



OV-chipkaart en informatiebeveiliging

Met de invoering van de OV-chipkaart halen de openbaar vervoerbedrijven een complex, transactieverwerkend systeem in huis. Om de kwaliteit van de informatievoorziening te kunnen blijven waarborgen, dient de informatiebeveiliging binnen het ov-bedrijf te worden aangepast aan de nieuwe situatie. Nieuwsberichten over gekraakte kaarten, overtreding van privacyregels en nieuwe mogelijkheden om zwart of grijs te rijden, zorgen voor een verdere druk bij de sector om de informatiebeveiliging op orde te hebben

HENK FEIJEN EN KEES BLOM

Ook vóór de komst van de OV-chipkaart hadden de openbaar vervoerbedrijven belang bij goede informatiebeveiliging. Met de komst van de OV-chipkaart is nut en noodzaak van de informatiebeveiliging echter sterk toegenomen. In dit artikel zullen wij, na een toelichting op de kaart zelf, de belangrijkste redenen toelichten voor de extra aandacht voor informatiebeveiliging. Vervolgens zullen wij inzicht bieden in onderwerpen die aandacht behoeven bij de informatiebeveiliging binnen een ov-bedrijf. Informatiebeveiliging is een breed begrip: het beleid, de processen en beheersmaatregelen

die bijdragen aan beschikbare, integere, vertrouwelijke en controleerbare gegevensverwerking, en aanvullend ook bijdragen aan voorkoming en detectie van fraude en naleving van privacy wetgeving.¹ Omdat het te veel is om alle onderwerpen rond de informatiebeveiliging te behandelen, zullen wij ons in dit artikel beperken tot de risico's en beheersingsmaatregelen die van belang zijn voor de betrouwbaarheid van de informatie, als basis voor een betrouwbare financiële gegevensverwerking en opbrengstenverantwoording.

WAT IS DE OV-CHIPKAART?

De OV-chipkaart is een plastic kaart met een microchip, waarmee de reiziger de ritprijs betaalt en toegang krijgt tot stations. Kaartlezers registreren het begin en het eind van de rit. Dit wordt *check-in* en *check-out* (CICO) genoemd. De reiziger hoeft niet meer van tevoren aan te geven waar de rit naar toegaat. Als een reiziger de kaart voor een check-in terminal houdt, wordt een vooruitbetaling in mindering gebracht op het saldo dat op de OV-chipkaart staat. Als de reiziger het voertuig verlaat en de OV-chipkaart voor de lezer van de check-out terminal houdt, berekent de terminal het werkelijke bedrag van de rit en wordt eventueel een bedrag teruggeboekt, afhankelijk van de ritprijs in vergelijking met het opstaptarief. De ov-bedrijven bieden ook specifieke trajectproducten, die de rei-

Arriva

Arriva is een van de Engelse bedrijven die in de jaren '80 en '90 ontstond door de privatisering van het busvervoer in Groot-Brittannië. Het Britse Arriva groeide al snel uit naar het buitenland en de naam werd gewijzigd in Arriva International. In 1998 nam Arriva International het vervoerbedrijf Vancom Nederland over. Een dochter van Arriva International werd toen geboren: Arriva Nederland. Arriva Nederland breidde al snel verder uit door de overname van VEONN en GADO in 1999. Inmiddels is Arriva Nederland een van de drie grootste openbaarvervoerbedrijven in Nederland.

ziger op de chipkaart kan zetten, bijvoorbeeld de 2-uurrittenkaart in Rotterdam. Deze producten maken het OV-chipkaartsysteem ingewikkelder dan het oorspronkelijke peersysteem in Hongkong, waar primair wordt gereisd met saldo (reizen op saldo).

Ter onderbouwing van de keuze voor het OV-chipkaartsysteem zijn door de politiek en de openbaar vervoersbranche de volgende doelen gedefinieerd:

- De drempels voor gebruik van het openbaar vervoer verlagen. Iemand die eenmaal een OV-chipkaart in bezit heeft, kan daar vervolgens iedere bus, tram, metro of trein mee instappen, zonder dat er tijd nodig is om een vervoersbewijs te kopen. ▣



- De marktwerking in het ov verbeteren. Het gebruik van de OV-chipkaart genereert een groot aantal gegevens over de vervoersproductie. Aan het eind van de dag weet het ov-bedrijf bijvoorbeeld hoeveel reizigers er die dag met lijn 5 zijn vervoerd en of het nodig is om de volgende dag gedurende de spits extra bussen in te zetten. Ook levert de OV-chipkaart betere informatie op over de behaalde resultaten in een bepaald concessiegebied.
- De rentabiliteit van het ov vergroten. De OV-chipkaart biedt mogelijkheden om meer te differentiëren in de tarieven, vooral tussen spits en dalperioden. Dit kan de verhouding tussen kosten en opbrengsten verbeteren.
- Zwart- en grijsrijden beperken en de sociale veiligheid in het openbaar vervoer verbeteren. De OV-chipkaart maakt het mogelijk spoor- en metrostations af te sluiten voor onbevoegden. Een groot deel van de incidenten binnen het openbaar vervoer wordt veroorzaakt door mensen die niet in het bezit zijn van een geldig vervoersbewijs.

