Betalingsverkeer: trends, ontwikkelingen en de IT-auditor

De Kennisgroep Betalingsverkeer van de NOREA heeft als doel bij te dragen aan de vaktechnische profilering en ondersteuning van de beroepsgroep door totstandbrenging van relevante producten op het gebied van (audit van) Betalingsverkeer. In het kader daarvan wil de Kennisgroep Betalingsverkeer een aantal relevante ontwikkelingen binnen het betalingsverkeer bespreken. Deze ontwikkelingen hebben invloed op de assurancebehoefte van partijen in de betalingsverkeerketen en hebben ook invloed op de eisen die gesteld worden aan IT-auditors die op enige manier bij de betalingsverkeerketen betrokken zijn.

KENNISGROEP BETALINGSVERKEER

De problemen die zich de afgelopen maanden hebben voorgedaan in het betalingsverkeer, de publiciteit daarover en de ongerustheid die dat met zich heeft meegebracht, zijn ernstig. De Nederlandse economie is zeer afhankelijk van het betalingsverkeer, dat in hoge mate steunt op betrouwbare informatietechnologie. Vooralsnog zijn er weinig tot geen gelijkwaardige alternatieven voor de afwikkeling van het digitale betalingsverkeer voorhanden in het geval dat zich in de keten ernstige verstoringen voordoen. Het betalingsverkeer heeft, gezien de maatschappelijke impact bij verstoringen, het karakter van een vitale infrastructuur en nutsvoorziening.

Iedereen heeft baat bij een goed functionerende betaalinfrastructuur; dat geldt voor individuele consumenten, het bedrijfsleven, financiële instellingen en de overheid. Als om welke reden dan ook de kwaliteit van het betalingsverkeer in het gedrang komt, zal dat snel een sterk ontregelende werking hebben op het gehele economische systeem.
Daarnaast is betalingsverkeer sterk aan verandering onderhevig. Technologische ontwikkelingen, zoals de opkomst van *mobile devices*, maar ook politiek-economische ontwikkelingen, zoals de Europese eenwording, hebben invloed op het betalingsverkeer. Dit heeft weer invloed op de betaalproducten die aan de markt worden aangeboden en op de spelers die in die markt actief zijn.

Het betalingsverkeer kent een vrij grote dynamiek en in dit artikel willen we enkele recente ontwikkelingen onder de aandacht brengen. We presenteren een model dat op een eenvoudige maar systematische manier inzicht kan geven in de met betalingsverkeer gemoeide risico's, waarbij we gekozen hebben voor een ketenbenadering.

In een volgend artikel zullen we dieper ingaan op het model en de ketenbenadering en geven we aan welke veranderingen in competenties en focus de IT-auditor naar onze mening aan de dag zou moeten leggen om zijn rol ten aanzien van het geven van assurance over betalingsverkeer te kunnen blijven vervullen.

BETALINGSVERKEER: DEFINITIE EN SCOPE

Het betalingsverkeer omvat het gehele systeem van de afhandeling van de monetaire verplichtingen door de overdracht van financiële middelen. Dit gebeurt tegenwoordig in hoge mate elektronisch. Het chartaal betalingsverkeer blijft in dit artikel buiten beschouwing.
In het elektronisch retailbetalingsverkeer in Nederland waren in 2012 circa 23 miljoen betaalrekeningen

IT Auditor_13_03.indd 27 03/09/13 5:04 PM

in gebruik, waarmee betalingen met een waarde van EUR 1.341 miljard werden verricht. Traditioneel lag de rol voor de verwerking van deze verplichtingen vrijwel geheel bij de banken. Met name het retailbetalingsverkeer wijzigt de laatste jaren snel door technologische ontwikkelingen, de toename van aanbieders van betaaldiensten, globalisering en wet- en regelgeving. Het betalingsverkeer wordt complexer doordat er meer spelers actief zijn en een groter assortiment aan betaalproducten wordt aangeboden. Ook de rol van niet-bancaire ondernemingen, die veelal globaal actief zijn, neemt in belangrijke mate toe.

