Internet zonder kabels, Internet zonder vertrouwen?

Mobile commerce en betrouwbaarheid

Auteur:
J. ter Hart
ANR: 157996
Katholieke Universiteit Brabant, Tilburg
Faculteit der Economische Wetenschappen,
Afstudeerscriptie Bestuurlijke Informatiekunde

Ter beoordeling voorgelegd aan:
Prof. Dr. P.M.A. Ribbers
Drs. R.R. Peterson

Voorwoord

Deze scriptie heb ik geschreven ter afronding van mijn studie Bestuurlijke Informatiekunde aan de Katholieke Universiteit Brabant. De afstudeerstage waarop de scriptie is gebaseerd heb ik uitgevoerd bij DigiNotar B.V., te Beverwijk.

Tijdens deze afstudeerstage heb ik onderzocht wat de rol van een Trusted Third Party is bij het bevorderen van de betrouwbaarheid van mobile commerce.

De stageperiode bij DigiNotar heb ik als zeer prettig ervaren. Met name de samenwerking met Kick, mijn begeleider bij DigiNotar, was erg goed. Ik wil hem bij deze dan ook bedanken voor alle ondersteuning tijdens mijn afstudeerstage. Tevens wil ik ook Joyce bedanken voor al haar adviezen op het juridische vlak. Verder wil ik alle andere collega's bij DigiNotar bedanken voor de leuke tijd die ik daar heb gehad.

Uiteraard ben ik ook dank verschuldigd aan Dhr. Ribbers voor zijn goede begeleiding vanuit de universiteit en aan Dhr. Peterson voor het zitting nemen in de examencommissie.

Tenslotte wil ik nog een aantal personen bedanken die mij tijdens de studententijd en de stageperiode altijd gesteund hebben. Mijn ouders verdienen hierbij een speciale plaats, omdat zij het mogelijk hebben gemaakt dat ik kon gaan studeren en altijd voor mij klaar stonden. Gabriëlle ben ik ook erg dankbaar voor haar steun tijdens het afstuderen en met name de laatste maanden heeft zij zeer veel voor mij betekend. Verder wil ik alle vrienden bedanken en Joost en Rinske in het bijzonder.

Joris ter Hart
Beverwijk, oktober 2001

Management samenvatting

Inleiding

Het gebruik van mobiele apparaten begint steeds meer toe te nemen in onze samenleving. In veel Europese landen is de penetratiegraad inmiddels de 60% grens gepasseerd. De mens heeft een stijgende behoefte om altijd en overal de beschikking te hebben over informatie en zijn zaken te allen tijde te kunnen regelen. In combinatie met het grote succes van het internet, is er een nieuwe ontwikkeling gaande: *Mobile commerce.* De definitie van mobile commerce die in dit onderzoek wordt gehanteerd luidt als volgt:

"Mobile commerce is defined as any transaction that is conducted via new wireless technology to public and private networks." (www.ieb.net, 2000)

Bij de doorbraak van electronic commerce speelt het gebrek aan vertrouwen van de gebruiker in elektronische transacties een grote rol. Men kan veronderstellen dat de betrouwbaarheid van de transacties ook bij m-commerce bepalend zal zijn voor de doorbraak hiervan. De betrouwbaarheid van een elektronische transactie wordt onder andere door de volgende factoren bepaald:

- Authenticiteit
- Integriteit
- Vertrouwelijkheid
- Beschikbaarheid

Deze factoren worden in de vaste wereld door een Trusted Third Party gewaarborgd. In dit onderzoek wil ik nagaan wat de rol van de Trusted Third Party is bij het betrouwbaar maken van mobiele transacties en hoe de TTP invulling aan deze rol kan geven. De probleemstelling is als volgt geformuleerd:

"Welke rol heeft een Trusted Third Party bij het bevorderen van het vertrouwen en de veiligheid bij het realiseren van mobiele transacties voor B2B en B2E m-commerce en hoe kan een TTP invulling geven aan deze rol?"

Mobile commerce

Zowel op het gebied van de techniek als de applicaties is de m-commerce markt op dit moment sterk in ontwikkeling. De ontwikkeling van de netwerktechnologieën speelt hierbij een belangrijke rol. Op dit moment is GSM de meest gebruikte standaard in Europa. GPRS begint nu langzamerhand door te breken. Met GPRS is de transmissiesnelheid hoger en dit maakt weer nieuwe applicaties mogelijk en bruikbaar. UMTS, het zogenaamde derde generatie netwerk, zal voorlopig nog niet geïmplementeerd worden. Voor m-commerce worden er andere protocollen gebruikt dan bij e-commerce, het meest gebruikte protocol is het Wireless Application Protocol.
M-commerce heeft een aantal onderscheidende kenmerken ten opzichte van e-commerce. Uiteraard zijn er ook een aantal beperkingen. Op basis van de kenmerken en beperkingen wordt duidelijk dat m-commerce een uitbreiding en geen vervanging is voor e-commerce. Om m-commerce tot een succes te maken, moeten er applicaties ontwikkeld worden, die gebruik maken van de onderscheidende kenmerken en rekening houden met de beperkingen. Een andere vereiste is de betrouwbaarheid van de

transacties. Deze eisen zijn niet anders dan bij e-commerce. Het soort transacties is hetzelfde, alleen het medium is veranderd. Hierdoor veranderen de betrouwbaarheidseisen niet. Deze eisen zijn:

- Authenticatie
- Integriteit
- Vertrouwelijkheid
- Onweerlegbaarheid

Cryptografie en de Trusted Third Party

Met behulp van cryptografie kunnen elektronische berichten worden beveiligd. Met deze techniek kan een bericht versleuteld en ontsleuteld worden en kan men een bericht digitaal ondertekenen. Dit versleutelen en ondertekenen gebeurt met digitale sleutels, die werken op basis van algoritmes. De volgende drie technieken zijn te onderscheiden:

- Symmetrische encryptie
- Asymmetrische encryptie
- Hybride encryptie

Het gebruik van alleen sleutelparen waarborgt echter niet de zojuist genoemde betrouwbaarheidseisen. Om dit te bereiken moet het sleutelpaar aan een fysieke identiteit worden gekoppeld. Hiervoor is de Trusted Third Party zeer geschikt. De definitie van een TTP die in dit onderzoek gedefinieerd is, luidt als volgt:

"Een Trusted Third Party is een vertrouwde, onafhankelijke en onpartijdige organisatie die vertrouwensdiensten levert voor het bevorderen van het vertrouwen in elektronische transacties."

De TTP koppelt de fysieke identiteit middels een digitaal certificaat aan een digitale identiteit. De gangbare digitale certificaten zijn gebaseerd op de X.509v3 standaard. Bij het uitgeven van de digitale certificaten zijn de volgende partijen betrokken:

- Registration Authority
- Certification Authority
- Authorizing Authority
- Gebruiker

Deze partijen voeren een aantal processen uit om tot een betrouwbare uitgifte van een digitaal certificaat te komen. De belangrijkste processen hierbij zijn: certificaataanvraag, controle van de aanvraag, uitgifte van het certificaat en het gebruik van het certificaat. Het geheel van certificaten en processen rondom de certificaten wordt een Public Key Infrastructure (PKI) genoemd.
De elektronische handtekening die gezet wordt op basis van cryptografie en het digitale certificaat is bij wet gelijkgesteld aan de geschreven handtekening. Hiervoor moet wel aan een aantal eisen en randvoorwaarden worden voldaan. De belangrijkste wet is de nationale implementatie van de Europese Richtlijn betreffende de elektronische handtekening, 1993/93/EG. Om betrouwbare diensten te leveren moet de TTP aan een aantal eisen en voorwaarden voldoen. De belangrijkste eisen zijn onder andere: onpartijdigheid en onafhankelijkheid.

Uitdagingen bij het leveren van mobiele identiteit

Het leveren van een mobiele identiteit verloopt anders dan het leveren van een identiteit bij e-commerce. Wanneer de kenmerken en beperkingen van m-commerce gecombineerd worden met de technieken en processen om elektronische berichten betrouwbaarder te maken, komen een aantal uitdagingen naar voren voor het leveren van mobiele identiteit. Deze uitdagingen worden enerzijds veroorzaakt door de technische beperkingen, zoals de beperkte bandbreedte en de beperkte rekencapaciteit van het mobiele apparaat. Anderzijds worden de uitdagingen veroorzaakt doordat de mobiele telecomoperator een belangrijke rol speelt in de mobiele markt en daarom ook een belangrijke speler kan zijn in de mobiele vertrouwensmarkt. De uitdagingen zijn op te splitsen naar technologische en procedurele uitdagingen. Deze uitdagingen leveren weer kansen en bedreigingen op voor 'traditionele' TTP's als DigiNotar. De kansen worden veroorzaakt doordat er een geheel nieuwe markt ontstaat en de bedreiging houdt in dat de telecomoperator de rol van TTP in de mobiele markt gaat vervullen. Indien de mobiele vertrouwensmarkt de vaste vertrouwensmarkt gaat vervangen, is dit een serieuze bedreiging.
Om met deze uitdagingen, kansen en bedreigingen om te gaan wordt in dit onderzoek een model ontwikkeld waarmee de rol van een TTP in de mobiele vertrouwensmarkt bepaald wordt en op basis van het model kan een invulling aan deze rol worden gegeven. Omdat er geen eenduidig antwoord mogelijk is op de probleemstelling, is het model een hulpmiddel bij het onderzoek om de probleemstelling te beantwoorden en is het geen doel op zich. Ter ondersteuning van de modelontwikkeling, wordt in dit onderzoek de regulatieve cyclus van van Strien gebruikt.

Het model voor het leveren van een mobiele identiteit

Het model bestaat uit twee fases. De eerste fase behelst de rolverdeling in de mobiele vertrouwensmarkt en in de tweede fase wordt invulling aan de gekozen rolverdeling gegeven.
Om tot een goede rolverdeling te komen, zijn er een vijftal scenario's gedefinieerd, waaruit één scenario wordt gekozen om de tweede fase van het model te starten. De scenario's zijn onder andere gebaseerd op de volgende drie kerntaken die uitgevoerd moeten worden om een Wireless PKI te realiseren:

- Het aanbieden van de mobiele applicatie door de dienstverlener
- Het aanbieden van de mobiele betrouwbaarheidsdiensten door een TTP
- Het faciliteren van het mobiele netwerk door de mobiele telecomoperator

Uit de volgende vijf scenario's is het derde scenario als uitgangspunt gekozen voor de tweede fase van het model.

1. Dienstverlener vervult en beheert zelf de functies van CA en RA
2. Dienstverlener maakt gebruik van een managed CA
3. De 'traditionele' TTP vervult de functies van CA en RA
4. De telecomoperator is de CA en besteedt de RA-functie uit
5. De telecomoperator vervult zowel de rol van RA als CA

De keuze is gebaseerd op de interviews die ik met diverse experts heb gehouden, de theorie en eigen inzicht. Hieruit is gebleken dat op basis van de eigenschappen van de verschillende partijen, de 'traditionele' TTP het meest geschikt is om de vertrouwensfunctie ook in de mobiele wereld te vervullen. De keuze voor het derde

scenario wil niet zeggen dat de overige scenario's niet mogelijk zijn. De scenario's kunnen naast elkaar bestaan.
In de tweede fase is er een checklist ontwikkeld. De checklist is een hulpmiddel voor het implementeren van een WPKI en geen vaststaande handleiding. In deze lijst wordt beschreven welke punten van belang zijn bij het implementeren van een WPKI. Op basis van de checklist kan een TTP invulling geven aan haar rol in de mobiele vertrouwensmarkt. De checklist is onderverdeeld in een aantal hoofdgroepen:

- Techniek
- Processen
- Onderlinge relaties
- Organisatie TTP
- Juridische eisen
- Mens en cultuur

Toetsing van het model

Om het model op juistheid te kunnen beoordelen is het noodzakelijk om het model te toetsen. In dit geval is het model getoetst aan een voorstel van Baltimore Technologies. Baltimore levert software voor een PKI en implementeert zelf ook PKI's. In dit voorstel wordt door Baltimore een oplossing gegeven voor het implementeren van een WPKI. Ik heb dit voorstel vergeleken met het ontwikkelde model en de verschillen geanalyseerd. Op basis van deze analyse is het model waar nodig aangepast. Het voorstel van Baltimore behandelde niet alle aspecten uit het model en daarom heb ik het model ook besproken met een expert van Baltimore op het gebied van een WPKI.
Uit de toetsing bleek dat de marktpartijen nog druk bezig zijn met ontwikkelen van een WPKI en dat er nog veel onzekerheden zijn. Daarom is het ook onmogelijk om op basis van de toetsing te veronderstellen dat het model volledig is. Wel is gebleken dat het model een zeer goede richtlijn is voor het implementeren van een WPKI.
Het model is ontwikkeld voor de B2B en B2E markt, maar na enkele aanpassingen kan het model ook gebruikt worden voor andere markten. Deze gedachtegang geldt ook voor de scenario's. Door de complexiteit van het derde scenario, kan de checklist waarschijnlijk ook voor de andere scenario's gebruikt worden.

Conclusies en aanbevelingen

Naar aanleiding van dit onderzoek kan geconcludeerd worden dat de 'traditionele' TTP in de mobiele vertrouwensmarkt een belangrijke rol kan spelen. De functie van de TTP zal niet wezenlijk verschillen van haar functie in de vaste wereld. De invulling van de rol van de TTP zal wel verschillen van de vaste wereld. Het geheel is veel complexer en er moet veel worden samengewerkt met andere partijen en vooral met de telecomoperator.
Omdat de mobiele markt nog volop in ontwikkeling en beweging is doe ik een aantal aanbevelingen voor verder onderzoek. Dit verdere onderzoek is noodzakelijk voor de TTP om een definitieve beslissing te nemen over het benaderen van de mobiele markt. Deze aanbevelingen zijn de volgende:

- De behoefte uit de markt aan een WPKI moet continu onderzocht worden.
- Er moet onderzocht worden wat de time to market van de WPKI is.
- Op basis van de uitkomst van bovenstaande punten moet het moment van levering van mobiele certificaten bepaald worden.
- Het ontwikkelde model is geen vaststaand statisch model en moet als gevolg van de dynamische markt regelmatig bekeken en zonodig herzien worden.
- De business case van de WPKI moet verder uitgewerkt worden.

Inhoudsopgave

Figuren

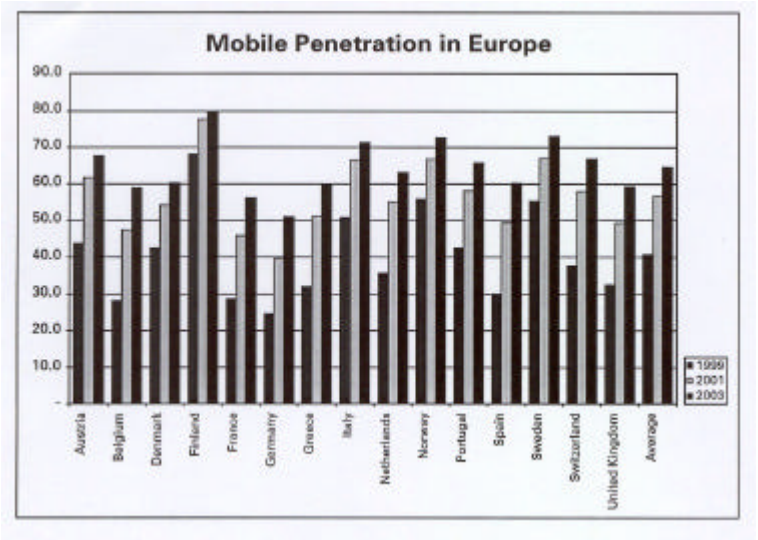
Tabellen

Hoofdstuk 1: Introductie

In dit eerste hoofdstuk leg ik uit waarom ik voor dit afstudeeronderwerp heb gekozen en wordt de structuur van het onderzoek beschreven.

1.1 Inleiding

Electronic commerce is al geruime tijd een hot item, veel personen en organisaties hebben tegenwoordig de beschikking over internet en maken hier regelmatig gebruik van. Je kunt dus zeggen dat het gebruik van internet in de samenleving behoorlijk is ingeburgerd. Door de toenemende penetratiegraad van mobiele apparaten en de behoefte van de mens om altijd en overal de beschikking te hebben over informatie en zijn zaken te allen tijde te kunnen regelen, is er een nieuwe ontwikkeling gaande: *Mobile commerce.* Uit onderstaande figuur blijkt dat het percentage van de bevolking dat de beschikking heeft over een mobiel apparaat tussen 1999 en 2001 het sterkst is toegenomen en dat de groei nu iets minder sterk doorzet. Men kan zien dat in bijna ieder land al een penetratiegraad van 60% bereikt is. Deze groep gebruikt het mobiele apparaat op dit moment hoofdzakelijk voor spraak en SMS.



Figuur 1.1 Mobiele penetratie in Europa, bron: Dataquest, Mobile Communications International

Maar wat is nu eigenlijk mobile commerce? De definitie van mobile commerce die ik in dit onderzoek zal gebruiken is:

"Mobile commerce is defined as any transaction that is conducted via new wireless technology to public and private networks." (www.ieb.net, 2000)

Middels technieken als Bluetooth en de ontwikkeling van nieuwe technieken zoals GPRS en UMTS waarmee mobiele netwerken steeds sneller worden, wordt m-commerce steeds toegankelijker voor de gebruiker. Een zeer belangrijk issue voor potentiële gebruikers is de mate van vertrouwen die ze hebben in de mobiele elektronische transacties. Bij de doorbraak van electronic commerce speelt het gebrek aan vertrouwen van de gebruiker in de elektronische transactie een grote rol en dit wordt dan ook als een belangrijk obstakel gezien. Je kunt dus veronderstellen dat de mate van vertrouwen die de gebruiker heeft in het gebruik van m-commerce ook bepalend zal zijn voor de doorbraak van m-commerce (Yankee Group, 2000).

De betrouwbaarheid van een transactie wordt door een aantal factoren bepaald. Deze zijn onder andere: (Koops, 1998)

- De *authenticiteit* van gegevens: zekerheid over de identiteit van de afzender, middels digitale handtekening, en over de herkomst van berichten en daarmee samenhangend;
- De *integriteit* van gegevens: zekerheid dat gegevens volledig zijn en niet door onbevoegden zijn gewijzigd;
- De *vertrouwelijkheid* van gegevens: zekerheid dat gegevens niet ingezien kunnen worden door personen die daartoe niet bevoegd zijn;
- De *beschikbaarheid* van gegevens: zekerheid dat gegevens op het juiste moment voor de rechthebbende toegankelijk zijn.

Dit vertrouwen is voor m-commerce waarschijnlijk nog moeilijker te realiseren dan bij "traditionele" e-commerce, omdat m-commerce een nieuw fenomeen is en dat schrikt mensen vaak af. In de beginfase van e-commerce waren de mensen ook wantrouwend over dit medium en werden er amper elektronische transacties afgesloten. Naarmate de gebruiker beter bekend werd met internet, nam het aantal transacties ook toe. Een goed voorbeeld hiervan is het internetbankieren, dat nu behoorlijk is ingeburgerd. Een andere reden is dat door de huidige stand van de techniek de mogelijkheden van m-commerce nog beperkt zijn, dit betekent dat de beveiligingstechnieken die nu bij electronic commerce gebruikt worden om vertrouwen te realiseren ook niet allemaal geschikt zijn voor m-commerce. Men moet dus onderzoek doen naar andere bruikbare technieken en methodes. Op deze problematiek wil ik middels dit afstudeeronderzoek een antwoord vinden.

1.2 DigiNotar

Dit afstudeeronderzoek heb ik uitgevoerd bij DigiNotar in Beverwijk. DigiNotar is een publieke Trusted Third Party ofwel betrouwbare derde partij op het internet. DigiNotar is het samenwerkingsverband van vooruitstrevende notarissen die met één gezicht naar de markt de klassieke vertrouwensrol van het notariaat nu ook op het internet vervullen. De combinatie van nieuwe technologieën met de vertrouwensfunctie van het notariaat creëert een synergie die het mogelijk maakt om betrouwbaarheidsdiensten aan te bieden.
Op dit moment zijn 74 notariskantoren verspreid over Nederland bij DigiNotar aangesloten. Daarin participeren meer dan 200 notarissen. Deze notarissen treden hierbij op als Trusted Third Party. In die rol kunnen zij elektronische handtekeningen verstrekken en natuurlijk- en rechtspersonen voorzien van een digitale identiteit. De DigiNotar-notaris realiseert hierdoor betrouwbaarheid op het internet.
Op het 'hoofdkantoor' van DigiNotar in Beverwijk zijn op dit moment ruim 30 mensen werkzaam. De afdeling consultancy waar ik mijn stage heb uitgevoerd bestaat momenteel uit acht personen. Deze afdeling ontwikkelt in samenwerking met de klant maatwerk oplossingen op het gebied van Public Key Infrastructure. Het gehele traject van advies geven over de te implementeren oplossing tot aan de implementatie daarvan wordt door deze afdeling begeleid. Verder bestaat DigiNotar uit de volgende afdelingen:

- *Sales & Marketing*
  Deze afdeling heeft vaak het eerste contact met potentiële klanten en onderhoudt ook de relaties. Indien de klant een maatwerk oplossing nodig heeft, dan wordt de hulp ingeroepen van een consultant. Tevens verzorgt S&M de publiciteit naar buiten toe.

- *Service centrum*
  Op het service centrum worden de certificaataanvragen gecontroleerd en uitgegeven. Het SC is de 'productiefabriek' van DigiNotar, omdat het eindproduct van DigiNotar het digitale certificaat is.
- *IT operationeel*
  Hieronder vallen alle diverse taken die thuishoren bij een IT-afdeling, zoals systeembeheer en dergelijke.
- *IT software development*
  Deze afdeling biedt ondersteuning bij projecten. Hier wordt software ontwikkeld die nodig is voor het implementeren van PKI in een toepassing. Tevens is er nog een designer in dienst, die onder andere de internetpagina onderhoudt.
- *Product ontwikkeling*
  Hier worden nieuwe producten voor DigiNotar ontwikkeld.
- *Financieel*
- *Secretariaat*
- *Directie*

1.3 Doel

In de inleiding heb ik beschreven dat vertrouwen een belangrijke factor is bij de doorbraak van mobile commerce. Dit vertrouwen wordt in de vaste wereld gewaarborgd door een Trusted Third Party. Het doel van mijn onderzoek is onderzoeken wat de specifieke betrouwbaarheidseisen zijn die de gebruiker aan m-commerce stelt en dan nagaan of en hoe een Trusted Third Party aan deze betrouwbaarheidseisen kan voldoen. De voorlopige definitie van een TTP die ik in dit onderzoek zal gebruiken luidt als volgt:

"*Een Trusted Third Party is een onafhankelijke en onpartijdige organisatie die vertrouwensdiensten levert voor het realiseren van elektronische data communicatie*." (Duthler 1998)

Het doel wat zojuist gedefinieerd is, wil ik bereiken voor de B2B en B2E mobile commerce markt. Onder B2E m-commerce wordt Business to Employee verstaan. Dit is de mobiele communicatie tussen werknemer en werkgever, zoals het lezen van mail of het benaderen van het bedrijfsintranet.

1.4 Probleemstelling

Op basis van de doelstelling van het onderzoek en de inleiding kom ik tot de volgende probleemstelling:

"Welke rol heeft een Trusted Third Party bij het bevorderen van het vertrouwen en de veiligheid bij het realiseren van mobiele transacties voor B2B en B2E m-commerce en hoe kan een TTP invulling geven aan deze rol?"

Om tot een antwoord te komen op de probleemstelling is het noodzakelijk om deze onder te verdelen in een aantal onderzoeksvragen die afzonderlijk behandeld en beantwoord zullen worden. De onderzoeksvragen luiden als volgt:

- Wat zijn de mogelijkheden van m-commerce?
- Welke stakeholders zijn er te onderscheiden bij m-commerce?
- Welke betrouwbaarheidseisen worden er aan een mobiele transactie gesteld?
- Welke technieken en diensten zijn er in de vaste wereld mogelijk om aan de betrouwbaarheidseisen te voldoen zoals die uit de vorige onderzoeksvraag naar voren zijn gekomen?
- Wat zijn de uitdagingen als de technieken en diensten uit bovenstaande onderzoeksvraag gebruikt gaan worden in de mobiele wereld?
- Wat wordt de rolverdeling tussen de verschillende partijen in de betrouwbaarheidsmarkt voor mobile commerce?
- Hoe moet de TTP haar gehele PKI-platform, zoals de interne processen en de processen richting de betrokken partijen bij mobiele identiteit, inrichten om op basis van de rolverdeling mobiele identiteit te leveren?

Op basis van de laatste twee onderzoeksvragen, ontwikkel ik een model waarin deze twee vragen beantwoord worden. Het model dient ter ondersteuning voor het beantwoorden van de probleemstelling. Het ontwikkelen van het model is dus geen doel op zich van dit onderzoek.

1.5 Aannames en afbakening voorafgaande aan het onderzoek

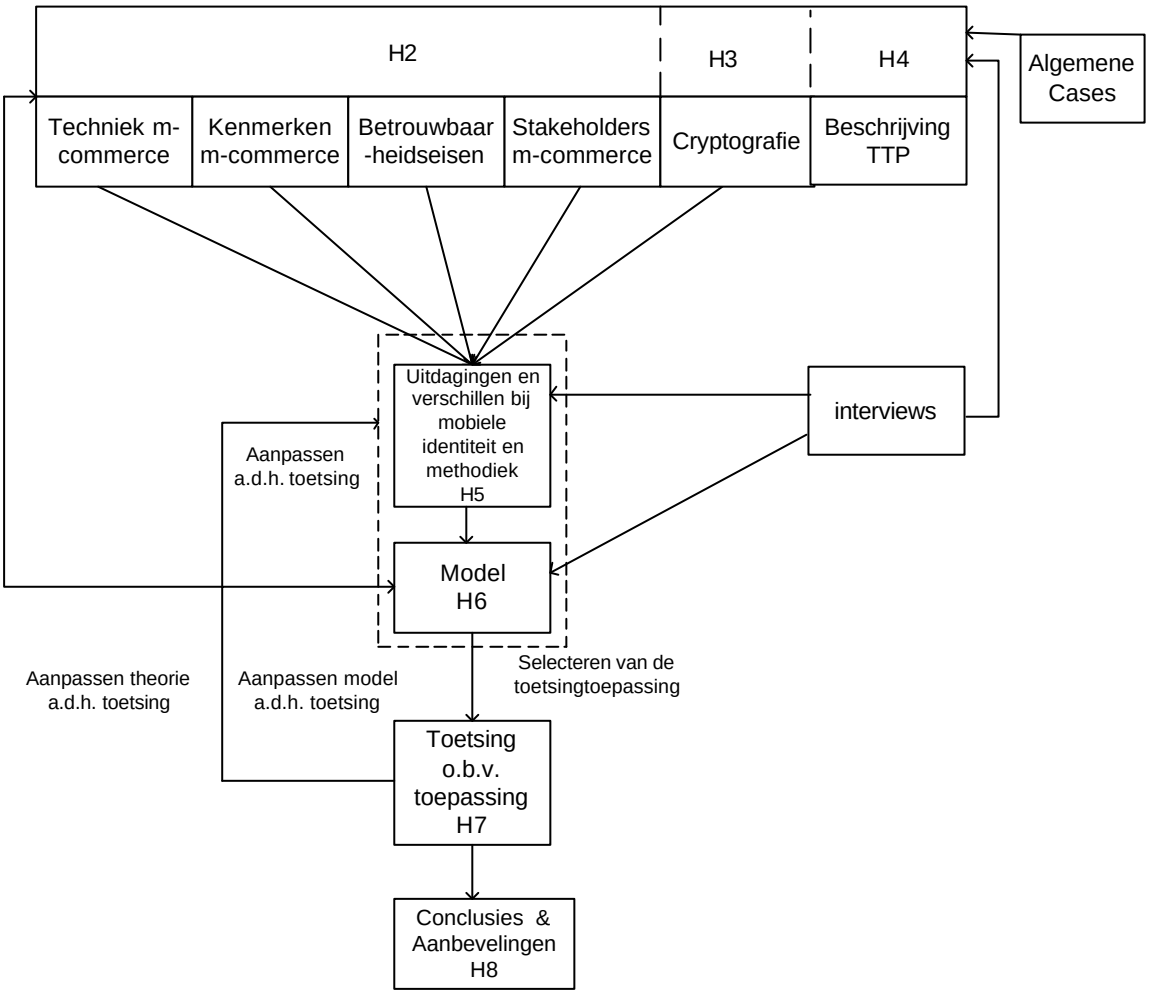
Voordat ik met het onderzoek van start ga, heb ik de volgende aannames gemaakt die van belang zijn voor het verdere verloop van het onderzoek.

- In dit onderzoek wordt onder een transactie niet alleen een financiële transactie verstaan, maar ook een transactie zonder directe financiële waarde. Tijdens een transactie kan bijvoorbeeld ook zeer vertrouwelijke informatie worden uitgewisseld.
- De tweede aanname is dat ik heb gekozen voor B2B en B2E m-commerce. Deze keuze heb ik gemaakt omdat bij zakelijke transacties de waarde van de transactie vaak hoger zal liggen dan bij een consument die met zijn mobiele apparaat een CD of een boek op het internet koopt. De zakelijke gebruiker zal een hogere mate van vertrouwen eisen voor zijn transactie en ik wil tot een oplossing komen die een zo hoog mogelijke betrouwbaarheid biedt, dus vandaar mijn keuze voor de zakelijke markt. Tevens leert de ervaring dat de consumentenmarkt in de vaste wereld nog geen behoefte heeft aan de huidige TTP-diensten, dus waarom wel in de mobiele wereld?
- De derde aanname is een afbakening van het begrip vertrouwen. Vertrouwen kan natuurlijk verschillende betekenissen hebben voor een consument. Bijvoorbeeld het vertrouwen dat een consument in een leverancier heeft dat bestelde goederen ook daadwerkelijk geleverd worden. Dit onderzoek richt zich echter op het verhogen van het vertrouwen van een transactie op basis van de punten in paragraaf 1.1. Het gaat hierbij dan onder andere om het authenticeren en identificeren van de verschillende partijen en het rechtsgeldig afsluiten van transacties en dus niet om het verhogen van het vertrouwen in de betrouwbaarheid van de verschillende partijen over bijvoorbeeld de kwaliteit van de geleverde diensten.

1.6 Onderzoeksmethode

Om tot een goede theoretische onderbouwing van het eindresultaat te komen is het noodzakelijk om eerst een goed literatuuronderzoek uit te voeren. Om meer kennis te krijgen over het onderwerp wordt deze literatuurstudie uitgebreid met een aantal

interviews met deskundigen op de diverse deelgebieden. Deze deskundigen zullen geselecteerd worden uit de nog nader te definiëren stakeholders bij mobile commerce. Deze interviews zijn uitgewerkt in de bijlage. In de bijlage zijn ook een aantal mobile commerce cases bijgevoegd. Deze cases dienen ter verduidelijking voor de lezer om een beter beeld te krijgen van wat de mogelijkheden van mobile commerce zijn. Deze cases zijn ook als input gebruikt voor de theorie, maar worden niet afzonderlijk behandeld.
Nadat het theoretisch kader helemaal duidelijk is en de uitdagingen en verschillen bij het leveren van mobiele identiteit geïdentificeerd zijn, kan er begonnen worden met het ontwikkelen van het model. Wanneer het model ontwikkeld is, moet het model natuurlijk ook getoetst worden. Deze toetsing zal waarschijnlijk uitgevoerd worden in samenwerking met een relatie van DigiNotar. Na deze toetsing wordt het model indien nodig aangepast.
Na al deze stappen, in figuur 1.2 schematisch weergegeven, kan het onderzoek worden afgerond en hoop ik een antwoord te hebben gevonden op de onderzoeksvragen en de probleemstelling.