Ieder ov-bedrijf geeft zijn eigen chipkaart uit, maar in principe is het de bedoeling dat alle chipkaarten bij alle ov-bedrijven zijn te gebruiken. Alle chipkaarten zijn herkenbaar als OV-chipkaart door het roze logo. Het is de bedoeling dat er drie soorten OV-chipkaarten komen.

Persoonlijke chipkaarten

Dit zijn kaarten die verbonden zijn aan de identiteit van de houder en niet uitwisselbaar zijn. Deze kaart kan opgeladen worden met een bedrag (reissaldo) en alle reisproducten, waaronder abonnementen. Ook heeft de kaart de mogelijkheid via automatische incasso (autoreload) te laten opwaarderen wanneer het saldo te laag is.

Anonieme chipkaarten

Dit zijn kaarten die niet persoonlijk gebonden zijn en door meer mensen gebruikt kunnen worden, maar niet tegelijk. Deze chipkaart kan, net als de persoonsgebonden kaarten, worden opgeladen met een reissaldo en reisproducten als een enkele reis op dagkaart, maar kan geen traditioneel abonnement bevatten. Ook zijn kor-

tingen niet van toepassing als je gebruik maakt van de anonieme chipkaart.

Wegwerpkaarten

Dit zijn kartonnen kaarten voorzien van een chip, voor eenmalig gebruik. Ze kunnen niet opgeladen worden. Een wegwerpkaart bevat een vast aantal dagen of ritten.

De OV-chipkaart is een gezamenlijk initiatief van vijf grote ov-bedrijven, zijnde Connexxion, Gemeentevervoersbedrijf Amsterdam (GVB), Haagse Tramweg Maatschappij (HTM), Nederlandse Spoorwegen (NS), en de Rotterdamse Elektrische Tram (RET). Latere deelnemers aan het project zijn onder andere Arriva en Veolia.

REDENEN VOOR EXTRA FOCUS OP INFORMATIEBEVEILIGING

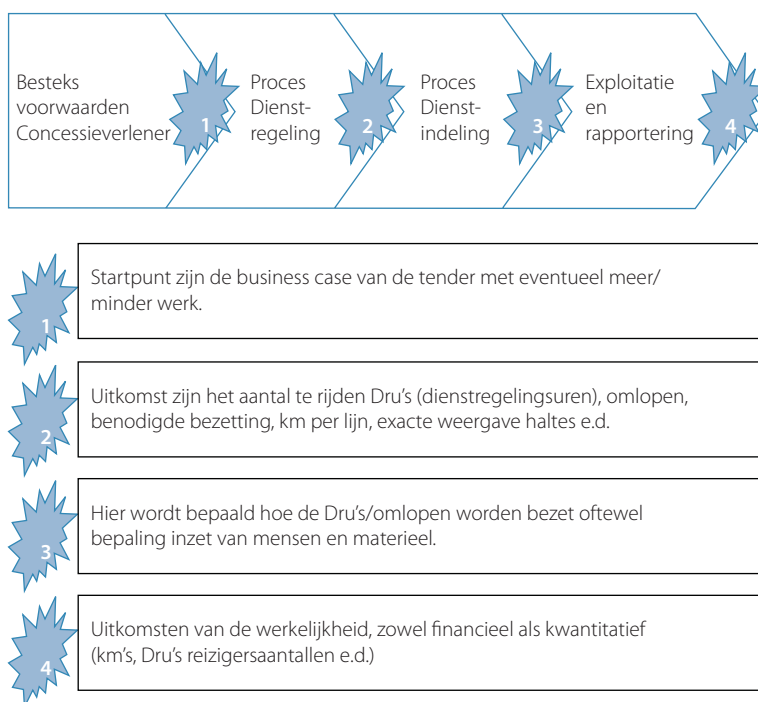
De komst van de OV-chipkaart vraagt extra aandacht voor de informatiebeveiliging. Hiervoor zijn de volgende redenen aan te voeren:

- De OV-chipkaart zorgt voor nieuwe processen en systemen voor het primaire proces en de opbrengstenverantwoording.
- Nieuwe mogelijkheden voor fraude, waaronder de bij het publiek bekende *hacking* van de Mifare-chipkaart.
- Op de OV-chipkaart worden reizen/of persoonsgegevens van reizigers opgeslagen. Echter, de Wet Bescherming Persoonsgegevens moet wel worden nageleefd.
- De toelatingseisen van de centrale partij Trans Link Systems (TLS).

De genoemde redenen worden in het vervolg verder toegelicht.

Nieuwe processen en systemen

Het is natuurlijk niet zo dat door de introductie van de OV-chipkaart het businessmodel en procesinrichting van de openbaar vervoerbedrijven compleet verandert. Nog steeds moeten concessiegebieden worden gewonnen, moeten de dienstregelingen worden opgesteld en ingedeeld,



Figuur 1: Vereenvoudigde weergave busexploitatie

moeten vooral reizigers worden vervoerd en moet financiële en kwantitatieve verantwoording worden afgelegd over de werkelijkheid. Zie figuur 1 voor een vereenvoudigde procesweergave van een ov-bedrijf (bus).

Binnen het hoofdproces Exploitatie & Rapportering leidt de komst van de OV-chipkaart echter wel degelijk tot nieuwe processen en systemen. Hieronder lichten wij dit toe.

