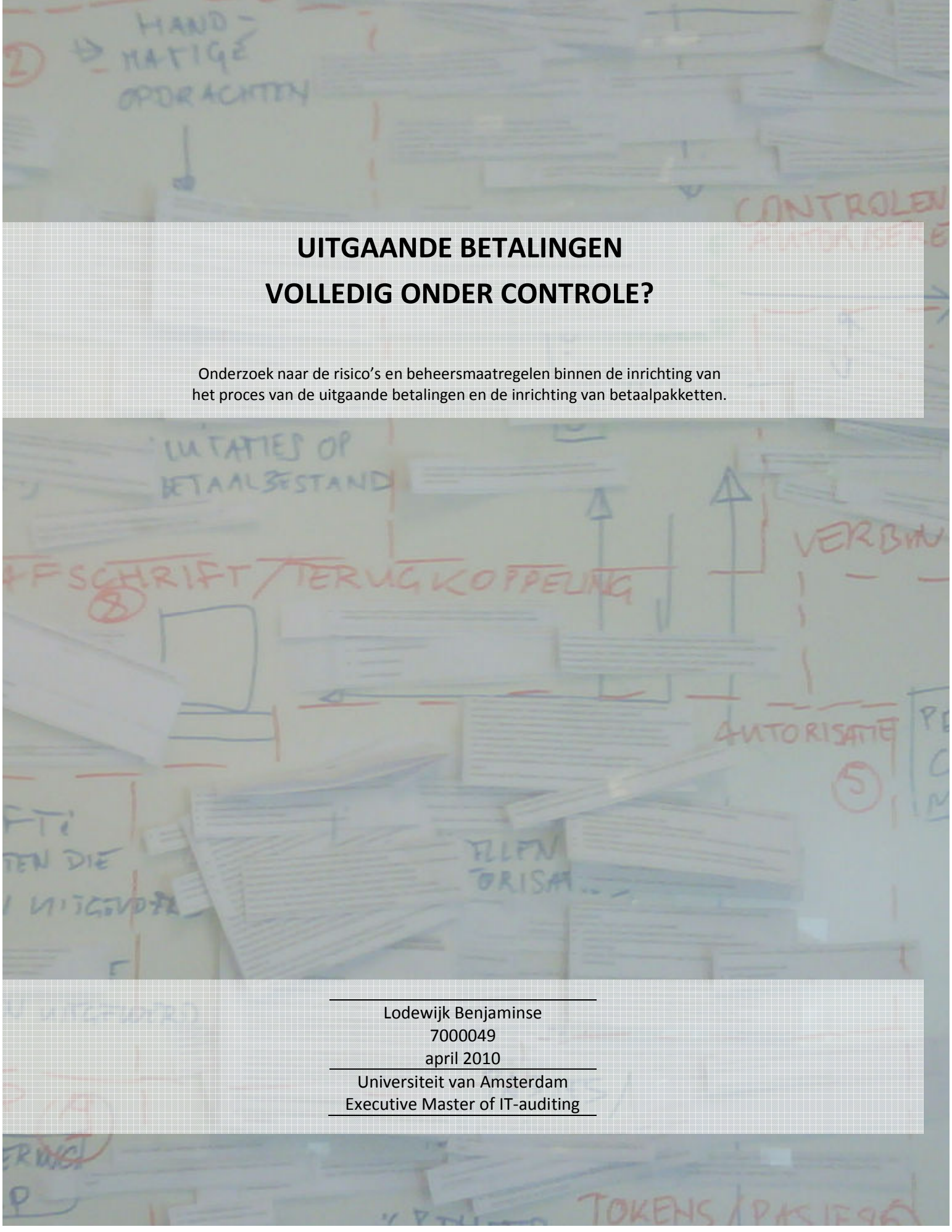


UITGAANDE BETALINGEN
VOLLEDIG ONDER CONTROLE?

Onderzoek naar de risico's en beheersmaatregelen binnen de inrichting van het proces van de uitgaande betalingen en de inrichting van betaalpakketten.

Lodewijk Benjaminse
7000049

april 2010

Universiteit van Amsterdam
Executive Master of IT-auditing

UITGAANDE BETALINGEN
VOLLEDIG ONDER CONTROLE?

Onderzoek naar de risico's en beheersmaatregelen binnen de inrichting van het proces van de uitgaande betalingen en de inrichting van betaalpakketten.

auteur:	drs. ing. L. Benjaminse l.benjaminse@gmail.com 7000049
begeleider:	drs. H. van Gils RE RA
datum:	april 2010
titel:	**Uitgaande betalingen onder controle?**
ondertitel:	Onderzoek naar de risico's en beheersmaatregelen binnen de inrichting van het proces van de uitgaande betalingen en de inrichting van betaal-pakketten
universiteit:	Universiteit van Amsterdam Executive Master of IT-auditing Plantage Muidergracht 12 1018 TV AMSTERDAM

Voorwoord

Voor u ligt mijn referaat dat is geschreven teneinde de opleiding Executive Master of IT-auditing aan de Universiteit van Amsterdam af te ronden. Dit referaat gaat over de risico's in het betaalproces en heeft als eindproduct een normenstelsel. Het beschrijft achtereenvolgens de literatuurstudie naar het betalingsverkeer, het proces van uitgaande betalingen en de bezoeken die ik aan enkele organisaties heb gebracht.

Hierbij bedank ik mijn begeleider Herman van Gils voor het kritisch meedenken en meelezen. Zijn tips zorgden voor een goede structuur en evenwicht tussen alle onderdelen van dit referaat.

Dennis Versteeg heeft met zijn kennis over betalingsverkeer mij goede tips gegeven die ik in het referaat heb verwerkt.

Tevens wil ik de medewerkers van diverse organisaties die zo vriendelijk waren mij te woord te staan bedanken voor hun gastvrijheid. Dit was erg interessant en heeft mij veel nuttige informatie opgeleverd. Niet alleen heb ik daardoor kennis opgedaan over betaalprocessen en betaalpakketten, ook heb ik de organisaties inzicht kunnen geven in de risico's in hun betaalproces.

Lodewijk Benjaminse

april 2010

Inhoudsopgave

1 Inleiding

In discussies over het belang van het bestuderen van het proces van uitgaande betalingen zijn reacties als “het zal zo’n vaart niet lopen” vaak gehoord. Diverse auditors geven aan dat ze wel “om het betaalpakket heen” controleren en organisaties zelf reageren met “de crediteur belt vanzelf wel een keer” als er iets mis gaat. In wet- en regelgeving, richtlijnen en raamwerken vindt men echter diverse aanknopingspunten om meer aandacht aan het betaalproces te besteden dan momenteel het geval is. Tevens is het betaalproces binnen de jaarrekeningcontrole een belangrijk onderdeel. Uiteraard is het voor de organisatie zelf ook van belang het proces van uitgaande betalingen te beheersen om zo te voorkomen dat ten onrechte geld aan de organisatie wordt onttrokken.

1.1 Aanleiding

In 2008 was er wereldwijde sprake van een flinke toename van het aantal fraudegevallen. Dat jaar steeg het verlies door fraude met gemiddeld 22 procent. CTO’s zijn alerter op de mogelijkheden van fraude dan CEO’s en CFO’s. Gebleken is dat organisaties met een slechte interne controle slachtoffer kunnen worden van fraude. Er valt veel te verbeteren op het gebied van IT en databeveiliging.[1] [2] Uit een onderzoek van Ernst & Young blijkt dat 55 procent van de respondenten verwacht dat het aantal fraudegevallen de komende jaren zal toenemen. Dit wordt door 20 procent verklaard door het gebrek aan control. De meerderheid stelt dat fraude voorkomen kan worden door zowel interne als externe audits en betere beheersmaatregelen.[3]

De opdrachtgever van de betaalopdracht zelf is gebaat bij een goed ingericht proces van uitgaande betalingen. Indien er niet voldoende beheersmaatregelen in het betaalproces zijn opgenomen, bestaat de kans dat niet tijdig wordt ontdekt dat een medewerker frauduleus bezig is, zie ook paragraaf 1.2 voor een voorbeeld. Dit kan door langere tijd te slepen of in één keer een groot bedrag aan de organisatie te onttrekken. Naast het geld dat de organisatie mogelijk blijvend kwijt is, levert dit boze leveranciers en werknemers op die hun geld niet ontvangen. Dit kan uiteindelijk ontaarden in reputatieschade en imagoschade.

Tevens wordt in diverse wet- en regelgeving, richtlijnen en in raamwerken op eigenschappen cq. elementen van het betaalproces gewezen. Dit gebeurt vanuit verschillende invalshoeken, zoals richtlijnen voor banken (Risk management principles for electronic banking), goed beheer van gegevens (Code van informatiebeveiliging en COSO ERM), privacy (Wet Bescherming Persoonsgegevens) en fraude (NV COS).

Binnen de jaarrekeningcontrole wordt veelal “om het betaalpakket heen” gecontroleerd. Dit wordt gecompenseerd door controlewerkzaamheden tijdens de jaarrekeningcontrole op basis van de verstuurde betaalopdrachten, bankafschriften en standaard bankverklaringen. Vanuit het oogpunt van fraude is het proces van uitgaande betalingen echter weldegelijk van belang voor de accountant. Fraude wordt in het Besluit toezicht accountantsorganisaties[4] en NV COS[5] omschreven als het “opzettelijk handelen of nalaten waarbij misleiding wordt gebruikt om een wederrechtelijk voordeel te behalen”. Hieraan wordt toegevoegd dat “de

[1] Kluwer, “Meer fraude door kredietcrisis”, oktober 2008 (http://www.kluwerfinancieelmanagement.nl/?subject=article&id=129)
[2] Kroll, “Global Fraud Report”, 2008 (http://www.kroll.com/library/fraud/FraudReport_English-US_Sept08.pdf)
[3] Ernst & Young, “European fraud survey 2009: is integrity a casualty of the downturn?”, 2009 (http://www2.eycom.ch/publications/items/fraud_eu_2009/European_Fraud_Survey.pdf)
[4] Overheid.nl, “Besluit toezicht accountantsorganisaties”, oktober 2009 (http://wetten.overheid.nl/BWBR0020184)
[5] NIVRA, “Handleiding regelgeving accountancy: NV COS”, p. 21

aard of de omvang zodanig is dat beslissingen die in het maatschappelijk verkeer worden genomen op grond van de financiële verantwoording van de controlecliënt zouden kunnen worden beïnvloed door die misleiding". De accountant dient echter alleen alert te zijn op frauduleuze handelingen wanneer die "een afwijking van materieel belang in de financiële overzichten veroorzaken". Daarom hoeven accountants niet vast te stellen of er in juridische zin fraude heeft plaatsgevonden, maar alleen of deze van materiele omvang is.[6]

Tevens wijst Starreveld[7] er op dat het betaalproces "dient te worden omgeven met bijzondere preventieve en repressieve controlemaatregelen, die er op gericht zijn zoveel mogelijk te voorkomen dat onrechtmatige of onjuiste betalingen worden verricht, respectievelijk achteraf vast te stellen dat alleen op grond van gecontroleerde en goedgekeurde inkoopfacturen rechtmatig erkenbare betalingen zijn verricht en dat die juist en op het juiste tijdstip zijn uitgevoerd".

1.2 Praktijkvoorbeeld

Hieronder staat het (iets aangepaste[8]) artikel "Het banksaldo aangevuld" uit Accountant[9] dat illustreert hoe (relatief) eenvoudig het in de praktijk is fraude te plegen bij uitgaande betalingen. In dit voorbeeld wordt aangegeven hoe door het muteren van bankrekeningnummers in betaalvoorstellijsten en bijwerken van tussenrekeningen werd gefraudeerd.

Een onderneming maakt bij het verrichten van betalingen gebruik van een betaalpakket. Het betaalproces is als volgt ingericht. Een medewerker van de administratie stelt vanuit de crediteurenadministratie een zogenaamde betaalvoorstellijst op. De medewerker geeft dit overzicht aan de directeur, inclusief de onderliggende facturen. De directeur controleert het overzicht met de onder liggende bescheiden en keurt de betalingen in het betaalpakket goed. Hierna vindt (geautomatiseerd) de betaling plaats.

Recentelijk is de onderneming gestuit op een aantal vreemde betalingen. Nader onderzoek heeft uitgewezen dat de medewerker verantwoordelijk voor het opstellen van de betaalvoorstellijst voor ruim één miljoen euro heeft gefraudeerd. Hoe? De medewerker wijzigde na aanmaak van de betaalvoorstellijst in het betaalpakket de naam en het bankrekeningnummer van de crediteur in zijn eigen naam en bankrekeningnummer. De directeur kreeg echter het oude ongewijzigde bestand, stelde vast dat het overzicht aansloot met de facturen en keurde de betaling goed. Hij was zich er niet van bewust dat de gegevens in het betaalpakket waren gewijzigd en dat in werkelijkheid de bedragen werden overgemaakt aan de fraudeur. Nadat de betaling was verricht werd het betaaloverzicht door de fraudeur op zodanige wijze gemanipuleerd dat het weer de juiste crediteurengegevens bevatte. Hierna werd de crediteurenadministratie bijgewerkt.

Als facturen niet worden betaald, gaan na verloop van tijd natuurlijk de crediteuren klagen. Dit werd door de fraudeur op eenvoudige wijze voorkomen. De fraudeur liet de facturen nogmaals betalen, maar nu op het juiste bankrekeningnummer. De directeur had dit toch niet door. Er werden dagelijks zoveel betalingen verricht dat hij een dubbele betaling niet op zou merken. Daar de crediteur al was afgeboekt, werden de betalingen op een tussenreke-

[6] NIVRA, "Handleiding regelgeving accountancy: NV COS 240 (De verantwoordelijkheid van de accountant voor het onderkennen van het risico van fraude in het kader van de controle van financiële overzichten)", oktober 2009 (http://www.nivra.nl/Sites/nivra_site/HRA/200903/html/38351.htm)
[7] Starreveld, "Bestuurlijke informatieverzorging, deel 2A: fasen van de waardekringloop", 2005, p. 87
[8] Enkele begrippen zoals "electronic banking", "betalingssysteem", "electronic bankingsysteem", "betalingsbetaalvoorstellijst" en "betalingsproces" zijn aangepast aan de terminologie die in dit onderzoek wordt gehanteerd. Deze begrippen zijn vervangen door "betaalpakket", "betaalvoorstellijst" cq. "betaalproces".
[9] Accountant, "Het banksaldo aangevuld", R. de Groot, M. Grummel en B. Prins, januari 2008 (http://www.accountant.nl/Accountant/Fraude+in+praktijk/Het+banksaldo+aangevuld)

ning geboekt. Nu zou je natuurlijk verwachten dat de accountant dit bij zijn controle wel zou ontdekken. Een tussenrekening met een hoog saldo valt natuurlijk op. Maar ook dit was snel opgelost. Op het moment dat de accountant zijn controle aankondigde, schoonde de fraudeur de tussenrekeningen en boekte de bedragen over naar diverse kostenrekeningen. Hij gebruikte hiervoor kostenrekeningen waarvan de realisatie ruim onder het budget en de realisatie van vorig jaar lag, zodat een en ander bij een cijferbeoordeling door de accountant niet op zou vallen. De medewerker kon op deze wijze jarenlang zijn banksaldo aanvullen, zonder dat hij tegen de lamp liep.

