# Mobiele telefoon als betaalmiddel

***Een advies- en onderzoeksrapport van mogelijkheden en bedreigingen***

Radboud Universiteit Nijmegen


Interpay

contact, interact, transact

**Mirko van Ede( 9902236)**
**Nijmeegs Instituut voor Informatica en Informatiekunde**
**Radboud Universiteit Nijmegen**
**mei 2008**

# Voorwoord

Ter afronding van mijn studie Informatica aan de Radboud Universiteit in Nijmegen heb ik onderzoek gedaan. Dit onderzoek is uitgevoerd naar aanleiding van een opdracht van Interpay, de grootste en belangrijkste paymentprocessor van Nederland. De resultaten ervan staan beschreven in deze scriptie.

Het onderzoek is begeleid door Dr. Martijn Oostdijk en Drs. Pepijn Vos, welke ik beide hartelijk wil bedanken voor hun ondersteuning, tips en geduld.

# Samenvatting

Dit document beschrijft mijn afstudeeronderzoek , uitgevoerd in opdracht van Interpay, dat zich richt op een inventarisatie van (combinaties van) bruikbare technologieën voor het implementeren van een systeem dat het mogelijk maakt om betalingen te verrichten met de mobiele telefoon. Deze inventarisatie houdt rekening met de technische eisen die de stakeholders stellen aan een dergelijk systeem.

Verschillende combinaties van Near Field Communication (NFC) of het GSM netwerk als transportlaag voor de uitwisseling van berichten en de opslag van betalingsgegevens op het toestel of juist op een centrale server, blijken te voldoen aan de eisen op technologisch gebied van de stakeholders. Van deze combinaties is vervolgens met behulp van de Attacktree methode een bedreigingsanalyse gemaakt, waarna ze onderling vergeleken zijn op basis van deze attacktree analyses.

Als gevolg van dit vergelijk is een rapport aan Interpay uitgebracht, waarin geadviseerd wordt om verder onderzoek te doen naar de mogelijkheden van NFC in combinatie met lokale opslag van betalingsgegevens, omdat uit dit onderzoek bleek dat deze combinatie potentieel het meest geschikt is om een betalingssysteem voor mobiele telefoons te implementeren.

Tot slot bespreekt deze thesis het gebruik van de attacktree methode in de praktijk als (semi-)formele methode voor het maken van bedreiging-sanalyses, ten einde ontwerpkeuzes te maken.

# Inhoudsopgave

# Illustraties

# H1 Project kader

## *1.1 Inleiding*

Om inzicht te geven waarom dit onderzoek is uitgevoerd, wordt in dit hoofdstuk het projectkader besproken van het onderzoek naar de (combinatie van) bruikbare technologieën voor het implementeren van een betalingssysteem voor mobiele telefonie, rekening houden met de eisen van verschillende stakeholders en rekening houdend met de veiligheidsaspecten, uitgevoerd in opdracht van de afdeling ECS van Interpay.

## *1.2 Opdrachtgever*

Dit onderzoek wordt uitgevoerd naar aanleiding van een opdracht van Interpay, specifieker: afdeling ECS. Interpay verzorgt het verwerken van het Nederlandse betalingsverkeer. Interpay verwerkt jaarlijks miljarden transacties, verricht met de meest uiteenlopende betaalproducten, waaronder Chipknip, PIN-transacties en girale betalingen. Interpay is hiermee één van de grootste payment processors van Europa. Begin 2006 is Interpay een verregaand samenwerkingsverband aangegaan met de Duitse collega Transaktionsinstitut.

De afdeling E-Commerce Services richt zich op de ontwikkeling en exploitatie van elektronische betaaldiensten en daaraan gerelateerde services voor bijvoorbeeld internet en mobiele telefonie. De ECS-diensten worden ontwikkeld ten behoeve van banken, telecom operators, issuers en acquirers en spitsen zich toe op het gebied van transactieverwerking, authenticatie en beveiliging[3]. Een voorbeeld van zo'n dienst is Mobiel Opwaarderen, waarbij de klanten van telecombedrijven hun beltegoed kunnen opwaarderen met behulp van hun mobiele telefoon, waarbij het bedrag direct wordt afgeschreven van de bankrekening. Interpay ECS ontwikkelde deze dienst en biedt die aan de telecombedrijven aan, die het als een eigen dienst weer aan hun klanten aanbieden. Een ander voorbeeld is iDeal, een methode om direct te betalen bij aankopen via het Internet en waarbij gebruikt wordt gemaakt van de eigen Internetbankier-omgeving van de klant's eigen bank.

## 1.3 Ontwikkelen van nieuwe systemen

Het ontwikkelen van een nieuwe systeem een een heel proces. Het voert te ver om dit tot in detail hier te bespreken, maar voor een beter begrip zal ik globaal uitleggen hoe zo'n proces verloopt.

Het begint uiteraard met een idee dat iemand heeft. Wanneer dit idee concreet genoeg is, begint er een inventarisatie-fase. In deze fase wordt gekeken naar de haalbaarheid van het idee. Die wordt niet alleen op technisch gebied getoetst, maar ook op andere gebieden, zoals financiële of markttechnische haalbaarheid. Het is belangrijk dat men zich goed oriënteert, inzicht krijgt in de haalbaarheid op allerlei gebieden, zodat er een gefundeerd besluit kan worden genomen. Immers, misschien is het idee technisch niet uitvoerbaar, of wijst marktonderzoek uit dat het hoogstwaarschijnlijk geen succes zal worden. Misschien is het wel goedkoper om het systeem te kopen, in plaats van het zelf te bouwen. Wanneer wel tot bouw wordt overgegaan, gaat men een nieuwe fase van het proces in. Er zijn boeken vol geschreven met theorieën over hoe men dit het beste aan kan pakken. Het resultaat is altijd min of meer hetzelfde: er komt, als het goed is, het gewenste eindproduct uit.

## 1.4 Betalingssysteem voor mobiele telefonie

Interpay ECS heeft interesse in een nieuw systeem voor het verrichten van betalingen via het mobiele telefonie-netwerk.. Hiermee wordt een systeem bedoeld waarmee online betalingen kunnen worden verricht, met de mobiele telefoon als betaalinstrument. Je zou het kunnen zien als een moderne vorm van de pinpas, maar dan één die ook mobiel te gebruiken is, dus niet alleen bij een pinterminal. Een ander voordeel daarvan zou zijn dat men zijn mobiele telefoon altijd bij zich heeft, dus weer een pasje minder mee hoeft te nemen. Wie er precies samen zullen gaan werken om dit systeem mogelijk te maken is nog niet bekend (er zijn verschillende combinaties mogelijk van de banken, Interpay en telecombedrijven), maar de eindgebruikers zullen hoe dan ook de consumenten zijn, die er immers mee moeten gaan betalen, en de merchants, die het systeem als betalingsmethode moeten gaan accepteren.

Interpay denkt dat hier, gezien de successen die in het buitenland al op dit gebied geboekt zijn en de vele Nederlandse initiatieven op dit gebied (zie ook hoofdstuk vier), ook in grote Nederland belangstelling voor zal zijn. Interpay ziet dus een goede kans op een nieuw, succesvol product.

Interpay bevindt zich, nu het idee is ontstaan, in de inventarisatiefase van het ontwikkelproces. Uit de opdracht en verschillende gesprekken die ik heb gevoerd, blijkt dat men nog maar weinig kennis heeft over de mogelijkheden van mobiel betalen. Wanneer men direct zou beginnen met

het ontwerpen en bouwen van een nieuw systeem, bestaat de kans dat het wiel opnieuw wordt uitgevonden, omdat het waarschijnlijk is dat een groot deel van de problemen op technisch gebied al opgelost zijn. Wanneer je daarvan gebruik kan maken, scheelt dat uiteraard in de ontwikkelingskosten.

Het is dus belangrijk dat ECS zich eerst inzicht verschaft in de bruikbare technieken die er zijn om de mobiele telefoon als betaalinstrument in te zetten. In deze fase dient er een overzicht te ontstaan met, al dan niet bestaande, technieken die gebruikt en gecombineerd zouden kunnen worden in een systeem voor mobiel betalen. Op basis van de verzamelde kennis en het advies kan Interpay ECS een keuze maken welke van de gestelde (combinatie van) technologieën het best geschikt is om in te gaan zetten voor de gewenste betaaldienst. In combinatie met andere onderzoeken, zoals financieel- en marktonderzoek, kan er dan een gefundeerd besluit worden genomen over het al dan niet bouwen van het systeem.

Dit onderzoek zal proberen Interpay ECS te voorzien van de ontbrekende kennis. Hierbij beperken we ons wel tot een inventarisatie van de mogelijkheden op technisch gebied. Andere gebieden, zoals marktonderzoek of kostentechnische haalbaarheid, komen dus niet aan bod.

## *1.5 Onderzoeksdoel*

We willen in dit onderzoek inventariseren welke (combinaties van) bruikbare technologieën om een mobiel betalingssysteem te implementeren er zijn, die tevens voldoen aan de eisen van de verschillende stakeholders. Eén van de eisen die gesteld zal worden, is dat het systeem veilig zal zijn om te gebruiken. Het is echter zeer lastig, onmogelijk, om iets zinnigs te zeggen over de veiligheid van een onbekend systeem. We zullen het onderzoek daarom opdelen in twee doelen. Het eerste doel van dit onderzoek:

> ***Onderzoeksdoel 1****: Inzicht geven in de mate waarin bruikbare technologieën voor het implementeren van een mobiel betalingssysteem voldoen aan de technische eisen, die door de stakeholders die in de toekomst gebruik gaan maken van het mobiele betalingssysteem, gesteld worden aan mobiel betalen*

Om dat te bereiken hebben we de volgende kennis nodig:

- Wat zijn de eisen die de stakeholders, die in de toekomst van het systeem gebruik gaan maken, aan een dergelijk systeem stellen
- Welke bruikbare technologieën er zijn om tot realisatie van een systeem voor mobiel betalen te komen
- In welke mate voldoen de gevonden technologieën aan de gestelde eisen.

Hierna zullen we kijken naar de veiligheid van de geselecteerde mogelijkheden. Daarmee komen we tot het tweede onderzoeksdoel:

> ***Onderzoeksdoel 2:*** *Inzicht geven in de mate waarin de gevonden (combinaties van) technologieën worden bedreigd door aanvallen die de veiligheid kunnen aan tasten.*

Om dit doel te bereiken, hebben we de volgende kennis nodig:

- Wat zijn de bedreigingen die er voor de geselecteerde systemen (combinaties van technologieën) voor mobiel betalen zijn?
- Welke van de systemen wordt het meest bedreigd?

## 1.6 Relevantie

De kennis die dit onderzoek oplevert, kan de staf van Interpay ECS helpen om een gefundeerde beslissing te nemen over het al dan niet ontwikkelen van een systeem dat betalen voor de mobiele telefoon mogelijk maakt. Dit onderzoek is niet de enige kennis die ze daarvoor nodig hebben, het is slechts een deel, maar wel een belangrijk deel. De kennis kan, wanneer men besluit te gaan bouwen,ook door systeem ontwerpers gebruikt worden. Ze kunnen rekening houden met de eisen en maatregelen die in dit onderzoek naar voren gekomen zijn.

De kennis die het eerste onderzoeksdoel oplevert, een lijst met mogelijke oplossingen die voldoet aan de eisen van de toekomstige gebruikers, kan Interpay zelf eventueel nog aan andere eisen toetsen. Hiermee zouden ze deze lijst dus kunnen beperken of juist uitbreiden door te toetsen op zaken als, bijvoorbeeld, financiële haalbaarheid. Ontwerpers kunnen in hun ontwerp rekening houden met de eisen van de toekomstige gebruikers die in dit onderzoek naar voren komen.

De kennis die het tweede onderzoeksdoel oplevert, verschaft Interpay inzicht in de mate waarin elk systeem van maatregelen moet worden voorzien om de veiligheid te garanderen. Op basis van die kennis zou men ervoor kunnen kiezen om bepaalde mogelijkheden uit te sluiten, omdat het nemen van de gestelde maatregelen niet haalbaar is (bijvoorbeeld omdat ze te duur zijn, of teveel implementatietijd vergen, etc). De voorgestelde maatregelen kunnen door de eventuele ontwerper gebruikt worden om de bedreigingen weg te nemen.

## 1.7 Document structuur

In dit document is zijn de twee onderzoeksdoelen gesplitst, waardoor het document er als volgt uitziet: in hoofdstuk 3 staat beschreven hoe het eerste

onderzoeksdoel bereikt gaat worden. De daaropvolgende hoofdstukken, 4 tot en met 6, bevatten achtereenvolgens een model van het betaalproces, een inventarisatie van de eisen die gesteld worden aan een mobiel betalingssysteem en een overzicht van bestaande mobiele betalingssystemen. In hoofdstuk 7 worden de bruikbare technologieën geïnventariseerd.

Hoofdstuk 8 beschrijft hoe we het tweede onderzoeksdoel gaan bereiken. Hoofdstuk 9 gaat over de te gebruiken methode voor de bedreigingsanalyse in hoofdstuk 10.

Het uiteindelijke advies en de conclusie staan in hoofdstuk 11.

# H2 Onderzoeksopzet onderzoeksdoel 1

Dit hoofdstuk beschrijft ten eerste hoe met de opgestelde onderzoeksvragen aan het eerste onderzoeksdoel kan worden voldaan. Vervolgens wordt in de daarop volgende paragrafen per onderzoeksvraag beschreven hoe deze beantwoord zal gaan worden.

## *2.1 Voldoen aan het onderzoeksdoel*

Het eerste onderzoeksdoel bestaat zoals gezegd uit:

> *Inzicht geven in de mate waarin (combinaties van) bruikbare technologieën voor het implementeren van een betaalsysteem, voldoen aan de technische eisen, die door de stakeholders die in de toekomst gebruik gaan maken van het mobiele betalingssysteem, gesteld worden aan mobiel betalen*

Om dit doel te bereiken is als volgt te werk gegaan. Allereerst is er een model opgesteld van het betaalproces in het algemeen. Dit model laat zien hoe een betaling verloopt, ongeacht of dit een traditionele of mobiele betaling betreft. Daarna zijn binnen het opgestelde model de subsystemen aangegeven waarin het betalen per mobiele telefoon afwijkt van een traditionele (PIN/Chip) elektronische betaling.

Met dit model van het betaalproces in handen is vervolgens aan een aantal stakeholders gevraagd welke eisen zij stellen aan een systeem voor mobiele betalingen. Om dat bij een dergelijk systeem een heel groot aantal stakeholders betrokken is, is er vanwege tijdsdruk gekozen om alleen naar de eindgebruikers, consumenten en merchants, te kijken. Echter, omdat Interpay de opdrachtgever is, is ook onderzoek gedaan naar haar eisen en verwachtingen. Dit resulteert uiteindelijk in een lijst van eisen waaraan een mobiel betalingssysteem moet voldoen. Voor de rest van het onderzoek zijn hieruit de eisen die betrekking hebben op het technisch aspect gedistilleerd. Met deze lijst van technische eisen wordt later gekeken naar de geselecteerde systemen.

In het model is vastgesteld op welke punten een mobiele betaling afwijkt van een traditionele PIN- of Chipknipbetaling. We gaan nu op zoek naar bestaande technologieën die mogelijk een oplossing bieden voor deze afwijkende fases in het betaalproces. Om een zo breed mogelijk perspectief te krijgen, bekijken we welke vergelijkbare betalingssystemen er al bestaan en hoe deze de afwijkende fases hebben ingericht. Deze lijst, in combinatie met deskresearch naar bestaande technologieën, leidt tot een inventarisatie van mogelijk bruikbare systemen. Hierbij kijken we meteen of deze ook aan

de hiervoor gestelde technische eisen voldoen. Dit levert dus een lijst op met manieren om een betalingssysteem voor mobiele telefonie te produceren die voldoen aan de gestelde technische eisen. Met deze lijst is er voldaan aan het eerste onderzoeksdoel.

## *2.2 Hoofdstuk indeling*

In hoofdstuk 4 wordt het model van een betaalproces opgesteld.
Hoofdstuk 5 komt tot een lijst van eisen van de eindgebruikers en Interpay. In hoofdstuk 6 wordt gekeken naar bestaande mobiele betalingsmethodes en in hoofdstuk 7 wordt de lijst samengesteld met technologieën die geschikt zijn om het mobiel betalen mogelijk te maken en die tevens in hoge mate voldoen aan de gestelde eisen.

# H3 Model van het betaalproces

## *3.1 Inleiding*

In dit hoofdstuk zal een model worden opgesteld van het betaalproces. Dit model dient inzicht te geven in de wijze waarop een betalingsproces verloopt, zodat we later de fases kunnen aanwijzen waarop mobiel betalen afwijkt van traditionele betalingen. Tevens wordt het model gebruikt als leidraad in het volgende hoofdstuk om te achterhalen welke eisen gebruikers stellen aan een betaalsysteem. De eis die we aan dit model stellen is dat het het betaalproces in het algemeen beschrijft, niet een specifieke betalingsmethode. Tevens levert dit hoofdstuk kennis op die beschrijft welke fases in het betaalproces afwijken van traditionele betalingen.

Om tot een model te komen dat een algemeen betaalproces beschrijft, bekijken we in de paragraaf 3.2 de vier scenario's die mogelijk zijn bij het verrichten van een betaling. Deze scenario's zijn doorgenomen met het team van Interpay ECS, om er zeker van te zijn dat alle scenario's gevonden en correct zijn.

In de volgende paragraaf bekijken we de rollen die gespeeld worden in de scenario's uit paragraaf 3.2. Deze rollen worden beschreven in de daarop volgende subparagrafen en grafisch weergeven om de onderlinge relaties duidelijk weer te geven.

Vanuit de beschreven scenario's gaan we vervolgens het model van het betaalproces opstellen. Hiervoor identificeren we welke fases in al deze scenario's voorkomen, zodat het model onafhankelijk van het scenario is. De verschillende fases worden vervolgens nader onder de loep genomen om te zien hoe zij precies verlopen. Om ervoor te zorgen dat dit model van de werkelijkheid betrouwbaar is, is het voorgelegd aan de de afdeling ECS van Interpay. De hier aanwezige experts, zowel ontwikkelaars als ontwerpers van betalingsdiensten, hebben er kritisch naar gekeken. Hun commentaar heb is verwerkt in het model en daarna is het nogmaals besproken. We mogen daarom aannemen dat het compleet is en een goed model van de werkelijkheid biedt.

Met dit model in de hand wordt in paragraaf 3.5 gekeken op welke punten een betaling met de mobiele telefoon als betaalinstrument afwijkt van een traditionele PIN- of Chipknip betaling. Deze kennis is wederom voorgelegd aan experts binnen Interpay.

Paragraaf 4.6 bevat de conclusie van dit hoofdstuk.

## *3.2 Betalingsscenario's*

We kunnen onderscheid maken tussen de onderstaande betalingsscenario's. Deze scenario's zijn onafhankelijk van de wijze van betalen en zijn gelden voor zowel nationale als internationale betalingen.

### 3.2.1 Toonbank betalingen

Toonbank betalingen zijn betalingen die worden verricht bij een verkooppunt van de merchant. De consument kiest een product uit en verricht een betaling. De merchant ziet meteen dat de betaling gedaan is en de consument kan het product meenemen.

Er zijn al diverse betalingsmethodes die worden geaccepteerd bij toonbank betalingen. Allereerst bestaat er de mogelijkheid van chartaal betalen. De voordelen voor de consument zijn dat het vrijwel overal geaccepteerd wordt, dat het simpel,snel en anoniem is.

Een andere manier van betalen is giraal betalen. De meest gebruikte methode is pinnen. De voordelen voor de consument is dat dit vrijwel overal mogelijk is, veilig en altijd beschikbaar: je hoeft geen geld op zak te hebben. Een andere variant is de Chipknip. Beide methodes zijn niet anoniem. De Chipknip heeft als ander nadeel dat hij niet gebruikt kan worden als de chip niet eerst is opgeladen bij een speciale terminal.

Overigens zijn voor giraal betalen (dure) terminals nodig, in tegenstelling tot de chartale methode en dat maakt het onbruikbaar om te gebruiken voor het vierde scenario, betalingen op afstand, tegen een lage kostprijs.

### 3.2.2 Onbemande verkooppunten

Onbemande verkooppunten zijn plekken waar de consument producten kan kopen, terwijl er geen merchant aanwezig is. Voorbeelden hiervan zijn onbemande tankstations, kaartjesautomaten voor bijvoorbeeld openbaar vervoer of parkeerkaartjes en snoepautomaten.

Bij onbemande tankstations wordt voornamelijk Pinnen als betaalmethode geaccepteerd. Bij andere onbemande verkooppunten is er vaak keuze uit betalen met contant geld, Pinnen of Chipknip.

Voor sommige producten staat van tevoren vast wat de prijs is. In dat geval voldoet de consument de betaling, waarna het product mee te nemen is.

Voor bijvoorbeeld benzine is het niet van tevoren zeker wat het gaat kosten, omdat dit afhangt van de afgenomen hoeveelheid. De consument voert dan zijn pinpas en code in, en na het tanken wordt bepaald welk bedrag er van de rekening wordt afgeschreven.

### 3.2.3 Betaling op afstand

Betaling op afstand zijn betalingen waarbij de consument op afstand een product uitkiest, veelal via het Internet. Er is een aantal mogelijkheden om de betaling te verrichten. Hieronder valt de creditcard, betaling per acceptgiro, vooruit betalen of één van de vele methodes die hiervoor ontwikkeld zijn, zoals iDEAL of PayPal.

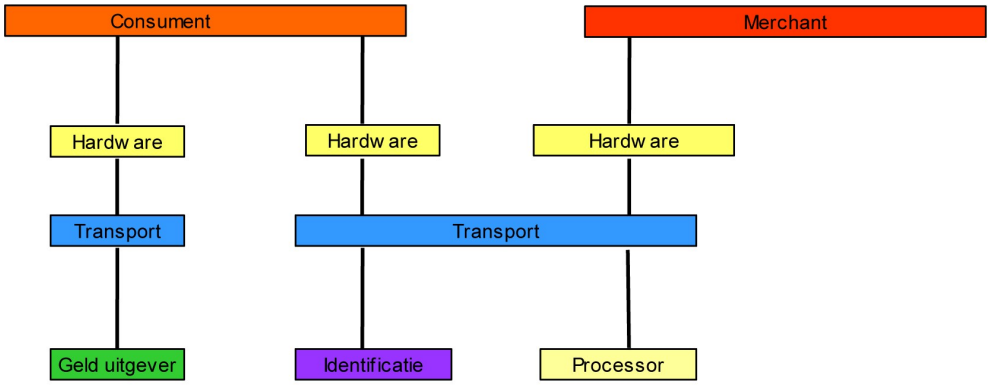
In tegenstelling tot de hierboven genoemde scenario's is het bij betaling op afstand niet van groot belang om direct te weten of een klant wel kan betalen. Mocht later blijken dat dit niet het geval is, dan wordt het product gewoon niet verstuurd door de leverancier.

### 3.2.4 Person to person betalingen

Betaling van de ene persoon aan de andere noemen we een person to person betaling. Zo'n betaling kan op dit moment contant gedaan worden, of overgemaakt worden (per acceptgiro of internetbankieren).

## *3.3 Rollen*

Bij elke betaling is een aantal actoren betrokken. Al deze actoren hebben hun eigen belangen bij een transactie. De lijst hieronder moeten worden gezien als de rollen die gespeeld worden in een betaalproces. Het is daarbij goed mogelijk dat één persoon of instelling meerdere rollen tegelijk vertolkt bij een betaling.




*Illustratie 1: Rollen in het betaalprcoes*

### 3.3.1 Consument

De consument is degene die een product of dienst afneemt van de merchant, in ruil voor een betaling. Deze rollen moet je zien in de context van de betalingsscenario's. De merchant hoeft dus niet perse een handelaar te zijn, in het geval van een person-to-person betaling betreft het een particulier.

### 3.3.2 Merchant

De merchant staat aan de andere kant van de handelsrelatie met de consument. Hij levert een product en ontvangt daarvoor een betaling.

### 3.3.3 Hardware leverancier

De hardware leverancier levert de benodigde apparatuur. Dat kan verschillende hardware zijn, zoals PIN-terminal, geldautomaat, pinpas of, in geval van mobiele betalingen, de telefoon of SIM. Omdat er in het hele proces meerdere hardware gebruikt wordt, is het waarschijnlijk dat er meerdere leveranciers betrokken zijn.

### 3.3.4 Identificatie / Authenticiteit verstrekker

De identificatie is het kenbaar maken van de identiteit van een, in dit geval, persoon. Identificatie is veelal het kenbaar maken door deze persoon van zijn identiteit, hij zegt als het ware: "Dit ben ik". Meestal gebeurd dit met iets wat deze persoon heeft, bijvoorbeeld zijn gebruikersnaam, of zijn bankpas met magneetstrip.

De volgende stap in het proces is vaststellen of de opgegeven identiteit inderdaad klopt. Dit wordt authenticatie genoemd. In de informatica wordt dit meestal gedaan door de persoon een bepaalde code (PIN of wachtwoord) te laten in toetsen om te zien of dat klopt met wat er verwacht wordt.