Figuur 1.2 Schematische weergave van de onderzoeksopzet

Hoofdstuk 2: Theoretisch kader mobile commerce

2.1 Inleiding

In dit hoofdstuk zal ik uitleggen wat mobile commerce is en wat de technieken achter m-commerce zijn. Bij de technieken heb ik een onderscheid gemaakt naar netwerktechnologieën, communicatieprotocollen, besturingssystemen, browsers en mobiele apparaten. De onderscheidende kenmerken van m-commerce zullen daarna behandeld worden en dan komt men vanzelfsprekend terecht bij de beperkingen van m-commerce ten opzichte van e-commerce. Vervolgens zullen de betrouwbaarheidseisen die aan m-commerce gesteld worden aan bod komen. Tenslotte zullen de diverse stakeholders betrokken bij mobile commerce besproken worden en zal aan de Trusted Third Party een plaats in de waardeketen worden toegewezen.

2.2 Techniek mobile commerce

2.2.1 Netwerktechnologie

Er zijn op dit moment een aantal netwerktechnologieën voor mobiele communicatie beschikbaar en in ontwikkeling. Dit zijn Global System for Mobile Communication, High Speed Circuit Switched Data, General Packet Radio Services, Enhanced Data Rates for Global Evolution en Universal Mobile Telephone System.

Global System for Mobile Communication

GSM is op dit moment de meest voorkomende standaard voor mobiele communicatie in Europa, Azië en de Pacific. GSM werkt in deze regio's via de 900 Mhz en 1800 Mhz frequentieband. In Amerika wordt er gebruik gemaakt van de 1900 Mhz band. GSM is een tweede generatie netwerk, een zogenaamd 2G netwerk. Het 1G netwerk is een voorloper van GSM. Deze generatie wordt hier niet behandeld, aangezien die nauwelijks meer gebruikt wordt. Wereldwijd zijn er nu 215 miljoen GSM-gebruikers (Durlacher, 1999), dit is meer dan 50% van de mobiele markt. Dit is het grote voordeel van GSM, veel mensen beschikken over een GSM toestel en softwareontwikkelaars zullen hun applicaties dus geschikt moeten maken voor gebruik over het GSM netwerk.
GSM maakt gebruik van de Time Division Multiple Acces techniek, deze techniek is gebaseerd op een circuit switched netwerk. Een nadeel van deze techniek is dat het eigenlijk te traag is voor mobiele internettoepassingen, de snelheid waarmee data verstuurd kan worden is 9,6 Kbit/s. Ter vergelijking een breedband internetverbinding werkt met een snelheid van ongeveer één Megabit/s, dit is ongeveer honderd maal zo snel. Het GSM netwerk is dus niet geschikt voor het versturen van grote bestanden. Een ander nadeel van een circuit switched netwerk is dat gebruiker betaalt per tijdseenheid dat hij online is. Met GSM moet men dus steeds een nieuwe verbinding met het internet maken, wat een tijdrovende bezigheid is.

High Speed Circuit Switched Data

HSCD is een techniek die op GSM gebaseerd is. Bij GSM heeft een gebruiker de beschikking over één radiokanaal, terwijl bij HSCD de gebruiker maximaal de beschikking heeft over vier radiokanalen en de snelheid dus ook vier keer zo hoog kan zijn ten opzichte van GSM. De snelheid die in theorie te behalen valt is 57,6 Kbit/s,

hierbij moeten dan wel alle vier de kanalen gebruikt worden, wat ook weer extra kosten met zich meebrengt.
Een groot nadeel van HSCD is dat deze techniek nauwelijks door mobiele operators ondersteund wordt. Ook de hardwarefabrikanten ondersteunen HSCD slechts mondjesmaat. De verwachting is dan ook dat HSCD slechts een interim technologie is totdat GPRS beschikbaar is (Durlacher, 1999).

General Packet Radio Services

GPRS, een 2,5G netwerk, is een technologie gebaseerd op packet switching. Door gebruik te maken van packet switching worden de resources van het radiokanaal efficiënter benut dan bij circuit switching. Het kanaal wordt alleen bezet gehouden door de gebruiker indien hij ook daadwerkelijk data aan het verzenden of ontvangen is. Met GPRS is het nu mogelijk om de gebruiker per verstuurde data-eenheid te laten betalen. Het grote voordeel hiervan is dat een gebruiker nu altijd online kan zijn, zonder dat dit veel geld gaat kosten. Men hoeft niet iedere keer een nieuwe verbinding te maken, zoals dat bij GSM het geval is.
De snelheden die je met GPRS kunt behalen liggen ook veel hoger dan bij GSM. In het begin sprak men over 171 Kbit/s, maar gezien de huidige ontwikkeling is het echter realistischer om voorlopig uit te gaan van 43 Kbit/s. In de toekomst zal misschien de beloofde snelheid van 171 Kbit/s behaald worden. GPRS is door de hoge snelheid veel beter geschikt dan GSM om het internet te benaderen.
GPRS kan met een paar aanpassingen aan het GSM netwerk gewoon gebruik maken van dit netwerk en er hoeft dus geen totaal nieuw netwerk te worden aangelegd zoals dat bij UMTS het geval is. Dit scheelt gigantisch in kosten en tijd. Op dit moment is GPRS nog niet op grote schaal beschikbaar, de netwerken moeten nog worden aangepast en een andere belangrijke voorwaarde is dat er ook apparaten op de markt zijn die gebruik kunnen maken van het GPRS netwerk. De verwachting is dat tegen het midden/einde van 2001 er een aantal GPRS toestellen te koop zijn (www.ericsson.com, www.nokia.com). Als aan deze twee voorwaarden is voldaan, kan GPRS pas echt doorbreken en zullen er applicaties beschikbaar komen voor GPRS.

Enhanced Data Rates for Global Evolution

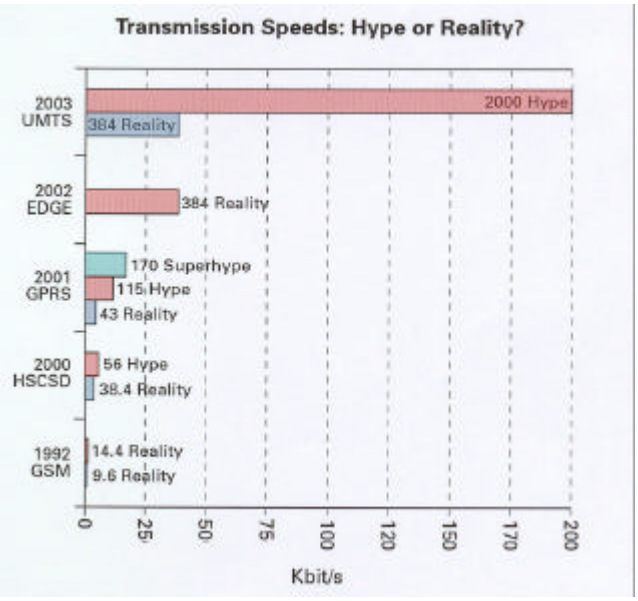
EDGE is een uitbreiding op GPRS, het is eigenlijk GPRS met een hogere bandbreedte. Middels EDGE kan er een realistische transmissiesnelheid van 384 Kbit/s behaald worden. De verwachting is dat EDGE in de loop van 2002 beschikbaar zal zijn. EDGE zal de overgang van GPRS naar het hieronder nog te bespreken UMTS versoepelen. Een aantal aanpassingen die nodig zijn voor EDGE, zijn namelijk ook noodzakelijk voor UMTS. Het succes van EDGE zal in hoge mate afhangen van de beschikbaarheid van applicaties en apparaten. Deze moeten snel beschikbaar zijn, omdat de levensduur van EDGE waarschijnlijk erg kort is, omdat UMTS snel na de introductie van EDGE beschikbaar zal zijn. Het succes van EDGE is dus ook deels afhankelijk van de ontwikkelingen van de UMTS technologie.

Universal Mobile Telephone System

UMTS is een zogenaamd 3G mobiel netwerk. UMTS is de 3G standaard voor Europa, in andere werelddelen zijn weer iets andere, maar vergelijkbare standaarden van toepassing. Om harmonisatie van deze standaarden te bereiken heeft de internationale

telecommunicatie unie (ITU) alle 3G standaarden opgenomen in de IMT-2000. De verwachting is dat UMTS vanaf 2003 in Europa beschikbaar zal zijn.
UMTS maakt gebruik van Frequency Division Duplex en Time Division Duplex, het combineert dus de beschikbare technologieën waarop de eerder besproken standaarden gebaseerd zijn.
In het begin is UMTS gepromoot als een technologie waarmee transmissiesnelheden van 2 Mbit/s gehaald kan worden. Dit is voorlopig geen realistische snelheid, deze snelheid zal naar verwachting pas in 2005 gehaald worden. De snelheid die voorlopig behaald zal worden is 384 Kbit/s. Dit is even hoog als bij EDGE, dit is ook de reden waarom sommige telecomoperators nu hun strategie op het gebied van UMTS aan het herzien zijn. Onderzoeksbureau Durlacher verwacht wel dat UMTS door zal breken, omdat het GSM-netwerk (waar GPRS/EDGE gebruik van maken) dicht zal slibben door het stijgende mobiele verkeer. Dit is ook een gevaar dat voor UMTS geldt, omdat de gebruikers de bandbreedte met elkaar moeten delen. Dit is vergelijkbaar met kabelinternet, waar de snelheid ook van het aantal actieve gebruikers afhangt.

In onderstaand figuur is goed zichtbaar dat de reële snelheden een stuk lager liggen dan de in eerste instantie verwachte snelheden. Vooral bij UMTS is dit verschil enorm.



Figuur 2.1 Ontwikkeling netwerktechnologieën en transmissiesnelheden, bron: Durlacher, 1999

Voor- en nadelen netwerktechnologieën

Technologie	Voordelen	Nadelen
GSM	• Zeer hoge penetratiegraad	• Traag • Betalen per tijdseenheid
HSCD	• Sneller dan GSM • Maakt gebruik van bestaand GSM netwerk	• Weinig ondersteuning • Betalen per tijdseenheid
GPRS	• Hoge snelheid • Betalen per data-eenheid • Kleine aanpassing nodig aan GSM netwerk	• Overhyped • Doorbraak UMTS
EDGE	• Voordelen GPRS • Hogere snelheid	• Doorbraak UMTS
UMTS	• Zeer hoge snelheid mogelijk • Betalen per data-eenheid	• Nieuw netwerk nodig • 2 Mbit/s pas in 2005 haalbaar

Tabel 2.1 Voor- en nadelen netwerktechnologieën

Bluetooth en Wireless Fidelity (WiFi)

Heel andere netwerktechnieken dan de hierboven besproken technieken zijn Bluetooth en WiFi. De eerder genoemde technieken zijn bedoeld voor lange afstandscommunicatie, terwijl Bluetooth en WiFi bedoelt zijn als communicatietechniek voor korte afstand. Bluetooth richt zich hierbij meer op de draadloze communicatie tussen apparaten onderling en WiFi wordt gebruikt om draadloos toegang te krijgen tot Local Area Networks. Er zijn op dit moment nog weinig toestellen die Bluetooth en/of WiFi ondersteunen en evenals bij GPRS, zullen deze toestellen waarschijnlijk rond midden/eind 2001 op de markt komen. Deze technieken hebben geen extra invloed op de betrouwbaarheid en beveiliging van de mobiele communicatie.

2.2.2 Protocollen

Een protocol bestaat uit een aantal regels die gebruikt worden door eindpunten in een telecommunicatieverbinding om met elkaar te communiceren (www.whatis.com, 2001). Bij vast internet maakt men gebruik van het TCP/IP protocol. Dit protocol is echter niet geschikt voor een mobiele benadering van het internet, omdat op dit moment de capaciteit van de mobiele technologie te laag is om het internet op de standaardwijze te benaderen. Er zijn hiervoor verschillende nieuwe protocollen ontwikkeld, de meest gebruikte zijn de SIM Application Toolkit en het Wireless Application Protocol. Een nieuw protocol dat nu in ontwikkeling is het Mobile Station Application Execution Environment. Deze drie protocollen worden achtereenvolgens behandeld in deze paragraaf.

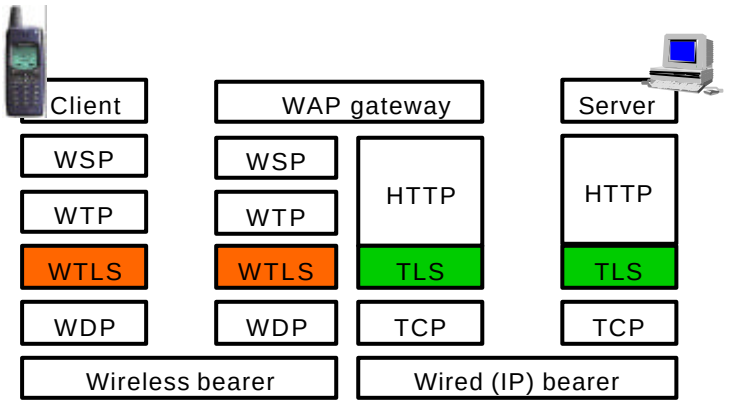
SIM Application Toolkit

Met SAT worden applicaties via SMS of cell broadcast naar de SIM-kaart van de gebruiker gestuurd. De Subscriber Identity Module is een kaart die in iedere mobiele telefoon zit en waar persoonlijke gegevens van de gebruiker opstaan. De applicaties staan dus op de SIM-kaart. Om van een toepassing gebruik te kunnen maken moet eerst de benodigde applicatie door de netwerk provider naar de SIM-kaart gestuurd worden. Er is dan eigenlijk een één op één relatie met de leverancier. SAT leent zich dus uitstekend voor statische toepassingen, maar voor dynamische toepassing zoals

webbrowsing is SAT niet geschikt. Een groot voordeel van SAT is dat het veel veiliger is dan het nog te bespreken WAP en uitermate geschikt is voor toepassingen die een hoge veiligheid eisen, mobiel bankieren bijvoorbeeld. Een ander pluspunt van SAT is dat het in de GSM standaard is opgenomen en dus door bijna alle netwerk providers ondersteund wordt. Het grote voordeel van SAT tegenover de andere technieken is dat SAT al enige tijd op de markt is en de andere technieken nog grotendeels in de kinderschoenen staan en hun kritieke massa nog moeten bereiken. SAT is ontwikkeld door smartcard fabrikanten (onder andere Gemplus en Giesecke & Devrient) en is gebaseerd op de GSM technologie.
Een voorbeeld van een toepassing die van dit protocol gebruik maakt, is de toepassing voor mobiel bankieren van de Postbank en Telfort. Voor deze toepassing is echter wel een aangepaste telefoon nodig en op dit moment leveren de Postbank en Telfort alleen een Siemens-telefoon, deze telefoon is geschikt gemaakt voor de bancaire toepassing. Deze toepassing is eigenlijk een soort combinatie van WAP en SAT.

Wireless Application Protocol

Het wireless application protocol is ontwikkeld door de grote hardwarefabrikanten zoals Nokia, Ericsson en Motorola, die zich verenigd hebben in het WAPforum (www.wapforum.org). Inmiddels hebben veel partijen zich bij het WAPforum aangesloten en dit is ook meteen een groot voordeel van WAP. De standaard wordt door veel organisaties ondersteunt en WAP heeft dus de kans om *de* open standaard voor mobiele datacommunicatie te worden.
WAP is ontwikkeld omdat de capaciteit van de mobiele technologie te laag is om het internet op de gebruikelijke wijze via een mobiel apparaat te benaderen. De internetpagina's moeten aangepast worden voor mobiel gebruik. Via een WAP gateway worden de standaard internetprotocollen geconverteerd naar protocollen die geschikt zijn voor mobiel gebruik. Bij WAP bijvoorbeeld is WML het equivalent van HTML en die twee moeten geconverteerd worden voor de onderlinge communicatie, hetzelfde geldt voor WTP en http.



Figuur 2.2 WAP netwerk architectuur, bron: Ericsson, 2001

De gekleurde laag in het figuur is de beveiligingslaag. De gateway converteert WTLS naar TLS/SSL. Hier wordt de beveiliging onderbroken en is de informatie zeer korte tijd leesbaar. Doordat men gebruik moet maken van de gateway wordt er geen end-to-end security geleverd. De oplossingen om de informatie toch veilig van cliënt naar server te sturen, worden in hoofdstuk zes beschreven.

Het wireless application protocol is ontwikkeld als een open standaard. Dat wil zeggen dat het protocol apparaatonafhankelijk is en dus met ieder apparaat gebruikt kan worden. Tevens is WAP compatible met de verschillende netwerktechnologieën zoals GSM, GPRS en UMTS. Deze doelen kunnen alleen bereikt worden omdat de standaard door zeer veel organisaties uit de wereld ondersteund wordt. Het WAPforum blijft ook steeds nieuwe versies van de standaard ontwikkelen. Zo zal bijvoorbeeld WAP 2.0 ook SAT ondersteunen en biedt versie 2.0 ook betere beveiligingsmogelijkheden middels een WPKI, waarover ik later meer zal uitleggen.
Wanneer de nieuwe netwerktechnieken beschikbaar zijn, kan de gebruiker via WAP steeds beter het internet op de gebruikelijke manier benaderen, hoewel er nog steeds beperkingen zullen zijn ten opzichte van vast internet.

Mobile station application EXecution Environment

MExE 'bouwt' een Java Virtual Machine in het mobiele apparaat. Java is de "write once run anywhere" programmeertaal (S. Buckingham, Futurefonezone.com). MExE heeft een aantal overeenkomsten met WAP, beide protocollen zijn met alle netwerktechnologieën compatible en maken het mogelijk om met dynamische toepassingen te werken. Omdat MExE 'full application execution environment' toelaat is het erg belangrijk dat MExE ook zeer goed beveiligd is om ongeautoriseerde toegang van buitenaf tot de gebruikersdata tegen te gaan.
De MExE standaard is opgebouwd uit een aantal klasses, iedere klasse heeft weer andere meer uitgebreide mogelijkheden. Het is niet vanzelfsprekend dat alle klasses naar beneden toe compatible zijn, dit moet voor elke klasse opnieuw bekeken en gedefinieerd worden. Het is wel zo dat hogere klasses meer mogelijkheden hebben. De mobiele apparaten die MExE ondersteunen zullen ook in klassen moeten worden ingedeeld. Als je met je mobiele apparaat contact maakt met een MExE-server worden de klasses automatisch aan elkaar bekend gemaakt en zodoende wordt bepaald van welke toepassingen men gebruik kan maken.
Om alle nieuwe mogelijkheden die MExE biedt ten opzichte van de overige protocollen te benutten, is het noodzakelijk dat er gebruik wordt gemaakt van apparaten met een grotere rekencapaciteit dan de huidige apparaten en dat er de beschikking is over een hoge bandbreedte. Daarom zal het nog wel even duren voordat MExE door zal breken en WAP eventueel kan gaan vervangen

Voor- en nadelen protocollen

Voor het slagen van ieder protocol is het belangrijk dat het protocol aan de volgende eisen voldoet.

- Er moeten voldoende apparaten op de markt zijn die het protocol ondersteunen.
- Er moeten voldoende applicaties voor het protocol beschikbaar zijn en deze applicaties moeten toegevoegde waarde hebben.

Alle protocollen zijn op een client-server architectuur gebaseerd en hebben enige overlap met elkaar. Zo zal WAP 2.0 ook het SAT protocol bevatten en zal WAP op haar beurt weer worden opgenomen is het MExE protocol.
Waarschijnlijk zal er in de nabije toekomst niet één protocol bestaan aangezien de markt zich blijft ontwikkelen en er steeds nieuwe protocollen ontwikkeld zullen worden. Softwareontwikkelaars en aanbieders van informatiediensten voor mobiele gebruikers zullen hun toepassingen voorlopig dus geschikt moeten maken voor meerdere protocollen.

Protocol	Voordelen	Nadelen
SAT	• Op GSM gebaseerd • Is al breed beschikbaar • Veilig	• Statisch • Downloaden applicatie • Netwerkprovider heeft toegang tot SIM-kaart
WAP	• Dynamisch • Breed draagvlak	• Traag over GSM • Overhyped • Beveiligingsproblemen
MExE	• JAVA VM • Compatible met WAP • Device onafhankelijk	• Hoge eisen aan device • Nog in kinderschoenen • Functioneert het beste met UMTS

Tabel 2.2 Voor- en nadelen protocollen

2.2.3 Besturingssysteem/ Operating system

Op dit moment is het besturingssysteem voor het mobiele apparaat nog niet gestandaardiseerd en is er een strijd gaande tussen de diverse fabrikanten om het systeem te leveren dat de standaard zal worden. De drie bedrijven die de grootste rol spelen in deze markt zijn: Microsoft, Symbian en 3COM. Het succes van de besturingssystemen zal in hoge mate afhangen van de keuze van het besturingssysteem door de hardware en software fabrikanten. Het besturingssysteem dat het meeste ondersteund wordt door de content providers en applicatie ontwikkelaars, zal uiteindelijk de standaard gaan worden. Dit is te vergelijken met wat er op de PC markt gebeurd is tussen Windows en OS/2, het besturingssysteem van IBM.

Microsoft Pocket PC
Pocket PC is een lichtere versie van de PC versie van Windows. Pocket PC is voornamelijk ontwikkeld voor gebruik op kleine hand held computers en personal digital assistants. Pocket PC bevat een onderdeel van de WIN32 applicatie programmeer interface (API) dat door softwareontwikkelaars wordt gebruikt om applicaties voor de PC te ontwikkelen. Dit betekent dat de ontwikkelaars geen nieuwe taal hoeven te gebruiken om applicaties voor Pocket PC te ontwikkelen en dit is natuurlijk een groot voordeel voor Pocket PC.

Symbian Epoc
Symbian is een consortium opgericht in 1998 door onder andere: Nokia, Ericsson en Psion. Het besturingssysteem dat Symbian ontwikkeld heeft heet Epoc en is gebaseerd op het besturingssysteem voor de Psion. Epoc richt zich op twee soorten draadloze apparaten. De smartphones, dit zijn mobiele toestellen met een PC connectie, voorbeelden hiervan zijn: Nokia 7110, Ericsson R380s. De andere soort is de communicator met een connectie voor of een ingebouwde mobiele telefoon, een voorbeeld hiervan is de Nokia Communicator 9210.

3COM
3COM is de kleinste speler in de markt voor besturingssystemen voor mobiele apparaten, echter in de Personal Digital Assistant (PDA) markt is 3COM de belangrijkste speler. 3COM fabriceert de welbekende Palm en levert hier ook het besturingssysteem voor. Het besturingssysteem is inferieur aan de overige systemen, maar is toch succesvol doordat de Palm zelf uitblinkt in bedieningsgemak en software. Inmiddels werken 3COM en Symbian samen om de twee besturingssystemen te combineren.

2.2.4 Mobiele browsers

Een mobiele browser is noodzakelijk om het internet te benaderen. Een mobiele browser wordt vaak een microbrowser genoemd. De browser is in de telefoon zelf geïntegreerd of staat op de SIM. Phone.com is marktleider op het gebied van de microbrowsers. Haar UP.Browser mag door 90% van de mobiele fabrikanten gratis gebruikt worden, alleen Nokia en Ericsson zijn hierop een uitzondering. Zij gebruiken hun eigen browsers. Microsoft heeft voor Pocket PC ook een microbrowser ontwikkeld. Een aantal smartcardfabrikanten hebben hun eigen browsers ontwikkeld, deze zijn veelal bedoeld voor de SIM Application Toolkit. Verder zijn er nog een aantal kleine spelers die microbrowsers leveren.

2.2.5 Mobiele apparaten

Wanneer er over mobile commerce wordt gepraat, denkt men vaak direct aan een mobiele telefoon. Er is echter een grote variëteit aan mobiele apparaten op de markt, die ieder weer verschillende segmenten in de markt als doelgroep hebben. Daarom zal er ook geen universeel apparaat op de markt komen dat dienst zal gaan doen als *het* apparaat dat zal voldoen aan de eisen van de alle verschillende gebruikers. Onderzoeksbureau Durlacher Ltd maakt een onderscheid in vier categorieën.

1. *Mobiele telefoon:* De huidige mobiele telefoon zoals die nu op de markt met als hoofdfuncties spraak en SMS.
2. *Smartphone:* Een mobiele telefoon met applicaties en PC connectie (WAP). Voorbeelden van de smartphone zijn de Nokia 7110 en de Ericsson R380
3. *Communicator:* Een Personal Digital Assistant geïntegreerd met een mobiele telefoon. Een communicator is geschikt voor data- en spraakverkeer. Voorbeelden hiervan zijn de Nokia Communicator 9210 en de Ericsson Mobile Companion MC218.
4. *De laptop PC:* In deze categorie vallen alle sub-notebooks. Een notebook kan via een mobiel netwerk contact maken met het internet. Deze apparaten worden steeds kleiner en lichter, het onderscheid met de high-end PDA wordt dan ook kleiner, maar is nog steeds aanzienlijk. Een voorbeeld van zo'n notebook is de Sony Vaio.

Een mobiel apparaat bestaat uit een aantal componenten die bepalend zijn voor de functionaliteit en mogelijkheden die het apparaat kan bieden. De componenten die het meest bepalend zijn, staan hieronder beschreven.

- *Scherm*
  Het beeldscherm van het mobiele apparaat is in hoge mate bepalend voor de mogelijkheden van het apparaat. De huidige PC gebruiker is een groot scherm gewend met veel kleuren en een hoge resolutie, terwijl dit op dit moment nog niet mogelijk is voor een mobiel apparaat. Een mobiel apparaat zal niet zo'n groot scherm hebben als een normale monitor, simpelweg om de reden dat het apparaat dan niet meer mobiel zal zijn. De mobiele industrie is nu hard aan het werk om de andere twee eigenschappen van een normale monitor ook geschikt te maken voor een mobiel apparaat. Zo heeft Nokia nu een behoorlijk goed kleurenscherm ontwikkeld voor de Communicator 9210. De grootte van het scherm is afhankelijk van het soort apparaat zoals hierboven gedefinieerd, zo beschikt een communicator over een groter scherm dan een smartphone.

- *Geheugencapaciteit*
  Net als bij een gewone PC speelt het geheugen bij een mobiel apparaat ook een belangrijke rol bij de performance van het apparaat. Hoe meer geheugen het apparaat heeft, hoe beter de prestaties zullen zijn en de mogelijkheden die het apparaat biedt qua applicaties en dergelijke zullen ook toenemen met een groter geheugen.
  De mobiele apparaten die geschikt zijn voor mobile commerce zijn nu meestal uitgerust met flash geheugen, dit geheugen is op dit moment nog behoorlijk duur, $100 voor 32 MB. Dit is de reden waarom de apparaten tot nu toe zijn uitgerust met een klein geheugen.
- *Central Processing Unit*
  De nieuwe toepassingen vragen ook steeds meer processorkracht, de processoren die in de huidige generatie mobiele apparaten zitten, zijn nog niet krachtig genoeg om aan deze eisen te voldoen. Op korte termijn zullen er volgens de hardware fabrikanten echter apparaten verschijnen met nieuwe krachtigere processoren die wel toereikend zullen zijn voor de nieuwe applicaties.
- *Capaciteit batterij*
  De capaciteit van de batterij is een belangrijke eigenschap van het mobiele apparaat. Deze capaciteit bepaalt hoelang de gebruiker zijn mobiele apparaat kan gebruiken zonder dat deze opgeladen moet worden en bepaalt dus hoelang de gebruiker mobiel kan zijn.
  Het scherm, geheugen en de processor verbruiken veel stroom en plegen dus een zware aanslag op de batterij. Om de stand-by tijd van de batterij te verlengen is het noodzakelijk om bovenstaande componenten zo te produceren dat ze een zo laag mogelijk stroomverbruik hebben. Hier kun je een vergelijking maken met de laptop, die een zelfde problematiek kent. Tevens is het van belang om een zo krachtig mogelijke batterij of accu te ontwikkelen die ook nog eens klein genoeg is om in een mobiel apparaat te passen.

2.3 Kenmerken mobile commerce ten opzichte van electronic commerce

2.3.1 Onderscheidende kenmerken mobile commerce

Mobile commerce moet niet gezien worden als een alternatief voor vast internet en men moet dus niet proberen vaste gebruikers los te weken naar mobiel internet. Je moet mensen iets bieden dat het vaste internet niet kan bieden, de applicatie moet duidelijk toegevoegde waarde hebben. Mobiel internet moet gezien worden als een uitbreiding op vast internet op basis van onderstaande onderscheidende kenmerken van het mobiele netwerk. Deze onderscheidende kenmerken worden in veel rapporten (Durlacher Mobile Commerce Report, 1999 en Wireless Applications for Business, Daitch/Kamath, 2001) iedere keer weer anders omschreven, maar zijn allemaal terug te voeren op de volgende kenmerken:

- *Anyplace*
  Anyplace houdt in dat de gebruiker niet gebonden is aan een vaste plaats met een vaste terminal van waaruit hij zijn data moet versturen. Middels de mobiele techniek kan de gebruiker vanuit iedere locatie toegang krijgen tot het internet. Hierbij moet men echter wel één beperking in het achterhoofd houden, namelijk dat het mobiele netwerk nog geen 100% dekking in de meeste landen heeft. In de Westerse wereld hebben de 2G mobiele netwerken nu een dekking van 90% (Oasis Technology, 2000).

- *Anytime*
  Anytime houdt in dat de gebruiker ieder moment van de dag de beschikking heeft over het internet en dus data kan versturen of ontvangen. Men is niet tijdgebonden. Deze eigenschap is zeer belangrijk indien de waarde van informatie afhankelijk is van het tijdstip van ontvangst. Je kunt hierbij denken aan de aandelenkoersen of communicatie tijdens ongevallen waar tijd een levensbepalende rol kan spelen.
- *Personalisatie*
  Het mobiele apparaat is een zogenaamd personal device. Met behulp van de SIM kaart kan er een persoonlijk profiel van de gebruiker worden samengesteld, waardoor een service provider gepersonaliseerde diensten aan de gebruiker kan aanbieden. Dit is zowel positief voor de gebruiker als de service provider. De gebruiker krijgt alleen informatie die nuttig voor hem is en de provider heeft een grotere kans dat zijn diensten worden afgenomen. Met vast internet zijn ook gepersonaliseerde diensten mogelijk doordat de gebruiker in moet loggen op een portal. Maar doordat het mobiele apparaat een personal device is, zijn de mogelijkheden qua personalisatie groter dan bij vast internet.
- *Locatie gebaseerde en pushdiensten*
  Door bovenstaande eigenschappen worden twee andere eigenschappen van mobile commerce mogelijk. Doordat de service provider in staat is te bepalen waar de gebruiker zich bevindt, kan deze diensten aanbieden die afhankelijk zijn van de locatie waar de gebruiker zich bevindt. Wanneer de dienstverlener weet wat de voorkeuren van de gebruiker zijn, kan deze informatie toesturen zonder dat de gebruiker daarom vraagt. Het grote voordeel hierbij is dat de gebruiker de informatie direct ziet en men niet hoeft te wachten totdat de gebruiker achter zijn computer zit. Dit wordt ook wel push-technologie genoemd.