Fraude in het betaalproces komt in de praktijk zeer veel voor. Dit is ook logisch, aangezien hier het geld de onderneming verlaat. Toch blijkt de accountant deze vorm van fraude in de praktijk maar zelden te ontdekken, terwijl het in veel gevallen om omvangrijke (materiële) bedragen gaat. Uit oogpunt van fraude is het betaalproces dan ook een proces dat de nodige aandacht van de accountant verdient.

1.3 Doelstelling

Dit onderzoek is er op gericht het proces van uitgaande betalingen beter onder controle te krijgen. De doelstelling van dit onderzoek luidt dan ook:

Het ontwerpen van een normenstelsel om de betrouwbaarheid van de beheersmaatregelen in het proces van uitgaande betalingen te toetsen.

Daarnaast kan dergelijk normenstelsel ook als leidraad dienen om beheersmaatregelen in het betaalproces in te richten en het betaalpakket te configureren. Tevens kunnen de beheersmaatregelen als normen / eisen worden gehanteerd bij het selecteren van een nieuw betaalpakket.

1.4 Onderzoeksvragen

Om de hierboven genoemde doelstelling op te lossen, zijn de volgende onderzoeksvragen geformuleerd:

1. **Hoe verloopt het betalingverkeer in Nederland en waar zitten in dat proces de risico's voor de opdrachtgever zelf?**

2. **Wat zijn de belangrijkste kenmerken van de meest gebruikte betaalpakketten?**

3. **Is een standaard aanpak (gelet op de kenmerken van deze betaalpakketten) haalbaar om de maatregelen binnen het proces van uitgaande betalingen te kunnen beoordelen?**

4. **Zo ja, welke audit werkzaamheden (a) dienen er in algemene zin te worden verricht en (b) moeten in enge zin per betaalpakket worden uitgevoerd? Zo nee, waarom is deze standaard aanpak niet haalbaar?**

1.5 Scope

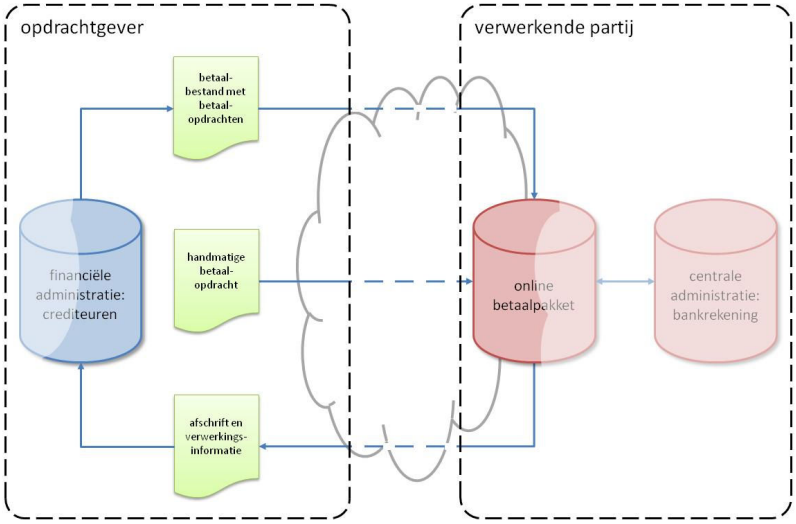
Het betaalproces staat in dit onderzoek centraal. Ondanks dat (volledigheidshalve) het gehele proces van uitgaande betalingen wordt omschreven in hoofdstuk 2, wordt verderop in dit onderzoek alleen gekeken naar dat deel van het betaalproces waar de organisatie (die de betaalopdrachten verstuurt) zelf op de inrichting invloed kan uitoefenen of beheersmaatregelen kan treffen.

In onderstaande figuren zijn de onderdelen die buiten de scope van dit onderzoek vallen lichter gekleurd, voor zowel het online betaalpakket (figuur 1) als een lokaal geïnstalleerd betaalpakket (figuur 2). In paragraaf 2.1.2 wordt uitgebreider op deze twee figuren ingegaan.

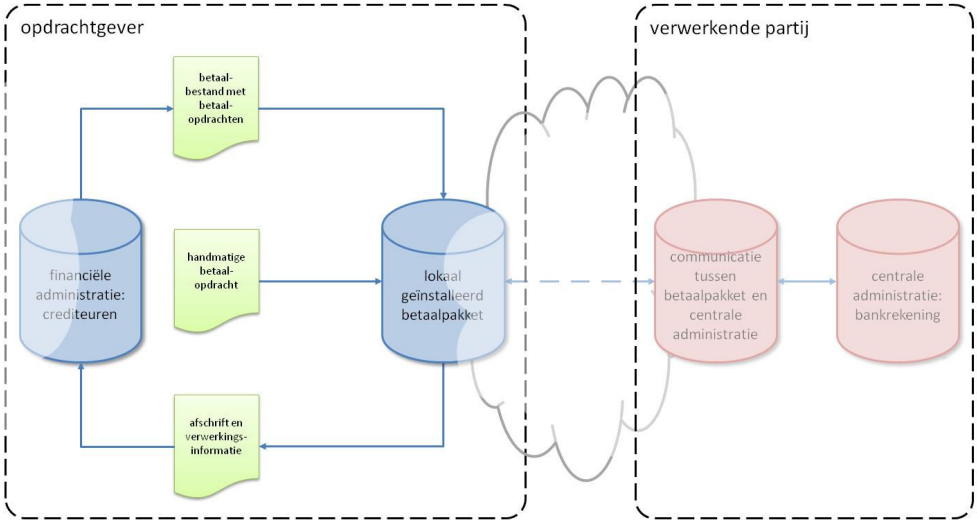
- Het proces van uitgaande betalingen start op het moment dat is bepaald dat aan een crediteur dient te worden betaald. Het proces eindigt daar waar de afschriften (met transactie- en saldoinformatie) en verwerkingsinformatie zijn verwerkt en de boeking in het grootboek heeft plaatsgevonden. In beide figuren is te zien dat de financiële administratie deels in scope is, alleen daar waar het de crediteurenadministratie betreft.

- Tevens geldt in beide situaties dat het betaalpakket alleen in scope is, daar waar de opdrachtgever (als gebruiker) daar invloed (bijvoorbeeld door configuratie) op kan uitoefenen.

- In de figuren is weergegeven dat de uitvoering van de betaalopdrachten door de verwerkende partij buiten de scope van dit onderzoek valt.



figuur 1: online betaalpakket op website van verwerkende partij



figuur 2: betaalpakket lokaal geïnstalleerd bij de opdrachtgever

1.6 Aanpak onderzoek en opbouw rapport

Voor het onderzoek zoals dat in hoofdstuk 1 is beschreven zijn aan de hand van de onderzoeksvragen de volgende stappen doorlopen:

- Op basis van literatuurstudie is in hoofdstuk 2 “Betalingsverkeer en betaalproces” beschreven hoe (in brede zin) het betalingsverkeer in Nederland is ingericht. Voor de organisatie die de betaalopdrachten verstuurd is (in enge zin) de inrichting van het proces van uitgaande betalingen beschreven. Tevens worden in dat hoofdstuk diverse wet- en regelgeving, richtlijnen en raamwerken besproken die van toepassing zijn op het betaalproces.

- Aan de hand van de uitkomsten van hoofdstuk 2 is in hoofdstuk 3 “Veldwerk“ nagegaan welke beheersmaatregelen in de praktijk worden aangetroffen. Door middel van bezoeken aan een aantal organisaties is zowel de inrichting van het betaalpakket als het betaalproces zelf bestudeerd.

- In hoofdstuk 4 “Totstandkoming normenstelsel” staat beschreven hoe de theorie en praktijk worden gecombineerd tot één normenstelsel.

- In hoofdstuk 5 zijn de samenvatting en de conclusies van dit onderzoek opgenomen. Daar worden tevens enkele suggesties gedaan voor toekomstig onderzoek ten einde het betaalproces beter in te richten.

Aansluitend zijn de volgende onderdelen opgenomen:

- In de literatuurlijst staan alle bestudeerde bronnen vermeld.

- In de bijlagen is een toelichting op de gehanteerde terminologie terug te vinden. De behandelde algemene voorwaarden volgen daarna. Als laatste is het volledige normenstelsel vermeld.

2 Betalingsverkeer en betaalproces

Om tot het normenstelsel te komen dienen eerst in brede zin het betalingsverkeer en in enge zin het proces van uitgaande betalingen in kaart te worden gebracht. Aan de hand daarvan worden de risico's inzichtelijk gemaakt en kunnen de beheersmaatregelen worden geformuleerd ten behoeve van het normenstelsel.

2.1 Betalingsverkeer in Nederland

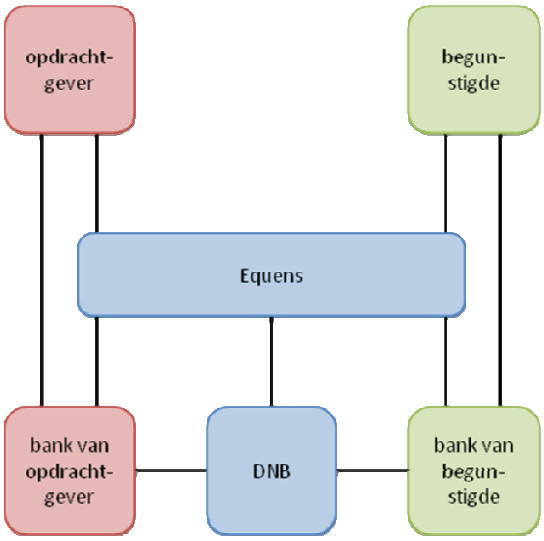
In Nederland is het betalingsverkeer ingericht volgens het *four party-model*, waar de volgende vier partijen een rol spelen: de opdrachtgever (*consumer*) en de begunstigde (*merchant*) met elk een bank (*issuing bank* cq. *acquiring bank*).

- De *issuing bank* regelt voor de *consumer* dat het geld wordt overgemaakt naar de bankrekening van de *merchant*.
- De *acquiring bank* onderhoudt de relatie met de *merchant* en zorgt er onder andere voor dat hij zijn geld ontvangt.

Hieronder wordt ingegaan op de specifieke indeling van het lokale betalingsverkeer in Nederland.

2.1.1 Betrokken partijen

Bij het betalingsverkeer zijn naast de twee banken, de opdrachtgever en de begunstigde de volgende partijen betrokken: DNB en Equens. De relaties tussen deze partijen zijn eveneens in onderstaand figuur weergegeven.



figuur 3: organisaties binnen het betalingsverkeer

In Nederland zijn de volgende partijen betrokken bij het betalingsverkeer:

- Als zelfstandig bestuursorgaan oefent DNB (De Nederlandsche Bank) prudentieel toezicht uit op financiële instellingen. DNB maakt onderdeel uit van het ESCB (Europees Stelsel van Centrale Banken) en is medeverantwoordelijk voor het vaststellen en uitvoe-

ren van het monetaire beleid in de landen die de euro hebben ingevoerd en voor taken in het betalingsverkeer.[10] DNB heeft een aantal taken, namelijk financiële stabiliteit, monetair beleid, betalingsverkeer, toezicht en economisch advies.[11] DNB ziet toe op een veilig en betrouwbaar betalingsverkeer, zowel chartaal als giraal.

Ten aanzien van het giraal betalingsverkeer onderhoudt DNB als centrale bank het betaalsysteem waarmee banken en effecteninstellingen onderlinge geldtransacties uitvoeren. Hierbij speelt de financiële stabiliteit een belangrijke rol.[12] Voor het mogelijk maken van dit betaalsysteem verwerkt DNB geldoverboekingen en beheert het bankrekeningen en saldi voor de financiële instellingen.[13]

Binnen het girale betalingsverkeer[14] onderscheidt men:

- Concernverkeer, waarbij een overboeking plaatsvindt tussen twee bankrekeningen bij dezelfde bank.
- Circuitverkeer, waarbij een overboeking plaatsvindt tussen twee bankrekeningen bij verschillende banken.
- Circuitoverschrijdend verkeer, waarbij een overboeking plaatsvindt tussen een bankrekening, die niet bij Equens is aangesloten en een bankrekening bij een andere bank, die wel is aangesloten bij Equens.

- Equens verwerkt als *automated clearing house* transacties in het elektronisch betalingsverkeer.[15] Equens is gemachtigd om namens de aangesloten banken hun bankrekeningen door DNB te laten debiteren en crediteren.[16]
- Banken houden een bankrekening aan bij DNB en ontvangen informatie van Equens over de transacties. De NVB behartigt de gemeenschappelijke belangen van de Nederlandse banken.[17] Zowel de opdrachtgever als de begunstigde heeft een bankrekening bij een bank. (Dit kan uiteraard dezelfde bank zijn.) Banken bieden betalingsmethoden en -producten aan zodat rekeninghouders geld kunnen overboeken tussen verschillende bankrekeningen.[18]
- Een opdrachtgever verstuurt een betaalopdracht om zo geld over te maken naar de begunstigde.

