Een Vergelijking van Elektronische Betaalmethoden voor E-commerce

Bart Schotten - 0313319
bschotten@student.ru.nl

Onder begeleiding van dr.ir. E. (Erik) Poll

26 juni 2007

Bachelorscriptie Informatiekunde
Radboud Universiteit Nijmegen

Samenvatting

In deze scriptie wordt een aantal elektronische betaalmethoden vergeleken. De te vergelijken betaalmethoden maken allemaal primair gebruik van internet, worden in de praktijk gebruikt en hebben twee fundamentele eigenschappen: de betaling kan binnen korte tijd, en over lange afstand plaatsvinden. De centrale vraag is waarin deze betaalmethoden verschillen en wat deze verschillen betekenen voor de kwaliliteit van de methoden op het gebied van security. In het eerste deel van de scriptie wordt een aantal dimensies beschreven aan de hand waarvan de betaalmethoden te classificeren zijn. In het tweede deel worden de securitydoelen gepresenteerd waaraan de methoden getoetst kunnen worden. In het derde deel wordt uitgebreid besproken hoe de belangrijkste betaalmethoden kunnen worden geclassificeerd en gekwalificeerd aan de hand van die securitydoelen. Tot slot worden er conclusies getrokken uit de classificatie en de kwalificatie.

Inhoudsopgave

1 Inleiding

Steeds meer mensen maken gebruik van e-commerce. Uit een onderzoek van het Centraal Bureau voor de Statistiek blijkt dat 61% van de Nederlanders in 2006 wel eens iets online heeft gekocht, terwijl dit in 2002 nog maar 40% was. In 2005 werd er in totaal 2,2 miljard euro aan uitgegeven, bijna 2,5 keer zo veel als in 2002. 10% van de online shoppers maakt zich zorgen over de veiligheid van de betaalmethode. Van de groep die zelden of nooit iets online koopt noemde in 2005 35% de veiligheid als reden. In 2006 noemde 38% als reden het privacy-aspect. Zij hadden er problemen mee om hun persoonlijke informatie af te staan [16].

Veel van de online aankopen worden betaald via traditionele betaalmethoden, zoals betaling via acceptgiro of contante betaling bij aflevering. elektronische betaalmethoden winnen echter terrein. In 2006 werd de creditcard door 39% van de consumenten gebruikt om online te betalen, en was het gebruik van iDEAL [13] toegenomen tot 27% [5]. elektronische betaalmethoden bieden duidelijk voordelen ten opzichte van traditionele betaalmethoden, maar het is nog niet duidelijk welke methode nu echt de beste is.

Om wat orde in de chaos te scheppen willen we in deze scriptie verschillende elektronische betaalmethoden voor e-commerce vergelijken. Specifieker zijn we op zoek naar het antwoord op twee deelvragen.

1. Welke verschillende soorten/categorieën van elektronische betaalmethoden voor e-commerce zijn er te onderscheiden?
2. Aan welke securitydoelen moeten deze betaalmethoden voldoen, en hoe voldoen verschillende soorten betaalmethoden daaraan?

Echter, nog voordat we kunnen beginnen met het beantwoorden van de eerste deelvraag, moet eerst, om deze taak te verduidelijken, een tweetal andere vragen gesteld worden. Ten eerste willen we weten wat we verstaan onder een betaalmethode, en ten tweede moet het duidelijk zijn over welke betaalmethoden we het precies gaan hebben. Wat is een elektronische betaalmethode voor e-commerce?

1.1 Betaalmethoden

Waar hebben we het eigenlijk over als we het hebben over een betaalmethode? Een betaalmethode is meer dan een betaling op zich. We moeten kijken naar de transactie als geheel. Figuur 1, uit [7] geeft een generiek betaalmodel weer. Dit lijkt complex, maar alle concepten beschreven in dit model zijn nodig om betaalmethoden te begrijpen. Hieronder volgt een beschrijving van die concepten.

Payer/Betaler De betaler krijgt een betaalmiddel van de uitgever in ruil voor geld.

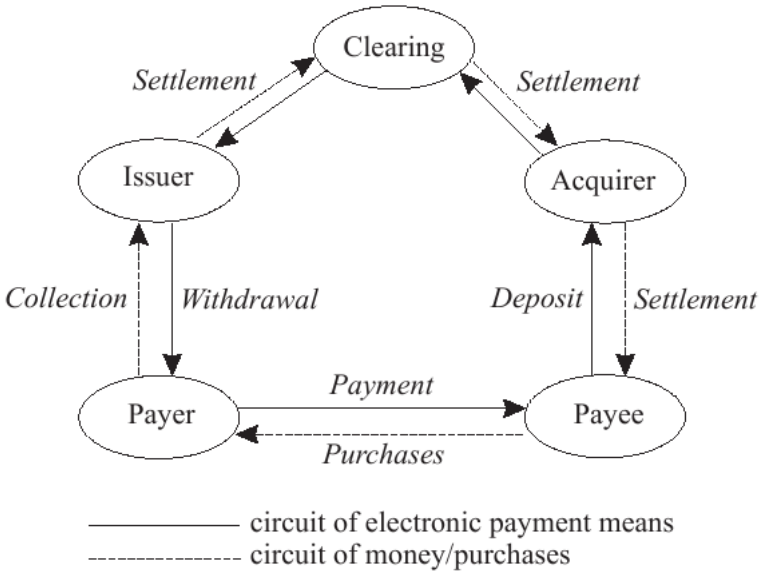
Payee/Betaalde De betaalde krijgt een betaalmiddel (als bewijs van betaling) van de betaler, en levert in ruil daarvoor goederen of diensten.

Issuer/Uitgever De uitgever krijgt geld van de betaler en geeft in ruil daarvoor een betaalmiddel uit.

Acquirer/Ontvanger De ontvanger krijgt van de betaalde een betaalmiddel en geeft, als het betaalmiddel geldig is, geld aan de betaalde.

Clearing Het proces waarbij het betaalmiddel nog eens op geldigheid wordt gecontroleerd en de schuld van de uitgever aan de ontvanger wordt voldaan. Dit is uiteraard alleen nodig als de uitgever en ontvanger niet dezelfde partij zijn.

Interessant is dat dit model zo generiek is dat het ook opgaat voor niet-elektronische betaalmiddelen zoals contant geld. De vraag is dan alleen wat de betaler aan de uitgever geeft in ruil voor dat betaalmiddel.



Figuur 1: Generiek model van een elektronisch betaalsysteem [7]

1.2 Elektronische betaalmethoden voor e-commerce

Belangrijk is om vast te stellen wanneer een betaalmethode een elektronische betaalmethode voor e-commerce is. Het belangrijkste aspect van e-commerce is de rol van internet[1]. Betalen met een pinpas is een voorbeeld van een elektronische betaalmethode waarbij internet geen rol speelt. Het grote verschil hiermee is dat betaler en betaalde niet fysiek bij elkaar aanwezig zijn en dat ze gescheiden zijn door potentieel onveilige hard- en software. Dit betekent dat allerlei security controls (met name fysieke) om fraude te voorkomen niet mogelijk zijn. Dit moet vanzelfsprekend gecompenseerd worden door andere controls.

Een andere eigenschap van e-commerce is de mogelijkheid om niet alleen fysieke goederen, maar ook elektronische goederen [11], zoals muziek in mp3-formaat, te kopen. Het is belangrijk om dit onderscheid in de aard van het product te maken, aangezien dit andere mogelijkheden biedt wat betreft security controls. Zo kun je bij elektronische goederen bijvoorbeeld streven naar *Certified Atomic Delivery*, wat betekent dat zowel betaling als product correct ontvangen moeten zijn om de transactie door te laten gaan. Dit kan afgedwongen worden met cryptografische methoden [27]. Bij dit soort transacties is het in ieder geval essentieel dat de betaling vrijwel direct plaatsvindt, en hierdoor lijken traditionele betaalmiddelen geen optie. Deze scriptie richt zich op betaalmethoden die voor e-commerce in het algemeen bruikbaar zijn, en zal dus kijken naar methoden waarbij betaling vrijwel direct plaats kan vinden.

Deze scriptie gaat dus over betaalmethoden die aan twee basiseisen voldoen:

1. De betaling moet op grote afstand kunnen plaatsvinden.
2. De betaling moet binnen zeer korte tijd kunnen plaatsvinden.

2 Classificatie

We kunnen op verschillende manieren onderscheid maken tussen elektronische betaalmethoden. Een aspect waarop onderscheid gemaakt kan worden noemen we een dimensie. In

[1] Er zijn ook vormen van e-commerce die geen gebruik maken van internet, maar van bijvoorbeeld GSM [9]. Hier zullen we ons in deze scriptie niet op richten.

deze sectie zullen we een selectie van dimensies geven op basis van welke er in de literatuur worden onderscheiden. Het doel is een zo compleet mogelijk overzicht te geven.

2.1 Dimensies

Account-gebaseerd versus token-gebaseerd Dit is een verschil dat veel gemaakt wordt [1]. Het wordt ook aangeduid als respectievelijk *pay-by-instruction* en *prepaid electronic cash* [26] of *credit-debit* en *digital currency* [12] systemen. Met digital currency wordt bedoeld dat deze variant het meest lijkt op contant geld, omdat het werkt met tokens die een waarde voorstellen, zoals ook bankbiljetten een waarde voorstellen, en de tokens niet verbonden zijn aan een bepaald persoon. Dit in tegenstelling tot account-gebaseerde systemen, waarbij een account wel aan persoon verbonden moet zijn.

Credit versus debet Dat account-gebaseerde systemen ook aangeduid worden als credit-debit systemen suggereert dat er daarin ook een onderscheid ligt: wordt er uitgegaan van een positief saldo bij de betaler, of wordt het geld eerst afgeschreven bij de ontvanger en wordt dat vervolgens op de betaler verhaald?

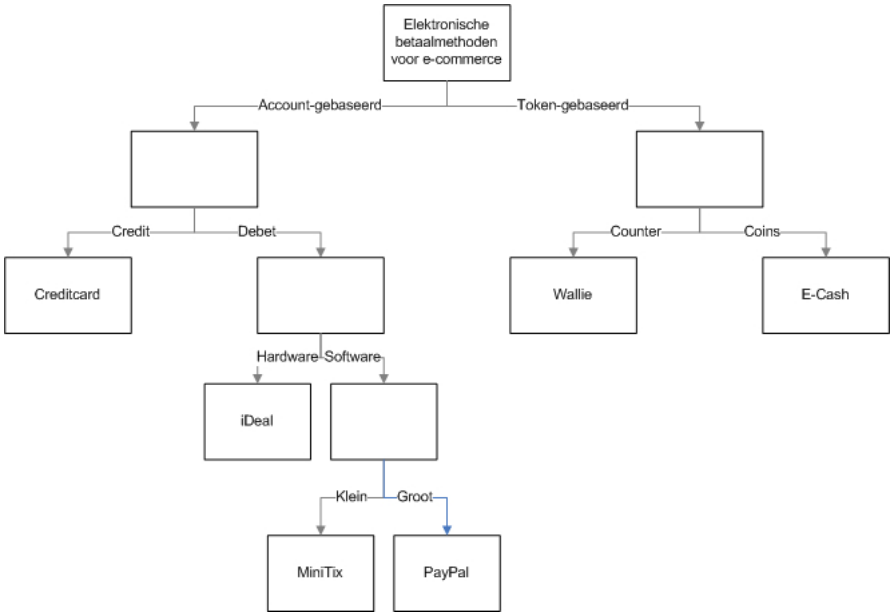
Counter versus coins Ook binnen token-gebaseerde systemen is een onderscheid te maken volgens Schoenmakers [26]. Een token kan namelijk op twee manieren gebruikt worden. De token kan een teller bijhouden met hoeveel waarde hij nog representeert, zodat één token voor meerdere betalingen gebruikt kan worden, en een token kan simpelweg een vaste waarde representeren, zoals bij contant geld.

Online versus offline Er kan een onderscheid gemaakt worden tussen systemen waarbij de betaler en de betaalde live in contact moeten staan met een derde partij (uitgever en/of ontvanger) en systemen waarbij dat niet hoeft. De eerste noemen we *online* en de tweede *offline* [26]. Bij offline systemen kan de uitgever of ontvanger niet tijdens de transactie controleren op mogelijke fraude. Dit dient dus ervóór te gebeuren, door te zorgen dat het uitgegeven betaalmiddel zelf veilig is (het principe van token-gebaseerde systemen), of eventueel erna, door te vertrouwen op het detecteren in plaats van het voorkomen van fraude [3].

Hardware versus software In de inleiding hebben we beschreven dat de realiteit bij elektronische betaalmethoden voor e-commerce is dat betaler en betaalde gescheiden zijn door potentieel onveilige hard- en software. Dit is echter niet helemaal waar. Een betaalmethode kan ook gebruik maken van speciale hardware waarvan de veiligheid wel gegarandeerd kan worden. Een voorbeeld van dergelijke hardware is een smartcard [26]. Dit onderscheid kan zowel interessant zijn vanuit security-oogpunt als vanuit praktisch oogpunt, want het gebruik van speciale hardware is misschien niet de goedkoopste en makkelijkste oplossing.

Grootte van de betaling Hoewel er geen zwart-wit onderscheid in te maken is, is de grootte van de betaling ook een belangrijke dimensie. In theorie zou bij iedere betaling misschien optimale security gewenst zijn, maar in de praktijk heb je te maken met bepaalde trade-offs. Aan elke transactie zijn wel kosten verbonden en bij zogenaamde *micropayments* (bijvoorbeeld betalen per geopende webpagina) wil je die eigenlijk minimaliseren [3]. Ook de benodigde inspanning voor de gebruiker moet minimaal zijn. Aan de andere kant is de potentiële schade bij een fout in het systeem minder, omdat het om minder grote bedragen gaat. Het ligt dus voor de hand om bij micropayments minder uitgebreide beveiligingsmiddelen te eisen.