Exploitatie en rapportering zonder OV-chipkaartsysteem

De opbrengsten voor gereisde kilometers worden verdeeld en uitbetaald via een landelijk verdeelsysteem. De toegekende opbrengst wordt verwerkt in de boekhouding. Systemen ter ondersteuning van dit deel zijn beperkt tot een boekhoudsysteem, een systeem voor registratie en incasso van verkochte abonnementen en een kassasysteem voor contant verkochte strippenkaarten. Het ov-bedrijf kan in deze situatie geen registratie bijhouden van individuele reistransacties en de hierbij horende opbrengsten.

Exploitatie en rapportering met OV-chipkaartsysteem

Met de komst van het OV-chipkaartsysteem moet het ov-bedrijf een systeem invoeren voor registratie van de verkochte OV-chipkaarten, reissaldo, OV-chipkaart reisproducten en van individuele reisbewegingen. Dit systeem dient vervolgens weer aan te sluiten op het landelijke BackOffice systeem van TLS². Dit betekent voor het ov-bedrijf de bouw en introductie van een complex systeem. Een systeem met interactie tussen verkoop- en controleapparatuur (zoals verkoopterminals en CICO-apparaten), de bijbehorende software, het eigen transactieverwerkende BackOffice systeem en het centrale BackOffice systeem van TLS. Het systeem dient te worden gebouwd op basis van het door TLS ter beschikking gestelde functioneel ontwerp. De openbaar vervoerbedrijven mogen zelf de leverancier voor realisatie van het systeem kiezen.

Toelichting OV-chipkaartsysteem

Om de impact op processen en systemen te kunnen begrijpen, is het noodzakelijk dat eerst wat verder wordt uitgelegd hoe het OV-chipkaartsysteem is opgebouwd. In figuur 2 is een vereenvoudigde weergave opgenomen van het OV-chipkaartsysteem. Hierin kun je zien dat het OV-chipkaartsysteem is opgebouwd uit vijf lagen. Deze lagen zijn:

Level 0

De OV-chipkaarten. Dit is de kaart zelf, een smartcard met MIFARE[®] 4k Classic chip van NXP.

Level 1

Apparaten (Terminals/leesapparatuur). Via interactie tussen de kaart en apparaten vinden verkopen plaats (L1 Sales) zoals verkoop van saldo of reisproducten en vindt registratie plaats van het gebruik van de kaart via Check-in en Check-Out (L1 Usage).

Level 2

Lokale of regionale systemen voor het verzamelen van de op L1-niveau geregistreerde transacties. Zo worden de L1-transacties van een bus verzameld in een L2-computer van het busdepot.

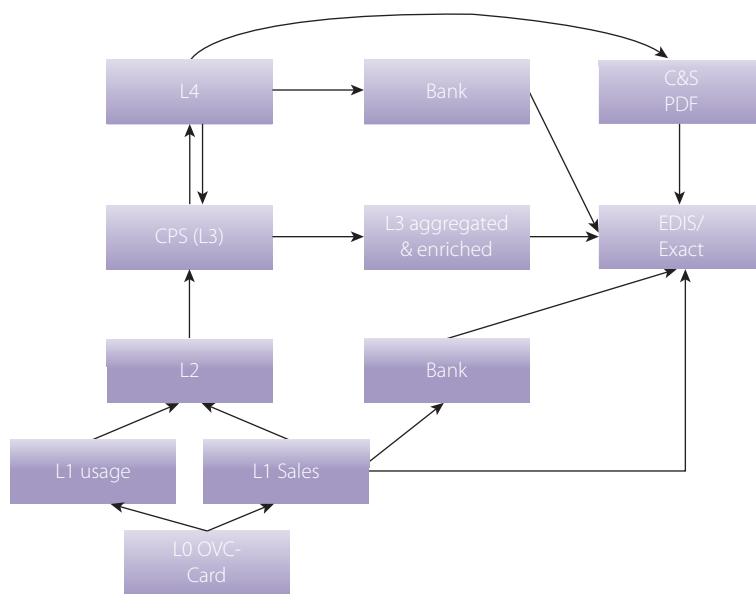
Level 3

BackOffice systeem van het ov-bedrijf. Hierin worden alle via L1 en L2 geregistreerde transacties verzameld. De transacties worden vervolgens één op één doorgezeten naar TLS (Level 4). TLS koppelt via een *feedback file* per transactie terug of wel of niet sprake is geweest van succesvolle verwerking. Ook worden journaalposten aangeboden aan de boekhouding.

Level 4

Centrale BackOffice systeem. Dit deel van het systeem is ondergebracht bij TLS. De transacties van alle vervoerders worden aangeboden aan TLS. TLS zorgt na uitvoering van diverse validaties voor *clearing* en *settlement* van de transacties en zorgt ervoor dat het ov-bedrijf haar opbrengsten krijgt. De weergave in figuur 2 is sterk vereenvoudigd. Elk blok bestaat vaak weer uit vele met elkaar verbonden programma's en dataverzamelingen.

