www.pwc.nl

Toets rapportage TLS/ vervoersbedrijven OV-chipkaart fraude

A-2011-0391/MB/wg/az

24 februari 2011

Versie 1.0

Management samenvatting

De aanleiding

De vervoerbedrijven Connexxion, GVB Amsterdam, HTM, RET en NS hebben in 2001 een gezamenlijke dochter Trans Link Systems (hierna TLS) opgericht voor de ontwikkeling, realisatie en exploitatie van de OV-chipkaart, als opvolger van de strippenkaart.

In 2002 is aan de markt gevraagd om te komen met een oplossing via een openbare aanbesteding. Dit heeft geleid tot de contractering van het East-West E-Ticketing Consortium geleid door Thales en Viales. Dit consortium bracht de werkende oplossing van MTR Corporation uit Hong Kong in. Vanaf 2005 is gestart met de uitgifte van OV-chipkaarten, nadat er enige jaren is gewerkt aan het aanpassen van de kaart aan de Nederlandse situatie.

In december 2007 kwam de OV-chipkaart in het nieuws doordat hackers de Mifare Classic chip hadden weten te kraken. TLS heeft TNO onderzoek laten uitvoeren waaruit bleek dat de chip wel gemigreerd moest worden, maar dat er geen acute noodzaak toe was. De drie lagen van beveiliging (op kaart, applicatie en backoffice niveau) waren afdoende. Nadat ook de Radboud Universiteit van Nijmegen de beveiliging ter discussie had gesteld is door de Royal Holloway University of London (RHUL) een contra-expertise uitgevoerd in april 2008.

Recent is de OV-chipkaart wederom in het nieuws geweest in relatie tot de mogelijkheid om deze kaart te 'kraken' waarbij het mogelijk bleek met eenvoudig verkrijgbare apparatuur (NFC kaartlezer en PC) en via internet verkrijgbare software het saldo op de kaart te verhogen en op de kaart additionele informatie te plaatsen. TLS heeft aangegeven deze fraude te hebben gedetecteerd in haar backoffice en hiervan het Openbaar Ministerie van op de hoogte te hebben gebracht via een formele aangifte. Het lid Monasch van de Tweede Kamer heeft een op 27 januari 2011 een motie terzake ingediend welke is aangenomen.

Naar aanleiding van deze motie Monasch heeft de minister van Infrastructuur en Milieu TLS en de vervoerders verzocht om in een rapport antwoord te geven op de volgende vragen:

1. De risico's van de recente kraakacties: de omvang en impact van de recente kraakacties op de OV-chipkaart waarbij onderscheid wordt gemaakt naar drie typen fraude:

    a. Het ophogen van saldo met als doel vrij te reizen

    b. Het ophogen van saldo met als doel verzilvering bij de balie

    c. De frauduleuze [nep] check-in

    De impactanalyse beschrijft onder meer de businesscase voor de verschillende fraudetypen en de gevolgen voor (niet-frauderende) reizigers.

2. De wijze waarop deze fraude/frauderisico's worden beheerst

3. De kosten waarbij onderscheid gemaakt kan worden naar:

    a. Inzicht in de kosten van de beheersmaatregelen

    b. Inzicht in de kosten van het uitstel van het uitzetten van het NVB (strippenkaart)

Het ministerie van Infrastructuur en Milieu heeft PwC gevraagd de rapportage van de vervoerders en TLS te valideren. Het voorliggende document betreft de uitkomsten van dit onderzoek.

Het onderzoek

Het te beoordelen rapport is opgesteld door TLS en de vervoerders, waarbij TLS als penvoerder van de rapportage fungeerde. Om deze reden heeft PwC primair contact gehad met TLS. Het gevalideerde rapport betreft '*Rapportage Fraude met de OV-chipkaart, 23 februari 2011, versie 1.2*'.

PwC is voor de validatie in hoofdlijn uitgegaan van het model beschreven in ISO 27005 (een algemene standaard voor risicomanagement rondom informatiebeveiliging).

PwC heeft voldoende medewerking gekregen van TLS voor het uitvoeren van het onderzoek. Alle gesprekken verliepen in constructieve sfeer. Naar onze inschatting heeft TLS hierbij in alle openheid een beeld van de situatie trachten te geven.

Onze bevindingen

1. *De risico's van de recente kraakacties: de omvang en impact van de recente kraakacties*

    Samen met de aangeleverde documentatie en nadere toelichting geven TLS en de vervoerders een goed beeld van de gevraagde fraudescenario's, de dreigingen en technische en procesmatige kwetsbaarheden in- en rond de OV-chipkaart infrastructuur, te weten het 'ophogen van het saldo en er mee reizen', 'het ophogen van het saldo en het verzilveren' en het 'uitvoeren van een nep-check-in'. De fraudescenario's zijn inderdaad reëel en kunnen worden toegepast. TLS heeft in de eerste maanden van dit jaar van het eerste fraudescenario enkele tientallen fraudegevallen per dag geconstateerd, tot een maximum van 60 per dag. TLS kent de feitelijke omvang van de fraude die zij (nog) niet kan detecteren (uiteraard) niet. De rapportage van TLS geeft tevens een beeld van de fraude ontwikkeling van deze scenario's tot en met 17 februari jongstleden.

    TLS geeft in haar rapport een schatting van de kans van optreden en de impact van deze fraudescenario's. TLS maakt hierbij, per scenario, gebruik van een rudimentaire 'fraude business case', waarin een aantal parameters uit het huidige transactiebestand van TLS is opgenomen. Op basis hiervan is een omslagpunt berekend waarbij het uitvoeren van de

fraude voor een fraudeur gemiddeld genomen lonend is. Een aantal zaken, waaronder de gemiddelde fraudebereidheid wordt mede bepaald door de aard van de relatie van een fraudeur met het object van fraude (in dit geval de OV-chipkaart), pakkans, strafmaat, persoonlijke integriteit en dergelijke en deze kunnen door de tijd heen veranderen. Het is niet eenvoudig om deze parameters, zoals de gepercipieerde pakkans, in te schatten, daar deze ook door diverse communicatieve uitingen ten positieve of ten negatieve kan worden beïnvloed. De door TLS gedane inschatting in het rapport van 200 tot 500 gevallen per dag is niet onplausibel op basis van het historisch verloop vanaf 2008 (toen de fraudemogelijkheid bekend werd) tot en met 17 februari jongstleden.

De eerste uitwerking van de fraude business case per scenario achten wij op dit moment toereikend, gegeven de tijdsspanne van het onderzoek; immers de meest relevante parameters van de businesscase zijn door TLS genoemd en (rudimentair) ingeschat. Wel verdient het aanbeveling deze fraude business case verder te ontwikkelen en up-to-date te houden met de laatste gegevens uit de transactiedatabase. TLS heeft aangegeven deze fraude business case inderdaad verder te ontwikkelen, onderdeel te maken van het reguliere fraudemanagement en te gebruiken voor hun besluitvorming omtrent eventuele versnelling van het doorvoeren van maatregelen als de werkelijke fraudegetallen over een vast te stellen tolerantiewaarde heen dreigen te gaan.