We zullen bij deze dimensie onderscheid maken tussen klein en groot. Als een methode geschikt is voor kleine bedragen, dan betekent dit dat de kosten per transactie laag zijn en de vereiste inspanning van de partijen klein is. Als een methode geschikt is voor grote bedragen, dan betekent dit dat er geen limiet is die kleiner is dan een paar duizend euro.



Figuur 2: De classificatieboom

In verschillende artikelen [26, 3] wordt de gebruikte cryptografische methode ook als een onderscheidende dimensie gezien, maar wij zien dit soort eigenschappen niet als functionele verschillen, maar als middel om een doel te bereiken. Om die reden beperken we ons tot deze dimensies.

Aan de hand van daadwerkelijk in de praktijk gebruikte betaalmethoden zullen we kunnen beoordelen of deze dimensies in de praktijk ook zinvol blijken. Het lijkt er bijvoorbeeld op dat er niet veel systemen zijn die volgens de definitie offline functioneren.

2.2 Classificatieboom

Om elektronische betaalmethoden te onderscheiden aan de hand van deze dimensies hebben we ervoor gekozen een boom te maken. Elke dimensie kun je als een splitsing in de boom zien, net als bij bijvoorbeeld determinering in de biologie. Dit idee wordt ook toegepast door Abrazhevich [1], maar onze uitwerking van de boom is anders (figuur 2).

De keuze voor een boom is niet alleen visueel interessant, maar dient ook om aan te geven dat niet elke mogelijke indeling van een betaalmethode zinnig is. Zo sluit de positionering in de ene dimensie soms positionering in een andere dimensie uit. Het indelen van een methode als account-gebaseerd impliceert bijvoorbeeld dat er vervolgens nog wel een onderscheid tussen credit en debet gemaakt kan worden, maar niet tussen counter en coins.

2.3 Klassen

De knopen van de boom representeren klassen van methoden die we (theoretisch) kunnen benoemen. De bladeren representeren klassen van methoden die we niet verder opsplitsen omdat verschillen binnen deze klassen een kwestie van concrete implementatie zijn. Alle betaalmethoden zijn in deze laatste klassen in te delen. Hiermee is de eerste deelvraag van dit onderzoek beantwoord. In sectie 4 wordt verder ingegaan op de verdeling van de methoden over de klassen en hun eigenschappen.

3 Kwalificatie

Voor de tweede deelvraag richten we ons op de eisen die gesteld worden aan elektronische betaalmethoden en hoe de klassen van methoden die we hebben onderscheiden daar aan voldoen. Het is belangrijk om vast te stellen dat de eisen aan betaalmethoden niet eenduidig zijn. Een voor de hand liggend onderscheid is de hoeveelheid geld waar het om gaat. Soms gaat het om transacties van minder dan 1 euro, waarbij gemak, lage kosten en snelheid gewenst zijn, en soms gaat het om bedragen van meer dan 1000 euro, waarbij voornamelijk security belangrijk is. Wanneer we kijken naar kwalificaties van verschillende methoden hebben we dus ook te maken met trade-offs. Een ander voorbeeld daarvan is het aspect privacy versus traceability [12].

3.1 Securitydoelen

In de computer security worden verschillende securitydoelen onderscheiden waar een systeem aan moet voldoen. In deze sectie zullen we bekijken hoe securitydoelen betrekking hebben op betaalmethoden voor e-commerce. We moeten eerst vaststellen om welke doelen het gaat en wat ze precies inhouden.

Tanenbaum noemt in "Computer Networks" [29] de doelen confidentialiteit, authenticiteit, onloochenbaarheid (nonrepudiation) en integriteit. Bij confidentialiteit kan vervolgens een onderscheid gemaakt worden tussen confidentialiteit van de inhoud van een bericht (geheimhouding), en confidentialiteit van de bron van het bericht (anonimiteit) [2]. Authenticiteit heeft te maken met of een bericht te vertrouwen is. Authenticiteit van de partijen betekent dat deze kunnen bewijzen dat ze zijn wie ze zeggen. Authenticiteit van het bericht zelf betekent dat dat informatie over het bericht, zoals de bron en het tijdstip van verzenden, te vertrouwen is. Integriteit betekent dat bepaalde informatie niet veranderd kan worden. Dit betekent dat bijvoorbeeld een verzonden bericht onderweg niet veranderd kan worden. In het verlengde daarvan betekent onloochenbaarheid dat de ene partij kan bewijzen dat de andere partij een bepaalde actie heeft gedaan (bijvoorbeeld dat hij een heeft bestelling geplaatst) [29].

Daarnaast wordt beschikbaarheid (availability) ook vaak als securitydoel genoemd. Als bepaalde diensten niet beschikbaar zijn werkt het hele systeems immers überhaupt niet. Het doel in dit geval is voornamelijk om te voorkomen dat kwaadwillenden het gebruik van het systeem onmogelijk maken (bijvoorbeeld door denial-of-service aanvallen).

Hieronder beschrijven we hoe we deze securitydoelen opvatten in het kader van betaalmethoden. Wat zijn de specifieke eisen bij elektronische betalingen en hoe kan daaraan voldaan worden? Belangrijk is om hierbij onderscheid te maken tussen de verschillende partijen in het betaalmodel (figuur 1) en de verschillende communicatielijnen tussen die partijen.

3.1.1 Geheimhouding

Een voor de hand liggende eis is dat de informatie die betrokken is bij een transactie niet voor iedereen zichtbaar is. Deze bevat immers voornamelijk privacy-gevoelige informatie. Dit kan informatie zijn die te maken heeft met de betaalmethode zelf, zoals een creditcard nummer, maar ook informatie over de aankoop of de prijs kan privacy-gevoelig zijn. Hier moet onderscheid tussen gemaakt worden, want het is belangrijk om te overwegen hoe erg het is als de informatie uitlekt. Als het gaat om informatie waarmee iedereen die deze kent een betaling kan doen, dan is dit een ander soort probleem dan wanneer het gaat om persoonlijke informatie in combinatie met de inhoud van de transactie, wat in het ergste geval gebruikt kan worden voor bijvoorbeeld chantage.

Daarnaast zijn ook de persoonlijke gegevens (van met name de betaler) op zich privacy-gevoelig. Je naam, adres, telefoonnummer en e-mailadres moeten niet zo maar op straat komen te liggen.

In de praktijk blijkt het veilig verzenden van informatie op zich niet zo'n probleem. Er bestaan prima versleutelingsmethoden voor, zoals *Secure Sockets Layer* (SSL). Vaker gaat het mis als gegevens van klanten op de computer van de verkoper bewaard worden, en die computer later gehackt wordt [2]. Er moet dus gekeken worden naar alle plekken waar informatie verzonden en opgeslagen wordt. Ook is het interessant om te zien hoe informatie over transacties teruggekoppeld wordt naar de betaler (meestal ter controle). Gaat dit per post, per e-mail, of via een website en welke risico's zijn hier aan verbonden?

Een nog interessanter probleem ontstaat wanneer het doel is om geheim te houden dat er überhaupt een transactie heeft plaatsgevonden. Ook al wordt een boodschap versleuteld, hij is nog wel als versleutelde boodschap herkenbaar. Een transactie is als zodanig herkenbaar wanneer betaler en betaalde beide bekend zijn en aan elkaar verbonden kunnen worden.

Bij het aspect geheimhouding zullen we dus op de volgende punten letten:

- Wat is de aard van de informatie die al dan niet geheim wordt gehouden? Daarbij onderscheiden we in volgorde van belangrijk naar minder belangrijk (hoe ernstig zijn de gevolgen wanneer het niet geheim blijft): informatie waarmee betaald kan worden, de inhoud van de transactie in combinatie met persoonlijke informatie, de deelnemers aan de transactie, en persoonlijke informatie op zich.
- Waar wordt de informatie gecommuniceerd en opgeslagen en hoe is dit beveiligd? Zijn er mogelijke zwakke plekken?

Er moet hierbij opgemerkt worden dat we ons primair concentreren op geheimhouding vanuit het oogpunt van de betaler. Dit is misschien in het kader van volledigheid niet correct, maar we hebben ons enigszins moeten beperken om dit aspect niet te complex te maken.

3.1.2 Anonimiteit

Bij een betaling kan het gewenst zijn dat bepaalde partijen anoniem blijven. We kunnen echter verschillende gradaties van anonimiteit onderscheiden. De meest voor de hand liggende eis lijkt dat de betrokken partijen anoniem blijven ten opzichte van derde partijen. Dit zien we echter meer als een aspect van geheimhouding, en dit zal dus niet meegenomen worden in de beoordeling van anonimiteit.

In plaats daarvan is de vraag in hoeverre de partijen anoniem kunnen blijven ten opzichte van elkaar. Bij sommige betaalmethoden kunnen betaler en betaalde anoniem blijven ten opzichte van elkaar doordat de uitgever/ontvanger voor hun authenticiteit in staat. Ze kunnen naar de buitenwereld toe alleen bekend zijn onder een schuilnaam, omdat de uitgever/ontvanger weet dat er achter die schuilnaam een authentiek persoon zit. Het is daarmee alleen nog steeds mogelijk om verschillende betalingen van dezelfde persoon aan elkaar te koppelen, en ook dit kan een privacy-gevoelige kwestie zijn.

Het hoogste niveau van anonimiteit is de situatie zoals we die kennen bij contant geld, waar alle partijen anoniem zijn voor elkaar en verschillende betaling van dezelfde persoon niet aan elkaar verbonden kunnen worden. Bij de meeste elektronische betaalmethoden bestaat die mogelijkheid niet. Dit lijkt inherent te zijn aan account-based systemen, omdat een account gekoppeld is aan een persoon. Token-based systemen bieden hier misschien wel een mogelijkheid, omdat deze door het los koppelen van betaler en betaalmiddel wat dat betreft meer op contant geld lijken.

De vraag is echter of volledige anonimiteit gewenst is. Anonimiteit maakt het niet alleen moeilijker om fraude (bijvoorbeeld het dubbel uitgeven van tokens) te ontdekken, maar het biedt ook mogelijkheden voor allerlei criminele activiteiten zoals chantage of het witwassen van geld. Het is daarom misschien wenselijk dat de anonimiteit in geval van nood op te heffen is door een *trusted third party* [6].

Bij het aspect anonimiteit zullen we dus op de volgende punten letten:

- Welke informatie komen de verschillende partijen van elkaar te weten?
- Kunnen verschillende betalingen van dezelfde betaler aan elkaar gekoppeld worden?

3.1.3 Authenticiteit

Het doel van anonimiteit lijkt te conflicteren met dat van authenticiteit. Er lijkt sprake te zijn van een trade-off. Authenticiteit betekent het kunnen authenticeren van van de deelnemers aan de transactie en/of de betrokken betaalmiddelen. Authenticatie van personen is gebaseerd op één van de volgende drie aspecten: wat je weet (bijvoorbeeld een wachtwoord), wat je hebt (bijvoorbeeld een smartcard), of wat je bent (biometrie) [7]. Dit laatste aspect is op dit moment nog niet realistisch te gebruiken bij online betaalmethoden, maar de andere twee wel.

Als we kijken naar de positie van de betaler ten opzichte van de betaalde, dan is het creditcard systeem bijvoorbeeld geheel gebaseerd op het "wat je weet" aspect, want hoewel er sprake is van een fysieke kaart heb je alleen het nummer op de kaart nodig om te betalen. Een systeem als iDEAL is bijvoorbeeld gebaseerd op beide aspecten. De gebruiker moet een wachtwoord weten, en een mobiele telefoon of ander apparaat hebben om een code te kunnen krijgen.

Wat betreft de betaalde ten opzichte van de betaler spelen er andere overwegingen, met name als deze twee partijen niet gelijkwaardig zijn. Denk hierbij aan een consument die een webwinkel bezoekt. Deze consument zal zelf waarschijnlijk al snel een oordeel vormen over de authenticiteit van de webwinkel. Als het gaat om een bekend bedrijf zal hij dat bedrijf eerder zijn privacy-gevoelige informatie toevertrouwen dan bij een voor hem onbekende webwinkel. Tegenwoordig zijn er bovendien allerlei keurmerken, zoals het *thuiswinkel waarborg* [30] waaruit moet blijken dat webwinkels betrouwbaar zijn.

Een bekend risico van het beoordelen van authenticiteit op basis van een website is echter het fenomeen *phishing*, waarbij een website van als betrouwbaar bekend staand bedrijf nagemaakt wordt om aan consument gevoelige informatie te ontlokken.

Bij token-based systemen authenticeer je niet een persoon, maar een betaalmiddel (een token). Tokens kunnen bijvoorbeeld ondertekend worden met een cryptografische sleutel. Daarnaast kan bijvoorbeeld in een centrale database bijgehouden worden welke tokens nog geldig zijn, zodat tokens niet twee keer uitgegeven kunnen worden [26].

Bij het aspect authenticiteit zullen we dus op de volgende punten letten:

- Wat wordt er geauthenticeerd (betaler, betaalmiddel, betaalde, ontvanger, uitgever)?
- Hoe vindt authenticatie plaats (wat je hebt en/of wat je weet.)?
- Hoe erg zijn de gevolgen wanneer authenticatie ten onrechte plaatsvindt?

3.1.4 Integriteit

Integriteit kan betrekking hebben op veel verschillende zaken. Alle partijen in het systeem hebben allemaal *assets* die ze willen beschermen. Asokan et al. [3] stellen dat op een globaal niveau integriteit betekent dat er door geen van de partijen binnen het systeem nieuw geld wordt gecreëerd, en dat daarnaast iedere partij wil dat er geen geld van hem kan worden afgenomen zonder zijn toestemming. Dit is een complete maar niet makkelijk toepasbare definitie. De verdeling van geld kan namelijk op allerlei verschillende manieren onrechtmatig beïnvloed worden.

Je moet er bijvoorbeeld voor zorgen dat de bestelling die de betaler plaatst niet onderweg aangepast wordt door een derde partij. Dit is misschien niet de meest voor de hand liggende manier om te frauderen, maar een hacker zou de bestelling bijvoorbeeld zo kunnen aanpassen dat het product naar een ander adres verzonden wordt. In dat geval verliest de betaler geld, omdat hij het product niet ontvangt waar hij geld aan uit heeft gegeven.