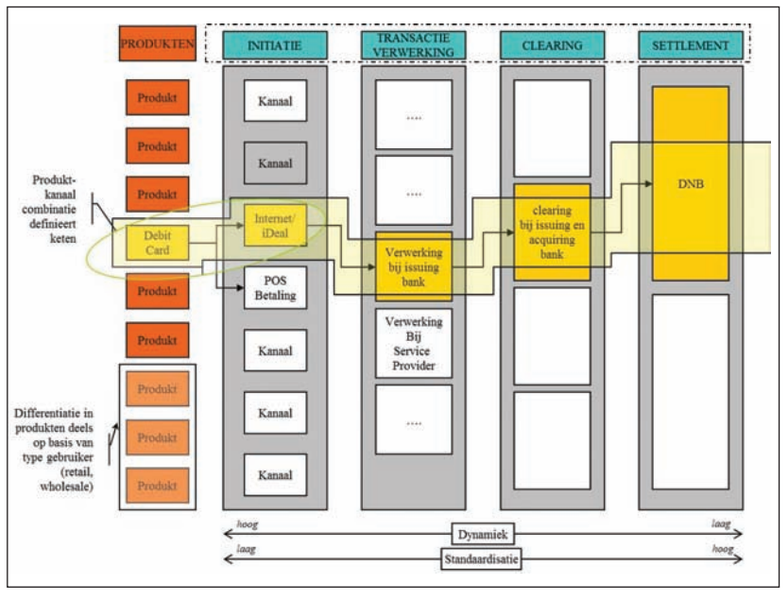
Het hoogwaardig betalingsverkeer (*clearing* en *settlement*) speelt weliswaar een zeer belangrijke rol in het betalingsverkeer voor de afwikkeling van transacties, maar zal in dit artikel grotendeels buiten beschouwing blijven.

MODEL VAN BETALINGSVERKEER

Betalingsverkeer wordt van oudsher functioneel gemodelleerd. Hieronder beschrijven we op hoofdlijnen een gangbare functionele zienswijze op het betalingsverkeer zoals die door de leden van de kennisgroep wordt gebruikt. Het voordeel van dit functionele model is dat het ondanks de dynamiek en complexiteit van betalingsverkeer zijn bruikbaarheid behoudt in een bespreking van de met betalingsverkeer gemoeide risico's.

De functionaliteit van het betalingsverkeer is gericht op het verwerken van transacties met betaalproducten. Die producten zijn weergegeven in de linkerkolom van figuur 1. Het zijn producten waarmee op afstand (overschrijving, acceptgiro, online betaling) en over de toonbank (met een bankpas oftewel debit card, credit card, de chipknip) betalingen kunnen worden verricht.

De ketenprocessen (weergegeven in de kolommen) binnen figuur 1 zijn de volgende:



Figuur 1: Functioneel model van betalingsverkeer

a. Initiatiekanalen waaronder geldautomaten, betaalautomaten, internet (internetbankierenapplicaties) en online betalen, bijvoorbeeld met IDEAL.
b. Transactieverwerking bij de bank of partij die de producten uitgeeft (*issuer*) of de *acquirer* (de partij die namens de *merchants* optreedt (verkopers, zoals houders van betaalautomaten)).
c. Clearing omvat de activiteiten van de partijen die aangewezen zijn om de betalingen van de banken met elkaar te verrekenen.
d. Settlement gebeurt bij de settlementinstellingen die namens de banken uiteindelijk de saldi beheren en daarmee (schuld)posities van de banken onderling met elkaar verrekenen.

De combinaties van producten en kanalen bepalen hoe de verwerkingsketen van een bepaald soort betaling er precies uitziet. Dat zijn tevens de ketenprocessen die in termen van innovaties en verandering de grootste dynamiek kennen. Aan de rechterzijde van het schema zijn ketenprocessen (clearing en settlement) in algemene zin stabiel en minder aan verandering onderhevig. Alle ketenprocessen staan aan risico's bloot en de betrouwbare verwerking van een betaling is afhankelijk van het goed functioneren van de gehele keten.

De aandacht die spelers in het betalingsverkeer voor de beheersing van risico's hebben, is vooral gericht op hun eigen rol in die keten. Dat is verklaarbaar vanuit de eigen verantwoordelijkheid die een speler (zoals een bank) heeft, en vanuit invloedssfeer. In de eigen omgeving kunnen immers relatief gemakkelijk beheersingsmaatregelen worden getroffen. Toch wordt het risico van een betrouwbare verwerking van betaaltransacties bepaald door maatregelen in de gehele keten. Het model is dan ook een goed uitgangspunt om, voor specifieke combinaties van producten en kanalen, de betaalketen specifieker en met meer precisie in kaart te brengen. Het resultaat kan vervolgens dienen voor verdere (risico) analyse.

RISICO'S IN BETALINGSVERKEER

Betalingsverkeer heeft een drietal kenmerken die risico's met zich mee brengen [RAMB08].

IT Auditor_13_03.indd 28 03/09/13 5:04 PM

Op de eerste plaats is dat het enorme economische belang van de keten (met het eerder genoemde karakter van een vitale infrastructuur en nutsvoorziening), gekoppeld aan de volumes en bedragen die erdoor worden verwerkt. Verstoringen in de keten leiden onherroepelijk tot kleinere of grotere ontwrichtingen van de financieel-economische machine. Op de tweede plaats is de keten dynamisch. Geregeld treden nieuwe spelers toe, en er is een voortdurende innovatie op technisch en financieel gebied. Dit wordt gedreven door nieuwe regelgeving, door productontwikkeling, maar ook door de behoefte van spelers in de keten om steeds grotere volumes betrouwbaar te kunnen afhandelen. Tenslotte wordt de keten, als gevolg van de eerste twee kenmerken, steeds complexer en daarmee lastiger beheersbaar.