2. *De wijze waarop deze fraude/frauderisico's worden beheerst*

TLS geeft in haar rapportage een opsomming van de maatregelen die zij voornemens is te gaan nemen om het frauduleus handelen te beheersen.

Met de aanvullende toelichting en documentatie is een redelijk beeld ontstaan van de voorgestelde maatregelen.

De maatregelen die TLS en de vervoerders reeds hebben geïmplementeerd zijn:

- hogere frequentie van controles in de backoffice
- het verplichtstellen van legitimatie bij restitutie van saldo aan de balie om restitutiefraude te beperken

De 'korte termijn' (binnen 6 maanden) beheersmaatregelen die zijn voorgesteld om de fraude te beheersen bestaan uit:

- permanent blokkeren van OV-chipkaarten waarbij fraude is vastgesteld
- het aanmaken van een transactie bij controle aan boord (zodat fraude door de backoffice kan worden vastgesteld)

TLS heeft de voorgestelde maatregelen ingebracht in het formele wijzigingsproces.

Op grond van de voorgestelde maatregelen en de veronderstelling dat ze ook naar behoren worden geïmplementeerd, mag TLS terecht veronderstellen dat het fraudescenario 'ophogen van het saldo en verzilveren' een acceptabel restrisico zal opleveren in termen van resulterende financiële schade.

Voor het fraudescenario 'ophogen van het saldo en ermee reizen' geldt dat de door TLS voorgestelde maatregelen, als ze zijn geïmplementeerd, naar verwachting een positief effect zullen hebben op het terugbrengen van het frauderisico. Op basis van de rapportage en de aangeleverde documentatie is PwC niet in staat de omvang van het restrisico te valideren, daar het restrisico niet wordt gespecificeerd.

Met betrekking tot het fraudescenario van de 'nep-check-in' zal de maatregel 'aanmaken van transactie aan boord', mits correct geïmplementeerd, naar verwachting een positieve werking hebben op het terugdringen van deze fraude. Het restrisico na invoering van deze maatregel is ongeveer gelijk aan het huidige risico rond 'ophogen saldo'. Voor het totale restrisico dienen ook de maatregelen zoals opgesomd onder 'ophogen van het saldo en ermee reizen' te worden meegenomen. Het effect zal naar verwachting positief zijn, echter op basis van de rapportage en de aangeleverde documentatie is PwC niet in staat de omvang van het restrisico te valideren, daar het restrisico niet wordt gespecificeerd.

Ten aanzien van de planning van de implementatie van de beheersmaatregelen heeft TLS inzage geven in een invoeringsstrategie, alsmede de onderliggende 'change notes'. Er is sprake van een in opzet beheerst wijzigingsproces binnen de OV-chipkaart infrastructuur. De federatieve aard van het OV-chipkaart systeem betekent dat implementatie van maatregelen de verantwoordelijkheid van individuele vervoerders is, die elk een relatie hebben met een eigen leverancier. Het daadwerkelijk doorvoeren van wijzigingen zal geschieden langs de besluitvormingsgremia van TLS en de vervoerders.

De 'lange termijn' (meer dan 6 maanden) maatregelen betreffen:

- het verbeteren van de blacklistfunctionaliteit, gericht op de distributie en de capaciteit van de blacklist
- toevoegen extra kenmerk aan transacties. Deze maatregel wordt eerst verder gespecificeerd en de risico's van invoering worden geanalyseerd
- de migratie naar de kaart gebaseerd op de smartMX chip

Het rapport meldt over het migratieplan: *'In de tussenliggende tijd is sprake van een duale situatie, waarbij Mifare classic en SmartMX naast elkaar in de markt bestaan. Om dit technisch te realiseren is de SmartMX chip in staat om de Mifare classic te emuleren, oftewel in een Mifare classic modus te werken.* Wij stellen vast dat TLS voorstelt in eerste instantie de smartMX in emulatiemodus van de Mifare Classic te

gebruiken. Hierdoor is naar verwachting een aantal aanvalsscenario's nog steeds mogelijk. Onderzoek hiernaar is buiten scope van ons onderzoek. Aanvankelijk zullen deze wellicht alleen interessant zijn voor 'academische hacks', maar ook die leiden tot nieuwe aandacht in de media. In het rapport wordt hier zijdelings melding van gemaakt: '*In die modus zijn de kaarten nog gevoelig voor fraude*'. Wij onderschrijven deze stelling.

3.a De kosten van de beheersmaatregelen

TLS stelt dat zij slechts indicatief de bijbehorende kosten van de maatregelen kunnen aangeven. Gegeven de fase waarin TLS op dit punt verkeert, te weten de analysefase, kunnen wij ons dit voorstellen; immers de kosten zijn ook sterk afhankelijk van de wijze en het tempo waarop de maatregelen geïmplementeerd zullen worden. Daarnaast moet ook hier rekening gehouden worden met de federatieve opzet van het OV-chipkaart systeem. Implementatie van maatregelen komt voor rekening van individuele vervoerders, die ieder bij hun eigen leveranciers een quote dienen uit te vragen. Dit maakt het lastig om op korte termijn met een voldragen schatting te komen van de totale kosten. Het is aanbevelenswaardig om deze indicatieve bedragen uit de schatting zo snel mogelijk te onderbouwen met de hiervoor benodigde besluitvormingsparameters (met andere woorden: welke maatregel wordt afhankelijk waarvan ingeroepen en welke onderlinge afhankelijkheden zijn er en langs welke voorwaarden worden ze uitgevoerd).

3.b Kosten van het uitstel van het uitzetten van het NVB (strippenkaart)

Door TLS is een kostenraming opgegeven in hun rapportage. Na toelichting achten wij deze voldoende plausibel.

TLS stelt terecht dat *'Als men wil frauderen, dan kan dat nu dus al. Door het wel of niet uitzetten van het NVB wordt dit frauderisico niet groter (of kleiner)'*. Het al dan niet uitzetten van het NVB is financieel niet gerelateerd aan de fraudemogelijkheden van de OV-chipkaart, in die regio's waar de systemen naast elkaar actief zijn.

Inhoudsopgave

1. Inleiding

De vervoerbedrijven Connexxion, GVB Amsterdam, HTM, RET en NS hebben in 2001 een gezamenlijke dochter opgericht voor de ontwikkeling, realisatie en exploitatie van de OV-chipkaart, als opvolger van de strippenkaart, Translink Systems (hierna TLS).

In 2002 is aan de markt gevraagd om te komen met een oplossing via een openbare aanbesteding. Dit heeft geleid tot de contractering van het East-West E-Ticketing Consortium geleid door Thales en Viales. Dit consortium bracht de werkende oplossing van MTR Corporation uit HongKong in. Vanaf 2005 is gestart met de uitgifte van OV-chipkaarten, nadat er enige jaren is gewerkt aan het aanpassen van de kaart aan de Nederlandse situatie.