Een ander voorbeeld is dat er binnen het systeem de mogelijkheid kan bestaan om een token meerdere keren uit te geven, zodat het lijkt alsof er uit het niets geld wordt gecreëerd. De uitgever zal uiteindelijk voor deze kosten moeten opdraaien, omdat wordt aangenomen dat hij de token heeft uitgegeven.

Een bedreiging voor de integriteit kan dus zowel van binnen als van buiten het systeem komen. Belangrijk is wel om op te merken dat een gebrek aan authenticiteit of geheimhouding een inbreuk op de integriteit tot gevolg kan hebben. Problemen die onder deze twee aspecten vallen zullen echter niet meegenomen worden in het oordeel over het aspect integriteit. In die zin is het aspect integriteit eigenlijk een soort restcategorie waaronder alle overgebleven securityproblemen vallen die ten koste kunnen gaan van de integriteit.

Bij het aspect integriteit zullen we dus op de volgende punten letten:

- Kan van buiten het systeem een partij invloed uitoefenen op de verdeling van geld?
- Kan een partij binnen het systeem de verdeling van geld onrechtmatig beïnvloeden, en zo ja, is dit makkelijk te detecteren?

3.1.5 Onloochenbaarheid

Het zeker stellen van integriteit en authenticiteit is met name voor de betaalde belangrijk, omdat dit een situatie van onloochenbaarheid (*nonrepudiation*) oplevert. De betaler kan niet ontkennen dat hij het was die die specifieke aankoop heeft gedaan en kan zijn geld niet terugeisen. Een eigenschap van creditcards is dat ze juist wel altijd een mogelijkheid bieden voor *repudiation*: een klant kan de transactie altijd annuleren bij zijn creditcard uitgever. Dit moet ook wel omdat het creditcard systeem technisch niet waterdicht is, zoals we later zullen zien. Wat het nastreven van onloochenbaarheid problematisch maakt is dat *repudiation* als een verworvenheid van de klant wordt gezien [2]. De klant krijgt bij een waterdicht systeem opeens meer verantwoordelijkheid, en dat lijkt niet gewenst. Dat zou kunnen betekenen dat een waterdicht systeem voor een aanbieder commercieel dus ook niet aantrekkelijk is.

Bij het aspect onloochenbaarheid zullen we dus op het volgende punt letten:

- Wat gebeurt er als de betaler beweert een betaling niet gedaan te hebben?

3.1.6 Beschikbaarheid

E-commerce is een 24-uurs economie, dus het is wenselijk dat het ook 24 uur per dag mogelijk is om te betalen. Bij veel betaalmethoden betekent dit dat een centrale server altijd online moet zijn. Een potentieel voordeel van offline betaalmethoden is dat ze hier niet van afhankelijk zijn.

Ook houden uitgevers en ontvangers zich over het algemeen het recht voor een betaler dan wel betaalde niet langer te bedienen wanneer er bijvoorbeeld verdenking is van fraude. Hier moet uiteraard wel zorgvuldig mee om worden gegaan. Wanneer gebruikers om het minste of geringste worden afgesloten is dit negatief voor de beschikbaarheid.

Bij het aspect beschikbaarheid zullen we op de volgende punten letten:

- Is het nodig dat een centraal deel van het systeem online is voor een transactie?
- Wat beweert de eigenaar van dit deel van het systeem over de beschikbaarheid ervan?
- Is er specifieke informatie bekend over of dit in de praktijk verschilt?
- Zijn er andere problemen bekend waardoor beschikbaarheid voor de betaler of betaalde tegen kan vallen?

Hierbij moet opgemerkt worden dat het niet mogelijk is om een precies in te schatten hoeveel procent van de tijd een systeem beschikbaar is. Een exacte vergelijking op dat punt is dus ook niet te geven.

4 Een overzicht van betaalmethoden

In deze sectie zullen we een overzicht geven van verschillende betaalmethoden die voldoen aan de basiseisen die gepresenteerd zijn in sectie 1.2. We zullen ons proberen te concentreren

op betaalmethoden die ook daadwerkelijk in de praktijk gebruikt worden. Bovendien zullen de geselecteerde betaalmethoden allemaal in te delen zijn in een verschillende klasse, volgens de definitie die we in sectie 2.3 gepresenteerd hebben.

Deze betaalmethoden zullen vervolgens in detail bekeken worden, en beoordeeld worden op de punten die besproken zijn in sectie 3.1. Voor de beoordeling zal gebruik gemaakt worden van de volgende schaal: - -, -, +/-, +, ++. Deze symbolen staan respectievelijk voor "slecht", "matig", "voldoende", "goed", en "zeer goed". Deze schaal zal gebruikt worden bij de aspecten "geheimhouding", "anonimiteit", "authenticiteit", "integriteit", en "beschikbaarheid". Bij het aspect "onloochenbaarheid" zal geen waardeoordeel gegeven worden omdat het wel of niet aanwezig zijn van onloochenbaarheid niet per se goed of slecht is. In plaats daarvan zal aangegeven worden in hoeverre onloochenbaarheid aanwezig bij de betreffende methode.

4.1 Creditcard

4.1.1 Beschrijving

Een van de populairste manieren om online te betalen is met behulp van een creditcard. Het creditcard systeem bestond al voordat e-commerce populair werd, en is dus niet speciaal ontworpen voor online betalingen. De basis van de transactie is dat de betaler zijn creditcard informatie naar de betaalde stuurt. De betaalde wordt echter vertegenwoordigd door een zogenaamde *Payment Gateway* [4]. Deze Payment Gateway stuurt de informatie naar de ontvanger (de bank waar de betaalde is aangesloten), die deze informatie weer authenticeert bij de uitgever.

Vervolgens kan de ontvanger het geld uitkeren aan de betaalde. Bij het creditcard systeem zijn de ontvanger en de uitgever over het algemeen verschillende partijen (banken of andere financiële instellingen), en vervult de creditcard maatschappij een overkoepelende rol bij het proces van *clearing*.

Dit systeem is van zichzelf behoorlijk onveilig. Het geheim waar alles op steunt (het creditcard nummer) moet immers rond gestuurd worden [7]. Het is duidelijk dat er een probleem ontstaat wanneer er niet voorzichtig wordt omgegaan met dit nummer. Iedereen die het nummer kent kan er immers mee betalen. Er zijn allerlei methoden bedacht om het systeem toch voldoende te beveiligen. De eenvoudigste en meest gebruikte methode is het gebruik van het *Secure Sockets Layer* protocol (SSL), een encryptiesysteem dat in de meeste webbrowsers ingebouwd zit. Hierdoor kan in ieder geval de geheimhouding en de integriteit van de informatie die tussen de browser van de betaler en de server van de betaalde verzonden wordt gegarandeerd worden.

In tabel 1 is te zien hoe het creditcard systeem is in te delen volgens de dimensies die we hebben gepresenteerd in sectie 2.1. Het creditcard systeem is account gebaseerd, aangezien het creditcard nummer gekoppeld is aan een persoon met een account bij de bank die de creditcard uitgeeft. Het gaat zoals de naam al zegt om een credit systeem. De betaalde kan eerst het geld van zijn bank krijgen, alvorens de bank van de betaler het bedrag weer verhaalt op de betaler.

Het systeem is in principe software gebaseerd, ook al komt er een fysieke kaart aan te pas. De kaart is uiteindelijk niet meer dan een nummer, en dus is hardware niet essentieel voor het protocol. Daarnaast wordt het creditcard systeem geclassificeerd als een online systeem, aangezien ontvanger en uitgever online moeten zijn om de betaling goed te keuren. Tot slot kunnen we vaststellen dat het creditcard zich vooral richt op grote bedragen, omdat er voor de betaalde behoorlijke kosten in rekening worden gebracht per transactie.

4.1.2 Kwalificatie

Geheimhouding

Aard van de informatie Bij een creditcard betaling op internet zijn privacy-gevoelige gegevens betrokken. In het algemeen gaat het om informatie over de kaart zelf (nummer, vervaldatum en eventueel een extra beveiligingscode). Deze informatie mag niet uitlekken, omdat iedereen die de informatie kent er mee kan betalen. Informatie over de kaarthouder die op de kaart staat (initialen en achternaam) is op zich niet vereist bij een betaling op internet, maar een webwinkel vraagt in principe wel altijd om een factuuradres. Dit factuuradres kan in sommige gevallen gebruikt worden om de betaler mee te authenticeren, maar dit is nog niet standaard [31].

Zo'n factuur koppelt typisch de inhoud van een transactie aan een naam, en dit is ook privacy-gevoelige informatie.

Bij een creditcard transactie op internet speelt dus de geheimhouding van: persoonlijke informatie, informatie waarmee betaald kan worden, informatie over de inhoud van de transactie in combinatie met de betaler, en informatie over tussen welke partijen er een transactie heeft plaatsgevonden.

Communicatie en opslag Hier boven schreven we al dat door middel van SSL de geheimhouding van de informatie die tussen de browser van de betaler en de server van de betaalde wordt wordt verzonden gegarandeerd wordt. Dit is echter maar één aspect. De vraag is ook wat de betaalde met de gegevens doet. Deze lopen namelijk het meeste kans om uit te lekken wanneer de betaalde de gegevens (tegen de instructies van de bank in) bewaart, en zijn systeem gehackt wordt [2]. Dit probleem geldt voor alle soorten informatie die hierboven genoemd zijn, maar de gevolgen zijn het ergst wanneer het gaat om informatie waarmee betaald kan worden.

Uiteraard kunnen dergelijke gegevens ook op klassieke manieren verkregen worden. De kaart zelf kan gestolen worden van de eigenaar of zelfs direct na uitgave uit de post gevist worden. Daarnaast is er nog een kans op *skimming*, waarbij de inhoud van de magneetstrip op de kaart gekopieerd wordt. Dergelijke problemen zijn dus niet nieuw. Het verschil is echter wel dat op internet een crimineel niet gelimiteerd is door fysieke aanwezigheid.

De informatie waarmee betaald kan worden, in combinatie met een bedrag, moet natuurlijk ook worden verzonden van de betaalde naar de ontvanger. Dit kan alleen via de hierboven genoemde Payment Gateway. Die zorgt dat ook deze communicatie veilig verloopt. Het komt er op neer dat ook hier SSL gebruikt wordt.

Over het algemeen krijgt de betaler van de uitgever van de kaart elke maand per post een overzicht van welke betalingen er zijn verricht, zodat deze gecontroleerd kunnen worden. Een geïnteresseerde derde partij zou deze gegevens dus kunnen achterhalen door in de post te snuffelen. Hetzelfde probleem geldt voor de factuur die de betaalde naar de betaler stuurt. Dit zien we echter als een niet zo heel realistisch scenario, en dit zal dus niet zo zwaar wegen.

Wel zwaarwegend is dat alle informatie die voor de betaler privacy-gevoelig is bij de betaalde terecht komt, en dat het niet te garanderen is dat deze daar zorgvuldig mee omgaat. We beoordelen we de geheimhouding daarom als *matig*.

Anonimiteit Een betaling met een creditcard biedt weinig anonimiteit voor de betaler. De betaalde, de Payment Gateway, en de ontvanger kennen sowieso het creditcard nummer, maar hoeven in principe niet de naam van de betaler te kennen. In de praktijk wordt er bij een betaling met een creditcard ook altijd om persoonlijke informatie gevraagd, zoals een factuuradres. Uiteraard is de betaler ook bij zijn eigen bank niet anoniem. We gaan er van uit dat de banken te vertrouwen zijn wat betreft hun omgang met deze informatie.

Dat de betaalde het creditcard nummer van de betaalde kent betekent automatisch ook dat hij kan zien dat verschillende betalingen van dezelfde persoon afkomstig zijn. In die zin is de betaler dus ook niet anoniem.

De andere partijen in dit systeem zijn niet anoniem, maar hier is een goede reden voor. De betaler moet immers de gegevens van de betaalde kennen om te kunnen beoordelen of hij betrouwbaar is. Een betaler is bij het creditcard systeem in principe altijd verbonden aan

een website en het is als het goed is altijd mogelijk om te achterhalen wie de eigenaar van een website is. Alle zakelijke informatie is dus normaal gesproken bekend voor een betaler. Dat de banken niet anoniem kunnen blijven is ook logisch, al hoeven betaler en betaalde van elkaar niet te weten aan welke bank ze verbonden zijn.

We beoordelen de anonimiteit kortom als *matig*.

Om geheimhouding en anonimiteit te verbeteren is er halverwege de jaren 90 een nieuw beveiligingsprotocol ontwikkeld, genaamd *Secure Electronic Transaction* (SET). Hierbij komt de betaalde nooit het creditcard nummer van de betaler te weten, en krijgt de bank nooit de exacte inhoud van de transactie te zien. Eén van de voorwaarden voor dit protocol was dat iedere betaler een *public key* certificaat had, en de benodigde infrastructuur hiervoor is nogal duur. In de praktijk bleek dat de voordelen niet opwogen tegen de nadelen, dus SET is nooit echt een succes geworden [2].

Authenticiteit

Authenticiteit van betaalmiddel en betaler De creditcard kent een lange historie van fraude, en een centraal punt daarbij is de authenticiteit van de kaart. De gegevens op de kaart moeten op één of andere manier gecontroleerd worden. Hiermee doe je eigenlijk twee dingen. Je controleert de authenticiteit van het betaalmiddel (is het een echt kaartnummer, uitgegeven door een legitieme financiële instelling), en de authenticiteit van de betaler (is dit de echte eigenaar van de kaart). Het eerste kan nagegaan worden bij de uitgever van de kaart. Het tweede is echter problematischer. Wanneer je in de winkel met een creditcard betaalt vraagt de winkelier bijvoorbeeld om een handtekening of een andere vorm van identificatie, maar op internet kan dit niet.