Zoals blijkt uit het hiervoor geschetste beeld van het systeem is de betrouwbaarheid van de opbrengsten van het ov-bedrijf in belangrijke mate afhankelijk geworden van de integriteit en beschikbaarheid van de transacties in het ov-chipkaartsysteem. Ook de ▣



Figuur 2: Vereenvoudigde weergave OV-chipkaartsysteem



verkoop van producten en reissaldo en de correcte administratieve afwikkeling van de reis, is afhankelijk geworden van de werking van het in eigen huis aanwezige systeem. Wezenlijke onderdelen van de bedrijfsvoering van het ov-bedrijf zijn afhankelijk geworden van een complex IT-systeem, waarin nieuwe technieken zijn verwerkt. Adequate maatregelen van informatiebeveiliging zijn daarom noodzakelijk om risico's voor de beschikbaarheid en integriteit van de gegevensverwerking te mitigeren.

Nieuwe mogelijkheden voor fraude

De OV-chipkaart met haar nieuwe technieken biedt nieuwe mogelijkheden voor fraude en zwart- of grijsrijden³. Zo publiceerden hackers in december 2007 dat zij het standaard beveiligingsmechanisme van de MIFARE[®] 4k Classic chip van NXP hebben achterhaald. De OV-chipkaart maakt gebruik van deze chip. Overigens kent de beveiliging van de OV-chipkaart meer lagen waaronder, naast het standaard beveiligingsmechanisme van NXP, een tweede laag in de chip en een derde laag via de transactievalidaties in de BackOffice van TLS. De beveiligingsmechanismen in tweede en derde laag zijn niet gekraakt. Via tientallen in de TLS BackOffice software ingebouwde validaties moeten fraudes alsnog worden gedetecteerd. In de BackOffice worden transacties met een afwijkend patroon gemonitord en, indien noodzakelijk, wordt de kaart bij eerstvolgend gebruik geblokkeerd. In tabel 1 zijn voor enkele voorbeelden van fraudescenario's detectiecontroles opgenomen.

Andere controles die plaatsvinden, zijn controles op dubbele transacties, controles op niet bestaande producten

of kaarthouders of controles op transacties die afkomstig zijn van apparaten die niet bekend zijn, niet via de PKI SAM⁴-procedure zijn aangemeld of als gestolen bekend staan. Als een kaart wordt geblokkeerd wordt deze geblokkeerd in het gehele werkingsgebied van de OV-chipkaart. Dus bij alle aangesloten ov-bedrijven. Tot nu toe zijn geen transacties voorgekomen die duiden op frauduleus handelen met de OV-chipkaart. Aanvullende aandacht voor informatiebeveiliging en maatregelen van fraudepreventie en detectie bij de ov-bedrijven zelf kan verder bijdragen aan reductie van de frauderisico's.

Persoonsgegevens

De angst bij reizigers dat hun reisgegevens in combinatie met hun persoonsgegevens worden misbruikt, heeft gezorgd voor verscherpte aandacht voor de OV-chipkaart van het College Bescherming Persoonsgegevens. Voor de openbaar vervoerbedrijven betekent het dat ook vanuit het aspect 'beveiliging van persoonsgegevens' voeding wordt gegeven aan het onderwerp informatiebeveiliging.

Toelatingsnormen TLS

De meest concrete aanjager van het onderwerp informatiebeveiliging is het normenkader van TLS. Via audits door TLS wordt onder andere de gereedheid van het ov-bedrijf voor operatie volgens het OV-Chipkaart normenkader beoordeeld. Voorafgaand aan de aansluiting van een ov-bedrijf zal het onderzoek zich richten op opzet en bestaan van de aan de OV-chipkaart gelieerde ICT-systemen en organisatorische maatregelen. Na de aansluiting zal periodiek de werking van het geheel van systemen

en organisatie van het ov-bedrijf onderzocht worden om blijvend de goede werking van het OV-chipkaartplatform veilig te stellen. Het gehele normenkader is vastgelegd in een documentatieset, bestaande uit:

- + Handboek Regels en Procedures (HRP). Het HRP beschrijft waar een deelnemer aan moet voldoen. Het HRP is leidend voor alle deelnemers.
- + System Documentation Open Architecture (SDOA). De SDOA bevat uitsluitend functionele eisen die gesteld worden aan systeemcomponenten. Andere kwaliteitseisen ten aanzien van de systeemcomponenten, zoals bruikbaarheid, efficiëntie, onderhoudbaarheid en portabiliteit, dienen door de deelnemers te worden gesteld. De SDOA beschrijft wat kán. Systemen die worden ontwikkeld worden tegen deze maatlat gehouden (=certificatie).
- + Registar-document. Hierin zijn de laatst geldende voorgeschreven parameterinstellingen vastgelegd. De registrar is een set van overeengekomen parameterinstellingen die van invloed zijn op het (interoperabel) gedrag van het OV-chipkaart-systeem.

Specifiek voor het onderwerp 'informatiebeveiliging' zijn in het HRP ook regels en richtlijnen opgesteld.