In december 2007 kwam de OV-chipkaart in het nieuws doordat hackers de 'Mifare Classic' chip hadden weten te kraken. TLS heeft TNO onderzoek laten uitvoeren waaruit bleek dat de chip wel gemigreerd moest worden, maar dat er geen acute noodzaak toe was. De drie lagen van beveiliging (op kaart, applicatie en backoffice niveau) waren afdoende. Nadat ook de Radboud Universiteit van Nijmegen de beveiliging ter discussie had gesteld is door de Royal Holloway University of London (RHUL) een contra-expertise uitgevoerd in april 2008.

Recent is de OV-chipkaart in het nieuws geweest. Het bleek mogelijk met eenvoudig verkrijgbare apparatuur (computer en een NFC kaartlezer) en via internet verkrijgbare software de informatie op de kaart aan te passen, zoals verhogen van het saldo op de kaart en op de kaart additionele informatie te plaatsen. Trans Link Systems (TLS) heeft aangegeven deze fraude te hebben gedetecteerd in haar backoffice systeem en hiervan formeel aangifte te hebben gedaan bij het Openbaar Ministerie. Het lid Monasch van de Tweede Kamer heeft op 27 januari 2011 een motie ingediend welke is aangenomen.

'De Kamer […] verzoekt de regering om binnen een maand met een nadere rapportage te komen om de risico's van de recente kraakacties van de OV-chipkaart in kaart te brengen op basis waarvan de Kamer kan besluiten of en wanneer verdere invoering verantwoord is; […].'

De minister van Infrastructuur en Milieu heeft hierop de vervoerders en TLS verzocht om middels een rapportage inzicht te bieden in:

1. De risico's van de recente kraakacties: de omvang en impact van de recente kraakacties op de OV-chipkaart waarbij onderscheid wordt gemaakt naar 3 typen fraude:
    a. Het ophogen van saldo met als doel vrij te reizen
    b. Het ophogen van saldo met als doel verzilvering bij de balie
    c. De frauduleuze [nep] check-in

De impactanalyse beschrijft onder meer de businesscase voor de verschillende fraudetypen en de gevolgen voor (niet-frauderende) reizigers.

2. De wijze waarop deze fraude/frauderisico's worden beheerst
3. De kosten waarbij onderscheid gemaakt kan worden naar:
    a. Inzicht in de kosten van de beheersmaatregelen
    b. Inzicht in de kosten van het uitstel van het uitzetten van het NVB (strippenkaart)

Het ministerie van Infrastructuur en Milieu heeft PwC gevraagd de rapportage van de vervoerders en TLS, waarin zij antwoord geven op de bovenstaande gestelde vragen, te valideren.

2. Doel en reikwijdte

Het doel van het onderzoek is het uitvoeren van een *validatie* op de rapportage van TLS en de vervoerders met daarin het antwoord op de drie vragen. De onderzoeksvraag voor PwC is, met andere woorden:

Wat is de mate van betrouwbaarheid van de antwoorden op de vragen van de minister van Infrastructuur en Milieu?

We merken hierbij op dat de *motie Monasch* en de vragen van de minister van Infrastructuur en Milieu betrekking hebben op de risico's in enge zin: de risico's van de recente kraakacties. Er wordt de vervoerders en TLS niet gevraagd om een risico-analyse op het gehele systeem uit te voeren.

De beperkte doorlooptijd voor zowel de vervoerders/TLS als PwC heeft mede de diepgang van de validatie bepaald. PwC baseert zich in dit onderzoek op de schriftelijke rapportage zoals uitgebracht door TLS en de vervoerders *'Rapportage fraude met de OV-chipkaart'*, de mondelinge toelichting door medewerkers van TLS en op door TLS aangeleverde documentatie. PwC heeft niet gevalideerd of de beschreven beheersingsmaatregelen daadwerkelijk zijn geïmplementeerd, noch is de juiste werking van deze beheersingsmaatregelen naar het verleden en de toekomst getoetst.

3. Methodologie

Het onderzoek kent een korte tijdslijn. Gelet op deze beperkte doorlooptijd hebben wij ons moeten beperken tot het bestuderen van de door TLS opgestelde en aangereikte rapportage, en het voeren van gesprekken met sleutelpersonen en het bestuderen van door TLS aangereikte relevante documentatie.

PwC is voor de validatie in hoofdlijn uitgegaan van het model beschreven in ISO/IEC 27005[1] (een algemene standaard voor risicomanagement rondom informatiebeveiliging):

1. Onderkenning van potentiële scenario's bestaande uit dreigingen ('wie' of 'wat') en technische en procesmatige kwetsbaarheden in en rond de OV-chipkaart infrastructuur, zoals aangereikt door het ministerie.

2. Inschatting van de risico's op basis van de kans van optreden en impact per scenario in ieder geval kwantitatief (kosten) en mogelijk ook kwalitatief.

3. Risico behandeling van de risico's middels maatregelen en bepaling van de restrisico's (bepaling effectiviteit van de maatregelen, i.e. deductie van de scenario relevantie).

4. Kwaliteit van het implementatieplan (planning en kosten).

Een *mapping* van bovenstaande 'precisering' op de drie vragen levert de volgende structuur voor de validatie:

	Vraag	Nadere precisering	Antwoord TLS	Bevinding PwC
1a	Risico's van recente kraakacties	De potentiële scenario's gebaseerd op dreigingen ('wie' of 'wat') en kwetsbaarheden in en rond de OV-chipkaart zijn in voldoende mate onderkend		
	Het ophogen van saldo met als doel vrij te reizen	Is het fraudescenario voldoende eenduidig en volledig beschreven?		
	Het ophogen van saldo met doel verzilvering bij balie	Is het fraudescenario voldoende eenduidig en volledig beschreven?		
	De frauduleuze check-in	Is het fraudescenario voldoende eenduidig en volledig beschreven?		
1b	Businesscase voor de verschillende fraudetypen; gevolgen voor (niet-frauderende) reiziger	De risico's per onderkend scenario zijn in voldoende mate geanalyseerd op basis van de kans van optreden en impact: in ieder geval kwantitatief (kosten) en mogelijk ook kwalitatief		
	Het ophogen van saldo met als doel vrij te reizen	Zijn de kans van optreden en impact met een voldoende mate van betrouwbaarheid ingeschat?		
	Het ophogen van saldo met doel verzilvering bij balie	Zijn de kans van optreden en impact met een voldoende mate van betrouwbaarheid ingeschat?		
	De frauduleuze check-in	Zijn de kans van optreden en impact met een voldoende mate van betrouwbaarheid		