Het is simpelweg een feit dat creditcard gegevens gebruikt kunnen worden door iemand die niet de rechtmatige eigenaar van de kaart is. Dit is niet op te lossen met preventieve middelen, en daarom vertrouwt het creditcard systeem op detectie. Wanneer de eigenaar van een kaart bijvoorbeeld op zijn afschrift transacties ziet die hij niet gedaan kan hebben meldt hij dat bij zijn bank, waarna de betreffende kaart geblokkeerd kan worden. Omdat de kaart nu niet meer geldig is, wordt het probleem gereduceerd tot de authenticatie van het betaalmiddel zelf. De gevolgen van het niet kunnen authenticeren van de betaler zijn echter nog steeds dat de betaalde het geld weer gewoon terug moet geven.

Authenticiteit van betaler Een heel ander probleem is dat de betaler ook de betaalde op authenticiteit moet controleren. Of de betaalde te vertrouwen is is iets dat de betaalde zelf moet beoordelen [14]. De betaler loopt onder andere het risico slachtoffer te worden van *phishing*, waarbij een website zich voordoet als een andere, als betrouwbaar bekend staande, website. Het gevolg hiervan is dat de creditcard informatie niet langer geheim is. Een goede manier om dit te controleren is het het bekijken van het *public key* certificaat van de betaalde dat nodig is voor het SSL protocol.

Niet alleen in de communicatie tussen betaler en betaalde speelt authenticatie een rol. Het authenticeren van een creditcard nummer kan bijvoorbeeld niet door iedereen gedaan worden. Als iedereen zomaar contact kon leggen met een authenticatieserver, dan kon ook iedereen net zo lang creditcard nummers raden totdat er een keer een geldige tussen zat [2]. Een betaalde kan dus alleen een nummer laten authenticeren via een Payment Gateway, waar hij een account heeft [4].

Authenticiteit van uitgever/ontvanger Dit betekent in dit geval voor de betaalde authenticiteit van de Payment Gateway. De betaalde moet echter wel controleren of hij wel de authentieke Payment Gateway voor zich heeft. Er is een scenario denkbaar waarin een

[2] Er zijn op internet allerlei programmaatjes te vinden waarmee je een creditcard nummer kan verifiëren, maar die doen niet meer dan controleren of het laatste cijfer van het nummer een correcte checksum is van de rest van het nummer

aanvaller zich voordoet als Payment Gateway en zo de betaalde laat geloven dat een valse creditcard authentiek is. Dit lijkt echter geen realistisch scenario.

Wat het oordeel betreft is de doorslaggevende factor dat het normaal gesproken eigenlijk niet mogelijk is om de betaler te authenticeren. We beoordelen het aspect authenticiteit daarom als *matig*.

Integriteit We kunnen ons afvragen of het mogelijk is om binnen het creditcard systeem geld te creëren of te laten verdwijnen. In principe is dit de verantwoordelijkheid van de uitgever en de ontvanger, en die zorgen wel dat het geld dat bij de betaalde terecht komt ook verhaald wordt op de betaler. Dit lijkt dus geen probleem te zijn.

Vanuit de betaalde gezien is het belangrijk dat hij al het geld krijgt waar hij recht op heeft en vanuit de betaler is het essentieel dat er niet meer geld bij hem wordt afgeschreven dan waar hij toestemming voor heeft gegeven. De betaalde kan bijvoorbeeld een hoger bedrag opgeven aan de ontvanger dan hij met de betaler overeen is gekomen. De betaler moet daarom zelf goed in de gaten houden dat hij niet meer heeft betaald dan de bedoeling was.

Ook is er altijd een risico dat derde partijen, al is het maar voor de lol, transacties aanpassen. Dit wordt bij het creditcard systeem echter voorkomen door het gebruik van SSL. Er is dus alleen binnen het systeem een kans dat de integriteit wordt aangetast, en de kans op detectie daarvan is erg groot. Integriteit is dus niet perfect, maar normaal gesproken wel goed genoeg. We beoordelen dit aspect dus als *goed*.

Onloochenbaarheid Het creditcard systeem staat erom bekend dat betalers de mogelijkheid hebben om te ontkennen dat ze een bepaalde betaling gedaan hebben, waarna het bedrag dat de betaalde heeft ontvangen weer teruggeëist wordt door zijn bank [2]. Er is dus *geen* sprake van onloochenbaarheid. Het doel hiervan is om de betaler te beschermen tegen de gevolgen van fraude, als alternatief voor het beschermen tegen fraude op zich.

Er wordt dus een last van de schouders van de betaler afgenomen, maar die last komt te liggen bij de betaalde. Die moet nu extra goed oppassen dat hij geen frauduleuze transacties accepteert, anders is hij zijn geld kwijt. Bovendien bestaat er een risico dat een betaler zelf fraude pleegt door een betaling te ontkennen, terwijl hij bijvoorbeeld het product wel heeft ontvangen. In dit geval kan de betaalde weer aantonen dat hij het product toch echt naar het adres van de betaler heeft gestuurd, maar doordat veel transacties tegenwoordig internationaal zijn kan het lastig zijn voor de betaler om zulke conflicten succesvol op te lossen [2].

Beschikbaarheid In theorie moet je 24 uur per dag met je creditcard kunnen betalen. De grote creditcard maatschappijen opereren wereldwijd, en als hun systemen niet beschikbaar zijn hebben heel veel mensen daar last van. Problemen met deze systemen lijken niet veel voor te komen. De beschikbaarheid hangt echter ook af van de banken die er bij betrokken zijn, en dit kan per bank natuurlijk sterk verschillen. Over het algemeen zijn er echter geen specifieke problemen qua beschikbaarheid bij creditcard systemen, dus we beoordelen dit aspect als *goed*.

4.2 PayPal

4.2.1 Beschrijving

PayPal is geen op zichzelf staand systeem, maar is gebaseerd op bestaande infrastructuur van creditcard maatschappijen en banken [18]. Het is een initiatief van eBay dat in 1998 gestart is en inmiddels meer dan 100 miljoen gebruikersaccounts heeft.

PayPal biedt verschillende manieren om geld te betalen en te ontvangen. Elke gebruiker heeft een soort bankrekening waarop hij geld kan ontvangen van een andere gebruiker met een PayPal account. De betaler kan het geld direct betalen met een creditcard, of met

Methode	Creditcard	Paypal	iDEAL	Wallie
Account vs Token	Account	Account	Account	Token
Credit vs Debet	Credit	Debet	Debet	
Counter vs Coins				Counter
On- vs Offline	Online	Online	Online	Online
Hard- vs Software	Sofware	Software	Hardware	Software
Grootte van betaling	Groot	Groot	Groot	Klein
Geheimhouding	-	+	+/-	-
Anonimiteit	-	+	-	+
Authenticiteit	-	-	+	+/-
Integriteit	+	+	++	+
Onloochenbaarheid	Geen	Deels	Volledig	Volledig
Beschikbaarheid	+	+/-	+/-	+

Tabel 1: Classificatie en kwalificatie van de betaalmethoden

zijn PayPal account zelf, waar hij eerst vanaf een andere bankrekening geld naar heeft overgemaakt. De betaalde kan vervolgens het geld weer van zijn PayPal rekening op een andere rekening laten storten [10].

In tabel 1 is te zien hoe PayPal is in te delen. Het is duidelijk dat PayPal een account gebaseerd systeem is. De identiteit van de gebruiker, die aan een account gekoppeld is, wordt door PayPal op authenticiteit gecontroleerd, zoals hieronder verder wordt uitgelegd. Hierop is de security van het systeem grotendeels gebaseerd. Omdat PayPal methoden van creditcards en banken combineert is het niet direct voor de hand liggend om een onderscheid te maken tussen credit en debet. PayPal zelf biedt echter geen kredietsysteem, en is wat dit aspect betreft volledig afhankelijk van creditcard maatschappijen. Het bedrijf lijkt wat dat betreft veel op een bank. Als we alleen kijken naar de functie van PayPal zelf, dan kan het het best als debet geclassificeerd worden.

Het systeem is verder geheel softwarematig en online. Bij elke transactie wordt de betaler naar de site van PayPal geleid. Deze moet dus online zijn om het systeem te laten werken.

Wat betreft de grootte van betalingen geeft PayPal geen limiet aan wanneer alle authenticatiestappen zijn doorlopen (je moet je account eerst upgraden voor “uitgebreid gebruik”). PayPal lijkt minder geschikt voor het betalen van kleine bedragen, omdat er per transactie een vast bedrag van 35 eurocent in rekening wordt gebracht [23].

4.2.2 Kwalificatie

Geheimhouding

Aard van de informatie Informatie waarmee betaald kan worden betekent in het geval van PayPal een combinatie van e-mailadres en wachtwoord, die toegang geeft tot een PayPal account. Deze informatie is zelf geen onderdeel van een transactie. De persoonlijke informatie die betrokken is bij een transactie is ook beperkt. Het gaat hierbij alleen om een gebruikersnaam en een e-mailadres (zie het aspect anonimiteit). Dit betekent dat een transactie door een buitenstaander niet direct aan een persoon te verbinden is. Er komt bij PayPal dus eigenlijk geen gevoelige informatie over de betaler bij de betaalde terecht.

Deze persoonlijke informatie is natuurlijk echter wel bekend bij PayPal zelf.

Communicatie en opslag Volgens PayPal is de geheimhouding van de persoonlijke en financiële gegevens van de gebruiker één van hun belangrijkste prioriteiten. Verzonden gegevens worden beveiligd met SSL met een coderingssleutel van 128 bits, en PayPal claimt dat ook hun servers in de VS zowel elektronisch als fysiek streng beveiligd zijn [20].

Hiermee zijn echter niet alle wegen afgesloten waarmee een derde partij aan informatie over een transactie zou kunnen komen. Ten eerste wordt bij elke betaling ter bevestiging een e-mail gestuurd naar de betrokken partijen. In het bericht dat de betaler ontvangt staan zijn persoonlijke gegevens (naam en adres), en daarnaast het e-mailadres van de betaalde en de grootte van het bedrag. Het achterhalen van iemands betalingsgedrag is in de praktijk zo moeilijk als het lezen van zijn e-mail.

Op de website van PayPal wordt van een gebruiker ook de volledige transactiegeschiedenis bijgehouden. Dit betekent dat al deze informatie in de praktijk alleen beschermd wordt door het wachtwoord van het gebruikersaccount. Dit wachtwoord is, zoals gezegd, ook gelijk de informatie waarmee betaald kan worden. De geheimhouding hiervan is uiteraard de verantwoordelijkheid van de gebruiker zelf.

Voor PayPal pleit dat, vanwege de mogelijkheid tot anonimiteit van de betaalde, de precieze deelnemers aan de transactie geheim kunnen blijven. Persoonlijke informatie en informatie over de inhoud van de transactie zijn wel te achterhalen, maar hiervoor moet de e-mail van de betaler gelezen worden. Daarom beoordelen het aspect geheimhouding als *goed*.

Anonimiteit PayPal biedt gedeeltelijke anonimiteit aan voor zijn gebruikers. Volgens de gebruikersovereenkomst hebben de betaler en de betaalde alleen zicht op elkaars gebruikersnaam, e-mailadres en optionele andere contactinformatie, zoals een telefoonnummer [22]. Hierdoor kunnen dus de echte naam en de financiële informatie van een gebruiker geheim blijven. PayPal is dus in zoverre anoniem dat verschillende betalingen van dezelfde persoon wel aan elkaar verbonden kunnen worden, maar dat gebruikersinformatie niet zomaar teruggevoerd kan worden op een persoon.

De vraag is echter nog wel welke informatie PayPal zelf allemaal kent en wat hier verder mee gebeurt. De minimale informatie die PayPal wil hebben is naam, adres, telefoonnummer en e-mailadres, om te kunnen betalen zijn gegevens over creditcard of bankrekening vereist, en als het om hoge bedragen gaat ook een SOFI-nummer. Als “aanvullende controle” kan PayPal de gebruiker ook vragen bijvoorbeeld een kopie van zijn rijbewijs te faxen.

In de gebruikersovereenkomst geeft PayPal een lijst van partijen waaraan informatie over gebruikers en rekeningen verstrekt kan worden. De aard van deze partijen loopt uiteen van politie- en veiligheidsdiensten en kredietbureaus tot bedrijven die PayPal ondersteunen bij de marketing aan zijn eigen klanten. De lijst met voorbeelden die per categorie gegeven wordt is bovendien “niet-limitatief”. Hier zullen we PayPal echter niet op beoordelen, omdat het niet duidelijk is hoe dit zich verhoudt tot banken en creditcard maatschappijen.

PayPal biedt dus meer anonimiteit voor met name de betaler ten opzichte van de betaalde dan bijvoorbeeld creditcardsystemen, en dit kan zeker voordelen hebben, dus we beoordelen de anonimiteit als *goed*.

Authenticiteit

Authenticiteit van betaler Een gebruiker kan toegang krijgen tot zijn PayPal account door een combinatie van een e-mailadres en wachtwoord in te voeren. Die authenticatie is dus gebaseerd op “wat je weet”. Als de gebruiker zijn wachtwoord niet meer weet kan hij een bericht naar zijn e-mailadres laten versturen met daarin een link naar een pagina waarop hij twee “beveiligingsvragen” moet beantwoorden. Een voorbeeld van zo’n vraag is: “Wat is de geboorteplaats van uw vader?”. Een derde partij kan redelijkerwijs achter de antwoorden op deze vragen komen, en heeft dan vervolgens aan toegang tot het e-mail account genoeg om toegang tot PayPal te krijgen.

Deze vorm van authenticatie is niet bijzonder sterk, maar hoe groot zijn de gevolgen als een aanvaller toegang krijgt tot een PayPal account dat niet van hem is? Ten eerste kan hij het geld dat op dat moment op de PayPal rekening staat overmaken naar iedere andere PayPal rekening of bankrekening. Ten tweede kan hij een creditcard gebruiken die aan de

rekening is verbonden om geld naar een andere PayPal rekening sturen. Hij hoeft hier verder geen informatie over die creditcard voor te kennen of extra handelingen voor te verrichten. De gevolgen voor de rechtmatige eigenaar van het account kunnen dus vrij dramatisch zijn. PayPal stelt dat de gebruikers zelf verantwoordelijk is voor het geheimhouden van zijn wachtwoord [22]. De gebruiker kan wel aankloppen bij PayPal [21], maar het is niet duidelijk of hij dan een poot heeft om op te staan. Als er gebruik is gemaakt van zijn creditcard kan hij wel zijn geld terug laten storten via zijn bank.