Slechts weinigen hebben een volledig inzicht in en begrip van de complexiteit van de gehele keten [RAMB08]. Daarom vereist een goed functionerend betalingsverkeer coördinatie tussen de verschillende partijen in de keten, met een optimale afstemming van de verschillende expertisegebieden, te weten: financieel, wettelijk, IT, risk management en audit.

We volgen hier de ordening van risico's die het Committee on Payment & Settlement Systems (CPSS) van de BIS [RAMB08] hanteert:

1. Financieel risico
   Dit risico houdt in dat een partij in de betaalketen zijn financiële verplichtingen niet kan nakomen (kredietrisico), of over onvoldoende middelen beschikt om zijn verplichtingen na te komen op een bepaald moment in de tijd waarop dat wel nodig is (liquiditeitsrisico).

2. Wettelijk risico
   Dit risico houdt in dat er onzekerheid bestaat over (de afdwingbaarheid van) contractuele verplichtingen tussen partijen in de keten, en over wettelijke voorwaarden in geval van insolventie of faillissement.

3. Operationeel risico (security, continuity)
   Dit risico houdt in dat zich mogelijk operationele verstoringen in het betalingsverkeer voordoen, met name ten aanzien van beschikbaarheid en beveiliging van de keten.

4. Systeemrisico
   Dit is het zogenaamde 'domino-effect': het risico dat verstoringen in de keten, bijvoorbeeld door het 'omvallen' van een van de spelers, zal leiden tot grote financiële problemen bij andere partijen, met als gevolg een systemische crisis en ernstige disruptie van de gehele keten en daarmee van het maatschappelijk verkeer.

De bovengenoemde risicocategorieën beïnvloeden elkaar. Als voorbeeld: verstoringen in het operationele betalingsverkeer door beveiligingsincidenten of continuïteitsverstoringen kunnen leiden tot financiële risico, wettelijke consequenties en claims, en uiteindelijk mogelijk zelfs tot systeemrisico's.

De eerder genoemde kenmerken van het moderne betalingsverkeer (toenemend belang, dynamiek, en complexiteit) leiden in algemene zin tot een toename van inherente risico's in alle genoemde categorieën. In het kader van dit artikel richten we ons met name op de (toegenomen) operationele risico van betalingsverkeer. De reden hiervoor is dat de keuze voor deze groep risico's goed aansluit bij de actualiteit en binnen het aandachtsgebied van de IT-auditor valt.

ONTWIKKELINGEN IN HET BETALINGSVERKEER

De veranderingen in het betalingsverkeer hebben niet zozeer impact op de uiteindelijke functie daarvan (het faciliteren van maatschappelijk verkeer en handel) maar wel op de inrichting van de keten, de spelers die daarin een rol vervullen, en de technologie waarvan gebruik wordt gemaakt. Voor de beheersing van de risico's in de betalingsverkeerketen (en dus ook voor de IT-auditor die zich daarover een opinie vormt) is dit relevant.
Er zijn enkele belangrijke *change drivers* aan te wijzen voor de huidige veranderingen in de betalingsverkeer keten:

1. Internationalisering en globalisering.
2. Nieuwe spelers in betalingsverkeer.
3. Technologische ontwikkelingen.

Deze drie drivers sluiten elkaar niet uit; ze versterken elkaar vaak zelfs. Zo zien we dat internationalisering invloed heeft op wet- en regelgeving in de markt, die het eenvoudiger maakt voor partijen om toe treden (bijvoorbeeld door SEPA, waarover hieronder meer). En technologische ontwikkelingen dragen op hun beurt bij aan mondiaal betalingsverkeer waarin vele verschillende (markt) partijen een rol hebben. Deze change drivers leiden tot een versterking van de risico's die inherent al aanwezig zijn in de betalingsverkeerketen. In de navolgende paragrafen gaan we in op enkele voorbeelden van veranderingen door deze change drivers.

Internationalisering/globalisering

Dit zijn internationale of zelfs mondiale tendensen en processen waarbij samenhang en samenwerking tussen individuen, organisaties, en landen steeds meer op een internationale schaal vorm krijgen. Dit zet spelers in de betalingsverkeerketen onder druk om mee te bewegen om in een geglobaliseerde wereld hun faciliterende rol te blijven vervullen. In die zin is betalingsverkeer olie in de motor van de wereldeconomie. Hieronder noemen we twee voorbeelden van ontwikkelingen die duidelijk terug te voeren zijn op globalisering en internationalisering.

IT Auditor_13_03.indd 29 03/09/13 5:04 PM

SEPA

SEPA staat voor *Single Euro Payments Area* en komt voort uit Europese wetgeving. De wetgeving, die begin 2012 definitief werd, geldt voor de zeventien landen die de euro hebben ingevoerd, aangevuld met vijftien andere EU-landen en de landen van de Europese Vrijhandelsassociatie.