[1] ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management

		ingeschat?		
2a	De wijze waarop deze frauderisico's worden beheerst	De behandeling van de risico's binnen een scenario middels maatregelen is voldoende beschreven		
	Het ophogen van saldo met als doel vrij te reizen	Zijn de maatregelen met voldoende detaillering beschreven? Is de effectiviteit van de maatregel(en) (inschatting van de restrisico's) met een voldoende mate van betrouwbaarheid ingeschat?		
	Het ophogen van saldo met doel verzilvering bij balie	Zijn de maatregelen met voldoende detaillering beschreven? Is de effectiviteit van de maatregel(en) (inschatting van de restrisico's) met een voldoende mate van betrouwbaarheid ingeschat?		
	De frauduleuze check-in	Zijn de maatregelen met voldoende detaillering beschreven? Is de effectiviteit van de maatregel(en) (inschatting van de restrisico's) met een voldoende mate van betrouwbaarheid ingeschat?		
2b	De wijze waarop deze frauderisico's worden beheerst	Het plan om de onderkende maatregelen te implementeren is van voldoende kwaliteit: er is een planning afgegeven inclusief onderbouwing; deze is in voldoende mate realistisch		
3a	Inzicht in de kosten van de beheersmaatregelen	Het plan om de onderkende maatregelen te implementeren is van voldoende kwaliteit:er is een kostenoverzicht afgegeven inclusief onderbouwing; deze is in voldoende mate realistisch		
3b	Inzicht in de kosten van het uitstel van het uitzetten van het NVB (strippenkaart)	Er is een kostenoverzicht afgegeven inclusief onderbouwing; deze is in voldoende mate realistisch		

4. Het onderzoek

De te beoordelen rapportage wordt opgesteld door TLS en de vervoerders, waarbij TLS als penvoerder van de rapportage fungeerde. Om deze reden heeft PwC primair contact gehad met TLS.

PwC heeft voldoende medewerking gekregen van TLS voor het uitvoeren van het onderzoek. Alle gesprekken verliepen in constructieve sfeer. Naar onze inschatting heeft TLS hierbij in alle openheid een beeld van de situatie trachten te geven.

4.1. Voorbereiding

Bij aanvang van de opdracht op 14 februari jongstleden was de rapportage van TLS nog niet beschikbaar. Ter voorbereiding zijn enkele gesprekken gevoerd met TLS voor een mondelinge toelichting op de recente fraude en de werkwijze en planning om te komen tot de rapportage. Hierbij zijn afspraken gemaakt voor het uitvoeren van de validatie. Deze afspraken zijn door PwC afgestemd met de opdrachtgever, het ministerie van Infrastructuur en Milieu.

- Een gesprek met de directie van TLS - 9 februari 2011
- Een nadere mondelinge toelichting op de recente fraude door TLS - 14 februari 2011
- Een gesprek met de opdrachtgever (I&M) - 16 februari 2011

4.2. Validatie

Het conceptrapport ter validatie ontvingen wij van TLS op woensdagmiddag 16 februari 2011. Dit betrof een concept dat nog diende te worden afgestemd met de verschillende vervoerders. Door TLS is aangegeven dat dit concept naar hun mening in voldoende vergevorderde staat van volledigheid was om de validatie door PwC op te kunnen uitvoeren. Het met de vervoerders afgestemde rapport ontvingen wij op maandag 21 februari 2011.

De uitvoering van de validatie vond plaats ten burele van TLS in verband met de noodzakelijke bestudering van achterliggende documentatie en het spreken van ter zake kundige specialisten van TLS. In verband met de *security policy* van TLS was het niet toegestaan documenten mee te nemen of te kopiëren. Dit heeft het proces van validatie in onze ogen niet in de weg gestaan.

- Validatie - 17 en 18 februari 2011
- Opstellen rapportage – 18, 21 en 23 februari 2011
- Toetsing van de voorlopige bevindingen van de validatie bij TLS – 22 tot en met 24 februari 2011

De concept rapportage bevat geen verwijzingen naar gehanteerde bronnen. Hierop is door PwC tijdens de validatie aangegeven op welke punten in de rapportage nadere onderbouwing (door documentatie of een ter zake kundige specialist) wenselijk was. Hierop is door TLS documentatie ter inzage aangeleverd.

PwC heeft niet kunnen beoordelen of de aangeleverde informatie rond een aspect ook de volledige, of meest relevante, bij TLS of vervoerders beschikbare informatie rondom dat aspect betrof.

5. Bevindingen

5.1. Risico's van recente kraakacties

Zijn de potentiële scenario's gebaseerd op dreigingen ('wie' of 'wat') en kwetsbaarheden in en rond de OV-chipkaart in voldoende mate onderkend?

5.1.1. Het ophogen van saldo met als doel vrij te reizen

- *Is het fraudescenario voldoende eenduidig en volledig beschreven?*

Het scenario *'ophogen van saldo'* staat beschreven in sectie 3.2 van de rapportage. Na een nadere toelichting en met aangeleverde documentatie [2], [4], [14] en [16] kunnen de noodzakelijke elementen worden gereproduceerd voor een goed beeld van het fraudescenario. Deze documentatie is noodzakelijk om tot een voldoende beoordeling te komen op dit aspect.

5.1.2. Het ophogen van saldo met doel verzilvering bij balie

- *Is het fraudescenario voldoende eenduidig en volledig beschreven?*

Het scenario *'ophogen van saldo met doel verzilvering bij balie'* staat beschreven in sectie 3.2 van de rapportage. Na een nadere toelichting en uit de door TLS aangeleverde documentatie [2], [4], [14] en [16] kunnen deze elementen worden gereproduceerd.

5.1.3. De frauduleuze check-in

- *Is het fraudescenario voldoende eenduidig en volledig beschreven?*

Na een nadere toelichting en uit de door TLS aangeleverde documentatie [2], [4], [14] en [16] kunnen deze elementen worden gereproduceerd.

5.1.4. Overige fraude scenario's

In paragraaf 4.3 van de rapportage wordt het volgende aangegeven: *'Naast de voornoemde actuele scenario's zijn ook andere mogelijke fraudescenario's uitgewerkt. Hierbij valt onder andere te denken aan het manipuleren van producten (abonnement) op de OV-chipkaart of het ongedaan maken van een blokkade van een kaart.'*

In de aangeleverde documentatie, in het bijzonder [16] en [17] wordt een beeld geschetst van de verschillende fraudescenario's, alsmede een schets van maatregelen tegen deze fraude.

5.2. Businesscase voor de verschillende fraudetypen

Zijn de risico's per onderkend scenario in voldoende mate geanalyseerd op basis van kans van optreden en impact: in ieder geval kwantitatief (kosten) en mogelijk ook kwalitatief?