Authenticiteit van uitgever/ontvanger Een ander aspect dat van belang is, is de authenticatie van PayPal ten opzichte van de gebruiker. De betaalde kan op zijn website een link zetten waar de betaler op kan klikken, waardoor hij naar een webpagina van PayPal geleid wordt. Op deze pagina moet de betaler nu zijn e-mailadres en wachtwoord invullen zodat hij de betaling kan voltooien. Dit betekent dat de betaler zelf moet controleren of hij wel echt op een pagina van PayPal zit en niet het slachtoffer dreigt te worden van *phishing*. De betaalde zou op vrij subtiele manier aan het wachtwoord van de betaler kunnen komen, door de betaler eerst zijn wachtwoord in te laten vullen op een pagina van hemzelf, waarna hij zelf de gegevens doorgeeft aan de echte website, zodat de betaler alsnog zijn betaling kan uitvoeren en niet vermoedt dat er iets mis is.

Authenticiteit van betaalde De authenticatie van de betaalde ten opzichte van de betaler gebeurt door naar de gegevens te kijken die de gebruikers van elkaar kunnen zien. De betaler zal aan de hand van het e-mailadres van de betaler moeten beoordelen of hij de goede voor zich heeft. Om het hem makkelijk te maken staat er bij bedrijven ook het adres van de website bij vermeld.

We kunnen concluderen dat het aspect authenticiteit bij PayPal nogal problematisch is. Eigenlijk zou je een betere beveiliging verwachten bij een systeem waar zo veel geld in omgaat. We beoordelen het aspect authenticiteit daarom als *matig*.

Integriteit Zoals we al schreven bij het aspect geheimhouding lijkt PayPal zijn eigen systemen wel goed beveiligd te hebben. Dankzij versleuteling kunnen betalingsopdrachten niet zomaar onderweg aangepast worden, en het hacken van de databases van PayPal lijkt ook zeker geen makkelijke opgave.

Ook binnen het systeem kan de integriteit niet aangetast worden. De betaler kan zelf zien hoe veel geld hij overmaakt naar de betaler en PayPal zorgt dat precies dit bedrag ook wordt overgemaakt. We beoordelen de integriteit daarom als *goed*.

Onloochenbaarheid PayPal kent geen absolute onloochenbaarheid. Een betaler kan claimen dat bepaalde betaling niet door hem is "geautoriseerd" [21], waarna PayPal een onderzoek instelt dat binnen tien dagen afgerond wordt. Het volledige bedrag kan dan eventueel teruggestort worden. In welke gevallen de claim van een betaler gehonoreerd wordt is niet geheel duidelijk. De gebruiker is bijvoorbeeld zelf verantwoordelijk voor het wachtwoord dat toegang biedt tot zijn account [22], dus als hij per ongeluk zijn wachtwoord aan een ander bekend maakt zal dat niet genoeg zijn voor een succesvolle claim.

Wat ook interessant is, is dat gebruikers bij PayPal kunnen claimen dat ze in ruil voor hun betaling geen juist (fysiek) product hebben ontvangen, en dat PayPal in deze situaties als bemiddelaar functioneert. De betaalde moet dan bewijzen dat het product wel degelijk correct verzonden is [19].

Terwijl een dergelijk geschil loopt wordt het omstreden bedrag bij de betaalde ingehouden, zodat hij het niet kan opnemen. PayPal garandeert echter niet dat de betaler zijn geld terug krijgt.

PayPal heeft dus een interessant beleid wat betreft wat betreft onloochenbaarheid. Er is geen sprake van absolute onloochenbaarheid, maar de betaler kan ook niet zomaar zijn

geld terugkrijgen. PayPal kiest voor de weg van bemiddeling. We beoordelen het aspect onloochenbaarheid daarom als *deels*.

Als de betaler gebruik heeft gemaakt van een creditcard kan hij nog wel op dit systeem terug vallen en zo zijn geld laten terugboeken, maar dit is geen eigenschap van PayPal zelf en wordt dus niet meegenomen in de beoordeling.

Beschikbaarheid PayPal is, als wereldwijde organisatie, in principe 24 uur per dag beschikbaar. Dit betekent echter niet dat gebruikers er van uit kunnen gaan dat ze altijd gebruik kunnen maken van hun account. PayPal heeft de reputatie gekregen dat ze bij het minste of geringste een account van een gebruiker bevriezen om eventuele fraude te voorkomen. Uit de website van PayPal zelf blijkt al dat ze dit bijvoorbeeld doen wanneer er "misbruik" wordt gemaakt van het terugboekmogelijkheid van creditcard instanties, of wanneer er niet correct wordt gehandeld in het geval van een geschil. Hier kan ook misbruik van worden gemaakt door kwaadwillenden, want je haalt een verkoper heel wat gedoe op de hals door een claim in te dienen.

Ook zijn er gevallen bekend waarbij een account werd bevroren omdat er in het kader van een geldinzamelingsactie in korte tijd veel geld naar toe stroomde [36]. Tot voor kort had PayPal niet de status van bank, zodat gebruikers geen klacht in konden dienen over dit soort zaken bij een regulerende instantie. Echter, sinds kort heeft PayPal in de EU wel de status van bank gekregen [35].

Normaliter is de beschikbaarheid van PayPal dus goed, maar in bijzondere situaties is de beschikbaarheid misschien minder dan verwacht mag worden. We beoordelen de beschikbaarheid daarom als *voldoende*.

4.3 iDEAL

4.3.1 Beschrijving

Net als PayPal is ook iDEAL geen op zichzelf staand systeem, maar is het gebaseerd op de bestaande systemen voor internetbankieren van de eraan deelnemende banken (ABN AMRO, Rabobank, Postbank, ING, Fortis en SNS) [13].

Het principe van iDEAL is dat de consument op de website van de webwinkel zijn eigen bank kiest en vervolgens met één klik naar de website van die bank wordt geleid, zodat hij daar in kan loggen en direct de betaling kan voldoen. Als de betaler genoeg geld op zijn rekening heeft kan de bank vervolgens voor de winkelier garant staan voor het bedrag, en kan de winkelier dus direct overgaan tot levering van het product.

In tabel 1 is te zien hoe iDEAL is in te delen. Omdat het systeem uit gaat van een bankrekening van de betaler is het duidelijk dat het gaat om een account gebaseerd systeem. Omdat de betaler een positief saldo moet hebben om de transactie door te laten gaan wordt het systeem ingedeeld als debet-gebaseerd.

De vraag of iDEAL hardware gebaseerd is is een interessante. De deelnemende banken bieden namelijk uiteenlopende betaalmethoden aan. De overeenkomst is echter, dat er bij allemaal wel een stuk hardware nodig is. Bij de Rabobank gaat het bijvoorbeeld om een *Random Reader*, een apparaatje waar de betaler zijn pinpas instopt, en dat na invoering van de bijbehorende pincode codes genereert waarmee ingelogd kan worden en waarmee betalingen ondertekend kunnen worden [25]. De meeste andere banken hebben een vergelijkbaar systeem. De Postbank vereist ook dat gebruikers de betaling ondertekenen, maar de benodigde codes worden in een SMS-bericht naar de mobiele telefoon van de gebruiker gestuurd, of kunnen van een papieren lijst gehaald worden die de gebruiker van tevoren heeft besteld [24]. Ook deze middelen kunnen onder hardware gerekend worden.

Daarnaast is het duidelijk dat het gaat om een online systeem, omdat een derde partij (de bank) online moet zijn om de transactie uit te voeren.

Wat de grootte van de betaling betreft lijkt iDEAL zich niet te richten op kleine betalingen, aangezien de betaling, gezien vanuit de betaler behoorlijk complex is, en de kosten

per transactie voor de betaalde vrij hoog zijn (50 tot 80 eurocent). Een maximumbedrag dat betaald kan worden geeft iDEAL niet aan, dus deze betaalmethode is duidelijk gericht op grote bedragen.

4.3.2 Kwalificatie

Geheimhouding

Aard van de informatie Geheimhouding van informatie waarmee betaald kan worden is bij iDEAL geen issue, aangezien er bij authenticatie een "wat je hebt" aspect betrokken is, en alleen informatie dus niet genoeg is om mee te kunnen betalen.

Wat de rest van de informatie betreft lijkt iDEAL op het creditcard systeem. Persoonlijke informatie van de betaler komt bij de betaalde terecht, aangezien de betaler in het systeem bekend staat onder zijn echte naam, en er bovendien over het algemeen een factuuradres vereist wordt door de betaalde. Hierdoor is het afhankelijk van de betaalde of deze persoonlijke informatie, mogelijk in combinatie met de inhoud van de transactie, goed beveiligd is.

Communicatie en opslag De geheimhouding van een transactie bij iDEAL is in principe hetzelfde als bij een normale overschrijving via internet, en dus niet perfect. Als we bijvoorbeeld kijken naar de iDEAL implementatie van de Postbank, dan laat een transactie op allerlei plekken zijn sporen na. De betaler krijgt bijvoorbeeld een SMS-bericht waarin het te betalen bedrag (als controlemiddel) vermeld staat. Daarnaast zijn er natuurlijk de ouderwetse bankafschriften die misschien door de verkeerde mensen gelezen kunnen worden.

Dit betekent natuurlijk wel dat een geïnteresseerde derde partij fysiek in de buurt moet van zijn doelwit om bijvoorbeeld in zijn post te kunnen snuffelen, en dat beperkt zijn mogelijkheden behoorlijk. Er bestaat geen groot risico dat een transactie via internet afgeluisterd wordt, omdat ook iDEAL gebruik maakt van SSL. Wel hebben we in het geval van de Postbank te maken met een SMS-bericht waarvan de geheimhouding niet gegarandeerd wordt. Hierdoor zijn er opeens allerlei andere partijen betrokken, zoals de eigenaar van het telefoonnetwerk en de provider.

De andere banken die iDEAL aanbieden kiezen niet voor het gebruik van SMS, dus aan de geheimhouding van iDEAL op zich doet dit niet zo veel af. Wel hebben we vastgesteld dat persoonlijke informatie bij de betaalde bekend is, en dat dit risico's op kan leveren. Persoonlijke informatie weegt echter niet zo zwaar als informatie waarmee betaald kan worden. We beoordelen de geheimhouding van iDEAL daarom als *voldoende*.

Anonimiteit Bij iDEAL is er slechts beperkt sprake van anonimiteit. Een gebruiker van iDEAL wordt in het systeem gerepresenteerd door een bankrekening. In de praktijk betekent dit een naam en een rekeningnummer. Deze naam moet in principe een echte naam van een persoon of bedrijf zijn. Gebruikers kunnen dus niet deelnemen onder een schuilnaam. Wanneer er een transactie plaatsvindt kunnen zowel de betaler als de betaalde van elkaar de naam zien. Daarnaast zijn deze partijen uiteraard ook ten opzichte van de bank niet anoniem. Ook bestaat er dus de mogelijkheid om verschillende betalingen van dezelfde persoon aan elkaar te koppelen.

De deelnemende banken kunnen vanzelfsprekend ook niet anoniem zijn, al hoeven betaler en betaalde van elkaar niet te weten via welke bank ze deelnemen aan iDEAL.

Over het algemeen genomen lijkt anonimiteit bij iDEAL geen prioriteit te zijn, en dit aspect wordt dan ook met *matig* beoordeeld.

Authenticiteit

Authenticiteit van de betaler Bij iDEAL controleert de bank de authenticiteit van de betaler met een combinatie van "wat je hebt" en "wat je weet", zoals al behandeld is in de beschrijving. Bij alle implementaties lijkt dit een zeer solide systeem, dus hier zullen geen authenticatieproblemen plaatsvinden.

Authenticiteit van de betaalde Interessanter is hoe de betaler de authenticiteit van de betaalde controleert. De betaler moet zelf controleren dat degene waar hij geld naar verzendt dezelfde is als degene op wiens website hij zojuist op een link heeft geklikt, door bij het bevestigen van de betaling naar de naam van de begunstigde te kijken. Er bestaat altijd een risico dat de betaler door een aanvaller zo geleid is dat de betaling nu naar een andere persoon gaat. In principe is dit bij iDEAL goed geregeld, omdat de betaler de naam van de betaalde krijgt te zien terwijl hij op de website van zijn bank zit. De betaalde moet dus echt onder die naam geregistreerd staan.

Authenticiteit van de uitgever/ontvanger Een andere reden voor een aanvaller om de betaler naar een andere pagina te leiden kan zijn om hem door middel van *phishing* zijn wachtwoord te ontfutselen. Dit heeft vervolgens weer te maken met de authenticatie van de bank ten opzichte van de betaler, en we hebben gezien dat met alleen het wachtwoord van een rekening de aanvaller nog geen betalingen in naam van zijn slachtoffer kan uitvoeren, dus de schade blijft hierbij beperkt.

We hebben vastgesteld dat de authenticatie van de betaler ten opzichte van de bank uitstekend is, en dat er bij andere vormen van authenticatie weliswaar wat mogelijke problemen zijn, maar dat de betaler die kan voorkomen door gewoon goed op te letten. Daarom beoordelen we de authenticatie als *goed*.

Integriteit Zoals al genoemd bij geheimhouding heeft de Postbank bijvoorbeeld een mechanisme waarbij de betaler een SMS-bericht krijgt met het te betalen bedrag. Hiermee kan gecontroleerd worden dat de betaler ook echt het bedrag betaalt dat hij heeft toegezegd te betalen. Dit is goed voorbeeld van een mechanisme waarmee iDEAL integriteit wil garanderen (zoals we hier boven gezien hebben gaat dit wel weer ten koste van de geheimhouding). Daarnaast is iDEAL natuurlijk gebaseerd op bestaande systemen van banken, die er op ingesteld zijn om het te detecteren als er uit het niets geld gecreëerd wordt of verdwijnt. We beoordelen de integriteit daarom als *zeer goed*.

