstgebruiker weet waarvoor de toestemming wordt gegeven.[40] Betaaldienstverleners zullen derhalve vooraf duidelijk dienen te communiceren over de wijze waarop biometrische gegevens worden verwerkt en opgeslagen.[41]

De privacybezwaren worden deels ondervangen doordat betaaldienstverleners veelal werken met biometrische templates.[42] Op basis van deze biometrische templates moet dan de oorspronkelijke afbeelding, bijvoorbeeld de foto van een iris, niet kunnen worden gereproduceerd.[43] Hierdoor kunnen op basis van de biometrische template geen gegevens over bijvoorbeeld het ras van de betaaldienstgebruiker worden vastgesteld, waardoor er geen sprake is van bijzondere persoonsgegevens in de zin van de Wbp.[44] Biometrische templates gelden overigens wel als persoonsgegevens onder de Wbp.[45] Een ander privacy gerelateerd bezwaar is dat betaaldienstgebruikers niet weten of betaaldienstverleners de verzamelde ruwe persoonsgegevens verwijderen.[46] Daar komt bij dat de gemiddel-

33. Consultatieversie van het Finale Rapport RTS, p. 12.
34. Maghsoudi en Tappert, 'A Behavioural Biometrics User Authentication Study Using Motion Data from Android Smartphones', Seidenberg School of CSIS, Pace University.
35. Hoewel er in de literatuur melding wordt gemaakt van eventuele godsdienstige bezwaren ten aanzien van het gebruik van biometrische systemen, behandelen wij deze bezwaren niet in deze bijdrage. Hetzelfde geldt voor praktische bezwaren bij het gebruik van biometrische systemen door bijvoorbeeld mindervaliden, ouderen of zieken.
36. Een veelgebruikte term in dit kader is '*function creep*'; het langzaam veranderen van het gebruik van verzamelde data, waardoor het gebruik steeds verder af komt te staan van het oorspronkelijke doel waarvoor de data werd verzameld. Zie hierover bijvoorbeeld het Wetenschappelijk Onderzoek- en Documentatiecentrum Ministerie van Veiligheid en Justitie, Justitiële verkenningen, jrg. 37, nr. 8, 2011 Function creep en privacy.
37. Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies', 27 april 2012, p. 21.
38. Art. 16 Wbp merkt persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag aan als bijzondere persoonsgegevens.
39. Art. 23 Wbp. Met betrekking tot de wettelijke grondslag bepaalt dit artikel dat de uitzondering op het verwerkingsverbod slechts geldt indien dit noodzakelijk is met het oog op een zwaarwegend algemeen belang en er passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer.
40. Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies', 27 april 2012, p. 11.
41. Art. 33 Wbp.
42. Noch PSD2 noch het Finale Rapport RTS verplicht het gebruik van dergelijke templates bij de toepassing van een biometrisch systeem voor authenticatiedoeleinden. EBA noemt in overweging (6) van het Finale Rapport RTS overigens wel de bescherming van templates als aandachtspunt bij de toepassing van sterke cliëntauthenticatie.
43. Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies', 27 april 2012, p. 4.
44. CBP 19 maart 2001, nr. z2000-0080.
45. Zie noot 44.
46. Art. 10 Wbp schrijft voor dat persoonsgegevens niet langer in een vorm die het mogelijk maakt de betrok-

de betaaldienstgebruiker geen inzicht heeft in wat er met diens gegevens gedaan wordt en of er informatie wordt gedeeld met derden. Dit punt wordt grotendeels ondervangen door de informatieplicht die op gegevensverwerkers rust. Betaaldienstverleners moeten betaaldienstgebruikers informeren over de doeleinden van de verwerking waarvoor de gegevens bestemd zijn.[47] Daarnaast biedt de Wbp betaaldienstgebruikers de mogelijkheid om de betaaldienstverlener te verzoeken hen mede te delen of de betaaldienstverlener persoonsgegevens verwerkt die betrekking hebben op de betaaldienstgebruiker.[48] De betaaldienstverlener moet de betaaldienstgebruiker dan schriftelijk en binnen vier weken meedelen of deze de betaaldienstgebruiker betreffende persoonsgegevens verwerkt. De betaaldienstgebruiker kan de betaaldienstverlener vervolgens verzoeken om zijn persoonsgegevens te verwijderen.[49]

4.2. Gevaar van identiteitsfraude

Een van de grootste veiligheidsrisico's in het betalingsverkeer is identiteitsfraude. Bij identiteitsfraude maakt een persoon gebruik van valse of gestolen identiteitsgegevens.[50] Identiteitsfraude is relatief eenvoudig bij de meer traditionele methoden van authenticatie zoals het gebruik van een betaalkaart in combinatie met een pincode. Een betaalkaart en pincode kunnen immers worden overgedragen aan derden. Daarbij komt dat consumenten vaak onzorgvuldig omgaan met hun gegevens. Zo'n 25% van de mensen bewaart de pincode bij de betaalpas en hetzelfde wachtwoord wordt vaak voor verschillende doeleinden gebruikt.[51] De gevolgen van identiteitsfraude bij biometrische systemen zijn echter groter. In tegenstelling tot bijvoorbeeld een wachtwoord, kan een vingerafdruk nooit worden gewijzigd. Een persoon wiens biometrische gegevens ontvreemd zijn, kan hier de rest van zijn leven nadeel van ondervinden.