Wanneer we het over de PIN-betaling hebben, levert de combinatie van pinpas en pincode dus de identificatie en authenticatie. De bank is daarbij meestal degene die dit kan controleren. Telecomoperators zouden identificatie kunnen leveren op basis van de SIM, eventueel in samenwerking met banken.

### 3.3.5 Transporteur

De transporteur verzorgt het transport van gegevens zoals identiteit van betaler en ontvanger, de gegevens over de betalingsopdracht, enzovoorts.

Deze rol kan bijvoorbeeld door een Internet Service Provider of Telecom Operator vertolkt worden.

### 3.3.6 Geld uitgever

Een Elektronische Geld Instelling (EGI) is een instelling die geld uitgeeft op een elektronische drager. Een voorbeeld hiervan is de Chipknip, of de nog in te voeren OV-kaart.

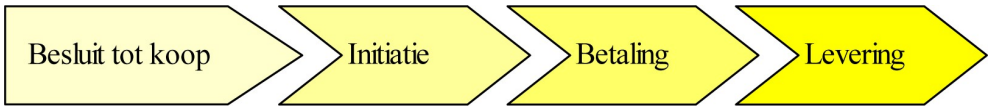
Geld kan ook niet-elektronisch worden uitgegeven, zoals gebeurd door financiële instellingen aan de balie of bij geldautomaten.

### 3.3.7 Payment processor

Een payment processor is een instelling die betalingsopdrachten verwerkt. Zij zorgt ervoor dat het geld van bankrekening x bij bank A wordt afgeschreven en bij bank B op rekening y bijgeschreven. De processor functioneert dus tevens als intermediair tussen de banken. Deze betalingsopdrachten worden veelal elektronisch verstrekt, bijvoorbeeld via het Internet of via PIN-terminals. Overigens is Interpay de enige in Nederland die PIN transacties mag verwerken.

## *3.4 Betaalproces*

Laten we nu wat specifieker gaan kijken naar een betaalproces. Na het bekijken van alle betalingsscenario's, kunnen we in alle scenario's de volgende fases indentificeren:




*Illustratie 2: Fases in het betaalproces*

### 3.4.1 Besluit tot koop

De consument ziet een product en besluit dat hij dat graag wil hebben. Hij kan het product op verschillende plaatsen ‘ontdekken’: in een winkel, via internet, een onbemand verkooppunt. Wanneer de consument besluit tot koop over te gaan, begint de volgende fase.

### 3.4.2 Initiatie

In deze fase geeft de consument aan wat hij wil kopen en hoe hij wil betalen. Hierna wordt de betaling geïnitieerd. Er zijn twee manieren om een betaling te initiëren: push- en pullinitiatie. Afhankelijk van het betalingsscenario, wordt één van de twee gebruikt.

- **Push-initiatie**: de consument start de betalingsprocedure.
- **Pull-initiatie**: de merchant start de betalingsprocedure.

### 3.4.3 Betalingsafwikkeling

De betalingsafwikkeling zelf is ook onder te verdelen in een aantal onderdelen [14]. Deze hoeven niet per se in genoemde volgorde te gebeuren, of misschien wel helemaal niet.

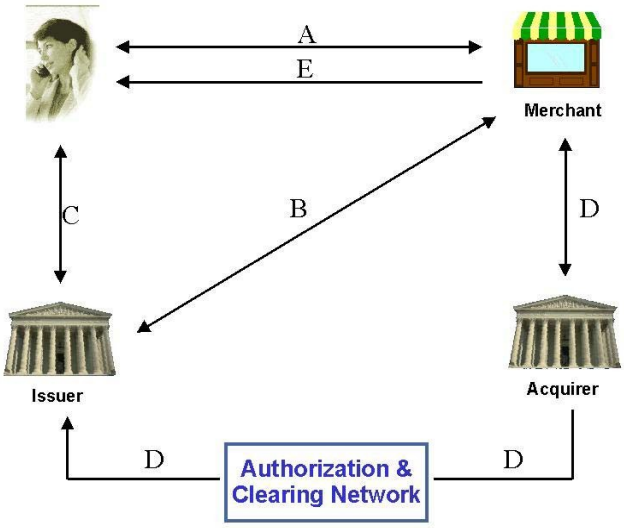
- **Betalingsgegevens verstekken** (Payment Credential Provisioning, PCP)
- **Identificatie;** het aangeven van de identiteit, meestal door het gebruik van een bankpas.
- **Autorisatie;** het controleren van de opgegeven identiteit, meestal door het vragen naar een persoonlijke code (PIN)
- **Accorderen;** degene die wil betalen wordt gevraagd of hij werkelijk bedrag X aan persoon Y wil betalen.
- **Notificatie;** zowel de betaler als de ontvanger krijgen bericht of de betaling succesvol is voltooid.

### 3.4.4 Levering

Afhankelijk van de situatie worden goederen/of diensten geleverd. Dit kan direct gebeuren, bij toonbankbetalingen en onbemande verkooppunten, later zoals bij kopen op afstand, of wellicht wordt er niks geleverd, bijvoorbeeld bij schenkingen of person-to-person betalingen.

### 3.4.5 Transportlaag

De transportlaag is de laag waarover de data wordt getransporteerd naar het achterliggend systeem. In het algemeen ziet een betalingssysteem er als volgt uit [MPF Arch]:




*Illustratie 3: Transport in een betalingssysteem*

Er is een aantal verbindingen te zien, waarop data niet noodzakelijk, sterker nog: niet waarschijnlijk, via hetzelfde medium worden uitgewisseld.

Verbinding A is de verbinding waarop de consument en de merchant de betalingsgegevens (payment credentials) uitwisselen. Verschillende media kunnen hiervoor worden gebruikt, zoals het Internet, bluetooth of de PIN-terminal.

Via verbinding B stuurt de merchant de betalingsgegevens naar de bank van de klant (deze bank heet de *issuer*). Deze verbinding gaat bij de conventionele systemen meestal via Internet, maar een stuk ervan kan uiteraard ook via draadloze communicatie verlopen.

Via verbinding C controleert de bank bij de consument of deze inderdaad wil betalen. Ook deze verbinding kan deels draadloos verlopen, bijvoorbeeld in een WAP-omgeving waarbij de consument via de telefoon contact maakt met het Internet.

Via verbinding D wordt het geld getransporteerd van de bank van de klant naar die van de merchant en wordt de merchant op de hoogte gesteld dat die goed is verlopen. Voor deze verbinding geldt hetzelfde als voor de anderen: hij hoeft niet noodzakelijkerwijs van begin tot eind over hetzelfde medium te lopen.

Bij stap E gaat het betalingsbewijs en eventueel de aanschaf van de merchant naar de consument.

Er gaan dus verschillende boodschappen heen en weer tussen de verschillende spelers in het proces. Deze verbinding hoeven echter niet van begin tot eind over hetzelfde medium te gaan.

Dit deel van het systeem is voor mobiel betalen uiteraard essentieel anders als bij traditionele betalingen.

## *3.5 Welke fases zijn afwijkend voor mobiele betalingen*

Nu we weten hoe een betalingsproces er uit ziet, gaan we kijken naar betalingen waarbij de mobiele telefoon dient als betaalinstrument. Zonder in te gaan op een specifieke oplossing, zal dit hoofdstuk laten zien welke fases van het proces afwijkend zijn wanneer de mobiele telefoon gebruikt wordt om te betalen. In de voorgaande paragraaf hebben we al geconcludeerd dat de transportlaag ten dele verschilt van traditionele betalingen.

### 3.5.1 Initiatie fase

In de initiatiefase van het betaalproces geeft de consument aan welk product hij wil kopen en welke methode hij wil gebruiken om de betaling te doen. Afhankelijk van het scenario gebeurt dit elektronisch, bij betalen op afstand, of mondeling, bij toonbankbetalingen. Deze fase wijkt verder dus niet af van wat er gebeurt met de huidige betalingsmethodes.

### 3.5.2 Betaling

Deze fase van het hele betalingsproces is het belangrijkste deel van een betaling en tevens de fase waarin betalen per mobiele telefoon het meeste afwijkt van de conventionele methodes.

### 3.5.3 Payment Credentials Providing

In de PCP (Payment Credentials Providing) worden de betalingsgegevens verstrekt. Gebaseerd op deze gegevens kan identificatie plaatsvinden. Afhankelijk van de betaalmethode zijn dit onder andere de volgende gegevens:

- Kaartnummer, zowel voor debit- als creditcard kan dat nodig zijn.
- Rekeningnummer van de consument.

Er valt ook te denken aan het verstrekken van extra gegevens, zoals:

- Persoonlijke gegevens zoals adres, naam en dergelijke.

- Gegevens over het gebruikte betaalmedium, zodat deze bijvoorbeeld geblokkeerd kan worden in geval van diefstal of verlies.

Bij de bestaande betalingsmethodes, chippen en pinnen, staan de noodzakelijke gegevens op de pas. De passen bewaren deze data respectievelijk op een chip en een magneetstrip op de kaart en bij methodes zoals PIN gedeeltelijk online. Deze informatie zal bij betalingen met een mobiele telefoon dus ergens anders opgeslagen moeten worden. Hiervoor zijn een aantal manieren denkbaar, welke in het volgende hoofdstuk beschreven worden.

### 3.5.4 Identificatie

Tijdens de identificatie fase vertelt de gebruiker wie hij is. Op een computer doet men dat door een gebruikersnaam in te vullen. Bij het betalen met een debitcard haalt men de pas door een lezer. Op de magneetstrip staat een code en aan de hand van die code kan de gebruiker geïdentificeerd worden. Bij gebruik van de Chipknip gebeurt de identificatie aan de hand van een code die op de smartcard staat.

Bij gebruik van een mobiele telefoon voor het afhandelen van betalingen, zal dit niet mogelijk zijn. De identificatiecode dus ergens anders opgeslagen moeten worden. In principe zal deze code opgeslagen kunnen worden samen met de rest van de betalingsgegevens.

### 3.5.5 Authenticatie

Voor sommige betalingen is authenticatie van de consument nodig. Authenticatie houdt in dat men bewijst dat men is wie men zegt te zijn. Bij pinnen doet men dit door het invoeren van een PINcode. Bij chippen wordt er wel gecontroleerd of er sprake is van een echte officiële Chipknip, maar wordt niet de gebruiker geauthenticeerd. Het Chipknip systeem authenticeert twee kanten op: de Chipknip authenticeert zich naar de PoS, zodat deze weet dat hij met een echte Chipknip te maken heeft, en de automaat authenticeert zich naar de Chipknip, zodat deze weet dat hij gaat betalen aan een echte PoS.

Deze fase wijkt voor mobiel betalen niet af, tweeweg authenticatie is zelfs gewenst voor optimale veiligheid, zoals is te lezen in de bedreigingsanalyse in hoofdstuk 10.

### 3.5.6 Accorderen

In de accordatiefase wordt er aan de gebruiker gevraagd of hij inderdaad de

betaling wil voltooien. Vaak wordt hierbij aangegeven om welk bedrag het gaat en soms aan wie het betaald gaat worden. Deze fase zal niet verschillen voor mobiel betalen.

### 3.5.7 Notificatie

Zowel consument als merchant willen weten dat de transactie succesvol is afgehandeld. Hiervan hangt af of de consument zijn goederen mee krijgt. Dit is met mobiel betalen niet anders.

## *3.6 Conclusie*

Dit hoofdstuk diende een model van een betaalproces op te leveren. Dit model is inderdaad in paragraaf 4.4 opgesteld. Tevens is in paragraaf 4.5 gekeken welke fases voor mobiel betalen afwijken van traditionele betalingen. Deze kennis is voorgelegd aan experts van Interpay ECS en we kunnen daarom aannemen dat het correct is. In het volgende hoofdstuk zal dit model gebruikt worden om aan gebruikers van een mobiel betalingssysteem voor te leggen.

# H4 Eisen van stakeholders

## *4.1 Inleiding*

In dit hoofdstuk dienen we te komen tot een lijst met eisen die de belanghebbenden stellen aan een mobiel betalingssysteem. Deze lijst dient echter alleen eisen te bevatten op technisch gebied.

Deze gegevens zijn van groot belang, omdat een nieuwe betaalmethode niet snel geaccepteerd zal worden door consumenten. Hiervan getuige ook het grote aantal initiatieven dat ontplooid is, maar waarvan er niet één door een breed publiek gedragen wordt. Een nieuw systeem moet daarom terdege rekening houden met deze eisen. Maar een betaalmiddel moet niet alleen door consumenten, maar door alle stakeholders worden geaccepteerd. Merchants nemen uiteindelijk een betaaldienst af, maar zullen zich bij het kiezen van deze dient laten leiden door de wensen van de consument.

Vanwege tijdsdruk kijken we echter niet naar alle stakeholders. De twee genoemde groepen, consumenten en merchants, zijn echter essentieel voor succes en daarom nemen we juist deze twee onder de loep. Daar is ook Interpay aan toegevoegd, omdat zij de opdrachtgever van dit onderzoek is.

Om de technische eisen van merchants en consumenten te inventariseren, is gekeken naar een grootschalig onderzoek dat in opdracht van het ministerie van Economische Zaken door LogicaCMG en HyperCube Business Innovation recent is gedaan. De resultaten daarvan zijn gepubliceerd in [12] en de in paragraaf 2 en 3 staan de samenvattingen uit dit onderzoek. Het was wellicht ter controle beter geweest om dit onderzoek zelf uit te voeren, maar zo groots opgezet zou dit een afstudeeronderzoek op zichzelf vormen. Het onderzoek is goed verantwoord en beschreven en ik acht de resultaten van dit onderzoek daarom betrouwbaarder dan wanneer ik het in rudimentaire vorm zelf had gedaan.

Om de eisen en verwachtingen van Interpay te inventariseren, zijn er interviews afgenomen. In paragraaf 3 staat een uitgebreide uitleg over welke mensen geinterviewd zijn en waarom juist deze.

In de laatste paragraaf van dit hoofdstuk wordt de lijst met eisen samengevat. Daarbij wordt een schifting gemaakt tussen technische en niet-technische eisen.

## 4.2 Eisen van de consument

Voor de consument is er voor zowel betalen op afstand als toonbank betalingen een ruime keuze aan methodes. Een nieuwe methode zal dus voordelen moeten bieden. Gebruik van de mobiele telefoon voor het verrichten van betalingen kan twee grote voordelen hebben:

- Eén betaalmiddel voor zowel toonbank- als betalingen op afstand.
- Geen aparte pas meer nodig om te betalen, de telefoon is genoeg.

Naast het feit dat een nieuwe betaalmethode iets nieuws moet bieden, is er een aantal andere eisen die de consument stelt aan een betalingsproduct:

- **Gebruiksgemak**; een betaalmethode moet simpel in het gebruik zijn. Dat geldt voor eventueel vooraf aanmelden voor een dienst (liever doet men dat helemaal niet, zeker niet voor diensten die men slechts incidenteel gebruikt, zoals parkeren tijdens een dagje Amsterdam) en voor het aantal handelingen om een transactie te doen. Hoe meer het op bekende methodes lijkt, zoals pinnen en SMS'en , hoe gemakkelijker. Op speciale hardware zit de consument ook niet te wachten.

- **Garantie van levering**; de consument wil zeker weten dat hij krijgt waar hij voor betaalt. Zeker bij betalingen op afstand is dat belangrijk. In feite is dat de verantwoordelijkheid van de leverancier en niet die van de betalingsprovider. Deze zou wel ondersteuning kunnen bieden door het bijvoorbeeld mogelijk te maken om betalingen te storneren.

- **Betrouwbaarheid**: consumenten zijn conservatief, zeker waar het geldzaken betreft. Men vertrouwt zijn geld en het afhandelen van betalingen niet graag toe aan kleine en/of onbekende partijen. Een nieuwe betaalmethode zal dus grote namen achter zich moeten hebben. Bij voorkeur die van financiële instellingen, maar ook telecombedrijven of grote merknamen zouden voldoen. Deze merken dienen uiteraard enige affiniteit met bankverkeer te hebben.

- **Privacy**; de zekerheid dat zowel de persoonlijke gegevens als de gegevens over de koop niet aan derden te beschikking worden gesteld, maar alleen gebruikt worden om de betaling te verrichten.

- **Geen extra kosten**; consumenten betalen liever niets extra om een bepaalde betaalmethode te kunnen gebruiken.

- **Dekkingsgraad**; deze eis is absoluut cruciaal. Consumenten zullen een nieuwe methode alleen gaan gebruiken wanneer dit mogelijk is bij veel, of nog beter: alle, merchants en het liefst voor meerdere

scenario's, dus zowel voor toonbank- als betalingen op afstand.

- **Anoniem**; sommige goederen wil een consument anoniem kunnen aanschaffen. Dit betreft voornamelijk goederen (of diensten) uit de zogenaamde 'adult industry'.

- **Snelheid**; een betaling moet niet alleen simpel, maar ook snel kunnen worden gedaan.

Samenvattend wil de consument een betaalmiddel dat snel en betrouwbaar is, dat door alle merchants wordt geaccepteerd, voor toonbank- en betalingen op afstand, en dat anoniem is, of kan zijn.

## *4.3 Eisen van de merchant*

Niet alleen de consument, maar ook de merchant bepaalt het lot van een nieuwe methode van betalen. Hij is zelfs de eerste stap op weg naar succes, zoals in de vorige paragraaf vermeld staat zal een consument alleen overstappen naar een nieuwe manier van afrekenen wanneer de dekkingsgraad heel hoog is. Het is dus van belang dat een nieuwe methode ook voor de merchant voordelen biedt.

De merchant heeft uiteraard zijn eigen eisen die hij stelt aan een dergelijk nieuw product:

- **Betalingsgarantie**; de zekerheid dat hij zijn geld krijgt. Alleen prepaid-systemen kunnen die absolute garantie bieden. Aanbieders van debit-methodes doen dit ook wel, maar daar is het vaak mogelijk voor consumenten om het geld achteraf terug te halen.

- **Continuïteit**; de zekerheid dat de dienst gecontinueerd zal worden. Hiermee hangt samen dat, net als bij consumenten, een merchant niet snel zal vertrouwen op een kleine, onbekende partij, maar het liefst in zee gaat met bekenden zoals banken of gerenommeerde financiële dienstverleners.

- **Eén aanbieder**; de merchant heeft het liefst één aanbieder voor al zijn betaaldiensten.

- **Gebruiksgemak**; niet alleen het gebruiksgemak tijdens een betaling is van groot belang, ook het gemak waarmee een nieuwe methode kan worden aangesloten op de bestaande systemen speelt een belangrijke rol.

- **Kosten**: merchants zijn uiteraard gewend te betalen voor betaaldiensten. Dure diensten zullen uiteraard veel minder snel

afgenomen worden. De merchant vindt een percentage van de transactiewaarde lager dan 5% acceptabel als prijs, mits daarmee het debiteurrisico af wordt gekocht. Is dat niet het geval, dan is een percentage van 2% of lager acceptabel.

- **Dekkingsgraad**; een betaalmethode die slechts door een handje vol consumenten wordt gebruikt is niet interessant voor merchants. Zij zullen een nieuwe betaalwijze pas invoeren wanneer een groot deel van de consumenten hiervan kan en wil gebruik maken.

- **Leeftijd verificatie**; voor de 'adult industry' is het soms nodig om de leeftijd van de consument te kunnen controleren, zeker bij betalingen op afstand is dat lastig. Het zou voor sommige ondernemers dus absoluut een voordeel zijn als de betaaldienst dit kan bieden. Echter niet essentieel.

## *4.4 Eisen en verwachtingen van Interpay*

Er is een viertal mensen die ik geinterviewd heb, te weten
- Dhr. E. Gerritsen (product-manager)
- Dhr. E. van Vuuren (product-manager)
- Dhr. J. de Jong (Interim-hoofd afdeling Ontwikkeling ECS)
- Ir. J. Snijders (oa. Hoofd ECS)

Dhr Gerritsen en dhr. Van Vuuren zijn product-managers en daarmee verantwoordelijk voor het ontwikkelen en uitwerken van (ideeën voor) nieuwe producten en diensten van Interpay ECS. Dhr. de Jong is hoofd van de afdeling Ontwikkeling van E-commerce Services, de afdeling binnen ECS die nieuwe diensten en producten uitwerkt en ontwikkeld. Aan het hoofd van ECS staat Dhr. Snijders, hoewel hij daarnaast nog meer functies heeft binnen Interpay.

Ik heb, na overleg met Dhr. De Jong die mij heeft begeleid, voor deze mensen gekozen, omdat zij binnen de afdeling ECS te maken hebben met, en invloed hebben op, het ontwikkelen van nieuwe producten en diensten. Door middel van de interviews wilde ik erachter komen of Interpay al bepaalde ideeën had voor het gebruik van de mobiele telefoon als betaalinstrument, of misschien zelfs al enigszins uitgewerkte plannen en in hoeverre deze vastomlijnd waren. Verder wilde ik weten of Interpay bepaalde voor- of afkeuren had voor technieken of eventuele partners. De vragen die ik heb voorgelegd waren als volgt:

- Hoe moet het product "betalen met mobiele telefoon" er volgens Interpay uitzien?
- Voor wat voor soort betalingen moet een dergelijk systeem kunnen

worden gebruikt?
- Wie zijn de beoogde gebruikers van een dergelijk systeem?
- Zijn er technieken of partners die wel of juist niet wenselijk zijn?

Van deze interviews heb ik allereerst een verslag naar de betreffende geïnterviewde gestuurd. Zodoende heb ik geverifieerd of mijn conclusies van het gesprek juist waren. De uiteindelijke resultaten van alle interviews gecombineerd staan in de volgende paragraaf.

### 4.4.1 Interview samenvatting

Uit deze interviews is voor mij naar voren gekomen dat voor Interpay feitelijk alle mogelijkheden nog open zijn. Er zijn geen concrete, zelfs geen vage, plannen voor een dergelijk nieuw product. Wel wordt er eerst met de banken overlegd, omdat het de voorkeur heeft deze te betrekken bij een dergelijke nieuwe dienst.

Het is de vraag of de visie van de productmanagers zwaar moet meewegen in het te vormen advies. De wijze waarop zij beide betalen per mobiele telefoon zien, is de invulling die er op korte termijn aan gegeven kan worden en die voortbouwt op de net ontwikkelde dienst van ECS die het opwaarderen van het beltegoed via de mobiele telefoon mogelijk maakt. In feite is hun werk ook om dingen op korte termijn basis te ontwikkelen.

Uit gesprekken met de manager van ECS en van de ECS ontwikkelafdeling blijkt echter dat Interpay het hier wel heeft over een dienst op langere termijn, die een volwaardige betaalwijze moet worden, gelijkwaardig aan de wijze waarop nu de pinpas gebruikt wordt. Dit idee over de vorm van de betaaldienst is dan ook het belangrijkste waarmee we rekening gaan houden in het vervolg van het onderzoek. Overigens is een andere belangrijke conclusie dat het opzetten van een dergelijke nieuwe dienst vooral een groot en ingewikkeld politiek spel is, met veel verschillende spelers die allemaal andere belangen hebben. De grootste moeilijkheid zal daarom wellicht niet liggen in de technische realisatie, maar in het proberen iedereen op één lijn te krijgen. Deze conclusie is verder niet van groot belang voor de rest van mijn onderzoek, waarin ik vooral kijk naar de technische kant van dit verhaal.

Na gesprekken met Dhr. De Jong en Dhr. Snijders heb ik helder wat Interpay verwacht van het gebruik van de mobiele telefoon voor het verrichten van betalingen: een volwaardig betaalsysteem waarbij er best eisen mogen worden gesteld aan de te gebruiken apparatuur. Omdat er binnen Interpay verder niet veel mensen zijn die bezig zijn met het ontwikkelen van nieuwe betaaldiensten, denk ik dat ik met deze gesprekken een helder beeld heb gekregen van Interpay's verwachtingen, en hiermee kan rekening worden gehouden bij het vervolg van dit onderzoek.

## 4.5 Samenvatting

Van alle eisen die de merchant en consument samenstellen aan een nieuwe betaalmethode, is de eis met betrekking tot de dekkingsgraad absoluut de meest cruciale. Merchants willen dat zoveel mogelijk consumenten de methode (kunnen) gebruiken en consumenten willen de methode bij zoveel mogelijk winkels kunnen gebruiken. Het risico bestaat hier dat er een soort 'deadlock'-situatie ontstaat: bij het invoeren van een betaalmethode doen slechts een paar merchants mee, omdat men nog niet weet hoeveel consumenten de dienst zullen gaan gebruiken. Vervolgens zullen niet veel consumenten gebruik maken van de betaalmethode, omdat de dekkingsgraad laag is. Merchants zitten dan te wachten tot veel consumenten de dienst gaan gebruiken en consumenten op hun beurt wachten tot veel merchants de methode aanbieden. Dit scenario zal moeten worden vermeden, wellicht door een grootscheepse invoering bij veel merchants tegelijk

Een soortgelijk scenario bestaat voor de prijs van een betaaldienst. Zowel consumenten als merchants zullen bij een te hoge prijs de nieuwe dienst niet snel in gebruik nemen. Een lage prijs bieden wordt echter gemakkelijker naarmate het aantal transacties stijgt. Een lage introductieprijs, wellicht zelfs onder kostprijs, is dus absoluut gewenst voor een succesvol resultaat.