Onloochenbaarheid iDEAL gaat net als internetbankieren en ouderwetse overschrijvingen uit van onloochenbaarheid. De betaler is in principe altijd verantwoordelijk voor elke overschrijving vanaf zijn account. Een betaling is niet terug te draaien [13]. Er is bij iDEAL dus sprake van *volledige* onloochenbaarheid.

Beschikbaarheid iDEAL zou in principe altijd beschikbaar moeten zijn, maar het kan zijn dat een bank bijvoorbeeld incidenteel onderhoud pleegt aan zijn internetbankiersysteem [24], of dat er een technische storing ontstaat. Hoe vaak een dergelijk incident voorkomt verschilt natuurlijk per bank, maar de beschikbaarheid van de Postbank is problematisch gebleken, met 16 storingen binnen drie maanden. [8]. Omdat dit probleem niet voor alle banken geldt is een negatief over iDEAL als geheel niet gerechtvaardigd, maar iDEAL springt er ook zeker niet in positieve zin uit. We beoordelen de beschikbaarheid daarom als *voldoende*.

4.4 Wallie

4.4.1 Beschrijving

Een heel ander soort betaalmethode is Wallie [32]. Het principe van Wallie is dat de consument in een gewone winkel een kaart koopt met daarop een code. Deze code representeert

een waarde van 5, 10, 20, of 50 euro. De consument kan nu bij een webwinkel betalen door simpelweg deze code in te voeren. In de praktijk betekent dit dat de winkelier de consument doorverwijst naar de website van Wallie zelf, zodat Wallie kan bijhouden hoeveel saldo de desbetreffende code nog representeert.

In tabel 1 is te zien hoe Wallie is in te delen. In tegenstelling tot de hierboven besproken methoden is een betaling via Wallie niet verbonden aan een account. Het enige dat je nodig hebt is een kaart/code, oftewel een token. Het gaat hier dus om een token-gebaseerd systeem. Er valt wel een kanttekening te plaatsen bij deze indeling omdat je het ook zo kunt bekijken dat iedere Wallie kaart zelf een account voorstelt. Volgens de definitie van account die wij hanteren (een account is verbonden aan een persoon) ligt dit echter minder voor de hand. Binnen de token-gebaseerde systemen is nog een onderscheid te maken tussen counter en coins. De tokens bij wallie werken met een counter. Je kunt met één token meerdere betalingen doen.

Het Wallie-systeem maakt weliswaar gebruik van een fysiek artikel, maar een transactie kan ook uitgevoerd worden zonder dit artikel. Uiteindelijk gaat het namelijk alleen om een code. Daarom wordt Wallie toch geclassificeerd als een software systeem. Net als bij de andere methoden moet er een derde partij online zijn om de betaling goed te keuren. Het gaat dus om een online-systeem.

Tot slot kunnen we vaststellen dat Wallie zich, in tegenstelling tot de andere methoden, vooral richt op kleine betalingen. Er bestaat een betalingslimiet van 150 euro (en hiervoor zijn zelfs meerdere kaarten nodig), en het doel van Wallie lijkt vooral te zijn dat de betaling snel en makkelijk gaat.

4.4.2 Kwalificatie

Geheimhouding

Aard van de informatie Wat betreft geheimhouding heeft Wallie als voordeel dat een Wallie-card niet verbonden is aan een persoon, en dat er dus geen persoonlijke gegevens in het spel zijn. De enige informatie die geheim gehouden moet worden is de Wallie-code, oftewel de informatie waarmee betaald kan worden. De geheimhouding hiervan is zeker niet gegarandeerd.

Communicatie en opslag Wanneer de betaler een Wallie-card in de winkel koopt dan kan dat op twee manieren. Of hij krijgt een kaart met een kraslaag waaronder de code verborgen is, of hij krijgt een zogenaamde “e-voucher”; een bon die bij de kassa wordt uitgeprint. Hoe dit precies beveiligd is, is niet duidelijk. Het lijkt erop dat de winkel de code in principe gewoon zou kunnen kopiëren. Als een winkel die bij Wallie is aangesloten fraude pleegt valt dit natuurlijk wel erg op, dus heel realistisch is dit scenario niet.

Het volgende probleem ontstaat echter wanneer de betaler zijn saldo wil besteden. De manier waarop de code tussen de betaler, de betaalde, en Wallie gecommuniceerd wordt lijkt niet zo goed beveiligd te zijn. Wallie claimt dat een betaler het systeem in twee tot vier uur aan de praat kan krijgen [34], en dit lijkt niet zo gek, omdat het gaat om niets meer dan een HTML formulier. De betaalde is niet verplicht om iets als SSL te gebruiken. Natuurlijk betekent dit niet dat dit in de praktijk niet gedaan wordt.

Niet alleen de betaalde kan dus de code bekijken, maar voor een derde partij lijkt dit ook geen onmogelijke opgave. Ondanks dat er relatief weinig geld op het spel staat valt de geheimhouding van Wallie dus enigszins tegen, en we beoordelen dit aspect dan ook als *matig*.

Anonimiteit Bij Wallie is de betaler in principe volledig anoniem voor zowel de betaalde als voor Wallie. De enige situatie waarin een gebruiker zijn persoonlijke gegevens moet opgeven, is wanneer hij zijn kaart in wil ruilen voor geld bij Wallie zelf. Hij moet hiervoor

deze gegevens, inclusief de Wallie code in kwestie naar Wallie communiceren (schriftelijk of per e-mail [33]). Als de Wallie-card eerder gebruikt is kan Wallie op dat moment dus zien wat de gebruiker gekocht heeft.

De betaalde kan bij Wallie niet anoniem blijven, omdat de betaler zelf moet kunnen beoordelen of deze te vertrouwen is.

Verder kunnen verschillende aankopen die met dezelfde kaart zijn gedaan wel aan elkaar gekoppeld worden (zowel door de betaalde als door Wallie), maar als de betaler dit wil voorkomen kan hij natuurlijk ook meerdere kaarten gebruiken. De anonimiteit is bij Wallie dus zeker geen groot probleem, en we beoordelen dit aspect dan ook als *goed*.

Authenticiteit

Authenticiteit van het betaalmiddel Bij Wallie kan de betaalde niet de authenticiteit van de betaler vaststellen maar alleen van het betaalmiddel. Dit proces van authenticatie wordt echter uitbesteed aan Wallie zelf. De betaalde stuurt simpelweg de code door naar Wallie, en Wallie geeft aan of het gaat om een authentieke Wallie-card. Als deze authenticatie niet goed gaat wordt er misschien betaald met een kaart die nooit uitgegeven is, en gaat het Wallie geld kosten.

Authenticiteit van de uitgever/ontvanger Wanneer de betaler een kaart koopt doet hij er goed aan om dit alleen te doen in een winkel die aangesloten is bij Wallie. Als hij bijvoorbeeld een kaart tweedehands koopt kan het zijn dat deze vervalst is, en dus geen waarde heeft. Wallie staat wederverkoop dan ook niet toe [33]. Omdat dit een fysieke handeling is, is authenticatie hier bij uizondering gebaseerd het aspect “wat je bent”.

Authenticiteit van de betaalde Vervolgens moet de betaler wanneer hij wil gaan betalen de authenticiteit van de betaalde vaststellen. Ook bij deze methode is er namelijk weer een risico op *phishing*. Wallie probeert dit te voorkomen door de betaler zelf een bevestiging van een geslaagde betaling op zijn scherm te laten zien. De gebruiker moet echter ook controleren of dit bericht wel van Wallie is. Er is dus tegelijkertijd ook sprake van authenticatie van de uitgever/ontvanger.

Tot slot moet Wallie ook nog de authenticiteit van de betaalde vaststellen, want niet iedereen kan zomaar gebruik maken van de authenticatieservice van Wallie. Als dat het geval was kon je immers zelf codes raden totdat je een goede te pakken had. Wallie authenticeert de betaalde met behulp van een MerchantID, die de betaalde naar Wallie stuurt. Hier lijkt een zwakte te zitten. Als je de MerchantID van een gebruiker van Wallie weet te achterhalen kan je in zijn naam authenticatieverzoeken naar Wallie sturen.

De authenticiteit wordt bij Wallie dus op een eenvoudige, maar over het algemeen effectieve manier gecontroleerd. De zwakte zit waarschijnlijk in de authenticatie van de betaalde door Wallie. Het is echter niet helemaal duidelijk hoe makkelijk het is om een MerchantID te achterhalen, en wat vervolgens de gevolgen zijn. We beoordelen het aspect authenticiteit daarom nog steeds als *voldoende*.

Integriteit Bij het aspect integriteit kijken we onder andere of het mogelijk is om binnen het systeem geld te creëren of te laten verdwijnen. Dit is waarschijnlijk alleen mogelijk door de systemen van Wallie te hacken en de gegevens over welke codes wel en niet uitgegeven zijn te manipuleren, dus dit is niet erg realistisch.

Verder betekent integriteit dat betalers niet meer uitgeven dan waar ze toestemming voor hebben gegeven en dat betaalden al het geld krijgen waar ze recht op hebben. De betaalde zou natuurlijk een hoger bedrag aan Wallie kunnen doorgeven dan dat hij met de betaler is overeengekomen. De betaler krijgt echter na de betaling altijd een bevestiging van Wallie op zijn scherm, dus hij zou het direct merken. Het lijkt niet waarschijnlijk dat deze bevestiging door de betaalde gemanipuleerd kan worden.

Ook voor een derde partij is het door deze bevestiging moeilijk om iets aan de transactie te veranderen zonder dat dit opgemerkt wordt. We beoordelen de integriteit daarom als *goed*.

Onloochenbaarheid Artikel 3.3 van de voorwaarden van Wallie [33] zegt dat betaling onherroepelijk plaats vindt zodra de betaler de code heeft ingevoerd en zijn saldo toereikend is. Bij Wallie is er dus sprake van *volledige* onloochenbaarheid. Dit is voor de gebruiker acceptabel, omdat het niet om zulke grote bedragen gaat. Wallie roept gebruikers echter wel op om eventuele fraude te melden. Deze informatie hebben ze waarschijnlijk nodig om eventuele betrokkenen te kunnen identificeren.

Beschikbaarheid Wallie streeft er naar dat gebruikers altijd bij hun saldo kunnen, maar zegt dit niet te kunnen garanderen in verband met technische storingen [33]. Dit zegt natuurlijk niet zo veel, maar er zijn geen specifieke problemen bekend met de beschikbaarheid van Wallie. Wallie houdt zich verder het recht voor een gebruiker het betalen onmogelijk te maken als daar "zwaarwegende redenen" voor zijn. Ook hier zijn geen problemen mee bekend. We beoordelen de beschikbaarheid daarom als *goed*.

5 Vergelijking

We hebben vier betaalmethoden in detail bekeken. In deze sectie zullen we deze betaalmethoden nog eens naast elkaar leggen en aangeven wat de belangrijkste verschillen en overeenkomsten zijn. Dit zullen we wederom doen door de securitydoelen een voor een te bespreken. Daarna zullen we nog een aantal verbanden noemen die tussen verschillende aspecten zijn gebleken.

Geheimhouding Bij het aspect geheimhouding hebben we eerst gekeken naar wat de aard is van de informatie die in het spel is. Dit verschilt sterk per betaalmethode. Bij creditcard en Wallie wordt er bijvoorbeeld informatie waar mee betaald kan worden verzonden, en bij PayPal en iDeal niet. Dit is ook de voornaamste reden dat de eerste twee slechter zijn beoordeeld dan de laatste twee. De risico's zijn groter, dus eventuele problemen met geheimhouding wegen automatisch zwaarder.

Naast informatie waarmee betaald kan worden hebben we gezien dat ook de rol van persoonlijke informatie verschilt. Bij Wallie is per definitie helemaal geen persoonlijke informatie betrokken, en bij PayPal krijgt de betaalde geen persoonlijke informatie van de betaler te zien. Creditcard en iDEAL zijn wat dat betreft in het nadeel. Dat is ook de reden dat PayPal een hogere waardering heeft gekregen dan iDEAL.

Anonimiteit Bij dit aspect zien we deels een overlap met het aspect geheimhouding, maar anonimiteit gaat specifiek over welke persoonlijke informatie er bij andere deelnemende partijen bekend is, terwijl geheimhouding gaat over welke informatie er voor buitenstaanders mogelijk zichtbaar is. Een methode die goede anonimiteit biedt zal echter ook makkelijker kunnen scoren op geheimhouding, want als persoonlijke informatie al niet bij andere deelnemende partijen bekend is, dan zal een derde partij deze zeker niet kunnen achterhalen. Tussen deze twee aspecten zien we dan ook in de meeste gevallen een verband.

Wallie is wat dat betreft een uitzondering. De anonimiteit is daar per definitie goed omdat er geen persoonlijke informatie in het spel is, maar omdat de geheimhouding van de Wallie-code zwaar weegt valt het aspect geheimhouding toch tegen.

Als we kijken naar de onderlinge verschillen dan is er een duidelijke tweedeling. Bij creditcard en iDEAL moeten zowel betaler als betaalde onder hun echte naam bekend zijn, en dit scoort dus laag. PayPal en Wallie zijn qua opzet zeer verschillend, maar scoren toch even goed. PayPal biedt geen volledige anonimiteit, maar heeft wel weer als voordeel dat de

betaalde net zo anoniem kan zijn als de betaler. Bij Wallie is de anonimiteit voor de betaler wel 100%, maar kan de betaalde weer niet anoniem blijven.

Bij dit aspect moet verder opgemerkt worden dat een "goede" anonimiteit niet per se wenselijk hoeft te zijn. Zoals we al schreven in sectie 3.1.2 kan anonimiteit het moeilijker maken om fraude te ontdekken, en biedt het bovendien mogelijkheden voor chantage of het witwassen van geld.