5.2.1. *Het ophogen van saldo met als doel vrij te reizen*

- *Zijn de kans van optreden en impact met een voldoende mate van betrouwbaarheid ingeschat?*

De kans van optreden

Ten aanzien van de kans van optreden wordt in de rapportage in sectie 4.1 gesteld *'dit scenario is reëel en wordt op dit moment toegepast door fraudeurs'* . Dit is aannemelijk daar dit risico zich concreet heeft voorgedaan, en op dit moment nog steeds lijkt voor te doen, hetgeen blijkt uit de grafiek in sectie 3.2 in de rapportage van TLS. Er zijn ook voldoende aanwijzingen dat dit scenario zich ook in de nabije toekomst nog zal blijven voordoen, vanwege de geschatte ontwikkel- en implementatietijd van maatregelen tegen dit fraudescenario.

Impact

Ten aanzien van de impact wordt een schatting gemaakt in sectie 4.1.. Hierin staat *'Voor de business case is het belangrijk dat de reiziger voordeel kan halen uit het gebruik van een gefraudeerde kaart. Dus dat de baten hoger zijn dan de kosten. De kosten in deze business case bestaan uit de directe kosten van aanschaf materiaal en eventueel software. Verder zijn er indirecte kosten in termen van 'transactiekosten' voor de fraudeur, ofwel de inspanning die een fraudeur moet plegen om de fraude uit te voeren. Tot slot is er de 'pakkans maal sanctie' die wordt meegenomen. Bij een hoge pakkans en sanctie is de business case minder aantrekkelijk. De baten in de business case zijn in dit geval het gratis vervoer'*.

TLS maakt voor de schatting van de fraude gebruik van een fraude business case analyse, waarbij een individu kan overgaan tot fraude als de baten hoger zijn dan de kosten. In de kosten worden ook niet-directe cq. externe kosten meegenomen, zoals de transactiekosten om te komen tot fraude, en de pakkans maal sanctie. Tot slot wordt er rekening gehouden met een 'fraudebereidsheidsfactor', (niet iedereen is bereid tot het plegen van fraude ook al is er financieel gewin) die is afgeleid van bestaande fraude in het OV. De gehanteerde elementen in deze business case zijn in opzet goed. Tijdselementen die van invloed zijn op fraudeontwikkeling zijn nog niet meegenomen. Dit maakt de business case wat rudimentair. Gegeven de beperkte tijdslijnen die zijn gegeven voor de analyse is dit voorstelbaar.

In de rapportage wordt de volgende schatting van de impact gemaakt: *'Onze aannamen voor de kosten voor een fraudeur zijn als volgt: aanschaf kaart € 7,50, afschrijving NFC reader, € 2. Daarnaast dient de fraudeur een inspanning te plegen; er dient software te worden verkregen en geïnstalleerd, er dient een aantal handelingen te worden verricht op een computer, er is tijdsbesteding voor het verkrijgen van een nieuwe kaart als de oude wordt geblokkeerd. Uitgaande van een monetaire prijs van één uur van circa €10 en een tijdsbesteding van circa 10 minuten per fraudehandeling komt dit op circa €1,50 aan administratieve lasten. Totale kosten van een gefraudeerde kaart is dus circa € 11,-. Op basis van bekende fraude in het OV domein*

kan de fraudebereidheid worden afgeleid – exclusief 'pakkans maal sanctie'. Deze wordt door ons ingeschat op 15 tot 20%, gerelateerd aan de cijfers over zwartrijden.

De pakkans schatten wij in als relatief laag, maar de boete voor frauderen met een OV-Chipkaart is hoog, zie paragraaf 2.5. Door de relatief hoge boete voor misbruik van de chipkaart, schatten wij in dat de fraudebereidheid wordt beperkt tot 2 tot 3%. Iedere dag worden momenteel ruim 15.000 reizen (op saldo) gemaakt met een minimale waarde van € 7,50. De gemiddelde waarde van deze reizen is € 11,08. Zoals de business case laat zien zijn deze reizen interessant voor een fraudeur. 3% fraude houdt in dat er bij 450 reizen gefraudeerd wordt. De impact hiervan is ca € 5.000,- per dag of € 150.000,- per maand. Bij gemiddeld 2 reisbewegingen per dag horen ca 200 gefraudeerde kaarten '

Uitgaande van een juiste interpretatie van het transactiebestand achten wij de onderbouwing van de impact, gegeven de status van het onderzoek op dit moment als toereikend. De door TLS gedane inschatting in het rapport van het aantal gevallen per dag is niet onplausibel op basis van het historisch verloop vanaf 2008 (toen de fraudemogelijkheid bekend werd) tot en met 17 februari jongstleden. We bevelen aan om de fraude business case onderdeel te maken van het reguliere fraudemanagement proces, de werkelijke fraudegevallen te plotten op de geprognosticeerde fraude en om een tolerantie te definiëren (maximaal toegestane verschil tussen werkelijke en geprognosticeerde fraudegevallen). Indien deze tolerantie wordt overschreden zou een escalatie- of exceptieplan in werking dienen te treden voor besluitvorming rondom versneld doorvoeren van additionele maatregelen.

5.2.2. Het ophogen van saldo met doel verzilvering bij balie

- *Zijn de kans van optreden en impact met een voldoende mate van betrouwbaarheid ingeschat?*

De kans van optreden

Ten aanzien van de kans van optreden wordt in de rapportage in sectie 4.1 gesteld *'dit scenario is reëel en wordt op dit moment toegepast door fraudeurs'*.

Impact

In sectie 4.1 wordt gesteld dat: *'De afgesproken maximale restitutie per kaart is € 30. Bij gemiddeld 100 gefraudeerde kaarten is het maximale schadebedrag per dag € 3.000. Per maand is dit € 90.000. Sinds twee weken is een proces ingericht dat bij restitutie een restitutieformulier moet worden ingevuld en de kaarthouder zich bij uitbetaling moet legitimeren. Daarnaast zijn de meeste balies uitgerust met camera's. Hierdoor verwachten we op dit moment dat deze restitutiefraude marginaal is.'*

Bij restitutiefraude moet een fraudeur zich bekend maken. Hierbij zou een fraudeur in theorie gebruik kunnen maken van 'katvangers'. Echter het maximaal te behalen bedrag is slechts €30,

wat laag is in verhouding tot de transactiekosten voor de fraudeur. Hierdoor zal een fraudeur zich naar verwachting richten op andere, meer lucratieve fraudes. Samengevat achten wij de onderbouwing van de impact als voldoende plausibel.

5.2.3. De frauduleuze check-in

- *Zijn de kans van optreden en impact met een voldoende mate van betrouwbaarheid ingeschat?*

De kans van optreden

Sectie 4.1 stelt dat *'Dit scenario wordt op dit moment naar verwachting nog vrijwel niet toegepast, omdat de noodzakelijk software op internet pas sinds kort beschikbaar is en nog niet optimaal werkt*.