2.1.2 Betaalproces

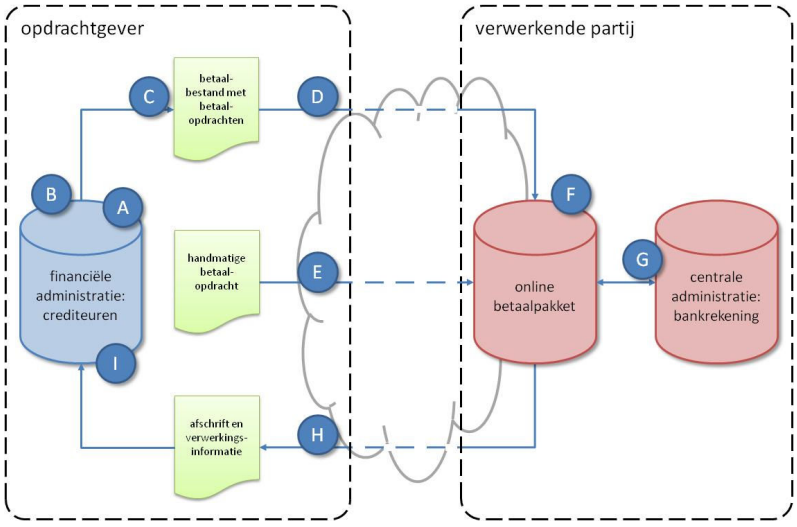
Hieronder wordt het gehele proces van uitgaande betalingen omschreven. De omschrijving van het proces begint bij het moment dat binnen de organisatie (opdrachtgever) is bepaald dat een bedrag aan een crediteur (begunstigde) dient te worden betaald. Er wordt daarbij vanuit gegaan dat deze betaalopdracht op een juiste wijze tot stand is gekomen, dus dat er

[10] DNB, “Partijen”, oktober 2009 (http://www.allesoverbetalen.nl/achtergrondinformatie/organisaties/partijen)
[11] DNB, “Taken”, oktober 2009 (http://www.dnb.nl/over-dnb/taken/index.jsp)
[12] DNB, “Betalingsverkeer: veilig en betrouwbaar”, oktober 2009 (http://www.dnb.nl/over-dnb/taken/betalingsverkeer/index.jsp)
[13] DNB, “Giraal betalingsverkeer”, oktober 2009 (http://www.dnb.nl/betalingsverkeer/giraal-betalingsverkeer/index.jsp)
[14] NVB, “Betalingen”, oktober 2009 (http://www.nvb.nl/index.php?p=17930)
[15] DNB, “Partijen”, oktober 2009 (http://www.allesoverbetalen.nl/achtergrondinformatie/organisaties/partijen)
[16] DNB, “Jaarverslag DNB 2008”, maart 2998, p. 128 (http://www.dnb.nl/binaries/JV DNB 2008_tcm46-214840.pdf)
[17] NVB, “Rol NVB”, oktober 2009 (http://www.nvb.nl/index.php?p=10822)
[18] Innopay, “Online betalen: internetbetalingen in Europa”, februari 2008, p. 38

bijvoorbeeld een geleverde dienst en/of product tegenover staat en dat deze gefiatteerd is door een daartoe geautoriseerd persoon. Aan het einde van het proces worden de afschriften (met transactie- en saldoinformatie) en verwerkingsinformatie verwerkt. Het proces eindigt vervolgens met een boeking in het grootboek, zie ook paragraaf 1.5.

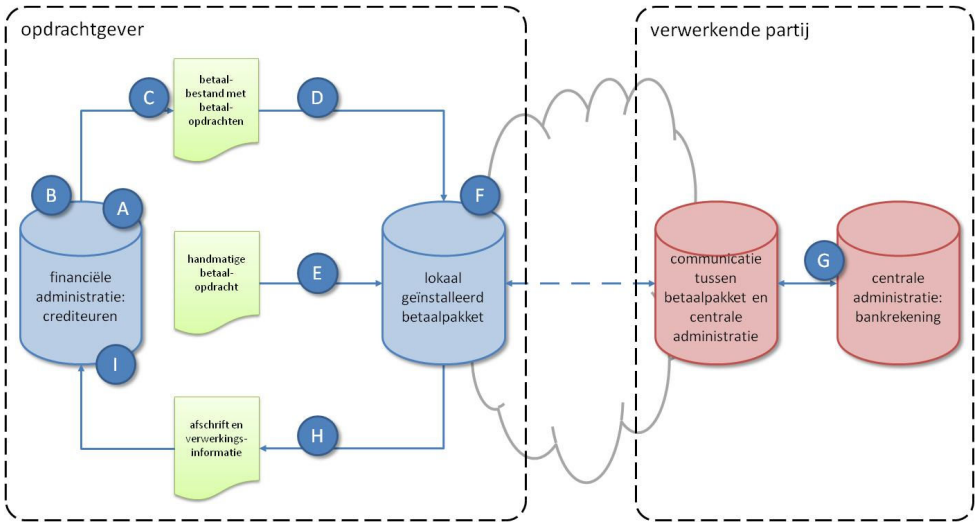
In onderstaande twee figuren zijn in het kort de stappen weergegeven die worden doorlopen bij versturen van betaalopdrachten via een betaalpakket. In het eerste geval is dit een online betaalpakket (figuur 4) en in het tweede geval betreft het een lokaal geïnstalleerd betaalpakket (figuur 5). In beide figuren is links door middel van de stippellijnen de organisatie weergegeven die de betaalopdrachten verstuurt. De verwerkende partij zelf is in beide figuren eveneens doormiddel van stippellijnen aan de rechter kant weergegeven: betaalopdrachten kunnen zowel aan Equens als aan een bank waar de opdrachtgever een bankrekening aanhoudt worden verstrekt. Communicatie tussen beide partijen vindt veelal via internet plaats.

1. De eerste figuur geeft de situatie weer waarbij het online betaalpakket via een website van de verwerkende partij (rechts) wordt benaderd. De betaalopdrachten worden vanuit de financiële administratie gegenereerd en geïmporteerd in het online betaalpakket of direct handmatig in het online betaalpakket ingevoerd. In de figuur is duidelijk zichtbaar dat het betaalpakket zich op een webserver binnen infrastructuur van de verwerkende partij bevindt. Vanaf de webserver wordt met de centrale administratie van de bankrekeningen (transacties en saldi) gecommuniceerd. Het online betaalpakket wordt door middel van een browser via internet benaderd voor zowel het invoeren van betaalopdrachten als het downloaden van de afschriften en de verwerkingsinformatie.



figuur 4: online betaalpakket op website van verwerkende partij

2. In de tweede figuur wordt een betaalpakket gebruikt dat lokaal bij de opdrachtgever is geïnstalleerd. Het lokaal geïnstalleerde betaalpakket ontvangt betaalopdrachten uit de financiële administratie of deze worden rechtstreeks ingevoerd. Daarvandaan worden betaalopdrachten naar de verwerkende partij verstuurd. Deze zal de betaalopdrachten in haar centrale administratie van bankrekeningen verwerken. De verwerkingsinformatie wordt vervolgens door de verwerkende partij beschikbaar gesteld in het lokaal geïnstalleerde betaalpakket.



figuur 5: betaalpakket lokaal geïnstalleerd bij de opdrachtgever

De letters A. tot en met G. in bovenstaande figuren verwijzen naar stappen in het proces van uitgaande betalingen in onderstaand tabel. Dit is een geaggregeerde weergave van de diverse activiteiten binnen dit proces. De details van die activiteiten worden in de volgende paragraaf (2.1.3) beschreven.

#	Processtap	Financiële administratie: crediteuren	Betaalpakket	Centrale administratie: bankrekeningen
A	betaalvoorstellijst aanmaken	√		
B	betaalbestand aanmaken	√		
C	betaalbestand exporteren	√		
D	betaalbestand importeren		√	
E	betaalopdracht invoeren		√	
F	betaalopdrachten versturen		√	
G	betaalopdrachten uitvoeren			√
H	afschriften en verwerkingsinformatie downloaden		√	
I	afletteren betalingen	√		

2.1.3 Processtappen

Hieronder is een omschrijving weergegeven van de activiteiten uit het proces van uitgaande betalingen. Deze is gebaseerd op literatuurstudie van Starreveld[19], die met name het betaalproces binnen de organisatie van de opdrachtgever beschrijft. Specifieke details ten aanzien van het betalingsverkeer worden door de partijen Equens[20], NVB[21], DNB[22] en het ministerie van Financiën[23] gegeven. Tevens heeft het veldwerk (zie hoofdstuk 3) er voor gezorgd dat deze omschrijving aansluit bij het gebruik van betaalpakketten in de praktijk.

Het betaalproces verloopt als volgt:

A. betaalvoorstellijst aanmaken

Het systeem genereert op basis van de crediteurenadministratie een lijst "per vervalperiode van alle reeds vervallen en in de betreffende periode te vervallen nog openstaande [...]bedragen". Tevens zal de lijst met benodigde liquiditeitsgegevens wordt gegenereerd. Nadat deze informatie aan de medewerker die hiervoor beschikkingsbevoegdheden heeft is overhandigd, kan deze medewerker de beslissing nemen welke worden betaald. Hij autoriseert de betreffende betaalopdrachten.[19]

B. betaalbestand aanmaken

"De aldus genomen besluiten worden vervolgens in het systeem ingevoerd, waarna de betaalopdrachten per betaalwijze gereed worden gemaakt."[19] Afhankelijk van het soort betaalbestand worden daarin controletotalen opgenomen. Deze controletotalen verwijzen veelal naar het totaalbedrag, aantal betaalopdrachten en de bankrekeningnummers.[20]

C. betaalbestand exporteren

Vanuit de financiële administratie worden de betaalopdrachten in een betaalbestand opgeslagen op een medium cq. netwerklocatie.

D. betaalbestand importeren

Vervolgens zal het betaalbestand in het betaalpakket worden geïmporteerd. Dit kan zowel een online betaalpakket als een lokaal geïnstalleerd betaalpakket zijn. Afhankelijk van het betaalpakket worden enkele controles uitgevoerd aan de hand van de in het betaalbestand opgenomen controletotalen. Idealiter voert het betaalpakket ook de elfproef uit op de bankrekeningnummers.

E. betaalopdracht invoeren

Bij de meeste betaalpakketten is het tevens mogelijk buiten de financiële administratie om handmatig betaalopdrachten aan te maken.

F. betaalopdrachten versturen

[19] Starreveld, "Bestuurlijke informatieverzorging, deel 2A: fasen van de waardekringloop", 2005, p. 87-99
[20] Equens, "CLIEOP cliënt opdrachten: bestandsbeschrijving", maart 2009 (http://www.equens.com/Images/CLIEOP NL.pdf)
[21] NVB, "Betalingen", oktober 2009 (http://www.nvb.nl/index.php?p=17930)
[22] DNB, "Jaarverslag DNB 2008", maart 2998 (http://www.dnb.nl/binaries/JV DNB 2008_tcm46-214840.pdf)
[23] Ministerie van Financiën, "Handboek betalingsverkeer Rijksoverheid", februari 2008 (http://www.minfin.nl/dsresource?objectid=2529)

De betaalopdrachten die zijn geïmporteerd cq. handmatig ingevoerd worden gecontroleerd aan de hand van de originele facturen en daarna aan de verwerkende partij aangeboden. Nadat de betaalopdrachten in het betaalpakket zijn gefiatteerd, worden deze verstuurd naar de verwerkende partij. “Iedere batch dient vergezeld te gaan van een opdrachtbrief.”[20] Deze opdrachtbrief bevat onder andere de controletotalen die betrekking hebben op de betreffende betaalopdrachten.

Het feit dat het betaalbestand met de betaalopdrachten is verzonden, wordt in de crediteurenadministratie verwerkt door dit op de juiste grootboekrekeningen te boeken. Op dit moment in het proces vindt dat veelal plaats op de grootboekrekeningen “crediteuren” en “betaling onderweg”.

G. betaalopdrachten uitvoeren

De verwerkende partij zal de betaalopdrachten zelf verwerken indien de bankrekeningen van de opdrachtgever en begunstigde bij deze bank worden aangehouden. De bank stelt vast dat het saldo toereikend is en de bankrekening niet is geblokkeerd.

Overige betaalopdrachten zet de verwerkende partij door naar het *clearing and settlement mechanism*. In het geval van binnenlandse betalingen is dat Equens.[21] “Equens vraagt de bank [...] om fiat voor het verwerken van zakelijke betalingen ten laste van uw rekening. De bank verleent een eventueel fiat onder andere op grond van de gegevens in de opdrachtbrief.”[20]

Vervolgens “stelt Equens periodiek [...] de bedragen vast die banken aan elkaar zijn verschuldigd namens de rekeninghouders [...] Dit wordt clearing genoemd. De clearingbedragen worden doorgegeven aan DNB, waar alle in Nederland gevestigde banken een rekening hebben [...] Equens is gemachtigd om deze rekeningen door DNB te laten debiteren en crediteren en daarmee de betalingen af te wikkelen”.[22] Dit laatste heet settlement.

H. afschriften en verwerkingsinformatie downloaden

“Nadat settlement heeft plaatsgevonden, informeren de banken hun eigen rekeninghouders over mutaties in hun banksaldo, op basis van de verwerkingsinformatie die zij van Equens ontvangen.”[22] De bank zal dit door middel van afschriften doen. Over de betaalopdrachten verstrekt de verwerkende partij tevens een rapport dat inzicht geeft over de betaalopdrachten die niet konden worden verwerkt.[19] “Tevens [wordt gerapporteerd over] posten [...] die Equens in eerste instantie wel heeft uitgevoerd doch die nadien door een bank zijn geretourneerd (de zogenaamde teruggebogen posten)”.[23]

I. afletteren betalingen

De organisatie stelt aan de hand van de verwerkingsinformatie van de verwerkende partij vast dat de betaalopdrachten juist en volledig zijn verwerkt. De verkregen informatie over transacties en saldi wordt aan de financiële administratie doorgeven zodat dit kan worden geboekt op de grootboekrekeningen “betaling onderweg” en “bank”. De betalingen die op de afschriften staan vermeld worden aan de hand van de eerder verzonden betaalopdrachten gecontroleerd.[19]

Voor alle activiteiten in de systemen geldt dat authenticatie en autorisatie van de gebruiker plaats moet vinden.[24] Dit kan op de volgende manieren geschieden:

- door middel van iets dat men 'weet': bijvoorbeeld een gebruikersnaam, het wachtwoord of een pincode
- met iets wat men 'heeft': bijvoorbeeld een token, een bankpas of een digitaal certificaat
- met behulp van iets wat men 'is': bijvoorbeeld een vingerafdruk, stemherkenning, iriscopie of gezichtsherkenning

Onder F. (betaalopdrachten versturen) en I. (afletteren betalingen) wordt over het boeken op de grootboekrekeningen "crediteuren", "betaling onderweg" en "bank" gesproken. In paragraaf 3.4 wordt uitgebreid ingegaan op de momenten in het betaalproces waarop de verschillende grootboekrekeningen kunnen worden gebruikt. Tevens worden de voor- en nadelen van diverse manieren om te boeken toegelicht.

In onderstaand tabel zijn de afzonderlijke activiteiten uit bovenstaande omschrijving samengevat.