Het doel van SEPA is dat bij alle betalingen de kosten, snelheid, rechten en plichten gelijk zijn. Hiermee ontstaat één eurobetaalgebied en wordt betalen transparanter en efficiënter. De veronderstelling is dat dit de handel in de lidstaten verder zal bevorderen en de concurrentie tussen en innovatie door banken zal vergroten. Na invoering van SEPA zal er alleen nog verschil bestaan tussen betalingen binnen de SEPA-landen en betalingen naar en vanuit landen buiten SEPA.

De huidige betaalproducten worden omgezet naar SEPA-betaalproducten. Belangrijk verschil met de huidige betaalproducten is dat ze zijn gebaseerd op de IBAN/BIC[1] in plaats van het huidige Nederlandse rekeningnummer. Daarnaast kennen de betaalproducten bijvoorbeeld andere tijdslijnen voor aanlevering en verwerking, en is de opbouw anders (zoals het bestandsformaat bij batchbetalingen). De nieuwe SEPA-wetgeving omvat nieuwe standaarden, waarin is afgesproken hoe toekomstige betalingen gaan plaatsvinden. Een groot deel van de huidige nationaal georiënteerde betaalproducten komt te vervallen en is per bovengenoemde datum dan ook niet meer te gebruiken. Organisaties moeten een nieuwe set SEPA-betaalproducten gaan gebruiken. Hetzelfde geldt voor klanten en leveranciers. Aanpassen van de huidige IBAN en BIC-codes is niet voldoende om de continuïteit in de inkomende en uitgaande geldstromen te waarborgen. Deze verplichtingen gaan spelen vanaf begin 2014. SEPA heeft een grote impact: banken moeten hun producten aanpassen, bedrijven hun administratie en ook burgers moeten BIC en IBAN gaan gebruiken. SEPA heeft niet alleen impact op de ICT binnen organisaties, maar ook op de inrichting van (financiële) processen, procedures en koppelingen met andere deelnemers.

PayPal

De geschiedenis en het succes van PayPal zijn nauw verbonden met het globaliseringseffect van internet. PayPal betrad de markt in 1998 en bood een oplossing om wereldwijde betalingen te faciliteren voor productaankopen bij onbekende tegenpartijen, bijvoorbeeld via veilingsites zoals eBay (die inmiddels ook eigenaar van PayPal is). PayPal vervult een intermediaire rol tussen verkoper (merchant) en koper en lost daarbij een tweetal problemen op. Op de eerste plaats zijn veel aanbieders van producten op het internet geen merchants in de traditionele zin; het zijn vaak particulieren, die niet de middelen hebben om credit- of debitcardbetalingen te ontvangen. Ten tweede zijn kopers terughoudend in het verstrekken van betaalgegevens (creditcardnummers, rekeninginformatie) aan een onbekende derde. Door deze gegevens uitsluitend aan PayPal ter beschikking te stellen, in combinatie met het aanhouden van een rekening bij PayPal waarop tegoeden voor het aankopen van producten kunnen worden aangehouden, of waarop aankoopbedragen kunnen worden gestort, worden deze problemen opgelost.

PayPal is een voorbeeld van *disintermediation*: de rol van de traditionele bank als facilitator van betalingen tussen koper en verkoper wordt overgenomen door een andere partij. En in aanzienlijke mate: het totale volume van verwerkte betalingen door PayPal liep in 2012 op tot 145 miljard dollar. Alhoewel het door sommige traditionele banken nog wordt gezien als een 'nieuwe speler', is PayPal inmiddels het belangrijkste platform voor internetbetalingen [KING13].

Nieuwe spelers in Betalingsverkeer

Traditioneel gezien was de toegang tot betalingsverkeersystemen voorbehouden aan de banken, maar daarin is allengs verandering gekomen. In Europa wordt dit in belangrijke mate mogelijk gemaakt door de Payment Services Directive. Deze staat ook niet-bancaire instellingen toe om als zogenaamde *Payment Institutions* betaaldiensten op de markt aan te bieden. Maar daarnaast moet ook worden gedacht aan nieuwe spelers, die hun plaats te danken hebben aan verschuivingen in consumentengedrag als gevolg van technologische ontwikkelingen: zo spelen aanbieders van mobiele telefonie een belangrijke concurrerende rol voor de banken als het gaat om mobiel betalen, zoals bij M-Pesa, waarover later meer. En er zijn partijen die zich als dienstverlener positioneren tussen consument en bank, zoals het volgende voorbeeld illustreert.