De kans om betalen via mobiele telefonie van de grond te krijgen, neemt uiteraard toe wanneer er minder spelers in het spel zijn. Er zijn twee gevaren als bepaalde spelers buiten het spel worden gehouden. Wanneer de telecom operators buiten de dienst worden gehouden, moet er heel duidelijk blijken dat het bereik van de dienst groot genoeg is. Wanneer banken niet worden betrokken, moet men bedenken dat consumenten en merchants juist veel vertrouwen hebben in banken, zeker waar het geldzaken betreft. Een nieuwe dienst zal meer consumentenvertrouwen hebben wanneer banken erbij betrokken zijn.

## 4.6 Conclusie

In de voorgaande paragrafen hebben we gezien dat de verschillende belanghebbenden verschillende essentiële eisen stellen aan een mobiel betalingsproduct. Dit zijn echter niet allemaal eisen op technisch gebied, een eis die we aan het begin we stelden aan onze inventarisatie. Hieronder staan daarom nogmaals de eisen, echter nu slechts de eisen die betrekking hebben op het technische vlak:

- **Gebruiksgemak;** zeker een eis op technisch gebied, omdat de opzet van het systeem bepaalt hoe makkelijk er mee te werken valt.
- **Privacy;** tevens een technische eis omdat het systeem de mate van privacy bepaalt die vrijgegeven moet worden bij betalingen.

- **Dekkingsgraad;** de opzet van het systeem zou van invloed kunnen zijn op het feit of het met slechts één, geen of meerdere telecombedrijven werkt. En dit bepaalt op zijn beurt de dekkingsgraad. Deze eis is ook van cruciaal belang.
- **Anoniem;** de inrichting van het systeem bepaalt of betalingen anoniem gedaan kunnen worden. Het gaat daarbij natuurlijk met name om betalingen op afstand.
- **Snelheid;** hangt feitelijk samen met gebruiksgemak.
- **Gemak als van een pinpas**

Het feit dat we hier naar slechts een aantal stakeholders hebben gekeken, betekent niet dat de overige stakeholders niet van belang zijn. Zij zijn slechts niet bekeken vanwege tijdsdruk. Er zal dus nog vervolgonderzoek moeten worden gedaan naar de overige stakeholders en de eisen die zij stellen, voordat er een succesvol systeem ontwikkelt kan worden..

Hetzelfde geldt voor eisen op niet-technisch gebied. Deze zijn wel degelijk van vitaal belang, maar vielen echter buiten de scope van dit onderzoek. Verder onderzoek, bijvoorbeeld op kostentechnisch gebied, is dus zeker gewenst.

De vragen die gesteld zijn tijdens interviews waren gebaseerd op de zaken die nodig waren om te weten voor het vervolg van het onderzoek. Er zijn ook vele interview-methoden, die nu niet gebruikt zijn. De resultaten waren waarschijnlijk niet anders, maar wel op theoretische wijze ondersteund geweest wanneer de interviews volgens een dergelijke methode waren uitgevoerd. Voor een volgend onderzoek is het zeker een verbetering om deze te raadplegen.

# H5 Bestaande mobiele betaalproducten

## *5.1 Inleiding*

Dit hoofdstuk probeert een zo volledig mogelijk overzicht van bestaande mobiele betalingsmethodes te geven. De markt verandert echter snel; er komen doorlopend nieuwe initiatieven op en regelmatig worden er initiatieven weer afgebroken. De inventarisatie beperkt zich niet alleen tot Nederlands initiatieven (paragraaf 1), er is ook naar het buitenland gekeken in paragraaf 2. De resultaten zijn voornamelijk bijeengebracht door deskresearch; zoeken via het Internet, het volgen van referenties bij artikelen, het uitpluizen van websites van electronicafabrikanten en banken en het lezen van een tijdschriften [5] en artikelen[1], [2]. Sommige diensten die inmiddels niet meer actief zijn, staan toch vermeld omdat ze belangrijk zijn geweest in de ontwikkeling van mobiele betalingsmethodes.

Tevens staat er in paragraaf 3 een overzicht van samenwerkingsverbanden, ter volledigheid.

De gevonden informatie is van belang in het volgende hoofdstuk, waar een inventarisatie plaatsvindt van technologieën die geschikt zijn voor een mobiel betalingssysteem. Kennis van bestaande betaaldiensten helpt mee een overzicht te krijgen van de technologie die beschikbaar is.

## *5.2 Nederlandse initiatieven*

In deze sectie staan Nederlandse initiatieven voor betalen met de mobiele telefoon.

### 5.2.1 Tootz

*Gestart in*: december 2003
*Initiatiefnemer(s):* ING Groep

Consumenten die gebruik willen maken van Tootz dienen zich van tevoren aan te melden. Hierbij wordt er door ING een aparte Tootz-rekening geopend voor de gebruiker. Daarop kan een saldo worden gestort vanaf de eigen reguliere rekening. We hebben het hier dus over een prepaid (e-wallet) systeem.

Met Tootz kan men bedragen tot €10,00 afrekenen bij aangesloten webwinkels. Om af te rekenen, klik je op het Tootz-logo en vult men het eigen telefoonnummer in. Daarna moet er gebeld worden met 0800-TOOTZNU. Er is geen wachtwoord nodig, nummerweergave zorgt ervoor dat de gebruiker geïdentificeerd wordt. Het bedrag wordt hierna afgeschreven van het tegoed.

*Per 1 oktober 2004 is de Tootz-service stopgezet.*

### 5.2.2 Premium SMS betalingen

Betalen per SMS is een veel gebruikte methode in Nederland. Dat is ook niet verwonderlijk, aangezien er in 2005 zo'n 14 miljoen GSM-gebruikers waren. Bovendien is deze methode door iedereen te gebruiken en is het gebruiksgemak relatief hoog.

De klant betaalt een vooraf vastgesteld bedrag door een SMS te sturen naar een bepaald nummer. Hierna krijgt hij zijn producten, bijvoorbeeld een ringtone, toegestuurd. Deze wijze waarbij de gebruiker direct betaalt wordt Mobile Originated (MO) genoemd. SMS betaling wordt tegenwoordig ook veel gebruikt voor stemmen bij TV-programma's zoals Idols, en voor diensten zoals nieuws, sport of horoscopen. Bij de laatste abonneert men zich op een nieuwsservice en betaald per ontvangen bericht. Deze wijze waarbij de ontvanger betaalt noemt men Mobile Terminated (MT). De afrekening vindt in alle gevallen plaats via het prepaid beltegoed of de maandelijkse telefoonrekening.

In 2002 oversteeg het aantal betalingen per Premium SMS het aantal chipknip betalingen met respectievelijk 100 miljoen tegenover 81 miljoen. Er zitten ook nadelen aan deze methode. Zo kan er maximaal € 1,50 per bericht worden betaald, met een minimum van € 0,25. Voor producten of diensten die meer kosten dan dit drempelbedrag is het dus noodzakelijk om meerdere SMS-berichten te versturen. Overigens ligt deze grens in andere landen hoger, in Duitsland bijvoorbeeld op € 3,00. Dit bedrag is ook niet simpelweg te verhogen, omdat de telecomproviders dan wettelijk verplicht worden om over een EGI licentie te moeten beschikken. Dat zij dit nu niet hoeven is omdat er uitzonderingen zijn gemaakt voor betalen van kleine bedragen per SMS. Bovendien is het daarnaast de vraag of de telco's het hogere financiële risico willen nemen, aangezien de kans (zo wijst de geschiedenis uit) vrij groot is dat consumenten hun telefoonrekening niet kunnen of willen betalen.

Bovendien is het erg kostbaar voor de aanbieder van het aangeboden product of dienst. Hoewel de SMS-dienstverleners hier erg schimmig over doen, is het zeker dat er in ieder geval 19% BTW naar de belastingdienst

gaat. Afhankelijk van de gebruikte dienstverlener gaat er vervolgens zo'n 50% van het resterende bedrag naar de telecomoperator, 10% naar de aanbieder van de SMS-betaalservice en ongeveer 40 procent komt bij de uiteindelijke aanbieder terecht.

### 5.2.3 Postbank Mobiel Bankieren

*Gestart in*: najaar 2001
*Initiatiefnemer(s):* Postbank, Telfort en Genie.

In het najaar van 2001 startte de Postbank een actie, in samenwerking met Telfort en Genie. Hierbij kregen Postbank klanten een mobiele telefoon cadeau, het allernieuwste model van Siemens (de M35i) wanneer ze 1000 gulden op een spaarrekening zetten. Deze had een zogenaamde SIM-lock waardoor er alleen via Telfort gebeld kon worden, op prepaid basis.

Met deze telefoon was het tevens mogelijk om via een WAP (een hele simpele browser voor mobiele telefoons) geld over te maken naar andere rekeningen, het saldo op te vragen en beurskoersen te bekijken. Postbank droeg hierbij de zorg voor het afhandelen van alle bankzaken, Telfort voor de infrastructuur en Genie voor de WAP-omgeving. Overigens werkte deze bankomgeving alleen in combinatie met de verstrekte telefoon en Telfort als telecomoperator.

Een jaar na de introductie bleek dat een meerderheid de telefoon alleen maar gebruikte om te bellen. Slechts 40 procent gebruikte het toestel om mobiel te bankieren (bron: Postbank). Veel mensen bleken aan hun oude betaalgewoonten vast te houden. Degenen die wel gebruik maakten van m-bankieren deden dit veelal om hun beltegoed op te waarderen of geld over te maken.

*Postbank Mobiel Bankieren is gestopt per december 2004.*

### 5.2.4 Moxmo

*Gestart in*: december 2001.
*Initiatiefnemer(s):* Global Payways NV.

Moxmo is een aanbieder van betaaldiensten voor mobiele en online betalingen. Voor gebruik dienen klanten zich aan te melden bij Moxmo. Ze krijgen dan een aparte Moxmo-rekening. Deze is te beheren via een website en kan worden gevuld door er geld van de eigen bankrekening op te storten.

Met deze mobiele portemonnee kan vervolgens geld worden overgeboekt naar andere Moxmo rekeningen. De consument stuurt dan, per SMS of via

een website, het bedrag en het mobiele nummer van de ontvanger. Daarop volgt een telefoontje door een voicecomputer. De gebruiker wordt dan gevraagd om zijn Moxmo PIN-code. Wanneer deze correct in gevoerd wordt, is de betaling bevestigd.

Behalve tussen gebruikers onderling, zijn ook webshops aangesloten op het systeem. Bij ruim 100 webwinkels is het mogelijk om producten via Moxmo te betalen. Webshops betalen abonnementskosten en een percentage (afhankelijk van de abonnementsvorm tussen 0.75% en 3%) per transactie.

In juli 2003 ging Moxmo een samenwerkingsverband aan met Ogone, leverancier van betaaldiensten.

*Moxmo en moedermaatschappij Global Paywaysˆ NV zijn september 2004 failliet verklaard.*

### 5.2.5 Mobile2pay

*Gestart in*:.juli 2002.
*Initiatiefnemer(s):*. Mobile2Pay.

Om gebruik te maken van Mobile2Pay meldt een consument zich aan op de website van deze mobile payment-provider. De consument geeft Mobile2Pay een doorlopende incasso machtiging om geld af te kunnen schrijven van zijn rekening en krijgt een pincode. Het rekeningnummer wordt gecontroleerd door €2,50 af te schrijven; dit is tevens de jaarlijkse contributie.

Bij ongeveer 50 webwinkels is het mogelijk om, geheel via het Internet, producten of content te kopen met betaling via Mobile2Pay. Daarnaast is het mogelijk om dit per mobiele telefoon aan te schaffen.

Een consument ziet een product in bijvoorbeeld een magazine of wil een bepaalde content. Om het product aan te schaffen, stuurt hij de bijbehorende productcode naar een bepaald telefoonnummer. Dit kan via SMS (mobiele betalingen) of via het Internet. De Mobile2pay gebruiker wordt vervolgens gebeld op zijn mobiele telefoon en een voicecomputer vraagt om de bestelling te bevestigen met de Pincode

Hierna wordt het bedrag per incasso direct afgeschreven. De consument kan via een persoonlijke webpagina zien welke aanschaffen hij gedaan heeft en eventueel betalingen storneren. Na 24 dagen (wanneer de storneringstermijn is verstreken) wordt de merchant uitbetaald. Het minimum bedrag bedraagt €2,50 en er kan maximaal €150 betaald worden via het systeem.

De merchant betaald per transactie gemiddeld €0,45 plus 1,3% (voor fysieke

goederen) of 1,6% (voor content) van het transactiebedrag.

### 5.2.6 Betaalnummers

Betaalnummers (0900 of 0906-nummers) zijn speciale telefoonnummers. Dat houdt in dat het bellen naar een dergelijk nummer per minuut of per gesprek extra kosten met zich meebrengt, bovenop de normale telefoonkosten. Dit nummer werkt onafhankelijk van het gebruikte telecom-netwerk. De extra kosten komen op de telefoonrekening of gaan af van het beltegoed.

Om een product af te rekenen belt de consument het 0900 nummer. Wanneer er een vast bedrag moet worden afgerekend, zijn dat de eenmalige extra kosten per gesprek. Een voicecomputer geeft vervolgens een code af die toegang verschaft tot het gewenste product.

Soms wordt er afgerekend per tijdseenheid, bijvoorbeeld de tijd dat men op een website rondsurft. Het betaalnummer brengt dan extra kosten per minuut met zich mee. Nadat de consument dit nummer heeft gebeld, krijgt hij een code die hem toegang verschaft. Zolang de telefoonverbinding in stand is, kan men over de website beschikken. Zodra de verbinding verbroken wordt, heeft men ook geen toegang meer.

### 5.2.7 Park-line

Park-line is een methode om parkeergeld te betalen in onder andere Groningen, Rotterdam, Den Haag, Emmen, Haarlem, Delft en Deventer.

De consument dient zich van tevoren aan te melden, waarbij hij onder andere een doorlopende incasso machtiging tekent. De consument dient inschrijfgeld en een jaarlijks abonnementsgeld te betalen en ontvangt een zogenaamde transponder.

Wanneer men wil parkeren bij een aangesloten parkeerplaats, zoekt je het nummer van de zone op, die op borden in de buurt staan, en legt de transponder op zijn dashboard.. Hij belt een 0900-nummer van Park-line en geeft de gevonden code door. Dit kan ook via een I-mode website. Wanneer men klaar is met parkeren, neemt men weer contact op met Park-line, zodat de meter gestopt wordt. Het parkeergeld wordt periodiek afgeschreven per incasso.

De parkeerwachter kan de transponder draadloos uitlezen om te zien of de consument zich wel aan heeft gemeld.

### 5.2.8 Mobiel opwaarderen

Mobiel opwaarderen is een methode om prepaid beltegoed op te waarderen, zonder dat daarvoor een kraskaart gekocht moet worden. Deze dienst wordt door de telecomproviders aangeboden aan hun klanten, maar de onderliggende dienst is ontwikkeld door Interpay.

Om deze dienst te kunnen gebruiken, moet men zich van tevoren aanmelden. Hiertoe wordt een telefoonnummer gebeld, waar door een voicecomputer een aantal gegevens gevraagd wordt. Hierna wordt een pincode verstrekt. De provider maakt €0,01 over naar de rekening van de gebruiker, waarbij de pincode in de bijbehorende omschrijving staat.

Met deze pincode kan het beltegoed worden opgewaardeerd. Ook dit gaat door het bellen naar het servicenummer, waar de opwaardeeractie door een voicecomputer afgehandeld wordt. Mobiel opwaarderen is ook mogelijk vanuit het buitenland.

### 5.2.9 Minitix

Minitix is een prepaid betaalmethode voor het Internet, ontwikkeld door Rabobank, maar ook beschikbaar als men hier geen klant is. Voor Minitix moet men zich aanmelden en vervolgens geld storten op de daarmee geopende rekening.

Betalen gaat vervolgens op eenvoudige wijze bij de aangesloten webwinkels. De pagina van de webshop hoeft niet te worden verlaten: na een druk op het Minitix logo wordt gevraagd een gebruikersnaam en wachtwoord in te vullen. Hierna wordt de betaling meteen voldaan.

### 5.2.10 KPN Switchpoint

Switchpoint is een volledige productlijn van KPN die zich richt op betalen op afstand. De betaling gaat via reversed billing (het verschuldigde bedrag komt op de KPN-rekening) en is in de meeste gevallen alleen geschikt voor KPN-klanten. De lijn bestaat uit 7 producten:

- Switchpoint Modem
- Switchpoint Telefoon
- Switchpoint Incasso
- Switchpoint Mobile
- Switchpoint Creditcard
- Switchpoint SMS

Hiervan zijn alleen Telefoon, SMS en Mobile geschikt om mobiele betalingen mee te verrichten, de andere producten zijn gericht op internetbetalingen.

Switchpoint Telefoon is bedoeld om consumenten betaalde toegang te verschaffen tot websites en werkt op dezelfde wijze als 0900-betalingen. Switchpoint- SMS en Mobile werken op basis van Premium SMS.

### 5.2.11 Proef met contactloos parkeren

Q-park is een exploitant van parkeergarages in Nederland, België, Denemarken, Duitsland, Frankrijk, Engeland en Ierland. In Nederland is Q-Park marktleider met 130 openbare parkeeraccommodaties en 65.000 parkeerplaatsen in vrijwel alle belangrijke steden.

In haar Amsterdamse parkeergarage Byzantium gaat Q-park Near Field Communication inzetten als toegangskaart. Bij het binnenrijden van de parkeergarage houdt men de mobiele telefoon voor de toegangsapparatuur en krijgt men toegang. Op dezelfde wijze wordt de parkeergarage weer verlaten. De parkeerkosten worden achteraf, maandelijks, afgerekend.

Men moet hiervoor een geschikte mobiele telefoon hebben, die momenteel alleen door Nokia en Samsung op de markt zijn gebracht.

## *5.3 Buitenlandse initiatieven*

In de hierop volgende paragrafen worden een aantal opvallende buitenlandse initiatieven op het gebied van m-commerce getoond.

### 5.3.1 M-banxafe

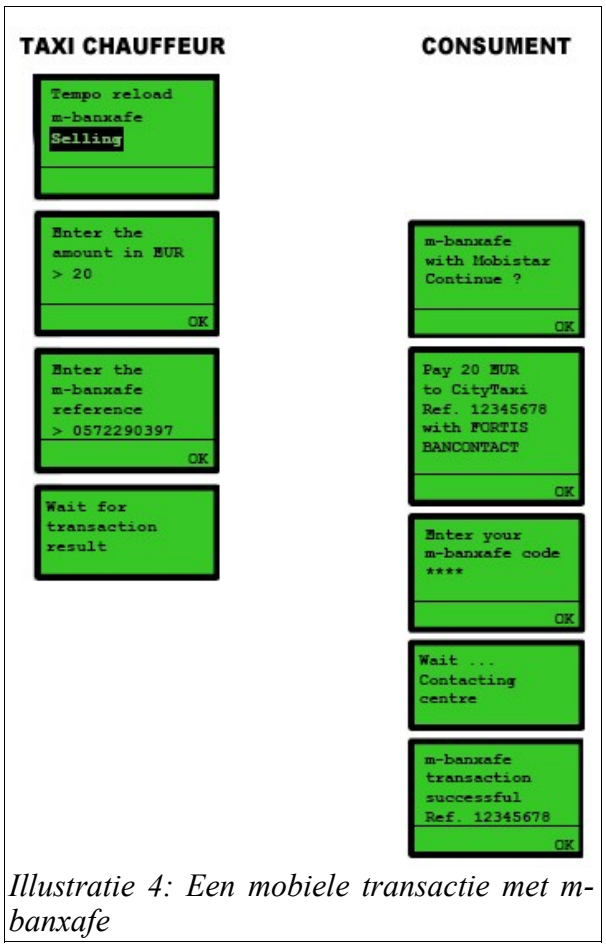
Banxafe is een veiligheidslabel voor m-commerce en e-commerce, dat in 2000 geïntroduceerd werd door de Belgische banken en de Belgisch nationale payment-processor Banksys.

M-banxafe is een dienst die voortkomt uit een samenwerkingsverband tussen telecomoperator Mobistar, Banksys en Gemplus Smartcard Solutions. Alleen klanten van Mobistar kunnen daarom van de dienst gebruik maken.

Om gebruik te maken van m-banxafe is een speciale SIM-kaart nodig, die gratis door Mobistar verstrekt wordt. Met deze aangepaste chip en de software (Java SIM Toolkit applicatie met Smart Card security) kunnen nu betalingen worden verricht. Het nummer van de SIM (IMSI) wordt gekoppeld aan het bankrekeningnummer van de klant, die een speciale PIN-code voor het systeem toegewezen heeft gekregen. Betalingen kunnen nu direct ten laste van de bankrekening komen.

Op dit moment biedt m-banxafe de mogelijkheid om het beltegoed op te waarderen. In 2003 waren er al 850.000 opwaardeertransacties. Vanaf maart 2006 is daar de Bankbalance dienst aan toegevoegd, een service om via de GSM het banksaldo te raadplegen.

M-banxafe gaat echt mobiele betalingen mogelijk maken. Hierbij hoort het overmaken via de GSM van bedragen naar andere rekeningen, maar ook realtime betalingen in bijvoorbeeld een taxi. Een betaling zou als volgt kunnen gaan:



*Illustratie 4: Een mobiele transactie met m-banxafe*

Wanneer deze diensten beschikbaar komen, is echter nog niet bekend.

### 5.3.2 NTT Docomo

In Japan is het mogelijk om met bepaalde mobiele telefoons te betalen. NTT Docomo biedt daar een betaaldienst dat gebruik maakt van Near Field Communication (NFC). Het gebruikte toestel moet daarvoor geschikt zijn en de voorzien zijn van een FeliCa smartcard, het onderliggende systeem.

FeliCa is het Contactless Smart Card systeem van Sony. Overigens is

Philips industrieel marktleider op gebied van contactloze smartcards. Philips en Sony zijn in 2002 een samenwerking aangegaan voor het ontwikkelen van nieuwe NFC-technologie.

NTT Docomo werkt samen met 39 Japanse providers, waardoor bijna alle gebruikers in Japan in principe gebruik kunnen maken van het systeem, mits ze, zoals gezegd, een geschikt toestel hebben.

De mobiele telefoon is door deze service te gebruiken om bij meer dan 9000 winkels te kunnen betalen. Ook kunnen allerlei soorten tickets, zoals treinkaartjes of concertkaarten, op de telefoon worden opgeslagen, waardoor deze het toegangsbewijs kan vormen.

## *5.4 Samenwerkingsverbanden*

Wereldwijd zijn er een aantal belangengroeperingen op het gebied van m-commerce. Deze fora hebben allemaal hun eigen doelstellingen, maar behartigen vooral de gemeenschappelijke belangen van hun leden en proberen bepaalde standaards geaccepteerd te krijgen. Er zijn meer fora geweest dan de onderstaande, maar deze zijn ofwel opgeheven ofwel opgegaan in één van onderstaande groeperingen.

### 5.4.1 Mobile Payment Forum

Het Mobile Payment Forum is een wereldwijd initiatief van een aantal grote bedrijven uit de telecom- en financiële sector en is opgericht door MasterCard, Visa en JCB Cards in de maand november van 2001. Het doel van het Forum is “to realize the full potential of mobile commerce”[..] en dit wil men bereiken door de expertise op het gebied van m-payments te vergroten om zo standaarden te creëren voor zowel te gebruiken technology als functionaliteit.

De samenwerking richt zich verder op:

- De ontwikkeling van de markt voor m-payments versnellen
- Versimpelen van gebruikservaring bij het verrichten van een betaling
- Een gezamenlijke richting bepalen voor de toekomst van m-commerce.

Het MPF heeft een dertigtal leden, voornamelijk vooraanstaande bedrijven waaronder:

- T-mobile
- Mastercard
- Visa
- Nokia
- Orange

- Vodafone
- JCB
- Rabobank

### 5.4.2 Mobey Forum

Het Mobey Forum is in mei 2000 opgericht door een aantal belangrijke banken, waaronder ABN Amro, Deutschebank, HSBC en Nordea. Later kwam daar fabrikant Nokia bij en een aantal softwarebedrijven zoals Accenture, Meridea en HP zijn als 'associate members' verbonden aan deze groep.

De missie van het forum is:
*"The mission of Mobey Forum is to encourage the use of mobile technology in financial services. Mobey Forum aims to accelerate the take-off of user-friendly mobile financial services by promoting open, non-proprietary technology standards."*

Mobey forum is voorstander van het ontwikkelen van techniek voor zowel micro- als macropayments. Er zijn geen telecomproviders verbonden aan dit forum.