#	Activiteit	Omschrijving
A	**betaalvoorstellijst aanmaken**	
01	**lijst met openstaande bedragen genereren**	Het systeem genereert op basis van de crediteurenadministratie een lijst per vervalperiode van alle reeds vervallen en in de betreffende periode te vervallen nog openstaande bedragen.
02	**overzicht van liquiditeitsgegevens genereren**	Lijst met benodigde liquiditeitsgegevens wordt gegenereerd.
03	**autoriseren betaalopdrachten**	De medewerker met beschikkingsbevoegdheden neemt de beslissing welke betaalopdrachten mogen worden betaald. Hij autoriseert de betreffende betaalopdrachten.
B	**betaalbestand aanmaken**	
04	**betaalopdrachten gereed maken in betaalbestand**	De betaalopdrachten worden per betaalwijze opgeslagen in een betaalbestand.
C	**betaalbestand exporteren**	
05	**betaalbestand opslaan**	Het betaalbestand met de betaalopdrachten wordt opgeslagen op een medium cq. netwerklocatie.
D	**betaalbestand importeren**	
06	**importeren betaalopdrachten**	Het betaalbestand wordt in het betaalpakket geïmporteerd.
E	**betaalopdracht invoeren**	

[24] Basel committee on banking supervison, "Risk management principles for electronic banking", juli 2003 (http://www.bis.org/publ/bcbs98.pdf), p. 13

#	Activiteit	Omschrijving
07	**handmatig betaalopdrachten aanmaken**	Het is mogelijk handmatig betaalopdrachten aan te maken in het betaalpakket.
F	**betaalopdrachten versturen**	
08	**betaalopdrachten fiatteren**	De betaalopdrachten worden gecontroleerd aan de hand van de originele facturen en daarna aan de verwerkende partij aangeboden.
09	**opdrachtbrief versturen**	De opdrachtgever verstuurt tevens een opdrachtbrief naar de verwerkende partij, met daarin een aantal controletotalen die op de betreffende betaalopdrachten zijn gebaseerd.
10	**betaalopdracht boeken**	Het feit dat het betaalbestand met de betaalopdrachten is verzonden, wordt in de crediteurenadministratie verwerkt door dit op de juiste grootboekrekeningen te boeken.
G	**betaalopdrachten uitvoeren**	
11	***book to book* betaalopdrachten verwerken**	De verwerkende partij zal de betaalopdrachten zelf verwerken indien de bankrekeningen van de opdrachtgever en begunstigde bij deze bank worden aangehouden.
12	**uitvoeren controles**	De bank stelt vast dat het saldo toereikend is en de bankrekening niet is geblokkeerd.
13	**doorsturen naar *clearing and settlement mechanism***	Overige betaalopdrachten zet de verwerkende partij door naar het *clearing and settlement mechanism*.
14	**fiat vragen bij de bank**	Equens vraagt de bank om fiat voor het verwerken van de betaalopdracht ten laste van de bankrekening van de opdrachtgever.
15	**machtiging controleren**	De bank controleert of de opdrachtgever gemachtigd is ten aanzien van de betreffende bankrekening.
16	**clearing**	Vervolgens bundelt Equens de gegevens van de betaalopdrachten per bank en verstrekt deze informatie naar de desbetreffende banken. Equens saldeert betalingen en ontvangsten per bank.
17	**settlement**	Equens laat de nostrorekeningen die alle banken in Nederland aanhouden bij de DNB debiteren en crediteren. Hiermee zijn de vorderingen en schulden verrekend.
H	**afschriften en verwerkingsinformatie downloaden**	
18	**rapporteren over verwerkte betaalopdrachten**	De bank zal daarna door middel van afschriften de uitgevoerde betalingen terugmelden. Over de betaalbestanden verstrekt de verwerkende partij tevens een rapport dat inzicht geeft over de betaalopdrachten die niet konden worden verwerkt. Tevens kunnen daarop posten voorkomen die in eerste instantie wel zijn uitgevoerd, maar die nadien door

#	Activiteit	Omschrijving
		een bank zijn geretourneerd.
19	**rekeningoverzicht opleveren met transactie- en saldoinformatie**	Er wordt een rekeningoverzicht met transactie- en saldoinformatie opgeleverd.
I	**afletteren betalingen**	
20	**controleren van betaalopdrachten**	De organisatie stelt aan de hand van de verwerkingsinformatie van de verwerkende partij vast dat de betaalopdrachten juist en volledig zijn verwerkt.
21	**afschriften en verwerkingsinformatie verwerken**	De verkregen informatie over transacties en saldi worden aan andere informatiesystemen doorgeven zodat dit kan worden geboekt op de grootboekrekeningen.
22	**betalingen controleren**	De betalingen die op de afschriften staan vermeld worden aan de hand van de eerder verzonden betaalopdrachten gecontroleerd.

2.2 Wet- en regelgeving, richtlijnen en raamwerken

Aan de hand van diverse bronnen is nagegaan welke eisen worden gesteld binnen het proces van uitgaande betalingen. De uitkomsten hiervan zijn uiteindelijk verwerkt in het normenstelsel.

- Inrichten van het betaalproces:
    - Ondanks dat de adviezen in Risk management principles for electronic banking vanuit het perspectief van de banken zijn geformuleerd, vormt dit een goede bron voor beheersmaatregelen in het betaalproces.
    - Verder richten raamwerken als de Code van informatiebeveiliging en COSO ERM zich op de inrichting van IT-omgevingen.
    - Relevante wet- en regelgeving is met name in de Wet Bescherming Persoonsgegevens opgenomen.
    - De verwerkende partijen schrijven in hun algemene voorwaarden diverse voorwaarden voor waaraan hun klanten dienen te voldoen.
- Beoordelen van beheersingsmaatregelen:
    - Vanuit de hoek van de IT-audit dienen de algemene IT beheersmaatregelen in acht te worden genomen.
    - Regelgeving die op accountancy van toepassing is in NV COS en Besluit toezicht accountantsorganisaties verwerkt.

De hierboven genoemde wet- en regelgeving, richtlijnen en raamwerken die impact hebben op de inrichting en het beoordelen van het betaalproces en het betaalpakket worden hieronder besproken.

2.2.1 Risk management principles for electronic banking

De Risk management principles for electronic banking[25] van Basel committee on banking supervison van Bank for international settlements zijn opgesteld om banken adviezen (*"risk management principles"*) mee te geven bij het inrichten van online betaalpakketten. Ondanks dat dit document is opgesteld vanuit het perspectief van de bank (als verwerkende partij) zelf, geeft het de gebruiker (als opdrachtgever) genoeg handvatten voor de inrichting van het betaalproces en het betaalpakket.

Onder *"security controls"* worden adviezen gegeven ten aanzien van de authenticatie van gebruikers, functiescheiding en autorisatie. *"The following issues are particularly pertinent: authentication, non-repudiation, data and transaction integrity, segregation of duties, authorisation controls, maintenance of audit trails [and] confidentiality of key bank information."*

2.2.2 Code van informatiebeveiliging

De Code van informatiebeveiliging is door het International Organisation for Standardisation en het International Electrotechnical Commission opgesteld en biedt een uitgebreide lijst aan beheersmaatregelen voor informatiebeveiliging. Informatiebeveiliging wordt daarin omschreven als de beveiliging van informatie tegen een breed scala van risico's.[26]

Er wordt in de Code van informatiebeveiliging verwezen naar wet- en regelgeving op het gebied van de beveiliging van gegevens, privacy, intellectueel eigendommen en de verwerking van gegevens:

- De organisatie dient te allen tijde rekening te houden met de gevolgen op de informatiebeveiliging door het versturen van gegevens via het internet. Betaalopdrachten worden via het internet naar de verwerkende partij verstuurd. Hierbij kan worden gedacht aan ongewenste mutaties (juistheid), publiekelijk bekend worden van de inhoud (vertrouwelijkheid) en de kans dat berichten niet of dubbel aankomen (volledigheid).

- Het overtreden van wet- en regelgeving dient te worden vermeden. Hier valt onder andere te denken aan wetgeving voor privacy.

- Medewerkers moeten op de hoogte worden gesteld van hun verantwoordelijkheden ten aanzien van informatiebeveiliging en geheimhouding. Tevens dienen zij op een gepaste wijze te worden gescreend.

2.2.3 COSO ERM

Het COSO ERM-raamwerk is een raamwerk voor administratieve organisatie en interne beheersing. Eén van de doelstellingen van dit raamwerk is *"safeguarding of resources"* ook wel bekend als*"safeguarding of assets"*. Er dienen volgens het COSO ERM-raamwerk dan ook beheersmaatregelen aanwezig te zijn die voorkomen dat bezittingen ten onrechte aan de organisatie worden ontrokken.[27] Het proces van uitgaande betalingen is in het bijzonder een proces waar bezittingen (geld) de organisatie verlaten.

[25] Basel committee on banking supervison, "Risk management principles for electronic banking", juli 2003 (http://www.bis.org/publ/bcbs98.pdf)
[26] British Standard, "Information technology: Security techniques, code of practice for information security management", juni 2005, p. viii
[27] Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management, Integrated Framework", september 2004, p. 38

2.2.4 Wet Bescherming Persoonsgegevens

De Wet Bescherming Persoonsgegevens schrijft voor dat organisaties persoonsgegevens op een zorgvuldige wijze verwerken, verstrekken en verzamelen (artikel 6, 7 en 8). In deze wet staat onder andere dat persoonsgegevens niet verwerkt mogen worden “op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen” (artikel 9). De verantwoordelijke organisatie dient “passende technische en organisatorische maatregelen” te nemen om “persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking”. Deze maatregelen dienen “een passend beveiligingsniveau” te garanderen “gelet op de risico’s die de verwerking en de aard van te beschermen gegevens met zich meebrengen” (artikel 13).

Aansluitend is bepaald dat een verwerkende partij voldoende waarborgen dient te bieden ten aanzien van “de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen” (artikel 14).[28]

Binnen het betaalproces worden op diverse momenten en locaties persoonsgegevens opgeslagen en verstuurd. In het begin worden gegevens van medewerkers verzameld om bijvoorbeeld salarissen en declaraties te kunnen betalen. Deze gegevens in de betaalopdrachten bevatten de namen van de betreffende medewerkers, hun bankrekeningnummers, de bedragen (netto salaris en declaraties) en een bijbehorende omschrijving.

2.2.5 Algemene voorwaarden

Organisaties dienen aan diverse voorwaarden van de verwerkende partij te voldoen. Dit staat omschreven in de algemene voorwaarden voor (zakelijk) internet bankieren. Deze voorwaarden zijn van invloed op de wijze waarop de organisaties het betaalproces inrichten.

De algemene voorwaarden van deze verwerkende partijen hebben veel met elkaar gemeen. De organisatie dient zelf controles uit te voeren ten aanzien van de juistheid, volledigheid en tijdigheid van de verwerking van de betaalopdrachten. Verder eist de verwerkende partij dat de organisatie over een beveiligde (internet)verbinding beschikt. Veelal hebben medewerkers van de organisatie persoonlijke authenticatiemiddelen waarvan men alle elementen geheim dient te houden en niet aan derden ter beschikking mag stellen.

2.2.6 Algemene IT beheersmaatregelen

De algemene IT beheersmaatregelen (*IT general controls*) zijn uiteraard ook van toepassing. Niet alleen op het betaalpakket zelf, maar (juist) op de gehele keten van betrokken systemen: zowel vóór als ná het betaalpakket. Vanaf het moment dat bijvoorbeeld het betaalbestand is aangemaakt moet worden vermeden dat deze kan worden gemuteerd.

Algemene IT beheersmaatregelen worden in de volgende vier categorieën ingedeeld:

Categorie	Onderwerpen
Access to programs and data	Hieronder vallen onderwerpen als fysieke en logische toegangsbeveiliging. Tevens zijn binnen “access to programs and data” autorisaties, identificatie en authenticatie opgenomen.
Program changes	Onder “program changes” vallen aspecten die met het testen, goedkeuren en migreren van de wijzigingen aan de programmatuur hebben te maken.

[28] Overheid.nl, “Wet bescherming persoonsgegevens”, oktober 2009 (http://wetten.overheid.nl/BWBR0011468)

Categorie	Onderwerpen
Program development	De ontwikkeling van programmatuur valt onder "program development" en kent onderwerpen als het scheiden van ontwerp, ontwikkelen, testen, goedkeuren en implementeren. Tevens wordt aandacht besteed aan de migratie van gegevens.
Computer operations	Onder "computer operations" zijn jobs, backup, herstel, uitwijk en het beheer van incidenten en problemen opgenomen.

2.2.7 NV COS en Besluit toezicht accountantsorganisaties

Binnen NV COS (Nadere voorschriften controle- en overige standaarden) van het Nivra en Besluit toezicht accountantsorganisaties wordt eveneens verwezen naar fraude. Fraude (van materieel belang) wordt in Besluit toezicht accountantsorganisaties[29] (artikel 36) gedefinieerd als "opzettelijk handelen [...] om een wederrechtelijk voordeel te behalen en waarbij de aard of de omvang zodanig is dat beslissingen die in het maatschappelijk verkeer worden genomen op grond van de financiële verantwoording van de controlecliënt zouden kunnen worden beïnvloed door die misleiding".

- NV COS 240[30] schrijft voor dat de accountant verantwoordelijkheid is voor "het onderkennen van het risico van fraude in het kader van de controle van financiële overzichten". Hierbij wordt voorgeschreven dat de accountant een "professioneel-kritische instelling" moet aannemen en "afwijking van materieel belang als gevolg van fraude" moet bespreken.

- De accountant dient "het risico van een afwijking van materieel belang als gevolg van fraude" in te schatten, zoals in NV COS 315[31] staat geschreven. Aansluitend daarop zal hij aanvullende controlewerkzaamheden moeten verrichten.

Zoals verderop zal blijken bevat het betaalproces diverse risico's, waaronder fraude. De accountant is verplicht inzicht te verkrijgen in de beheersmaatregelen die binnen het betaalproces zijn genomen, de omvang van het risico in te schatten en (indien nodig) aanvullende werkzaamheden te verrichten. De accountant steunt hierbij veelal op de IT-auditor die de beheersmaatregelen in kaart brengt.