In de business case gaat TLS er wel vanuit dat deze software binnenkort werkend beschikbaar is. Dit is in onze ogen een terechte aanname, daar de noodzakelijke inspanning voor het produceren van dergelijke software niet zeer complex is, er een community actief is, en de kaart zelf immers reeds als volledig gekraakt moet worden beschouwd. Er zijn ook voldoende aanwijzingen dat dit scenario zich ook in de nabije toekomst nog zal blijven voordoen, vanwege de geschatte ontwikkel- en implementatietijd van de belangrijkste maatregel tegen dit fraudescenario, 'het aanmaken van een transactie aan boord'.

Impact

De rapportage geeft in 4.1 terecht aan dat doordat de fraude op dit moment nog niet gedetecteerd kan worden, de kaarten waarmee dit type fraude plaatsvindt ook nog niet geblokkeerd kunnen worden. Hierdoor valt de business case voor een fraudeur significant positiever uit tot het moment dat de maatregel is geïmplementeerd: *'In dit scenario zijn de kosten voor een fraudeur, voor zolang er geen transactie aan boord van de trein plaatsvindt, lager. Immers, de kaart wordt vooralsnog niet geblokkeerd. Dit betekent dat vooralsnog de kosten voor een nieuwe kaart en de administratieve lasten die hierbij horen, nog niet in de business case kunnen worden meegenomen. Ook schatten wij in dat op dit moment de pakkans in de trein zeer laag is. Wel moet de software nog breed beschikbaar te komen, en zal de maatregel om een transactie aan boord aan te maken wordt binnen afzienbare tijd gerealiseerd. Om deze reden gaan wij uit van een scenario met maatregel en een scenario zonder maatregel.*

Zonder maatregel 'transactie aanmaken aan boord': de impact is significant hoger dan scenario 1. Wij gaan uit van een fraudebereidheid die stijgt van 2-3% naar ongeveer 10%. Omgerekend komt dit neer op ca € 15.000,- per dag of € 500.000,- per maand. Wij gaan uit van circa 750 kaarten per maand. Met maatregel 'transactie aanmaken aan boord': de business case en impact zijn gelijk aan scenario 1 ongeveer € 150.000,- per maand. Hierbij zijn ook ongeveer 200 kaarten in het geding'.

De fraudebereidheid zou in dit scenario wellicht nog wat hoger kunnen liggen, daar de pakkans en de transactiekosten op dit moment vrijwel nihil zijn. Daar staat tegenover dat werkende software voor zover wij dat hebben kunnen constateren, op dit moment nog niet breed beschikbaar is. Dat zal wel snel kunnen veranderen. Ook is het zo dat het voor een fraudeur niet duidelijk is wanneer de maatregel van het aanmaken van een transactie aan boord wordt geïmplementeerd. Dit brengt een psychologische onzekerheid met zich mee, wat een dempend effect op de omvang van de fraude zou kunnen hebben. Al met al achten wij deze onderbouwing van de impact als voldoende plausibel.

5.3. Gevolgen voor (niet-frauderende) reiziger

De rapportage stelt in 3.5 dat er *'Geen financiële schade voor de reiziger'*, en *'Het is daarmee bijna ondenkbaar dat een reiziger financiële schade ondervindt door fraude'.* Hierbij wordt uitgegaan van zuiver economische schade voor een reiziger. Voor de volledigheid zou een aantal niet-financiële gevolgen geduid kunnen worden. Als voorbeeld kan het mogelijk worden van fraude ('gratis of goedkoper reizen') een aanzuigende werking hebben op het openbaar vervoer. Het openbaar vervoer kan dus drukker worden, de bussen en treinen voller. Hierdoor kan de gepercipieerde kwaliteit, het comfort voor de reiziger, omlaag gaan. Een fraudeur kan een product 'reizen eerste klas trein' op zijn kaart plaatsen. Tesamen met de frauduleuze check-in kan deze dan gratis reizen in de eerste klas van de trein, wat tot derving van comfort voor de betalende reiziger kan leiden (naast het feit dat de fraudekosten uiteindelijk ook terechtkomen in het tarief van de reiziger).

Voor de goede orde, het kan wel degelijk zo zijn dat door de introductie van de OV-chipkaart bepaalde oude fraudescenario's (met de strippenkaart) onmogelijk zijn gemaakt, waardoor het netto effect toch positief uitvalt. De door vervoersbedrijven aangeleverde cijfers ten aanzien van de verlaging van het zwartrijden wijzen daar ook op. Het verdient aanbeveling om dit netto effect nader te onderzoeken en de uitkomsten te duiden.

5.4. De wijze waarop deze frauderisico's worden beheerst (deel 1)

Is de behandeling van de risico's binnen een scenario middels maatregelen voldoende beschreven?

5.4.1. Het ophogen van saldo met als doel vrij te reizen

- *Zijn de maatregelen met voldoende detaillering beschreven?*

Ter bestrijding van deze fraude zijn de volgende maatregelen genoemd in hoofdstuk 5 van het rapport: *'hogere frequentie van controles in de backoffice', 'toevoegen extra kenmerk aan transacties'* het *'verbeteren blacklistfunctionaliteit', 'permanent blokkeren'* en tot slot het migratieplan.

Samen met de aanvullende toelichting en documentatie is daarmee een redelijk beeld ontstaan van de voorgestelde maatregelen.

- *Is de effectiviteit van de maatregel(en) (inschatting van de restrisico's) met een voldoende mate van betrouwbaarheid ingeschat?*

Voor het kunnen doen van een schatting over de effectiviteit is van belang dat er voldoende zekerheid bestaat over werkelijke invoering van maatregelen *die onderlinge samenhang kennen*. Maatregelen die samenhang kennen zijn die maatregelen die betrekking hebben op de verbetering van de blacklisting functionaliteit en het permanent blokkeren. In het rapport zelf worden voorbehouden gegeven: *'een aantal maatregelen moet eerst verder uitgewerkt worden voordat tot invoering kan worden overgegaan'.* Dit maakt het lastig om de concrete relevantie van de genoemde maatregelen te achterhalen.

Bij de maatregel *'hogere frequentie van controles in de backoffice'* is een aantal opmerkingen te plaatsen. Ten eerste is de vraag welk percentage van fraude met het ophogen van het saldo inderdaad gedetecteerd kan worden in de backoffice. Vervolgens is de vraag of, *als* een exceptie wordt gesignaleerd, welk percentage met voldoende zekerheid kan worden aangemerkt als zijnde veroorzaakt door fraude (en niet veroorzaakt door een fout of storing in level 1 t/m 4 apparatuur). Naar aanleiding van het bekend worden van de zwakheden van de Mifare Classic in 2008 is door onderzoek van TNO en Royal Holloway vast komen te staan dat niet alle vormen van fraude gedetecteerd konden worden in de backoffice [14]. Naar aanleiding hiervan heeft TLS zelf fraudescenario's opgesteld [2] en tests uitgevoerd om te bepalen welke typen fraude door de backoffice kon worden gedetecteerd [14]. In de test werd een bepaalde fraude (test 2) met ophogen saldo niet zelfstandig gedetecteerd. Mede op basis hiervan is een aantal nieuwe validatieregels geïmplementeerd [4], [16]. Uit gesprekken met TLS bleek dat er geen hertest heeft plaatsgevonden na implementatie van deze validatieregels. Daarnaast kunnen er verschillende redenen zijn voor het optreden van een 'exceptie' in de backoffice [4]. Het kan op fraude wijzen, echter het kan ook veroorzaakt worden door een fout of storing aan level 1, 2 of 3 apparatuur, of door een fout in level 4 (de clearing & settlement backoffice van TLS).