### 5.4.3 Mobile Electronic Transactions forum

In april 2000 is het Mobile Electronic Transactions Forum (MeT) door een drietal handset-fabrikanten opgericht. De drie fabrikanten, Motorola, Ericsson en Nokia, werden al snel bijgestaan door Panasonic, Siemens en NEC. Motorola heeft zich later teruggetrokken.

Ook andere leden sloten zich aan (ongeveer 50 in totaal), waaronder Orange, Interpay en Telefonica. Het forum leek een stille dood gestorven, maar in 2005 is het nieuw leven ingeblazen. Het bestaat nu alleen nog uit de handset-fabrikanten Ericsson, Nokia, NEC en Panasonic.

De focus van het MeT is gericht op mobiele transactie met behulp van Near Field Communication (NFC). Daarmee beperkt het zich dus tot betalingen die niet op afstand zijn. De samenwerking heeft tot een aantal succesvolle proeven geleid, onder andere in Frankrijk, Duitsland en Finland

## *5.5 Conclusie*

Deskresearch heeft een flinke lijst opgeleverd van initiatieven op het gebied van m-commerce. Dat deze lijst niet compleet is, is duidelijk. Sommige initiatieven zijn bewust uit deze opsomming gehouden, omdat ze inmiddels

al failliet zijn en verder geen rol van betekenis hebben gespeeld. Het bleek ook moeilijk te zijn om duidelijkheid te krijgen over buitenlandse initiatieven. Over grote projecten is op het Internet flink wat te vinden, maar er is niet met zekerheid te zeggen dat er over kleinere projecten ook gepubliceerd is. Het raadplegen van experts is in die zin wel gebeurd, dat zij rapporten publiceren, maar wellicht had telefonisch contact een nog completere lijst opgeleverd.

Uit al deze initiatieven kan wel wat geleerd worden. Op het gebied van m-commerce hebben de initiatieven elkaar een tijd lang snel afgewisseld. Veel diensten zijn vrij snel na de introductie alweer opgeheven, sommigen zelfs al voordat ze überhaupt de markt hadden bereikt. Het grote manco lijkt hierbij te zijn dat deze betaalmethodes een veel te kleine doelgroep hadden om succesvol te kunnen worden. Ook waren veel van deze diensten te ingewikkeld om breed geaccepteerd te kunnen worden. De diensten die nu nog over zijn, hebben een relatief grote doelgroep. Het komen en gaan van nieuwe initiatieven is ook afgenomen, de markt heeft zich meer 'gesettled'.

Er zijn op het gebied van m-commerce veel samenwerkingsverbanden, waarvan de drie grootse in dit hoofdstuk zijn besproken. Elk van deze fora heeft zijn eigen belanghebbenden en hun ideeën staan niet bepaald in één lijn. Nokia lijkt in ieder geval niet van plan de boot te missen, zij zijn in elke groepering vertegenwoordigd. De vraag is of de fora op deze manier bijdragen aan het ontwikkelen van m-commerce, of dat ze het alleen maar vertragen, omdat ze zulke verschillende belangen en ideeën hebben. Het nadeel van al deze fora is ook dat het in de meeste gevallen geen multidisciplinaire groepen zijn. Alleen het Mobile Payment Forum is dit wel, en dit lijkt dan ook de meest invloedrijke groep te zijn. Telecomproviders zijn erg ondervertegenwoordigd in de fora, alleen bij MPF zijn er een aantal aangesloten.

# H6 Inventarisatie bruikbare technologieën

Dit hoofdstuk levert een inventarisatie op met (combinaties van) mogelijk bruikbare technologien om een mobiel betalingsstysteem te implementeren. Uit het model dat is opgesteld in hoofdstuk 4 weten we welke gebieden afwijken voor een mobielbetalingssysteem en dat zijn dan ook de gebieden waarvoor er een oplossing dient te komen. Deze fases zijn allemaal uit de betalingsfase zelf: de Payment Credentials Provisioning en de Identificatie fase. Deze twee hangen overigens nauw samen. Deze oplossingen dienen te voldoen aan de eisen die er in de conclusie van hoofdstuk 5 aan gesteld worden. Daar zullen zij op getoetst worden.

In de eerste paragraaf zullen we de mogelijkheden bekijken hoe de payment credentials verstrekt kunnen worden. Hiervoor zijn een vijftal manieren die beschreven worden en waar een waardeoordeel aan gekoppeld wordt.

Ook hebben we in hoofdstuk 4 gezien dat de wijze van transport van data (deels) verschilt met traditionele betalingen. In paragraaf twee bekijken we twee manieren van datatransport; via het GSM-netwerk of met gebruik van Near Field Communicatie.

Deze technische oplossing dienen in zo groot mogelijk mate te voldoen aan de eisen zoals die beschreven staan in de conclusie van hoofdstuk 5.

## *6.1 PCP en Identificatie*

In de Payment Credentials Provisioning-fase worden de betalingsgegevens verstrekt. Waar deze precies uit bestaan, hangt af van de uiteindelijke implementatie, maar in ieder geval moet het bestaan uit het rekeningnummer van de consument. Omdat de manier van betalings-gegevens verstrekken afwijkt van conventionele methodes, zal er een andere wijze moeten worden gebruikt. Dit zou op een vijftal manieren kunnen worden opgelost. Deze staan in de volgende paragrafen beschreven.

### 6.1.1 Verstrekken via de handset

Eén oplossing om de betalingsgegevens te verstrekken, is de handset dit te laten doen. De data wordt eenmalig op de handset ingevoerd, hetzij geautomatiseerd, hetzij handmatig door de gebruiker en kan daarna gebruikt worden tijdens transacties. De betalingsgegevens zijn echter gevoelige data. Dit betekent dat het op een veilige manier op de handset opgeslagen zal moeten worden, zodat ze niet door derden uit te lezen zijn. Er zijn drie

manieren om de data veilig te bewaren.

#### 6.1.1.1 SIM-kaart

Ten eerste kunnen betalingsgegevens op SIM worden opgeslagen. Een nadeel daarvan is dat de SIM eigendom is van de telecomprovider. Wanneer betalingsgegevens hier worden opgeslagen, zal er een samenwerkings-verband moeten worden aangegaan. Omdat we al hadden geconcludeerd dat een hoge dekkingsgraad een vereiste is voor succes, betekent het gebruik van de SIM dat er overeenstemming moet worden bereikt met het liefst alle, maar in ieder geval het grootste gedeelte, van de telecomproviders Dit zal een lastig politiek spel zijn en derhalve een nadeel van deze oplossing.

De gemiddelde levensduur van een SIM-chip bedraagt nog geen drie jaar. Dat betekent dat de consument opnieuw de betalingsgegevens op de chip moet (laten) zetten wanneer hij een nieuwe krijgt. Dit heeft als voordeel dat er op dat moment meteen aanpassingen kunnen worden gedaan, bijvoorbeeld omdat er veranderingen zijn geweest aan het betalingssysteem. Het nadeel is uiteraard het meerwerk dat hieraan vastzit.

Consumenten kunnen tevens wisselen van telecomprovider. Hierbij wordt hun oude SIM ongeldig en vervangen door een versie van de nieuwe provider. Bij de ontwikkeling van het systeem zal er dus rekening mee gehouden moeten worden dat een consument absoluut niet altijd bij dezelfde telco zal blijven.

Gebruik van de SIM maakt het wel makkelijk om het toestel te identificeren in het (GSM-) netwerk, via het gekoppelde IMSI-nummer. Identificatie van de handset in het GSM-netwerk is nodig wanneer dit netwerk als transportlaag zal worden gebruikt.

#### 6.1.1.2 Dualchip toestel

Een meer voor de hand liggende oplossing is daarom een toestel met twee chips, de zogenaamde dualchip handset. De eerste chip (SIM) is van de provider van de consument en zorgt ervoor dat deze alle door de telecom operator geboden functionaliteit van het netwerk kan gebruiken. Op de tweede chip, WIM genoemd (WAP Identity Module), kan dan de betalingsdata veilig worden opgeslagen.

Identificatie van de handset in het netwerk wordt hiermee lastiger, omdat dit (bij de huidige netwerken) alleen op basis van IMSI nummer kan. Er zal dan een koppeling moeten worden gemaakt met dit nummer, iets wat hoogstwaarschijnlijk ook medewerking van de telecomoperator vereist. Dit is alleen van toepassing wanneer het GSM-netwerk als transportlaag wordt gebruikt.

Er zijn al een aantal succesvolle pilots van mobiel betalen geweest met dualchip toestellen via het GSM-netwerk. Een voorbeeld hiervan is de pilot van Nokia, Visa en de Nordea bank in Finland.

Gebruik van een aparte chip brengt uiteraard extra kosten met zich mee en stelt tevens extra eisen aan de handsets die gebruik kunnen maken van het betalingssysteem.

#### 6.1.1.3 Secure Memory Card

Een Secure Memory Card, afgekort SMC, is een tweede manier om data zo op te slaan dat het niet door derden uit te lezen valt. Deze oplossing werkt verder hetzelfde als bij een dualchip handset gebaseerde oplossing. Het verschil zit hem dus alleen in de gebruikte media, een SMC in plaats van een chip.

Nadeel van deze oplossing zijn de kosten die gebruik van een dergelijke kaart met zich meebrengt. En ook deze oplossing stelt extra eisen aan het gebruikte toestel.

### 6.1.2 Consument

De consument kan natuurlijk ook zelf de gegevens verstrekken aan het systeem wanneer dit erom vraagt. Hier zijn verschillende mogelijkheden:

- **Dicteren**; de consument dicteert al zijn gegevens aan de merchant, die ze vervolgens invoert in het systeem. Het mag duidelijk zijn dat dit verre van ideaal is en absoluut vertragend werkt.

- **Typen**; de klant voert de gegevens zelf in met (bijvoorbeeld) behulp van een toetsenbord, aan zijn mobiel of bij de merchant.

- **Spraakherkenning**; feitelijk hetzelfde als bij dicteren, de klant somt zijn gegevens op en door middel van spraakherkenning worden ze in het systeem gevoerd.

Omdat alle implementaties van deze methode zeer vertragend werken, en bovendien vereisen dat de klant al zijn gegevens kent. Gezien het feit dat dit zeer waarschijnlijk onder andere reeksen van cijfers zullen zijn, kunnen we wel concluderen dat deze wijze van het verstrekken van betalingsgegevens niet voldoet. Bovendien kan dit fraude door consumenten in de hand werken, doordat zij verkeerde cijferreeksen zouden kunnen opgeven. Dit is uiteraard niet wenselijk.

### 6.1.3 Server

De betalingsgegevens kunnen worden opgehaald vanuit een centrale server. De gegevens van alle consumenten die gebruik maken van het systeem staan hier opgeslagen. Aan de hand van een uniek ID dat naar de server wordt gestuurd, kunnen dan de betalingsgegevens (in ieder geval het rekening-

nummer) worden opgezocht.

Wanneer men kiest voor een oplossing die gebruikt maakt van het GSM-netwerk, is dit misschien wel de beste oplossing. Het unieke identificatie-nummer is dan al beschikbaar (elke SIM-kaart heeft zijn eigen unieke IMSI nummer) en aan de hand daarvan kan de consument aan zijn rekening worden gekoppeld.. Er zijn minder eisen aan de te gebruiken handsets en geen kosten voor een extra SIM of SMC-kaart. Bovendien hoeft er bij een wijziging van de betalingsgegevens, bijvoorbeeld wanneer de consument een andere bank(rekening) krijgt, geen, relatief lastige, update van de chip te worden gedaan. De gegevens kunnen op de server gewijzigd worden. Een nadeel is echter dat er bij overstappen naar een andere telecomprovider een nieuw IMSI-nummer gekoppeld moet worden aan deze gegevens. Het is dus een afweging welke van de twee situaties vaker voor zal komen.

Wanneer gekozen wordt voor NFC, is deze oplossing minder goed van toe-passing. Er moet in dat geval al ergens op de telefoon een uniek identifi-catienummer komen te staan, daarmee worden er al bepaalde eisen aan de handset gesteld, en dan kan net zo goed het rekeningnummer meteen worden opgeslagen, in plaats van een ID dat dan later weer gekoppeld wordt aan het rekeningnummer.

## *6.2 Transportlaag*

Met de transportlaag wordt de wijze bedoeld waarop berichten worden uitgewisseld tussen (applicatie op de) MS en het betalingsnetwerk. Er zijn een tweetal mogelijkheden, waarvan de eerste een aantal sub-mogelijkheden biedt.

### 6.2.1 GSM netwerk

Een van de manieren om de berichten van het betalingssysteem te versturen, is gebruik te maken van het GSM-netwerk. Alle mobiele telefoons kunnen gebruik maken van de mogelijkheden die het netwerk biedt. Om de risico's van een eventueel gebruik te kunnen inschatten, zullen we in deze paragraaf bekijken hoe het GSM-netwerk functioneert.

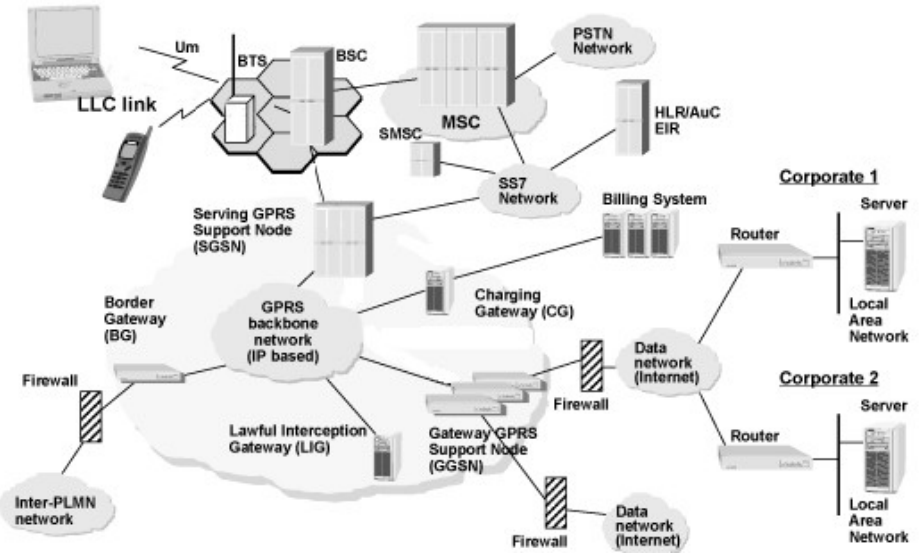
#### 6.2.1.1 GSM netwerk

De afkorting GSM staat voor Global System for Mobile communications, hoewel het hiervoor "Groupe Spéciale Mobile" betekende. GSM is de tweede generatie (2G) mobiele telefonie. De verschillen met de eerste generatie mobiele netwerken zijn:

- Digitaal versturen van de spraak over het netwerk
- Andere frequentiebanden, in combinatie met een honingraat-opzet van het netwerk zorgen voor een veel hogere dekkingsgraad bij 2G-netwerken.

### 6.2.1.2 Architectuur van het netwerk

De onderstaande tekening laat zien hoe het GSM-netwerk in elkaar steekt:




*Illustratie 5: Structuur van het GSM/GPRS netwerk*

Het mobile station, ook wel mobile device genoemd, maakt verbinding met de GSM-mast (Base Transceiver Station, **BTS**) met het sterkste signaal. Dat zal meestal de dichtstbijzijnde zijn, maar omdat een BTS maar een beperkt aantal gesprekken tegelijk kan afhandelen, is dat niet noodzakelijk het geval.

Het mobile device wordt uniek geïdentificeerd door zijn International Mobile Equipment Identity (**IMEI**). Tevens heeft het MS een Subscriber Identity Module (**SIM**). Deze smartcard bevat de International Mobile Subscriber Identity (**IMSI**) , aan de hand waarvan het GSM-systeem de gebruiker kan identificeren. IMEI en IMSI zijn onafhankelijk van elkaar.

De BTS wordt gemanaged door een Base Station Controller, **BSC**. De BSC zorgt onder andere voor handovers (wanneer een MS naar een andere BTS over moet schakelen) en de verbinding met het Mobile Switching Centre, de **MSC**. De BSC kan meerdere BTS'en beheren. Zo'n cluster vormt samen het **BSS**, Base Station Subsystem.

Het Mobile Switching Centre zorgt het voor alle noodzakelijke services als registratie, authenticatie, routing naar andere mobiele devices en het bijwerken van de locatie van het MS. Dit gebeurd in combinatie met een aantal andere onderdelen, die samen met het MSC het Network System vormen. Overdracht tussen deze onderdelen gaat via het Signaling System 7, **SS7**.

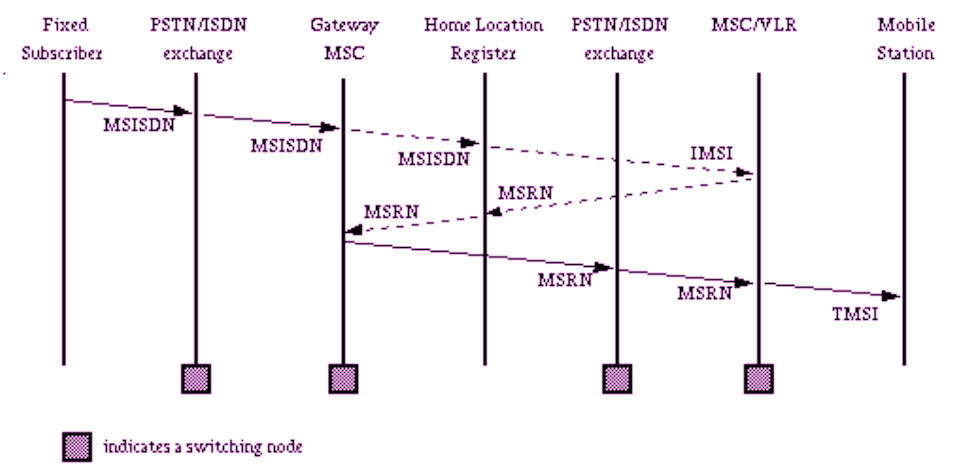
Vanuit het MSC wordt rechtstreeks de verbinding met het vaste-, **PSTN** of **ISDN**, telefoonnetwerk gemaakt.

Voor de authenticatie van de gebruiker op het netwerk wordt gezorgd door de Authentication Centre, **AuC**; een database die een kopie van de geheime sleutel van de gebruikers bevat. Hiermee wordt authenticatie verricht en tevens het verkeer over het netwerk versleuteld. In het Equipment Identity Register (**EIR**) staat een lijst van alle mobile stations op het netwerk, aan de hand van hun IMEI-code. In deze database staat voor elk toestel de toegang een status (*whitelisted*, *greylisted* of *blacklisted*) op basis waarvan toegang tot het netwerk verleend of juist ontzegd kan worden. Dit laatste kan bijvoorbeeld wanneer een toestel als gestolen te boek staan.

Met behulp van de **HLR** (Home Location Register) en **VLR** (Visitor Location Register) kan het MSC zorgen voor het routen van de gesprekken en berichten over het netwerk. De HLR bevat allerlei semi-permanente informatie over alle gebruikers, waaronder het IMSI, de **MSISDN** (het telefoonnummer) en de huidige locatie. Dit vertelt bij welke VLR de gebruiker momenteel geregistreerd is. Typisch is er dus maar één HLR per netwerk, hoewel het uiteraard een gedistribueerde database kan zijn. Het is niet ondenkbaar dat, vanwege de enorme groei die deze netwerken (en daarmee de HLT-database) hebben doorgemaakt, er in de toekomst een structuur met meerdere HLR's zal komen.

De VLR is een database met tijdelijke informatie. Wanneer een toestel contact maakt met het netwerk, steeds als deze opstart of wanneer het van locatie is veranderd en contact met een andere BTS heeft gelegd, krijgt het van de VLR een identificatiecode toegewezen, het Mobile Station Roaming Number (**MSRN**). Deze wordt naar het HLR van het toestel gestuurd, die immers altijd de huidige locatie bijhoudt. In het VLR staat dus een koppeling tussen het IMSI van het device en het eraan toegewezen MSRN.

Bij een verbinding kan het toestel nu als volgt in het netwerk gevonden worden:




*Illustratie 6: Routing van een verbinding naar een MS*

### 6.2.1.3 Berichten versturen

Data versturen over het netwerk is logischerwijs mogelijk op drie manieren:

- Met behulp van een dataconnectie
- Met behulp van **SMS** (Short Message Service) berichten
- Met behulp van Unstructured Suplementary Data Service (**USSD**-) berichten.

Huidige (2G) netwerken bieden de mogelijkheid tot dataconnecties. Deze kunnen worden opgezet vanaf het MS. Het MSC zal deze verbindingen via het SS7 netwerk naar de Serving GPRS Support Node (**SGSN**) sturen. Vanaf hier kan de verbinding worden gerouteerd naar bijvoorbeeld het Internet. Een voordeel van deze manier van berichten versturen is dat het, in tegenstelling tot SMS, connection-based is. Een nadeel is dat alleen het mobile station de verbinding kan initiëren, er kan geen verbinding vanuit het netwerk naar het MS worden gestart. Een ander nadeel is dat het een aantal secondes duurt voordat een verbinding tot stand is gebracht. De verbinding gaat op basis van IP.

SMS-berichten zijn korte berichten van maximaal 160 karakters. Het is een store-and-forward en transaction-oriented protocol. Een SMS bericht die vanaf de MS wordt gestuurd, wordt via het BSS afgeleverd op de SMS Centrale (**SMSc**). Deze zal proberen om het bericht af te leveren op zijn bestemming. Andersom zal een SMS bericht dat naar een MS toe wordt gezonden ook op de SMSc terecht komen. Dat betekent dus dat de gegevens op de SMSc bewaard wordt zolang het nog niet op het MS kon worden afgeleverd. SMS berichten kunnen niet naar een applicatie op de GSM worden gestuurd, maar komen terecht in de 'inbox' van de telefoon. Deze zou uiteraard wel uitgelezen kunnen worden door een bepaald programma.

USSD is een session-based manier om berichten te sturen over het GSM-netwerk. De responstijden zijn veel lager dan bij SMS, dat immers store-and-forward is en daardoor een stuk langzamer. USSD werkt op alle bestaande mobiele telefoons en alle netwerken. Het maakt bij deze service niet uit of een gebruiker op zijn eigen netwerk zit, of dat hij aan het roamen is. USSD wordt nu bijvoorbeeld gebruikt voor chat-applicaties.

#### 6.2.1.4 Conclusie

Van de mogelijkheden die het GSM-netwerk biedt voor het versturen van data, is USSD het meest geschikt voor een eventuele methode om mobiel te betalen. Het feit dat de responstijden laag zijn, veel lager dan bij een dataconnectie of SMS-verkeer, is daarbij erg belangrijk. Eén van de eisen die worden gesteld aan een dergelijk systeem is immers een snelle afwikkeling van de betaling; zowel consumenten als merchants hebben geen zin om lang te wachten voordat een betaling voltooid is. Bovendien is de connection-based eigenschap van USSD een ander groot voordeel boven het gebruik van SMS.

Wat men in het achterhoofd moet houden, is dat het GSM netwerk op den duur vervangen zal worden door andere netwerken. Nu al zijn telecombedrijven bezig met het uitrollen van een nieuwe, derde, generatie netwerk, het UMTS-netwerk. Het is daarmee niet gezegd dat de mogelijkheden van de huidige, 2G, netwerken in de toekomst niet meer beschikbaar zijn.

Verkeer over het GSM-netwerk is eenvoudig af te luisteren, omdat al het verkeer over grote afstand door de lucht verzonden wordt. Het netwerk versleuteld deze boodschappen wel, maar de betrouwbaarheid daarvan staat ter discussie. Dit is dus iets om rekening mee te houden in een eventueel ontwerp.

### 6.2.2 Near Field Communicatie

Near Field Communication is een uitbreiding op het gebruik van RFID tags. RFID staat voor Radio Frequency Identification, een methode om op afstand informatie te lezen uit RFID chips (“tags”), die op of in objecten zitten.

De originele RFID technologie is eenrichtingsverkeer: de tag kan alleen worden uitgelezen, er kan niets opgeslagen worden. De tags zijn ook passief, wat wil zeggen dat ze niet zelf signalen uitzenden. RFID tags hebben dan ook geen energiebron nodig. Bij het uitlezen ervan gebruikt de chip uiteraard wel energie, maar deze wordt gehaald uit de radiogolven (inductie). De afstand waarop uitgelezen kan worden, hangt af van de

gebruikte frequentie.

Near Field Communication is ontwikkeld door Philips, Sony en Nokia en is wel een tweeweg protocol. Behalve uitlezen is dus ook opslaan mogelijk. De verbinding is contactloos, de verbinding wordt gemaakt door een korte 'touch', even het toestel vlakbij een ander NFC-apparaat houden, waarna ze elkaar ontdekken en verbinding maken. Philips onderscheidt vier categorieën van NFC-applicaties:

- **Touch and Go**; applicaties waarbij de gebruiker alleen zijn toestel vlakbij de lezer hoeft te houden. Dit soort applicaties zijn vooral toegangscontroles, waarbij het kaartje voor de trein of het concert op de chip in het mobiele device staat. Een ander voorbeeld is het verzamelen van data, zoals bijvoorbeeld een Internet URL van een RFID-tag op een poster.