[29] Overheid.nl, "Besluit toezicht accountantsorganisaties", oktober 2009 (http://wetten.overheid.nl/BWBR0020184)
[30] NIVRA, "Handleiding regelgeving accountancy: NV COS 240 (De verantwoordelijkheid van de accountant voor het onderkennen van het risico van fraude in het kader van de controle van financiële overzichten)", oktober 2009 (http://www.nivra.nl/Sites/nivra_site/HRA/200903/html/38351.htm)
[31] NIVRA, "Handleiding regelgeving accountancy: NV COS 315 (Kennis van de entiteit en haar omgeving en het inschatten van het risico van een afwijking van materieel belang)", oktober 2009 (http://www.nivra.nl/Sites/nivra_site/HRA/200903/html/38644.htm)

3 Veldwerk

Om het betaalproces en de betaalpakketten in de praktijk te kunnen bestuderen, zijn diverse organisaties bezocht. Dit betrof organisaties in diverse sectoren (zowel publiek als privaat) en van zeer verschillende omvang:

- De in het onderzoek betrokken organisaties bevinden zich in de volgende sectoren: voedingsmiddelenindustrie, diverse onderdelen binnen de overheid (gezondheidszorg, onderwijs, ministeries, ...) en bouwsector.
- Het aantal personeelsleden varieert van circa 1.500 tot 75.000.
- De hoogste omzet binnen deze organisaties bedraagt 9 miljard euro.

Met diverse medewerkers van deze organisaties zijn interviews gehouden. Dit betrof veelal enerzijds technisch en functioneel beheerders en anderzijds een medewerker en het hoofd van de administratie cq. de directie van de organisatie. Tijdens de interviews is eerst het proces besproken aan de hand van de processtappen zoals die in paragraaf 2.1.3 staan omschreven. Aan de hand van die processtappen is op de specifieke situatie bij die betreffende organisatie ingegaan. Vervolgens zijn die processtappen met de medewerkers die normaliter ook bij het betaalproces zijn betrokken van begin tot eind doorlopen. Hierbij zijn eveneens de beheersmaatregelen uit de theorie (zie hoofdstuk 2) besproken. Naderhand zijn in aparte gesprekken de geconstateerde risico's met de betreffende medewerkers besproken.

Tevens zijn enkele gesprekken gevoerd met IT-auditors en accountants over het belang van het beoordelen van de beheersmaatregelen in het betaalproces.

3.1 Bewustwording

Uit de interviews die zijn gehouden komt naar voren dat de kennis binnen organisaties over het proces van uitgaande betalingen en de betaalpakketten zelf en de bijbehorende risico's zeer gering is. Dit komt onder andere bij de volgende waarnemingen terug:

- Organisaties denken te snel dat in het betaalproces voldoende beheersmaatregelen zijn getroffen en dat het "zo'n vaart niet zal lopen". In de praktijk blijken er nog legio (andere) risico's te bestaan waarvan men niet op de hoogte is.
    - Veel medewerkers die verantwoordelijk zijn voor het betaalproces hebben nog nooit een betaalbestand geopend. (Dit kan gewoon in de eenvoudigste tekstverwerker.) Als men informatie kennis zou nemen van de opbouw van het bestandsformaat, zou men zich snel van de risico's bewust zijn. Zo bevatten veel betaalbestanden controletotalen voor het aantal betaalopdrachten, het totale bedrag en de som van de bankrekeningnummers. Deze controletotalen zijn – na het aanpassen van de betaalopdrachten – op eenvoudige wijze opnieuw zelf te berekenen en in het betaalbestand op te slaan. Indien er wordt vastgesteld dat deze controletotalen niet zijn gemuteerd, geeft dit echter (nog steeds) geen zekerheid dat de bedragen binnen het betaalbestand niet zijn gemuteerd. Het is immers ook mogelijk het controletotaal gelijk te laten en toch bedragen binnen het betaalbestand te muteren. Een controle op de som van de bedragen zal dit niet kunnen vaststellen. In onderstaand figuur wordt aangetoond dat twee bedragen kunnen worden gemuteerd terwijl het controletotaal gelijk blijft.

      In het voorbeeld wordt een groot deel van het bedrag van de vierde regel naar de zesde regel 'verplaatst', terwijl het controletotaal gelijk blijft. Hierdoor zal dit bedrag naar een andere bankrekening worden overgemaakt.

bankrekeningnummer	bedrag
346625653	8,20
456254624	140,24
256728652	93,16
356835683	3.643,21
869835653	453,23
947675355	2.465,34
	6.803,38

bankrekeningnummer	bedrag
346625653	8,20
456254624	140,24
256728652	93,16
356835683	0,21
869835653	453,23
947675355	6.108,34
	6.803,38

figuur 6: muteren van bedragen terwijl het controletotaal (som van de bedragen) gelijk blijft

- Men neemt onbewust hoge risico's door onbekendheid met (de risico's van) IT. Zo werd de situatie aangetroffen waar het betaalbestand (met daarin de salarisbetalingen) onversleuteld per email van de ene computer via een extern emailadres naar een andere computer werd verstuurd. Vanaf deze laatste computer werd het betaalbestand vervolgens ingelezen in het online betaalpakket. Dat onversleuteld emailverkeer over het internet naar een extern emailadres als inherent onveilig wordt beschouwd is blijkbaar niet bekend bij die organisatie.
- Tevens blijkt dat de functionaliteiten en beperkingen van de betaalpakketten niet volledig bekend zijn. Hierdoor is men enerzijds onbekend met de risico's die het betaalpakket met zich meebrengt. Tegelijkertijd is men zich er anderzijds niet van bewust welke beheersmaatregelen met het betaalpakket kunnen worden ingericht.

- Er heerst veelal een groot vertrouwen in eigen medewerkers cq. collega's: PIN-codes worden gedeeld met collega's en passen worden bij de PIN-codes bewaard. Daarnaast worden er minimale controles op juistheid van de betaalopdrachten uitgevoerd en vindt vastlegging van deze controles nauwelijks plaats. In sommige gevallen worden slechts de bedragen van een paar facturen gecontroleerd of wordt alleen het controletotaal beoordeeld.
- Tijdens het veldwerk viel regelmatig van accountants te horen dat voor de jaarrekeningcontrole de afschriften van de bank met de financiële administratie worden aangesloten. Een veelgehoord argument vanuit de organisaties was dat "de crediteur vanzelf wel een keer belt" als hij zijn geld niet (op tijd) krijgt. Medewerkers die betrokken zijn bij het betaalproces die voor dit onderzoek zijn geïnterviewd reageerden verrast dat het betaalpakket "eindelijk ook een keer" werd bekeken. Als het bewustzijn en de druk op de verantwoordelijke medewerkers zouden worden verhoogd, zou er door organisaties wellicht meer aandacht aan het betaalproces worden besteed.

3.2 Algemene voorwaarden

De verwerkende partijen schrijven voorwaarden voor waar de organisatie die het betaalpakket gebruikt aan moet voldoen. De algemene voorwaarden hebben veelal het volgende gemeen:

- De organisatie blijft te allen tijde zelf verantwoordelijk voor de juistheid, volledigheid en tijdigheid van de verwerking van de betaalopdrachten. De verwerkende partij is niet zelf verantwoordelijk voor de betrouwbaarheid van het verwerken van betaalopdrachten.

  Hierbij rijst de vraag of een organisatie genoeg informatie en middelen aangereikt krijgt van de verwerkende partij om de benodigde controles überhaupt zelf uit te kunnen voe-

ren. Niet alle verwerkende partijen vermelden namelijk controletotalen of hashtotalen na het importeren van het betaalbestand. Tevens blijken de gehanteerde bestandsformaten (zoals CLIEOP03) niet voldoende beveiliging te bieden tegen mutaties.

- De organisatie moet zelf vaststellen dat de communicatie over een beveiligde (internet)verbinding plaatsvindt. Hierbij is de vraag in welke mate hij daar invloed op kan uitoefenen en welk soort beveiliging door de betaalapplicatie cq. webserver wordt toegepast.

- De verwerkende partij stelt de organisatie authenticatiemiddelen ter beschikking. Dit kan iets zijn wat men 'weet' (bijvoorbeeld een gebruikersnaam, het wachtwoord of een pincode), wat men 'heeft' (bijvoorbeeld een token, een bankpas of een digitaal certificaat) of wat men 'is' (bijvoorbeeld een vingerafdruk, stemherkenning, iriscopie of gezichtsherkenning). Authenticatiemiddelen zoals vingerafdruk of iriscopie worden vooralsnog niet gebruikt door verwerkende partijen. Tevens verschillen de gehanteerde authenticatiemiddelen van de banken onderling zeer weinig. Veelal blijft het bij een gebruikersnaam cq. -code, geheime PIN-code met een token, calculator of generator eventueel in combinatie met een pas met een chip.

- De organisatie kan aan de hand van de algemene voorwaarden weinig zekerheid ontlenen ten aanzien van de beschikbaarheid of correcte werking van de programmatuur van het internetbankieren. Voor fouten legt de verwerkende partij de verantwoordelijkheid naast zich neer, tenzij er sprake is van opzet of grove schuld. De vraag is wel, hoe de gebruiker opzet of grove schuld kan aantonen aangezien deze weinig tot geen inzicht heeft in de gegevens van de verwerkende partij.

Ondanks dat er geen heel concrete voorschriften zijn waar verwerkende partijen die elektronische betaaldiensten aanbieden zelf aan moeten voldoen, wordt in Risk management principles for electronic banking[32] banken wel geadviseerd een aantal zaken op orde te hebben. Er wordt echter keer op keer benadrukt dat dit geen harde vereisten zijn die als standaard of *best practice* zouden moeten worden gehanteerd. Dit betreft onder andere beheersmaatregelen op het gebied van authenticatie, niet-weerlegbaarheid, integriteit, functiescheiding, autorisatie en audit trails.

Ondanks dat het Basel committee on banking supervison de bank adviseert *"risk management principles"* te hanteren, leggen banken een groot deel van de verantwoordelijkheid via de algemene voorwaarden bij hun klanten (de gebruikers) neer.

3.3 Betaalpakketten

Gedurende de bezoeken aan de organisaties zijn tevens de belangrijkste eigenschappen van de betaalpakketten in kaart gebracht. Deze eigenschappen zijn van belang voor het bepalen van de risico's en de benodigde beheersmaatregelen.

Om meer over de betaalpakketten te weten te komen is ook geprobeerd handleidingen van de betaalpakketten te bestuderen. De algemene voorwaarden voor zakelijk internet bankieren zijn in dit onderzoek wel aangetroffen op de website van de banken, zie paragraaf 3.2. Handleidingen van de betaalapplicaties zijn echter niet te vinden. Als er al iets is aan docu-

[32] Basel committee on banking supervison, "Risk management principles for electronic banking", juli 2003 (http://www.bis.org/publ/bcbs98.pdf)

mentatie, dan betreft het een korte demo of een informatiebrochure maar geen uitgebreide uitleg over de inrichting en configuratie van het betreffende betaalpakket.

De betaalpakketten die tijdens de bezoeken aan de organisaties zijn aangetroffen waren voornamelijk Access Online en Access Direct Client (ABN AMRO en Royal Bank of Scotland), Rabo Telebankieren Extra (Rabobank), Inside Business (ING) en BNG Betalingsverkeer (Bank Nederlandse Gemeenten).

Wat hierbij opviel is dat er een verschuiving plaatsvindt naar de online betaalpakketten, waarbij de lokaal geïnstalleerde betaalpakketten steeds minder worden gebruikt. Enkele banken geven zelfs aan met de ondersteuning van lokale versies te zullen stoppen.

Bankpakketten lijken qua functionaliteit en layout erg op elkaar. Desondanks bestaan er verschillen tussen de betaalapplicaties die de verwerkende partijen aanbieden. De grootste verschillen zitten voornamelijk in de volgende eigenschappen:

- De mate van detail waarmee de autorisaties kunnen worden ingericht. In de meest uitgebreide betaalpakketten is het mogelijk per persoon de rechten per scherm, bankrekening, authenticatiemiddel, ... te beheren. In de eenvoudigere betaalpakketten hebben alle gebruikers dezelfde rechten.

- Het beheren van gebruikers, autorisatie en authenticatiemiddelen voor het betaalpakket kan door de verwerkende partij of de organisatie zelf worden beheerd. Er zijn betaalpakketten waarbij de organisatie geheel zelfstandig nieuwe gebruikers kan opvoeren. Er zijn betaalpakketten waarbij de verwerkende partij het wijzigingen van gebruikers, authenticatiemiddelen en autorisaties grotendeels zelf uitvoert.

- De mogelijkheid om controles uit te voeren op basis van controletotalen en hashtotalen.

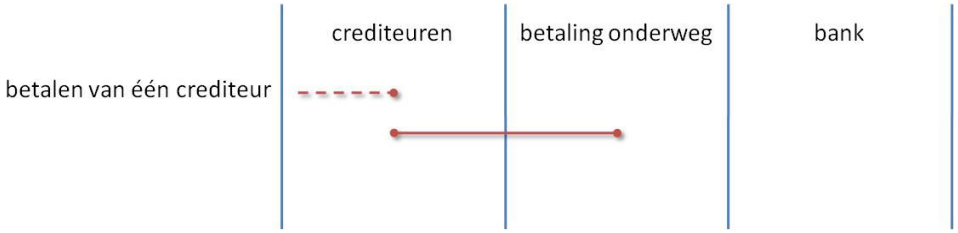
- Het in één keer (boeken en) betalen van alle betaalopdrachten uit betaalbestanden als één geheel kent enkele risico's. Per pakket verschilt het of er mogelijkheden zijn betalingen per afzonderlijke betaalopdracht uit te voeren.

3.4 Grootboekrekeningen

In de praktijk blijken uitgaande betalingen op verschillende momenten in het proces en op verschillende grootboekrekeningen te worden geboekt. Binnen het betaalproces moeten op enig moment boekingen worden gemaakt op de grootboekrekeningen "crediteuren", "betaling onderweg" en "bank".

Hierbij zijn de volgende aspecten van belang: enerzijds het moment waarop de grootboekrekening "crediteuren" wordt afgeboekt en anderzijds de wijze waarop de grootboekrekening "betaling onderweg" wordt gebruikt.

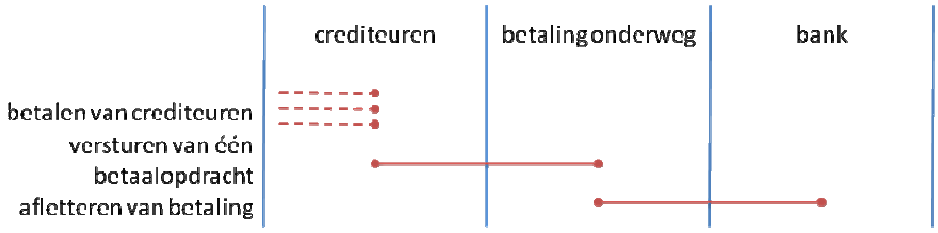
- Indien voordat de betaling aan de crediteur daadwerkelijk heeft plaatsgevonden, de grootboekrekening "crediteuren" al direct wordt afgeboekt, brengt dat risico's met zich mee.



figuur 7: boekingen op "crediteuren" en "betaling onderweg"

Het kan gebeuren dat de betaalopdrachten niet kunnen worden uitgevoerd. In de crediteurenadministratie lijkt het dan toch dat aan de betreffende crediteur is betaald. Tevens zal op de grootboekrekening een bedrag blijven openstaan. Een beheersmaatregel hiervoor is de verwerkingsinformatie te raadplegen en een procedure om niet uitgevoerde betaalopdrachten terug te boeken.