SofortBanking

Het Duitse bedrijf Payment Network AG biedt consumenten en webwinkeliers een online betaalservice aan onder de naam SofortBanking. Als merchants daarvoor kiezen, kan deze service worden geïncorporeerd in hun website als een geldige betaaloptie, die door de online-klant met een eenvoudige klik kan worden opgestart. Aangezien de service betalingen vanuit een aantal Europese landen (waaronder Nederland en België) ondersteunt, opent een SofortBanking-enabled webshop eenvoudige online-betaalmogelijkheden voor een internationaal publiek. In beginsel doet de service ook erg denken aan een internationale variant van iDeal. Een belangrijk verschil is echter dat een koper/betaler nu niet terecht komt in de omgeving van zijn bank, maar bij Sofort. De klant verstrekt zijn betaalgegevens (rekeningnummer, pasnummer, challenge/responsegegevens en elektronische handtekening of TAN-code) aan SofortBanking, die als een

IT Auditor_13_03.indd 30 03/09/13 5:04 PM

tussenpersoon het verkeer met de bank afhandelt en de merchant op de hoogte stelt als de betaling is voldaan.

Bij dit model worden inloggegevens met een derde partij gedeeld, en die derde partij (SofortBanking) kan daardoor richting de bank optreden als ware zij de betalende klant. Vanuit beveiligingsoogpunt is dit op zijn minst opmerkelijk. DNB heeft zich dan ook al eens kritisch uitgelaten over deze zogenaamde *overlay services* [DNB09], en de Europese Centrale Bank werkt momenteel aan richtlijnen voor wat zij 'Payment Initiation Services' noemt [ECB13]. Door de gevestigde naam van iDeal is Sofort Banking in Nederland niet erg bekend, maar in Duitsland is het wel degelijk een belangrijke speler voor online-betalingen.

M-Pesa

In Nederland is M-Pesa onbekend en daardoor speelt deze betaalvorm geen rol van betekenis. Niettemin is deze mobiele betaaldienst een goed voorbeeld van de veranderingen die als gevolg van innovaties in de (mobiele) technologie aan een razendsnelle groei bezig zijn. M-Pesa is een door telecomoperator Safaricom (dochteronderneming van Vodafone) opgerichte service in Kenia die tegenwoordig ook in Tanzania actief is. Het grootste gedeelte van de bevolking van deze landen heeft geen toegang tot banken en reguliere bankdiensten, of heeft onvoldoende financiële armslag om een bankrekening aan te kunnen houden. Datzelfde bevolkingsdeel heeft wel degelijk grote behoefte aan financiële diensten, zoals het kunnen aanhouden van bescheiden tegoeden en vooral het kunnen verzenden van geld (*money transfer,* bijvoorbeeld voor zogenaamde *remittances* van arbeiders in de steden naar familie op het platteland). De mobiele telefoon, die in tegenstelling tot bankfilialen wél alom aanwezig is, biedt uitkomst. De SIM-kaart is geschikt gemaakt voor M-Pesa, en de klant kan voor het openen van een M-Pesa rekening en voor het storten van cash geld terecht bij een omvangrijk netwerk van retailers die optreden als agent, waaronder tankstations en winkeliers die vaak al mobiele beltegoeden verkopen. Dat geld wordt bewaard op de M-Pesa rekening van de klant, die vervolgens het tegoed naar believen met behulp van een eenvoudig sms-bericht naar een willekeurige andere telefoongebruiker kan overmaken. De ontvanger kan zijn opgehoogde tegoed op zijn rekening laten staan, of het desgewenst contant opnemen bij een M-Pesa agent.

Alhoewel de Afrikaanse marktomstandigheden zich moeilijk laten vergelijken met die van Europa, illustreert de M-Pesa case uitstekend hoe succesvol mobiele technologie kan zijn, bijvoorbeeld in het aanbieden van betaaldiensten op plaatsen waar traditionele spelers zoals banken voor kleinere consumenten geen rol spelen of onbereikbaar zijn. Bovendien laat het zien hoe mobiele operators een lacune in het betalingsverkeer opvullen met een verdienmodel waarin de traditionele banken geen rol van betekenis spelen. Meer dan 15 miljoen mensen (ongeveer de helft van de Keniaanse bevolking) gebruikt M-Pesa.

Technologische ontwikkelingen

Zoals eerder opgemerkt, is de betalingsverkeerketen altijd al sterk technologisch gekleurd geweest. Illustratief hiervoor is SWIFT, dat al in 1977 zorgde voor een beveiligd internationaal communicatienetwerk en, belangrijker nog, voor het definiëren van standaarden voor financieel berichtenverkeer die elektronische verwerking mogelijk maakten. SWIFT is er nog steeds, maar wie terugdenkt aan de tijd dat we met Euro- en Kascheques betaalden en we naar een bankfiliaal gingen om overschrijvingen voor elkaar te krijgen, kan niet anders concluderen dan dat het betalingsverkeer een grote ontwikkeling heeft doorgemaakt. Die veranderingen zijn in belangrijke mate mogelijk gemaakt door technologische ontwikkelingen en de adoptie daarvan door consumenten en aanbieders in de betalingsverkeerketen. Internetbankieren en internetbetalingen zijn inmiddels gemeengoed. Cheques zijn (althans in Nederland) praktisch verdwenen, en in plaats daarvan betalen we met een plastic kaart voorzien van een chip. Een bezoek aan een fysiek bankkantoor is iets wat we tot een minimum kunnen beperken; zoals King terecht opmerkt op de omslag van zijn boek 'Bank 3.0' is *banking no longer somewhere you go, but something you do*' [KING13].