- **Touch and Confirm**; applicaties waarbij de gebruiker een handeling moet bevestigen, bijvoorbeeld een betaling, door een (PIN)code of wachtwoord in te typen.

- **Touch and Connect**; twee apparaten met elkaar verbinden, zodat data, bijvoorbeeld adresboek of muziek, uitgewisseld kan worden.

- **Touch and Explore**; het verbinden met een ander NFC apparaat, waarna gekeken kan worden welke services deze biedt. Bijvoorbeeld internettoegang of een bestelling opgeven.

Apparaten kunnen een NFC verbinding ook gebruiken om een ander soort, snellere, verbinding op te zetten. Er wordt dan een NFC verbinding gemaakt voor de autorisatie, waarna een Bluetooth of Wifi-verbinding gemaakt kan worden tussen de twee apparaten. Het opzetten van een ander en snellere soort verbinding zal voor een betalingssysteem niet nodig zijn; NFC biedt een snelheid van 106 – 424 Kbps.

Het NFC protocol is vastgelegd in een ISO specificatie, namelijk ISO-18092. In deze standaard is geen encryptie opgenomen. Implementaties van de techniek, zoals FeliCa van Sony en MIFARE van Philips bieden dat wel.

Dit is niet het enige systeem dat met NFC betalingen mogelijk maakt. In Europa zijn een groot aantal succesvolle pilots geweest die betalingen mogelijk maakten met een daarvoor geschikte mobiele telefoon. In Japan biedt NTT Docomo een goed lopende dienst aan voor het verrichten van betalingen met een mobiel.

Fabrikant Nokia maakt NFC-enabled mobiele telefoons, evenals Samsung. Een betalingssysteem dat gebruik maakt van NFC vereist dus dat zowel de consument als de merchant speciale apparatuur hebben.

## 6.3 Conclusie

Voor de twee afwijkende elementen (Payment Credentials Providing en de transportlaag), hebben we verschillende oplossingen geïdentificeerd. In totaal maakt dat drie combinaties mogelijk:

- GSM netwerk, in combinatie met lokale opslag van betalingsgegevens
- GSM netwerk, in combinatie met centrale opslag van betalings-gegevens
- NFC, in combinatie met lokale opslag van betalingsgegevens.

Een systeem dat gebruik maakt van NFC, heeft als groot voordeel dat er een aantal min of meer kant-en-klare systemen voor bestaan. Een nadeel is dat er bij een dergelijk systeem alleen valt te betalen bij een point-of-sale, omdat er speciale apparatuur voor nodig is. In feite biedt NFC dus een vervanging van de debitkaart door de telefoon. Qua gebruikersgemak lijken systemen op basis van NFC heel goed te voldoen aan de gestelde eisen en het is een wijze van betalen die reeds in andere landen geïmplementeerd is en meet veel succes wordt gebruikt.

Een voordeel van het gebruik van GSM als transportlaag is dat het mogelijk is een systeem te ontwikkelen dat op alle telefoons kan werken. Hierbij is het meest logisch om te kiezen voor USSD en niet voor SMS of dataconnecties, gezien de eigenschappen die USSD biedt. Een ander voordeel is dat er in België al een goed werkend systeem bestaat dat gebruik maakt van deze techniek. Het systeem zou ook uitgebreid kunnen worden naar andere Europese landen. Een nadeel van het GSM netwerk is dat het op den duur zal verdwijnen. Langzaam zal in de loop van de jaren het tweede generatie netwerk door een derde generatie netwerk worden vervangen. Dit hoeft echter geen belemmering te zijn voor het ontwikkelen van een betalingssysteem, maar dient wel in het achterhoofd gehouden te worden. Het GSM netwerk is tevens makkelijk af te luisteren, iets waar rekening gehouden moet worden bij het ontwerp van de dienst. Een laatste moeilijkheid is dat het opzetten van de dienst via het GSM-netwerk de medewerking van, het liefst alle maar in ieder geval het grootste deel van, de telecomoperators.

Met een keuze van het GSM-netwerk voor transport van de data van transacties, is de keuze voor het opslaan van de betalingsgegevens er één tussen de SIM of opslag op een server. Betalingsgegevens op een server zijn relatief makkelijker bij te werken dan op een SIM, maar het biedt ook een groter risico ten opzichte van het privacy-aspect. Als alle privacy-gevoelige gegevens geclusterd staan, kan één lek ervoor zorgen dat gegevens van alle gebruikers bloot komen te liggen. Opslag op de SIM maakt de kans op massale schending van de privacy kleiner.

# H7 Onderzoeksopzet onderzoeksdoel 2

Dit hoofdstuk beschrijft ten eerste hoe met de opgestelde onderzoeksvragen aan het tweede onderzoeksdoel, zoals beschreven in hoofdstuk 2, kan worden voldaan. Vervolgens wordt in de daarop volgende paragrafen per onderzoeksvraag beschreven hoe deze beantwoord zal gaan worden.

## *7.1 Voldoen aan het onderzoeksdoel*

Om inzicht te krijgen in de mate waarin de gevonden combinaties van technologieën worden bedreigd, moeten we allereerst weten welke bedreigingen er voor die, in het eerste onderzoeksdoel geselecteerde, systemen zijn. Met een analyse per geselecteerd systeem kan er vervolgens een onderling vergelijk worden gemaakt.

## *7.2 Bedreigingen voor de geselecteerde systemen*

In deze onderzoeksvraag willen we analyseren welke bedreigingen er zijn op securitygebied voor elk van de geselecteerde technologieën. Aan deze bedreigingen moet ook een soort waarde kunnen worden verbonden, zodat we de systemen onderling kunnen vergelijken.

Hiervoor is allereerst een (semi-) formele methode nodig om deze analyse uit te kunnen voeren. Om die te vinden gaan we door middel van literatuur-onderzoek worden bekeken welke methodes voor bedreigingsanalyse er zijn, om er daarvan één te kunnen gebruiken. Daarna zal met behulp van deze methode de bedreigingen voor de verschillende systemen worden geanalyseerd. Het resultaat daarvan is een analyse met welke bedreigingen er zijn voor elk systeem.

## *7.3 Vergelijken van de systemen*

Met de drie analyses, eén per systeem, kan er vervolgens een vergelijking worden gemaakt tussen de verschillende systemen. Op basis hiervan zal er in de conclusie een advies worden uitgebracht aan Interpay ECS.

# H8 Attacktrees

## *8.1 Inleiding*

Dit hoofdstuk beschrijft de formele attacktree methode die we gaan gebruiken om in het volgende hoofdstuk een bedreigingsanalyse gemaakt. Attacktrees is een (semi-) formele methode om de bedreigingen op een systeem in kaart te brengen. Mogelijke aanvallen op het systeem worden gerepresenteerd in een boomstructuur, waarbij de wortel en de knopen van de boom het aanvalsdoel bevatten en de bladeren de concrete aanvallen om die doelen te bereiken. De methode is in 1999 geïntroduceerd door Bruce Schneier[16].

**Veiligheidsanalyses**
Veiligheidslekken in software vinden is erg moeilijk, omdat de structuur van hedendaagse software uitermate complex is. Vaak wordt een stuk software uit meerdere componenten gebouwd, gemaakt door meerdere programmeurs, die allemaal afhankelijk zijn van elkaar. Aanvallen vinden vaak plaats op plekken waar de ontwerpers bij het design nooit aan gedacht hadden, of op punten die individueel wel veilig waren, maar in combinatie met andere componenten ineens gevaar opleveren.

Voor de veiligheid van software bestaat geen echte maat. Idealiter zou daarvoor een objectieve maat bestaan, het totale risico van een bepaald ontwerp of implementatie. De klassieke formulier daarvoor is natuurlijk:

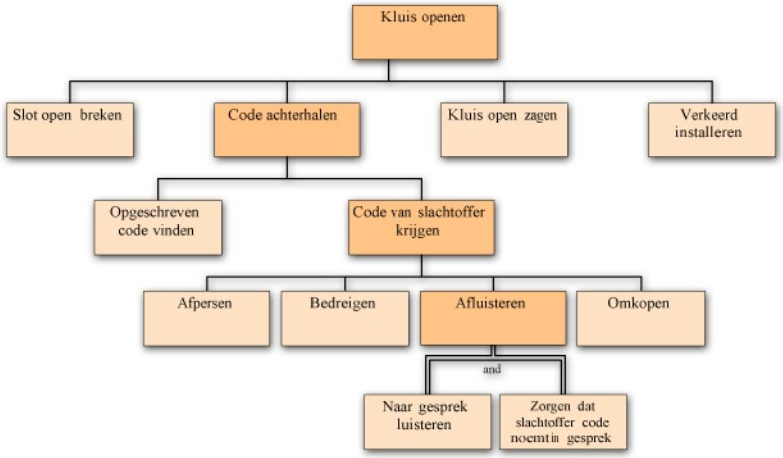
**Risico = Kosten * Kans**

Als je dat voor elke mogelijke aanval voor een systeem bij elkaar optelt, zou je een uitspraak kunnen doen over de veiligheid van een systeem en zelfs onderling kunnen vergelijken. Het probleem is dat de genoemde formule in de praktijk volkomen waardeloos is. Immers, hoe bereken je de kans op een aanval? Dat is onmogelijk, het enige wat men kan doen is een inschatting maken. En daarmee is de objectiviteit die we zo graag zouden hebben, helemaal weg.

De enige maat die bruikbaar lijkt te zijn, is het aantal experts dat zich het hoofd hebben gebroken over veiligheidsbedreigingen van een systeem[17]. Echter, een (semi)formele methode die helpt bij het maken van bedreigingsanalyses maken de betrouwbaarheid ervan veel groter. Zo'n methode is de attacktree-methode.

## 8.2 Attacktree methode

De methode laat zich het beste uitleggen aan de hand van een aantal voorbeelden. Als voorbeeld nemen we de attacktree om een kluis te openen. Het doel van een aanvaller is uiteraard om de kluis open te krijgen.




*Illustratie 7: Attacktree om een kluis te openen*

## 8.3 OR- en AND-Knopen

Er bestaan twee soorten knopen in de attacktrees: OR- en AND-knopen. Zonder aanduiding is een knoop een OR-knoop. Dit betekent dat een aanvaller kan kiezen uit één van onderstaande kinderen (onderliggende knopen) om de aanval succesvol te kunnen doen. Om de kluis open te krijgen kan een aanvaller dus kiezen uit vier aanvallen: hij kan het slot openbreken, zorgen dat hij de code krijgt, de kluis open zagen of zorgen dat de kluis niet goed geïnstalleerd wordt (zodat hij makkelijk opengaat).

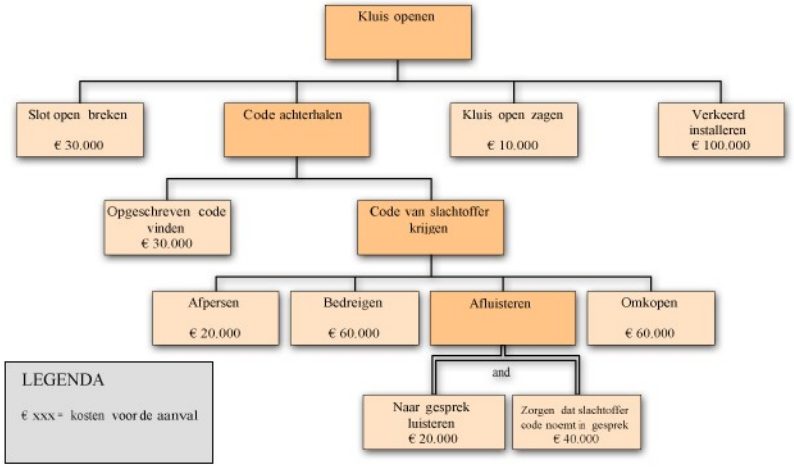
In het geval van een AND-knoop moeten alle onderliggende doelen worden gecompleteerd om de aanval te kunnen uitvoeren. Als de aanvaller de code van de kluis dus te weten wil komen door af te luisteren, moet hij zowel de conversatie af kunnen luisteren als zorgen dat het slachtoffer in die conversatie de code van de kluis hardop uitspreekt.

In het originele voorstel van Bruce Schneier kunnen knopen slechts één ouder hebben. Mauw en Oostdijk hebben in hun paper[21] een aangepaste attacktree formeel beschreven, en een uitbreiding beschreven waarbij een knoop wel meerdere ouders (bovenliggende knopen) kan hebben. Dit is absoluut zinvol, omdat in de praktijk al snel blijkt dat met een bepaalde

aanval meerdere doelen bereikt zouden kunnen worden. Zo zou het afpersen van een persoon niet alleen kunnen leiden tot het kennen van de code, maar bijvoorbeeld ook tot de vindplaats van de kluis.

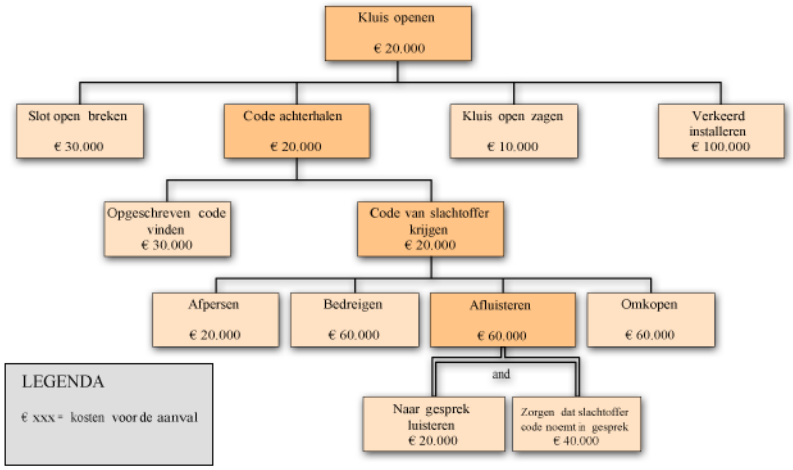
## 8.4 Waardes toekennen

Aan elk blad in de boom kunnen waardes worden toegekend. Dit kan bijvoorbeeld de kosten zijn van een dergelijke aanval, of een indicatie of de aanval wel of niet mogelijk is.




*Illustratie 8: Waardes toekennen aan de attacktree*

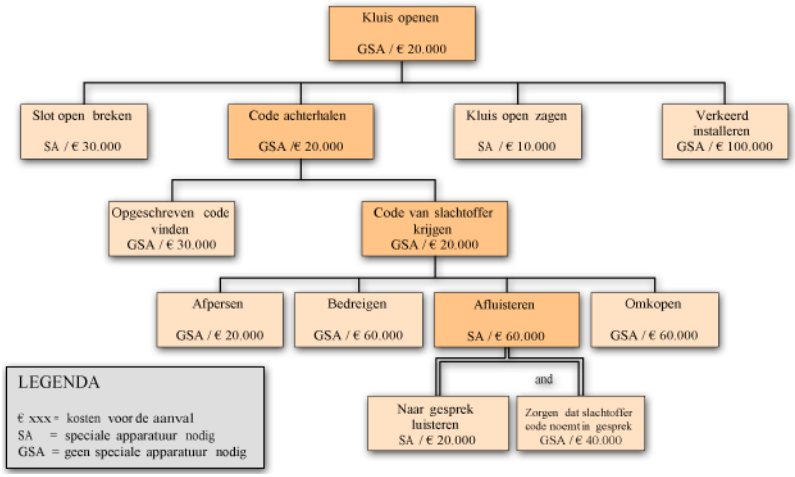
De waardes kunnen vervolgens van beneden naar boven gepropageerd worden. Afhankelijk van het type knoop (OR of AND), worden de waardes naar boven toe gepropageerd. Hoe dit gedaan wordt, hangt af van het doel dat men wil bereiken. Stel dat bij elke aanval de kosten van die aanval zijn aangegeven. Als men wil zien wat het minimaal kost om de kluis te kunnen openen, krijgt elke OR-knoop de laagste waarde van zijn kinderen. Bij een AND-knoop dienen de kosten uiteraard te worden opgeteld.




*Illustratie 9: Waardes propageren door de boom*

## 8.5 Meerdere waardes

Het is mogelijk om tegelijkertijd meerdere waardes aan elke knoop toe te kennen en deze afzonderlijk te propageren. Aan de attacktree voor het openen van de kluis voegen we toe voor welke aanval speciale apparatuur nodig is en voor welke niet. De boom komt er dan als volgt uit te zien:




*Illustratie 10: Meerdere waardes toekennen en propageren*

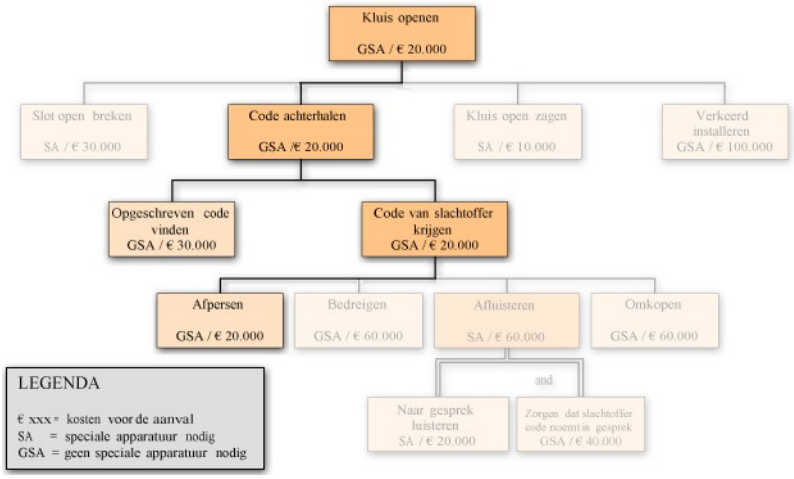
Merk hierbij op dat bovenstaande projectie dus niet wil zeggen dat er een aanval bestaat die €20.000 kost en geen speciale apparatuur nodig heeft. Die bestaat wel, maar dat kan niet direct worden geconcludeerd wanneer men

alleen de wortel van de boom bekijkt. “GSA/ €20.000” in het bovenstaande voorbeeld betekent dus dat er een aanval is die geen speciale apparatuur gebruikt en dat er een aanval is die 20.000 euro kost.

## 8.6 Projecties

Nu de boom voorzien is van waardes, kunnen er zogenaamde projecties worden gemaakt. Feitelijk is dit niets anders dan uit de boom weglaten wat men niet wil zien. Stel dat men alle aanvallen wil zien waarvoor geen speciale apparatuur nodig is. Er kan dan een projectie worden gemaakt.

Zo kunnen projecties ook worden gecombineerd. Bijvoorbeeld een projectie die alle aanvallen laat zien die een grote impact hebben en waarvoor de kans groot is dat ze uitgevoerd worden. Het mooie is dat wat voor projectie men ook maakt bij een attacktree, er altijd weer een geldige attacktree uitkomt. Voor onze attacktree maken we een projectie voor de aanvallen waarvoor geen speciale apparatuur nodig is en die tevens maximaal €30.000 kosten.




*Illustratie 11: Projectie van aanvallen waarvoor geen SA nodig is en die maximaal €30.000 kosten*

## 8.7 Tools

Om attacktrees te tekenen, voldoet in principe een stuk papier. Ook een programma als Microsoft Visio is geschikt om bomen mee te tekenen. Het nadeel van deze methodes is dat het lastig is om eenmaal gemaakte bomen simpel te wijzigen.

Voor het tekenen van attacktrees is een aantal specialistische programma's geschreven. Een voorbeeld daarvan is het commerciële Attacktree+, van

IsoGraph Software. Het lijkt erop dat dit een bruikbaar stuk gereedschap is. Het is mogelijk, aldus de fabrikant, attacktrees te creëren en te bewerken. Het programma laat ook toe dat er meerdere, willekeurige, waardes aan de leaves toegekend worden. Aangezien deze software geld kost, is gezocht naar een alternatief.

Aan de Technische Universiteit Eindhoven is in een afstudeerproject gedaan door Alexander Opel[27]. Dit project, dat geëindigd is in 2004, heeft een tool opgeleverd voor het tekenen van Attacktrees. De software is geschreven in Java en vrij beschikbaar. Dit programma, dat geen naam heeft, zullen we proberen te gebruiken om de attacktrees in het volgende hoofdstuk te tekenen.

## *8.8 Conclusie*

Attacktrees is een semi-formele methode om aanvallen op een systeem te beschrijven, bekeken vanuit het oogpunt van een eventuele aanvaller. Omdat het op een gestructureerde manier wordt vastgelegd, helpt het om overzicht te krijgen in de bedreigingen voor een systeem.

Wanneer de aanvallen in kaart zijn gebracht, kunnen er op allerlei wijzen waardes aan worden toegekend. Op basis daarvan kunnen keuzes worden gemaakt over de te nemen maatregelen om het systeem te beschermen.

Omdat attacktrees formeel zijn gedefinieerd[21], is het mogelijk geworden om hulpmiddelen te gebruiken. Daarmee wordt het tekenen en analyseren van attacktrees vereenvoudigd. Het gebruik van attacktrees biedt echter, net als elke andere modelleringsmethode, geen enkele garantie dat men aan alle mogelijke aanvallen heeft gedacht.

Het is overigens absoluut niet verstandig om alleen te vertrouwen op het in kaart brengen van de bedreigingen waar het gaat om de veiligheid van software. Wat de modellen niet doen, is het in kaart brengen van maatregelen om de aanvallen te voorkomen. Er zijn daarom aanvullende maatregelen nodig, zoals gebruik van s*ecurity patterns* en *programming guidelines*. Dit valt echter buiten de grenzen van dit onderzoek en zullen daarom niet verder besproken worden.

# H9 Bedreigingsanalyse casestudy

Om een keus te kunnen maken welke van de drie systemen, geselecteerd in hoofdstuk 7, het beste gebruikt kan worden vanuit veiligheidsoogpunt, met gebruikmaking van de attacktree-methode, dient kennis te worden verkregen over de volgende punten:

a) Op welke gebieden kunnen er bedreigingen zijn voor de systemen, oftewel: wat zijn de mogelijke aanvalsdoelen?
b) Welke aanvallen zijn er mogelijk voor een aanvaller om deze doelen te bereiken en hoe ziet de attacktree hiervan eruit?
c) In welke mate zijn de verschillende aanvallen van toepassing op de verschillende systemen?
d) Welke van de systemen is het minst kwetsbaar per aanvalsdoel?

Om antwoord te geven op vraag A en er zorg voor te dragen dat de inventarisatie van deze aanvalsdoelen zo volledig mogelijk is, is er zowel overleg geweest met experts van Interpay en de universiteit, en een literatuuronderzoek gedaan[15,13, 20]. De resultaten van het antwoord op deze vraag zijn te vinden in paragraaf 1.

Het inventariseren van alle aanvallen die mogelijk zijn op een mobiel systeem, wordt gedaan met behulp van de attacktree-methode. Een uitleg van deze methode staat in vorige hoofdstuk. De methode begint met de aanvalsdoelen, die geïnventariseerd zijn in paragraaf 1. Om te zorgen dat deze boomstructuur een zo compleet mogelijk beeld geeft van alle aanvallen die nodig is, is er uitgebreid overleg geweest met de experts van Interpay en een uitgebreid literatuuronderzoek. Dit is geen garantie dat er geen aanval over het hoofd is gezien, maar het risico hierop is wel zo klein mogelijk gemaakt door met meerdere experts te overleggen. Om de attacktree te maken, is geprobeerd gebruik te maken van de softwaretool die in het vorige hoofdstuk beschreven is. Deze attacktree staat beschreven in paragraaf 2.

Om vervolgens te zien in welke mate de verschillende aanvallen van toepassing zijn op de geselecteerde systemen, moeten we per aanval weten op welke van de systemen hij van toepassing is en in welke mate.
Deze classificatie geeft aan hoe groot het risico op deze aanval wordt ingeschat. Er zijn daarbij drie klassen gemaakt: hoog, middel en laag.. Er is gekozen voor deze drie klassen, omdat het niet mogelijk is om deze indeling nauwkeuriger te doen, dit is immers geen maat die hard te meten is. Een aanval komt in de categorie *laag* wanneer de impact klein is (dwz: de aanval is niet op massale schaal mogelijk) of de waarschijnlijkheid klein is. In de categorie *hoog* vallen aanvallen waarvan de waarschijnlijkheid of de impact groot is. De categorie *middel* is voor alle aanvallen die daar tussenin zitten. De aanvallen en indeling in risicoklasses staan beschreven en gemotiveerd

in paragraaf 3. Om deze indeling in klasses zo betrouwbaar mogelijk te maken, is hij voorgelegd aan groep experts van InterPay, die beroepsmatig hiermee bezig zijn. Hun bevindingen zijn verwerkt, waarna het eindresultaat nogmaals is besproken.