- Wanneer de te versturen betaalopdrachten in het betaalbestand als één geheel van de bankrekening worden afgeschreven en dit ook zo wordt geboekt op de grootboekrekening "betaling onderweg", is het achteraf onmogelijk met zekerheid vast te stellen dat de betalingen juist zijn uitgevoerd. De details van de (nog openstaande cq. uitgevoerde) betalingen per crediteur zijn immers niet meer bekend, noch in de eigen financiële administratie noch in de afschriften die de verwerkende partij verstrekt.



figuur 8: boekingen op "crediteuren", "betaling onderweg" en "bank"

Het afletteren zal dan op het niveau van het totaalbedrag van het betaalbestand plaatsvinden, er vanuit gaande dat van alle afzonderlijke betaalopdrachten de juiste bedragen naar de juiste bankrekening zijn overgemaakt. Er blijft in dit geval een risico bestaan dat betaalopdrachten niet juist zijn uitgevoerd.

4 Totstandkoming normenstelsel

Om tot het normenstelsel te komen zijn zowel de theorie uit hoofdstuk 2 als de ervaringen uit de praktijk die in hoofdstuk 3 staan beschreven gebruikt. In hoofdstuk 2 zijn de stappen uit het betaalproces en relevante wet- en regelgeving, richtlijnen en raamwerken die van toepassing zijn op dat betaalproces in kaart gebracht. Vervolgens zijn in hoofdstuk 3 de opvallendste zaken naar aanleiding van het veldwerk beschreven.

4.1 Wet- en regelgeving, richtlijnen en raamwerken

De wijze waarop de diverse bronnen die in paragraaf 2.2 zijn besproken in het normenstelsel zijn verwerkt is hieronder toegelicht:

4.1.1 Risk management principles for electronic banking

Onder *"security controls"* worden door het Basel committee on banking supervison van Bank for international settlements[33] een aantal adviezen gegeven ten aanzien van de inrichting van het betaalpakket. Drie voorbeelden van dergelijke adviezen die zijn meegenomen bij het opstellen van het normenstelsel zijn:

- *"Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications."*
- *"Banks should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications."*
- *"Banks should ensure that clear audit trails exist for all e-banking transactions."*

4.1.2 Code van informatiebeveiliging

De Code van informatiebeveiliging[34] kent diverse concrete normen die in het normenstelsel zijn opgenomen. Voorbeelden hiervan zijn:

- *"Duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets."*
- *"Data protection and privacy should be ensured as required in relevant legislation, regulations and, if applicable, contractual clauses."*

4.1.3 COSO ERM

COSO ERM-raamwerk richt zich op het instellen van een strategie en doelstellingen om "een optimale balans tussen groei, resultaat en gerelateerde risico's te realiseren en daarbij op effectieve en efficiënte wijze middelen inzetten om de ondernemingsdoelstellingen te realiseren" [35]. Dit raamwerken is echter dermate generiek dat hieruit geen concrete beheersmaatregelen zijn overgenomen in het normenstelsel.

[33] Basel committee on banking supervison, "Risk management principles for electronic banking", juli 2003 (http://www.bis.org/publ/bcbs98.pdf)
[34] British Standard, "Information technology: Security techniques, code of practice for information security management", juni 2005
[35] Committee of Sponsoring Organizations of the Treadway Commission, "Enterprise Risk Management, Integrated Framework", september 2004

4.1.4 Wet Bescherming Persoonsgegevens

De Wet Bescherming Persoonsgegevens[36] schrijft voor dat organisaties technische en organisatorische maatregelen nemen om een passend beveiligingsniveau te garanderen om zo verlies of onrechtmatige verwerking van persoonsgegevens te voorkomen. Deze wet schrijft voor dat organisaties passende technische en organisatorische beveiligingsmaatregelen moeten nemen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Concrete beheersmaatregelen noemt deze wet niet. De beveiliging van persoonsgegevens wordt echter grotendeels door “access to programs and data” uit de algemene IT beheersmaatregelen verzorgd.

4.1.5 Algemene voorwaarden

Hieronder staan enkele voorbeelden van voorwaarden vermeld die veel banken in hun algemene voorwaarden hebben opgenomen. Deze voorwaarden zijn eveneens in het normenstelsel opgenomen. Een uitgebreider overzicht van deze algemene voorwaarden van enkele banken is in de bijlagen opgenomen.

- “Een toegangsmiddel is uniek verbonden aan een natuurlijke persoon.”[37]
- “De cliënt is verplicht te controleren of zijn [...] opdrachten correct zijn uitgevoerd.”[38]
- “De klant mag een beveiligingscode nergens (schriftelijk) vastleggen of op zodanige wijze bewaren dat andere personen daarvan kunnen kennisnemen.”[39]
- “De rekeninghouder en gebruiker dienen, alvorens opdrachten te verzenden, te controleren of er sprake is van een beveiligde sessie met de bank.” [40]

4.1.6 Algemene IT beheersmaatregelen

Vanwege het hoge risico van het betaalproces zijn met name de beheersmaatregelen uit de categorie “access to programs and data” van groot belang. De categorie “program changes” is van alleen toepassing ten tijde van het testen en in gebruik nemen van het betaalpakket en wat betreft de configuratie van het betaalpakket.

Van “program development” is in de regel geen sprake, aangezien de wijzigingen op en ontwikkeling van het pakket door de eigenaar van het betaalpakket zelf worden verricht. Hooguit zal de verwerkende partij de organisatie achteraf informeren over eventuele wijzigingen die in het betaalpakket zijn doorgevoerd. Om diezelfde reden is ook “computer operations” vanuit de organisatie gezien nauwelijks van toepassing op het betaalpakket.

In onderstaande tabel is per categorie (zie ook de tabel uit paragraaf 2.2.6) weergegeven in welke mate deze van toepassing zijn op het betaalpakket.

[36] Overheid.nl, “Wet bescherming persoonsgegevens”, oktober 2009 (http://wetten.overheid.nl/BWBR0011468)
[37] ABN AMRO, “Algemene voorwaarden toegang ABN AMRO”, november 2009 (http://www.abnamro.nl/nl/images/Generiek/PDFs/020_Zakelijk/01_Bankieren/IB_algemene_voorwaarden_toegang.pdf)
[38] ING, “Zakelijk internetbankieren met Mijn ING”, november 2009 (http://www.ing.nl/Images/225353 1208 Voorwaarden Zakelijk internetbankieren met Mijn ING_tcm7-23764.pdf)
[39] Rabobank, “Algemene voorwaarden elektronische diensten”, november 2009 (http://www.rabobank.nl/images/Algemene_voorwaarden_voor_elektronische_diensten_2920548.pdf)
[40] Triodos Bank, “Algemene voorwaarden Internet Bankieren voor zakelijk gebruik”, november 2009 (http://www.triodos.nl/nl/static/pdf/nlnl_algvwibzak0205.pdf)

Categorie	Van toepassing	Onderbouwing
Access to programs and data	+	Van groot belang vanwege het hoge risico van het betaalproces.
Program changes	±	Van toepassing voor wat betreft het testen en in gebruik nemen van het betaalpakket en wijzigingen op de configuraties daarvan.
Program development	–	Niet van toepassing omdat het betaalpakket niet door de organisatie zelf wordt ontwikkeld.
Computer operations	–	Er is binnen de organisatie zelf geen sprake van jobs, backups en uitwijk.

Enkele beheersmaatregelen die aan “access to programs and data” zijn gerelateerd die zijn gebruikt voor het normenstelsel zijn:

- Er is een formeel goedgekeurde procedure voor het beheer van gebruikers, autorisaties en authenticatiemiddelen in het systeem.
- Gebruikers hebben passende rechten binnen het systeem die in lijn zijn met hun functie binnen de organisatie.
- Het systeem koppelt elke activiteit aan de gebruiker, zodat deze te allen tijde zijn te herleiden naar individuele personen.

4.1.7 NV COS en Besluit toezicht accountantsorganisaties

Volgens NV COS[41] moet de accountant een kritische houding aan te nemen en dient hij het risico op fraude (van materieel belang) in te schatten. Diverse andere beheersmaatregelen bieden reeds als geheel bescherming tegen fraude. Door in samenwerking met de IT-auditor onderzoek te verrichten aan de hand van dit normenstelsel, kan de accountant tevens het risico op fraude inschatten.

4.2 Analyse van het betaalproces

Aan de hand de omschrijving van het proces van uitgaande betalingen (zie paragraaf 2.1), zijn risico’s en beheersmaatregelen opgenomen in het normenstelsel. Enkele voorbeelden hiervan zijn:

- De betaalbestanden en ontvangen afschriften worden door het betaalpakket automatisch bewaard op een locatie waar deze niet kunnen worden gemuteerd.
- Het authenticatiemiddel betrekt bij het fiatteren van de betaalopdrachten de inhoud van die betaalopdrachten.
- Registreer betaalopdrachten die niet juist of volledig zijn uitgevoerd volgens de afschriften en verwerkingsinformatie.

[41] Overheid.nl, “Besluit toezicht accountantsorganisaties”, oktober 2009 (http://wetten.overheid.nl/BWBR0020184)

4.3 Veldwerk

Het normenstelsel is in eerste instantie opgesteld aan de hand van de theorie. Tijdens het veldwerk zijn medewerkers van diverse organisaties geïnterviewd en enkele betaalpakketten zijn bestudeerd. Door dit veldwerk zijn aanvullingen op het normenstelsel gemaakt doordat ook rekening wordt gehouden met risico's uit de praktijk. Enerzijds wordt hiermee de bruikbaarheid in de praktijk van het normenstelsel vergroot en anderzijds worden tegelijkertijd typische risico's uit de praktijk geraakt. Enkele voorbeelden van dergelijke beheersmaatregelen zijn:

- In het betaalpakket is het bedrag dat per keer/periode en per gebruiker kan worden betaald beperkt tot een maximum.
- De URL van de verwerkende partij is van het formaat www.betalen.bank.nl en niet www.betalenbijmijnbank.nl of www.bank.nl/betalen.

4.4 Opbouw normenstelsel

Door bovenstaande theorie, wet- en regelgeving, richtlijnen, raamwerken en ervaringen uit de praktijk te combineren is één overkoepelend normenstel opgesteld voor het gehele betaalproces. Door de verschillen tussen de afzonderlijke betaalpakketten, zijn de opgenomen beheersmaatregelen in het normenstelsel generiek geformuleerd. De beheersmaatregelen moeten derhalve worden afgestemd op de specifieke situatie waarbinnen deze worden toegepast.

De beheersmaatregelen uit het normenstelsel zijn in twee delen in de bijlage opgenomen:

- Beheersmaatregelen per processtap
- Beheersmaatregelen van algemene aard

Zoals in onderstaande figuur is te zien, staan per risico beheersmaatregelen vermeld in het normenstelsel. Voor elke beheersmaatregel is omschreven hoe het opzet en bestaan daarvan kan worden getoetst.

#	Risico	Beheersmaatregel	Audit werkzaamheden voor opzet en bestaan
A	betaalvoorstellijst aanmaken		
01	Gebruikers die daartoe niet zijn geautoriseerd muteren de betaalvoorstellijst in de crediteurenadministratie wat tot onrechtmatige betalingen leidt.	Alleen daartoe geautoriseerde gebruikers hebben bevoegdheden de betaalvoorstellijst aan te maken in de crediteurenadministratie.	Neem kennis van de bevoegdheden per gebruiker uit de crediteurenadministratie en bespreek het aanmaken van de betaalvoorstellijst. Stel vast dat alleen daartoe geautoriseerde gebruikers de betaalvoorstellijst kunnen aanmaken in de crediteurenadministratie.
02	Crediteuren worden onterecht of vaker dan één keer betaald en geld verlaat onrechtmatig de organisatie, doordat: • facturen dubbel worden ingevoerd • er onzekerheid bestaat over het feit of reeds is betaald • er geen tegenprestatie is geleverd	Stel vooraf vast dat betaalopdrachten op de betaalvoorstellijst alleen op basis van gecontroleerde en goedgekeurde facturen zijn gebaseerd en waarvoor daadwerkelijk een tegenprestatie is geleverd.	Bespreek de uitvoering van deze beheersmaatregel en neem kennis van werkinstructies. Stel aan de hand van een betaling vast dat op de betaalvoorstellijst alleen betaalopdrachten voorkomen op basis van gecontroleerde en goedgekeurde facturen, waarvoor daadwerkelijk een tegenprestatie is geleverd.
		De crediteurenadministratie signaleert dubbele betaalopdrachten.	Inspecteer de crediteurenadministratie en stel [illegible] dubbele betaalopdracht vast dat de [illegible]

figuur 9: opbouw normenstelsel

5 Samenvatting en conclusies

De samenvatting en belangrijkste conclusies van dit onderzoek zijn dit hoofdstuk opgenomen. Hierbij wordt een verwijzing gemaakt naar de eerder genoemde onderzoeksvragen van dit onderzoek. Het opgestelde normenstelsel is gebaseerd op de theorie en de praktijk. Hierdoor wordt een breed scala aan risico's afgedekt door passende beheersmaatregelen.

5.1 Beantwoording onderzoeksvragen

Aan de hand van de uitkomsten van het onderzoek worden de onderzoeksvragen uit paragraaf 1.3 hieronder beantwoord. Deze zijn geformuleerd naar aanleiding van onderstaande doelstelling van het onderzoek:

Het ontwerpen van een normenstelsel om de betrouwbaarheid van de beheersmaatregelen in het proces van uitgaande betalingen te toetsen.

Het proces van uitgaande betalingen kent theoretisch beschouwd diverse risico's. In de praktijk worden deze risico's echter niet altijd in voldoende mate onderkend. In diverse wet- en regelgeving, richtlijnen en raamwerken vindt men vele redenen om meer aandacht te besteden aan de risico's en beheersmaatregelen binnen het betaalproces.