Toch wordt het gebruik van biometrische systemen gezien als een belangrijk wapen in de strijd tegen identiteitsfraude. Fysieke of gedragseigenschappen zijn immers moeilijker te vervalsen dan een wachtwoord. Dit geldt met name voor dynamische biometrie, aangezien het moeilijker is om iemands gedragspatroon te kopiëren dan om een enkele vingerafdruk na te maken.

Overigens bieden biometrische systemen geen garantie tegen identiteitsfraude. Aangezien mensen overal vingerafdrukken achterlaten, kunnen criminelen relatief eenvoudig aan een vingerafdruk komen om te vervalsen. Daarnaast is vaak geen volledige vingerafdruk vereist maar zijn enkele unieke kenmerken van de vingerafdruk voldoende voor een positieve authenticatie. Dit is bijvoorbeeld de reden geweest dat Albert Heijn in 2009 is gestopt met een proef met betalen via vingerafdrukken. Een beveiligingsspecialist wist het systeem te misleiden met een rubberen kopie van een vingerafdruk.[52] Hierbij moet overigens worden opgemerkt dat het op grote schaal namaken van vingerafdrukken nog altijd moeilijker is dan het op grote schaal hacken van wachtwoorden, aangezien er steeds een vorm van interactie moet zijn met de betaaldienstgebruiker om aan diens vingerafdruk te komen, terwijl dit voor het hacken van wachtwoorden niet vereist is.

Indien gebruik wordt gemaakt van biometrische templates blijft bovendien het risico bestaan dat een consument slachtoffer wordt van *phishing*; de consument geeft zijn gegevens, bijvoorbeeld een vingerafdruk, aan een fraudeur in de veronderstelling verkerende dat dit zijn betalingsinitiatiedienstverlener is.[53]

Betaaldienstgebruikers weten bovendien niet of het programma dat gebruikt wordt door een betaaldienstverlener een biometrische template creëert dat uniek is voor die specifieke betaaldienstverlener, of dat er meerdere partijen zijn die hetzelfde programma gebruiken. In het laatste geval zou een hacker die templates bij een betaaldienstverleners heeft ontvreemd zich ook toegang kunnen verschaffen tot betaalrekeningen die worden aangehouden bij andere betaaldienstverleners. Met het oog op zowel dit risico als het risico dat gegevens in de template databank door een fraudeur worden gewijzigd, is het raadzaam om biometrische templates niet centraal op te slaan, maar bij voorkeur op een apparaat dat de betaaldienstgebruiker in zijn bezit heeft. Dit zorgt ervoor dat de kans op grootschalige aanvallen wordt verkleind.[54] Daarnaast kan identiteitsfraude worden bestreden door een vitaliteitscontrole in te bouwen, waarbij wordt gecontroleerd of de gebruiker van het systeem levend is.[55] Een nagemaakte vinger zou dan bijvoorbeeld niet werken.

5. Slotbeschouwing

Met EBA zijn wij van mening dat het gebruik van statische biometrische systemen een goede invulling kan zijn van het element inherente eigenschap

kene te identificeren bewaard mogen worden dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.

47. Art. 33 Wbp.
48. Art. 35 Wbp.
49. Art. 36 Wbp.
50. Artt. 231a en 231b Wetboek van Strafrecht.
51. Jain, Hong, Pankanti, 'Biometric Identification', Communication of the ACM, februari 2000/Vol 43, No 2, p. 92.
52. https://tweakers.net/nieuws/59066/ah-vindt-betalen-via-vingerafdruk-nog-niet-veilig-genoeg.html.
53. Zie bijvoorbeeld de opmerking van de Association of Latvian Banks in haar commentaar op de consultatieversie van het Finale Rapport RTS.
54. Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies', 27 april 2012, p. 31.
55. Prabhakar, Pankanti, Jain, 'Biometric Recognition: Security and Privacy Concerns', *IEEE Security and Privacy Magazine*, april 2003, p. 39.

als onderdeel van de sterke cliëntauthenticatie. Biometrische gegevens zijn immers persoonsspecifiek en daardoor bij uitstek geschikt voor de identificatie van betaaldienstgebruikers. Daarnaast lijkt er een breed draagvlak onder consumenten te zijn voor het gebruik van deze systemen en beschikt de meerderheid van de Nederlandse consumenten reeds over de noodzakelijk technologie, bijvoorbeeld omdat moderne smartphones vaak al zijn uitgerust met biometrische sensoren. Dynamische biometrische systemen lijken bij de huidige stand van de technologie minder geschikt als invulling van het element inherente eigenschap als onderdeel van de sterke cliëntauthenticatie, maar vormen wel een waardevol instrument in de strijd tegen identiteitsfraude indien deze worden gebruikt in aanvulling op de sterke cliëntauthenticatie. Betaaldienstverleners kunnen dynamische biometrische systemen bijvoorbeeld inzetten als real-time risicoanalyse mechanisme in het kader van de vrijstelling van het sterke cliëntauthenticatievereiste.
Bezwaren tegen het gebruik van biometrische systemen zijn onder meer de daaraan verbonden privacy risico's en de kans op identiteitsfraude. Hoewel betaaldienstgebruikers zich rekenschap dienen te geven van deze risico's, menen wij dat deze risico's voldoende kunnen worden ondervangen en daardoor geen belemmering hoeven te vormen voor een succesvolle toepassing van biometrische systemen als onderdeel van het sterke cliëntauthenticatievereiste.