Om tot slot een antwoord te geven op vraag d, welke van de systemen het minst kwetsbaar is per risicogebied, dient inzichtelijk te zijn, in welke mate de verschillende aanvalsdoelen het risico lopen om gerealiseerd te worden. Om dit te bereiken is in paragraaf 4 voor elk van de systemen een projectie gemaakt, op basis van of een aanval wel of niet van toepassing is op het betreffende systeem. Binnen deze projectie is vervolgens de waarde van de risicoklasse gepropageerd door de boom, tot aan de aanvalsdoelen. De waarde die het aanvalsdoel dan heeft, is een maat voor het niveau van bedreiging hiervoor.

Op basis van de projecties en de gepropageerde waardes per aanvalsdoel, wordt er in paragraaf 5 een vergelijk gemaakt tussen de drie systemen, per risicogebied. Dit is een vergelijk vanuit veiligheidsoogpunt, dat is daarom de enige factor die mee is genomen hierin.

Het probleem in deze case is natuurlijk dat er nog geen echt systeem is om te analyseren, de definitieve ontwerpkeuzes liggen nog niet vast. Het enige wat er is, zijn de globale keuzes die we hebben gemaakt in hoofdstuk 7. De vraag is dus of het mogelijk is om met zo weinig vaststaande ontwerpkeuzes toch een gefundeerde analyse te maken. In de reflectie aan het einde van het hoofdstuk zullen we hierop terugkomen.

Tot slot gaat de reflectie in op het nut van gebruik van de attacktree methode voor deze casestudy en het nut en betrouwbaarheid van het maken van een bedreigingsanalyse voor een systeem waarvoor nog veel ontwerpkeuzes gemaakt moeten worden.

## *9.1 Veiligheidsbedreigingen*

We kunnen drie bedreigingen onderscheiden voor een mobiel betalingssysteem. De meest belangrijke daarvan is **fraude**. Hiermee wordt bedoeld het doen van oneigenlijke betalingen. Er zijn twee manieren om een frauduleuze betaling te verrichten: personificatie; betalen uit naam van iemand anders, of het opvangen, aanpassen en doorsturen van berichten; een “man-in-the-middle”-aanval.

Personificatie vereist dat de aanvaller een aantal gegevens heeft. Bij het PIN-systeem zou de aanvaller een kopie van de PIN-pas en de pincode nodig hebben. Het hangt nu af van de opzet van het systeem, welke gegevens een aanvaller nodig heeft om zich voor te kunnen doen als iemand anders en op die wijze een valse betaling te doen. Afhankelijk van de

implementatie van het systeem zou dit één of meer van de volgende gegevens kunnen zijn:

- Wachtwoord of “PIN”-code
- MSISDN of IMSI  of bankrekening nummer (de betalingsgegevens)
- Bepaalde versleutelingscode, bijvoorbeeld de masterkey van het systeem.

Omdat er nog niets vastligt voor wat betreft de implementatie van een betaalsysteem, is het niet zeker welke gegevens van toepassing zullen zijn op het systeem. Zeker is dat deze gegevens confidentieel zijn.

**Privacyschending** van klantinformatie is de tweede bedreiging voor het systeem. Hieronder wordt verstaan het uitlekken van gebruikersgegevens, zoals adresgegevens, saldo informatie, informatie over aankopen die de gebruiker gedaan heeft.

De derde grote dreiging is het lamleggen van het systeem, ervoor zorgen dat het systeem onbruikbaar is voor (een deel van) alle gebruikers. Dit wordt een **Denial of Service** (DoS) aanval genoemd.

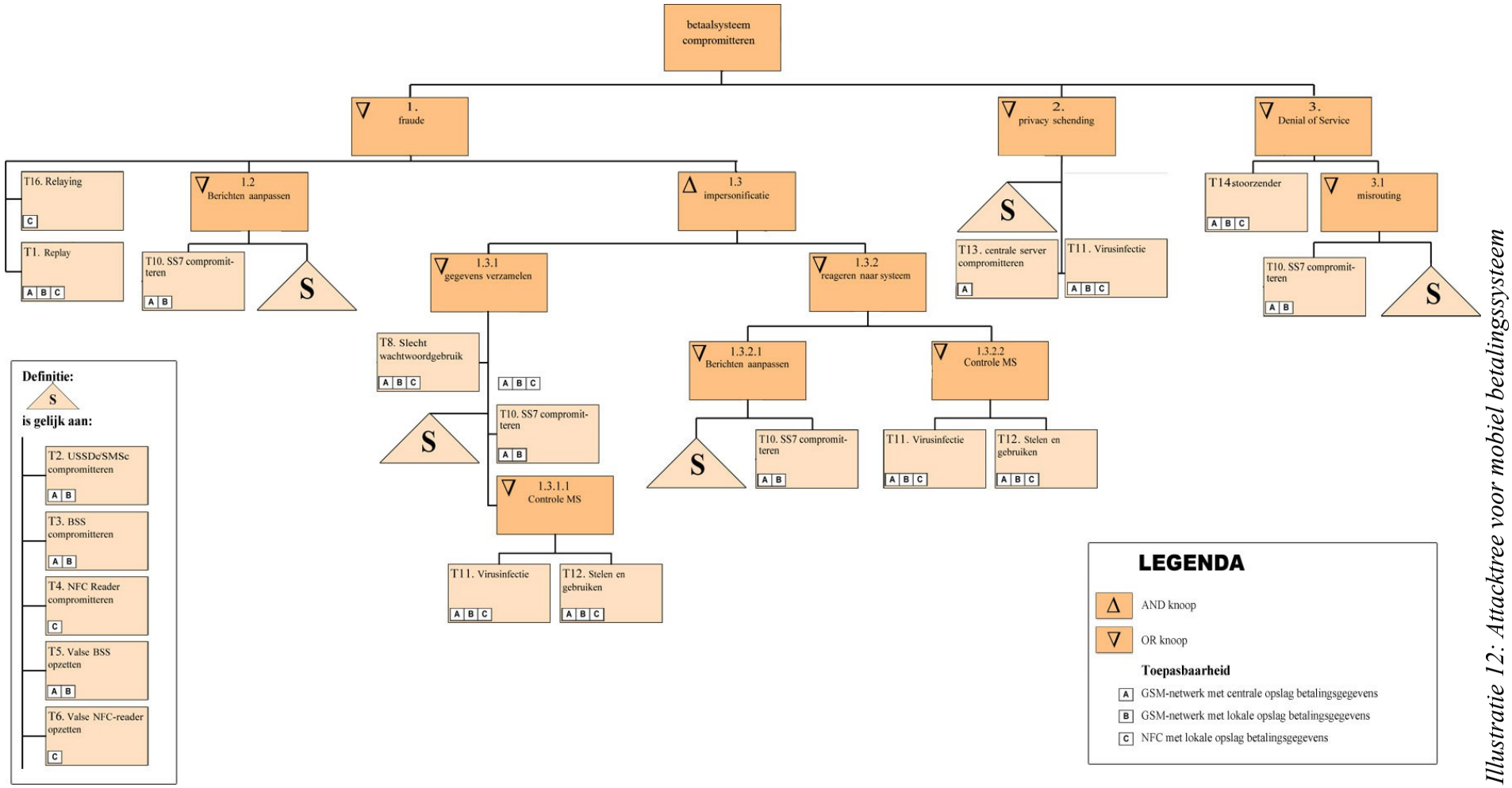
## *9.2 Attacktree*

Met bovengenoemde bedreigingen van het systeem, kunnen we een attacktree opstellen. In deze attacktree staan bedreigingen voor het systeem. Daarnaast bevat de boom de aanvallen die mogelijk zijn voor elk van de oplossingen. Dat houdt dus in dat zowel aanvallen voor de twee oplossingen van de transportlaag, namelijk gebruik maken van het GSM-netwerk of van Near Field Communication als die op de twee oplossingen voor het bewaren van betalingsgegevens (op een centrale server of op het mobile station).

De aanvallen zijn vervolgens geclassificeerd. Tevens is voor elke aanval is beschreven voor welke van de drie geselecteerde systemen hij wel en voor welke niet mogelijk is. Die waardes zijn vervolgens alvast naar de wortel van de boom toe gepropageerd.

In een attacktree is het mogelijk dat één aanval meerdere doelen kan bereiken. In de boom zou dat eruit zien als een node met meerdere parents. In de opgestelde attacktree is daar geen gebruik van gemaakt, omwille van de leesbaarheid. Het zou anders een wirwar van lijnen zijn geweest, dus wanneer een aanval meerdere doelen dient, staat hij even zo vaak in de boom.

De attacktree ziet er nu als volgt uit:




*Illustratie 12: Attacktree voor mobiel betalingssysteem*

## 9.3 Beschrijving van aanvallen

In deze paragraaf worden de aanvallen besproken die op het systeem gepleegd kunnen worden. Deze aanvallen zijn terug te vinden in de attacktree die is opgesteld. Elke aanval zal kort worden beschreven, vervolgens wordt gekeken naar de impact die de aanval kan hebben en tot sloot de tegenmaatregelen die genomen kunnen worden om de aanval te voorkomen.

### T1. Replay van berichten

**Beschrijving**
Een aanvaller zou berichten kunnen opvangen en 'replayen'; nog een keer dezelfde berichten gebruiken. Op deze wijze kan een complete transactie worden “nagespeeld” of een deel ervan zoals de authenticatiefase.

**Impact**
Replay kan ervoor zorgen dat betalingen dubbel kunnen worden uitgevoerd, of dat een aanvaller zich kan authenticeren als een ander. Wanneer berichten simpel kunnen worden opgevangen, kan dit op grote schaal gebeuren.

**Waarschijnlijkheid**
De kans dat deze aanval op grote schaal kan worden uitgevoerd, hangt af van het gemak waarmee het berichten verkeer kan worden afgeluisterd. Voor NFC aanvallen is dit lastig, omdat je hierbij op een hele kleine afstand moet zitten van het mobiele toestel. Kwaadwillende merchants zijn beter in de positie om deze aanval uit te voeren, waarmee de aanval dan wel niet op massale, maar eventueel wel op grote schaal kan worden gedaan. Via het GSM netwerk gaan de berichten door de lucht en deze zijn dus veel simpeler af te vangen. Mochten de berichten makkelijk af te luisteren zijn, dan kan deze aanval op grote schaal worden uitgevoerd.

**Tegenmaatregelen**
Replay is een bekende aanval op vele systemen en is eenvoudig te voorkomen door het geven van volgnummers aan de berichten. Hierdoor is te achterhalen of een boodschap al eens verstuurd is. Daarbij moet de integriteit van de berichten wel gewaarborgd zijn.

**Klasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Hoog |
| GSM netwerk met lokale opslag betalingsgegevens | Hoog |
| NFC met lokale opslag betalingsgegevens | Middel |

## T2. Compromitteren van USSDc cq. SMSc

**Beschrijving**
Als een aanvaller toegang heeft tot de USSDc / SMSc, dan kan hij de berichten die hier passeren afluisteren, of zelfs aanpassen.

**Impact**
Met toegang tot de USSDc kunnen transacties worden aangepast (fraude), belangrijke gegevens achterhaald (zoals bijvoorbeeld het wachtwoord van de gebruiker), kan privacygevoelige informatie vrijkomen of kunnen de berichten op zodanige wijze bewerkt worden dat ze onbruikbaar worden, hetgeen leidt tot een DoS.

**Waarschijnlijkheid**
Het beveiligingsniveau van de SMSc is onbekend, net zoals voor de rest van het GSM-netwerk wordt deze informatie niet openbaar gemaakt. Gezien het belang van een goede beveiliging voor het functioneren van het netwerk, lijkt het redelijk om aan te nemen dat dit goed beveiligd is. Het is echter verstandig om toch maatregelen te nemen. Daarnaast heeft de eigenaar van het netwerk natuurlijk volledige controle over de SMSc.

**Tegenmaatregelen**
Een versleuteling van al het verkeer van MS tot aan het achterliggend systeem (end-to-end encryptie), zorgt ervoor dat eventueel afgeluisterde berichten geen informatie prijsgeven en dat ze ook niet aangepast kunnen worden.

**Klasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Hoog |
| GSM netwerk met lokale opslag betalingsgegevens | Hoog |
| NFC met lokale opslag betalingsgegevens | - |

## T3. Compromitteren van het BSS

**Beschrijving**
Het in verkeerde handen vallen van het BSS, zodat deze volledig wordt beheerst door de aanvaller. Hij kan dus alle berichten
die binnen komen lezen, ze aanpassen of compleet vervangen en wel of niet doorsturen naar het achterliggende systeem of naar het MS.

**Impact**
De impact van deze aanval is dezelfde als van aanval T2. Wanneer een aanvaller controle heeft over het BSS dan:

- Kan hij berichten afluisteren en zo privacy-gevoelige informatie

achterhalen.
- Kan hij berichten afluisteren en zo belangrijke betalingsgegevens, bijvoorbeeld de pincode, achterhalen en daarmee fraude plegen
- Berichten aanpassen en op die manier fraude plegen
- Berichten verminken, misroutes op weggooien, met een DoS tot gevolg

**Waarschijnlijkheid**
Het BSS is fysiek beschermd, maar niet eigendom van één instantie. De beveiliging zal dus verschillen per operator en per land. De kan s dat het goed beschermd is, is echter wel groot, omdat het belang hiervan erg groot is voor de telecombedrijven. Daarbij komt wel dat de operator volledige controle heeft over de BSS.

Maar ook al mocht de BSS minder goed beschermd zijn, dan nog is de kans op massale impact erg klein, omdat er enorme hoeveelheden data over het netwerk gaan en het vrijwel onmogelijk zal zijn om de berichten die bij dezelfde transactie horen bij elkaar te 'zoeken' (zelfs als dit geautomatiseerd gaat en de merchant hierbij helpt met de gegevens die hij heeft).

**Tegenmaatregelen**
Encryptie is hier ook de oplossing. Wanneer verkeer tussen het MS en het betalingssysteem worden versleuteld, dan kunnen berichten niet worden aangepast en geven ze geen informatie prijs aan degene die ze afluistert.

**Klasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Hoog |
| GSM netwerk met lokale opslag betalingsgegevens | Hoog |
| NFC met lokale opslag betalingsgegevens | - |

## T4. Compromitteren van NFC reader

**Beschrijving**
Wanneer een aanvaller de controle heeft over de NFC-reader, kan hij alle verkeer dat hierlangs komt onderscheppen.

**Impact**
Zie de impact van aanval T3.

**Waarschijnlijkheid**
Het is goed mogelijk dat de NFC onder controle van een kwaadwillend persoon komt. Merchant kunnen zelfs in alle rust eventuele aanpassingen doen, maar het zou ook kunnen dat aanvaller van afstand probeert de NFC te controleren.

**Tegenmaatregelen**
De tegenmaatregelen zijn hetzelfde als die van aanval T3; encryptie.

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | - |
| GSM netwerk met lokale opslag betalingsgegevens | - |
| NFC met lokale opslag betalingsgegevens | Hoog |

### T5. Man-in-the-middle middels een valse BSS

**Beschrijving**
In het GSM netwerk, wordt er maar één kant op geauthenticeerd. De MS authenticeert zich naar het BSS, maar niet andersom. Het toestel weet dus nooit of het met een echt BSS van doen heeft.

Een aanvaller kan dus doen alsof hij een BSS is, mits de benodigde apparatuur aanwezig is. Deze valse BSS zal echter niet aangesloten kunnen worden op de rest van het GSM-netwerk, omdat hij niet over de benodigde encryptiesleutels beschikt.

**Impact**
Opzetten van een BSS kan tot gevolg hebben dat de aanvaller betalingen kan aanpassen, of naspelen. Wanneer een gebruiker in een winkel wil betalen en de transactie wordt opgezet door de valse BSS, zal hij dat niet merken. De BSS heeft beschikt waarschijnlijk niet over de juiste gegevens om de verbinding naar de MS te encrypten, maar omdat de BSS hier controle over heeft, kan hij er simpelweg voor kiezen om geen de verbinding zonder encryptie op te zetten. De consument geeft zijn gegevens, bijvoorbeeld zijn pincode, dan aan de aanvaller prijs. Deze kan transactie hierna afkappen, waardoor deze faalt (en de gebruiker en merchant het waarschijnlijk opnieuw zullen proberen).

Daarnaast kan deze aanval leiden tot het achterhalen van privacygevoelige gegevens, en ingezet worden voor een Denial of Service aanval, door het verminken of verwijderen van de berichten.

**Waarschijnlijkheid**
De benodigde apparatuur is niet erg duur en het is ook niet moeilijk om eraan te komen. Om de aanval systeemwijd te kunnen uitvoeren, is er echter heel veel apparatuur nodig. De aanval zal dus waarschijnlijk alleen lokaal worden uitgevoerd, maar kan daar wel op massale schaal worden toegepast.

**Tegenmaatregelen**
Tweeweg authenticatie kan deze aanval voorkomen. Encryptie zorgt er ook voor dat een valse BSS de gegevens niet kan lezen, en er dus feitelijk niet

veel aan heeft.

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Hoog |
| GSM netwerk met lokale opslag betalingsgegevens | Hoog |
| NFC met lokale opslag betalingsgegevens | - |

### T6. Man-in-the-middle middels een valse NFC reader

**Beschrijving**
Een aanvaller kan een eigen NFC-reader opstellen en op die manier (een deel van) de interactie met het MS overnemen van de echte NFC-reader. De aanval is verder gelijk aan T5.

**Impact**
De impact van de aanval is gelijk aan de impact van aanval T5 en heeft dus invloed op zowel fraudegevoeligheid, privacy en DoS.

**Waarschijnlijkheid**
Een valse NFC-reader zal erg dichtbij het mobile device moeten staan. NFC heeft immers maar een hele korte afstand waarop gecommuniceerd kan worden, afhankelijk van de gebruikte frequentie. De kans dat dit onopgemerkt blijft is dus vrij klein. Een merchant zou wel in de gelegenheid zijn om dit te doen. Zelfs als deze aanval uitgevoerd kan worden, is de impact niet systeemwijd, maar slechts lokaal.

**Tegenmaatregelen**
Een authenticatie van de reader aan het MS en vice versa kan deze aanval voorkomen. Deze methode wordt ook bij het Chipknip systeem gebruikt. Encryptie van de berichten zorgt er ook nog eens voor dat de aanvaller niets heeft aan de afgeluisterde berichten.

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | - |
| GSM netwerk met lokale opslag betalingsgegevens | - |
| NFC met lokale opslag betalingsgegevens | Hoog |

### T8. Stelen of raden van (zwakke) pincodes

**Beschrijving**
Het komt vaak voor dat mensen hun wachtwoorden voor meerdere dingen tegelijk gebruiken, of een pincode gebruiken die goed te onthouden is, omdat het hun geboortedatum is. Gebruik van dergelijke 'zwakke'

wachtwoorden zorgen ervoor dat een aanvaller het gemakkelijk kan raden.

**Impact**
Met de pincode of het wachtwoord is het doen van een transactie een grote stap dichterbij voor een aanvaller. Wanneer hij de mobiele device in handen heeft, staat het hem vrij om te kunnen betalen. Het is vergelijkbaar met het uit handen geven van de pincode die bij de debitkaart hoort.

Massale fraude is echter niet mogelijk, slechts de gebruiker waarvan het wachtwoord te raden viel, zou slachtoffer kunnen worden. Het raden van wachtwoorden zou wel geautomatiseerd kunnen worden, wat de kans op massale fraude vergroot.

**Waarschijnlijkheid**
De kans op het raden van een wachtwoord is reëel, zeker wanneer een aanvaller de gebruiker kent, of wanneer het systeem het toelaat om vrij wachtwoorden uit te proberen.

**Tegenmaatregelen**
Het systeem moet verhinderen dat er oneindig vaak wachtwoorden of pincodes geprobeerd kunnen worden. Net als bij pinnen zou dit tot bijvoorbeeld drie pogingen gelimiteerd kunnen worden. Massale fraude kan zo voorkomen worden.

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Laag |
| GSM netwerk met lokale opslag betalingsgegevens | Laag |
| NFC met lokale opslag betalingsgegevens | Laag |

## T10. Afluisteren van berichten over het Signalling System 7 netwerk

**Beschrijving**
De USSD / SMS berichten die over het SS7 netwerk worden verstuurd afluisteren. Het SS7 netwerk maakt voor het versturen van berichten zowel gebruik van bekabelde als draadloze communicatie.

**Waarschijnlijkheid**
Voor de bescherming van het SS7 netwerk geldt hetzelfde als voor de rest van het GSM-netwerk; dit is niet bekend. Hiervoor geldt verder hetzelfde als voor aanval T3: de eigenaar van het netwerk heeft volledige controle. Afhankelijk van de opzet van het systeem, moet je er dus vanuit gaan dat dit niet te vertrouwen is.

**Impact**

De impact van het afluisteren van deze berichten is hetzelfde als het afluisteren van de berichten op willekeurig welke plaats in het netwerk; de aanvaller kan er gegevens mee achterhalen die ofwel privacy-gevoelig zijn, of hem de kans geven fraude te kunnen plegen of het mogelijk maken om de berichten te laten verdwijnen of verminken en zo een DoS te bewerkstelligen.

**Tegenmaatregelen**
Wederom maakt end-to-end encryptie de berichten onleesbaar, waar ze ook afgeluisterd mogen worden.

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Hoog |
| GSM netwerk met lokale opslag betalingsgegevens | Hoog |
| NFC met lokale opslag betalingsgegevens | - |

## T11. Infectie van het mobile device door een virus

**Beschrijving**
Wanneer een mobiele device geïnfecteerd raakt met een virus, betekent dat dat er software op staat die uitgevoerd wordt, meestal zonder dat de gebruiker daar erg in heeft.

Virussoftware zou bijvoorbeeld (delen van) een transactie kunnen opvangen en doorsturen naar kwaadwillenden, de aanvaller. Het is ook mogelijk dat de software toetsaanslagen doorstuurt en dat de aanvaller op die manier de pincode of wachtwoord te weten komt.

**Impact**
Virussoftware kan ervoor zorgen dat er gegevens worden achterhaald waarmee een aanvaller fraude kan plegen. Ook kan het leiden tot het schenden van de privacy van de gebruiker. Door de aard van virussen, automatische verspreiding, het is mogelijk hiermee fraude te plegen op massale schaal.

**Waarschijnlijkheid**
Het hangt af van het soort mobiele telefoon dat de gebruiker heeft of deze kwetsbaar is voor virussen. Telefoons die communiceren met het Internet en waarmee programma's kunnen worden gedownload en uitgevoerd worden echter steeds meer gemeengoed. De kans is groot dat toekomstige toestellen dit allemaal in een bepaalde vorm kunnen. Het hangt af van de architectuur en besturingssoftware of het toestel voor virussen vatbaar is.

**Tegenmaatregelen**
Een oplossing zou kunnen zijn om alleen nog gecontroleerde software te

mogen uitvoeren op een MS. Het is echter niet aan het betalingssysteem om dit te regelen. Over de veiligheidsrisico's van het uitvoeren van programmacode op mobiele telefoons is een onderzoek gedaan in 2004 door T. Smulders, [15].

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Middel |
| GSM netwerk met lokale opslag betalingsgegevens | Hoog |
| NFC met lokale opslag betalingsgegevens | Hoog |

## T12. Het stelen van het mobile device om te gebruiken

**Beschrijving**
Een mobiele telefoon kan, al dan niet met toestemming van de eigenaar, worden meegenomen door iemand.

**Impact**
Met het MS, is men al halverwege een transactie. Als de aanvaller de pincode weet te achterhalen (gesteld dat dit überhaupt nodig is in het systeem), kan hij betalingen verrichten zonder toestemming van de eigenaar.

Als betalingen worden opgeslagen, zou het stelen van de mobiele telefoon ook een inbreuk zijn op de privacy van de gebruiker, omdat daarmee duidelijk kan worden wat hij waar en wanneer gekocht heeft. Massale fraude is daarmee niet mogelijk.

**Waarschijnlijkheid**
Diefstal, en dus ook die van mobiele telefoons, is aan de orde van de dag. Het wordt pas een bedreiging voor de gebruiker wanneer de dief ook zijn pincode of wachtwoord weet te achterhalen. Gebruikers die dat ergens op hun telefoon opslaan, lopen dus een groot risico om slachtoffer te worden.

**Tegenmaatregelen**
Tegenmaatregelen door het systeem zijn er niet. Het enige wat men kan doen, is de gebruiker goed voorlichten over het feit dat hij zorgvuldig moet omgaan met zowel telefoon als wachtwoord.

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Laag |
| GSM netwerk met lokale opslag betalingsgegevens | Laag |
| NFC met lokale opslag betalingsgegevens | Laag |

## T13. Compromitteren van centrale gegevens server

**Beschrijving**
De aanvaller verschaft zich toegang tot de centrale server waarop de betalingsgegevens van de gebruikers van het betalingssysteem worden bewaard. Dit kan een aanvaller van buitenaf zijn, maar ook een kwaadwillende beheerder die al toegang heeft tot het systeem.

**Impact**
Toegang tot de gegevens van de gebruikers van het systeem, leidt tot privacyschending op grote schaal.

**Waarschijnlijkheid**
De mogelijkheid tot een aanvaller van binnenuit is nooit uit te sluiten. De kans op een indringer die van buitenaf komt, is echter heel klein te maken door het nemen van uitgebreide beveiligingsmaatregelen.