INFORMATIEBEVEILIGING EN BETROUWBAARHEID

In deze paragraaf beschrijven wij het controleraamwerk dat is opgesteld ter waarborging van de betrouwbaarheid van de informatievoorziening met de OV-chipkaart. Ter bepaling van het *framework* hebben wij in samenwerking met proces- en systeemeigenaren de volgende aanpak gehanteerd:

1. Vaststellen van het uitgangspunt: betrouwbare gegevensverwerking en financiële verslaglegging.
2. Kennis nemen van de OV-chipkaart procesbeschrijvingen en systeemontwerp.
3. Uitvoeren risicoanalyse; per (sub) proces benoemen en kwantificeren van de risico's ten aanzien van de

Fraude scenario	Detectie
Manipulatie van de kaart	De inhoud van de fysieke kaart wijkt af van de inhoud van de kaart van de door TLS beheerde cardmaster database. Detectie onder meer via controle op afwijkend reisgedrag.
Kopiëren van de kaart	Card (card id) is onbekend in de cardmaster database van TLS en valt uit.
Kaart cloning/emulering	Als kaarten (of emulatoren) met hetzelfde kaart ID (een uniek nummer op de kaart) tegelijk worden gebruikt voor reizen zal dit opvallen via de controles op vreemd of onmogelijk reisgedrag.

Tabel 1: Fraude scenario en detectiecontroles BackOffice TLS

juistheid, tijdigheid en volledigheid van de gegevensverwerking.

4. Selecteren van bestaande maatregelen en/of benoemen van nieuw in te voeren maatregelen ter beheersing. Vastlegging in gedetailleerd controleraamwerk.
5. Invoeren en werkend krijgen van de maatregelen.

In navolgende deel hebben wij een samenvatting van het controleraamwerk opgenomen met de hierin opgenomen *key risks* en *controls*. In figuur 3 is het proces- en systeemmodel weergegeven dat als uitgangspunt is gehanteerd voor de bepaling van het controleraamwerk

De risico's en controls zijn uitgewerkt voor a) het inrichten en beheren van het systeem en b) voor het gebruiken van het systeem.

Inrichten en beheren van het systeem

1. Autorisatiebeheer: het toekennen, wijzigen en intrekken van autorisaties op het systeem.
2. Productbeheer: ontwikkeling en configuratie van producten en tarieven in het systeem.
3. Apparatenbeheer: het (de)activeren en aansluiten van, het voeren

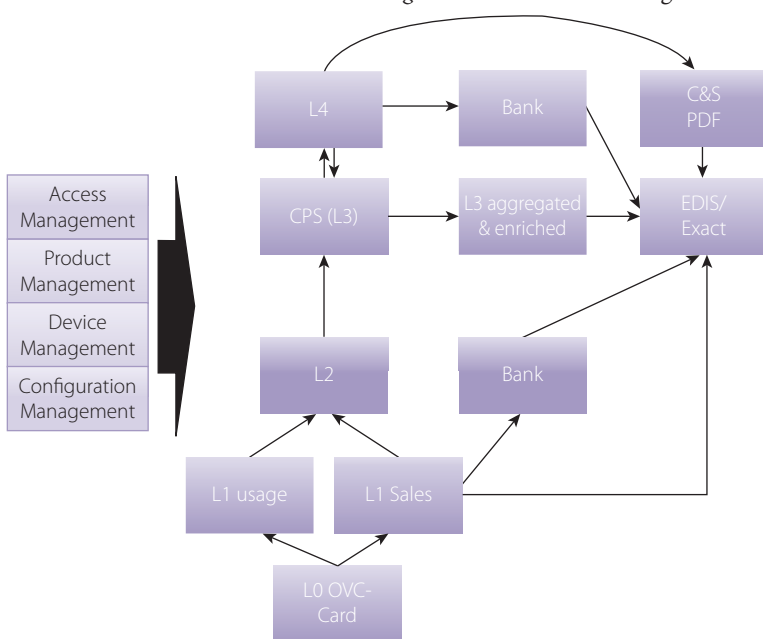
van voorraden met en het registreren van apparaten (zoals check-in/check-out apparatuur, kaart- en saldooverkoop apparatuur).

4. Configuratiebeheer: configureren van het OV-chipkaartsysteem via aanpassing van parameters, tabellen en vast interface waarden.

Gebruiken van het systeem

5. Level 1: front office-gebruik, verkoop en check-in/check-out transacties.
6. Level 2: Tijdelijke lokale/regionale opslag van verzamelde L1-transacties.
7. Level 3: Centrale BackOffice gegevensverzameling, doorsturen van transacties naar TLS, verwerken van TLS-feedback files en voeden boekhouding (Fin Adm).
8. Voorraadbeheer van geld en OV-Chipkaarten.
9. Financiële verslaglegging: opstellen van periodieke financiële verslaglegging over de OV-Chipkaart transacties.

Het risicomodel geeft een beeld van de voor procesbeheersing benodigde maatregelen. De effectiviteit van het model is in de praktijk sterk afhankelijk van borging in goede structuren van *governance* en risicomanagement. In



Figuur 3: Uitgangspunt voor bepaling controleraamwerk

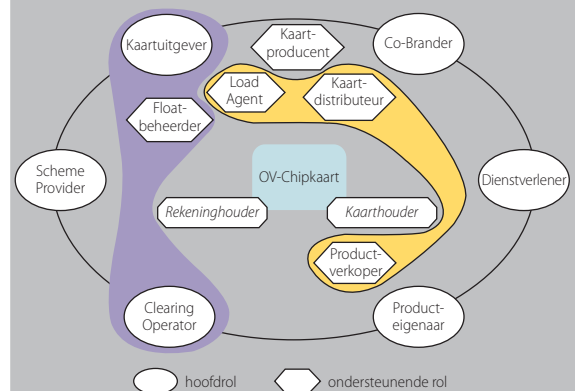
tabel 2 'Controleraamwerk OV-chipkaart' hebben wij de key risks en key controls opgenomen per deelgebied.