Authenticiteit Dit is een behoorlijk breed aspect gebleken, waarbij het lastig is om alle vormen van authenticiteit erbij te betrekken, vooral omdat dit per methode verschilt. Toch zijn er ook zeker overeenkomsten. Zo speelt bij alle betaalmethoden het probleem van *phishing*. Bij PayPal en iDEAL was dit wel een minder groot probleem, omdat daar de daadwerkelijke betaling op de website van respectievelijk PayPal en de bank plaatsvindt. Aangezien deze websites bekend zijn bij de betaler zijn deze waarschijnlijk moeilijker te vervalsen.

Het meest in het oog springende verschil tussen de methoden is dat PayPal en iDEAL zich richten op de authenticatie van de betaler, en dat Wallie zich richt op de authenticatie van het betaalmiddel, waarbij voor lief wordt genomen of de betaler de rechtmatige eigenaar is. Bij een creditcard wordt in principe geprobeerd allebei te doen, en dit is problematisch, want de authenticiteit van de betaler kan eigenlijk niet gegarandeerd worden. Om die reden scoort de creditcard hier minder.

PayPal scoort om andere redenen minder. De sterkte van de authenticatie van de betaler door PayPal staat niet helemaal in verhouding met de mogelijke gevolgen wanneer dit mis gaat. PayPal is geheel afhankelijk van één enkel wachtwoord. iDEAL scoort het beste omdat de authenticatie van de betaler door iDEAL buitengewoon sterk is, met een combinatie van "wat je weet" en "wat je hebt", en ook de authenticatie van de betaalde door de betaler goed zit.

Integriteit Dit aspect is eigenlijk niet zo interessant gebleken. De meeste problemen die betaalmethoden hebben kunnen onder geheimhouding of authenticiteit geschaard worden, zodat er voor integriteit weinig overblijft. Wanneer we kijken naar aanvallen op de integriteit van buiten af zien we dat, als een transactie al niet goed beveiligd is met bijvoorbeeld SSL, er altijd iets van een bevestiging gestuurd wordt zodat de deelnemers kunnen zien dat er iets niet in de haak is. Dit betekent natuurlijk wel dat de integriteit van deze bevestiging zelf ook gegarandeerd moet zijn, maar dit lijkt in het algemeen geen probleem te zijn.

Ook als er binnen het systeem iets mis gaat waardoor het geld niet zo verdeeld wordt dat alle partijen krijgen waar ze recht op hebben, dan wordt dit uiteraard opgemerkt. Het enige mogelijke probleem kan ontstaan wanneer de centrale systemen van de uitgever/ontvanger gehackt worden. Bij Wallie zou dit bijvoorbeeld kunnen betekenen dat nummers als uitgegeven kunnen worden aangemerkt terwijl ze nooit echt uitgegeven zijn. Dit is typisch iets dat niet per se gedetecteerd wordt. We hebben echter geen reden om aan te nemen dat dit een realistisch risico is, en daarom scoren alle methoden uiteindelijk goed.

iDEAL krijgt zelfs een zeer goed omdat de bevestiging van een transactie zeer solide geregeld is. De betaler kan via een stuk hardware controleren of de betaling vanuit zijn oogpunt correct plaatsvindt.

Onloochenbaarheid Het aspect onloochenbaarheid is een vreemde eend in de bijt. We geven hier namelijk geen waardeoordeel, omdat afhankelijk van vanuit welke partij je kijkt, het hebben van onloochenbaarheid zowel positief als negatief kan zijn. We zien wel duidelijke verschillen in hoe de verschillende methoden met onloochenbaarheid omgaan. Wallie en iDEAL kiezen voor volledige onloochenbaarheid, wat betekent dat als een betaling heeft plaatsgevonden de betaler deze niet meer terug kan draaien. Dit is in beide gevallen redelijk. Bij Wallie gaat het uiteindelijk om relatief kleine bedragen, dus het is waarschijnlijk niet de

moeite om hier een rechtzaak over te beginnen. In het geval van iDEAL wordt er simpelweg vertrouwd op een goede authenticiteit en integriteit.

Creditcard en PayPal bieden allebei geen volledige onloochenbaarheid. In het geval van de creditcard wordt er uitgegaan van het gelijk van de betaler, en ligt de bewijslast bij de betaalde. Bij PayPal ligt dit subtieler. Hier heeft niemand bij voorbaat gelijk, maar wordt het betwiste bedrag vastgehouden door PayPal zelf totdat er bemiddeld is in het conflict.

Beschikbaarheid We moeten vaststellen dat het heel lastig is gebleken om het aspect beschikbaarheid te beoordelen. Alle betaalmethodes streven volledige beschikbaarheid na, en het is niet altijd duidelijk in hoeverre ze dit kunnen waarmaken. Bij sommige methoden zijn specifieke problemen bekend (PayPal en iDEAL), maar in hoeverre problemen bekend zijn hoeft helemaal niet representatief te zijn voor in hoeverre ze zich voordoen, ook omdat een storing in een weinig gebruikt systeem eerder onopgemerkt voorbij gaat dan in een veel gebruikt systeem. Aan dit aspect kunnen dus niet echt conclusies worden verbonden.

Verbanden Nu we een aantal betaalmethoden in detail hebben bekeken kunnen we kijken of er bepaalde patronen te zien zijn. Zo kan er sprake zijn van een trade-off tussen twee securitydoelen, wanneer iets een positief effect op het ene doel, maar een negatief effect op het andere heeft. Bij iDEAL hebben we bijvoorbeeld gezien dat, ondanks dat de geheimhouding goed werd beoordeeld, deze nog beter had kunnen zijn als bepaalde maatregelen om integriteit te bevorderen niet waren genomen (het versturen van een sms-bericht).

Ook zien we dat de systemen met een betere authenticatie (iDEAL en Wallie) volledige onloochenbaarheid bieden, terwijl de minder scorende systemen dit niet doen. Dit was te verwachten, want om redelijkerwijs onloochenbaarheid als beleid te hebben moet je een goed beveiligd systeem hebben, anders is het erg nadelig voor de betaler. Hier zien we dus ook een duidelijk verband.

6 Classificatie versus kwalificatie

In deze scriptie hebben we geprobeerd de volgende twee deelvragen te beantwoorden:

1. Welke verschillende soorten/categorieën van elektronische betaalmethoden voor e-commerce zijn er te onderscheiden?
2. Aan welke securitydoelen moeten deze betaalmethoden voldoen, en hoe voldoen verschillende soorten betaalmethoden daaraan?

Nu we de methoden met de beantwoording van de eerste deelvraag geclassificeerd hebben, en met de beantwoording van de tweede deelvraag gekwalificeerd hebben, is het natuurlijk ook interessant om te kijken of er verbanden te vinden zijn tussen de classificatie en de kwalificatie. Uiteraard hebben we niet genoeg methoden besproken om statistische verbanden te ontdekken, maar we kunnen gesuggereerde verbanden wel verdedigen met inhoudelijke argumenten.

We hebben om te beginnen onderscheid gemaakt tussen account- en token-gebaseerde systemen. Wallie is het enige token-gebaseerde systeem, en deze methode scoort goed op het onderdeel anonimiteit. Dit lijkt logisch, omdat een token niet verbonden is met een persoon, en er dus ook geen persoonlijke gegevens op het spel staan. Vermoedelijk kan anonimiteit nog beter scoren bij een coin-gebaseerde methode, omdat daarbij, in tegenstelling tot bij Wallie (een counter-gebaseerde methode), ook geen verschillende betalingen van dezelfde betaler aan elkaar gekoppeld kunnen worden.

Als enige credit-gebaseerde systeem verschilt de creditcard methode qua kwalificatie van de debet-gebaseerde systemen PayPal en iDEAL, voornamelijk op het gebied van geheimhouding. Bij creditcard wordt er bijvoorbeeld informatie waarmee betaald kan worden verzonden, en bij PayPal en iDEAL niet. Het lijkt echter zeer onwaarschijnlijk dat dit verschil

het gevolg is van het credit-gebaseerd zijn. Hier kunnen dus geen conclusies aan worden verbonden.

De dimensie online versus offline is verder niet van belang gebleken omdat alle methoden die we hebben besproken online zijn. De theorie was dat het offline zijn een betere beschikbaarheid tot gevolg had, maar dit hebben we dus niet kunnen testen.

Het onderscheid tussen hardware- en software-gebaseerde systemen is wel gebleken. Als enige methode die gebruik maakt van hardware (een random reader of mobiele telefoon) valt iDEAL op met goede authenticiteit en zelfs zeer goede integriteit. Dit komt waarschijnlijk omdat dankzij de hardware authenticatie niet alleen plaatsvindt op basis van "wat je weet", maar ook op basis van "wat je hebt". Een combinatie hiervan is altijd sterk.

Tot slot hebben we ook nog een onderscheid gemaakt tussen kleine en grote betalingen. Wallie is de enige methode die zich richt op kleine betalingen. Dit zou in theorie kunnen leiden tot een betere score op het gebied van geheimhouding. Bij gelijkblijvende controls op het gebied van geheimhouding beoordelen wij een methode waarbij er minder geld op het spel staat wanneer de geheimhouding faalt positiever. In het geval van Wallie is de geheimhouding echter ook duidelijk minder sterk dan bij de andere methoden (het staat in verhouding tot de grootte van het bedrag). Om die reden scoort Wallie dus alsnog niet zo hoog.

Wel kunnen we zien dat de geringe grootte van het bedrag bij Wallie een reden kan zijn waarom er voor volledige onloochenbaarheid is gekozen. De betaler is hierdoor misschien in het nadeel, maar zal dit eerder accepteren omdat het om kleine bedragen gaat. Ook hier is dus een duidelijk verband te zien.

7 Overige betaalmethoden

7.1 MiniTix

Een systeem dat in veel opzichten lijkt op PayPal is MiniTix [15] van de Rabobank. MiniTix is in tegenstelling tot PayPal echter vooral gericht op de betaling van kleine bedragen. Een MiniTix account is verbonden aan een e-mailadres. De gebruiker heeft een zogenaamde "on line portemonnee" waar hij een klein bedrag in kan stoppen via bijvoorbeeld iDEAL. Om te betalen hoeft hij vervolgens alleen nog maar een wachtwoord in te voeren. MiniTix is zelfs zo in te stellen dat de gebruiker gewoon ingelogd kan blijven zodat er echt met één klik betaald kan worden.

7.2 Ecash

Een systeem dat verder zeker interessant zou zijn geweest om te vergelijken met de hiervoor besproken methoden is ecash [26], dat ontwikkeld is door David Chaum. Ecash is een token-gebaseerd systeem dat uitgaat van coins in plaats van counters. De betaler kan zelf coins van verschillende waarden genereren bij de "munt", in ruil voor geld. De betaler stuurt daarvoor een verzoek naar de munt dat bestaat uit een random coin nummer en zogenaamde *blinding factor*, waardoor de munt niet kan zien welk nummer er precies wordt uitgegeven.

Het bericht van de betaler wordt versleuteld door de munt, en teruggestuurd, waarna de betaler de blinding factor weer verwijdert en de zo verkregen coin veilig opslaat op zijn harde schijf.

Wanneer er een betaling plaatsvindt stuurt de betaler een bericht naar de betaalde, dat bestaat uit het unieke ID van de betaalde, een hash van de inhoud van de transactie (product en prijs), en een serie coins. Dit geheel wordt versleuteld met de public key van de ontvangende bank.

De betaalde kan vervolgens (eventueel op een later tijdstip), geld ontvangen van de bank door dit versleutelde bericht naar de bank te sturen, samen met nogmaals een hash van de inhoud van de transactie. De bank kan de twee hashes vergelijken om te controleren of

betaler en betaalde het eens zijn over de transactie, zonder zelf de inhoud van de transactie te kennen. Daarnaast controleert de bank of de coins nog niet uitgegeven zijn, waarna ze als uitgegeven geregistreerd worden, en de betaalde zijn geld kan krijgen.

Het interessante van ecash is dat de betaler volledig anoniem is. Het is zelfs niet mogelijk om twee verschillende betalingen van dezelfde persoon aan elkaar te koppelen, omdat de bank niet weet welke coins aan wie zijn uitgegeven. In deze zin lijkt het van alle besproken betaalmethoden het meest op betalen met contant geld (vandaar ook de naam ecash). Verder is ecash ook als offline methode te classificeren, omdat er bij betaling geen authenticatie van de betaler bij een centrale server hoeft plaats vinden, en het ontvangen van het geld door de betaalde op een later tijdstip kan plaatsvinden.

Ecash is nooit echt een succes geworden. Tot 1998 heeft het geopereerd onder de bedrijfsnaam DigiCash, en na een faillissement is het exploiteerd door eCash Technologies [17]. Het laatste teken van leven lijkt echter uit 2002 te stammen.

8 Conclusie & toekomstig onderzoek

We sluiten deze scriptie af met een conclusie, waarin we bespreken hoe, en in hoeverre de onderzoeksvragen zijn beantwoord, en op welke punten de aanpak verbeterd had kunnen worden. Vervolgens zullen we ook nog een aantal aanbevelingen doen voor mogelijk toekomstig onderzoek. Daarbij kijken we welke vragen nog niet zijn beantwoord, en welke andere onderzoeksvormen er ook nog mogelijk zijn.

8.1 Conclusie

In deze scriptie hebben we een aantal elektronische betaalmethoden voor e-commerce vergeleken. Dit hebben we gedaan door ten eerste een aantal dimensies te onderscheiden aan de hand waarvan de betaalmethoden geclassificeerd kunnen worden. Hierdoor kan duidelijk gemaakt worden op welke punten verschillende betaalmethoden qua ontwerp verschillen.