**Tegenmaatregelen**
De server dient uitermate secuur te worden beveiligd. Hiervoor zijn voldoende 'proven technologies' voorhanden..

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Middel |
| GSM netwerk met lokale opslag betalingsgegevens | - |
| NFC met lokale opslag betalingsgegevens | - |

## T14. Opzetten van een stoorzender

**Beschrijving**
Het opzetten van een stoorzender maakt het ontvangen van berichten door de BSS (in geval van GSM-netwerk) of NFC-reader en de MS onmogelijk. Zowel in het geval van NFC als GSM als transportlaag is deze aanval mogelijk.

**Impact**
Het storen van verkeer over het netwerk kan ervoor zorgen dat het betalingssysteem onbruikbaar wordt, een DoS aanval. Omdat er apparatuur geplaatst dient te worden, kan dit alleen in de omgeving daarvan gebeuren. Het is vrijwel onmogelijk om dit voor het gehele netwerk te kunnen doen, daar hier veel apparatuur voor nodig is. De impact van een dergelijke aanval op het GSM-netwerk is waarschijnlijk groter, omdat er veel meer merchants zullen communiceren met één GSM-mast (BTS) en er daarom met één stoorzender meerdere merchants 'aangevallen' kunnen worden. Met NFC is deze kans veel kleiner dat van één stoorzender veel merchants last zullen hebben, vanwege de gebruikte frequenties.

**Tegenmaatregelen**
In feite is deze aanval niet te voorkomen door het systeem zelf. De enige remedie is om te proberen stoorzenders actief op te sporen en ze uit te schakelen voordat ze schade aanrichten.

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | Middel |
| GSM netwerk met lokale opslag betalingsgegevens | Middel |
| NFC met lokale opslag betalingsgegevens | Laag |

## T15. Relay aanval

**Beschrijving**
Relay aanvallen zijn voor het eerst beschreven door Conway, middels een voorbeeld waar hij uitlegt hoe iemand die geen verstand van schaken heeft een schaakgroot-meester kan verslaan[23].

**Aanval bij een push-initiatie (initiatie door de consument)**
Alice, te goeder trouw, wil haar maaltijd van €20,- afrekenen in het restaurant van Bob, die een aangepaste PoS-terminal heeft. Op het moment dat Alice wil afrekenen en haar telefoon verbinding maakt met de terminal, seint Bob dit door naar Carol, die in een juwelierszaak een ring van €2000 euro wil afrekenen. Carol start de betaling bij de juwelier, met een aangepast toestel dat in verbinding staat met Bob, maar die er verder normaal uitziet. De communicatie van en naar Carol's toestel wordt via Bob 'gerelayed' naar Alice. Afhankelijk van het systeem dient Alice haar pincode in te voeren, die Bob doorseint (via een headset bijvoorbeeld) naar Carol. Wanneer Carol de transactie afrondt met deze pincode, is de transactie klaar en hebben Bob en Carol de ring betaald met het geld van Alice. De enige troost voor Alice is dan dat haar maaltijd 'gratis' is.

**Aanval bij een pull-initiatie (initiatie door de verkoper)**
Carol wil haar ring van €2000,- afrekenen bij de juwelierszaak. De verkoper start de betaling en maakt daarvoor contact met het toestel van Carol. Carol stuurt deze berichten rechtstreeks door naar Bob, die met een eigen, gemodificeerde, PoS ergens anders zit. Hij start daar een betaling met een nietsvermoedende Alice en op deze wijze wordt de hele betaling 'gerelayed' via Carol en Bob naar Alice. Wanneer het protocol geen pincode of andere bevestiging nodig heeft, kan de betaling simpelweg worden afgerond op de kosten van Alice. Wanneer dat wel nodig is, is het minder waarschijnlijk dat Alice zomaar haar pincode in toetst om de betaling te bevestigen.

**Impact**
Op deze wijze kan op grote schaal fraude worden gepleegd. Het vereist wel

een goede timing en wat apparatuur, die verder niet heel specialistisch en makkelijk te verkrijgen is. Dat het een aanval is die goed mogelijk is, wordt bewezen in [24].

**Tegenmaatregelen**
De belangrijkste tegenmaatregel die genomen kan worden, is door gebruik te maken van een *distance bounding* protocol. Daarbij wordt door middel van het meten van de tijd die nodig is om een pakketje heen en weer te sturen tussen het PoS en het toestel. Aan de hand daarvan kan vrij accuraat de afstand tussen deze twee worden vastgesteld[25,26]. Als deze te groot wordt, kan er dan een 'alarm' afgaan.

**Risicoklasse**

| | |
|---|---|
| GSM netwerk met centrale opslag betalingsgegevens | - |
| GSM netwerk met lokale opslag betalingsgegevens | - |
| NFC met lokale opslag betalingsgegevens | Hoog |

## *9.4 Projecties en propagatie*

Om duidelijker te kunnen zien welke aanvallen een bedreiging vormen voor welk systeem, zullen we projecties van de boom maken. Daarin worden de risicofactoren gepropageerd, zodat op basis daarvan een vergelijk kan worden gemaakt.

### 9.4.1 Propagatiefunctie

In de projecties zijn de toegekende risicofactoren gepropageerd. Zoals Mauw en Oostdijk beschreven hebben in hun formalisatie van de attacktree[21], dient de propgatiefunctie distributief te zijn, wanneer je waardes wilt propageren in een boom die niet naar een normaalvorm is getransformeerd.

De volgende definities worden gehanteerd [21, blz 9]
***Definition 5.*** *Let $\mathbb{C}$ be a set of attack components. An attribute domain is a structure $(V, \nabla, \Delta)$, where $V$ is the set of attribute values, $\nabla: V \times V \to V$ is the disjunctive combinator for attribute values and $\Delta: V \times V \to V$ is the conjunctive combinator for attribute values. We require that the combinators are associative and commutative:*

$$(x \nabla y) \nabla z = x \nabla (y \nabla z)$$
$$x \nabla y = y \nabla x$$
$$(x \Delta y) \Delta z = x \Delta (y \Delta z)$$
$$x \Delta y = y \Delta x$$

*Given an attribute domain $(V, \nabla, \Delta)$ an attribute $\alpha$ is a function from $\mathbb{C}$ to*

*V . An attribute domain is distributive if the following property holds:*

$$x \Delta (y \nabla z) = (x \Delta y) \nabla (x \Delta z)$$

***Definition 6.*** *Let S be an attack suite and α an attribute with attribute domain (V, ∇, Δ), then the value attributed by α to S is*

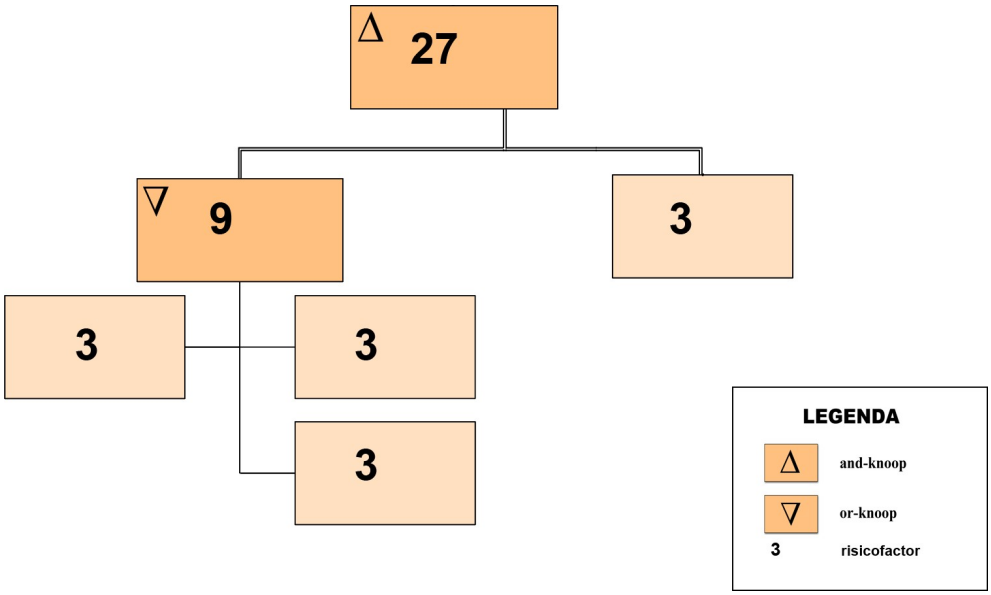
$$\alpha(S) = \nabla_{A \in S} \Delta_{c \in A} \alpha(c)$$

De propagatiefunctie die gebruikt is, had tot doel om tot uitdrukking te brengen dat een aanvalsdoel of aanval met 2 subaanvallen met risicofactor x, 'bedreigder' is dan eentje met slechts 1 aanval met diezelfde risicofactor x.

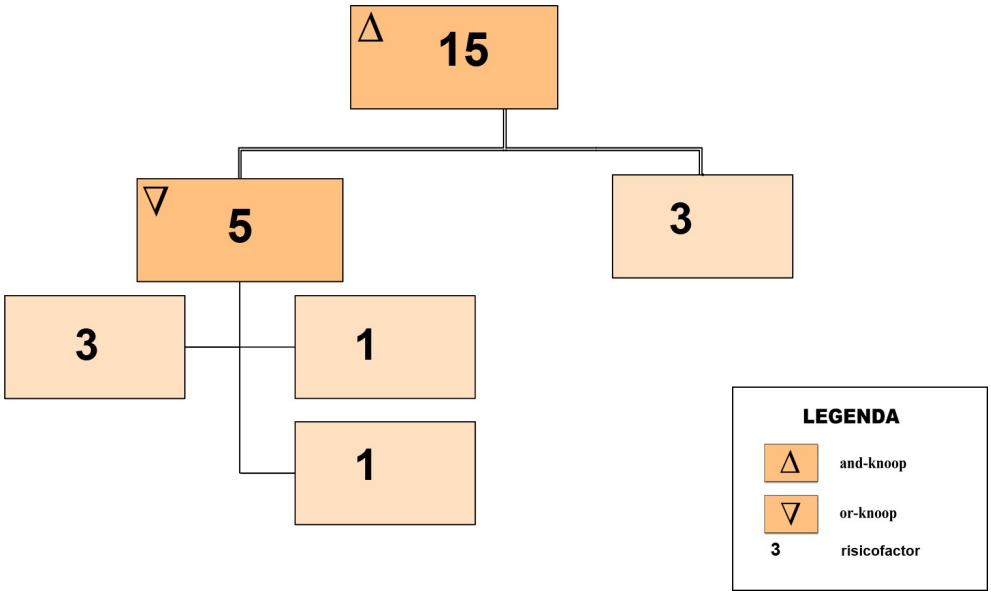
Als disjuncte operator($\nabla$) gebruiken we de +, als conjuncte operator ($\Delta$) de *-functie. Het is triviaal om te zien dat deze beide functies zowel associatief als commutatief zijn. Het attribuut domein is dan ($\mathbb{N}$,+,*), en dat is inderdaad distributief:

$$x * (y+z) = (x*y) + (x*z)$$

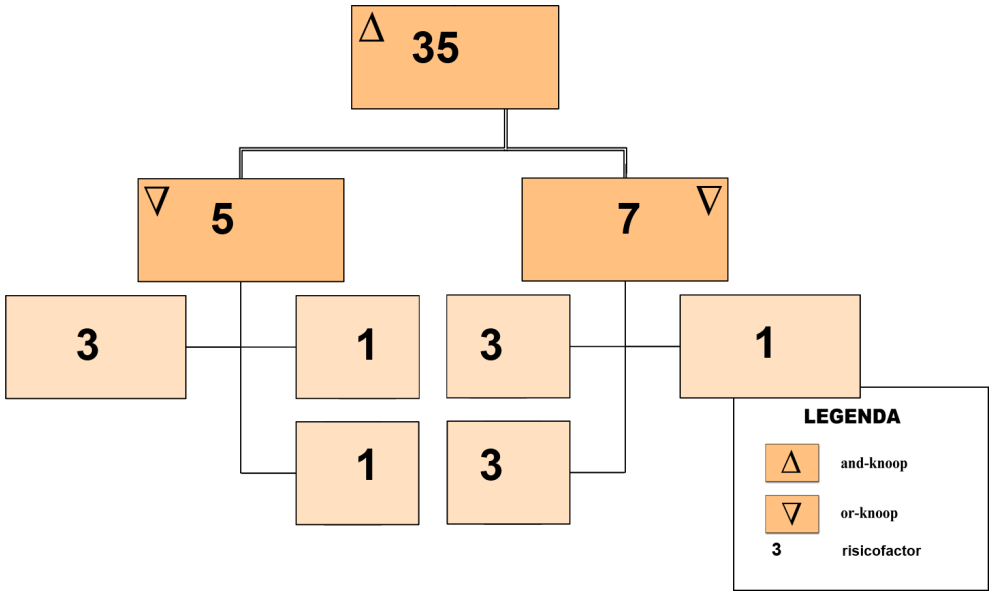
En de resultaten die dit oplevert zijn ook intuïtief juist. Neem de volgende drie voorbeeld attacktrees:




*Illustratie 13: Voorbeeld attacktree 1*




*Illustratie 14: Voorbeeld attacktree 2*

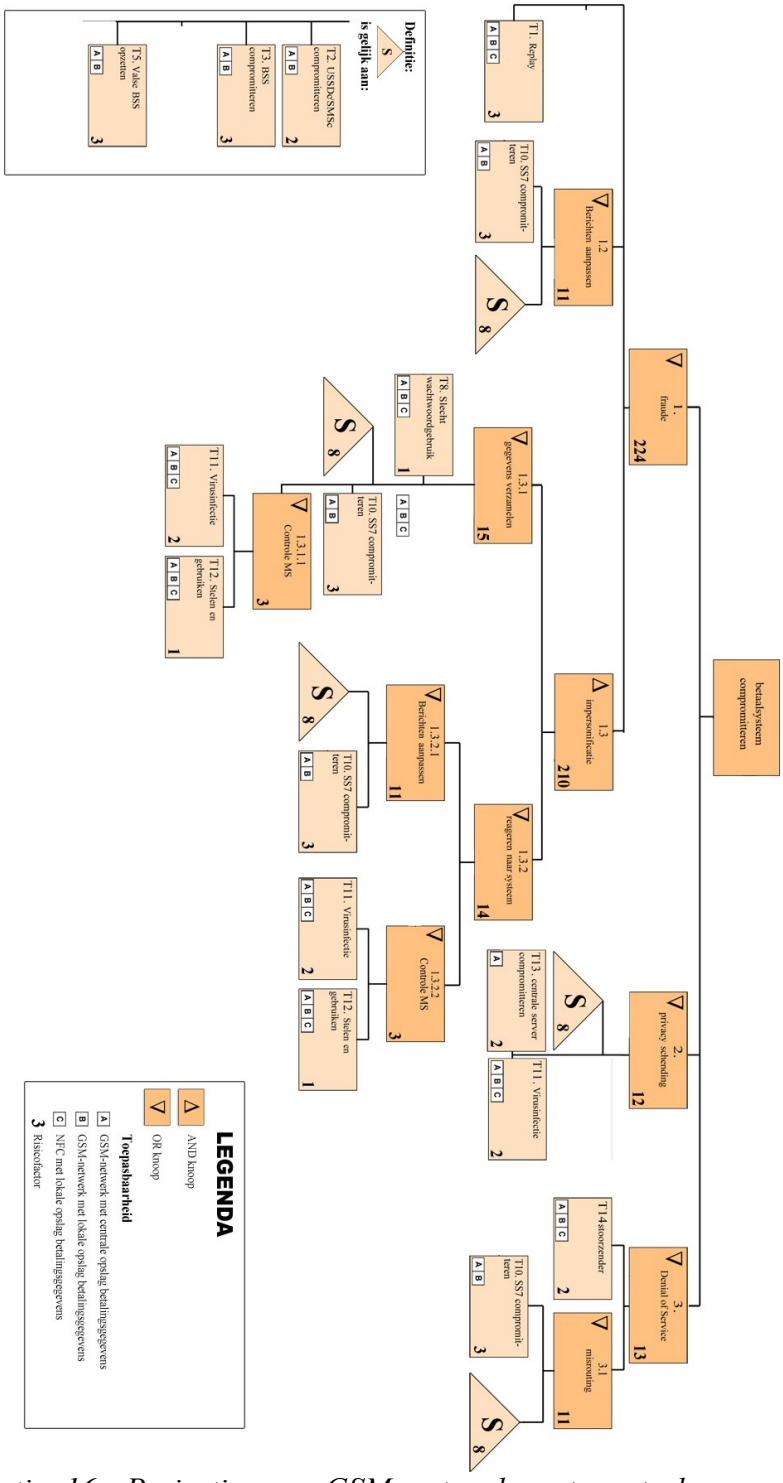



*Illustratie 15: Voorbeeld attacktree 3*

Voorbeeldboom 1 is 'bedreigder' dan boom 2, wat ook logisch is, omdat ze allebei 4 aanvallen hebben, maar deze aanvallen bij boom 1 een veel groter risico hebben. Voorbeeld 3 heeft, de losse knopen bij elkaar opgeteld, 'evenveel risico' als voorbeeld 1, maar omdat boom 3 meer aanvallen heeft, is hij toch 'bedreigder'.

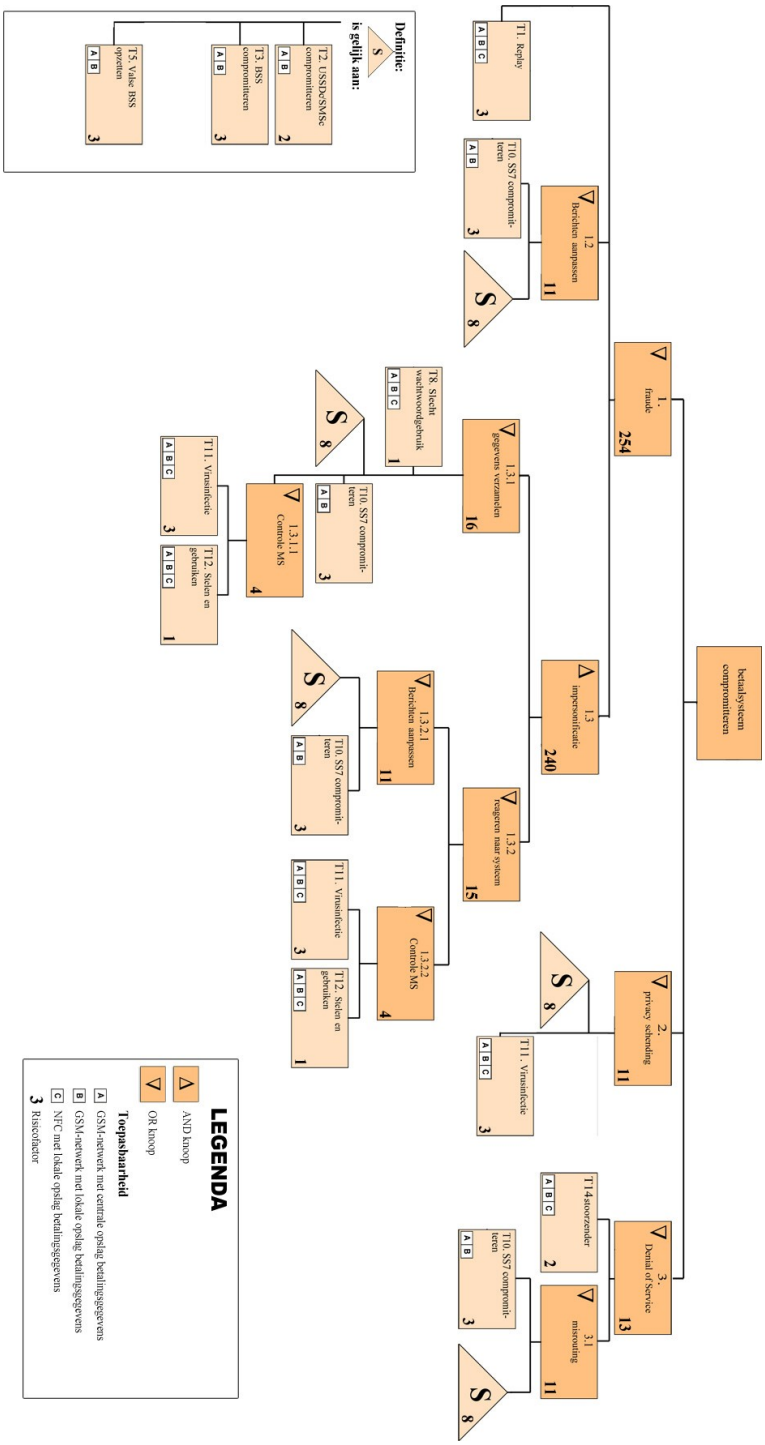
Om te de operaties te kunnen uitvoeren, nemen we voor de categorie *laag* een waarde van 1, voor categorie *middel* een waarde van 2 en voor categorie *hoog* een waarde van 3.

### 9.4.2 Projectie van GSM netwerk met centrale opslag betalings-gegevens



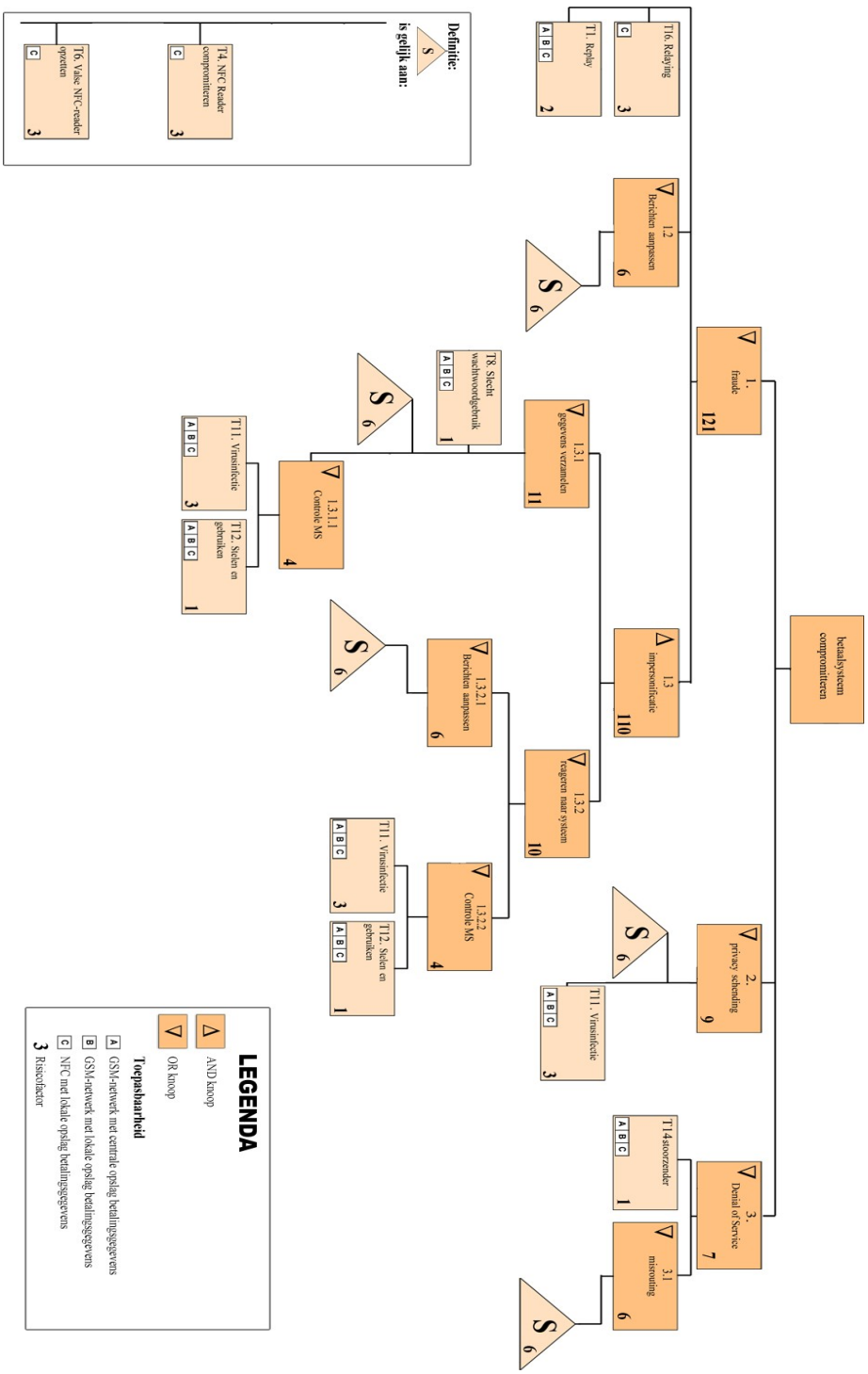

*Illustratie 16: Projectie van GSM netwerk met centrale opslag betalingsgegevens*

### 9.4.3 Projectie van GSM netwerk met lokale opslag betalings-gegevens




*Illustratie 17: Projectie van GSM netwerk met lokale opslag betalings-gegevens*

### 9.4.4 Projectie van NFC met lokale opslag betalingsgegevens




*Illustratie 18: Projectie van NFC met lokale opslag betalingsgegevens*

## 9.5 Vergelijk van de systemen

Op basis van de gemaakte projecties en de gepropageerde risicoklasses, komen we tot de onderstaande score:

| | **Fraude** | **Privacy** | **Denial of Service** |
|---|---|---|---|
| GSM netwerk, centrale opslag | 224 | 12 | 13 |
| GSM netwerk, lokale opslag | 254 | 11 | 13 |
| NFC, lokale opslag | 121 | 9 | 7 |

Uit dit overzicht blijkt dat, vanuit het oogpunt van veiligheid, de beste keuze op alle drie de gebieden voor implementatie van een mobiel betalingssysteem een systeem zou zijn op basis van Near Field Communication, waarbij de betalingsgegevens op het mobiele toestel opgeslagen zijn.