Ten aanzien van de blacklistfunctionaliteit is uit de documentatie duidelijk geworden dat deze nu een beperkt aantal posities kent. Hierdoor kan de capaciteit mogelijk vollopen. Vaker distribueren en een hogere capaciteit kunnen dan effectieve maatregelen zijn. Onduidelijk is welke maximale capaciteit haalbaar is. Deze maatregel is niet bestand tegen doelbewust *blacklist flooding* door aanvallers.

De maatregel van permanent blokkeren wordt beschreven in [10], [11], [12], [13]. Hierdoor worden kaarten geblokkeerd die ook niet meer gedeblokkeerd kunnen worden, noch door een fraudeur, noch door TLS. In welke mate dit consequenties heeft voor het blacklistbeleid wordt niet geschetst. Immers, door falen van deelsystemen op level 1, 2, 3 of 4 kan in theorie sprake zijn van een 'false positive', waarbij een kaart ten onrechte wordt geblokkeerd. In de huidige situatie

kan de kaart weer worden gedeblokkeerd door TLS. In de nieuwe situatie kan dat niet meer. In sectie 1.5 van de rapportage maakt TLS melding van het onterecht blokkeren van kaarten door systeemfouten: '*In vrijwel alle gevallen bleek achteraf geen sprake van fraude maar was de oorzaak een foutieve instelling in en/of werking van het systeem'.* Dit kan betekenen dat bij permanent blokkeren het blacklisten gevoeliger moet worden afgesteld, waardoor er een groter aantal fraudeurs door de mazen heen kan slippen.

Opgemerkt moet worden dat het vergroten van de blacklist of het permanent blokkeren op zichzelf geen sluitende maatregel tegen de fraude. Het zal de business case mogelijk wel minder aantrekkelijk maken omdat de fraudeur nu meer kaarten à €7,50 moet aanschaffen, met extra moeite van dien. Door TLS is niet inzichtelijk is gemaakt in welke mate dit de business case verkleint.

Samengevat zijn wij op basis van de rapportage en de aangeleverde documentatie niet in staat de omvang van het restrisico te valideren, daar het restrisico niet wordt gespecificeerd.

Tot slot wordt in 5.3 het migratieplan genoemd: Het rapport meldt over het migratieplan: *'In de tussenliggende tijd is sprake van een duale situatie, waarbij Mifare classic en SmartMX naast elkaar in de markt bestaan. Om dit technisch te realiseren is de SmartMX chip in staat om de Mifare classic te emuleren, oftewel in een Mifare classic modus te werken. '*. Wij stellen vast dat TLS voorstelt in eerste instantie de SmartMX in emulatiemodus van de Mifare Classic wil gebruiken. Hierdoor is mogelijkerwijs een aantal aanvalsscenario's nog steeds mogelijk. Onderzoek hiernaar is buiten scope van ons onderzoek.

5.4.2. Het ophogen van saldo met doel verzilvering bij balie

- *Zijn de maatregelen met voldoende detaillering beschreven?*

Naast de genoemde maatregelen onder 5.4.1 is voor dit scenario een aantal specifieke maatregelen genoemd onder 4.1: *'Sinds twee weken is een proces ingericht dat bij restitutie een restitutieformulier moet worden ingevuld en de kaarthouder zich bij uitbetaling moet legitimeren. Daarnaast zijn de meeste balies uitgerust met camera's'.* En onder 5.1: *'[…]Een baliemedewerker kan niet controleren of er een legale oplaadtransactie heeft plaatsgevonden. De restitutieprocessen aan de balies zijn aangescherpt door identificatie van de kaarthouder aan een balie te vragen. Daarnaast is een maximum te restitueren bedrag van €30,- van toepassing. Volledige restitutie in geval van hogere bedragen vindt plaats door de backoffice van TLS. In de backoffice bestaat de mogelijkheid om de restitutie nauwkeuriger te onderzoeken.'* Na toelichting en inzien documentatie hebben wij een voldoende beeld van deze maatregel verkregen.

- *Is de effectiviteit van de maatregel(en) (inschatting van de restrisico's) met een voldoende mate van betrouwbaarheid ingeschat?*

De effectiviteit maatregelen is met voldoende mate van betrouwbaarheid ingeschat. Mogelijk zal een kleine populatie 'katvangers' actief zijn, maar gegeven de beperkte omvang van de baten in de vorm van het maximaal te restitueren bedrag, gekoppeld met een aanzienlijke gepercipieerde pakkans zal het restrisico inderdaad laag kunnen zijn.

5.4.3. De frauduleuze check-in

- *Zijn de maatregelen met voldoende detaillering beschreven?*

Ten aanzien van de frauduleuze check-in is, naast het reeds genoemde blacklisting en permanent blokkeren, de volgende maatregel genoemd in 5.2: *'Aanmaken transactie bij controle aan boord. Dit is een uitbreiding op een bestaande inspectiemaatregel, waarbij ervoor wordt gezorgd dat er bij controle een transactie wordt aangemaakt. Nadat deze transactie naar de TLS- backoffice is verstuurd wordt daar de vervalste check-in gedetecteerd en wordt de kaart op de blokkeringslijst geplaatst. De vervoerders moeten bij deze maatregel aanpassingen voorzien in de controleapparatuur en TLS moet de validatieregels uitbreiden.'* Voor deze beschrijving is nadere informatie aangeleverd middels de documenten [7], [8] en [9].

Samen met de aanvullende toelichting en documentatie is daarmee een redelijk beeld ontstaan van de voorgestelde maatregelen.

- *Is de effectiviteit van de maatregel(en) (inschatting van de restrisico's) met een voldoende mate van betrouwbaarheid ingeschat?*

Specifiek voor de maatregel '*Aanmaken transactie bij controle aan boord*': de maatregel gaat uit van het aanmaken van een transactie, waarbij, als in de backoffice blijkt dat deze transactie niet gerelateerd kan worden aan een check-in, de kaart op een blokkeringslijst wordt geplaatst. De blacklist wordt ook ingeladen op de zogeheten MCL, de handheld van de conducteur. In dat geval zal de fraudeur in het voertuig geconfronteerd worden met een geblokkeerde kaart, en wellicht nog belangrijker, daar ook in een afgesloten omgeving (rijdende trein) waar veelal ook andere passagiers aanwezig zijn, op kunnen worden aangesproken. Een dergelijk vooruitzicht kan voor een aanzienlijk deel van de fraudeurs de psychologische drempel om te frauderen te hoog maken. Om dit te voorkomen zou een fraudeur vooraf op een betaalzuil moeten kijken of de kaart al dan niet is geblokkeerd. Dit maakt de transactiekosten voor de fraudeur hoger, en vanwege de camerabewaking kan dit ook een aanzienlijk aantal potentiële fraudeurs afschrikken.