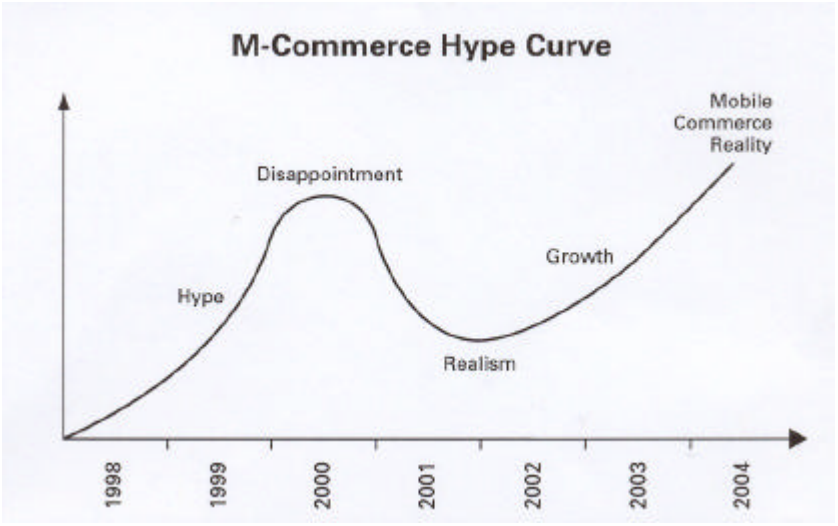
Anytime	**Anywhere**	**Locatie gebaseerd**
E-mail alert	Intranet access	Traffic conditions
Fax alert	Transport schedules	Weather details
Stock details	Dealing in shares	Transport schedules
News headlines	Altering travel arrangements	Navigation
	Vertical support for sales staff	Entertainment/ dining details
	Banking	
	Unified messaging	
	Entertainment booking	
	Internet access	

Tabel 2.3 Applicaties die gebruikmaken van unieke eigenschappen mobiel, Bron: ARC Group, 2001

2.3.2 Beperkingen mobile commerce

De gebruiker legt bij m-commerce minder nadruk op het surfen en browsen, maar zal een sterke focus hebben op het verrichten van een transactie (Oasis Technology, 2000). De verwachting die bij gebruikers van mobiel internet gewekt wordt, moet als gevolg van de beperkingen voor mobiel internet anders zijn dan bij vast internet, anders volgt er alleen maar teleurstelling bij de gebruiker. Bij de introductie van mobiel internet en WAP is echter de indruk naar de gebruiker toe gewekt dat mobiel internet wel een vervanging was van vast internet en dat men met mobiel internet minimaal dezelfde zoniet meer mogelijkheden zou hebben als met vast internet. Deze hype heeft tot een teleurstelling geleid. Nu komt de markt tot inkeer en vindt er rationalisering plaats over de mogelijkheden die mobile commerce biedt. Deze marktbeweging wordt in de

onderstaande curve weergegeven. De curve komt zeer goed overeen met wat er zich nu in de praktijk afspeelt.



Figuur 2.3 Mobile commerce hype curve, bron: Durlacher, 1999

De ARC groep verdeelt de beperkingen van mobile commerce in twee groepen.

Beperkingen veroorzaakt door het apparaat:

- Klein scherm met lage resolutie
- Beperkte invoermogelijkheden
- Minder krachtiger processor dan PC
- Minder geheugen dan PC

Beperkingen veroorzaakt door het netwerk:

- Beperkte bandbreedte.
- Hogere gebruikerskosten dan bij vast internet.
- Gevoeliger voor ruis tijdens het verzenden en grotere kans op uitvallen verbinding.

Overige beperkingen:

- De gebruikte protocollen zijn incompatible met de huidige internetstandaarden. WAP kan niet rechtstreeks communiceren met TCP/IP, WML moet bijvoorbeeld geconverteerd worden naar HTML en vice versa.
- Onvoorspelbaar: De bandbreedte is afhankelijk van het aantal gebruikers en men heeft dus niet de beschikking over een vaste bandbreedte en de dekking van het netwerk is ook niet altijd gegarandeerd.
- Beperkte capaciteit van de batterij.

Deze beperkingen betekenen dat de providers van draadloze diensten gedwongen worden om hun diensten in een simpele vorm aan te bieden en dat de mogelijkheden voor de gebruikers ook anders zullen zijn. Volgens onderzoeksbureau Forrester verlaagt iedere extra handeling die de gebruiker moet uitvoeren, het aantal transacties met 50%. Dit houdt dus in dat de applicatie niet meer handelingen dan nodig is, moet vergen van de gebruiker. Dit is vaak een lastig punt, omdat ontwikkelaars gewend zijn om zoveel

mogelijk functionaliteit in een applicatie te stoppen. Dit moet voor mobiele applicaties vermeden worden, omdat dit een averechtse werking heeft.

2.3.3 Kritische Succesfactoren

Een groot deel van de kritische succesfactoren (KSF) bij mobile commerce hangen samen met de beperkingen en onderscheidende kenmerken van mobile commerce. Het oplossen van de belangrijkste technologische beperkingen is dan ook een belangrijke KSF. Een belangrijke KSF voor mobile commerce is natuurlijk ook het ontwikkelen van de juiste applicatie. Ik zal hier niet in gaan op de inhoudelijke eigenschappen van de applicatie, maar op de functionele eisen waaraan een applicatie moet voldoen.
Een goede applicatie moet rekening houden met de beperkingen van mobile commerce en daar moeten de mogelijkheden op afgestemd zijn. Tevens moet de applicatie gebruik maken van de onderscheidende kenmerken van mobile commerce, de toepassing moet duidelijk toegevoegde waarde bieden ten opzichte van vast internet. Zoals al eerder gezegd moeten de toepassingen gezien worden als een toevoeging en niet als een vervanging.
Bij e-commerce speelt het gebrek aan vertrouwen dat de consument heeft in de beveiliging een grote rol. Dit gebrek aan vertrouwen verhinderd dat gebruikers massaal het internet opgaan om daar hun transacties te verrichten. Men kan dus veronderstellen dat veiligheid ook een belangrijke rol zal spelen bij de doorbraak van mobile commerce. (Yankee Group, 2000) De mate van betrouwbaarheid die geëist wordt is natuurlijk wel afhankelijk van de waarde en vertrouwelijkheid van de transactie.

KSF mobile commerce

- Oplossen belangrijkste technologische beperkingen.
- Ontwikkelen van applicaties die rekening houden met beperkingen.
- Ontwikkelen van applicaties die toegevoegde waarde voor de gebruiker hebben en gebruik maken van de onderscheidende kenmerken van mobile commerce.
- Oplossingen ontwikkelen om het vertrouwen van de gebruiker in mobile commerce te bevorderen en end-to-end beveiliging te realiseren.
- Beschikbaar komen van toestellen die geschikt zijn voor mobile commerce.
- Logistieke keten achter de mobiele handel moet in orde zijn, deze vereiste geldt ook voor e-commerce. Mobile commerce is een extra kanaal voor de dienstverlener die aan moet sluiten bij de overige kanalen en de back office. Een belangrijke factor is dus het op elkaar aan laten sluiten van de diverse kanalen en daarmee samenhangend de logistieke keten.

2.3.4 B2B m-commerce applicaties

Een breed scala aan bedrijfsprocessen kan gestroomlijnd worden met behulp van mobiele toepassingen. Middels de mobiele techniek en de bijbehorende kenmerken kunnen de processen dynamisch en real-time worden. De processen kunnen dus veel efficiënter worden uitgevoerd omdat de gebruiker de informatie mobiel kan benaderen. Hieronder worden een aantal toepassingen opgesomd die door onderzoeksbureau Durlacher gezien worden als toepassingen waarop m-commerce een belangrijke impact zal hebben.

- *Mobiele supply chain integratie*
  De integratie van de supply chain speelt in de vaste internetwereld ook een grote rol bij B2B e-commerce. Wanneer deze informatie tijdgevoelig is en de gebruikers

daarvan steeds vaker mobiel zijn, dan zal de mobiele techniek ook een grote rol gaan spelen in de supply chain integratie.

- *Telemetrie en sturing op afstand*
  Dit is vooral van belang bij het onderhoud van machines. In de machine zit dan een chip die de toestand van de machine bijhoudt en de informatie doorstuurt naar het servicebureau en vice versa. Bij machines die zich telkens op verschillende locaties bevinden is mobiel dus een goede oplossing. Deze toepassing heeft natuurlijk ook vele mogelijkheden in de auto-industrie. De fabrikant of de garage kan zo zeer nauwkeurig controleren of de auto nog naar behoren functioneert en of er onderhoud nodig is.
- *Mobiele service monteurs*
  Werknemers die voor hun werk de gehele dag mobiel zijn, kunnen met behulp van de applicatie geïnformeerd worden over de werkzaamheden die uitgevoerd moeten worden. Zo kan iemand van een reparatiedienst zijn opdrachten over zijn mobiele apparaat doorgestuurd krijgen als hij onderweg is.
- *Mobiele verkopers/ account managers*
  Vertegenwoordigers zitten natuurlijk het grootste gedeelte van de dag bij klanten of zijn aan het reizen. Voor deze groep is het dus ideaal als ze met hun mobiele apparaat het bedrijfsnetwerk kunnen benaderen en de laatste informatie over een klant kunnen uitwisselen met het hoofdkantoor. Dit levert niet alleen strategische voordelen op, maar ook behoorlijke efficiency-verbeteringen.

Voor een uitgebreide beschrijving van mogelijke applicaties die gebruik maken van de unieke eigenschappen die mobiel heeft, verwijs ik naar de bijlage waarin een aantal cases beschreven zijn. Deze toepassingen vergroten het inzicht in de mogelijkheden die mobile commerce biedt.

2.4 Betrouwbaarheidseisen bij mobile commerce

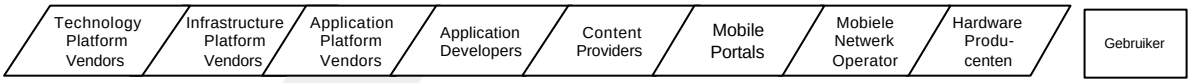
Zoals bij de KSF al is aangegeven, is het vertrouwen van de gebruiker erg belangrijk voor het doen slagen van een mobiele toepassing. De vier belangrijkste vereisten voor elektronische beveiliging waarmee het vertrouwen in een transactie gewaarborgd kan worden zijn (Leegwater, 1998):

- *Authenticatie*
  In plaats van alleen authenticatie wordt ook wel gesproken van identificatie en authenticatie. Deze twee houden sterk verband met elkaar. Identificatie heeft betrekking op de vraag “Wie bent u?” en authenticatie op de vraag “Kunt u bewijzen dat u degene bent die u zegt te zijn?” Volgens Ford en Baum (1997) is authenticatie de belangrijkste eis waaraan moet worden voldaan. Zonder een betrouwbaar authenticatieproces kan niet aan de overige eisen worden voldaan.
- *Integriteit*
  Onbevoegden mogen informatie niet wijzigen of vernietigen, noch meerdere malen verzenden.
- *Vertrouwelijkheid*
  Onbevoegden mogen informatie niet lezen. Dit wordt ook wel confidentialiteit of exclusiviteit genoemd en houdt in dat een bericht tijdens transport of opslag wordt beschermd tegen inzage door derden.
- *Onweerlegbaarheid*
  Verzending dan wel ontvangst van het bericht kunnen niet worden ontkend.

Er is geen reden om aan te nemen dat deze eisen voor mobile commerce anders zullen zijn dan bij electronic commerce. De eisen worden immers niet bepaald door het medium, want in beide gevallen is er geen direct face-to-face contact tussen de communicerende partijen. De betrouwbaarheidseisen worden bepaald door de waarde van de transactie, een mobile commerce transactie kan dezelfde betrouwbaarheidseisen hebben als een transactie bij electronic commerce. Men kan dus veronderstellen dat de betrouwbaarheidsdiensten geleverd door een Trusted Third Party aan dezelfde eisen moeten voldoen als de eisen die van toepassing zijn bij electronic commerce.
Aangezien er bij mobile commerce gebruik wordt gemaakt van een ander medium dan bij e-commerce is de invulling van deze eisen wel anders. Dit wordt veroorzaakt door de beperkingen van de mobiele techniek zoals eerder geschetst en de veranderende waardeketen bij m-commerce ten opzichte van e-commerce en mobiele telefonie. Wat de specifieke uitdagingen zijn bij het invullen van de betrouwbaarheidseisen wordt in hoofdstuk vijf besproken. Maar voor het zover is, worden in hoofdstuk drie en vier eerst de methoden besproken die gebruikt worden om e-commerce betrouwbaar te maken

2.5 Stakeholdersanalyse bij mobile commerce

In deze paragraaf zal ik de diverse betrokken partijen bij mobile commerce behandelen. Deze stakeholders zal ik behandelen aan de hand van de waardeketen bij mobile commerce zoals die gedefinieerd is in diverse onderzoeksrapporten van onder andere Durlacher Ltd en de Kellog TechVenture 2000 Anthology. In figuur 2.4 wordt de waardeketen weergegeven zoals die uit de diverse rapporten naar voren is gekomen.



Figuur 2.4 Stakeholders uit de mobile commerce waardeketen

2.5.1 Inventarisatie van de stakeholders bij mobile commerce

- *Technology Platform Vendors*
  Deze leveranciers leveren het besturingssysteem voor de diverse mobiele apparaten. De belangrijkste spelers zijn al behandeld bij het gedeelte over de besturingssystemen. Onder de leveranciers vallen ook de fabrikanten die de browsers leveren. Belangrijkste speler in deze markt is Phone.com, voorheen Unwired Planet.
- *Infrastructure Equipment Vendors*
  Deze partijen bouwen de infrastructuur voor de mobiele netwerken zoals bijvoorbeeld de nieuw aan te leggen UMTS infrastructuur. De leidende leveranciers in deze markt zijn: Motorola, Ericsson, Nokia, Siemens en Lucent.
- *Application Platform Vendors*
  Een belangrijke vereiste voor mobiel internet is de beschikbaarheid van de middleware, zoals de wireless application protocol gateways. Deze gateways kunnen zowel bij de mobiele operator als bij de contentprovider staan. De middleware maakt de mobiele applicaties mogelijk. Wederom zijn Nokia en Ericsson belangrijke spelers in deze markt.
- *Application Developers*
  Dit zijn de ondernemingen die zich bezig houden met het ontwikkelen van mobiele applicaties. Men kan hier een onderscheid maken naar applicaties ontwikkeld voor de diverse protocollen en besturingssystemen. In de Scandinavische landen zijn er

al redelijk wat applicaties ontwikkeld, dit in tegenstelling tot de overige West Europese landen. Dit zijn echter applicaties die geen betrouwbaarheid vereisen zoals in paragraaf 2.4 gedefinieerd is.

- *Content Providers*
  De traditionele informatieaanbieders breiden hun activiteiten nu naar mobiel uit. Hiervoor kiezen ze veelal verschillende distributiekanalen. De aanbieders zetten bijvoorbeeld hun eigen portal op en werken ook nog eens samen met diverse andere portals.
  Het in rekening brengen van de informatie blijft nog een probleem voor de aanbieders. De aanbieders kunnen meedelen in de belopbrengsten van de telecomoperator, maar aangezien alle opbrengsten in de toekomst gebaseerd zullen zijn op basis van de waarde van de informatie, zal dit opbrengstenmodel geen lang leven hebben. De opbrengst zal dan ook uit advertentie, sponsor en abonnementsgelden gehaald moeten worden.
- *Mobiele Portals*
  Mobiele portals worden gevormd door het samenvoegen van informatie en applicaties van diverse aanbieders. Mobiele portals moeten voor de gebruiker het toegangsmedium worden voor internetapplicaties. Het kenmerk van mobiele portals ten opzichte van de traditionele webportals is dat mobiele portal een hogere graad van personalisatie hebben. MSN Wireless en Yahoo! Mobile zijn de leidinggevende mobiele portals in de VS, in Europa worden de meeste mobiele portals beheerd door de mobiele operators.
- *Mobiele Netwerk Operator*
  De mobiele netwerkoperator heeft al een relatie met de klant middels de overeenkomsten voor mobiele spraakcommunicatie. Dit is een groot voordeel voor de operator, waardoor de mobiele operator zich als een spin in het web van mobile commerce kan positioneren. Het belang dat aan de klantendatabase wordt gehecht kan men meten aan de enorme overnamegolf tussen de operators onderling en de gigantische bedragen die voor deze overnames zijn betaald.
  Er zijn ook nog mobiele service operators. Dit zijn operators zonder eigen netwerk en maken dus gebruik van een netwerk operator. Deze vorm wordt steeds minder belangrijk, het marktaandeel van de service operator loopt ook steeds verder terug en de meest waardevolle service operators worden overgenomen door de netwerk operators.
- *Hardwareproducenten*
  De hardwareproducenten spelen ook een hele belangrijke rol in de waardeketen. Consumenten kiezen vaak eerst het merk van het apparaat en pas daarna voor een bepaalde service of netwerk operator. De mobiele apparaten zijn het toegangsmechanisme voor mobile commerce. Zolang er nog niet voldoende apparaten zijn die technieken als WAP en GPRS ondersteunen, zal m-commerce nog niet doorbreken. De hardwareproducenten bepalen dus voor een groot deel wat de mogelijkheden van de gebruikers zijn.
- *Gebruiker*
  De gebruiker maakt gebruik van de mobiele applicatie en is de laatste schakel in de mobiele waardeketen.

De verschillende rollen in de waardeketen worden zowel door andere als door dezelfde partijen ingevuld. Zo vervult bijvoorbeeld een KPN Telecom zeer veel rollen in deze waardeketen. Ook is er een spanningsveld aanwezig bij bedrijven tussen enerzijds opschuiven in de waardeketen en anderzijds bij je core business blijven. Verticale

integratie houdt in dat bedrijven meerdere rollen uit de waardeketen gaan vervullen. In de praktijk is er een trend van verticale integratie te ontdekken. In de praktijk is er niet een keten, maar een netwerk (Tapscott, Ticoll en Lowy, 1999). Dit betekent dat veel partijen onderling communiceren en diensten aan elkaar leveren en dit niet via een vast traject door de keten verloopt.

2.5.2 Plaats TTP in waardeketen

In de waardeketen is er nog geen vaste plaats toegewezen aan de TTP. Een reden hiervoor is dat er in de waardeketen zelf nog veel veranderingen en integraties plaats zullen vinden. Dat het moeilijk is om de Trusted Third Party een plaats toe te wijzen, blijkt ook uit het feit dat de onderzoeksbureau's ook niet weten waar ze de vertrouwensfunctie onder moeten brengen. Vertrouwen is geen doel op zich, maar een middel om bepaalde transacties mogelijk te maken. Om deze reden denk ik dat de onderneming die de vertrouwensfunctie gaat vervullen geen application developer of application platform vendor is. Daarom stel ik ook voor om een aparte plaats voor de vertrouwensfunctie in de waardeketen te definiëren.
Over het feit welke partij de vertrouwensfunctie gaat vervullen, heerst op dit moment nog veel onduidelijkheid. Middels de volgende hoofdstukken hoop ik hierop een antwoord te vinden.

2.6 Samenvatting

In dit hoofdstuk is duidelijk geworden dat de mobile commerce markt op dit moment een sterke ontwikkeling doormaakt. Op het gebied van de techniek is de ontwikkeling van de netwerktechnologieën een zeer belangrijke factor voor het doen slagen van mobile commerce. GSM wordt op dit moment het meest gebruikt en GPRS komt nu mondjesmaat beschikbaar terwijl UMTS nog in ontwikkeling is. Voor mobile commerce worden andere protocollen gebruikt dan voor e-commerce. WAP is op dit moment het meest gebruikte protocol.
M-commerce heeft een aantal onderscheidende kenmerken ten opzichte van e-commerce. Deze kenmerken zijn: anyplace, anytime, personalisatie, locatie gebaseerde diensten en push diensten. Om mobile commerce tot een succes te maken, moeten applicaties van deze eigenschappen gebruik maken. De applicatieontwikkelaars moeten ook rekening houden met de beperkingen van mobile commerce, die veelal veroorzaakt worden door de mobiele techniek, zoals beperkte bandbreedte. Op basis van deze kenmerken en beperkingen wordt duidelijk dat mobile commerce een uitbreiding is op e-commerce en geen vervanging is voor het vaste internet.
Na bestudering van de betrouwbaarheidseisen van electronic commerce ben ik tot de conclusie gekomen dat de eisen voor mobile commerce niet anders zijn dan bij e-commerce. Het medium waar de transactie mee wordt uitgevoerd is anders, maar hierdoor veranderen de betrouwbaarheidseisen niet. Deze eisen zijn: authenticatie, integriteit, vertrouwelijkheid en onweerlegbaarheid.
Om te onderzoeken wat de rol van een Trusted Third Party is bij het betrouwbaar maken van mobiele transacties, is het noodzakelijk om eerste alle spelers uit de mobiele waardeketen te identificeren. In paragraaf 2.5 heb ik negen soorten spelers geïdentificeerd en hun taken omschreven. Op dit moment is het nog niet duidelijk welke partijen mobiele vertrouwensdiensten gaan aanbieden. Deze vraag wordt in hoofdstuk zes beantwoord, nadat in de volgende hoofdstukken de technieken en processen van een TTP in de vaste wereld zijn beschreven, van waaruit de uitdagingen voor een TTP volgen om mobiele identiteit te leveren.

Hoofdstuk 3: Technieken om elektronische transacties betrouwbaarder te maken

3.1 Inleiding

Uit hoofdstuk twee is gebleken dat de betrouwbaarheidseisen voor mobile commerce niet anders zijn dan bij e-commerce. Cryptografie is in de vaste wereld een belangrijke techniek om elektronische transacties betrouwbaarder te maken, het is dus te verwachten dat cryptografie ook een rol gaat spelen in de mobiele wereld. Daarom wordt er nu eerst een algemene introductie van cryptografie gegeven onafhankelijk van het gebruikte medium. Deze technologische beschrijving is vervolgens input voor het identificeren van uitdagingen bij het betrouwbaar maken van mobiele transacties. Deze uitdagingen worden in hoofdstuk vijf beschreven.

3.2 Cryptografie

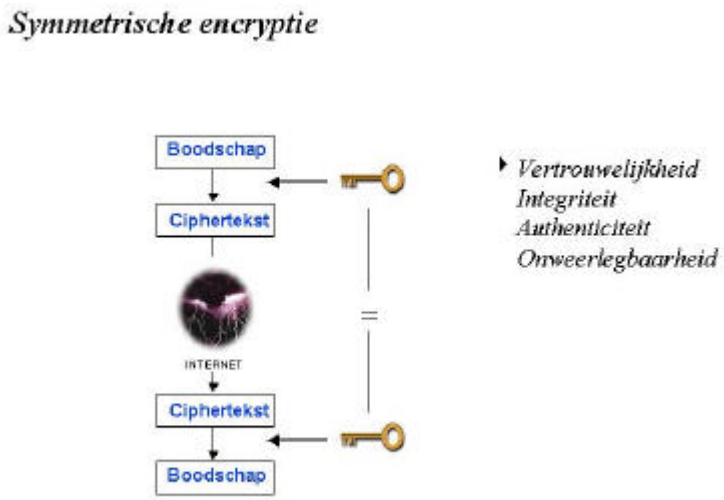
Cryptografie is een belangrijke techniek om aan de betrouwbaarheidseisen genoemd in paragraaf 2.4 te voldoen. Deze eisen zijn resumerend: authenticatie, integriteit, vertrouwelijkheid en onweerlegbaarheid. Middels cryptografie kunnen berichten versleutelt en ontsleutelt worden, zodat het bericht alleen maar door de juiste personen gelezen kan worden.
Cryptografie is een zeer oude techniek die al in de oudheid werd toegepast om berichten te versleutelen en geheim te houden. Voor dit versleutelen en ontsleutelen kun je gebruik maken van diverse soorten sleutels. Zo kun je bijvoorbeeld werken met een sleutel die de tekst achterste tevoren versleutelt, ‘mobile commerce’ wordt dan ‘ecremmoc elibom’.
De huidige cryptografie technieken werken op basis van wiskundige algoritmes, waarmee berichten versleuteld worden. Door de interactie met de sleutel werkt het algoritme iedere keer anders en hoeft het algoritme zelf niet geheim te zijn (van Ham, 1999). Er worden op dit moment drie cryptografie systemen gebruikt, deze systemen zullen in de volgende paragrafen behandeld worden.

- Symmetrische encryptie
- Asymmetrische encryptie
- Hybride encryptie

3.2.1 Symmetrische encryptie

Bij symmetrische encryptie wordt het berichtenverkeer tussen partijen versleuteld middels één sessie-sleutel. Deze sleutel wordt gebruikt voor zowel de versleuteling als de ontsleuteling van het bericht. De verzender versleutelt het bericht en de ontvanger ontsleutelt het bericht met dezelfde sleutel. Het versleutelde bericht wordt ook wel ciphertekst genoemd. Een voorwaarde hiervoor is dat beide partijen over de symmetrische sessie-sleutel beschikken. Dit is nu net het probleem bij electronic en mobile commerce. In deze situaties kennen de betrokken partijen elkaar vaak niet persoonlijk en is het met symmetrische encryptie onmogelijk om de sessie-sleutel op een betrouwbare wijze uit te wisselen. Met behulp van symmetrische encryptie wordt voldaan aan de vertrouwelijkheidseis, maar aan de overige eisen wordt met deze techniek nog niet voldaan. Een ander nadeel is dat men voor iedere partner weer een andere symmetrische sleutel heeft en men uiteindelijk over veel sleutels zal beschikken en dit is natuurlijk geen ideale situatie als men het gebruik van elektronische media wil

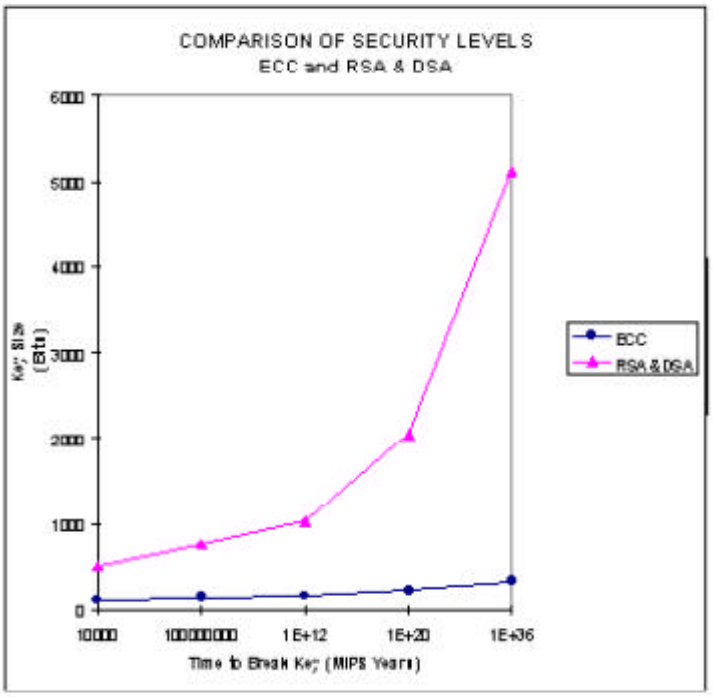
bevorderen. Het bekendste voorbeeld van een symmetrisch encryptiesysteem is DES (Data Encryption Standard). In figuur 3.1 is schematisch weergegeven hoe symmetrische encryptie werkt.



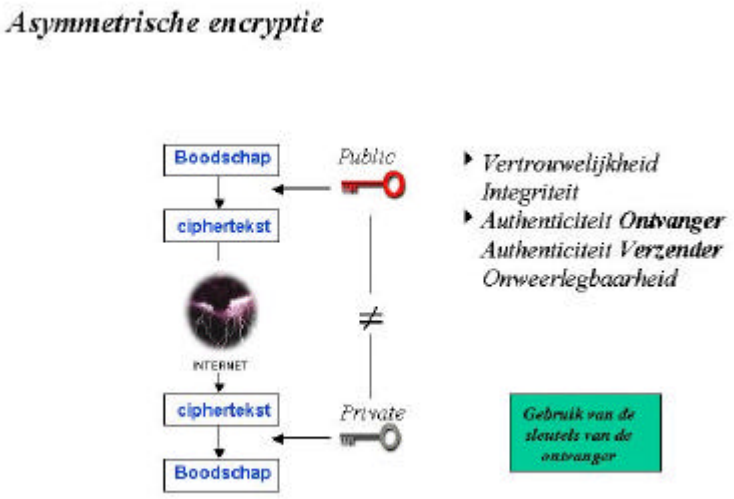
Figuur 3.1 Symmetrische encryptie, bron: DigiNotar

3.2.2 Asymmetrische encryptie

Bij asymmetrische encryptie wordt er gebruik gemaakt van een sleutelpaar bestaande uit een publieke en een private sleutel. Zoals de naamgeving al doet vermoeden, is de publieke sleutel middels een publiek toegankelijke database openbaar en is de private sleutel alleen kenbaar voor de gebruiker. Voor het functioneren van dit systeem is het van groot belang dat de gebruiker op een juiste wijze omgaat met zijn private sleutel, zodat deze alleen maar voor hem toegankelijk is. Het meest voorkomende asymmetrische encryptiesysteem is het RSA-algoritme (Rivest, Shamir en Adleman, 1978). Een encryptiesysteem dat nog niet zo lang op de markt is, is het ECC-algoritme (Elleptic Curve Cryptosystem). Deze encryptie-techniek werkt via een ander algoritme dan het RSA-algortime. Het grote voordeel van het ECC-algoritme is dat men een veel kleinere sleutellengte nodig heeft om hetzelfde beveiligingsniveau te bereiken dan bij het RSA-algoritme (Certicom, 2000). Dankzij deze kleinere sleutellengte vergt het ECC-algoritme veel minder processorkracht en dit is uiteraard weer gunstig als men encryptie bij mobile commerce gaat toepassen. In figuur 3.2 kan men de verschillen in beveiligingniveau van beide algoritmes zien. Het ECC-algoritme is echter nog niet zo uitvoerig getest als het RSA-algoritme en daarom is het dus lastig om uitspraken omtrent de betrouwbaarheid van dit algoritme te doen.
De verzender versleutelt een bericht met de publieke sleutel van de ontvanger, de ontvanger ontsleutelt dit bericht met zijn private sleutel. Op deze wijze kunnen beide partijen versleutelde berichten uitwisselen zonder dat daarvoor de private sleutels uitgewisseld moeten worden, dit is een groot voordeel van het asymmetrische systeem. Door gebruik te maken van asymmetrische encryptie wordt de vertrouwelijkheid van een bericht en de authenticiteit van de ontvanger gegarandeerd, maar aan de overige eisen is dan nog steeds niet voldaan. Hiervoor kan men gebruik maken van de verderop beschreven digitale handtekening. Figuur 3.3 geeft weer hoe asymmetrische encryptie werkt.