Technologie is relatief goedkoop en dat komt niet alleen de consumenten ten goede die met cards hun laptop of zelfs hun mobiele telefoon het grootste gedeelte van hun betalingen afhandelen. Commerciële partijen, zelfs de kleinere, hebben steeds eenvoudiger toegang tot krachtige technologie, vaak door het aangaan van partnerships met gespecialiseerde ondernemingen. In combinatie met een zekere liberalisering en transparantieverhoging van de markt die toetreding eenvoudiger maakt, noopt dit de spelers in de keten tot een voortdurende herbezinning op hun eigen rol en verdienmodel.

Hierna passeren enkele ontwikkelingen de revue die deze enorme technologische vlucht illustreren. Deze ontwikkelingen horen in ons model voornamelijk thuis in de eerste kolommen; met name in de productkanaalcombinaties is de veranderingsdynamiek zeer hoog.

Bitcoin

Bitcoins zijn een vorm van virtueel geld, ook wel aangeduid met de term *cryptocurrency*. Bezitters van bitcoins kunnen grensoverschrijdende betaaltransacties doen, zonder daarbij te hoeven steunen op traditionele aanbieders van betaaldiensten of afhankelijk te zijn van een regulerende centrale bank. Er wordt daarbij sterk gesteund op cryptografische technieken; de overdracht van een bitcoin vindt plaats door een digitale ondertekening van de gehele keten van transacties sinds het ontstaan van die bitcoin met de geheime sleutel van de bezitter. De creatie van bitcoins (het zogenaamde *mining*) is een mathematisch proces dat de introductie van nieuwe bitcoins in het 'monetaire' systeem reguleert en verdeelt over de tijd. Momenteel ▶

IT Auditor_13_03.indd 31 03/09/13 5:04 PM

Google Wallet

Google Wallet is een concept dat mobiel betalen mogelijk maakt, net als M-Pesa. Het stelt de gebruiker in staat credit- en debitcardgegevens door Google in de cloud op te laten slaan. Bij het doen van een aankoop online of in de 'reële wereld', kan de gebruiker via een app op zijn of haar mobiele telefoon een kaart selecteren en de betaling effectueren. Voor offline aankopen bij retailers wordt daarbij gebruik gemaakt van het contactloze NFC-protocol; de telefoonbezitter houdt zijn smartphone in de buurt van een speciale POS-terminal en de betaling wordt gedaan. Dit concept is qua technologie niet zeer schokkend maar er zit een enorm verdienpotentieel achter. Als geen ander is Google in staat context toe te voegen aan een aankoop [KING13] en anticipeert het bedrijf op de inkomsten van advertenties, aanbiedingen, en andere commerciële berichten die specifiek en zeer effectief op de betalende consument zijn gericht. Deze kunnen voor die betalende consument betekenisvol zijn op het moment dat hij of zij die context ontvangt.

worden ongeveer om de tien minuten 25 nieuwe bitcoins gegenereerd (de zogenaamde *block reward*); dit proces zal doorgaan tot een harde grens van 21 miljoen bitcoins zal zijn bereikt, waarbij het aantal bitcoins per block reward periodiek zal worden verkleind.

Het voert te ver op deze plaats uitgebreid in te gaan op de technische specificaties van bitcoins. In functionele zin is het een virtueel betaalmiddel dat als zodanig wordt gebruikt, niet in de laatste plaats vanwege het anonieme karakter van betalingen en het feit dat het zich onttrekt aan regulering door de gevestigde financiële sector. Als solide betaalmiddel/valuta zijn bitcoins aan fundamentele kritiek onderhevig. De koers is op zijn zachtst gezegd grillig en alhoewel er vele beurzen zijn waar bitcoins in traditionele valuta kunnen worden verhandeld, is er geen sprake van een zeer liquide markt. Ondanks die kritiek staan bitcoins sterk in de belangstelling, en worden ze door sommigen gezien als een eerste stap op weg naar een virtueel betaalmiddel dat de barrières van traditionele instrumenten wegneemt en daarmee betalingsverkeer verder vereenvoudigt. Een uitstekende beschouwing van deze aspecten is [SALM13].