Na implementatie van deze maatregel is het restrisico ongeveer gelijk aan het risico van het ophogen van het saldo.

Voor het overige zijn voor dit fraudescenario dezelfde maatregelen geschetst als onder 5.4.1.

Ook na implementatie van deze maatregelen rondom uitbreiden blacklistfunctionaliteit en permanent blokkeren blijft er sprake van een restrisico. Immers, er is in principe nog een

business case voor fraudeurs die de directe- en transactiekosten van het vervangen van een geblokkeerde OV-chipkaart voor lief nemen (dit zal voor langere ritten het geval kunnen zijn). Wij zijn op basis van de rapportage en de aangeleverde documentatie nog onvoldoende in staat de omvang van het restrisico te valideren, daar het restrisico niet wordt gespecificeerd door TLS.

5.5. De wijze waarop deze frauderisico's worden beheerst (deel 2)

- *Is het plan om de onderkende maatregelen te implementeren van voldoende kwaliteit?*

- *Is er een planning afgegeven inclusief onderbouwing; is deze in voldoende mate realistisch?*

Ten aanzien van de planning van de implementatie van de beheersmaatregelen heeft TLS inzage geven in een invoeringsstrategie, alsmede de onderliggende change notes. Er is sprake van een beheerst wijzigingsproces binnen de OV-chipkaart infrastructuur. TLS geeft een opsomming van de te treffen maatregelen en plaatst deze in afhankelijkheden zoals een positieve kosten-baten analyse.

De federatieve aard van het OV-chipkaart systeem betekent dat implementatie van maatregelen de verantwoordelijkheid van individuele vervoerders is, die elk een relatie hebben met een eigen leverancier. Het doorvoeren van wijzigingen zal geschieden langs deze besluitvormingsgremia. TLS bevindt zich nu in het wijzigingsproces met als gevolg dat nog niet met zekerheid gezegd kan worden dat genoemde maatregelen uiteindelijk ook geïmplementeerd worden.

5.6. Inzicht in de kosten van de beheersmaatregelen

- *Het plan om de onderkende maatregelen te implementeren is van voldoende kwaliteit:er is een kostenoverzicht afgegeven inclusief onderbouwing; deze is in voldoende mate realistisch*

Voor de voorgestelde maatregelen worden kosten en planning opgevraagd bij de leveranciers. TLS stelt dat zij slechts indicatief de bijbehorende kosten van de maatregelen kunnen aangeven. Gegeven de fase waarin TLS op dit punt verkeert, te weten de analysefase, kunnen wij ons dit voorstellen; immers de kosten zijn ook sterk afhankelijk van de wijze waarop de maatregelen geïmplementeerd zullen worden. Daarnaast moet ook hier rekening gehouden worden met de federatieve opzet van het OV-chipkaart systeem. Implementatie van maatregelen komt voor rekening van individuele vervoerders, die ieder bij hun eigen leveranciers een quote dienen uit te vragen. Dit maakt het lastig om op korte termijn met een voldragen schatting te komen van de totale kosten. Het is aanbevelenswaardig om deze indicatieve bedragen zo snel mogelijk te onderbouwen met de hiervoor benodigde besluitvormingsparameters.

5.7. Inzicht in de kosten van het uitstel van het uitzetten van het NVB (strippenkaart)

- *Er is een kostenoverzicht afgegeven inclusief onderbouwing; deze is in voldoende mate realistisch*

In paragraaf 6.3 in de rapportage van TLS wordt een inschatting van de kosten van uitstel van het NVB gegeven: *'Twee systemen naast elkaar betekent dubbele kosten. Het in de lucht houden van papieren vervoerbewijzen (waaronder de strippenkaart) met bijbehorende distributie en verkoopkanalen naast het OV-chipkaart systeem is een kostenfactor. In de huidige situatie(waarbij dus alleen het NVB in de stadsregio's Rotterdam en Amsterdam is uitgezet) wordt uitgegaan van een kostenpost voor stad- en streekvervoerders van tussen de € 10 à 15 miljoen voor 2011 (GVB en RET hebben beiden geen kosten NVB meer). NS raamt de kosten om twee systemen naast elkaar te laten bestaan op minimaal € 10 miljoen per jaar'.*

Wij hebben in een nader gesprek met TLS een nadere onderbouwing van de afgegeven raming verkregen. Deze is voldoende plausibel.

TLS stelt in haar rapportage dat *'Als men wil frauderen, dan kan dat nu dus al. Door het wel of niet uitzetten van het NVB wordt dit frauderisico niet groter (of kleiner)'*. Wij ondersteunen de gedachte van TLS dat het al dan niet uitzetten van het NVB is financieel is niet gerelateerd is aan de fraudemogelijkheden van de OV-chipkaart, in die regio's waar de systemen naast elkaar actief zijn.

6. Referenties

1. *Signing - Beveiliging van de kaartintegriteit*, 16-2-2011, 1.0 definitief
2. *Fraude scenario's – Fraudemanagement*, 11-2-2011, 0.94 concept
3. *Overzicht Validatieregels - Uitleg per exceptie*, 6-5-2010, 1.2 final
4. *Handboek Fraudemanagement C&S*, 14-7-2009, 1.0 definitief
5. *Handboek Regels en Procedures - OV-chipkaart Scheme,* 3-12-2010, 3.1 definitief
6. *Scheme Compliance Assessment,* 9-2-2011, 1.0 final
7. *RfC: Optional simplification of the inspection use case*, 1-2-2011
8. *Inspection Use Case (Ticketing rules use cases),* SDOA 3.2, versie H11
9. *Change note - Optionally no special event in the inspection use case*, 10-2-2011, Rev 5, draft
10. *memo - permanent blocking*, 10-11-2010, 0.2 draft
11. *RfC Permanent Card Blocking*
12. *Aankondiging Scheme Wijziging - permanent blokkeren CSC*, 2-2-2011, concept 0.1
13. *Change Note - Enhancement of Security Measure - permanent blocking*, 1-2-2011, Rev 1
14. *Fraude test resultaten*, 1-7-2009, versie 1.0
15. *Wijzigingsblad naslagwerk customer services*, 10-2-2011, definitief
16. *TNO: Residual Risk in the security of the Dutch OV chipkaart*, 29-6-2009, , H 8 en 9
17. *Short term measures evaluation report*, 29-9-2008, versie 0.9
18. *Recommended short term measures: High Level Designs, 24-9-2008*, versie 0.7