Figuur 3.2 Vergelijking van beveiligingsniveau, bron: http://www.certicom.com/research/wecc3.html, 2000



Figuur 3.3 Asymmetrische encryptie, bron: DigiNotar

3.2.3 Hybride encryptie

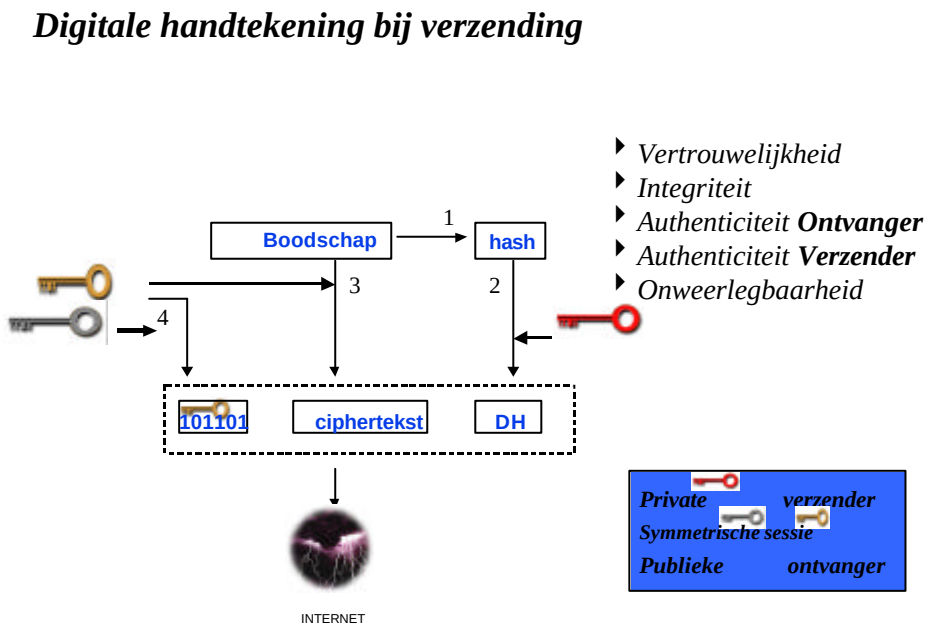
Een belangrijk verschil tussen symmetrische en asymmetrische encryptie is de snelheid waarmee beide systemen werken. Het snelheidsverschil tussen beide systemen is in het voordeel van symmetrische encryptie (Planning for PKI, 2001). Daarom heeft men naar een manier gezocht om de voordelen van beide technieken te combineren en is hybride encryptie ontwikkeld. In dit systeem wordt symmetrische encryptie gebruikt voor het versleutelen van het bericht en wordt asymmetrische encryptie gebruikt om op een

betrouwbare wijze de symmetrische sleutel te verzenden. Een toepassing van hybride encryptie is de digitale handtekening die hieronder beschreven is.

3.2.4 De digitale handtekening en het versleutelingsproces

Verzenden
Nu wordt het gehele versleutelingsproces en het zetten van de digitale handtekening bij verzending stapsgewijs uitgelegd, de nummers verwijzen naar de nummers in figuur 3.4.

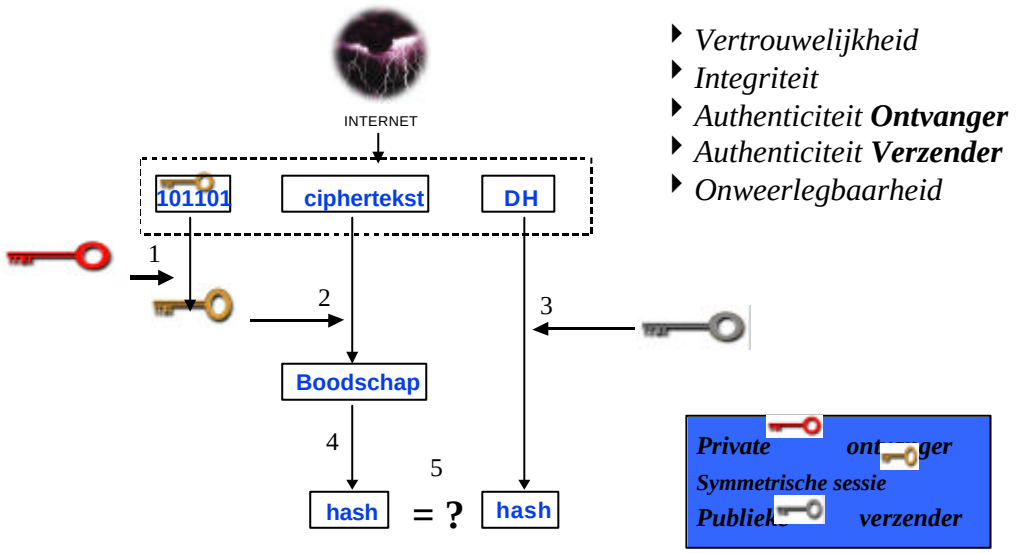
1. Voor het verzenden van het bericht wordt, automatisch door de programmatuur, de 'hash'waarde over het bericht berekend. Deze hashwaarde is een uniek getal dat afhankelijk is van met name de grootte van het document. Het kan worden beschouwd als een vingerafdruk van het bericht, aangezien iedere verandering in het bericht leidt tot een andere hashwaarde. Zelfs het weghalen en terugplaatsen van een komma levert een gewijzigde hashwaarde op.
2. Om meer zekerheden te verkrijgen kan men de hashwaarde, wanneer deze eenmaal is berekend, versleutelen met de private sleutel van de verzender. Op deze wijze krijgt de ontvangende partij zekerheid over de authenticiteit van de verzendende partij. De versleutelde hashwaarde is de digitale handtekening van de verzender, waarmee de onweerlegbaarheid gegarandeerd wordt.
3. Vervolgens wordt het bericht versleuteld met de symmetrische sessiesleutel.
4. De sessiesleutel waarmee het bericht versleuteld wordt, wordt zelf ook weer versleuteld met de publieke sleutel van de ontvanger. Hiermee wordt zekerheid verkregen over het feit dat alleen de rechtmatige ontvanger het bericht kan ontsleutelen en dus kan lezen.



Figuur 3.4 Gebruik van digitale handtekening bij verzending bericht, bron: DigiNotar

Ontvangen
Hier wordt het gehele ontsleutelingsproces en het ontsleutelen van de digitale handtekening bij ontvangst van het bericht stapsgewijs uitgelegd, de nummers verwijzen naar de nummers in figuur 3.5.

1. De sessiesleutel wordt ontsleuteld met de private sleutel van de ontvanger waarmee de authenticiteit van de ontvanger vast staat.
2. De ciphertekst wordt ontsleuteld met de symmetrische sessiesleutel, waarmee de vertrouwelijkheid van het bericht is gewaarborgd. Het bericht was onderweg niet te lezen voor derden.
3. De digitale handtekening wordt ontsleuteld met de publieke sleutel van de verzender, waardoor de authenticiteit van de verzender vast staat.
4. Bij aankomst van het bericht bij de ontvanger wordt, weder om automatisch door de programmatuur, de hashwaarde berekend.
5. De hashwaarde die de programmatuur zelf heeft berekend wordt dan vergeleken met de hashwaarde die uit proces 3 is gekomen. Indien ze niet gelijk zijn betekent dit dat het bericht is veranderd tijdens het transport. Daarmee wordt aangetoond dat de integriteit van het bericht niet langer gewaarborgd is.



Figuur 3.5 Gebruik van digitale handtekening bij ontvangst bericht, bron: DigiNotar

Een voorbeeld van een toepassing die gebruik maakt van de digitale handtekening is e-mail. De nieuwere e-mail programma's zoals Outlook 2000 ondersteunen het gebruik van encryptie, digitale handtekeningen en certificaten. Een andere toepassing is het gebruik van de digitale handtekening en encryptie bij een SSL verbinding.

3.2.5 Kanttekenigen bij encryptie

Encryptie biedt vele voordelen in het elektronische berichtenverkeer, maar deze techniek heeft natuurlijk ook enkele nadelen die hier behandeld zullen worden.

- *Toename rekenkracht van computers*
  Computers hebben in de loop der tijd steeds meer rekenkracht gekregen en dit proces zal volgens de wet van Moore in de toekomst doorzetten. Deze wet is vernoemd naar Gordon Moore, één van de oprichters van Intel, en zegt dat het aantal transistors op een processorchip elke achttien maanden met een factor twee toeneemt. Dit betekent dat de huidige sleutels gebaseerd op wiskundige algoritmes in de toekomst door brute rekenkracht gekraakt kunnen worden. Om dit te voorkomen kan men met grotere sleutels gaan werken. De huidige RSA-sleutels hebben meestal een lengte van 1024 bits en sommige toepassingen maken al gebruik van een 2048 bits sleutellengte. In de toekomst zal de sleutellengte dus alleen maar toenemen, of er worden nieuwe 'intelligentere' algoritmen zoals het ECC ontwikkeld om weerstand te bieden aan de toenemende rekenkracht van de computers.
- *Irreële eisen als gevolg van de technische mogelijkheden*
  Doordat de techniek steeds meer mogelijkheden biedt, worden de eisen van de gebruiker ook steeds hoger en dit geldt vaak ook voor de betrouwbaarheid. Ik vraag me af of het realistisch is om 100% betrouwbaarheid te eisen bij elektronische transacties, aangezien deze garantie naar mijn mening in de papieren wereld ook niet aanwezig is. Dus waarom zou deze eis dan wel moeten gelden in de elektronische wereld? Het is uiteraard wel vanzelfsprekend dat er naar 100% betrouwbaarheid gestreefd wordt, maar men moet wel in het achterhoofd houden dat dit nauwelijks realiseerbaar is en ook nog nooit gerealiseerd is.
- *Vernieuwing van de sleutel*
  Om het eerstgenoemde probleem tegen te gaan moeten de sleutels af en toe vernieuwd worden. In een ideale situatie krijgt de gebruiker een nieuw sleutelpaar en behoudt hij zijn huidige certificaat. Dit is een lastig proces aangezien de publieke sleutel in het certificaat is opgenomen en een gedeelte van het certificaat wel vervangen moet worden. Een ander probleem hierbij is dat de gebruiker natuurlijk nog wel de berichten moeten kunnen lezen die met zijn oude sleutelpaar zijn versleuteld. Programma's als Outlook zijn hier nog niet op ingericht en dit levert dus problemen op in de toekomst als men met nieuwe sleutels wil gaan werken.
- *Sleutelverlies*
  Indien de gebruiker zijn sleutel verliest kan hij de berichten niet meer ontcijferen en zijn alle versleuteld opgeslagen berichten onleesbaar geworden. Een oplossing hiervoor kan zijn om een reservesleutel bij een TTP in bewaring te geven. Vanuit de Europese richtlijn over digitale handtekeningen mag een TTP echter geen sleutels bewaren waarmee een digitale handtekening gezet kan worden. De reden hiervoor is dat de digitale handtekening dan niet meer op een unieke wijze verbonden is met de ondertekenaar, want de TTP beschikt ook over de middelen om de digitale handtekening te zetten. Om dit op te lossen kan er gebruik worden gemaakt van twee sleutelparen, één paar voor encryptie en het tweede paar wordt dan gebruikt voor het zetten van de digitale handtekening. In de praktijk wordt hier nog weinig gebruik van gemaakt. Een ander juridisch aspect dat hier in ogenschouw moet worden genomen is dat de overheid bezig is met een wet, waardoor het voor een TTP verplicht wordt om de uitgegeven sleutels te archiveren zodat de overheid te allen tijde het berichtenverkeer tussen personen kan ontsleutelen.

- *Waarde die gehecht moet worden aan de betrouwbaarheid van de digitale handtekening*
  Wanneer men gebruik maakt van encryptie en de digitale handtekening, is er nog steeds geen zekerheid omtrent de authenticiteit van de communicerende partijen. Deze zekerheid is wel weergegeven in de figuren, maar hiervoor is nog één stap noodzakelijk. De publieke sleutel moet gekoppeld worden aan een fysieke identiteit. Pas wanneer dit gerealiseerd is kunnen er betrouwbare elektronische transacties afgesloten worden. Deze taak kan door een Trusted Third Party met behulp van digitale certificaten worden uitgevoerd. Hoe dit kan gebeuren, wordt in hoofdstuk vier beschreven. Naar mijn idee is het oplossen van dit 'probleem' zeer belangrijk voor het bereiken van een optimaal betrouwbaarheidsniveau van een Public Key Infrastructure. Een PKI is de gehele infrastructuur die gebruikt wordt bij asymmetrische en hybride encryptie in combinatie met de digitale certificaten.

3.3 Samenvatting

Cryptografie is een belangrijke techniek om elektronisch berichtenverkeer te beveiligen. Middels cryptografie kan men berichten versleutelen en ontsleutelen. Er zijn drie technieken te onderscheiden: symmetrische, asymmetrische en hybride encryptie. Met behulp van onder andere de digitale handtekening kan aan de vier betrouwbaarheidseisen worden voldaan. Deze eisen zijn: authenticatie, integriteit, vertrouwelijkheid en onweerlegbaarheid.
Naast de voordelen van encryptie heeft deze techniek ook een aantal nadelen. Zo neemt onder andere de rekenkracht van de computers toe, met als gevolg dat versleutelde berichten na verloop van tijd gekraakt kunnen worden. Een andere kanttekening is dat om definitief aan bovenstaande eisen te voldoen, er nog een extra stap nodig is. Het is noodzakelijk dat het sleutelpaar aan een fysieke identiteit gekoppeld wordt. Dit is een belangrijke taak voor de Trusted Third Party, die deze taak uitvoert op basis van digitale certificaten. Wat een TTP nu precies is en hoe de TTP haar taken uitvoert, wordt in het volgende hoofdstuk beschreven.

Hoofdstuk 4: Taken en processen van een Trusted Third Party

4.1 Inleiding

In het vorige hoofdstuk is duidelijk geworden dat de fysieke identiteit aan een digitale identiteit moet worden gekoppeld om van betrouwbaar elektronisch berichtenverkeer te kunnen spreken. Hiervoor is een Trusted Third Party uitermate geschikt. In dit hoofdstuk wordt beschreven wat een TTP nu eigenlijk is en hoe een TTP elektronisch berichtenverkeer betrouwbaarder kan maken. Vervolgens worden de eisen waaraan een TTP moet voldoen besproken.

4.2 Wat is een Trusted Third Party en wat zijn de taken van een TTP?

Om de processen van een Trusted Third Party goed uit te leggen is het eerst van belang om duidelijk te krijgen wat nu een TTP eigenlijk is en daarom zal ik dat in deze paragraaf eerst behandelen. Vervolgens zullen de taken van een Trusted Third Party beschreven worden. Op basis hiervan worden dan de processen van een TTP behandeld. In hoofdstuk één heb ik onderstaande definitie van een TTP gegeven.

"Een Trusted Third Party is een onafhankelijke en onpartijdige organisatie die vertrouwensdiensten levert voor het realiseren van elektronische datacommunicatie." (Duthler, 1998).

De definitie van een TTP die DigiNotar in haar Certificate Practise Statement (CPS) hanteert is de volgende:

"Een vertrouwde, onafhankelijke partij, die diensten aanbiedt waardoor de betrouwbaarheid van de elektronische gegevensuitwisseling wordt vergroot."

De definitie die ik vanaf nu wil hanteren is een combinatie van bovenstaande twee definities en luidt als volgt:

"Een Trusted Third Party is een vertrouwde, onafhankelijke en onpartijdige organisatie die vertrouwensdiensten levert voor het bevorderen van het vertrouwen in elektronische transacties."

Een TTP kan diensten leveren gericht op de interne communicatie binnen een organisatie, dit is een interne TTP. Daarentegen heb je ook nog de publieke TTP, zoals DigiNotar. Een publieke TTP richt zich op de communicatie tussen verschillende partijen met als uitgangspunt dat het digitale certificaat voor meerdere communicatiepartners gebruikt kan worden.
In onderstaande lijst staan enkele Trusted Third Parties die internationaal en in Nederland actief zijn (DigiNotar, 2001).

- Verisign, met als distributeurs voor de Nederlandse markt:
  - PinkRoccade Megaplex
  - KPN
- Baltimore
- Entrust
- Globalsign.com
- Price Waterhouse Coopers
- Keymail (PTT Post)
- ABZ (Financiële dienstverlening)

Zoals uit hoofdstuk drie is gebleken, is een belangrijke taak van een TTP het koppelen van de fysieke identiteit aan de digitale identiteit. De TTP doet dit door een digitaal certificaat aan de publieke sleutel te koppelen. Een TTP kan ook nog andere taken uitvoeren zoals het tijdstempelen of archiveren van berichten. Maar omdat dit onderzoek erop gericht is om te onderzoeken hoe een TTP mobiele identiteit kan leveren, zullen de overige taken en diensten buiten beschouwing gelaten worden. Voordat de processen van een TTP beschreven worden, wordt hieronder eerst uitgelegd wat de termen digitale identiteit en digitaal certificaat nu eigenlijk inhouden.

4.3 Wat is digitale identiteit?

In de papieren wereld worden overeenkomsten door middel van ondertekening gesloten. We leven nu steeds meer in een digitale wereld, waarin mensen niet alleen maar middels papier met elkaar communiceren, het berichtenverkeer is steeds meer gedigitaliseerd. Maar om overeenkomsten digitaal af te sluiten, moet men het digitale bericht wel kunnen ondertekenen. Hiervoor heeft men een digitale identiteit nodig, middels die digitale identiteit kan iemand zich digitaal identificeren en rechtsgeldige transacties afsluiten. Maar hoe krijgt men deze digitale identiteit? Hierbij speelt een Trusted Third Party een belangrijke rol, deze kan de fysieke identiteit van een persoon vaststellen en indien de identiteit juist is vastgesteld, kan aan deze persoon een digitale identiteit worden toegekend. De TTP koppelt, middels een digitaal certificaat, de digitale identiteit aan de fysieke identiteit. Op deze wijze kunnen personen dus vertrouwen op de digitale identiteit van de partij waarmee ze communiceren. Een voorwaarde hiervoor is wel dat de TTP, die de digitale identiteit heeft uitgegeven, door alle partijen vertrouwd wordt en als een onafhankelijke en onpartijdige partij gezien wordt.

4.4 Het digitale certificaat

Het digitale certificaat wordt door de Trusted Third Party aan de gebruiker uitgegeven. Dit certificaat bevat gegevens over de gebruiker en de TTP die het certificaat heeft uitgegeven alsmede de publieke sleutel van de gebruiker. Door gebruik te maken van het digitale certificaat en de in hoofdstuk drie genoemde technieken kan men zekerheid krijgen over iemands identiteit op het internet en kunnen er op een betrouwbare en veilige manier transacties worden gedaan die voldoen aan de eerdergenoemde betrouwbaarheidseisen in hoofdstuk twee. Het digitale certificaat wordt meegestuurd met het versleutelde bericht.
Om een technische wirwar aan soorten digitale certificaten te voorkomen, heeft het Internet Engineering Task Force (IETF) de X.509 standaard ontwikkeld. Op dit moment is versie 3 het meest gebruikte certificaat. Deze standaard is gedefinieerd in RFC2459 en RFC3033, welke te vinden zijn op www.ietf.org. In het eerste document worden de meer technische eisen gedefinieerd en in het tweede document worden de eisen gedefinieerd waarmee een certificaat aan de juridische wet- en regelgeving kan voldoen zodat het een gekwalificeerd certificaat wordt.
DigiNotar levert verschillende certificaten die op de X.509v3 standaard gebaseerd zijn. Deze certificaten zijn ieder weer geschikt voor andere doeleinden en leveren ook verschillende betrouwbaarheidsniveaus. Ieder certificaat is bedoeld voor een bepaalde rol in de maatschappij. Zo is het natuurlijke persoonscertificaat bedoeld voor consumenten en het beroepscertificaat heeft als doelgroep beoefenaars van zelfstandige beroepen, zoals arts of notaris. Een persoon kan meerdere certificaten gebruiken, maar dan vervult die persoon ook meerdere rollen in de maatschappij. De exacte doeleinden en eigenschappen van deze certificaten zijn terug te vinden in het

CPS van DigiNotar, het CPS is in de bijlage opgenomen. De verschillende certificaten zijn:

- Natuurlijke Persooncertificaat
- Bedrijfscertificaat
- Persoonsgebonden Bedrijfscertificaat
- Beroepscertificaat
- Servercertificaat
- Envelopcertifcaat
- Entreecertificaat

Tevens zijn de certificaten ook in te delen in verschillende klasses, klasse 1, 2 en 3. Deze indeling is door Verisign opgezet. Bij de aanvraag van een klasse 1 certificaat wordt alleen gecontroleerd of de opgegeven naam bij het e-mail adres hoort. Bij klasse 2 vindt ook nog controle plaats op basis van de gegevens die bij de aanvraag opgegeven moeten worden. Klasse drie certificaten bieden het hoogste betrouwbaarheidsniveau omdat hier ook nog eens face-to-face controle heeft plaatsgevonden alvorens het certificaat is uitgegeven. Voor een uitgebreide beschrijving van de verschillende klasses verwijs ik naar het CPS van Verisign, dat op www.verisign.com te vinden is.
DigiNotar hanteert een andere klasse indeling, klasse A, B en C, waarbij klasse A vergelijkbaar is met klasse 3, klasse B met klasse 2 ½ (valt qua betrouwbaarheidsniveau tussen 2 en 3 in) en klasse C met klasse 2. De exacte eisen die aan de controle gesteld worden zijn terug te vinden in de certificaat lay-out die in de bijlage is opgenomen.

4.4.1 Processen rondom het digitale certificaat

Er zijn natuurlijk ook een aantal processen van toepassing rondom het gebruik van digitale certificaten. Deze processen zijn achtereenvolgens: aanvraag, verificatie, afgifte, verlenging, vernieuwing, wijziging, schorsing, intrekking, beheer en gebruik. Deze processen worden in het CPS van DigiNotar beschreven en zullen hier dan ook kort in het algemeen, dus los van DigiNotar, behandeld worden.

Aanvraag en verificatie
Tijdens dit proces wordt er een aanvraag voor een certificaat ingediend bij een Registration Authority (RA). De definitie van een RA volgens DigiNotar is: “Een vertrouwde autoriteit, die de gegevens die nodig zijn voor de aanvraag van het Certificaat verifieert en bij akkoordbevinding doorstuurt naar de CA” De RA controleert of de gegevens van de aanvrager juist zijn en honoreert de aanvraag alleen indien alle gegevens juist zijn bevonden. Voor ieder certificaat gelden weer andere controles, deze zijn allemaal in het CPS en de certificaat lay-out terug te vinden. Dit proces is van groot belang omdat hier de fysieke identiteit aan het digitale certificaat wordt gekoppeld. De RA geeft dus zelf geen certificaten uit.

Afgifte
Nadat de RA de aanvraag heeft goedgekeurd kan de Certification Authority (CA) tot afgifte van de digitale certificaten overgaan. De definitie van een CA volgens DigiNotar is: “Een vertrouwde autoriteit die Certificaten aanmaakt en toekent.” De CA kan bij het uitgeven van het certificaat het sleutelpaar genereren en de CA wijst dan een wachtwoord toe waarmee de private sleutel gebruikt kan worden, eventueel aangevuld met een beveiligingsmethode zoals biometrie. Biometrie is de identificatie van een persoon op basis van unieke lichamelijke kenmerken. In het andere geval genereert de

gebruiker zelf zijn sleutelpaar en kent hier zelf een wachtwoord aan toe, waaraan de CA het certificaat koppelt, ook hier kan gebruik gemaakt worden van biometrie. Het certificaat en bijbehorende sleutelpaar kunnen op verschillende media worden uitgegeven: smartcard, diskette en per e-mail. Waarbij de smartcard het meest betrouwbare medium is, aangezien deze het hoogste beveiligingsniveau heeft. Voor toepassingen waarbij hoge betrouwbaarheid een belangrijke rol speelt, wordt dan ook bijna altijd gebruik gemaakt van een smartcard. Voor het gebruik van een smartcard is ook een smartcard reader noodzakelijk, deze reader zorgt voor de communicatie tussen de smartcard en de computer.
Het uitgegeven certificaat is vaak niet voor eeuwig geldig en heeft een beperkte geldigheidsduur, dit kan voor iedere CA weer anders zijn. De geldigheidsduur van een certificaat staat altijd op het certificaat vermeld. De CA moet het in een openbare database publiceren.

Verlenging, vernieuwing en wijziging
Indien de geldigheidsduur van het certificaat verstreken is, is het certificaat onbruikbaar geworden. Wil de gebruiker dit certificaat blijven gebruiken dan zal het certificaat verlengd moeten worden. Bij verlenging blijven de sleutels en de inhoud van het certificaat gelijk, alleen de geldigheidsduur op het certificaat wordt gewijzigd. Wijziging houdt in dat er gegevens op het certificaat gewijzigd moeten worden, dus niet de sleutels. Wijziging kan nodig zijn doordat bijvoorbeeld het adres van de gebruiker of het bedrijf waarvoor de gebruiker werkt is gewijzigd. Bij vernieuwing wordt ook het sleutelpaar vervangen.
Een probleem bij deze processen is dat het technisch lastig is om één gegeven op de smartcard te vervangen en de andere gegevens hetzelfde te laten. Op dit moment wordt dan ook vaak bij verlenging, wijziging of vernieuwing de certificaatdrager vervangen en krijgt de gebruiker een nieuw certificaat met een nieuw sleutelpaar.

Schorsing
Indien een certificaat geschorst is, kan er tijdelijk niet op vertrouwd worden totdat de schorsing weer is ingetrokken. Een certificaat kan geschorst worden door de gebruiker, de RA en de CA. De RA en de CA kunnen dit doen op dezelfde gronden als waarop een certificaat kan worden ingetrokken, waarover later meer. Een schorsing kan ongedaan gemaakt worden door de verzoeker van de schorsing.

Intrekking
Indien een certificaat is ingetrokken dient de gebruiker het gebruik ervan en het gebruik van het sleutelpaar onmiddellijk te staken op straffe van een boete. Een verzoek van intrekking kan van de gebruiker zelf afkomen, als deze bijvoorbeeld zijn private sleutel is verloren. Tevens mogen de RA en CA het certificaat op bepaalde gronden intrekken.
Wanneer het certificaat is ingetrokken dient de CA ervoor te zorgen dat dit zo spoedig mogelijk op de Certification Revocation List (CRL) gemeld wordt. In het CRL staan alle ingetrokken certificaten van de betreffende CA. Overeenkomsten die gesloten zijn voorafgaande aan de intrekking van het certificaat blijven gewoon geldig, aangezien het certificaat geldig was ten tijde van sluiting van de overeenkomst.

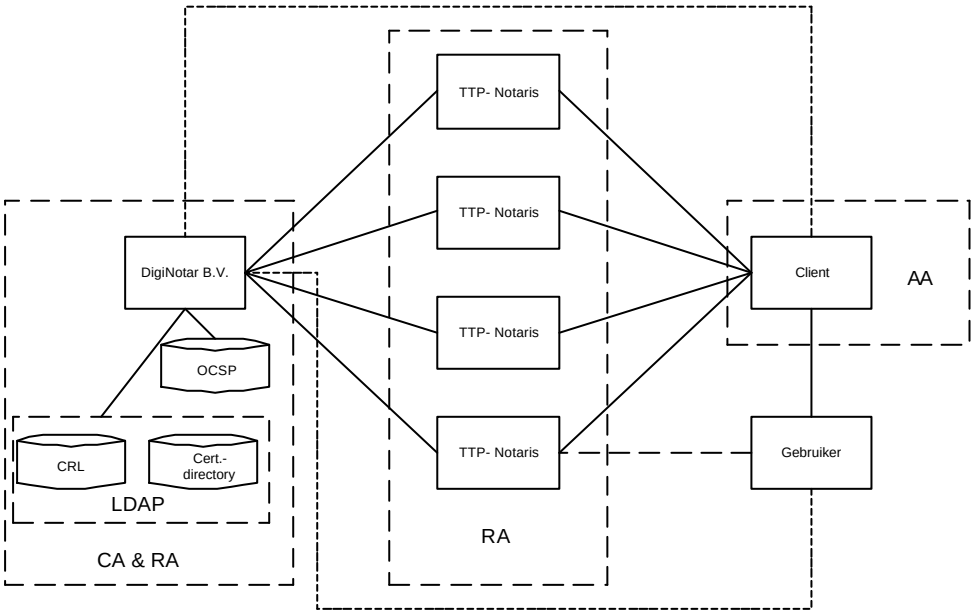
Beheer en gebruik
Vanaf het moment van afgifte van het certificaat is de gebruiker conform het CPS van de CA en de contractuele afspraken waarvan het CPS van de CA deel kan uitmaken verantwoordelijk voor het beheer van de private sleutel, de in het certificaat vastgelegde

informatie en de aan hen toegekende persoonlijke pincode. De overige gebruiksregels staan allemaal in het CPS vermeld en zullen hier verder niet behandeld worden.
Het gebruik van het certificaat en het sleutelpaar kan in een aantal processen worden opgesplitst:

- *Het zetten van de digitale handtekening*
  Het digitaal ondertekenen van een bericht gebeurt door de gebruiker van het digitale certificaat. Indien de gebruiker een bericht digitaal wil ondertekenen, geeft hij hiertoe een opdracht in het programma. De programmatuur vraagt dan om de certificaatdrager en de bijbehorende pincode.
- *Het valideren en zoeken van het digitale certificaat*
  Het valideren wordt door de vertrouwende partij uitgevoerd. Deze partij wil natuurlijk zekerheid hebben omtrent het meegestuurde certificaat van de verzender. In veel programma's is dit proces geautomatiseerd. Het programma controleert in een online database via het OCSP-protocol of het certificaat is ingetrokken of niet. Ik zal hier niet de technische specificaties van dit protocol behandelen, omdat dit niet nodig is voor het begrip van het validatie-proces. Het certificaat kan ook handmatig gecontroleerd worden. De vertrouwende partij gaat dan naar de website van de CA die het certificaat heeft uitgegeven en kan dan op zoek gaan naar het betreffende certificaat en vergelijken met het meegestuurde certificaat.

4.4.2 Betrokken partijen bij aanvraag, uitgifte en gebruik van een digitaal certificaat

In onderstaand figuur wordt schematisch weergegeven welke partijen er betrokken zijn bij het gehele certificatieproces. Het figuur is gebaseerd op de werkwijze die door DigiNotar gehanteerd wordt.



Figuur 4.1 DigiNotar-model voor aanvraag en uitgifte digitale certificaat

DigiNotar B.V.
In dit model is DigiNotar zowel een CA als een RA. DigiNotar is dus verantwoordelijk voor alle functies die bij een CA horen, zoals het bijhouden van de LDAP-directory,

waarin de CRL en de certificaten directory in opgenomen zitten. Tevens verzorgt de CA het OCSP.

TTP-Notaris
De TTP-Notaris treedt in dit model op als RA voor DigiNotar. Deze notarissen zijn door het hele land verspreid.