ONZE ERVARINGEN MET DE INVOERING VAN DE BEHEERSINGSMATREGELEN

Al vrij snel na de start van het OV-chipkaartproject bij Arriva waren procesbeschrijvingen en systeemontwerpen beschikbaar. Deze documentatie werd namelijk al vrij snel door TLS ter beschikking gesteld en vervolgens bij Arriva aangepast aan de situatie bij Arriva. Hiermee hadden wij al in een vroeg stadium (in jaar 1, 2005) van het project de mogelijkheid om ▣

Betrokken rollen en partijen

In figuur 2 bestaan er feitelijk twee soorten partijen die met elkaar samenwerken: de verschillende openbaar vervoerbedrijven (level 0 tot en met 3) en TLS (level 4). Dit is echter een vereenvoudigde voorstelling van zaken. Nadere beschouwing van het businessmodel van de OV-chipkaart geeft het volgende beeld van de met elkaar samenwerkende partijen en bijbehorende rollen.



Figuur 4: Business model OV-Chipkaart

TLS is de *scheme provider*: de beheerder van de specificaties en (beveiligings)standaarden van het systeem. TLS vervult de rollen in het roze kader: kaartuitgever, floatbeheerder (beheerder van de op de OV-chipkaart geladen saldi) en *clearing operator* (verrekenen van opbrengsten, kosten en oplaadtransacties met de ov-bedrijven). De in het gele kader opgenomen verkopende rollen van *load agent* (mogelijkheid bieden voor opladen van een kaart met saldo), kaartdistributeur en productverkoper (bijvoorbeeld een abonnement voor een bepaald traject) worden meestal uitgevoerd door het ov-bedrijf. Deze rollen kunnen ook door een andere distribuerende partij plaatsvinden (bijvoorbeeld postkantoor). Het ov-bedrijf vervult verder de rol van dienstverlener (vervoeren van reizigers), co-brander (in de markt zetten van OV-chipkaarten met merknamen; bijvoorbeeld met Arriva of NS logo) en producteigenaar (bijvoorbeeld het product NS jaarabonnement). TLS is ook producteigenaar, en wel van het product 'reizen op saldo'.