Mobile Payments

Mobile payments zijn betalingen die met een mobiel apparaat worden geïnitieerd. Velen zien dit als een product met een al belangrijk heden en een enorme toekomst: een *disruptive technology* die het traditionele betalingsmodel fundamenteel gaat veranderen. De wereldwijde adoptie van mobiele apparaten is enorm, ook in landen waar de traditionele betalingsinfrastructuur niet heel sterk ontwikkeld is en banken niet op iedere hoek van de straat aanwezig zijn. Bovendien is sprake van een technologie die consumenten in staat stelt altijd *connected* te zijn. Sterker nog: de consument *wil* zijn betalingen kunnen doen, onafhankelijk van tijd en plaats, en met behulp van de krachtige smartphone in zijn binnenzak.

Mobile payments zijn er in vele verschillende vormen. Het kan gaan om een betaalopdracht die via de mobiel bankieren-app van een bank wordt geïnitieerd, maar ook om een *peer-to-peer* betaling via het mobiele kanaal van Paypal of Bitcoin. De aankoop van de laatste cd van David Bowie is in een handomdraai voor elkaar met een mobiele betaling in Apple's iTunes store. Arbeiders in den vreemde kunnen mobiele *money transfers* naar huis met een paar *swipes* op hun smartphone in gang zetten, en de mobiele telefoon kan dienen als een portemonnee om in de 'reële wereld' aankopen te doen, zoals met Google Wallet. Ondanks deze variëteit hebben mobile payments een gemeenschappelijk aspect: ze zorgen voor veranderingen in de betalingsverkeerketen en introduceren daarmee, zowel qua marktverhoudingen als qua risico's, nieuwe uitdagingen voor bestaande spelers. Banken krijgen concurrentie van aanbieders van mobiele telefonie. Creditcardmaatschappijen worden gedwongen tot innovaties om hun marktaandeel bij de *points of sale* (POS) niet te verliezen aan spelers als Apple of Google. Dit is in de twee kaders kort toegelicht aan de hand van de voorbeelden M-Pesa en Google Wallet.

INCIDENTEN

In conceptversies van dit artikel was een belangrijke plaats ingeruimd voor een opsomming van incidenten die het betalingsverkeer in het afgelopen twee jaar op een of andere manier hebben geraakt. We vonden dat van belang, om te onderstrepen dat bedreigingen voor de betalingsverkeerketen wel degelijk reëel zijn. De actualiteit van de afgelopen maanden heeft ons dat werk uit handen genomen. De Nederlandse grootbanken werden in april van dit jaar geplaagd door verstoringen, variërend van onbeschikbaarheid door DdoS-aanvallen tot dubbele boekingen en verkeerde saldostatements via het mobiele kanaal. Consumenten hadden daar last van en gaven ruimschoots uiting aan hun verontwaardiging via sociale media. Ook de pers liet zich niet onbetuigd en mat de problemen breed uit.

Alhoewel een uitgebreide opsomming van die gebeurtenissen dus niet meer nodig is om de realiteit van risico's te onderstrepen, is het wel zinvol er een paar woorden aan te wijden.

Op de eerste plaats is het belangrijk de incidenten naar soort te ordenen. Dat maakt een systematische bespreking mogelijk en geeft structuur, iets wat soms ontbrak in de veelheid aan berichtgeving. Het betalingsverkeer is in algemene zin kwetsbaar voor bedreigingen op het gebied van:

- beschikbaarheid van de ketenprocessen (bijvoorbeeld het internetkanaal).
- exclusiviteit van informatie (bijvoorbeeld transactie- en rekeninggegevens).
- integriteit van de gegevensverwerking (bijvoorbeeld de juiste aanpassing van een saldo als resultaat van een transactie).

De weergave van foutieve saldi via het mobiele kanaal (integriteit)

IT Auditor_13_03.indd 32 03/09/13 5:04 PM

leidde tot grote onrust bij rekeninghouders, en de DdoS-aanvallen zorgden ervoor dat klanten gedurende korte of langere tijd via het internetkanaal geen transacties konden laten uitvoeren (beschikbaarheid). Voor zover bekend is de exclusiviteit van bancaire gegevens in de 'incidentenmaand' april echter niet in gevaar geweest. De banken hebben daarbij steeds benadrukt dat de verstoringen zich voordeden door (op zichzelf herstelbare) verwerkingsfouten en in de netwerkperiferie; de bancaire backoffice-omgeving stond naar verluidt stevig en betrouwbaar overeind.

In de onrust en publiciteit stonden de banken en hun dienstverlening centraal. Dat is logisch, aangezien de incidenten zich daar voordeden en de banken nu eenmaal het primaire contactpunt zijn voor betalende consumenten. Dat neemt echter niet weg dat een betrouwbaar betalingsverkeer alleen mogelijk is door het goed functioneren van de gehele keten. Beveiliging en robuustheid van de banken zijn essentieel en dat daarop wordt aangedrongen is begrijpelijk en goed. Het mag echter niet verbloemen dat de keten zo sterk is als de zwakste schakel. Een meer integrale risicobenadering, waarbij de beveiliging en robuustheid van de gehele betalingsverkeerketen (inclusief de onderlinge afhankelijkheden van de verschillende partijen in die keten) onder het vergrootglas komt, verdient naar onze mening de voorkeur.