We hebben de dimensies geselecteerd aan de hand van bestaande literatuur. Het doel daarbij was om een zo compleet mogelijk overzicht te geven van dimensies die in theorie een zinnig onderscheid zouden kunnen opleveren. In de praktijk zijn niet alle dimensies even betekenisvol gebleken. Zo blijkt bijvoorbeeld dat methoden die volgens de definitie offline functioneren in de praktijk niet veel gebruikt worden. Alle methoden die we in detail hebben bekeken waren daarom online.

Als we kijken naar de classificatieboom in figuur 2, dan zien we ook dat bij lange na niet alle combinaties van dimensies erin vertegenwoordigd zijn. De reden hiervoor is dat niet alle combinaties leiden tot een zinnige klasse van methoden.

Achteraf hadden we misschien nog één andere dimensie er bij kunnen betrekken. Het lijkt namelijk wel nuttig om onderscheid te maken tussen methoden die *peer to peer* zijn, oftewel waarbij de status van betaler en betaalde gelijkwaardig is, en methoden waarbij de status van betaler en betaalde duidelijk verschillend is. PayPal werkt van de onderzochte systemen als enige *peer to peer*, omdat je daarbij net zo makkelijk betaalde als betaler kunt worden.

We kunnen desondanks concluderen dat de eerste deelvraag ("Welke verschillende soorten/categorieën van elektronische betaalmethoden voor e-commerce zijn er te onderscheiden?") naar tevredenheid is beantwoord doordat we een aantal unieke klassen hebben kunnen onderscheiden die allemaal op minstens één belangrijke dimensie verschillen en waarvoor minstens één praktijkvoorbeeld van een betaalmethode bestaat.

Om de tweede deelvraag ("Aan welke securitydoelen moeten deze betaalmethoden voldoen, en hoe voldoen verschillende soorten betaalmethoden daaraan?") te beantwoorden moesten vervolgens nog twee dingen gedaan worden. Ten eerste hebben we op basis van bekende securitydoelen een raamwerk uitgezet waarin betaalmethoden getoetst konden worden. Ten tweede hebben we een aantal betaalmethoden geselecteerd om te toetsen.

Om tot het raamwerk te komen hebben we gekeken welke securitydoelen er in de literatuur onderscheiden worden. We hebben er voor gekozen om deze doelen zo precies mogelijk te kiezen. Dit betekent dat we bijvoorbeeld het aspect privacy hebben opgesplitst in geheimhouding en anonimiteit. Toch bleek later dat het vaak nuttig was om binnen de gekozen doelen ook nog een onderscheid te maken. Bijvoorbeeld bij authenticiteit moet er goed naar gekeken worden van wie of van wat de authenticiteit gecontroleerd wordt, om tot een preciezere vergelijking te komen. Dit onderscheid hebben we in een later stadium geprobeerd alsnog toe te voegen, maar het was beter geweest als dit al vanaf het begin duidelijk was geweest.

Ook het onderscheid tussen geheimhouding en anonimiteit bleek af en toe vooral verwarrend te werken. Misschien was het beter geweest om dit toch onder het kopje privacy te vatten, maar vervolgens wel preciezer onderscheid te maken in privacy van wie/wat, en voor wie. Op die manier zou het onderscheid dat we gemaakt hebben tussen geheimhouding voor deelnemende partijen en voor derde partijen minstens zo duidelijk zijn geweest.

De rol van het aspect integriteit was verder ook niet helemaal duidelijk. In de praktijk is het een soort restcategorie geworden voor problemen die niet onder geheimhouding of authenticiteit vallen. We zijn uiteindelijk niet veel punten tegen gekomen waarvoor geldt dat ze niet onder die twee aspecten vallen. Toch lijkt het weglaten van deze categorie ook geen optie. Voor de volledigheid moet dit aspect wel meegenomen worden.

We kunnen concluderen dat het opgestelde raamwerk werkbaar, maar niet perfect is. Het moet eigenlijk nog gedetailleerder gemaakt worden om de beoordeling van een betaalmethode meer objectief te maken, en minder te baseren op een “algemene indruk”.

Het selecteren van de te beoordelen betaalmethoden is niet volgens een hele specifieke methode gedaan. We hadden wel een aantal eisen. Zo moesten ze in ieder geval allemaal tot een verschillende klasse behoren. Verder was de belangrijkste eis dat ze in de praktijk redelijk succesvol zijn gebleken (of in ieder geval veel gebruikt worden). Het is namelijk zeer lastig om een methode die alleen op papier bestaat te vergelijken met een die ook echt in de praktijk gebruikt wordt. Bovendien kan over een aspect als beschikbaarheid niet veel gezegd worden bij een theoretische methode.

Uiteindelijk claimen we niet een volledig overzicht van in de praktijk gebruikte methoden te hebben gegeven, en hebben we het bij vier methoden gehouden. Toekomstig onderzoek zou de selectie van methoden nog kunnen uitbreiden.

De methoden die wel geselecteerd zijn, zijn uiteindelijk onderzocht aan de hand van informatie die er op internet beschikbaar is. In het geval van creditcard gaat het deels om wetenschappelijke artikelen, maar in het geval van de nieuwere methoden hebben we ons voornamelijk moeten baseren op informatie die de methoden zelf aanbieden, zoals gebruikersovereenkomsten. De informatie was vaak versnipperd en tamelijk oppervlakkig, maar na enig puzzelwerk was wel te achterhalen hoe bijvoorbeeld de communicatie beveiligd was.

Het tweede deel van de tweede deelvraag (“hoe voldoen verschillende soorten betaalmethoden daaraan?”) is misschien wat ambitieus gebleken, omdat we wel kunnen beoordelen hoe verschillende betaalmethoden aan de securitydoelen voldoen, maar niet weten in hoeverre de gekozen methoden representatief zijn voor een *soort* betaalmethode. Om hierover een zinnige uitspraak te doen moeten eigenlijk meerdere methoden uit dezelfde klasse bekeken worden, zodat beter onderscheid gemaakt kan worden tussen wat inherent aan het ontwerp is en wat implementatie-specifiek is. Dit lijkt in de praktijk echter niet haalbaar, omdat het aantal in de praktijk gebruikte betaalmethoden toch beperkt is.

In sectie 6 hebben we wel geprobeerd op inhoudelijke gronden verbanden te leggen tussen de classificatie en de kwalificatie van de methoden en hieruit is wel een aantal duidelijke verbanden gebleken. In die zin heeft de classificatie dus wel degelijk nut gehad.

De tweede deelvraag is hiermee naar onze mening redelijk goed beantwoord.

8.2 Toekomstig onderzoek

Deze scriptie heeft een aantal vragen geprobeerd te beantwoorden, maar roept ook nieuwe vragen op. Het zou bijvoorbeeld zeer interessant zijn om te onderzoeken hoe gebruikers de security van de verschillende betaalmethoden ervaren. De perceptie van de gebruikers hoeft natuurlijk helemaal niet overeen te komen met de conclusies die we getrokken hebben. Ook kan er dan gekeken worden of alle veiligheidsmaatregelen niet te veel inspanning van de gebruiker vereisen. Of een betaalmethode een commercieel succes is hangt ook af van de gebruiksvriendelijkheid. Als je snel iets wilt afrekenen kies je misschien toch voor de methode die het minste moeite kost.

Ons oorspronkelijke onderzoeksplan bevatte ook een deelvraag waarin een enquête antwoord had moeten geven op deze vragen. Dit bleek uiteindelijk niet haalbaar omdat zo'n enquête toch veel tijd kost en er pas mee kon worden begonnen wanneer de andere deelvragen beantwoord waren.

Zoals we al schreven in de conclusie was de methode waarmee de betaalmethoden onderzocht zijn niet ideaal. Het is daarom interessant om ook na te denken over mogelijke andere methoden. Om gerichtere informatie te krijgen zou het bijvoorbeeld een optie zijn om experts op het gebied van elke betaalmethode te interviewen.

Met preciezere informatie kan vervolgens ook objectiever bekeken worden hoe secure een betaalmethode is. Een goede methode om dit meetbaar te maken kan zijn om gebruik te maken van *attack trees* [28]. Dit kan echter alleen als er echt goede gegevens te verkrijgen zijn over risico's op aanvallen, en de gevolgen daarvan, en dit zal een probleem zijn omdat commerciële ondernemingen hoogstwaarschijnlijk toch terughoudend zijn met het vrijgeven van zulke gegevens.

Referenties

[1] Dennis Abrazhevich. Classification and characteristics of electronic payment systems. *EC-Web 2001*, pages 81–90, 2001.

[2] Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, 2001.

[3] N. Asokan, Phillipe A. Janson, Michael Steiner, and Michael Waidner. The state of the art in electronic payment systems. *IEEE Computer*, 30(9):28–35, 1997.

[4] Authorize.net. E-commerce guide. http://www.authorize.net/files/ecommerceguide.pdf. Opgehaald: 23 juni 2007.

[5] Millward Brown. Gebruik betaalmethode via internet ideal gestegen. http://www.millwardbrown.nl/?pm=millwardbrown_d&type=publicatie&id=95, December 2006. Opgehaald: 23 juni 2007.

[6] J. Claessens, B. Preneel, and J. Vandewalle. Anonymity controlled electronic payment systems. In A. M. Barbé et. al., editor, *20th Symp. on Information Theory in the Benelux*, pages 109–116, Haasrode (B), 27-28 1999. Werkgemeenschap Informatie- en Communicatietheorie, Enschede (NL).

[7] Joris Claessens. *Analysis and Design of an Advanced Infrastructure for Secure and Anonymous Electronic Payment Systems on the Internet*. PhD thesis, Katholieke Universiteit Leuven, 2002.

[8] Algemeen Dagblad. Website postbank lag al 16 keer plat. http://www.ad.nl/binnenland/article1424873.ece. Opgehaald: 23 juni 2007.

[9] Simon Fong and Edison Lai. Mobile mini-payment scheme using sms-credit. *Lecture Notes in Computer Science*, 3481:1106–1114, 2005.

[10] Andrés Guadamuz González. Paypal and ebay: The legal implications of the c2c electronic commerce model. In *18th BILETA Conference: Controlling Information in the Online Environment*, 2003.

[11] Petr Hanácek. Security of electronic money. In *SOFSEM '98: Proceedings of the 25th Conference on Current Trends in Theory and Practice of Informatics*, pages 107–121, London, UK, 1998. Springer-Verlag.

[12] Paul J.M. Havinga, Gerard J.M. Smit, and Arne Helme. Survey of electronic payment methods and systems. In *Euromedia*, pages 180–187, 1996.

[13] iDEAL. http://www.ideal-betalen.nl. Opgehaald: 23 juni 2007.

[14] MasterCard. Betaalgemak ook via internet. http://www.mastercard.com/nl/education /payoninternet/pay_on_internet_with_mc.html. Opgehaald: 23 juni 2007.

[15] MiniTix. http://www.minitix.nl/. Opgehaald: 23 juni 2007.

[16] Statictics Netherlands. The digital economy 2006. Statistics Netherlands - Prinses Beatrixlaan 428 2273 XZ Voorburg, 2007.

[17] PR Newswire. ecash technologies opens european office in amsterdam. http://www.prnewswire.co.uk/cgi/news/release?id=38042. Opgehaald: 23 juni 2007.

[18] PayPal. http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/about-outside. Opgehaald: 23 juni 2007.

[19] PayPal. Beleid inzake klachten van kopers. https://www.paypal.com/nl/cgi-bin/webscr?cmd=p/ gen/ua/policy_buyer_complaint-outside. Opgehaald: 23 juni 2007.

[20] PayPal. Gegevenscodering. https://www.paypal.com/nl/cgi-bin/webscr?cmd=xpt/cps/securitycenter/buy/DataEncryption. Opgehaald: 23 juni 2007.

[21] PayPal. Niet-geautoriseerd gebruik van uw paypal-rekening. https://www.paypal.com/nl/wf/f=sa_unauth. Opgehaald: 23 juni 2007.

[22] PayPal. Privacybeleid. https://www.paypal.com/nl/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy. Opgehaald: 23 juni 2007.

[23] PayPal. Transactiekosten voor binnenlandse betalingen - nederland. https://www.paypal.com/nl/cgi-bin/webscr?cmd=_display-receiving-fees. Opgehaald: 23 juni 2007.

[24] Postbank. http://www.postbank.nl. Opgehaald: 23 juni 2007.

[25] Rabobank. http://www.rabobank.nl. Opgehaald: 23 juni 2007.

[26] B. Schoenmakers. Basic security of the ecash payment system. In *State of the Art in Applied Cryptography, Course on Computer Security and Industrial Cryptography*, pages 338–352, Leuven, Belgium, 1997. Springer-Verlag.

[27] Heiko Schuldt, Andrei Popovici, and Hans-Jörg Schek. Execution guarantees in electronic commerce payments. *Lecture Notes in Computer Science*, 1773:193–202, 2000.

[28] Bruce Sneier. Modeling security threats. *Dr. Dobb's Journal*, december 1999.

[29] Andrew S. Tanenbaum. *Computer Networks*. Prentice Hall PTR, fourth edition, 2002.

[30] Thuiswinkel.org. http://www.thuiswinkel.org/onderdeel/thuiswinkelennl/. Opgehaald: 23 juni 2007.

[31] Visa. Address verification service. http://www.visaeurope.com/merchant/ handlingvisapayments/cardnotpresent/addressverificationservice.jsp. Opgehaald: 23 juni 2007.

[32] Wallie. http://www.wallie.com/. Opgehaald: 23 juni 2007.

[33] Wallie. Gebruiksvoorwaarden voor de wallie-card. http://www.wallie-card.nl/conditions.php. Opgehaald: 23 juni 2007.

[34] Wallie. Wallie stelt zich voor. http://www.wallie-card.nl/pdf/WallieSteltzichvoor.pdf. Opgehaald: 23 juni 2007.

[35] Webwereld. Paypal krijgt bankstatus binnen europa. http://www.webwereld.nl/articles/46419/paypal-krijgt-bankstatus-binnen-europa.html. Opgehaald: 23 juni 2007.

[36] Wired.com. Paypal freezes out katrina aid. http://www.wired.com/science/discoveries/news/2005/09/68788. Opgehaald: 23 juni 2007.