Deelgebied	Key Risks	Key Controls
1. Autorisatiebeheer	<ul style="list-style-type: none"> • Ongeautoriseerde wijzigingen in de settings van het systeem. • Ongeautoriseerde mutaties in transacties. 	<ul style="list-style-type: none"> • Door proceseigenaren en security officer goedgekeurde autorisatiematrix als baseline. • Verzoek autorisatie wijzigingen gefiatteerd door proceseigenaar. • Periodieke vergelijking werkelijke rechten met baseline en gefiatteerde rechten. • Functiescheiding tussen baseline goedkeuring, goedkeuring aanvragen, toekennen van de autorisaties en de periodieke monitoring.
2. Productbeheer	<ul style="list-style-type: none"> • Inregeling van ongeautoriseerde productwijzigingen. • Onvolledige inregeling of distributie naar L1 van productwijzigingen. • Niet tijdige inregeling/ activering van productwijzigingen. • Onjuiste inregeling van product wijzigingen. 	<ul style="list-style-type: none"> • Product eigenaar dient elk verzoek tot wijziging van producten goed te keuren. • Toegangsbeveiliging en functiescheiding rond de productbeheer menu's. • Change management controls als testen en scheiding van omgevingen. • Acceptatie van de doorgevoerde wijziging door de producteigenaar. • Controle op de volledige en tijdige uitrol van de wijziging naar alle L1 apparaten.
3. Apparatenbeheer	<ul style="list-style-type: none"> • Incorrecte aansluiting of koppeling of registratie van OV-Chipkaart apparaten. • Niet tijdige, dubbele of incomplete aansluiting van apparaten. 	<ul style="list-style-type: none"> • Applicatiecontroles op de uniekheid van een apparaat en de uniekheid van de koppeling apparaat-voertuig-locatie. • Via applicatiecontroles wordt voorkomen dat onjuist geregistreerde apparaten kunnen worden geactiveerd. • De apparatenregistratie functies zijn afgeschermd via autorisatiebeperking. • Elke apparatenwijziging wordt aangesloten op bijbehorend verzoek voor wijziging PKI-SAM en op de administratie van PKI-SAM gegevens. • Periodiek aansluiting tussen geregistreerde apparaten en werkelijk aanwezige apparaten. • Controle op tijdige verwerkingen verzoek tot apparatenwijziging.
4. Configuratie-beheer	<ul style="list-style-type: none"> • Onjuiste of ongeautoriseerde wijzigingen worden doorgevoerd in de configuratie van het OV-Chipkaart Systeem. 	<ul style="list-style-type: none"> • Classificatie van elk verzoek tot wijziging ter aanduiding van kritisch gehalte, impact en/of complexiteit (hoog, midden, laag). • Controle op adequate autorisatie van het verzoek tot wijziging. • Scheiding tussen ontwikkel, test, acceptatie en productie omgeving. • Afhankelijk van de classificatie van het verzoek: vier ogen controle, volledig testtraject of alleen zelfcontrole. • Toegangsbeveiliging op de configuratie menu's. • Bijwerking en goedkeuring van de systeemdocumentatie. • Logging van kritieke configuratie items en periodieke controle op onderbouwing door geaccepteerde verzoeken. • Gebruikersacceptatie op basis van onderbouwde test- of controlebevindingen.
5. Level 1	<ul style="list-style-type: none"> • Onvolledige registratie van L1 transacties • Onjuiste, niet tijdige of ongeautoriseerde registratie van L1 transacties. 	<ul style="list-style-type: none"> • Frequentie trend and error analyse van L1 transacties (per apparaat, locatie, dag van de week etc.). • Applicatiecontroles in het OVC-Systeem ter ondersteuning van juiste registratie van gegevens. • Apparaat registratie procedures inclusief PKI SAM beheer. • Logische toegangsbeveiliging op L1 apparaten (inclusief de verkoopapparaten) • Toegangspoorten, controles op geldig reisbewijs.
6. Level 2	<ul style="list-style-type: none"> • Onvolledige verzameling van de L1 transacties op L2 niveau. • Ongeautoriseerde toegang tot de L2 data. • Onjuiste registratie van de L2 data. 	<ul style="list-style-type: none"> • Periodieke controle op de volledigheid van data aanlevering door alle bussen en alle apparaten. • Aansluiting tussen L1, L2 en L3 transacties onder meer via auditregisters.⁵ • Authenticatie controles: alleen transacties van geregistreerde en geautoriseerde apparaten kunnen worden verwerkt. • Toegangscontrole (fysiek/ logisch) en encryptie van de L2 data.
7. Level 3	<ul style="list-style-type: none"> • Onvolledige registratie van de L1 en L2 transacties op L3 niveau. • Ongeautoriseerde toegang tot de L3 transacties. • Onjuiste registratie van de L3 data. 	<ul style="list-style-type: none"> • Aansluiting tussen L1, L2 en L3 transacties onder meer via auditregisters. • Controles op doorlopende transactienummering. • L3 applicatiecontroles ter borging van de datakwaliteit. • L4 (TLS) validatiecontroles en terugkoppeling door TLS van (in)valide transacties. • Beoordeling en analyse van transacties zonder TLS terugkoppeling. • Toegangscontrole en 'read only' van L3 data.
8. Voorraadbeheer (kaarten en kasgeld en apparaten)	<ul style="list-style-type: none"> • Onjuiste registratie van voorraadhoeveelheden en prijzen. • Ongeautoriseerde toegang tot de fysieke voorraden en tot de data van de voorraden. 	<ul style="list-style-type: none"> • Periodieke aansluiting van werkelijke voorraden met administratieve voorraden. • Fysieke en logische beveiliging van voorraden en voorraadadministratie. • Functiescheiding tussen voorraadbeheer, afstemming en controle getelde met administratieve voorraden, voorraden tellen, voorraad waarderen en afboeken. • Strikte specifieke procedures voor afdracht, registratie en toegang tot kasgeld beheer.
9. Financiële verslaglegging	<ul style="list-style-type: none"> • Onvolledige boeking van de OV-Chipkaart transacties. • Onjuiste of niet tijdige financiële registratie van de OV-Chipkaart. 	<ul style="list-style-type: none"> • Controle op aansluiting tussen de L3 transacties en het grootboek met frequente analyse van tussenrekeningen. • Aansluiting tussen L3 en L4 door gebruikt te maken van de terugkoppeling door TLS via feedback files. Beoordeling van transacties zonder feedback file. • Aansluiting tussen dagafschriften, grootboek (omzet en banksaldi) en de clearing & settlement overzichten van TLS. • Frequentie analyse van claims, niet door TLS goedgekeurde omzet en gerealiseerde kortingen. • Controles op betrouwbare werking interface. • Reguliere controles rond proces van financiële verslaggeving als cijferanalyses, afstemmingen met brondocumenten en- systemen en goedkeuring van handmatige correcties.

Table 2: Controleraamwerk OV-Chipkaart

risicoanalyses uit te voeren en om een eerste versie van het controlemodel, via een bureauoefening, uit te werken. De volgende stap was om de key controls concreet te maken; eigenaren toekennen, in procedures opnemen en invoeren. Dit was op z'n zachtst gezegd wat lastiger. Er was namelijk nog geen systeem. Aangezien het gros van de controls moet worden uitgevoerd met OV-chipkaarttransacties bleek het daarom niet zinvol om veel vaart te zetten achter de invoering van de controls. Pas in 2008/2009 werden steeds meer onderdelen van het systeem in stukjes opgeleverd, getest, soms afgewezen en weer opnieuw getest en kon langzaam aan geoefend worden met de eerste transacties en controles. Via *trial and error* en opgaand met de oplevering van het systeem werd zo heel geleidelijk concrete invulling gegeven aan de controls. Dit schetst direct het bijzondere karakter van de invoering van de OV-chipkaart. Door de geleidelijke oplevering en invoering in kleine brokjes bleek dat van een gefaseerde projectmatige aanpak niet meer te spreken was. Sterker nog: de bekende projectmechanismen als projectplanning, voortgangsbewaking en acceptatie van overgang van de een naar de andere fase, bleken niet toepasbaar. Zo verzuchtte de projectleider eens dat de invoering van het OV-chipkaartsysteem geen project is, maar een proces. Wij denken dat hij daar gelijk in had; de invoering van de OV-chipkaart is een uniek proces. Een proces dat veel vergt van de flexibiliteit en het geduld van de betrokkenen.