De incidenten hebben ook duidelijk gemaakt, dat het gemak waarmee individuen en organisaties hun betalingsverkeer heden ten dage kunnen uitvoeren een keerzijde heeft. Het intensieve en nog steeds toenemende gebruik van internet en mobiel om transacties te initiëren, heeft een maatschappelijke afhankelijkheid gecreëerd van een infrastructuur die praktisch inherent onbeheersbaar is. Voeg daarbij toe dat in het betalingsverkeer grote hoeveelheden geld omgaan (wat criminele activiteit aantrekt) en het om een groot maatschappelijk belang gaat (wat als een magneet werkt op activisme en terrorisme), en het wordt duidelijk dat we hier met een dreigingsprofiel te maken hebben dat enorm is en niet zal afnemen. Een 100 procent incidentloos betalingsverkeer is daarmee een illusie, en het is zinloos dit van de spelers in de keten te eisen. Een pleidooi voor een stevig en integraal risicobeheer in de keten, gericht op beveiliging, robuustheid, adequate communicatie, en snel herstel op het moment dat zich incidenten voordoen, is daarentegen zeker op zijn plaats.

TOT SLOT

Het betalingsverkeer is in toenemende mate kwetsbaar geworden voor verstoringen door de complexiteit in de keten waarin veel verschillende partijen (banken maar ook intermediërende partijen en bedrijven) een rol spelen en technologische ontwikkelingen zeer snel gaan. Regulering heeft de toetredingsdrempels verlaagd voor nieuwe spelers naast de gevestigde financiële partijen. Technologische innovaties stellen voortdurend nieuwe uitdagingen aan de beheersing van risico's in de keten. Het betalingsverkeer is in hoge mate een doelwit voor bedreigingen zoals cybercriminaliteit en de verwachting is dat dat zal zo blijven. De incidenten zoals die recent hebben plaatsgevonden zijn een *fact of life* en zullen niet geheel voorkomen kunnen worden.

Om hun kwetsbaarheid te verminderen, zullen de partijen in het betalingsverkeer niet alleen genoodzaakt zijn de robuustheid en betrouwbaarheid van hun eigen informatietechnologie op orde te hebben, maar zich ook rekenschap moeten geven van de afhankelijkheid van andere partijen in de keten. De interactie tussen partijen in de keten zal veel hoger moeten zijn en de coördinatie over de keten heen (bijvoorbeeld in het geval van grotere verstoringen) is van groot maatschappelijk belang. Het risicomanagement zal ketenbreed en continue moeten plaatsvinden om adequaat voorbereid te zijn op de toenemende dreiging van verstoringen en om de continuïteit van het betalingsverkeer te kunnen waarborgen. Uiteraard zijn er fora en overlegorganen waar verschillende spelers uit de betaalketen aanschuiven om (ook) over risicobeheersing te praten. Men kan zich echter afvragen of de grote onderlinge afhankelijkheden van partijen in de keten niet rechtvaardigen dat er een stevigere 'ketenvisie' op risicobeheersing vorm krijgt, ook van de zijde van de betrokken IT-auditors.

Voor IT-auditors betekent dit dat zij niet alleen de organisatiespecifieke risico's binnen de organisatie waarvoor zij werkzaam zijn moeten beoordelen, maar zich ook in sterke mate moeten gaan richten op de ketenbrede risico's. In het volgende deel van het artikel zullen we daarop verder ingaan.

De Kennisgroep Betalingsverkeer heeft de volgende leden, die gezamenlijk aan dit artikel hebben gewerkt:
Wandena Birdja-Punwasi
Peter Buur
Leon Dirks
Rocco Jacobs
Ed Ridderbeekx
Erus Schuurman ■

Literatuur

[DNB09] De Nederlandsche Bank, *Toelichting op Overlay Betaaldiensten*. http://www.dnb.nl/binaries/Toelichting_tcm46-223391.pdf.
[ECB13] European Central Bank. *Recommendations for "payment account access services".* http://www.ecb.int/press/pr/date/2013/html/pr130131_1_response.en.html.
[KING13] King, Brett. *Bank 3.0.* Marshall Cavendish 2013.
[RAMB08] Rambure, Dominique and A. Nacamuli. *Payment Systems. From the salt mines to the board room*. Palgrave MacMillan 2008.
[SALM13] Salmon, Felix. *The Bitcoin Bubble and the Future of Currency*. https://medium.com/money-banking/2b5ef79482cb.

Noot

IBAN: International Bank Account Number – rekeningnummer van achttien tekens, in het formaat van de internationale standaard, bijvoorbeeld: NL44RABO0123456789.
BIC: Bank Identifier Code – bankcode van 8 of 11 tekens, bijvoorbeeld: RABONL2U.

IT Auditor_13_03.indd 33 03/09/13 5:04 PM