## 9.6 Conclusie

Op basis van dit hoofdstuk, valt te concluderen dat een systeem op basis van Near Field Communication de beste keuze is om te implementeren.

Van de aanvalsdoelen die zijn vastgesteld, kunnen we zeggen dat deze compleet en juist zijn, omdat zowel literatuuronderzoek als overleg met securitymedewerkers van Interpay hier verder geen aanvullingen op hebben gehad.

Op het gebied van de attacktrees is een aantal factoren, waarmee nog rekening gehouden moet worden. Ten eerste garandeert het gebruik van de attacktree methode niet dat de gemaakte analyse alle mogelijke aanvallen bevat. Hoewel deze analyse is besproken met een aantal experts, is het mogelijk dat er aanvallen over het hoofd zijn gezien. Dat kan van invloed zijn op het resultaat, alhoewel de verschillen tussen de drie systemen nu nog vrij groot zijn. Daarnaast zijn er bij deze systemen natuurlijk nog nauwelijks implementatiedetails bekend, en de keuze van nadere details zou best tot andere mogelijke aanvallen kunnen leiden. Het is dus aan te raden om nogmaals een analyse uit te voeren wanneer er een definitief ontwerp is.

De indeling in risicoklassen van de aanvallen uit de analyse is van grote invloed op de uitkomst van de propagaties, voornamelijk omdat er bij AND-knopen vermenigvuldigd wordt. De kans dat een aanval verkeerd is

ingedeeld is echter zo veel mogelijk beperkt, allereerst door vooraf vast te stellen wanneer een aanval in een bepaalde klasse valt en bovendien door hem voor te leggen aan een aantal experts. Daarnaast is de kans op een grote afwijking bij verkeerd categoriseren ook niet zo groot, omdat er slechts drie klassen zijn.

Het bleek niet eenvoudig om de bedreigingen te modelleren. Dat kwam enerzijds door het feit dat er nog geen echte ontwerpen of systemen waren, maar slechts een paar globale implementatiekeuzes. Anderzijds zijn attacktrees wellicht niet geschikt voor analyse van grote(re) systemen. De bomen worden al snel erg ondoorzichtig wanneer een aanval tot meerdere (sub)goals kan leiden. Een onoverzichtelijke brei van lijntjes is dan het gevolg. Daarom heb ik (sub)aanvallen met meerdere doelen even zo vaak in de boom gezet, wat weer tot gevolg heeft dat deze groter lijkt dan hij eigenlijk is.

De gebruikte software van de TUE is veel te mager om een degelijke attacktree te kunnen tekenen. Aanvallen kunnen slechts één doel dienen en er kan slechts één van de drie voorgedefinieerde soorten waardes (boolean, long of double) aan een aanval worden toekekend. Daarbij is de grafische view niet geïmplementeerd. Uiteindelijk zijn de attacktrees en de projecties helaas dus gewoon met de hand getekend.

# H10 Conclusie

## *10.1 Inleiding*

Dit hoofdstuk bevat het uiteindelijke doel van dit onderzoek; een advies aan Interpay ECS over welk betalingssysteem, die voldoen aan de eisen van de verschillende stakeholders, vanuit veiligheidsoogpunt het meest geschikt is om te implementeren als mobiel betalingssysteem. Dat advies is gebaseerd op de resultaten van dit onderzoek, komt aan bod in paragraaf 2 en kan de staf van Interpay ECS helpen om een gefundeerde beslissing te nemen over het al dan niet ontwikkelen van een systeem dat betalen met de mobiele telefoon mogelijk maakt.

Hierna worden kort de resultaten van het onderzoek samengevat, waarbij wordt gereflecteerd op de betrouwbaarheid, volledigheid en de nauwkeurigheid van de resultaten en welke invloed dit heeft op het geformuleerde advies. Daarna geef ik aan op welke wijze deze resultaten te verbeteren zijn. Omdat het onderzoek gesplitst is in twee subdoelen, komt in paragraaf 2 onderzoeksdoel 1 en in paragraaf 3 onderzoeksdoel aan bod.

De laatste paragraaf gaat in op het gebruik van de attacktree methode en is interessant voor degenen die deze methode zelf willen gaan gebruiken voor het maken van een analyse, of voor degenen die er vanuit wetenschappelijk oogpunt mee bezig zijn.. Hier worden de voor- en na-delen van het gebruik van deze methode voor het maken van een bedreigingsanalyse aangegeven en de punten waarop de methode eventueel aangepast of verbeterd kan worden.

## *10.2 Advies*

Op basis van de resultaten van dit onderzoek, een analyse op het gebied van veiligheid, is het advies om een mobiel betalingssysteem te implementeren op basis een combinatie van Near Field Communication (NFC) met lokale opslag van betalingsgegevens. NFC biedt naast de minste bedreigingen ook gebruikersgemak, omdat de betaling vlot kan verlopen en met weinig handelingen voor de gebruiker.

Uit het onderzoek kwamen drie mogelijke systemen naar voren, die voldoen aan de door de stakeholders gestelde eisen

- GSM netwerk, in combinatie met lokale opslag van betalings-

gegevens
- GSM netwerk, in combinatie met centrale opslag van betalings-gegevens
- NFC, in combinatie met lokale opslag van betalingsgegevens.

Op basis van de daarna gemaakte bedreigingsanalyse is daarna gekozen voor de laatste optie.

Tot slot heeft dit onderzoek alleen het veiligheidsaspect betrokken in de resultaten en dit advies. Er zijn natuurlijk veel meer aspecten waar naar gekeken moet worden voor dat er beslissingen genomen kunnen worden. Te denken valt daarbij aan het kostentechnische aspect, een doelgroepanalyse, etc. Dat dient dus nog onderzocht te worden.

## *10.3 Onderzoeksdoel 1*

Het eerste onderzoeksdoel van dit onderzoek luidt als volgt:

> ***Onderzoeksdoel 1****: Inzicht geven in de mate waarin bruikbare technologieën voor het implementeren van een mobiel betalingssysteem voldoen aan de technische eisen, die door de stakeholders die in de toekomst gebruik gaan maken van het mobiele betalingssysteem, gesteld worden aan mobiel betalen*

Om dit doel te bereiken, was de volgende kennis nodig:
- Hoe ziet het een model van het betaalproces eruit?
- Wat zijn de eisen die de stakeholders, die in de toekomst van het systeem gebruik gaan maken, aan een dergelijk systeem stellen
- Welke bruikbare technologieën er zijn om tot realisatie van een systeem voor mobiel betalen te komen
- In welke mate voldoen deze technologieën aan de gestelde eisen.

### 10.3.1 Reflectie op de resultaten

In hoofdstuk vier is een model opgesteld van het algemene betaalproces. Dit model laat zien hoe een betaling verloopt en welke rollen er zijn, ongeacht of dit een traditionele of mobiele betaling betreft. Omdat dit model is voorgelegd aan experts van Interpay, kunnen we er vanuit gaan het betrouwbaar is en een goede uitgangsbasis heeft gevormd voor het vervolg van het onderzoek.

Aan de stakeholders is hierna gevraagd welke eisen zij stellen aan een mobiel betalingssysteem. Van deze eisen zijn vervolgens alleen de eisen op technisch gebied gebruikt voor de rest van het onderzoek. Om dat bij een

dergelijk systeem een heel groot aantal stakeholders betrokken is, mede afhankelijk van de gekozen implementatie, is er vanwege tijdsdruk gekozen om alleen naar de eindgebruikers, consumenten en merchants, te kijken. Echter, omdat Interpay de opdrachtgever is, is ook onderzoek gedaan naar haar eisen en verwachtingen. Vanwege deze beperking is dit overzicht wellicht niet volledig, omdat andere stakeholders nog aanvullende, of misschien zelfs conflicterende, eisen en belangen kunnen hebben. Omdat dit echter wel de meest belangrijke stakeholders zijn, degenen die altijd bij het proces betrokken zijn, is de inventarisatie waarschijnlijk wel redelijk volledig. Meer stakeholders zullen daarnaast alleen nog mogelijkheden weg kunnen strepen.

Voor een zo breed mogelijk perspectief, is er een inventarisatie gemaakt naar bestaande mobiele betalingssystemen, waarbij gekeken is naar de technologie die gebruikt is voor de afwijkende fases, zoals die zijn vastgesteld in het model. Deze inventarisatie is een lange lijst, maar deze is ook aan veel verandering onderhevig; er komen voortdurend initiatieven bij en er worden voortdurend initiatieven gestopt. Dat is voor de volledigheid en nauwkeurigheid van de lijst wel van belang, maar gezien het feit dat deze lijst slechts dient om te inventariseren welke technologieën er voorhanden zijn, is dat niet van grote invloed op de resultaten van het onderzoek.

### 10.3.2 Aanbevelingen voor vervolgonderzoek

Om de lijst met eisen die gesteld worden door de stakeholders nog vollediger te maken, moet er met alle belanghebbenden van het systeem rekening worden gehouden. Wie dit precies zijn, hangt af van het te implementeren systeem, maar onder andere de banken, fabrikanten van apparatuur en mobiele telefoons kunnen daar nog een rol in spelen.

Tevens kan de betrouwbaarheid van de eisen die al deze stakeholders stellen, vergroot worden door het onderzoek daarnaar in eigen hand te nemen. Dat biedt natuurlijk geen garantie dat dit een beter onderzoek is, maar de betrouwbaarheid ervan is dan wel beter in te schatten.

Het is mogelijk dat er inmiddels nieuwe technologieën en inzichten beschikbaar zijn geworden. Voordat er met deze lijst van mogelijke implementaties aan de slag wordt gegaan, is het daarom raadzaam om te onderzoeken of er inmiddels meer mogelijkheden zijn ontstaan.

## *10.4 Onderzoeksdoel 2*

Het tweede doel van dit onderzoek luidt als volgt:

***Onderzoeksdoel 2:*** *Inzicht geven in de mate waarin de gevonden*

*(combinaties van) technologieën worden bedreigd door aanvallen die de veiligheid kunnen aan tasten.*

Om dit doel te bereiken, was de volgende kennis nodig:

- Wat zijn de bedreigingen die er voor de geselecteerde systemen voor mobiel betalen zijn?
- Welke van de systemen wordt het meest bedreigd?

### 10.4.1 Reflectie op de resultaten

Om een bedreigingsanalyse te maken, is allereerst een (semi-)formele methode gekozen om een dergelijke bedreigingsanalyse uit te voeren. Er zijn niet veel van dergelijke formele methodes, en de keuze tussen een methode gebaseerd op Petrinetten en de Attacktreemethode is op de laatste gevallen, vanwege de complete formele beschrijving, het feit dat er meer over gepubliceerd is en de beschikbaarheid van een softwaretool voor het tekenen van attacktrees. De keuze voor een andere methode voor het maken van een analyse, is echter niet van invloed op het uiteindelijke resultaat.

Deze attacktree methode is vervolgens gebruikt om mogelijke aanvallen op een mobiel betalingssysteem in kaart te brengen. De attacktree methode garandeert echter niet daadwerkelijk alle mogelijke aanvallen worden gevonden, op dat gebied biedt het niet meer dan een soort structuur om in te denken. De attacktree en de daarbij behorende lijst met aanvallen is echter doorgesproken met experts, dus de kans dat er grote zaken over het hoofd worden gezien is daarmee aanzienlijk verkleind. Het achterwege laten van een aanval zou wel van invloed zijn op de resultaten, maar gezien het forse verschil tussen de systemen, is het niet waarschijnlijk dat het de uiteindelijke uitkomst zal beïnvloeden.

Aan alle aanvallen is vervolgens een risicofactor toegekend. Het indelen in deze categorieën is geen hele nauwkeurige maat. Het zou goed kunnen dat een ander onderzoeker de indeling net iets anders maakt. Dat zal ook zeker invloed hebben op het eindresultaat, maar omdat deze indeling aan een aantal experts is voorgelegd, mogen we er vanuit gaan dat hij betrouwbaar is.

### 10.4.2 Aanbevelingen voor vervolgonderzoek

Bij de start van dit onderzoek was er niet gepubliceerd over nog andere formele methodes voor het maken van een bedreigingsanalyse. Het zou kunnen zijn dat dat inmiddels wel het geval is, eventueel vervolgonderzoek zou daar rekening mee dienen te houden.

Tevens moet nog wel worden opgemerkt dat er nu een analyse is gemaakt van een niet-bestaand systeem, waarvan alleen de hele grote lijnen bekend zijn, en verder geen details. Wanneer het systeem uiteindelijk echt ontworpen is, is het zeer aan te bevelen opnieuw een dergelijke analyse uit

te voeren, omdat de invulling van details kan zorgen dat er andere aanvallen mogelijk zijn op het systeem.

Overigens is het ook zo dat er voor de meeste aanvallen een goede tegenmaatregel bestaat, iets waarmee deze analyse geen rekening houdt, alhoewel deze maatregelen wel beschreven staan.

## *10.5 Gebruik van de attacktree methode*

Het opstellen van een bedreigingsanalyse wordt door het gebruik van de Attacktree methode vereenvoudigd. Wanneer de boom eenmaal getekend is, is het ook makkelijker om er mee aan de slag te gaan; projecties te maken, waardes propageren, de boom normaliseren, etc, omdat de methode formeel beschreven is.

De methode garandeert echter niet dat je alle aanvallen zult vinden. Het biedt een denkstructuur daarvoor, waarmee de kans wordt verkleind dat je iets vergeet, maar de enige maat om te zien of je aan alle aanvallen gedacht hebt, blijft nog steeds het aantal experts dat er naar gekeken heeft. Tot het punt waarop programma's al in de ontwerpfase compleet formeel gespecificeerd zijn, zal dit echter wel zo blijven.

Het opstellen van de boom zou ervoor moeten zorgen dat er overzicht ontstaat. Het blijkt echter dat wanneer de boom groter wordt, en er veel aanvallen zijn die meerdere doelen kunnen dienen, dit overzicht snel verloren gaat. De software van de TUE om attacktrees te tekenen is niet bruikbaar voor dit soort bomen. Attacktrees worden dus al snel onoverzichtelijk. Met flink wat uitbreiding zou deze software echter wel geschikt kunnen worden gemaakt. Er bestaat overigens ook commerciële software die helpt attacktrees te tekenen, echter is daar in dit onderzoek niet naar gekeken. Voor nieuwe analyses zou dat wel de moeite waard kunnen zijn.

De extra moeilijkheid voor deze casus was natuurlijk dat er niet echt een systeem ontwerp was. Het analyseren van de bedreigingen die bestaan voor niet bestaande systemen is echter wel interessant. Het zou ontwerpers natuurlijk veel waard zijn om van tevoren bepaalde verschillende ontwerpkeuzes te kunnen vergelijken op hun potentiële veiligheid. De ontwikkeling van een formele analysemethode die tevens gebruikt kan worden om ontwerkeuzes te vergelijken op veiligheidsgebied zou dus zeker een vervolgonderzoek waard zijn.

Er is op dit gebied ook maar weinig academische theorie en ook in de studie wordt er weinig aandacht besteed aan het uitvoeren van dergelijke analyses. Ik denk dat het absoluut de moeite waard is om dit wel te gaan doen, omdat het wel iets is dat veel gebruikt wordt bij het ontwikkelen van software.

# Literatuurlijst


[1] Analysys Research, *The Western European Mobile Market: trends and forecasts 2005–2010*, April 2005.

[2] Ir. S.L. Lelieveldt, De telecommunicatiesector als 'nieuwe' aanbieder, December 2003, Bank- en Effectenbedrijf

[3] Interpay E-Commerce Services, *http://www.interpay.nl/Over_Interpay/Werkenbij interpay/Deorganisatie/E-Commerce_Services.asp*

[4] Ruud Kolijn en Martijn Verrijn Stuart, *Mobiel betalen in Nederland*, December 2003, Bank en Effectenbedrijf

[5] *Mobiel Betalen*, Januari / Februari 2005, Digitale Consument

[6] Casper: A Compiler for the Analysis of Security Protocols: *http://web.comlab.ox.ac.uk/oucl/work/gavin.lowe/Security/Casper/*

[7] FDR2: *http://www.fsel.com/software.html*

[8] Mobile2Pay *http://www.mobile2pay.nl*

[9] European Committee for Banking Standards, *Implementation Guidelines for Mobile Payments*, Maart 2005, IG606 v1.0

[10] Arjan Dasselaar, *Lastig Digitaal Afrekenen*, 30 maart 2004, NRC Handelsblad

[11] Tjeerd Wiersman, *Betaaldienst Moxmo failliet*, 11 Augustus 2004, PCM.

[12] Ministerie van Economische Zaken, *Betalen via Nieuwe Media*, uitgegeven in 2004.

[13] Stefan Stadlober, *An Evaluation of Security Threats and Countermeasures in Distributed RFID Infrastructures*, Technische Universität Graz, juli 2005.

[14] Denis Verdon & Gary McGraw, *Risk analysis in Software Design*, IEEE Security & Privacy juni 2004.

[15]T.H. Smulders, *Security threats of executing malicious applications on mobile phones*, masterthesis uit 2004.

[16]Bruce Schneier, *Attacktrees*, december 1999

[17]T. Tidwell, R. Larson, K. Fitch & J. Hale, ModelDesigning *Internet Attacks*, IEEE juni 2001

[18]Jan Steffan en Markus Schumacher, *Collaborative Attack Modeling*, In Proc. Sac 2002, blz. 253-259, 2002.

[19]J.P. McDermott, *Attack net penetration testing*, Proceedings of the 2000 workshop on new security Paradigms, pp 15-21, 2000.

[20]Mobile Payment Forum, *Risks and threats analysis and security best practices*, mei 2003

[21]Sjouke Mauw, Martijn Oostdijk, *Foundations of Attacktrees*, Proc. ICIS'06, LNCS 3935, pp 186-198, 2006

[22]http://www.isograph-software.com

[23]John Conway, *On numbers and games*, Academic Press, 1976

[24]Saam Drimer and Steven J. Murdoch, *Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks*

[25]Beth and Desmedt, *Identification tokens – or: Solving the chess grandmaster problem,* CRYPTO 537, pp. 169–17, 1990

[26]Brands and Chaum , *Distance-bounding protocols,* EUROCRYPT ’93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology, mei 1993, T. Helleseth, Ed., vol. 765 of LNCS, Springer, pp. 344–359.

[27] Alexander Opel, *Design and implementation of a support tool voor attack trees*, 2005

# Lijst van gebruikte afkortingen

| | |
|---|---|
| BSC | *Base Station Controller* |
| BSS | *Base Station (sub)System* |
| BTS | *Base Transeiver Station* |
| DoS | *Denial of Service* |
| EGI | *Electronische Geld Instelling* |
| HLR | *Home Location Register* |
| IMEI | *International Mobile Equipment Identity* |
| IMSI | *International Mobility Subscriber Identity* |
| MS | *Mobile Station* |
| MSISDN | *Mobile Station Integrated Services Digital Network* |
| NFC | *Near Field Communication* |
| PCP | *Payment Credential Provisioning* |
| PIN | *Persoonlijk Identificatie Nummer* |
| PoS | *Point of Sale* |
| RFID | *Radio Frequency IDentification* |
| SIM | *Subscriber Identity Module* |
| SGSN | *Serving GPRS Support Node* |
| *SMC* | *Secure Memory Card* |
| SMS | *Short Message Service* |
| SMSc | *SMS Centrale* |
| SS7 | *Signalling System 7* |
| USSD | *Unstructured Supplementary Service Data* |
| USSDc | *USSD Centrale* |
| VLR | *Visitor Location Register* |

# Bijlage A: Begripsbepalingen

Om verwarring te voorkomen staan hieronder een aantal begripsbepalingen die van belang zijn in deze thesis.

### Mobiel betalen

Onder mobiel betalen verstaan we een vorm van elektronisch betalen waarbij het betaalinstrument via een draadloos netwerk communiceert met de achterliggende systemen. Zulke betaalinstrumenten kunnen bijvoorbeeld PDA's of notebook zijn, maar ook de mobiele telefoon. Het gaat hierbij om een online-systeem.

### Betalingssyteem

Met een betalingssysteem wordt een systeem bedoelt waarmee betalingen kunnen worden verricht. Een dergelijk systeem kent feitelijk twee soorten gebruikers: degenen die wil betalen, veelal een consument en daarom in deze scriptie ook zo genoemd, en degene die de betaling ontvangt. Die laatste is meestal een verkopende partij (merchant), maar zou ook een particulier kunnen zijn. Een betalingssysteem zorgt ervoor dat het tussen beide partijen overeengekomen bedrag veilig van de bankrekening van de één naar de ander gaat. Tevens confirmeert een betalingssysteem de betaling aan beide partijen.

# Bijlage B: Wet Toezicht Kredietwezen

Volgens de Wet Toezicht Kredietwezen (uit 1992) moeten kredietinstellingen een vergunning hebben van de Nederlandse Bank. De definitie van een kredietinstelling staat in artikel 1, eerste lid van de WTK:

> *Voor de toepassing van het bij of krachtens deze wet bepaalde wordt verstaan onder:*
> ***a.*** *kredietinstelling:*
> > ***1°.*** *een onderneming of instelling die haar bedrijf maakt van het ter beschikking verkrijgen van, al dan niet op termijn, opvorderbare gelden en van het voor eigen rekening verrichten van kredietuitzettingen of beleggingen; dan wel*
> > ***2°.*** *een onderneming of instelling, anders dan bedoeld onder 1°, die gelden ter beschikking krijgt in ruil waarvoor elektronisch geld wordt uitgegeven waarmee betalingen kunnen worden verricht ook aan anderen dan de onderneming of instelling die het elektronisch geld uitgeeft.*

(De belangenvereniging voor kredietinstellingen, 11a2, heeft zijn naam hieraan ontleend.)

Kredietinstellingen vallen in principe onder toezicht van de Bank. Vrijstelling is echter mogelijk. De mogelijkheden hiertoe zijn vastgelegd in de Vrijstellingsregeling (ook uit 1992):

> ***Artikel 6***
> ***1.*** *Vrijstelling van het in artikel 6, eerste lid, van de wet genoemde verbod elektronisch geld uit te geven wordt verleend aan ondernemingen of instellingen die elektronisch geld uitgeven met een maximum geldswaarde van € 150 per elektronische waardedrager; voor zover:*
> > ***a.*** *de gezamenlijke waarde van de financiële verplichtingen van de ondernemingen of instellingen die met de uitgifte van elektronisch geld verband houden nooit hoger is dan € 6.000.000;*
> > ***b.*** *het elektronische geld slechts wordt aanvaard door ondernemingen of instellingen die behoren tot de groep, bedoeld in artikel 24b van Boek 2 van het Burgerlijk Wetboek, waartoe de ondernemingen of instellingen die elektronisch geld uitgeven, behoren; of*
> > ***c.*** *het elektronische geld slechts wordt aanvaard door een beperkt aantal gemakkelijk te onderscheiden*

*ondernemingen of instellingen dat hetzij hetzelfde gebouw, terrein of een andere feitelijk begrensde locatie deelt, hetzij nauwe financiële of zakelijke banden heeft met de ondernemingen of instellingen die elektronisch geld uitgeven.*

Een instelling moet minstens aan a of b of c voldoen, één van de drie is genoeg om vrijstelling te krijgen. Ook met vrijstelling is er nog enige controle verplicht, maar dit zijn geen ingrijpende zaken:

- Het jaarboek moet jaarlijks in worden gediend
- De waarde van het elektronische geld moet gelijk zijn aan de waarde van het ontvangen geld
- Er is een omwisselplicht

## *Telecom operators*

Met de bovenstaande definities zouden telecomoperators in de problemen komen met hun prepaid beltegoed kaarten. Het is immers mogelijk om betalingen aan derden te voldoen, bijvoorbeeld door middel van Premium SMS. Telecomoperators worden echter niet aangemerkt als EGI, het beltegoed wordt door de Bank gezien als vooruitbetaling van een dienst. Een gevolg hiervan is dat telecomoperators ook niet verplicht zijn beltegoed terug te betalen, wat wel verplicht is voor kredietinstellingen.