Cliënt
De cliënt is de aanvrager van het certificaat. In de huidige situatie kan hij dit bij de TTP-Notaris of DigiNotar doen. In de huidige situatie wordt de aanvraag vaak rechtstreeks bij DigiNotar ingediend. De reden hiervoor is dat het een vrij nieuw concept is en de notarissen er nog niet helemaal klaar voor zijn om als RA op te treden. In de toekomst moet dit natuurlijk veranderen, maar DigiNotar blijft zelf ook een TTP-notaris. De cliënt is vaak een onderneming die gebruik wil gaan maken van persoonsgebonden bedrijfscertificaten. De onderneming zal dan eerst een bedrijfscertificaat moeten aanvragen om vervolgens certificaten te kunnen aanvragen voor de gebruiker. Voor afgifte van het bedrijfscertificaat vindt er face-to-face controle plaats, vervolgens kan een geautoriseerd persoon binnen het bedrijf de certificaataanvragen voor de gebruikers doen. Deze persoon bepaald dus, eventueel op basis van procedures en regels, of iemand een certificaat krijgt of niet en voor welke doeleinden dit certificaat gebruikt mag worden. De geautoriseerde persoon doet de eerste registratie van de aanvraag, maar is toch geen RA omdat er in deze fase geen controle plaats vindt. Ik wil dan ook hier het begrip Authorizing Authority introduceren, aangezien de cliënt de gebruiker autoriseert voor gebruik van een certificaat.

Gebruiker
Deze partij is de daadwerkelijke gebruiker van het certificaat. De gebruiker zet hiermee zijn digitale handtekening onder een bericht. Tevens is de gebruiker ook vaak de vertrouwende partij, omdat hij ook veel zal communiceren met andere gebruikers van digitale certificaten. In zijn rol van vertrouwende partij maakt hij gebruik van de CRL en het OCSP om de digitale handtekening te verifiëren. In sommige gevallen mag de gebruiker ook zelf zijn certificaat aanvragen. Voor welke certificaten dit geldt, staat in het CPS van DigiNotar vermeld.

4.5 Juridische eisen

De juridische eisen die aan een elektronische handtekening gesteld worden, die op basis van een digitaal certificaat gezet kan worden, worden uiteengezet in de richtlijn 1999/93/EG betreffende elektronische handtekeningen. Deze richtlijn moet nog wel in de lidstaten afzonderlijk geïmplementeerd worden, maar deze nationale wetten mogen niet in strijd zijn met de EG richtlijn, daarom wordt deze richtlijn ook als uitgangspunt voor dit onderzoek genomen. De richtlijn had inmiddels al in Nederland geïmplementeerd moeten zijn, maar dit is nog niet het geval. De verwachting is nu dat de richtlijn middels een wetsvoorstel in oktober in de Nederlandse wet wordt opgenomen. De belangrijkste artikelen uit de richtlijn worden hier behandeld, de complete richtlijn is in de bijlage te vinden.

Artikel 2
1. “elektronische handtekening”: elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie;

2. “geavanceerde elektronische handtekening”; een elektronische handtekening die voldoet aan de volgende eisen”
    a. zij is op unieke wijze aan de ondertekenaar verbonden;
    b. zij maakt het mogelijk de ondertekenaar te identificeren;
    c. zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en
    d. zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;

Op basis van artikel 5, lid 1 wordt een geavanceerde elektronische handtekening gelijkgesteld aan een geschreven handtekening en is er dus geen juridisch onderscheid tussen deze twee. Een niet-geavanceerde elektronische handtekening, bijvoorbeeld een ingescande handtekening, mag op basis van artikel 5, lid 2 geen rechtsgeldigheid worden ontzegd louter op grond van het feit dat deze niet geavanceerd is. Maar om 100% zekerheid te hebben over de rechtsgeldigheid is het dus aan te bevelen om te werken met een geavanceerde elektronische handtekening. In dit onderzoek wordt dan ook gewerkt op basis van de geavanceerde elektronische handtekening. Het model wat in dit onderzoek ontwikkeld wordt zal dan ook moeten voldoen aan de richtlijn betreffende elektronische handtekeningen.
In deze richtlijn wordt niet gesproken over het verschil tussen electronic en mobile commerce. De richtlijn bespreekt alleen de eisen waaraan een elektronische handtekening moet voldoen om gelijkgesteld te worden aan de geschreven handtekening. Tevens worden er eisen gedefinieerd waaraan een gekwalificeerd certificaat moet voldoen, waaraan de partijen, die de elektronische handtekening uitgeven, moeten voldoen, waaraan de middelen waarmee het certificaat wordt aangemaakt moeten voldoen en er wordt een aanbeveling gegeven hoe de elektronische handtekening op een veilige wijze geverifieerd kan worden. Deze eisen en aanbeveling zijn terug te vinden in bijlage 1-4 van de richtlijn. Op basis van deze richtlijn kan gesteld worden dat er geen onderscheid is tussen de juridische eisen en gevolgen van een elektronische handtekening bij electronic en mobile commerce. Het gaat dus niet om het gebruikte medium maar om de invulling van de juridische eisen.
Voor de diensten die een TTP levert zijn ook nog een aantal andere wetten van toepassing, onafhankelijk van het feit of het om e-commerce of m-commerce gaat. Deze wetten zijn:

- Wet bescherming persoonsgegevens, deze wet is op één september 2001 ingevoerd ter vervanging van de wet persoonregistraties. De WBP is de implementatie van Richtlijn 95/46/EC;
- Telecommunicatiewet ;
- Wet computercriminaliteit 1 en 2;
- Wettelijke bewijs- en bewaarverplichtingen;
- Encryptieregelgeving;
- Wet op notarisambt (in het geval van DigiNotar);
- Richtlijn 2000/31/EC, richtlijn voor e-commerce;
- Richtlijn 97/7/EC, richtlijn voor handel op afstand;

Indien geen van deze wetten van toepassing is beroept men zich vaak op de Algemene Beginselen van Behoorlijk IT-gebruik. Dit zijn beginselen waarvan men redelijkerwijs mag verwachten dat deze worden nageleefd. Ze worden algemeen beschouwd als “best practice”.

Dat de invulling van de eisen die uit bovenstaande wetten en richtlijnen voor mobile commerce soms moeilijker is dan bij e-commerce valt uit onderstaand voorbeeld op te maken.
Om een elektronische transactie rechtsgeldig te laten zijn, is het noodzakelijk dat de klant de algemene voorwaarden duidelijk heeft moeten kunnen lezen (Directive 2000/31/EC van EU). Op het kleine scherm is het echter moeilijk om bijvoorbeeld twee A4-tjes met algemene voorwaarden te lezen. Tevens moet de gebruiker volgens artikel 10, lid 2 van deze directive de voorwaarden kunnen opslaan en reproduceren, dus het is nog maar de vraag of transacties afgesloten middels een mobiel apparaat hieraan voldoen. Ook zullen veel klanten afhaken als ze deze voorwaarden moeten lezen en goedkeuren. Voor het gemak worden deze voorwaarden veelal dan weggelaten met als gevolg dat de transactie zeker niet meer rechtsgeldig is (Krugten en Snels, 2000). Het is niet het doel van het te ontwikkelen model om dit probleem op te lossen, maar omdat het toch een belangrijke juridische beperking is, wordt dit hier toch genoemd.
Op basis van artikel K uit bijlage 2 van de richtlijn dient iedere Trusted Third Party ook te beschikken over een soort van Algemene Voorwaarden, deze worden ook wel het Certificate Practice Statement genoemd. Het CPS behandelt alle rechten en plichten die gelden voor de aanvraag, verstrekking en het gebruik van digitale identiteitscertificaten. Zowel de TTP als de certificaat aanvrager zijn in geval van certificaatverstrekking contractueel gebonden aan het CPS. In de bijlage is het volledige CPS van DigiNotar te vinden, hieraan kunnen geen rechten worden ontleend, aangezien het CPS aan verandering onderhevig is. Voor de meest actuele versie verwijs ik naar de website van DigiNotar, www.diginotar.nl.

4.6 Overige eisen en randvoorwaarden voor een Trusted Third Party

Om de certificatiedienst goed te kunnen uitvoeren en om een hoog betrouwbaarheidsniveau te leveren moet een TTP betrouwbaar zijn. Om deze betrouwbaarheid te waarborgen dient de TTP aan een aantal eisen en randvoorwaarden te voldoen. De juridische eisen behandel ik hier niet, aangezien die al in paragraaf 4.5 aan de orde zijn gekomen. De eisen en randvoorwaarden baseer ik op Duthler (1998) en de notitie “Nationaal TTP-project” (Tweede Kamer, vergaderjaar 1998-1999, 26581, nr. 1). Ik heb deze twee stukken met elkaar gecombineerd, omdat geen van beide naar mijn inzicht volledig was.

- *Onafhankelijkheid en onpartijdigheid*
  De TTP dient niet gebonden te zijn aan één of meer bestaande partijen en geen belang te hebben bij de te beveiligen informatie.
- *Deskundigheid en betrouwbaarheid personeel*
  De medewerkers van een TTP moeten aan een bepaald opleidingsniveau voldoen en over een bepaalde mate van ervaring beschikken. Zo heeft KPN in haar CPS een opleidingsniveau gedefinieerd waaraan de medewerkers van een CA/Local RA moeten voldoen. Tevens moet het personeel kunnen worden vertrouwd ten aanzien van de aan hun toevertrouwde taken.
- *Continuïteit*
  De continuïteit van TTP-diensten dient zoveel mogelijk te worden gewaarborgd, ook in geval van overname, fusie, bedrijfsstaking of faillissement. De financiële positie van de TTP-organisatie dient voldoende waarborgen te bieden ten aanzien van de continuïteit van de TTP-dienst.

- *Beveiliging*
  De organisatie en de diensten van een TTP dienen adequaat te zijn beveiligd. De in 1994 door het Ministerie van Economische Zaken uitgegeven Code voor Informatiebeveiliging lijkt een goede basis te bieden voor de beveiliging van TTP-organisaties, waarbij de hoge betrouwbaarheidseisen die aan een TTP worden gesteld aanvullende maatregelen noodzakelijk kunnen maken. De Information Technology Security Evaluation Criteria (ITSEC) en daarop mede gebaseerde Common Criteria bieden hierbij wellicht een goede basis voor de evaluatie van de gebruikte IT-producten.
- *Authenticatie*
  De TTP-organisatie dient bij het nemen van beslissingen en het uitvoeren van handelingen door management en medewerkers van de TTP-organisatie steeds ondubbelzinnig de identiteit van de hierbij betrokken personen te kunnen vaststellen. Het vaststellen van de identiteit van betrokken personen dient ook achteraf mogelijk te zijn.
- *Autorisatie*
  Specifieke bevoegdheden dienen duidelijk en ondubbelzinnig aan specifieke functies en functionarissen binnen de TTP-organisatie te zijn toegewezen.
- *Functiescheiding*
  Er dient een adequate controletechnische scheiding te bestaan tussen beschikkende, bewarende, uitvoerende en controlerende functies binnen de TTP-organisatie, onder meer inzake sleutelbeheer. Omdat functiescheiding een belangrijke rol speelt bij de betrouwbaarheid, wordt in paragraaf 4.6.1 wordt een beschrijving gegeven van de functiescheiding binnen het DigiNotar-model.
- *Aansprakelijkheid*
  Om te bereiken dat een partij vertrouwt op het gebruikte certificaat is het van belang dat de TTP garant staat voor het door haar uitgegeven certificaat. De aansprakelijkheid van een TTP moet dus duidelijk beschreven zijn, dit staat vaak in de algemene voorwaarden en het CPS. Op basis van de richtlijn voor elektronische handtekeningen artikel 6, kan gesteld worden dat de CA aansprakelijk is voor de door haar uitgegeven certificaten. Ook in het geval dat de RA een fout heeft gemaakt, is de CA aansprakelijk. De CA en RA kunnen onderling wel afspraken maken over de onderlinge aansprakelijkheid, maar richting externe partijen is de CA aansprakelijk. Onder externe partijen worden onder andere de gebruiker en de vertrouwende partij verstaan.
  Om deze aansprakelijkheid ook werkelijk financieel te kunnen waarborgen, kan een TTP een beroepsverzekering afsluiten om deze financiële risico's af te dekken die het loopt omdat de TTP aansprakelijk gesteld kan worden indien de door hem geleverde diensten niet voldoen en schade opleveren voor de afnemende partij. Een onderneming kan alleen zijn kerntaken middels een beroepsverzekering verzekeren. Natuurlijk kan alles verzekerd worden, maar hiervoor moet uiteraard ook een prijs betaald worden. Als de diensten niet onder de beroepsverzekering valt, dan zal de premie vele malen hoger liggen en is het zeer lastig/duur om een verzekering af te sluiten. Een telecomoperator kan zich dus wel middels een beroepsverzekering verzekeren tegen het uitvallen van haar kerntaken, maar niet tegen misbruik van certificaten die de operator heeft uitgegeven, aangezien dit niet als een kerntaak van de operator gezien wordt.
- *Toezicht op de TTP*
  De gebruiker van het certificaat en de partij die vertrouwt op het certificaat, de vertrouwende partij, moeten natuurlijk ook vertrouwen hebben in de TTP als

betrouwbare organisatie. Maar hoe weten deze partijen of een TTP betrouwbaar is. Bovenstaande punten dragen hier zeker aan bij, maar wat ook zeer belangrijk is dat er een partij boven de TTP staat, die toezicht houdt op de gang van zaken bij een TTP. Je kunt hierbij denken aan Trusted Third Parties die elkaar certificeren, ook wel cross-certificatie genoemd. Een andere oplossing is dat een overkoepelend orgaan toezicht gaat houden op de Trusted Third Parties en een kwaliteitskeurmerk aan de TTP gaat verstrekken. Vanuit de markt is er nu een certificeringstraject ingezet om TTP's te gaan certificeren. Dit moet niet verward worden met digitale certificaten, dit is een kwaliteitskeurmerk. Uit dit keurmerk kan worden afgeleid dat een TTP aan bepaalde eisen en randvoorwaarden voldoet. Deze eisen zijn door de Raad van Accreditatie opgesteld en de toetsing bij de TTP wordt uitgevoerd door een daartoe bevoegde organisatie zoals de accountantskantoren.
Op basis van de telecommunicatiewet gaat de OPTA toezicht houden op de gehele markt van Trusted Third Parties. Om dit toezicht mogelijk te maken moet de telecommunicatiewet aan de hand van de richtlijn voor elektronische handtekeningen aangepast worden.

- *Transparantie*
  De TTP dient inzicht te geven in de gehanteerde werkwijze, om toetsing van de TTP-organisatie en de TTP-dienst mogelijk te maken.

4.6.1 Functiescheidingen binnen het DigiNotar-model

Om meer zekerheid omtrent de betrouwbaarheid van de geleverde diensten te krijgen is het belangrijk dat er interne controle plaats vindt binnen de organisatie. Een nuttige maatregel hierbij is het aanbrengen van functiescheidingen. In deze paragraaf worden de functiescheidingen binnen het DigiNotar-model van paragraaf 4.4.2 beschreven. De volgende vijf functies zijn te onderscheiden (Starreveld, de Mare, Joëls, 1997):

- *Registreren*
  De registratie van de certificaataanvraag wordt door de RA uitgevoerd. Dit is een TTP-notaris. Een medewerker van dit kantoor controleert de aanvraag en voert de gegevens in. Vervolgens controleert de notaris de ingevoerde aanvraag en keurt deze goed. Deze twee processen zijn fysiek van elkaar gescheiden en kunnen niet door dezelfde persoon worden uitgevoerd. Na goedkeuring wordt de aanvraag doorgestuurd naar de CA.
- *Beschikken*
  In dit geval versta ik onder beschikken, de bevoegdheid om te mogen beslissen over de goedkeuring van de certificaataanvraag. Deze beslissing wordt uitgevoerd door de TTP-notaris. Dit is hierboven al beschreven
- *Uitvoeren*
  De CA geeft het certificaat uit. Tevens onderhoudt de CA de CRL en certificaat-directory. De CA-functie wordt door DigiNotar uitgevoerd.
- *Bewaren*
  De fysieke aanvraag wordt bewaard door de RA, het notariskantoor dus. De CA bewaart de digitale aanvraag. De digitale aanvraag wordt door de RA naar de CA toegestuurd. In het geval dat er een sleutelpaar voor encryptie wordt gebruikt, kan deze door de CA worden opgeslagen. Het sleutelpaar voor ondertekening mag niet worden opgeslagen.

- *Controleren*
  In het gehele proces zitten een aantal controlemomenten. De cliënt dient de aanvraag voor de gebruikers in. De cliënt controleert deze gegevens en of de gebruiker bevoegd zijn om van een certificaat gebruik te maken.
  Vervolgens vindt er bij het registratieproces de zojuist genoemde controles plaats.

Op basis van bovenstaande beschrijving kan men concluderen dat er een goede functiescheiding plaats vindt. Tevens worden de belangrijke functies door de notaris uitgevoerd. De notaris heeft in de maatschappij een vertrouwensfunctie en is dus ook zeer geschikt om de beschreven functies betrouwbaar uit te voeren.

4.7 Samenvatting

Om elektronisch berichtenverkeer betrouwbaar te maken moet men naast cryptografie gebruik maken van een Trusted Third Party. De TTP koppelt de fysieke identiteit aan een digitale identiteit middels een digitaal certificaat. De gangbare digitale certificaten zijn gebaseerd op de X.509v3 standaard.
Om een certificaat op een betrouwbare wijze uit te geven, moeten een aantal processen met grote zorg worden uitgevoerd. Deze processen zijn achtereenvolgens: aanvraag, verificatie, afgifte, verlenging, vernieuwing, wijziging, schorsing, intrekking, beheer en gebruik. De volgende partijen zijn bij deze processen betrokken: Registration Authority, Certification Authority, Authorizing Authority en de Gebruiker.
Bij het werken met digitale certificaten en digitale handtekeningen zijn uiteraard een aantal wetten van toepassing. De Europese richtlijn betreffende de elektronische handtekening is hierbij de belangrijkste. Uit de richtlijn blijkt dat de elektronische handtekening gelijk kan worden gesteld aan de geschreven handtekening. Om absolute zekerheid omtrent de rechtsgeldigheid van de digitale handtekening te krijgen, moet aan een aantal eisen uit de richtlijn worden voldaan. Om betrouwbare diensten te leveren, moet de TTP aan een aantal eisen en randvoorwaarden voldoen. Deze eisen zijn als volgt: Onafhankelijkheid en Onpartijdigheid, Deskundigheid en Betrouwbaarheid personeel, Continuïteit, Beveiliging, Authenticatie, Autorisatie, Functiescheiding, Aansprakelijkheid, Toezicht op de TTP en Transparantie.

Hoofdstuk 5: Wat zijn de uitdagingen bij mobiele identiteit en welke methodiek wordt er gebruikt om deze uitdagingen te benaderen?

5.1 Inleiding

In hoofdstuk twee heb ik de technologische eigenschappen en kenmerken van mobile commerce beschreven evenals de betrouwbaarheidseisen en de betrokken partijen bij m-commerce. Vervolgens is in hoofdstuk drie besproken welke technieken gebruikt kunnen worden om elektronisch berichtenverkeer betrouwbaar te maken. Op basis van deze technieken zijn de taken van een Trusted Third Party in hoofdstuk vier gedefinieerd. Tevens zijn in hoofdstuk vier de processen beschreven die aan bod komen rondom het gehele traject van aanvraag tot aan het uiteindelijke gebruik van een digitaal certificaat en zijn de betrokken partijen bij deze processen voor de huidige vaste, niet mobiele, situatie in kaart gebracht.
De combinatie van hoofdstuk twee, drie en vier leidt tot een aantal uitdagingen om mobiele identiteit te leveren, deze worden in paragraaf 5.2 beschreven. Deze uitdagingen leveren kansen en bedreigingen op voor de 'traditionele' TTP. Het geheel van uitdagingen, kansen en bedreigingen vormt aanleiding om het onderzoek voort te zetten waarmee duidelijk moet worden wat de rol van de TTP is in de mobiele vertrouwensmarkt. Omdat er over de rolverdeling nog veel onduidelijkheden heersen, wordt er een model ontwikkeld. Met behulp van dit model kan dan de rolverdeling bepaald worden. Vervolgens wordt de gebruikte methode van modelontwikkeling uitgelegd. Waarna de gebruikers en de doelstellingen van het model worden gedefinieerd. Nadat al deze stappen zijn afgerond wordt in hoofdstuk zes het model ontwikkeld.

5.2 Uitdagingen bij het gebruik van mobiele certificaten

In deze paragraaf wordt een onderscheid gemaakt tussen de technologische en proces gerichte uitdagingen. Met het woord gebruik in de titel van deze paragraaf wordt niet alleen 'gebruik' bedoeld zoals gedefinieerd in paragraaf 4.4.1, maar alle processen rondom het digitale mobiele certificaat.

Technologische uitdagingen
In paragraaf 2.3.2 zijn de technologische beperkingen van mobile commerce besproken en deze zal ik dan ook als uitgangspunt nemen voor het identificeren van de technologische uitdagingen bij mobiele certificaten.

- *Beperkte opslagcapaciteit*
  Hierdoor is er geen ruimte om het digitale certificaat in het mobiele apparaat op te slaan en moet er naar een andere wijze worden gezocht om een mobiel certificaat te gebruiken.
- *Beperkte bandbreedte*
  In de vaste wereld worden de digitale certificaten tussen de communicerende partijen heen en weer gestuurd. In de mobiele wereld, waar we te maken hebben met een beperkte bandbreedte, vergt dit teveel capaciteit en is het niet praktisch om de certificaten met de berichten mee te sturen.

- *Beperkte rekenkracht*
  Doordat de meeste mobiele apparaten en vooral de mobiele telefoon weinig rekenkracht hebben, kost het veel tijd om berichten te versleutelen en een digitale handtekening te zetten. Deze beperking kan ervoor zorgen dat de gebruiker geen digitale handtekening wil zetten, omdat dit teveel tijd kost. Dit houdt tevens in dat het veel tijd kost om een bericht te ontsleutelen en om een digitale handtekening te controleren.
- *Beperkte capaciteit batterij*
  Bovenstaande processen hebben natuurlijk ook stroom nodig om uitgevoerd te worden en omdat het behoorlijk complexe processen zijn, kosten ze veel energie van de batterij. Deze batterij heeft maar een beperkte gebruikersduur, dus is het niet wenselijk dat er veel van deze processen door het mobiele apparaat moeten worden uitgevoerd.
- *Verschillende protocollen*
  Doordat de mobiele en vaste protocollen van elkaar verschillen is het moeilijk om de vaste PKI en de Wireless PKI compatible met elkaar te houden. In een ideale situatie is er sprake van één PKI, die zowel voor vast als mobiel internet gebruikt kan worden.
- *Certificaatdrager*
  In de vaste wereld is de certificaatdrager veelal de smartcard, deze smartcard kan in een reader gestopt worden die is aangesloten op de PC. De meeste mobiele apparaten en zeker de telefoons hebben al een interne reader waar nu de SIM inzit. Deze reader wordt in de meeste oplossingen ook gebruikt om de SWIM te lezen. De SWIM is een gecombineerde smartcard van de traditionele SIM en de Wireless Identity Module. Op de WIM staat het sleutelpaar en het eventuele certificaat. Een gebruiker van een PC kun je achteraf makkelijk een digitale identiteit toekennen door een smartcardreader aan de PC te koppelen en een smartcard uit te geven. Maar voor een mobiele gebruiker is het niet praktisch om de SWIM uit de telefoon te halen en hiermee naar een RA/CA te gaan. Om het certificaat en sleutelpaar op de SWIM te krijgen, zal er dus een andere oplossing moeten worden bedacht en hieruit vloeien naast de technische veranderingen ook een aantal procedurele vraagstukken, die hieronder behandeld zullen worden.

Proces gerichte uitdagingen
Deze uitdagingen zijn gebaseerd op de procesbeschrijvingen uit paragraaf 4.4.1, het model uit paragraaf 4.4.2 en de veranderende waardeketen van mobile commerce ten opzichte van e-commerce met de centrale rol van de telecomoperator beschreven in hoofdstuk twee.

- *Sleutelgeneratie*
  Doordat de certificaatdrager bij aanschaf al in het mobiele apparaat zit, is het wenselijk dat het sleutelpaar dan ook al gegenereerd is. In de praktijk betekent dit dat de sleutels door de smartcard fabrikant bij fabricage gegenereerd worden, de meeste oplossingen van leveranciers zoals Baltimore en Smarttrust zijn hier ook op gebaseerd. Een nadeel hiervan is dat er een mogelijk beveiligingslek kan zitten in het proces van fabricage tot aan levering aan de klant. Dit proces zal dus op een veilige wijze moeten gebeuren en alle betrokken partijen moeten ervan overtuigd zijn dat iedere smartcard uniek is en niemand de sleutels heeft kunnen kopiëren.

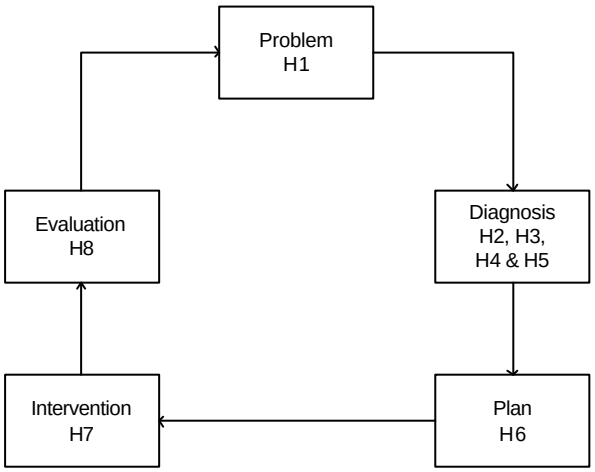
- *Wie gaat de RA en CA-functie vervullen?*
  De telecomoperator heeft tijdens de verkoop van een mobiel apparaat direct contact met de klant en tijdens het gebruik van dit apparaat is er ook een relatie tussen deze twee. De operator houdt bij hoeveel de klant gebruik maakt van zijn netwerk en stuurt hiervoor een rekening naar de klant. De telecomoperator zou dus de rol van CA of RA kunnen vervullen. Uit het model zal blijken welke partij het meest geschikt is om deze rollen te vervullen. Voor pre-paid toestellen ligt de situatie weer anders, omdat de klant dan geen direct contact met de telecomoperator hoeft te hebben.
- *Het aanvraagproces*
  Het aanvragen richt zich voornamelijk op de vraag door wie de aanvraag verwerkt, geregistreerd en goedgekeurd wordt en is dus terug te voeren op de vragen en problemen die bij het vorige punt behandeld zijn. Tevens moeten er procedures en methodes aanwezig zijn waarmee de RA kan controleren of de aanvrager ook daadwerkelijk over het sleutelpaar bezit.
- *Het uitgifteproces*
  De problemen die bij uitgifte van een certificaat aan de orde zijn, worden grotendeels door technische eigenschappen van een mobiel apparaat veroorzaakt, zoals beschreven bij de technische problemen. Hierdoor moeten verschillende procedures anders ingericht worden. Het digitale certificaat moet op de SWIM komen en eigenlijk zonder dat de gebruiker hiervoor naar de CA moet gaan. Er moeten dus procedures en technieken ontworpen worden waarmee het certificaat op een veilige wijze op de certificaatdrager van de gebruiker gezet kan worden.

5.3 Kansen en bedreigingen voor TTP

In de vaste wereld vervult de ‘traditionele’ TTP een grote rol in de vertrouwensmarkt en er zijn niet veel partijen in Nederland die deze diensten aanbieden. De mobile commerce markt is nog volop in ontwikkeling en daarmee samenhangend ook de vertrouwensmarkt voor mobile commerce. Uit bovenstaande paragraaf is op te maken dat er nog veel uitdagingen zijn voor de partijen om mobiele certificaten te leveren en om een wireless PKI op te zetten. Omdat het nog zo’n onontgonnen gebied is, biedt deze nieuwe markt veel kansen voor ondernemingen. Deze kansen gelden natuurlijk ook voor partijen die in het verleden nog geen TTP-diensten hebben geleverd, zoals de mobiele operators. De mogelijkheid dat nieuwe partijen zich in de mobiele vertrouwensmarkt gaan begeven, brengt automatisch bedreigingen voor de ‘traditionele’ TTP met zich mee. De kans bestaat dan dat de nieuwe partij een grote rol in de mobiele vertrouwensmarkt gaat spelen en dat de ‘traditionele’ TTP haar leidinggevende rol van de vaste markt niet naar de mobiele markt kan continueren. In het geval dat de mobiele vertrouwensmarkt de vaste markt gaat vervangen, is dit een zeer bedreigende situatie. Dit kan het geval zijn wanneer het mobiele apparaat als een ‘Personal Trusted Device’ wordt gebruikt. Dit houdt in dat ook transacties die via electronic commerce gestart worden, ondertekend worden met het mobiele apparaat. De dienstverlener stuurt dan een bericht ter ondertekening naar het mobiele apparaat van de gebruiker.
Daarom is het van belang voor een ‘traditionele’ TTP zoals DigiNotar om te onderzoeken wat haar rol kan zijn in de mobiele vertrouwensmarkt en hoe een TTP gebruik kan maken van de kansen die deze nieuwe markt biedt. In het te ontwikkelen model wordt dan ook onderzocht wat de rolverdeling is in de mobiele vertrouwensmarkt en hoe een TTP invulling kan geven aan haar mogelijke rol.

5.4 Methodiek van modelontwikkeling

Om tot een goed onderbouwd model te komen dat een oplossing biedt voor de uitdagingen rondom de mobiele certificaten zoals geschetst in paragraaf 5.2 zijn er een aantal punten van belang. Ten eerste is het noodzakelijk dat er gewerkt wordt volgens een gestructureerde werkwijze en enkele standaardtechnieken om een onderzoek op te zetten en ten tweede moet er gebruik worden gemaakt van bewezen modelleringstechnieken.
Het onderzoek dat ik uitvoer is meer een ontwerpgericht/exploratief onderzoek dan een theorievormend onderzoek. Dit onderzoek wordt ook wel een wetenschappelijk praktijk onderzoek genoemd. Dit soort onderzoek onderscheidt zich van fundamenteel wetenschappelijk onderzoek, omdat het niet gaat om de kennis zelf, maar om het oplossen van een praktijkprobleem (Veenker en van Geert, 1994).Volgens van Dijk (1991) is de regulatieve cyclus een geschikte methode om ontwerpgericht onderzoek te ondersteunen. Voor theorievormend onderzoek wordt vaak de empirische cyclus gebruikt. De regulatieve cyclus is ontworpen door van Strien (1986).



Figuur 5.1 De regulatieve cyclus, bron: van Strien, 1986

Zoals uit de figuur is af te lezen, identificeert van Strien vijf verschillende fases in een onderzoek. Deze fases worden hieronder besproken en gekoppeld aan een onderdeel/hoofdstuk van deze scriptie.