TOT SLOT

De invoering van het OV-chipkaartsysteem is voor een ov-bedrijf een enorme klus die vele jaren kan duren. De meeste ov-bedrijven in Nederland zijn al ongeveer vijf jaar bezig met de invoering. Van een *big bang*-achtige invoering is bepaald geen sprake. Nergens in de wereld bestond een systeem dat voldeed aan de in Nederland gewenste, ingewikkelde situatie. Het in Nederland gewenste OV-chipkaartsysteem moest voor het grootste deel nog worden ontwikkeld. De in

het buitenland al in gebruik zijnde smart card systemen⁶ pasten slechts voor een klein deel op de Nederlandse wensen. Een deel van de OV-bedrijven heeft de ontwikkeling laten doen door het East/West consortium⁷, een ander deel door Prodata. Het OV-chipkaartsysteem is erg complex door de eisen van beveiliging, de samenwerking tussen verkoop- en controleapparaten, voertuigen, depotcomputers en administratieve software. De complexiteit wordt versterkt door de situatie dat elk ov-bedrijf feitelijk zijn eigen OV-chipkaartsysteem heeft en dat deze naadloos dient aan te sluiten op het systeem van een landelijke partij die opereert als de beheerder van de OV-chipkaartgelden. Over extra complexiteit door toepassing van interoperabele producten (producten die gebruikt kunnen worden in gebieden van meer dan een vervoerder) hebben we het dan nog niet gehad. De ogenschijnlijk trage voortgang heeft wel als voordeel dat de organisaties redelijk rustig⁸ kunnen wennen aan de nieuwe situatie. Begin 2010 zijn er steeds meer gebieden (concessies) waar de OV-chipkaart operationeel is. Naarmate het aantal reisbewegingen met de OV-chipkaart en het aantal (interoperabele) proposities toeneemt, zal het OV-chipkaartsysteem tot het uiterste

worden getest. Pas nadat alle gebieden zijn aangesloten, kan worden vastgesteld of de OV-chipkaart haar doelen heeft gerealiseerd. ■

Noten

- 1 Deze van gangbare definities afgeleide omschrijving is opgenomen in het beleid Informatiebeveiliging van Arriva.
- 2 Zie het kader over rollen en partijen een nadere toelichting op de rol van TLS
- 3 Grijsrijden is minder betalen dan zou moeten door op oneigenlijke wijze gebruik te maken van de mogelijkheden of mazen van het systeem.
- 4 PKI (Public Key Infrastructure) is een verzamelnaam voor technische en organisatorische voorzieningen om versleuteling en digitale handtekening toe te passen op transacties. Elk OV-Chipkaart apparaat dient te zijn voorzien van een unieke PKI SAM (dit is te vergelijken met een SIM kaart in een telefoon). Deze PKI SAM zorgt voor versleuteling en authenticiteit van de gegenereerde transacties. Het beheer (uitgeven, plaatsen en administreren) van de PKI SAMs in de apparaten dient zorgvuldig te worden uitgevoerd. Mutaties in PKI SAMs worden gemeld aan TLS.
- 5 Auditregisters zijn afzonderlijke tabellen (secundaire stroom) met tellingen van aantallen uitgevoerde transacties op de verschillende levels. Deze auditregisters zijn een belangrijk hulpmiddel voor het maken van de totaalaansluiting tussen de L1, L2, L3 transacties.
- 6 Zoals de Oyster card in Londen, de Octopus card in Hongkong en de systemen uit Sydney, Berlijn en Boston.
- 7 East/West heeft het systeem in Hongkong ontwikkeld.
- 8 Op het gebied van systeemontwikkeling worden wel al heel lang alle zeilen bijgezet.



H. (Henk) Feijen MSc is controller openbaar vervoer bij Arriva Nederland. Voordat Henk als controller begon, heeft hij gewerkt als European internal auditor bij Arriva Plc en als accountant bij KPMG. Henk heeft voor de afronding van zijn RA-studie aan de Business Universiteit Nyenrode zowel zijn theoretische- als praktijkscriptie geschreven over de invoering van de OV-chipkaart. Voor de theoretische scriptie heeft Henk een *case study* uitgevoerd met de gevolgen van de invoering van de OV-chipkaart op het interne beheersingskader bij ov-bedrijven.



Drs. G.C. (Kees) Blom RE RA is gevestigd als zelfstandig adviseur op het gebied van financieel- en informatie risicomanagement. Voor de invoering van de OV-chipkaart en het bijbehorende OV-chipkaartsysteem bij Arriva heeft Kees ondersteuning verleend bij het aanpassen van interne beheersing en informatiebeveiliging aan de OV-chipkaartsituatie.