De organisatie die betaalopdrachten verstuurt (opdrachtgever) is er bij gebaat in dit proces voldoende beheersmaatregelen te nemen. Privacy (Wet Bescherming Persoonsgegevens) is een belangrijk aspect omdat in het betaalproces zeer privacygevoelige gegevens zijn betrokken, met name bij het betalen van salarissen. Tevens dient de organisatie maatregelen te nemen tegen fraude en zal ook de accountant (conform NV COS en Besluit toezicht accountantsorganisaties) in het kader van de jaarrekeningcontrole hier aandacht aan moeten besteden. Naast het feit dat geld ten onrechte aan de organisatie wordt onttrokken, bestaat het risico dat een frauduleuze betaling reputatieschade en imagoschade met zich meebrengt. Daarnaast is elke organisatie volgens de Code van informatiebeveiliging en COSO ERM gehouden aan het goed beheer van gegevens. Vanuit de Risk management principles for electronic banking van Basel committee on banking supervison van Bank for international settlements worden adviezen (*"risk management principles"*) gegeven voor het inrichten van online betaalpakketten. Het geeft handvatten (*"security controls"*) ten aanzien van de authenticatie van gebruikers, functiescheiding en autorisatie. Aangezien er in het betaalproces een betaalpakket is betrokken zijn enkele algemene IT beheersmaatregelen van toepassing.

Om de betrouwbaarheid van de beheersmaatregelen in het proces van uitgaande betalingen te kunnen toetsen, wordt in dit onderzoek een normenstelsel met beheersmaatregelen aangereikt. Deze beheersmaatregelen zijn afgestemd op de risico's die zich in het betaalproces bevinden. Door het betalingsverkeer in brede zin binnen Nederland in kaart te brengen en in enge zin het proces van uitgaande betalingen te analyseren, worden de risico's in het betaalproces inzichtelijk.

1. **Hoe verloopt het betalingverkeer in Nederland en waar zitten in dat proces de risico's voor de organisatie zelf?**

Het betalingsverkeer in Nederland is ingericht volgens het *four party-model*. Hierbij wordt onderscheid gemaakt tussen de *acquiring bank*, de *issuing bank*, de *merchant* en de *consumer*, dat betreft de banken, DNB, Equens en de organisaties (opdrachtgever en begunstigde) die onderling geld aan elkaar betalen. Het betaalproces begint met het aanmaken van een betaalvoorstellijst dat leidt tot het betaalbestand met daarin de betaalopdrachten. Dit betaalbestand zal uit de crediteurenadministratie worden geëxporteerd en vervolgens in het betaalpakket worden ingelezen. In het betaalpakket is het mogelijk aanvullend handmatige betaalopdrachten in te voeren. Alle betaalopdrachten dienen te worden gefiatteerd, waarna deze worden verzonden aan de verwerkende partij. Deze partij zal de betaalopdrachten uitvoeren in samenwerking met onder andere Equens, DNB en banken. Aan de hand van de verstrekte afschriften en verwerkingsinformatie zullen in de crediteurenadministratie de betalingen worden afgeletterd.

Door middel van een aantal bezoeken aan organisaties is duidelijk geworden dat ook daar meer aandacht aan het betaalproces moet worden besteed. Er heerst veelal (onterecht) het idee dat er reeds voldoende beheersmaatregelen zijn getroffen. Dit valt te wijten aan enerzijds een gebrek aan technische kennis en anderzijds een groot vertrouwen in eigen medewerkers cq. collega's. Tevens is uit de gesprekken gebleken dat ook auditors weinig aandacht besteden aan het proces van uitgaande betalingen.

Het Basel committee on banking supervision van Bank for international settlements adviseert banken maatregelen te nemen op het gebied van authenticatie, niet-weerlegbaarheid, integriteit, functiescheiding, autorisatie en audit trails. Desondanks worden via de algemene voorwaarde van de banken ten aanzien van (zakelijk) internet bankieren een groot deel van de verantwoordelijkheid bij de gebruiker neergelegd. De gebruiker dient zelf controles op de juistheid, volledigheid en tijdigheid van de verwerking van betaalopdrachten uit te voeren. Eveneens wordt de verantwoordelijkheid rondom het gebruik van authenticatiemiddelen volledig bij de organisatie zelf gelegd. De verwerkende partij legt de verantwoordelijkheid voor fouten in de verwerking naast zich neer en de gebruiker moet kunnen aantonen dat er sprake is van opzet of grove schuld. Een authenticatiemiddel kan iets bevatten wat men 'weet' en 'heeft'. Authenticatiemiddelen die gebaseerd zijn op iets wat men 'is' worden bij betaalpakketten echter nog niet toegepast. Verder is gebleken dat niet alle betaalpakketten voldoende controlemogelijkheden bieden zoals het gebruik van hashtotalen.

Het is van belang dat de gebruiker zich bewust is van de risico's wanneer alle betaalopdrachten uit een betaalbestand in één keer worden geboekt (op de grootboekrekeningen "crediteuren" en "betaling onderweg") en afgeschreven van de bankrekening. Dit maakt het moeilijker achteraf te kunnen vaststellen of conform de afzonderlijke betaalopdrachten door de verwerkende partij de juiste bedragen naar de juiste bankrekeningen zijn overgemaakt.

Op basis van de literatuurstudie en het veldwerk zijn de risico's in het betaalproces in kaart gebracht. Enkele van deze risico's zijn:

- betaalopdrachten worden ten onrechte gemuteerd
- betaalopdrachten worden niet gefiatteerd
- functiescheiding in het betaalproces ontbreekt
- afschriften en verwerkinginformatie van de verwerkende partij wordt gemuteerd
- door middel van slepen wordt geld aan de organisatie onttrokken
- details (audit trail) van betaalopdrachten zijn achteraf niet meer te herleiden

2. Wat zijn de belangrijkste kenmerken van de meest gebruikte betaalpakketten?

Betaalpakketten van de verschillende verwerkende partijen ondersteunen logischerwijs een groot aantal overeenkomstige functionaliteiten en verschillen grafisch gezien soms ook minimaal, wat maakt dat de onderlinge verschillen beperkt zijn. Op basis van het veldwerk is vastgesteld dat er een verschuiving optreedt naar online betaalpakketten.

Desalniettemin zijn de volgende eigenschappen aangetroffen die tussen de betaalpakketten sterk verschillen:

- De mate waarin gedetailleerd autorisaties kunnen worden ingericht verschil sterk tussen de pakketten. Dit varieert van betaalpakketten waarin alle gebruikers dezelfde rechten hebben en tot betaalpakketten waarin autorisaties minutieus kunnen worden toegekend door middel van profielen.
- Per verwerkende partij verschilt het sterk hoe gebruikers aan het betaalpakket worden toegevoegd. Het kan zijn dat organisaties geheel zelfstandig gebruikers, authenticatiemiddelen en autorisaties kunnen wijzigen aan het betaalpakket of dat dit via de verwerkende partij dient te verlopen.
- Voor de gebruiker zijn niet altijd even veel mogelijkheden beschikbaar om door middel van controletotalen en hashtotalen.
- Het verdient de voorkeur om de betaalopdrachten uit een betaalbestand als afzonderlijke betalingen door de verwerkende partij uit te laten voeren. Niet alle betaalpakketten bieden die mogelijkheid.

Bovenstaande eigenschappen zijn niet alleen van belang voor het beoordelen van de inrichting van het betaalpakket maar ook voor het selecteren van een nieuw aan te schaffen betaalpakket. Het is van belang om aan de hand van de functionele en technische eisen en wensen bovenstaande eigenschappen in ogenschouw te nemen.

3. Is een standaard aanpak (gelet op de kenmerken van deze betaalpakketten) haalbaar om de maatregelen binnen het proces van uitgaande betalingen te kunnen beoordelen?

Voor elke van de geïdentificeerde risico's is een beheersmaatregel geformuleerd. Aan de hand van deze beheersmaatregelen is ook bepaald welke audit werkzaamheden verricht moeten worden om opzet en bestaan vast te kunnen stellen. Deze risico's, beheersmaatregelen en audit werkzaamheden zijn tezamen in een normenstelsel verwerkt, waarin deze per processtap zijn gegroepeerd.

Het normenstelsel met generieke beheersmaatregelen kan als basis worden gebruikt voor het beoordelen van de inrichting van het proces van de uitgaande betalingen en de inrichting van betaalpakketten. De betaalpakketten verschillen onderling, waardoor de beheersmaatregelen moeten worden afgestemd op de specifieke situatie waarbinnen dit normenstelsel wordt toegepast.

Naast het beoordelen van de inrichting van het betaalproces en het betaalpakket, kan het normenstelsel ook als leidraad worden gebruikt bij de inrichting hiervan. De beheersmaatregelen kunnen tevens worden gebruikt als normen / eisen bij het selecteren van een nieuw betaalpakket.

5. Zo ja, welke audit werkzaamheden (a) dienen er in algemene zin te worden verricht en (b) moeten in enge zin per betaalpakket worden uitgevoerd? Zo nee, waarom is deze standaard aanpak niet haalbaar?

Ondanks dat de betaalpakketten op enige punten verschillen, kan het normenstelsel als standaard aanpak worden gehanteerd bij het beoordelen van de beheersmaatregelen in het betaalproces en de inrichting van het betaalpakket. De te verrichten audit werkzaamheden zijn evenals de risico's en beheersmaatregelen in het normenstelsel opgenomen.

5.2 Conclusies, discussie en vervolgonderzoek

Gedurende het onderzoek zijn enkele opvallende punten naar voren gekomen. Onderstaande punten vormen elk in meer of mindere mate zwakheden in het betaalproces of de betaalpakketten. Het is raadzaam aanvullend onderzoek te doen.

- Om meer informatie over de betaalpakketten te verkrijgen is diverse malen contact gezocht met banken. Het blijkt dat banken naast de algemene voorwaarden voor zakelijk internet bankieren en enkele demo's of informatiebrochures, weinig informatie willen verstrekken. Dit in tegenstelling tot andere veel gebruikte programma's zoals bijvoorbeeld SAP, PHP of Windows waarvoor op internet miljoenen documenten met informatie over beveiliging, functionaliteiten en bugs te vinden zijn. Dit maakt het doorgronden en beoordelen van de autorisaties, functiescheiding, versleuteling, ... onnodig lastig, waardoor ongezien risico's zich nog altijd in het betaalpakket kunnen bevinden.

- Helaas heeft het veldwerk in dit onderzoek bevestigd dat er veelal "om het betaalproces heen" wordt gecontroleerd door auditors. Daarnaast worden in organisaties onbewust hoge risico's genomen doordat men niet bekend is met de risico's van IT. Blijkbaar geven voorbeelden zoals in paragraaf 1.2 niet of nauwelijks aanleiding tot aanbrengen en controleren van beheersmaatregelen in het betaalproces. Bijgevoegd normenstelsel kan worden gebruikt door organisaties en auditors om het betaalproces en het betaalpakket in te richten cq. te beoordelen.

- Er zijn in dit onderzoek geen authenticatiemiddelen aangetroffen die bij het fiatteren zich baseren op de inhoud (zoals bedragen en bankrekeningnummers) van het bericht (betaalopdrachten). Hierdoor bestaat het risico dat ten tijde van het fiatteren de betaalopdrachten op de achtergrond zijn gewijzigd[42], terwijl in het betaalpakket aan de gebruiker nog de ongewijzigde betaalopdrachten in de browser toont. De betreffende authenticatiemiddelen geven alleen zekerheid over de identiteit van de gebruiker en betrekken daarbij niet de inhoud van het te fiatteren bericht.

- Zoals eerder aangegeven zijn authenticatiemiddelen in drie groepen te verdelen: iets wat men 'weet', 'heeft' of 'is'. Vooralsnog wordt er geen gebruik gemaakt van iets wat

[42] Dit kan door programmatuur (trojans, virussen, ...) worden gedaan die zich tussen de presentatielaag en de datalaag van de browser nestelen. Hierdoor worden binnenkomende gegevens weer aangepast, zodanig dat de gebruiker zijn originele betaalopdrachten herkent. Andersom kunnen ook uitgaande gegevens buiten het zicht van de gebruiker om worden aangepast voordat deze via het internet worden verstuurd.

men ‘is’ (bijvoorbeeld vingerafdruk, stemherkenning, iriscopie of gezichtsherkenning) terwijl deze vorm van authenticatie juist extra beveiliging kan bieden. De huidige mechanismen om betaalopdrachten te fiatteren maken geen gebruik van de volledige inhoud van alle betaalopdrachten. Het enige dat door de huidige authenticatiemiddelen wordt bevestigd is wie men is. Dit zegt niets over de feitelijke inhoud van de te fiatteren betaalopdrachten, die kan ondertussen best zijn gemuteerd zonder dat de gebruiker dit bemerkt.

- Men kan zich afvragen of de combinatie van onversleutelde open bestandsformaten (bijvoorbeeld zoals CLIEOP03) en de tussenkomst van personen wenselijk is. Dergelijke bestanden zijn zeer eenvoudig aan te passen zonder dat dit conflicten met de controletotalen oplevert. Dit in tegenstelling tot bijvoorbeeld het versturen van betaalbestanden via het SWIFT-netwerk, waar de tussenkomst van personen kan worden beperkt. Betaalbestanden voor het SWIFT-netwerk worden vanuit de financiële administratie via het netwerk naar SWIFT Alliance verstuurd, die ze zonder tussenkomst van personen direct naar het SWIFT-netwerk kan versturen. Doordat de tussenkomst van personen beperkt is, neemt het risico dat betaalbestanden worden gemuteerd af. De meeste betaalpakketten bieden echter geen mogelijkheid om een geautomatiseerde koppeling (door middel van bijvoorbeeld FTP of SQL-statements) aan te gaan met de financiële administratie. Dit zou de tussenkomst van gebruikers en daarmee ook de risico’s tot een minimum beperken. Tevens zal het gebruik van een bestandsformaat waarvan de inhoud niet leesbaar is voor personen de mogelijkheden om betaalopdrachten te muteren drastisch terugdringen. Hiervoor moet de financiële administratie wel in staat zijn dergelijk formaat of versleuteling toe te kunnen passen. De verwerkende partij zal dan als enige over de mogelijkheid moeten beschikking het versleutelde bestand te kunnen ontsleutelen.