- *Probleem*
  In de eerste fase wordt het probleem geïdentificeerd. Deze fase wordt bij aanvang van het onderzoek uitgevoerd en heb ik in hoofdstuk één beschreven, waar de probleemstelling en onderzoeksvragen gedefinieerd zijn.
- *Diagnose*
  In de tweede fase van de cyclus worden de problemen verder onderzocht. In dit onderzoek worden de problemen in hoofdstuk twee, drie, vier en vijf aan een verder onderzoek onderworpen. In de diagnosefase worden ook de uitdagingen geschetst die de aanleiding zijn voor het voorzetten van het onderzoek.
- *Plan*
  In de plan-fase wordt een plan of model ontwikkeld op basis waarvan de problemen kunnen worden opgelost. Dit model wordt in hoofdstuk zes beschreven.

- *De ingreep/intervention*
  Tijdens deze fase wordt het ontwikkelde model in de praktijk geïmplementeerd. In mijn onderzoek is dit de toetsingsfase. In hoofdstuk zeven wordt de toetsingstoepassing geselecteerd en beschreven, waarna vervolgens toetsing wordt over gegaan. Hierna zullen de toetsingsresultaten geanalyseerd worden.
- *Evaluatie*
  Met deze fase wordt het voorlopige eindpunt van het onderzoek bereikt. Hier worden de resultaten uit de vorige fases geëvalueerd en kan men dus concluderen of het ontwikkelde model een juist antwoord op de probleemstelling heeft gegeven. Indien er na deze fase nog problemen onbeantwoord zijn of er nieuwe problemen verschijnen, kan men weer opnieuw starten met de cyclus.

Modelleertechniek
Om bovenstaande onderzoeksopzet goed uit kunnen voeren, is het belangrijk om de probleemsituatie en de oplossingen op een juiste wijze in kaart te brengen. Hiervoor zal ik een conceptueel model ontwikkelingen. Vanuit het conceptuele model wordt geen empirisch model gemaakt, omdat dit meer richting simulatie gaat en de toetsing plaats zal vinden aan de hand van het conceptuele model. Om de processen en relaties in kaart te brengen, ga ik gebruik maken van het volgende model (van Eijck, 1996), die onderdeel uitmaken van het conceptuele model.

- *Netwerkmodel*
  Een manier om organisatorische relaties te begrijpen is om de informele en formele communicatie en interactie tussen de verschillende actoren die betrokken zijn bij een proces te beschrijven. (Lundquist en Huston, 1990, March en Simon, 1958, Qureshi,1995) Met behulp van het netwerkmodel kan zo'n beschrijving gemaakt worden. Het netwerkmodel kan zowel voor interne als externe relaties gebruikt worden.

Van Eijck heeft ook nog twee andere modellen gedefinieerd die als uitbreiding gebruikt kunnen worden op het netwerkmodel. Deze twee modellen gebruik ik in dit onderzoek niet, omdat ik middels het netwerkmodel alle processen zeer duidelijk in kaart kan brengen. Ik heb dus niet de overige twee modellen nodig om de processen een niveau dieper te beschrijven. Deze twee modellen zijn het procesmodel en het actorenmodel.

5.5 Opzet van het model

5.5.1 Indeling en doelstelling van het model

Indeling model
De probleemstelling die in hoofdstuk één gedefinieerd is, luidt als volgt:

"Welke rol heeft een Trusted Third Party bij het bevorderen van het vertrouwen en de veiligheid bij het realiseren van mobiele transacties voor B2B en B2E m-commerce en hoe kan een TTP invulling geven aan deze rol?"

Als je deze probleemstelling combineert met de uitdagingen die in dit hoofdstuk gedefinieerd zijn, dan kom je tot de conclusie dat er twee stappen nodig zijn om tot een beantwoording van de probleemstelling te komen.
Ten eerste moet de rolverdeling in de betrouwbaarheidsmarkt gedefinieerd worden. Hiermee bedoel ik dat duidelijk moet zijn welke partijen de verschillende functies gaan

vervullen, zoals de CA en de RA. Tijdens dit proces wordt duidelijk welke rol een 'traditionele' TTP heeft in de mobiele vertrouwensmarkt.
Vervolgens kan op basis van de rolverdeling invulling aan deze rol gegeven worden. In deze tweede fase wordt het gehele WPKI-platform beschreven. Met het WPKI-platform wordt het geheel bedoeld om mobiele certificaten te leveren en te gebruiken. Je kunt hierbij denken aan de technische infrastructuur en de onderlinge relaties tussen de betrokken partijen.
Deze tweede fase richt zich op het implementeren van een WPKI in een toepassing en ondersteunt het nemen van beslissingen die bij iedere toepassing weer opnieuw genomen moeten worden. Het voortraject van hoe een TTP haar platform moet inrichten om überhaupt een WPKI te kunnen implementeren, wordt hier niet behandeld. Dit zijn eenmalige beslissingen zoals investerings- en technische beslissingen en leverancierskeuze. Omdat ik een model wil ontwikkelen dat bij iedere toepassing gebruikt kan worden, kies ik ervoor om deze eenmalige beslissingen niet in het model op te nemen.

Doelstelling
De doelstelling van het model is eigenlijk om een antwoord te vinden op de bovenstaande probleemstelling en de geschetste uitdagingen uit dit hoofdstuk, dit probeer ik te bereiken door de modelontwikkeling in de zojuist genoemde twee fases op te splitsen. Nadat beide fases zijn afgerond en de toetsing van het model heeft plaatsgevonden, is de doelstelling van het model bereikt en is er een goed onderbouwd antwoord gevonden op de probleemstelling. Het ontwikkelen van het model is dus geen doel op zich, maar een middel om een gefundeerd antwoord te kunnen geven op de probleemstelling.

5.5.2 Voor wie is het model bedoeld?

Het beantwoorden van de probleemstelling is het hoofddoel van het model, maar daarnaast heeft het model ook nog een bijdoel. Bij het implementeren van een WPKI zijn een aantal partijen betrokken. Het bijdoel van het model is om deze partijen, middels het model, ondersteuning te bieden bij het implementeren van een WPKI. Hieronder zal ik per partij aangeven wat het nut van het model is en waarvoor ze het model kunnen gebruiken.

- *TTP*
  De TTP levert de vertrouwensdiensten en zal het model gebruiken om haar gehele WPKI platform juist in te richten, zodat de TTP mobiele certificaten uit kan gaan geven.
- *Adviesorganisatie*
  Deze partij adviseert de dienstverlener bij het implementeren van een WPKI in de toepassing. De consultant heeft een totaalbeeld van het gehele project en zal het model in zijn totaliteit gebruiken om een juist advies te geven. Het model is ontwikkeld vanuit het oogpunt van de consultant. De adviesorganisatie kan ook een onderdeel van de TTP zijn, zoals dat bij DigiNotar het geval is.
- *Dienstverlener*
  De WPKI wordt geïmplementeerd in de toepassing van de dienstverlener. De dienstverlener gebruikt het model om haar processen juist in te richten. Maar aangezien de dienstverlener meestal weinig kennis heeft van een WPKI zal de dienstverlener zich veelal baseren op de adviezen van de consultant.

- *Telecomoperator*
  Afhankelijk van welke rol de telecomoperator gaat vervullen, zal deze ook gebruik maken van het model om invulling te geven aan zijn rol. Aangezien de rol van de telecomoperator hier nog niet duidelijk is, kan ik nog niet definitief aangeven hoe deze het model gaat gebruiken.

Bovenstaande partijen werken natuurlijk niet los van elkaar aan het WPKI-project, ze zullen samenwerken in een projectgroep. Het gebruik van het model is dan ook niet zo strikt te scheiden als ik hierboven heb gedaan, maar het gebruik ervan zal een samenwerking zijn tussen alle betrokken partijen.

5.5.3 Definitieve aannames voor de modelontwikkeling

Voordat ik aan dit onderzoek begon, heb ik in hoofdstuk één een aantal aannames gedaan. Deze aannames worden hieronder herhaald, tevens worden hier nog enige aanvullingen gegeven. De definitieve aannames zijn:

- In dit onderzoek wordt onder een transactie niet alleen een financiële transactie verstaan, maar ook een transactie zonder directe financiële waarde. Tijdens een transactie kan bijvoorbeeld ook zeer vertrouwelijke informatie worden uitgewisseld.
- Dit onderzoek is erop gericht om een oplossing aan te dragen voor de B2B en B2E mobile commerce markt. Onder B2B worden niet alleen transacties tussen bedrijven onderling verstaan, maar ook transacties tussen overheid en bedrijfsleven en overheidsinstanties onderling. Onder B2E wordt business to employee verstaan, dit is de mobiele communicatie tussen werkgever en werknemer. Een belangrijke reden voor deze aanname is dat de consumentenmarkt in de vaste wereld nog amper gebruik maakt van digitale certificaten en er eigenlijk geen redenen zijn waarom de consument in de mobiele wereld wel ineens de behoefte zal hebben om gebruik te maken van mobiele digitale certificaten. Deze aanname wordt versterkt door de bevindingen uit het literatuuronderzoek en de interviews
- De derde aanname is een afbakening van het begrip vertrouwen. Vertrouwen kan natuurlijk verschillende betekenissen hebben voor een consument, bijvoorbeeld het vertrouwen dat een consument in een leverancier heeft dat bestelde goederen ook daadwerkelijk geleverd worden. Dit onderzoek richt zich echter op het verhogen van het vertrouwen van een transactie op basis van de punten in paragraaf 1.1. Het gaat hierbij dan onder andere om het authenticeren en identificeren van de verschillende partijen en het rechtsgeldig afsluiten van transacties en dus niet om het verhogen van het vertrouwen in de betrouwbaarheid van de verschillende partijen over bijvoorbeeld de kwaliteit van de geleverde diensten.
- Een nieuwe aanname die ik hier maak, is dat als gevolg van de keuze voor de B2B en B2E markt, ik mijn focus ook zal richten op de gebruikersmarkt voor abonnementen en niet op de pre-paid markt. De reden hiervoor is dat in de zakelijke markt veelal gebruik wordt gemaakt van abonnementen.
- De telecommunicatiemarkt maakt op dit moment grote veranderingen door. Met de komst van mobiel internet en de introductie van nieuwe technieken als GPRS en UMTS profileren de operators zich steeds meer als dienstenaanbieders in plaats van pure netwerkproviders. Het is op dit moment dan ook moeilijk te zeggen hoe de mobiele markt er over twee jaar uit zal zien en wat de rol van de mobiele operator zal zijn. Omdat de markt zo in beweging is, is het dus ook onverstandig om een model te willen ontwikkelen dat verder kijkt dan de komende twee jaar. De huidige situatie zal dan ook als basis dienen voor het te ontwikkelen model, waarbij ik

natuurlijk wel probeer om enigszins rekening te houden met de bruikbaarheid van het model in de toekomst door het model niet teveel afhankelijk te maken van de wisselende rollen in de mobiele markt.

- Dit onderzoek richt zich op de Nederlandse mobiele markt. E-commerce en mobile commerce maken wel grensoverschrijdende transacties mogelijk, maar gezien de complexiteit van de mobiele markt heb ik besloten om de Nederlandse markt als uitgangspunt te nemen. De complexiteit wordt onder andere veroorzaakt door het aantal betrokken partijen en de onzekerheid die in de mobiele markt over de te volgen strategieën heerst. Een andere reden voor deze keuze is dat de huidige PKI-projecten van DigiNotar en de overige TTP's in Nederland zich veelal richten op de binnenlandse markt.
- De overheid houdt zich sterk bezig met de elektronische identiteit van de burger, een belangrijk project hierbij is de Elektronische Nederlandse Identiteitskaart. Op de lange termijn is het de bedoeling dat iedere burger een digitaal paspoort/certificaat krijgt. Dit is echter nog verre toekomstmuziek aangezien de wet die de e-NIK mogelijk maakt pas in 2002 behandeld zal worden (GBA-rapport, 2001). De e-NIK is geen vervanging van de huidige certificaten die door de Trusted Third Parties worden uitgegeven, aangezien de e-NIK persoonlijk is en geen koppeling heeft met de werkgever, zoals dat nu vaak het geval bij de digitale certificaten. Om deze redenen wordt de overheid als zijnde een TTP dan ook niet meegenomen in het verdere verloop van dit onderzoek. De overheid als regelgevend orgaan speelt uiteraard wel een belangrijke rol in dit onderzoek.

5.6 Samenvatting

In dit hoofdstuk is gebleken dat er een aantal uitdagingen aanwezig zijn om mobiele identiteit te leveren. Deze uitdagingen liggen zowel op het technische vlak als de procedurele kant. De uitdagingen in deze nieuwe vertrouwensmarkt veroorzaken een aantal kansen en bedreigingen voor de 'traditionele' TTP. Kansen zijn de mogelijkheden voor de TTP om haar diensten ook voor de mobiele markt aan te bieden en een grotere afzetmarkt te genereren. Bedreigingen worden veroorzaakt doordat de mobiele operator een belangrijke rol in de mobiele markt speelt en de kans bestaat dat de operator de rol van een TTP wil gaan vervullen in de mobiele markt. Wanneer de mobiele vertrouwensmarkt de vaste vertrouwensmarkt gaat vervangen, dan verliest de TTP marktaandeel ten opzichte van de telecomoperator.
De uitdagingen, kansen en bedreigingen vormen de aanleiding om het onderzoek voort te zetten. In het te ontwikkelen model worden de verschillende rollen in de mobiele vertrouwensketen aan de verschillende partijen worden toebedeeld. Op basis van deze rolverdeling wordt het model verder ontwikkeld en wordt beschreven hoe een WPKI geïmplementeerd kan worden. Het model dient ter ondersteuning om de probleemstelling te beantwoorden en is geen doel op zich. In de modelontwikkeling zijn dus twee fases te onderkennen.
Om een goed bruikbaar model te ontwikkelen is het belangrijk dat dit op een gestructureerde wijze gebeurt. Hiervoor gebruik ik de regulatieve cyclus van van Strien.
Het hoofddoel van het model is om antwoord te vinden op de probleemstelling uit hoofdstuk één. Een bijdoel van het model is om aan de betrokken partijen ondersteuning te bieden bij het implementeren van een wireless PKI. Het gebruik ervan zal afhangen van de taken die door de partij wordt uitgevoerd.
Als laatste zijn in dit hoofdstuk de aannames uit hoofdstuk één herhaald en een aantal aannames toegevoegd.

Hoofdstuk 6: Definiëren van het model om mobiele betrouwbaarheid te bieden

6.1 Inleiding

In hoofdstuk vijf heb ik de aanleiding gegeven waarom ik een model voor de mobiele vertrouwensmarkt ga ontwikkelen. Het model bestaat uit twee fases: het definiëren van de rolverdeling en het verder invullen van deze rolverdeling. Om tot een goede rolverdeling te komen, worden er eerst een aantal mogelijke scenario's gedefinieerd. Op basis van de theorie en de interviews wordt er dan een scenario gekozen, waarmee de modelontwikkeling wordt voortgezet. In deze tweede fase ontwikkel ik een soort checklist die als ondersteuning dient voor de gebruiker van het model. In deze checklist worden alle punten aangehaald die van belang zijn bij het implementeren van een WPKI. Ik heb al aangegeven dat het model hoofdzakelijk ontwikkeld is om de probleemstelling te beantwoorden, maar het is ook een handvat voor de gebruiker bij het implementeren van een WPKI.

6.2 Het bepalen van de rolverdeling in de mobiele vertrouwensketen

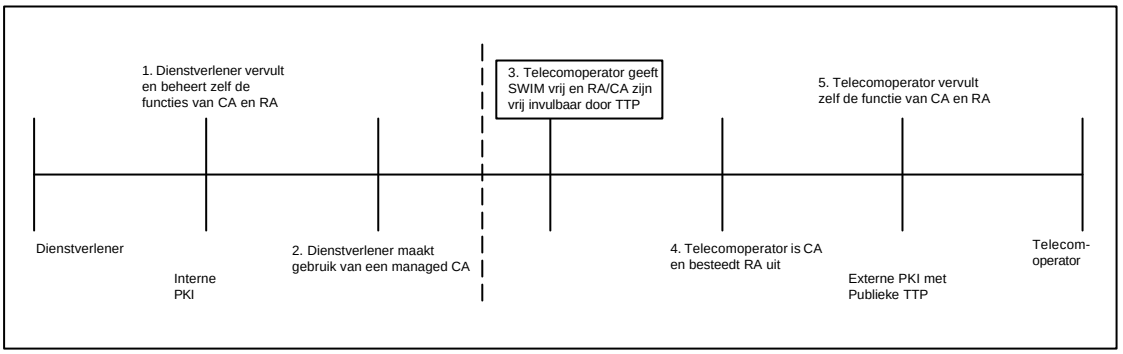
6.2.1 Het definiëren van de mogelijke scenario's

De mobiele markt is een zeer dynamische markt met veel verschillende spelers, die nog geen definitieve rol hebben gekozen. Daarom kan men op dit moment in de mobiele vertrouwensketen ook nog niet spreken van één mogelijke rolverdeling, er zijn verschillende scenario's mogelijk. Deze mogelijke scenario's zijn gebaseerd op de theorie die in hoofdstuk twee, drie en vier beschreven is, de geschetste uitdagingen uit hoofdstuk vijf en de meningen die uit de interviews naar voren zijn gekomen.
Bij het opstellen van de scenario's heb ik twee uitersten partijen uit de waardeketen genomen, de dienstverlener en de telecomoperator. Ik heb voor deze indeling gekozen omdat de dienstverlener de mobiele applicatie aanbiedt aan de eindgebruiker en dus het laatste contact met de eindgebruiker heeft. De dienstverlener kan de werkgever zijn die een mobiele applicatie aanbiedt aan zijn werknemer, B2E, of de dienstverlener biedt de dienst aan een ander bedrijf aan en dan is er sprake van B2B. De werknemer en het andere bedrijf zijn in dit geval de eindgebruiker. Om van de mobiele applicatie die de dienstverlener aanbiedt gebruik te kunnen maken, moeten de eindgebruikers beschikken over een mobiel certificaat. De telecomoperator heeft het eerste contact met de eindgebruiker en daarom staat de operator aan het andere uiterste van de scenario-indeling.
Een tweede reden om voor deze assenindeling te kiezen is de volgende: om een WPKI in een applicatie te implementeren, zijn er drie centrale spelers nodig die de volgende kernactiviteiten uitvoeren:

- Het aanbieden van de mobiele applicatie, dit gebeurt door de dienstverlener.
- Het aanbieden van de mobiele betrouwbaarheidsdiensten, zoals het uitgeven van mobiele certificaten. Deze taak wordt door de Trusted Third Party uitgevoerd.
- Het faciliteren van het mobiele netwerk, zodat de gebruiker en de dienstverlener met elkaar kunnen communiceren. Dit is een taak voor de telecomoperator.

In bovenstaande opsomming wijs ik nog geen rollen toe aan de partijen, er worden alleen een aantal kernactiviteiten geïdentificeerd. Een partij kan er natuurlijk ook voor

kiezen om alle kernactiviteiten zelf uit te voeren. Zo kan de telecomoperator ook optreden als TTP of dienstverlener.
In het onderstaande figuur zijn de verschillende scenario's weergegeven. Er zullen allicht nog meer scenario's mogelijk zijn, maar dit zijn slechts kleine afwijkingen van de hoofdscenario's die ik gedefinieerd heb. Deze subscenario's verschillen meer op basis van invulling van de scenario's dan dat het compleet andere scenario's zijn en zijn daarom niet als losstaande scenario's vermeld.



Figuur 6.1 Mogelijke scenario's in de mobiele vertrouwensketen

- *Scenario één*
  In dit scenario vervult de dienstverlener zelf de rol van de CA en RA. De dienstverlener moet uiteraard wel met de telecomoperator samenwerken om de certificaten op de certificaatdrager te zetten, die in het mobiele toestel zal zitten. De dienstverlener beheert zelf ook de infrastructuur die nodig is om de CA- en RA-functie te vervullen. Scenario één is een interne PKI.
- *Scenario twee*
  Het managed CA scenario is ook gebaseerd op een interne PKI. De dienstverlener vervult hierbij nog steeds de rollen van CA en RA, alleen het beheer van de CA is uit handen gegeven aan een externe partij. Dit betekent dat de CA technisch en fysiek ondergebracht is bij de service provider, de dienstverlener blijft juridisch de CA en is ook verantwoordelijk en aansprakelijk als CA. Om dit scenario te realiseren moet er wel weer worden samengewerkt met de telecomoperator. Dit scenario wordt in de vaste wereld door Roccade Megaplex op basis van Verisign-technologie aangeboden.
- *Scenario drie*
  Met scenario drie begeven we ons voor het eerst in een externe PKI met een publieke TTP. Dit scenario staat dichtbij het door publieke TTP's gehanteerde model in de vaste wereld. De telecomoperator speelt in dit scenario een faciliterende rol door een TTP toegang te geven tot de SWIM. In dit scenario is de 'traditionele' TTP de CA en kan de RA-functie door andere partijen of door de TTP zelf worden ingevuld. Deze partijen moeten natuurlijk wel vertrouwd worden door de CA en zijn vooraf geselecteerd door de CA.
  Een mogelijke invulling van dit scenario is, dat een TTP als DigiNotar de CA-functie vervuld en de RA-functie uitbesteed wordt aan een telecomoperator als KPN. In deze situatie is de 'traditionele' TTP de CA en vervult de telecomoperator de rol van RA. De invulling van de RA is sterk afhankelijk van het betrouwbaarheidsniveau waaraan de applicatie moet voldoen. Bij een hoog betrouwbaarheidsniveau zullen de RA- en CA-functie niet snel worden opgesplitst, omdat de CA eindverantwoordelijk is. Door gebruik te maken van dit scenario is het mogelijk om een mobiele PKI met

een publieke TTP te realiseren, waarbij de TTP in haar rol als CA verantwoordelijk en aansprakelijk is voor de uitgegeven certificaten.

- *Scenario vier*
  In dit scenario vervult de telecomoperator voor het eerst de rol van een publieke Trusted Third Party. De telecomoperator geeft zijn eigen mobiele certificaten uit en is dus ook verantwoordelijk en aansprakelijk voor de uitgegeven certificaten. In dit scenario heeft de operator de RA-functie uitbesteed. Er zijn een aantal mogelijke partijen die deze functie kunnen vervullen, bijvoorbeeld het verkooppunt van het mobiele apparaat, een notaris en eigenlijk iedere partij die door de telecomoperator vertrouwd wordt om deze belangrijke rol te vervullen. Zoals uit de figuur blijkt, leidt dit scenario ook tot een externe PKI met een publieke TTP.
- *Scenario vijf*
  De telecomoperator vervult in dit scenario zowel de rol van CA als RA en treedt op als een publieke Trusted Third Party. Het verschil met scenario vier is dat de operator nu ook de RA-functie vervult en de totale controle heeft over de geleverde betrouwbaarheidsdiensten.

Men zou kunnen zeggen dat scenario drie, vier en vijf veel op elkaar lijken en alleen op basis van de invulling van elkaar verschillen. Ik heb er echter toch voor gekozen om hiertussen een onderscheid te maken, omdat in deze scenario's de verschillende functies door totaal verschillende partijen vervuld worden en dit van grote invloed is op de verdere invulling van de rolverdeling.

6.2.2 De keuze van het scenario

Om fase twee van het model in te gaan en een invulling aan de rol van een Trusted Third Party te geven, is het noodzakelijk om één scenario als uitgangspunt te nemen. Dit is nodig om het model bruikbaar te maken, omdat er anders zeer veel opties en keuzemogelijkheden zijn en de gebruiker van het model zal verdwalen in de verschillende scenario's en keuzemogelijkheden.
Deze keuze is gebaseerd op de conclusies volgend uit de interviews en de bevindingen uit de hoofdstukken twee, drie, vier en vijf. Op basis van deze onderstaande conclusies, is scenario drie als uitgangspunt gekozen.

Conclusies op basis van de interviews
Omdat er nog grote onduidelijkheid is over de functieverdeling in de mobiele markt zijn de conclusies die uit de interviews met de verschillende partijen uit de markt naar voren zijn gekomen zeer belangrijk voor dit onderzoek. Door middel van deze interviews heb ik getracht om vanuit de markt meer duidelijkheid te krijgen omtrent de rolverdeling in met name de mobiele vertrouwensmarkt. Hieronder worden deze conclusies waarop de scenariokeuze gebaseerd is kort beschreven. Voor een volledig overzicht van de conclusies verwijs k naar bijlage B, waarin alle interviews zijn samengevat. In deze bijlage staat ook met welke partijen ik heb gesproken.

- *Voorsprong 'traditionele' TTP op basis van ervaring met vaste PKI*
  Uit de gesprekken met de verschillende partijen is duidelijk naar voren gekomen dat er ook in de mobiele wereld een rol is weggelegd voor de 'traditionele' TTP. Omdat de telecomoperator geen ervaring heeft met het opzetten van een PKI, hebben een aantal partijen hun twijfels over de geschiktheid van de telecomoperator om als CA en RA op te treden. Ze begeven zich dan in een voor hun geheel nieuwe markt, terwijl er al een aantal partijen zijn die hiermee wel ervaring hebben en dus een

voorsprong genieten ten opzichte van de telecomoperator en daarom waarschijnlijk beter geschikt zijn om ook in de mobiele wereld als TTP op te treden.

- *Plannen telecomoperator*
  Uit een gesprek met een grote telecomoperator is gebleken dat deze niet van plan is om de functies van CA en RA te gaan vervullen. Deze operator kiest ervoor om verschillende TTP's toegang te geven tot de SWIM en de operator speelt alleen een faciliterende rol. Deze benadering van de operator wordt in scenario drie weergegeven. De operator heeft voor deze benadering gekozen om de verschillende redenen die in deze paragraaf genoemd worden en omdat ze als gevolg van de UMTS-veilingen ook niet in de positie zitten om grote investeringen buiten hun core business te doen.
  Uit een aantal interviews is gebleken dat grote telecomoperators in Europa wel plannen hebben om als Trusted Third Party op te gaan treden. Dit onderzoek richt zich echter op de Nederlandse markt en aan de uitspraken van de binnenlandse telecomoperator zal het meeste waarde worden gehecht.
- *Praktijkvoorbeeld*
  Op dit moment zijn KPN, Nokia en Interpay een pilot-project gestart voor mobiel betalen. Hierin vervult Interpay de rol van RA en worden er Globalsign certificaten gebruikt. KPN en Nokia zijn de technische leveranciers die de toepassing mogelijk maken. In de toekomst wanneer de toepassing beschikbaar is voor de consumenten, gaan de banken de RA-functie vervullen. De financiële wereld is sowieso terughoudend om de RA-functie uit handen te geven, omdat de banken zelf de controle willen houden over hun klanten.
  De certificaten worden uitgegeven voor deze specifieke toepassing en de banken nemen dan ook geen verantwoordelijkheid voor het gebruik van deze certificaten voor andere toepassingen. De certificaten zijn alleen geschikt voor deze specifieke toepassing. De banken houden zelf de controle over de aanvraag en uitgifte van de certificaten. Bij deze processen wordt geen gebruik gemaakt van een publieke TTP. Als gevolg van deze twee redenen wordt in de toepassing gebruik gemaakt van een interne PKI.
  Wat deze pilot duidelijk maakt is dat de mobiele operator niet de intentie heeft om TTP-diensten te gaan leveren en deze functies door andere partijen uit de markt vervult kunnen worden.

Conclusies op basis van de theorie en eigen inzicht

- *Vergelijking met vertrouwensmarkt voor vast internet*
  Om een verwachting uit te spreken over ontwikkelingen in een nieuwe markt, is het altijd nuttig om een vergelijking te maken met een vergelijkbare markt waar deze ontwikkeling al heeft plaatsgevonden. In dit geval is dat de vertrouwensmarkt in de vaste internetwereld. In deze markt worden de betrouwbaarheidsdiensten geleverd door specialistische bedrijven als DigiNotar. De internet serviceproviders, die te vergelijken zijn met de mobiele operators, zijn in deze markt geen vertrouwensdiensten gaan leveren. Nu is de rol van een mobiele operator in de mobiele markt wel groter dan van de ISP in de vaste wereld, maar je kunt hieruit toch concluderen dat de mobiele operator zich waarschijnlijk niet in de mobiele vertrouwensmarkt zal begeven. KPN heeft in de vaste wereld wel een initiatief opgestart om digitale certificaten uit te geven, maar deze dienst is tot op heden nog niet echt succesvol geweest.

- *Beperkte betrouwbaarheid en onafhankelijkheid van de telecomoperator*
  Het leveren van betrouwbaarheidsdiensten behoort niet tot de kerntaken van een operator en je kunt je dus afvragen of een operator in staat is om diensten met hetzelfde betrouwbaarheidsniveau te leveren als een traditionele TTP en of alle partijen ook genoeg vertrouwen hebben in de kwaliteiten van de operator.
  In veel gevallen zal de operator ook mobiele diensten leveren. De onafhankelijkheid en onpartijdigheid wordt dan in twijfel getrokken als de operator ook digitale certificaten uitgeeft en zal het vertrouwen dat de gebruiker in de certificaten heeft afnemen. De onafhankelijkheid van een TTP is een zeer belangrijk criterium voor de vertrouwenswaarde die gebruiker hecht aan het uitgegeven certificaat.
- *Beperkte verantwoordelijkheid en aansprakelijkheid telecomoperator*
  Bij een 'traditionele' TTP behoort het leveren van betrouwbaarheidsdiensten tot de kerntaken van de onderneming en de aansprakelijkheid die hieruit voort vloeit is dan ook te verzekeren. De kerntaak van een mobiele operator is echter niet het leveren van betrouwbaarheidsdiensten en deze aansprakelijkheid is dus lastig tot niet te verzekeren, zie paragraaf 4.6. Dit brengt voor de operator een hoger risico met zich mee. De operator zal niet graag de aansprakelijkheid zelf willen dragen en dit kan hem doen besluiten om geen TTP-diensten te gaan verlenen. Indien de operator toch TTP-diensten gaat leveren is het nog maar de vraag hoeveel waarde de gebruikers hechten aan de aansprakelijkheid van de operator omdat deze hiervoor niet verzekerd is en dit komt het vertrouwen niet ten goede.
- *Voorsprong 'traditionele' TTP's op het gebied van certificering door toezichthoudende organen*
  In paragraaf 4.6 heb ik aangegeven dat er vanuit de markt een traject is opgestart om TTP's die aan bepaalde voorwaarde voldoen, een kwalititeitskeurmerk toe te kennen. Een bestaande TTP kan waarschijnlijk sneller aan deze voorwaarden voldoen dan een partij die nog moet beginnen met het opzetten van een PKI. Een Trusted Third Party die gecertificeerd is, komt betrouwbaarder over dan een TTP die niet gecertificeerd is en de gecertificeerde TTP zal dan een belangrijkere rol gaan spelen in de betrouwbaarheidsmarkt.
- *Overige eisen waaraan TTP moet voldoen*
  In paragraaf 4.6 behandel ik de eisen waaraan een Trusted Third Party moet voldoen. Een aantal van deze eisen zijn in deze paragraaf al aan bod gekomen, de nog niet behandelde eisen uit paragraaf 4.6 die van invloed zijn op de scenariokeuze zal ik nu behandelen. De deskundigheid en betrouwbaarheid van het personeel van een TTP bepalen mede de waarde die aan een certificaat kan worden gehecht. De 'traditionele' TTP heeft hier een voorsprong op de telecomoperator omdat het personeel al opgeleid is om op een nauwkeurige en vertrouwelijke wijze met alle gegevens om te gaan, zodat de diensten betrouwbaar zijn en de gebruiker ook vertrouwen heeft in de geleverde diensten en het personeel. Men kan zich afvragen of de dienstverlener en eindgebruiker wel voldoende vertrouwen hebben in de capaciteiten en betrouwbaarheid van bijvoorbeeld een medewerker van een verkooppunt van telefoons. Een telecomoperator zal ook een heel duidelijke functiescheiding moeten aanbrengen die voor een grote organisatie altijd lastig te controleren en te handhaven is.
- *Verschil tussen interne en externe PKI*
  Indien een onderneming gebruik wil maken van een PKI, moet de keuze gemaakt worden tussen een interne of een externe PKI. Een interne PKI houdt in dat de onderneming zijn eigen PKI opzet en dus optreedt als RA en CA. De certificaten zijn dan ook alleen bedoeld voor intern gebruik binnen de eigen toepassing. Omdat de

uitgevende partij niet aansprakelijk is voor extern gebruik van deze certificaten, zullen andere partijen niet vertrouwen op deze certificaten. Scenario één en twee maken gebruik van een interne PKI.
Bij een externe PKI wordt de PKI opgezet door een externe partij zoals DigiNotar. Die externe onafhankelijke derde partij treedt dan ook op als RA en CA en de uitgegeven certificaten kunnen daarom op basis van het CPS van de CA en de inhoud van het certificaat ook door andere partijen vertrouwd worden. Dit vertrouwen wordt gegarandeerd door de onafhankelijkheid van de derde partij.
Een externe PKI is complexer dan een interne PKI, omdat je bij een externe PKI met meerdere partijen moet samenwerken. Er zijn dan meer afhankelijkheden, onderlinge relaties en verschillende technieken en dit vergt meer afstemming. Dit maakt het ontwikkelen van een externe PKI een stuk complexer dan het ontwikkelen van een interne PKI. Door te kiezen voor een externe PKI kan ik een zo volledig mogelijk model ontwikkelen en dat komt de bruikbaarheid van het model alleen maar ten goede.