Literatuurlijst

Bestudeerde literatuur

ABN AMRO, “Algemene voorwaarden toegang ABN AMRO”, november 2009 (http://www.abnamro.nl/nl/images/Generiek/PDFs/020_Zakelijk/01_Bankieren/IB_algemene_voorwaarden_toegang.pdf)

Accountant, “Het banksaldo aangevuld”, R. de Groot, M. Grummel en B. Prins, januari 2008 (http://www.accountant.nl/Accountant/Fraude+in+praktijk/Het+banksaldo+aangevuld)

Basel committee on banking supervison, “Risk management principles for electronic banking”, juli 2003 (http://www.bis.org/publ/bcbs98.pdf)

British Standard, “Information technology: Security techniques, code of practice for information security management”, juni 2005

Committee of Sponsoring Organizations of the Treadway Commission, “Enterprise Risk Management, Integrated Framework”, september 2004

DNB, “Betalingsverkeer: veilig en betrouwbaar”, oktober 2009 (http://www.dnb.nl/over-dnb/taken/betalingsverkeer/index.jsp)

DNB, “Giraal betalingsverkeer”, oktober 2009 (http://www.dnb.nl/betalingsverkeer/giraal-betalingsverkeer/index.jsp)

DNB, “Jaarverslag DNB 2008”, maart 2998 (http://www.dnb.nl/binaries/JV DNB 2008_tcm46-214840.pdf)

DNB, “Partijen”, oktober 2009 (http://www.allesoverbetalen.nl/achtergrondinformatie/organisaties/partijen)

DNB, “Taken”, oktober 2009 (http://www.dnb.nl/over-dnb/taken/index.jsp)

Equens, “CLIEOP cliënt opdrachten: bestandsbeschrijving”, maart 2009 (http://www.equens.com/Images/CLIEOP NL.pdf)

Ernst & Young, “European fraud survey 2009: is integrity a casualty of the downturn?”, 2009 (http://www2.eycom.ch/publications/items/fraud_eu_2009/European_Fraud_Survey.pdf)

ING, “Zakelijk internetbankieren met Mijn ING”, november 2009 (http://www.ing.nl/Images/225353 1208 Voorwaarden Zakelijk internetbankieren met Mijn ING_tcm7-23764.pdf)

Innopay, “Online betalen: internetbetalingen in Europa”, februari 2008

Innopay, “Online payments: European market overview”, maart 2009

Kluwer, “Meer fraude door kredietcrisis”, oktober 2008 (http://www.kluwerfinancieelmanagement.nl/?subject=article&id=129)

Kroll, “Global Fraud Report”, 2008 (http://www.kroll.com/library/fraud/FraudReport_English-US_Sept08.pdf)

Ministerie van Financiën, “Handboek betalingsverkeer Rijksoverheid”, februari 2008 (http://www.minfin.nl/dsresource?objectid=2529)

NIVRA, “Handleiding regelgeving accountancy: NV COS 240 (De verantwoordelijkheid van de accountant voor het onderkennen van het risico van fraude in het kader van de controle van financiële overzichten)”, oktober 2009 (http://www.nivra.nl/Sites/nivra_site/HRA/200903/html/38351.htm)

NIVRA, “Handleiding regelgeving accountancy: NV COS 315 (Kennis van de entiteit en haar omgeving en het inschatten van het risico van een afwijking van materieel belang)”, oktober 2009 (http://www.nivra.nl/Sites/nivra_site/HRA/200903/html/38644.htm)

NIVRA, “Handleiding regelgeving accountancy: NV COS”, oktober 2009

NVB, “Betalingen”, oktober 2009 (http://www.nvb.nl/index.php?p=17930)

NVB, “Rol NVB”, oktober 2009 (http://www.nvb.nl/index.php?p=10822)

Overheid.nl, “Besluit toezicht accountantsorganisaties”, oktober 2009 (http://wetten.overheid.nl/BWBR0020184)

Overheid.nl, “Wet bescherming persoonsgegevens”, oktober 2009 (http://wetten.overheid.nl/BWBR0011468)

Rabobank, “Algemene voorwaarden elektronische diensten”, november 2009 (http://www.rabobank.nl/images/Algemene_voorwaarden_voor_elektronische_diensten_2920548.pdf)

SNS, “Productvoorwaarden SNS Zakelijk Internet Bankieren”, november 2009 (http://www.snsbank.nl/web/file?uuid=d5c3e712-6c1d-477f-bb2b-80d092d58dfe&owner=d5fe9abf-6784-4174-8c82-bc8310dcc108&contentid=894)

Starreveld, “Bestuurlijke informatieverzorging, deel 2A: fasen van de waardekringloop”, 2005

Starreveld, “Bestuurlijke informatieverzorging, deel 2B: typologie van de bedrijfshuishouding”, 2006

Triodos Bank, “Algemene voorwaarden Internet Bankieren voor zakelijk gebruik”, november 2009 (http://www.triodos.nl/nl/static/pdf/nlnl_algvwibzak0205.pdf)

Twinkle Magazine, “De wereld van Payment Service Providers”, oktober 2009 (http://twinklemagazine.nl/praktijk.aspx?id=9770)

Bijlagen

Terminologie

Ten behoeve van de duidelijkheid van het gebruik van enkele begrippen die in dit onderzoek worden aangehaald, worden deze hieronder toegelicht:

- Een **afschrift** bevat detailgegevens over de transacties en informatie over het saldo van de bankrekening.
- Om toegang te verkrijgen tot het betaalpakket of bijvoorbeeld betaalopdrachten te fiatteren moet veelal gebruik worden gemaakt van een token, smartcard, calculator, TAN-code, SMS, ... Vele andere benamingen en middelen zijn hiervoor in gebruik. Samenvattend worden deze aangeduid als **authenticatiemiddelen**.
- In een **betaalbestand** zijn één of meer **betaalopdrachten** opgeslagen. Betaalopdrachten kunnen los in het betaalpakket worden ingevoerd of door een betaalbestand (met betaalopdrachten) in te lezen. Dit betaalbestand wordt veelal (geautomatiseerd) door de financiële administratie aangemaakt.
- Met het **betaalpakket** worden alle varianten van programmatuur bedoeld waarmee betaalopdrachten naar de verwerkende partij worden verstuurd. Dit betreft zowel programmatuur die lokaal bij de organisatie wordt geïnstalleerd en via een verbinding met de verwerkende partij communiceert als websites die online diensten aanbieden om te kunnen betalen. Deze laatste wordt ook wel internet bankieren, e-banking of elektronisch bankieren genoemd, zie ook paragraaf 2.1.2.
- Met **clearing** wordt verwezen naar periodiek het uitwisselen van informatie over betaalopdrachten en het verrekenen van de bedragen die partijen aan elkaar zijn verschuldigd namens de rekeninghouders. Hierna vindt settlement plaats.
- Met **controletotalen** wordt verwezen naar getallen die zijn berekend aan de hand van de inhoud van het betaalbestand. Dit gebeurt veelal aan de hand van de sommatie van de bedragen of bankrekeningnummers van de afzonderlijk betaalopdrachten. Ook kan een controletotaal zijn gebaseerd op het aantal betaalopdrachten in het betaalbestand. Nadeel van dergelijke controletotalen is dat dit geen zekerheid geeft dat de betaalopdrachten niet zijn gemuteerd.
- In dit onderzoek wordt regelmatig over **crediteuren** gesproken in het kader van het betaalproces. Dit betreft niet alleen de (gebruikelijke) crediteuren die ingekochte diensten of producten leveren. Hieronder vallen ook de medewerkers aan wie periodiek salarissen worden uitbetaald.
- **Hashtotalen** worden berekend volgens een bekende formule en zijn gebaseerd op de gehele inhoud en de positie daarvan binnen het bestand. Het wordt als onmogelijk beschouwd een bestand te genereren waarvan het hashtotaal gelijk is aan een vooraf bepaalde waarde.
- Na clearing vindt **settlement** plaats waarmee de verevening van onderlinge verplichtingen.
- Als over de **organisatie** of **opdrachtgever** wordt gesproken, wordt hiermee de organisatie bedoeld die de betaalopdrachten verstuurt met behulp van het betaalpakket.
- Met **verwerkende partij** wordt elke organisatie bedoeld die betaalopdrachten verwerkt. Dit zijn onder andere banken en Equens.

- Op de **verwerkingsinformatie** staat vermeld welke betaalopdrachten wel en niet zijn geslaagd.

Algemene voorwaarden zakelijk internet bankieren

Bank	Bron	Voorwaarden
ABN AMRO	Algemene voorwaarden toegang ABN AMRO[43]	• "Een toegangsmiddel is uniek verbonden aan een natuurlijke persoon. Per toegangsmiddel is steeds slechts één persoon bevoegd (de houder) tot gebruik daarvan en het toegangsmiddel is niet overdraagbaar. Een wachtwoord, een PIN en dergelijke codes dienen geheim te worden gehouden."
ING	Zakelijk internetbankieren met Mijn ING[44]	• "De cliënt verbindt zich ertoe het wachtwoord, de gebruikersnaam, de activeringscode en de TAN-codes geheim te houden en verder alles te doen om de geheimhouding van gebruikersnaam, wachtwoord, activeringscode en TAN-codes te verzekeren." • "De gebruikersnaam, het wachtwoord en TAN-codes zijn persoonlijk en mogen derhalve door de cliënt aan niemand worden overgedragen of medegedeeld." • "De cliënt is verplicht te controleren of zijn via Mijn ING gegeven opdrachten correct zijn uitgevoerd."
Rabobank	Algemene voorwaarden elektronische diensten[45]	• "De klant dient zorgvuldig om te gaan met een beveiligingscode en hulpmiddel." • "Als de klant met behulp van een beveiligingscode en/of hulpmiddel in een beveiligde omgeving komt, dient hij voortdurend te controleren of hij zich nog in deze beveiligde omgeving bevindt." • "Een beveiligingscode is strikt persoonlijk en niet overdraagbaar. De klant is verplicht een beveiligingscode geheim te houden voor andere personen, daaronder mede begrepen familieleden, huisgenoten, mederekeninghouders en gevolmachtigden. De klant mag een beveiligingscode nergens (schriftelijk) vastleggen of op zodanige wijze bewaren dat andere personen daarvan kunnen kennisnemen." • "De klant zal een hulpmiddel niet aan andere personen ter beschikking stellen." • "De klant dient ervoor te zorgen dat de door hem gebruikte (internet- en/of telecommunicatie)diensten, apparatuur en programmatuur geschikt en veilig zijn voor het gebruik van een elektronische dienst en/of een functionaliteit."
SNS	Productvoorwaarden SNS Zakelijk Internet Bankie-	• "De klant is verplicht zorgvuldig om te gaan met en is geheel zelf verantwoordelijk voor de aan hem toegekende pincode en de beveiligingsmiddelen (waaronder mede wordt ver-

[43] ABN AMRO, "Algemene voorwaarden toegang ABN AMRO", november 2009 (http://www.abnamro.nl/nl/images/Generiek/PDFs/020_Zakelijk/01_Bankieren/IB_algemene_voorwaarden_toegang.pdf)
[44] ING, "Zakelijk internetbankieren met Mijn ING", november 2009 (http://www.ing.nl/Images/225353 1208 Voorwaarden Zakelijk internetbankieren met Mijn ING_tcm7-23764.pdf)
[45] Rabobank, "Algemene voorwaarden elektronische diensten", november 2009 (http://www.rabobank.nl/images/Algemene_voorwaarden_voor_elektronische_diensten_2920548.pdf)

Bank	Bron	Voorwaarden

	ren[46]	staan de persoonlijke vijfcijferige toegangscode) en terzake volstrekte geheimhouding te betrachten."
		
		• "De klant staat in voor de juistheid van de door de klant gegeven opdrachten en de daarin vermelde bankrekeningnummers en – indien de namen van de begunstigden worden opgegeven – tevens voor het corresponderen van de bankrekeningnummers met de namen van de begunstigden. De bank is niet gehouden de juistheid van de in de opdrachten vermelde gegevens te verifiëren."
		• "De bank is niet aansprakelijk voor enige schade, die niet door haar opzet of grove schuld is ontstaan en die direct of indirect voortvloeit uit:
		
		  • Gehele / gedeeltelijke niet beschikbaarheid van SNS Internet Bankieren.
		
		  • Uitvoering van een opdracht na verloop van de door de klant aangegeven termijn.
		
		  • Verstrekking van onjuiste en/of onvolledige informatie over saldi en/of mutaties en/of overige bankdiensten.
		
		  • Onjuistheid in of onvolledigheid (door welke oorzaak ook) van de software, waaronder mede wordt begrepen de software met betrekking tot de elektronische dienstverlening."
		
		• "Voor misverstanden, verminkingen, vertragingen of niet behoorlijk overkomen van opdrachten en mededelingen ten gevolge van het gebruik van SNS Internet Bankieren in het verkeer tussen de klant en de bank is de bank slechts aansprakelijk, voorzover haar opzet of grove schuld te verwijten is."

Triodos Bank	Algemene voorwaarden Internet Bankieren voor zakelijk gebruik[47]	• "De rekeninghouder dient zorgvuldig om te gaan met en is verantwoordelijk en aansprakelijk voor (ieder gebruik van) het wachtwoord, de identifier en de pincode." • "De gebruikersnaam, het wachtwoord, de identifier en de pincode zijn strikt persoonlijk en niet overdraagbaar. De rekeninghouder en de gebruiker zijn verplicht volstrekte geheimhouding te betrachten ten aanzien van het wachtwoord en de pincode ten opzichte van een ieder, daaronder mede begrepen familieleden, huisgenoten, (mede)rekeninghouders, (mede)gebruikers en gemachtigden. De rekeninghouder zal geen aantekening maken van het wachtwoord en/of de pincode." • "De rekeninghouder staat in voor de juistheid van de door hem of de gebruiker verstrekte opdrachten. De bank is niet

[46] SNS, "Productvoorwaarden SNS Zakelijk Internet Bankieren", november 2009 (http://www.snsbank.nl/web/file?uuid=d5c3e712-6c1d-477f-bb2b-80d092d58dfe&owner=d5fe9abf-6784-4174-8c82-bc8310dcc108&contentid=894)

[47] Triodos Bank, "Algemene voorwaarden Internet Bankieren voor zakelijk gebruik", november 2009 (http://www.triodos.nl/nl/static/pdf/nlnl_algvwibzak0205.pdf)

Bank	Bron	Voorwaarden

		gehouden de juistheid van de in de opdracht vermelde gegevens te verifiëren."
		
		• "De rekeninghouder en gebruiker dienen, alvorens opdrachten te verzenden, te controleren of er sprake is van een beveiligde sessie met de bank."
		
		• "De bank is niet aansprakelijk voor schade, die niet door haar opzet of grove schuld is ontstaan en die direct of indirect voortvloeit uit:
		
		  • Het niet of niet tijdig uitvoeren van een opdracht.
		
		  • Verminking, niet of vertraagd ontvangen, niet behoorlijk overkomen alsmede onbevoegde kennisneming of wijziging van een opdracht."