Zoals ik aan het begin van deze paragraaf al geconcludeerd heb, is scenario drie het meest geschikt om als uitgangspunt te dienen voor fase twee van de modelontwikkeling. Dit wil niet zeggen dat de overige scenario's niet voor kunnen komen, de scenario's kunnen goed naast elkaar bestaan in de markt. De voorkeur van de dienstverlener en de gebruiker zal uiteindelijk bepalen welk scenario doorbreekt. Maar op basis van bovengenoemde redenen kies ik ervoor scenario drie als uitgangspunt te nemen.

6.3 Het invullen van het gekozen scenario

Nu duidelijk is op basis van welk scenario het model verder ingevuld zal worden, kan bepaald worden hoe het model er verder uit gaat zien. Het doel van deze tweede fase van het model is om een invulling te geven aan het gekozen scenario.
Iedere toepassing heeft andere eisen qua beveiliging en betrouwbaarheidseisen, het is dus onmogelijk om één statisch model te ontwikkelen waarmee alle verschillende toepassingen benaderd kunnen worden. Daarom heb ik ervoor gekozen om een model te ontwikkelen dat de gebruiker van het model een handvat geeft bij het implementeren van een WPKI in een toepassing. In deze checklist liggen nog niet alle feiten vast en zijn er nog keuzes voor de gebruiker van het model. Ik heb deze keuzes bewust niet gemaakt omdat die keuzes onder andere afhankelijk zijn van de toepassing en de eisen die aan de betrouwbaarheid worden gesteld. Tevens is het opzetten van een WPKI voor alle partijen zeer nieuw en is er nog weinig ervaring mee opgedaan en is het daarom ook niet verstandig en realistisch om de keuzemogelijkheden zeer gedetailleerd in het model te gaan beoordelen. Dit kan beter aan de gebruiker van het model worden overgelaten. Uiteraard is het niet de bedoeling dat de gebruiker van het model kan kiezen uit zeer veel mogelijkheden omdat het model dan te breed wordt en aan functionaliteit zal inboeten. De kracht van een model zit naar mijn mening in het feit dat het model wel een bepaalde richting aangeeft, maar nog een beperkt aantal mogelijkheden open laat. In sommige gevallen heb ik daarom wel een keuze gemaakt. In deze gevallen bleek vanuit de markt dat er eigenlijk maar één oplossing mogelijk was en de overige mogelijke oplossingen geen reële opties waren. Om het model bruikbaar en overzichtelijk te houden heb ik deze irreële opties dan ook weggelaten.

6.3.1 De beoordelingscriteria

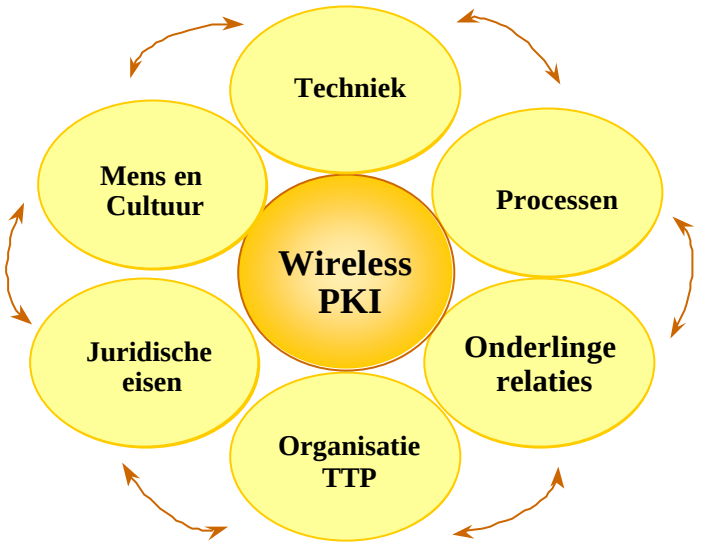
In de voorgaande paragraaf heb ik aangegeven dat het model nog een aantal keuzes openlaat. De gebruiker van het model moet hieruit een keuze maken, maar deze keuze moet natuurlijk wel goed onderbouwd zijn. De verschillende keuzemogelijkheden kunnen beoordeeld worden op basis van de onderstaande criteria. Deze lijst is echter niet uitputtend en dient alleen als richtlijn te worden gebruikt.
Bij iedere keuze moet er eigenlijk een afweging worden gemaakt tussen het gewenste betrouwbaarheidsniveau en onderstaande punten. Er is een continu spanningsveld tussen de betrouwbaarheidseisen en de overige eisen van de WPKI en er moet een goede balans gevonden worden tussen al deze eisen.

- *Technische en functionele eisen van de toepassing*
  De aard van de toepassing heeft implicaties op de keuze tussen de verschillende oplossingen. Voor bepaalde toepassingen is het bijvoorbeeld noodzakelijk dat de gebruiker de beschikking heeft over een soort van communicator en bij andere toepassingen kan een smartphone goed voldoen. De wensen en eisen van de eindgebruikers spelen hierbij natuurlijk ook een grote rol. Tevens hebben de gekozen oplossingen ook invloed op de performance van de toepassing en dit is natuurlijk een belangrijke factor voor het functioneren van de toepassing.
- *Betrouwbaarheidseisen waaraan de oplossing moet voldoen*
  De verschillende oplossingen hebben ieder andere eigenschappen die het betrouwbaarheidsniveau beïnvloeden en aangezien niet iedere toepassing dezelfde eisen heeft, moet dus de afweging worden gemaakt welke oplossing het meest geschikt is voor specifieke betrouwbaarheidseisen van de toepassing.
- *Gebruikersgemak*
  Voor de gebruiker is het van belang dat alle processen van aanvraag tot en met gebruik van het certificaat gebruikersvriendelijk zijn. Dit houdt in dat de gebruiker geen ingewikkelde ondoorzichtige procedures hoeft te doorlopen om een certificaat aan te vragen en te krijgen. Het gebruik van het certificaat moet niet veel handelingen van de gebruiker vergen, aangezien uit een onderzoek van Forrester is gebleken dat iedere benodigde extra handeling van de gebruiker het aantal transacties met 50% verlaagt.
- *Implementatie- en onderhoudsgemak*
  Sommige oplossingen zullen moeilijker te realiseren zijn dan andere oplossingen en kunnen problemen met zich meebrengen met het onderhoud van de toepassing indien er zich kleine wijzigingen in de toepassing voordoen. Hier draait het dus om het gemak van de implementatie en beheer van de toepassing.
- *Budget*
  Voor het realiseren van een WPKI is waarschijnlijk geen onuitputtelijke pot geld beschikbaar en er zullen dus afwegingen gemaakt moeten worden tussen de kosten van een oplossing en de invloed van die oplossingen op bovengenoemde beoordelingspunten.

6.3.2 De gekozen invalshoeken onderverdeeld in hoofdgroepen

Het opzetten van een WPKI is een zeer complex proces, om een juist handvat te geven, moet het model wat ik hier ontwikkel dus zeer volledig zijn. De keuze van de invalshoeken waarmee ik de invulling van de rolverdeling definieer is dan ook zeer belangrijk. De invalshoeken zijn in een aantal hoofdgroepen verdeeld waarin de gedetailleerde oplossingen en keuzemogelijkheden behandeld worden. Omdat de

hoofdgroepen en de invulling daarvan zo belangrijk zijn heb ik binnen DigiNotar met iedere consultant de hoofdgroepen en de invulling daarvan besproken. Op deze wijze heb ik een zo volledig mogelijke checklist ontwikkeld.
In het onderstaande figuur zijn de verschillende hoofdgroepen terug te vinden.



.
Figuur 6.2 Indeling van de invalshoeken

Op basis van deze indeling in de zes hoofdgroepen wordt het model verder ingevuld. Zoals uit de figuur blijkt, is iedere groep van invloed op andere groepen. Er is geen echt begin en eind in deze cyclus te ontdekken en het invullen van deze groepen is een continu proces van wisselwerking tussen de verschillende groepen.
Ik zal hier eerst kort uitleggen wat onder elke hoofdgroep wordt verstaan en waarom ik voor deze indeling heb gekozen en welke groepen het meest bepalend zijn voor het invullen van de groepen.

- *Techniek*
  De techniek is van belang omdat de techniek voor een groot deel de uiteindelijke oplossing bepaald en daarom veel invloed heeft op de overige factoren. Veel factoren uit de techniek zijn vanuit de markt een vaststaand feit en hier kan een TTP weinig aan veranderen, de TTP heeft alleen een aantal keuzes uit de mogelijke technieken. Ik zal dan ook niet zeer gedetailleerd op de techniek in gaan en alleen de mogelijke keuzes aangeven. Onder de techniek vallen de technische beslissingen over bijvoorbeeld de certificaatdrager en het sleutelalgoritme, alsmede de technische eisen en specificaties van de applicatie die gebruik gaat maken van een WPKI.
- *Processen*
  Onder de processen worden onder andere de registratie-, uitgifte- en validatieprocessen verstaan. De processen zijn de meest bepalende factoren van een PKI of WPKI, daarom hebben de procesbeschrijvingen zeer veel invloed op de andere factoren van de checklist en bepalen voor een groot gedeelte hoe deze checklist ingericht moet worden. Zo wordt bijvoorbeeld in de procesbeschrijvingen

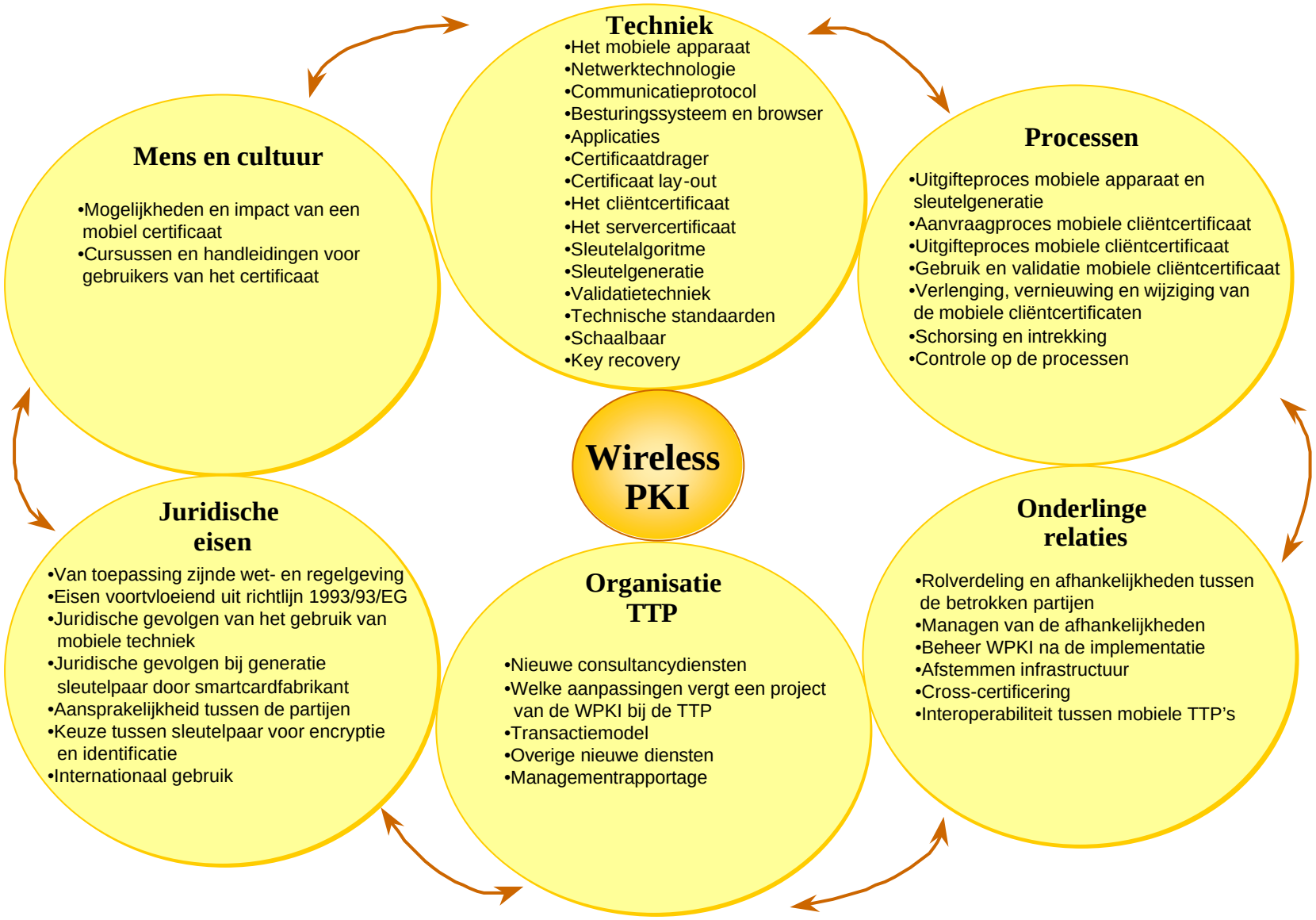
duidelijk welke partijen er betrokken zijn bij het gebruik van een certificaat en dit bepaalt voor een groot gedeelte de invulling van de hoofdgroep 'Onderlinge relaties'. De procesbeschrijvingen zullen dan ook een centrale rol spelen in deze checklist en zeer uitgebreid behandeld worden.

- *Onderlinge relaties*
  Vanuit de processen en techniek wordt duidelijk dat er bij een WPKI door verschillende partijen samengewerkt moet worden en er onderlinge afhankelijkheden zijn. De afhankelijkheden die uit de processen voortvloeien worden hier verder uitgewerkt. Tevens worden de gevolgen van de afhankelijkheden besproken en hoe men het beste met deze afhankelijkheden kan omgaan, zodat de risico's van de onderlinge afhankelijkheden zo laag mogelijk gehouden kunnen worden.
- *Organisatie TTP*
  Hier worden de veranderingen voor de organisatie van de TTP zelf behandeld. Er zullen natuurlijk een aantal veranderingen veroorzaakt worden door de opstartbeslissingen, maar iedere nieuwe toepassing kan ook weer zijn invloed hebben op de TTP en deze invloeden worden hier behandeld. Tevens wordt onder andere het transactiemodel op basis waarvan de TTP haar inkomsten genereert behandeld.
- *Juridische eisen*
  Bij de onderlinge verhoudingen zijn een aantal afhankelijkheden gedefinieerd en de relaties en aansprakelijkheden die hieruit voortvloeien, moeten natuurlijk juridisch vastgelegd zijn. Bij het implementeren van een WPKI komen ook nog veel andere juridische eisen kijken, zoals het voldoen aan de Europese richtlijnen. Alle juridische implicaties waarmee men rekening moet houden bij het opzetten van een WPKI worden hier behandeld.
- *Mens en cultuur*
  De mogelijkheden en de implicaties van het werken met mobiele certificaten moeten duidelijk worden gemaakt aan zowel de dienstverlener als de gebruiker. Mensen moeten er bewust van zijn dat een elektronische handtekening op basis van het mobiele certificaat gelijkwaardig is aan een geschreven handtekening. De mogelijkheden en implicaties hiervan worden in deze groep behandeld.

Bovenstaande zes invalshoeken en de invulling daarvan zijn tot stand gekomen door alle informatie uit de interviews en de gesprekken met de consultants van DigiNotar met elkaar te combineren. Door deze combinatie is het mogelijk om een zo volledig mogelijk checklist te ontwikkelen waarmee alle betrokken partijen naar mijn inziens in staat zijn om de juiste beslissingen te nemen bij het implementeren van een WPKI.

6.3.3 De checklist

In de checklist worden alle hoofdgroepen zoals die in paragraaf 6.3.2 gedefinieerd zijn verder ingevuld. De checklist is het model dat uiteindelijk als handvat gebruikt gaat worden om een WPKI te implementeren en waarmee de TTP een invulling kan geven aan haar rol. Een checklist van een aantal pagina's is natuurlijk niet handig te gebruiken. Daarom heb ik ervoor gekozen om de checklist echt als een checklist op te nemen. De checklist wordt in bijlage A zeer uitgebreid besproken. Naarmate de gebruiker het model vaker gebruikt, zal deze minder behoefte hebben aan de uitgebreide beschrijving en heeft de gebruiker voldoende aan de checklist zoals die in deze paragraaf gegeven wordt.


Techniek
•Het mobiele apparaat
•Netwerktechnologie
•Communicatieprotocol
•Besturingssysteem en browser
•Applicaties
•Certificaatdrager
•Certificaat lay-out
•Het cliëntcertificaat
•Het servercertificaat
•Sleutelalgoritme
•Sleutelgeneratie
•Validatietechniek
•Technische standaarden
•Schaalbaar
•Key recovery
Mens en cultuur
•Mogelijkheden en impact van een mobiel certificaat
•Cursussen en handleidingen voor gebruikers van het certificaat
Processen
•Uitgifteproces mobiele apparaat en sleutelgeneratie
•Aanvraagproces mobiele cliëntcertificaat
•Uitgifteproces mobiele cliëntcertificaat
•Gebruik en validatie mobiele cliëntcertificaat
•Verlenging, vernieuwing en wijziging van de mobiele cliëntcertificaten
•Schorsing en intrekking
•Controle op de processen
Wireless PKI
Juridische eisen
•Van toepassing zijnde wet- en regelgeving
•Eisen voortvloeiend uit richtlijn 1993/93/EG
•Juridische gevolgen van het gebruik van mobiele techniek
•Juridische gevolgen bij generatie sleutelpaar door smartcardfabrikant
•Aansprakelijkheid tussen de partijen
•Keuze tussen sleutelpaar voor encryptie en identificatie
•Internationaal gebruik
Organisatie TTP
•Nieuwe consultancydiensten
•Welke aanpassingen vergt een project van de WPKI bij de TTP
•Transactiemodel
•Overige nieuwe diensten
•Managementrapportage
Onderlinge relaties
•Rolverdeling en afhankelijkheden tussen de betrokken partijen
•Managen van de afhankelijkheden
•Beheer WPKI na de implementatie
•Afstemmen infrastructuur
•Cross-certificering
•Interoperabiliteit tussen mobiele TTP's

6.4 Samenvatting

Om tot een goede scenariokeuze te komen heb ik een vijftal scenario's gedefinieerd. Deze scenario's zijn onder andere gebaseerd op het feit dat om een betrouwbare mobiele applicatie te creëren er drie kernactiviteiten uitgevoerd moeten worden. Dit zijn: het aanbieden van de mobiele applicatie, het aanbieden van de mobiele betrouwbaarheidsdiensten en het faciliteren van het mobiele netwerk. Op basis van de theorie, interviews en eigen inzicht heb ik scenario drie gekozen om de volgende fase van de modelontwikkeling in te gaan.
In deze tweede fase heb ik een checklist ontwikkeld die als handvat gebruikt kan worden tijdens het implementeren van een WPKI. De checklist is onderverdeeld in de volgende categorieën:

- Techniek
- Processen
- Onderlinge relaties
- Organisatie TTP
- Juridische eisen
- Mens en cultuur

In de checklist worden per categorie aandachtspunten gegeven die van belang zijn bij het implementeren van een WPKI. De checklist is geen gedetailleerde standaardoplossing, maar geeft de gebruiker een handvat bij het nemen van de beslissingen bij het implementeren van een WPKI. In paragraaf 6.3.1 zijn een aantal beoordelingscriteria gegeven, die als hulpmiddel dienen bij het maken van de verschillende keuzes. Met deze checklist wordt invulling gegeven aan het geselecteerde scenario.

Hoofdstuk 7: Toetsing van het model

7.1 Inleiding

Een belangrijk aspect bij modelontwikkeling is de toetsing van het model. Wanneer je een model ontwikkelt moet natuurlijk nagegaan worden of het model juist is en dit kan bereikt worden door het model te toetsen. De toetsingsfase speelt een belangrijke rol in de regulatieve cyclus die ik in paragraaf 5.4 beschreven heb. In dit hoofdstuk wordt eerst uitgelegd waaraan het model getoetst wordt en vervolgens zal ik de methodiek van toetsing toelichten. Hierna wordt overgegaan tot de toetsing van het model en worden de resultaten besproken.

7.2 Toetsingsmateriaal

In een ideale situatie wordt het model aan een echte applicatie getoetst. Op deze wijze kan een model goed vergeleken worden met oplossingen uit de praktijk en kan men de verschillen analyseren. Voor dit onderzoek houdt dit in dat het model getoetst moet worden aan een applicatie die al gebruik maakt voor een WPKI. Het vinden van zo'n applicatie is juist het probleem. Ik heb al aangegeven dat de mobile commerce markt nog zeer nieuw is en in de kinderschoenen staat. Op dit moment zijn er dan ook geen B2B of B2E applicaties beschikbaar waaraan ik mijn model kan toetsen. Een aantal bedrijven ontwikkelen op dit moment wel dergelijke applicaties, maar die zijn nog niet operationeel en zijn ook niet beschikbaar voor de toetsing. Op dit moment is de in hoofdstuk twee beschreven toepassing van de Postbank en Telfort wel operationeel, maar deze was niet beschikbaar voor de toetsing. Tevens is deze toepassing ook niet ideaal voor de toetsing omdat hier niet gewerkt wordt met een publieke TTP en externe PKI.
Het toetsingmateriaal is nu via Baltimore Technologies verkregen. Voor een beschrijving van deze onderneming verwijs ik naar de bijlage waarin de interviews worden behandeld. Baltimore heeft van een mobiele telecomoperator een "Request for Proposal (RFP)" ontvangen. Baltimore heeft hierop geantwoord middels een voorstel hoe zij de WPKI bij deze operator in zouden richten. Het antwoord van Baltimore op dit RFP is een soort van pre-functioneel ontwerp en is daarom geschikt als toetsingsmateriaal. Het is een algemeen ontwerp onafhankelijk van B2C of B2B/B2E. Het voorstel richt zich dus niet specifiek op één applicatie, maar geeft aan hoe de operator een WPKI kan inrichten. Ik heb het model ook besproken met een expert op het gebied van WPKI bij Baltimore.

7.3 Toetsingsmethode

Het voorstel van Baltimore behandelt de volgende aspecten van een WPKI:
- Personalisatie van de smartcard;
- Registratie en uitgifte van de certificaten;
- Uitvoeren van transacties op basis van de certificaten;

Op basis van bovenstaande punten heeft Baltimore een mogelijke rolverdeling voor de vertrouwensketen gedefinieerd. De rolverdeling en de drie punten komen ook in het ontwikkelde model naar voren. Als toetsingsmethode ga ik de verschillen tussen het voorstel van Baltimore en het model opsporen en analyseren. Bij de analyse geef ik aan of ik het model aanpas aan de hand van de gevonden verschillen. Indien ik het model niet aanpas, geef ik aan waarom ik ervoor kies om mijn model te handhaven. Na dit hoofdstuk ga ik niet opnieuw een model definiëren, maar worden de aanpassingen doorgevoerd in het model uit hoofdstuk zes. Ik zal bij het bespreken

van de resultaten wel aangeven welke aanpassingen ik aan het model gemaakt heb op basis van de toetsing.
Met bovenstaande punten kan ik niet het gehele model toetsen. De overige punten van de checklist worden niet besproken in het voorstel van Baltimore. Om toch na te gaan of de checklist klopt en volledig is, heb ik deze besproken met een expert van Baltimore. Tevens is de checklist ook uitvoerig besproken met de consultants van DigiNotar. Op deze wijze heb ik de gehele checklist op een juiste wijze kunnen toetsen. Ook hier zal ik aangeven welke punten in de checklist gewijzigd zijn op basis van de toetsing.

7.4 Resultaten van de toetsing

Rolverdeling
Baltimore ziet de mobiele telecomoperator als een geschikte partij om de vertrouwensfunctie op zich te nemen en de operator vervult in dit scenario de RA en CA-functie. De reden hiervoor is dat de operator al een relatie met de klant heeft en een unieke partij is. Zoals al gebleken is uit hoofdstuk zes ben ik het hier niet helemaal mee eens. De operator heeft inderdaad een relatie met de klant, maar een 'traditionele' TTP kan diensten met een hoger betrouwbaarheidsniveau leveren dan de operator. Ik blijf er dan ook bij om scenario drie als uitgangspunt te nemen voor dit onderzoek. Dit wil niet zeggen dat er geen meerdere scenario's naast elkaar kunnen bestaan. Volgens een presentatie van een smartcardfabrikant is er een grote kans dat er meerdere scenario's naast elkaar zullen bestaan. Zeer waarschijnlijk zullen scenario vier of vijf dan ook uitgevoerd gaan worden. Ik denk dat de dienstverlener een keuze zal maken tussen deze drie scenario's op basis van het geëiste betrouwbaarheidsniveau, waarbij scenario drie het hoogste betrouwbaarheidsniveau zal bieden. Het is misschien ook wel logisch dat Baltimore de operator als TTP ziet, aangezien de RFP door een operator is ingediend.
Dat de operator in het voorstel van Baltimore als TTP gezien wordt, heeft natuurlijk ook gevolgen voor het vervolg van de toetsing, aangezien in alle processen de operator de TTP is. Daarom zal ik bij de verdere toetsing dit verschil niet meenemen.

Personalisatie van de smartcard
Baltimore gebruikt ongeveer dezelfde oplossing als in het model is gedefinieerd. Bij Baltimore stuurt de TTP de PKI file met daarin de eisen voor de SWIM naar de smartcardfabrikant. In het model gebeurt dit door de dienstverlener in overleg met de TTP. Ik denk dat dit verschil te rechtvaardigen valt omdat de dienstverlener vaak ook een speciaal mobiel toestel nodig heeft en deze bestelling ook zelf zal doen. De bestelling van toestel en SWIM zal gecombineerd worden. Het verschil met Baltimore is echter niet groot omdat de dienstverlener de keuze zal baseren op het advies van de TTP.
Een ander verschil is dat in het model het verzoek richting de telecomoperator gaat en bij Baltimore gaat dit rechtstreeks naar de smartcardfabrikant. Dit verschil wordt veroorzaakt doordat bij Baltimore de TTP ook de operator is. De dienstverlener en de TTP moeten zich tot de operator richten, omdat deze tot op zekere hoogte bepaalt welke gegevens er op de SWIM komen. Dit verschil wordt niet in het model aangepast.
Volgens Baltimore wordt het certificaatURL door de smartcardfabrikant op de SWIM gezet. In het model gaf de CA het URL door aan de operator die het vervolgens doorstuurde naar de SWIM van de gebruiker. Aangezien een CA op dit moment geen invloed heeft op dit technische proces, heb ik dit aangepast in het model.
In het model behandel ik het toesturen van de pincode om de privé-sleutel te activeren. In het voorstel van Baltimore wordt hierover niet gesproken en dit heb ik dan ook niet kunnen toetsen.

Registratie
In het model heb ik aangegeven dat de functie van RA nog open is, afhankelijk van het geëiste betrouwbaarheidsniveau. De RA kan dus ook door een winkel van de operator worden uitgevoerd zoals Baltimore aandraagt.
In het voorstel van Baltimore moet de gebruiker met zijn toestel naar de winkel van de operator toe om daar de certificaataanvraag te doen. De verkoper voert daar de benodigde gegevens in en deze worden op een veilige wijze elektronisch verstuurd naar operator die de RA-functie uitvoert. De RA voert dan de gebruikelijke controles uit en bij een positief resultaat geeft de RA de CA opdracht om een certificaat uit te geven.
In het model gebeurt het registratieproces op een andere wijze. Hier vraagt de dienstverlener een certificaat aan voor de gebruiker (haar werknemer). Dit verschil wordt veroorzaakt doordat het model zich richt op de B2B en de B2E markt en het voorstel van Baltimore markt onafhankelijk is. In het DigiNotar model uit paragraaf 4.4.2 worden de certificaten ook door de dienstverlener aangevraagd, dus dit wordt ook gehandhaafd in het ontwikkelde model. De RA moet onder andere controles uitvoeren op basis van gegevens die de operator heeft. Omdat bij Baltimore de operator de RA is, is deze stap niet beschreven. In het model wordt de database met de gegevens beheerd door de operator, het is eventueel ook mogelijk dat de database beheerd wordt door de RA en de operator hiervoor de gegevens aanlevert. Hierover zal pas duidelijkheid ontstaan wanneer de oplossing besproken wordt met een operator. Hier moet het model worden aangepast en moet aangegeven worden dat de database ook door de RA beheerd kan worden.
In het model hoeft de certificaataanvraag niet direct bij aanschaf van het mobiele toestel te gebeuren. Daarom moet er wel een techniek gebruikt die aantoont dat de rechtmatige gebruiker ook daadwerkelijk de beschikking heeft over het sleutelpaar. Dit is anders dan bij Baltimore, maar dit verschil is logisch aangezien de gebruiker niet bij de RA hoeft te verschijnen.

Uitgifte
In beide gevallen krijgt de CA van de RA de opdracht en de benodigde gegevens om een certificaat uit te geven. Bij de personalisatie is al een verschil aan bod gekomen over het certificaatURL. In het model is aangegeven dat de CA een URL naar de operator stuurt en die stuurt het vervolgens naar de SWIM van de gebruiker. Op basis van de oplossing van Baltimore wordt dit aangepast. De CA zet het certificaat op een vooraf gedefinieerde locatie, zoals is aangegeven op de SWIM.

Uitvoeren transacties op basis van de certificaten
Zoals in het model is beschreven verschilt dit proces niet bijzonder veel van de vaste wereld. Er zijn geen verschillen te ontdekken tussen de oplossing van Baltimore en het ontwikkelde model.

Overige punten uit het model
In de checklist worden nog veel andere punten besproken die niet in het voorstel van Baltimore zijn meegenomen. Om deze punten toch te kunnen toetsen, heb ik hierover contact gehad met de expert van Baltimore. Met hem is de indeling van de hoofdgroepen besproken en deze waren juist. Tevens heb ik de invulling van de hoofdgroepen met hem besproken. Hieruit kwam naar voren dat het op dit moment niet mogelijk is om met het mobiele apparaat een digitale handtekening te valideren. Dit bevestigt de uitspraken die hierover in het model worden gedaan.
Dat de overige punten van het model niet in het voorstel van Baltimore worden behandeld, geeft aan dat er in de markt nog vele vraagtekens zijn over het inrichten van een WPKI. Het is dan ook onmogelijk om te concluderen dat de checklist volledig is. Op basis van de gesprekken met de consultants van DigiNotar en het gesprek met Baltimore kan wel geconcludeerd worden dat de checklist de meest essentiële punten van een WPKI bevat.

7.5 Bruikbaarheid van het model op basis van de toetsing en eigen inzicht

Bij het ontwikkelen van het model zijn de B2B markt en de B2E markt als uitgangspunt genomen. De oplossing van Baltimore is markt onafhankelijk gedefinieerd. Dit geeft aan dat een eerste ontwerp voor een WPKI niet gebonden hoeft te zijn aan een specifieke markt.
Als men naar het uiteindelijke model kijkt, dan kun je concluderen dat het model zeer goed bruikbaar is voor de B2B of de B2E markt. Hiermee voldoet het model aan de doelstelling uit paragraaf 5.5.1 Maar hier houdt de bruikbaarheid van het model nog niet op. Naar mijn inziens is het model niet echt marktafhankelijk en kan het model ook gebruikt worden als uitgangspunt voor de B2C markt. De scenario's en de checklist zijn zo opgesteld dat er geen marktafhankelijke factoren in staan. De beoordelingscriteria zullen ook grotendeels hetzelfde zijn, alleen de manier waarop met die criteria wordt omgegaan zal verschillen. Doordat de markten van elkaar verschillen zal aan sommige criteria meer of minder belang worden gehecht en kunnen de keuzes van elkaar verschillen.
Het model moet dan waarschijnlijk wel op een aantal punten worden aangepast, maar hierover kan ik op dit moment geen uitspraken doen aangezien ik de consumentenmarkt niet heb onderzocht. Ik heb scenario drie gekozen om de tweede fase van het model in te gaan. Tijdens deze keuze heb ik aangegeven dat een externe PKI de meest complexe vorm van een PKI is. In scenario drie worden de TTP-diensten door een 'traditionele' TTP uitgevoerd en niet door de telecomoperator. Als gevolg van die rolverdeling is er een intensieve samenwerking noodzakelijk tussen de TTP en de telecomoperator. Hierdoor kan scenario drie als de meest complexe externe WPKI gezien worden. Omdat de checklist gebaseerd is op dit meest complexe scenario kan verondersteld worden dat de checklist zo volledig mogelijk is. Als gevolg van deze volledigheid is de checklist waarschijnlijk ook geschikt om de overige scenario's te benaderen. Weliswaar zal de checklist op een aantal punten moeten worden aangepast, maar net zoals bij de B2C markt, is het een goed uitgangspunt om de overige scenario's te benaderen.

7.6 Samenvatting

Tijdens de zoektocht naar een toetsingsapplicatie werd duidelijk dat er eigenlijk nog geen mobiele B2B of B2E applicaties op de markt zijn die gebruik maken van een WPKI. Daarom heb ik de toetsing uitgevoerd in samenwerking met Baltimore. Zij hebben een eerste ontwerp voor een WPKI opgestuurd op basis waarvan ik het in dit onderzoek ontwikkelde model kon toetsen. Omdat niet het hele model aan het voorstel van Baltimore getoetst kon worden, heb ik het model ook besproken met een expert van Baltimore op het gebied van WPKI.
Ik heb het model met de oplossing van Baltimore vergeleken en de gevonden verschillen geanalyseerd. Wanneer het nodig was om het model aan te passen, heb ik dit in hoofdstuk zes gedaan. Ik heb dus geen nieuw model ontwikkeld, deze wijzigingen heb ik wel in dit hoofdstuk aangegeven. Op basis van de toetsing is gebleken dat het model maar op een aantal punten moet worden aangepast. In de oplossing van Baltimore worden niet alle punten uit het model behandeld, dit geeft aan dat de marktpartijen nog druk bezig zijn met het uitwerken van de WPKI.
Het model is ontwikkeld voor de B2B en de B2E markt, maar nu blijkt dat het model na een paar aanpassingen waarschijnlijk ook toepasbaar zal zijn voor de B2C markt. Deze gedachtegang geldt ook voor de scenario's. Omdat scenario drie zo complex is, kan de checklist ook gebruikt worden om de overige scenario's te benaderen. Ook hiervoor zullen waarschijnlijk een paar aanpassingen nodig zijn, maar dit vergt verder onderzoek.

Hoofdstuk 8: Conclusies en aanbevelingen

8.1 Inleiding

In dit afsluitende hoofdstuk worden alle bevindingen uit de voorgaande hoofdstukken besproken. Dit vindt plaats aan de hand van de onderzoeksvragen die in hoofdstuk één van de probleemstelling afgeleid zijn. Vervolgens kom ik dan tot de slotconclusie en wordt de probleemstelling beantwoord. Ook worden er nog een aantal aanbevelingen voor vervolgonderzoek gegeven.

8.2 Conclusies

Het doel van dit onderzoek was om een antwoord te vinden op onderstaande, in hoofdstuk één gedefinieerde probleemstelling.

"Welke rol heeft een Trusted Third Party bij het bevorderen van het vertrouwen en de veiligheid bij het realiseren van mobiele transacties voor B2B en B2E m-commerce en hoe kan een TTP invulling geven aan deze rol?"

Om op deze probleemstelling een antwoord te vinden, heb ik de probleemstelling in een aantal onderzoeksvragen opgesplitst. Deze onderzoeksvragen zullen nu afzonderlijk behandeld worden aan de hand van de bevindingen uit de voorgaande hoofdstukken.

De eerste onderzoeksvraag luidde als volgt: *"Wat zijn de mogelijkheden van m-commerce?"* Deze vraag is in hoofdstuk twee beantwoord.
Door de unieke eigenschappen van de mobiele techniek kunnen er applicaties ontwikkeld worden die met e-commerce niet mogelijk zijn. Deze onderscheidende kenmerken zijn: anyplace, anytime, personalisatie, locatie en push gebaseerde diensten. Op dit moment zijn er nog veelal technologische beperkingen van toepassing bij mobile commerce. Deze kunnen uitgesplitst worden naar beperkingen van het toestel en het mobiele netwerk. Deze beperkingen zijn van invloed op de mogelijkheden van m-commerce. Mobile commerce moet dan ook op dit moment niet gezien worden als een vervanging van e-commerce, maar als een uitbreiding. Om mobile commerce tot een succes te maken, moeten er applicaties ontwikkeld worden die rekening houden met de beperkingen en gebruik maken van de zojuist genoemde onderscheidende kenmerken. Uit dit onderzoek is gebleken dat de mobiele markt nog volop in ontwikkeling en beweging is en dat het lastig is om een voorspelling te doen over de doorbraak van mobile commerce. Het lijkt erop dat we in ieder geval moeten wachten totdat GPRS haar intrede heeft gedaan. Wanneer deze technologie haar intrede heeft gedaan en mobile commerce doorbreekt, zal er in de B2B en B2E markt voor het eerst de behoefte ontstaan aan betrouwbare mobiele toepassingen.

Om te bepalen wat de rol van de TTP is in de mobiele vertrouwensmarkt, moeten eerst de stakeholders bij mobile commerce gedefinieerd worden. Dit was de doelstelling van de tweede onderzoeksvraag. De volgende stakeholders zijn in hoofdstuk twee gedefinieerd: Technology platform vendors, Infrastructure equipment vendors, Application platform vendors, Application developers, Content providers, Mobiele portals, Mobiele netwerk operators, Hardware producenten en de gebruikers. Als gevolg van de ontwikkelingen in de mobiele markt is er een spanningsveld aanwezig bij bedrijven tussen enerzijds opschuiven in de waardeketen en anderzijds bij je core business blijven.

"Welke betrouwbaarheidseisen worden er aan een mobiele transactie gesteld?" was de derde onderzoeksvraag. Bij e-commerce zijn een aantal standaard betrouwbaarheidseisen van toepassing: Authenticatie, Integriteit, Vertrouwelijkheid en Onweerlegbaarheid. Met mobile commerce kunnen dezelfde transacties gerealiseerd worden als bij e-commerce, logischerwijs kan gesteld worden dat dezelfde eisen dan van toepassing zijn. Welk niveau van vertrouwen geëist wordt hangt niet van het gebruikte medium af, maar van de (vertrouwens)waarde van de transactie. De van toepassing zijnde wet- en regelgeving wijkt voor mobile commerce niet af van e-commerce. De invulling hiervan zal wel anders zijn, omdat de mobiele techniek andere eigenschappen heeft ten opzichte van het vaste internet. Om aan de betrouwbaarheidseisen te voldoen, moet men beschikken over een digitale identiteit.

De vierde onderzoeksvraag luidde als volgt: *"Welke technieken en diensten zijn er in de vaste wereld mogelijk om aan de betrouwbaarheidseisen te voldoen zoals die uit de vorige onderzoeksvraag naar voren zijn gekomen?"* Cryptografie is een belangrijke techniek om elektronisch berichtenverkeer te beveiligen. Asymmetrische of hybride encryptie zijn de meest geschikte technieken om te gebruiken. Hierbij wordt er gebruik gemaakt van een sleutelpaar. Om aan de vier betrouwbaarheidseisen te voldoen, moet dit sleutelpaar aan een fysieke identiteit gekoppeld worden. Hier ligt de taak voor een Trusted Third Party, hiervoor wordt gebruik gemaakt van een digitaal certificaat. De TTP geeft onder een aantal voorwaarden een certificaat uit aan de gebruiker. Partijen die een belangrijke rol spelen hierbij zijn: Registration Authority, Certification Authority, Authorizing Authority en de gebruiker.

De vijfde onderzoeksvraag luidde als volgt: *"Wat zijn de uitdagingen als de technieken en diensten uit bovenstaande onderzoeksvraag gebruikt gaan worden in de mobiele wereld?"* Er zijn twee redenen waarom het leveren van mobiel vertrouwen anders zal zijn dan in de vaste wereld. De eerste reden is dat als gevolg van de technologische beperkingen van mobile commerce er andere technieken gebruikt moeten worden dan in de vaste wereld. De tweede reden wordt veroorzaakt doordat de mobiele markt anders is dan de vaste markt. In de mobiele markt speelt de telecomoperator een zeer grote rol en daarom moeten een aantal processen anders ingericht worden. Deze uitdagingen leveren een aantal kansen en bedreigingen op voor de 'traditionele' TTP. Een belangrijke kans is dat er een geheel nieuwe afzetmarkt is ontstaan met zeer veel mogelijkheden. De bedreiging hierbij is dat de mobiele operator de vertrouwensfunctie gaat vervullen en er geen rol is weggelegd voor de 'traditionele' TTP.

De zesde onderzoeksvraag luidde als volgt: *"Wat wordt de rolverdeling tussen de verschillende partijen in de betrouwbaarheidsmarkt voor mobile commerce?"* Bij het creëren van een betrouwbare mobiele toepassing moeten de volgende drie kerntaken worden uitgevoerd: aanbieden van de mobiele applicatie, faciliteren van het mobiele netwerk en het leveren van de mobiele betrouwbaarheidsdiensten. Op basis van deze taken en de centrale spelers zijn er vijf mogelijke scenario's gedefinieerd. Om een antwoord op de laatste onderzoeksvraag te vinden is het noodzakelijk om één scenario te kiezen. Op basis van de interviews en de theorie heb ik scenario drie gekozen. In scenario drie vervult de 'traditionele' TTP de vertrouwensfunctie en faciliteert de telecomoperator ruimte op de SWIM en het mobiele netwerk. Een belangrijke eigenschap van scenario drie is dat dit het meest complexe scenario is. Deze keuze wil niet zeggen dat de overige scenario's niet mogelijk zijn, de scenario's kunnen ook naast elkaar bestaan. Dit is grotendeels afhankelijk van de wens van de gebruiker. Op dit moment hebben de telecomoperators niet de financiële middelen om investeringen buiten hun core business om te doen en laten het implementeren van een WPKI over aan de

specialistische partijen. De outsource beslissing wordt dus mede veroorzaakt door de conjunctuur. Omdat het in deze markt moeilijk is om een aantal jaren vooruit te kijken, is het model ontwikkeld met een focus van ongeveer twee jaar. Uiteraard is wel geprobeerd het model zoveel mogelijk tijdsonafhankelijk te houden.

De laatste onderzoeksvraag luidde als volgt: *"Hoe moet de TTP haar gehele PKI-platform, zoals de interne processen en de processen richting de betrokken partijen bij mobiele identiteit, inrichten om op basis van de rolverdeling mobiele identiteit te leveren?"* Omdat de mobiele markt nog in ontwikkeling is en er nog onzekerheden omtrent de te volgen strategieën zijn, is het niet mogelijk om een zeer gedetailleerde beschrijving te geven over hoe een TTP mobiele certificaten kan leveren. Ik heb dan ook een checklist ontwikkeld die als ondersteuning dient bij het implementeren van een Wireless PKI. Op basis van de checklist wordt een invulling gegeven aan de gekozen rolverdeling. In de checklist staan alle punten die van belang zijn bij het implementeren van een WPKI. Deze punten zijn onderverdeeld in de volgende groepen: Techniek, Processen, Onderlinge relaties, Organisatie TTP, Juridische eisen en Mens & Cultuur. Uit de checklist is gebleken dat er op technisch gebied nog behoorlijk veel moet gebeuren om gebruik te gaan maken van een WPKI. Deze uitdagingen zijn echter niet de grootste bottleneck, die zal veroorzaakt worden door de onderlinge relaties die tot stand moeten komen. De aansprakelijkheden en afhankelijkheden spelen hierbij een belangrijke rol. De samenwerking tussen partijen is noodzakelijk om een WPKI op te zetten. Tevens is uit dit onderzoek gebleken dat de huidige PKI een goed referentiekader is om een WPKI te implementeren.
Na bestudering van de checklist, ben ik tot de conclusie gekomen dat deze, behoudens een aantal aanpassingen, ook goed te gebruiken is voor de overige scenario's en de B2C markt.

8.3 Aanbevelingen

Aanbevelingen voor DigiNotar
Tijdens dit onderzoek heb ik onderzocht hoe de rolverdeling in de mobiele vertrouwensmarkt eruit gaat zien, op basis van de checklist heb ik een invulling aan deze rolverdeling gegeven. Om echter een gefundeerde beslissing te nemen of men van start moet gaan met het leveren van mobiele certificaten, moeten er nog een aantal aanvullende stappen door DigiNotar uitgevoerd worden. In deze paragraaf doe ik hiervoor een aantal aanbevelingen:

- *Onderzoek de behoefte uit de markt*
  Uit dit onderzoek is gebleken dat mobile commerce nog in de kinderschoenen staat. Er zijn op dit moment nauwelijks toepassingen die al werken middels een WPKI. Op dit moment is het ook lastig om te voorspellen wanneer de markt vraagt om een WPKI. Voor DigiNotar is het van belang om de markt continu zeer nauwkeurig te bestuderen, zodat men weet wanneer de behoefte uit de markt aanwezig is. Op basis van alle gesprekken die ik heb gevoerd, verwacht ik dat het nog minstens één jaar duurt voordat deze behoefte ontstaat.
  De status van de markt kan bepaald worden door de ontwikkeling van de standaard mobiele toepassingen zonder WPKI te volgen. Wanneer deze beginnen door te breken, zal ook de vraag naar een WPKI starten.
- *Time to market*
  Omdat er nog onzekerheid is over het moment van vraag naar een WPKI is het voor DigiNotar van groot belang om te onderzoeken hoeveel tijd het kost om de organisatie geschikt te maken voor het leveren van een WPKI. Hierbij kun je denken aan de technische infrastructuur, maar wat zeker zo belangrijk is, is de inrichting van de onderlinge relaties met bijvoorbeeld de telecomoperator. Dit onderzoek kan eventueel gerealiseerd worden door gesprekken met een telecomoperator aan te gaan. Dit kan eventueel gevolgd worden door een pilot.

Uit het onderzoek en de gesprekken is gebleken dat de operators door verschillende partijen benaderd worden om samen te werken op het gebied van mobiele vertrouwensdiensten. Het is daarom van belang dat DigiNotar een pro-actieve houding richting de telecomoperator aanneemt. DigiNotar moet dus het contact zoeken, eventueel in samenwerking met een partij als Baltimore.

- *Moment van levering mobiele certificaten*
  Op basis van bovenstaande punten kan DigiNotar bepalen wat voor hun het gunstigste moment is om een WPKI op te gaan zetten. Hierbij heeft DigiNotar wel enige speling ten opzichte van bijvoorbeeld de telecomoperator. DigiNotar heeft op dit moment al een vertrouwensfunctie in de maatschappij en kan het zich waarschijnlijk veroorloven om de ontwikkelingen af te wachten. Dit moet natuurlijk niet tot in het extreme worden doorgetrokken, omdat dan een onoverbrugbare achterstand kan ontstaan.
- *Gebruik model*
  Het in dit onderzoek ontwikkelde model moet gezien worden als een leidraad en is geen vaststaand statisch model. Juist door de dynamische markt zal het model regelmatig bekeken moeten worden en indien nodig moet het model aan de markt worden aangepast.
- *Uitwerken business case*
  De business case moet ook worden uitgewerkt. Er zijn veel partijen bij een WPKI betrokken en al deze partijen willen uiteraard geld verdienen aan de WPKI. Voordat de WPKI tot stand komt moet er duidelijkheid over de wederzijdse geldstromen, zodat de TTP kan nagaan of de WPKI business case positief is. Op dit moment zijn een aantal partijen de business case aan het uitwerken, maar is er nog geen duidelijk over de uitkomst hiervan.

8.4 Algemene slotconclusie

Met behulp van de antwoorden op de onderzoeksvragen kan nu de probleemstelling beantwoord worden. De Trusted Third Party zal in de mobiele wereld ook een vertrouwensfunctie blijven vervullen en deze functie zal niet verschillen van haar functie in de vaste wereld. De TTP is op basis van haar eigenschappen het meest geschikt om de vertrouwensfunctie ook in de mobiele wereld te vervullen. De checklist geeft aan op welke wijze de Trusted Third Party invulling kan geven aan deze rol. De invulling van de rol van de TTP zal wel anders zijn dan in de vaste wereld, het geheel is veel complexer en er moet veel worden samengewerkt met andere partijen en vooral met de telecomoperator.
Uit dit onderzoek is gebleken dat de mobiele markt nog lang niet is uitgekristalliseerd en er nog veel ontwikkelingen gaande zijn. Daarom heb ik ook een aantal aanbevelingen gedaan die nog onderzocht moeten worden, voordat definitief duidelijk is hoe een Trusted Third Party de mobiele vertrouwensmarkt moet gaan benaderen.
Op basis van dit onderzoek blijkt dat internet zonder kabels niet gelijk is aan internet zonder vertrouwen. Dit vertrouwen is wel degelijk te realiseren.

Verklarende woordenlijst

- *Certificate Practise Statement (CPS)*
  Het CPS wordt door iedere TTP uitgegeven en is een soort van algemene voorwaarden voor de CA-activiteiten.
- *Certification Revocation List (CRL)*
  In de CRL worden de geschorste en ingetrokken certificaten vermeld. De CRL wordt bijgehouden door de CA.
- *Cyphertekst*
  Benaming voor een versleuteld bericht.
- *Data Encryption Standard (DES)*
  Algoritme dat gebruikt wordt om berichten te versleutelen en te ontsleutelen.
- *Elleptic Curve Cryptosystem (ECC)*
  Zie DES.
- *Enhanced Data rates for Global Evolution (EDGE)*
  Netwerktechnologie voor mobiele communicatie.
- *General Packet Radio Services (GPRS)*
  Zie EDGE.
- *Global System for Mobile communication (GSM)*
  Zie EDGE.
- *High Speed Circuit Switched Data (HSCD)*
  Zie EDGE
- *Lightweight Directory Access Protocol (LDAP)*
  LDAP is een software protocol om onder andere bestanden en apparaten in een netwerk zoals het internet te localiseren. LDAP is een lichtere versie van het Directory Access Protocol.
- *Mobile station application EXecution Environment (MExE)*
  Protocol voor mobiele communicatie.
- *Online Certificate Status Protocol (OCSP)*
  Protocol voor het online valideren van digitale certificaten.
- *RSA-algoritme*
  De standaard voor asymmetrische encryptie, deze standaard is ontworpen door Rivest, Shamir en Adleman.
- *SIM Application Toolkit (SAT)*
  Zie MExE.
- *Subscriber Identity Module (SIM)*
  Smartcard die in iedere mobiele telefoon zit. Op deze kaart staan specifieke gegevens van de gebruiker.
- *SWIM*
  Combinatie van de SIM en de Wireless Identity Module.
- *Universal Mobile Telephone System (UMTS)*
  Zie EDGE.
- Wireless Application Protocol (WAP)
  Zie MExE.
- *Wireless Fidelity (WiFi)*
  Communicatietechniek voor draadloze communicatie over korte afstand.
- *Wireless Identity Module (WIM)*
  Smartcard waarop het certificaatURL staat, evenals het cryptografische sleutelpaar. De WIM zit in het mobiele apparaat of is geïntegreerd met de SIM.

Literatuurlijst

- Aberdeen*Group,* Mobile electronic commerce, the new economy on the move,
  www.aberdeen.com, August 2000.

- Barnett, N., Hodges, S., Wilshire, M.J., M-commerce: an operators manual,
  The McKinsey Quarterly, 2000, No.3, p. 163-173.

- Berendt, A., STK vs WAP: Industry battle or peaceful coexistence?,
  Telecommagazine, January 2000, p. 51-54.

- Bogestam, K., Paying your way in the mobile world,
  Telecommunications, January 2000, p. 57-60.

- Buckingham, S., The FutureFoneZone whitepaper,
  Mobile Lifestreams Limited, www.mobile3g.com/wp/whitepaper.html.

- Capslock, Secure wireless acces technology, Technical Whitepaper,
  www.capslock.fi, 2001.

- Certicom, remarks on the security of the elliptic curve cryptosystem,
  www.certicom.com/research/wecc3.html, 2000.

- Chanay, X. Mobile commerce for everyone?,
  Telecommunications, June 2000, p. 29-30.

- Cherrill, D., Mobiele transacties betrouwbaarder,
  Mnet, januari 2001 nr. 1, p. 13-14.

- Chii-Hwa, L., Min-Shiang, H., Wei-Pang, Y., Enhanced privacy and authentication for the global system for mobile communications,
  Wireless Networks, 1999 No. 5, p. 231-243.

- Daitch, J., Kamath, R., Kapoor, R., Nemiccolo, A., Sahni, J., Varma S., Wireless applications for business,
  Kellog TechVenture 2000 anthology,
  www.ranjaygulati.com/art/tv2000/wireless.pdf.

- Donegan, M.P., Whose kingdom is it?,
  Telecommunications, July 2000, p. 57-58.

- Durlacher, The mobile commerce report,
  www.durlacher.com, november 1999.

- Duthler, A.W., Met recht een TTP!,
  Uitgeverij Kluwer, Deventer, 1998.

- Dijk, J. van, Goede, M. de, Hart, H. ‘t, Teunissen, J., Onderzoeken en veranderen: Methoden van praktijkonderzoek,
  Stenvert/Kroese. Leiden/Antwerpen, 1991.

- Eijk, D.T.T. van, Designing Organizational Coordination,
  Proefschrift Technische Universiteit Delft, 1996.

- Ford, W., Baum, M.S., Securing Electronic Commerce: building the infrastructure for digital signatures and encryption,
  Prentice-Hall, 1997.

- Fratto, M., Tutorial: Wireless security,
  www.nwc.com/shared/printArticle?article=nc/1202.1202f1dfull.html&pub=nwc,
  January 2001

- GartnerGroup, Wireless E-Business: The next wave?,
  Conference presentation, 2000.

- GBA-rapport, Eindrapportage vernieuwing Gemeentelijk Basisadministratie,
  www.gba.nl, maart 2001.

- Goldman, J., Wireless Security and M-commerce,
  www.thefeature.com/printable.jsp?pageid=982, 2001

- Gritzalis, S., Katsikas, S.K., Lekkas, D., Moulinos, K., Polydorou, E., Securing the electronic market: The Keystone Public Key Infrastructure Architecture,
  Computers & Security, 2000, No. 8, p. 731 – 746.

- Ham, D.B. van, Digitale zekerheid,
  Afstudeerscriptie Bestuurlijke Informatiekunde, Katholieke Universiteit Brabant, november 1999

- Hermans, J.A.M., Perils and pitfalls of PKI deployments,
  EEMA briefing, September 2000, p. 9.

- Hoeffnagel, R., Doorbraak van de handhelds: Beveiliging cruciaal voor acceptatie van mobiele informatievoorziening,
  Mnet, februari 2001, nr.2, p. 20-25.

- Hof, S. van der, Huydecoper, S., Zwartepieten met certificaataanbieders,
  Computerrecht, 1998/5. p 214-221.

- Housley, R., Polk, T., Planning for PKI,
  Wiley Computer Publishing, New York, 2001.

- Jönsson, S., PKI and Internet: may the real e-landgrab begin,
  EEMA Briefing, December 2000, p. 8.

- Kennedy, S., Bringing m-ccmmerce to the masses,
  www.m-commerceworld.com/articles/article.cfm?objectid=1230C51A-ECA5-11D4-A04D00C04FA0E16A&page=1, January 2001.

- Kleve, P., Zijn TTP's nuttig?,
  Computerrecht, 1998/5, p. 211-213.

- Krugten-Elgersma, P. van, Snels, T., M-commerce en beveiliging,
  Web Professional, november 2000, p. 27-31.

- Koops, B.J., Jong, H. de, De risico's van data recovery voor overheid en gebruikers,
  Computerrecht, 1998/5 p. 222-227.

- Koops, B.J., Kralingen, R. van, Wees, L. van der, De rol van een Trusted Third Parties in het elektronisch handelsverkeer,
  Computerrecht, 1998/5, p. 206-211.

- Leegwater, D.K., TTPS en TTP's,
  Telecommagazine, december 1998

- Logica, Security for the 3rd generation of mobile networks, whitepaper prepared by Logica
  www.logica.com, September 2000.

- Lundquist, E.T., Huston, M.M., Information-rich environments for continuous organic development in organisations: research in progress,
  Journal of Applied Systems Analysis, vol. 17, p. 79-87, 1990.

- Malin, G., The substance between online security,
  Telecommagazine, May 2000, p. 35-36.

- March, J.G., Simon, H.A., Organizations,
  John Wiley & sons, Inc., New York, 1958.

- Maynard, S., Duffy, R., Wireless industry showing us the future for the internet,
  The ARC Group, www.the-arc-group.com/press/wi.htm, 2001.

- McCarthy, P.,Digital signatures on the move,
  Telecommagazine, July 2000, p. 74-75.

- McRae, S.J., WAP in the enterprise,
  EEMA Briefing, December 2000, p. 16-17.

- McRae, S.J., WAP – under the covers,
  EEMA Briefing, September 2000, p.19-21.

- Metricom, Desktop quality internet and intranet acces for mobile workers,
  www.metricom.com/ricochet_advantage/resource_center/desktop_access.html, 2000.

- Mortier, P., WAP and J2ME,
  www.mexeforum.org/articles.htm.

- Nokia, Securing corporate WAP services,
  http://www.nokia.com, November 2000.

- Oasis Technology Ltd., Mobile banking: no wires, no worries, new customers,
  www.oasis-technology.com, 2000.

- Pappo, N., Walls and bridges,
  Telecommunications, September 2000, p.129-130.

- Parekh, S.N., A closer look at the Wireless Application Protocol,
  www.mit.edu/people/sohil/research/itcc/WAP-SohilParekh.pdf.

- Persson, F., Rosengren, J., Wilshire, M.J., The soft side of telecoms,
  The McKinsey Quarterly, 1999, No. 4, p. 123-133.

- PriceWaterhouseCoopers, World Wide Wireless. Mobile Internet, de kracht van een draadloze toekomst,
  Technology Forecast, mei 2001.

- Prins, J.E.J., Electronic commerce: International Legal Aspects 1: Directives,
  Dictaat behorende bij bovenstaand vak, gegeven aan de KUB, 2000.

- Qureshi, S.S., Organisations and Networks,
  Proefschrift London School of Economics, 1995.

- Rackley, J., Securing the wireless internet – seven critical success factors,
  www.wirelessinanutshel.com/news/newsbody.php?code=983015830&cat=, February 2001

- Singh, G., Waterdichte beveiliging,
  Web Professional, November 2000, p.37-39

- Starreveld, R.W., Mare H.B. de, Joëls, E.J., Bestuurlijke informatieverzorging, deel 1,
  Samson Bedrijfsinformatie, Alpen aan den Rijn, 1997.

- Strien, P.J. van, Praktijk als wetenschap. Methodologie van het sociaal wetenschappelijk handelen,
  Van Gorcum, Assen, 1986.

- Tollenaar, A.H., De Notaris als Trusted Third Party inzake het legaliseren van digitale handtekeningen,
  Afstudeerscriptie Rechten, Universiteit Utrecht, 2000.

- Veenker, H., Geert, P. van, Bij zinnen
  Vakgroep Psychologie, Rijksuniversiteit Groningen, 1994.

- Vos, I., Kar, E. van de, Na e-commerce komt m-commerce,
  I&I, 2000. nr. 2, p.28-35.

- Vries, J.M. de, Nationaal TTP-project, brief van de staatssecretaris van V&W,
  Tweede Kamer, 26 681, vergaderjaar 1998- 1999.

- Whittle, S., David and Goliath, WAP takes on i-mode,
  www.m-commerceworld.com/articles/article.cfm?objectid=E13821F3-1845-11D5-A04E00C04FA0E16A&page=1, March 2001.

- Wieland, K., In search of a business-like approach,
  Telecommunications, June 2000, p. 41-44.

- Yankee Group, Convergence of the wireless and internet value chains,
  http://www.yankeegroup.com, 2000.

Geraadpleegde internetpagina's

- www.3gpp.org
- www.baltimore.com
- www.dataquest.com
- www.entrust.com
- www.ericsson.com
- www.etsi.org
- www.f-secure.com
- www.gemplus.com
- www.globalsign.com
- www.ietf.org
- www.mobilecommerceworld.com
- www.mobilegprs.com
- www.mobiletransaction.org
- www.nokia.com
- www.radicchio.org
- www.rsasecurity.com
- www.smarttrust.com
- www.verisign.com
- www.wapforum.org
- www.webwereld.nl
- www.whatis.com