3) 1

Review of the *Project Plan* and *Regional Fraud Management Plan* *by RHUL*

08.09.08

1. Introduction

As a result of the counter expertise (CE) review of the TNO report concerning the Mifare Classic security problems and the OV-Chipkaart, the Information Security Group/Smart Card Centre (ISG/SCC) of Royal Holloway University of London (RHUL) advised to set a migration planning Milestone (MPM) prior to the national roll-out of the OV-Chipkaart. The public transport companies have adopted this RHUL recommendation to develop a *migration plan* for the transition to a new card technology. Following on from this recommendation by RHUL, the Ministry of Transport of the Netherlands (VenW) requires Trans Link Systems (TLS) and the public transport operators (PTOs) to have a *migration plan* in place, prior to lifting the general obligation to accept the paper-based Strippenkaart in local and regional Dutch public transport. However, the Rotterdamse Elektrische Tram company (RET) and TLS have asked permission to discontinue the Strippenkaart in Rotterdam prior to the general decision referred to above. For an informed judgement on this request, VenW required RET and TLS to submit the following documents[1]:

- A *regional fraud management plan* for Rotterdam, for the period preceding the MPM
- The *project plan* for realising the *migration plan*, by the MPM

VenW assigned RHUL to review these documents with respect to a number of criteria defined in the letter of assignment (VenW/DGMO/2008/1296). The Het Expertise Centrum (HEC) was responsible for general facilitation of the task and acted as the interface between VenW and RHUL.

2. The Review Task and Adopted Methodology

RHUL was asked to carry out an urgent review of two documents i.e. the *regional fraud management plan and* the *project plan*. Whilst it would have been feasible to carry out two separate studies, a single combined review was adopted due to the close linkages between the documents and the underlying activities to which they relate. It should be noted that both input documents supplied to RHUL were marked as confidential and supplied under the NDA with TLS. There was a reliance on TLS to check this document for "leaked" confidential information prior to release, however none was found. Note also that the original CE report from RHUL is now a public document and so where appropriate may be used as a background reference.

This review will proceed by first recapping on the significance of the migration planning Milestone (MPM) and clarifying its meaning in order to remove some persistent misinterpretation. This section will also summarise some of the critical criteria from VenW with respect to the final *migration plan* and provide some brief information on the Rotterdam network. The report will then go on to review the *project plan*. Note that for the avoidance of doubt, the *project plan* is the

[1] Towards the end of the review, VenW also provided a copy of the original terms and conditions for discontinuing the obligation to accept paper-based national transport tickets (pre Mifare problems)

detailed plan of activities and preparations to create the *migration plan* (as evidence of a state of migration readiness) by the MPM; it is not the *migration plan* itself. When reviewing the *project plan* with respect to the VenW criteria we are considering whether those criteria are likely to be satisfied by the MPM, given the scheduled activities/tasks defined within the *project plan*. The next section of the report will consider the *regional fraud management plan* for Rotterdam with respect to the main VenW criterion. Essentially VenW seek assurance that the measures set out in the *regional fraud management plan* form a good basis to manage fraud risks and support customer service processes with the present Mifare Classic OV-Chipkaart in Rotterdam, in the period between transfer to an e-ticketing only solution and the MPM. The background to this is the request from TLS and RET to abolish paper based tickets (Strippenkaart) in Rotterdam prior to the MPM date. The final section of the report will draw conclusions from both of the reviewed plans and recommendations will be made.

2.1. Clarification of the Migration Planning Milestone

The MPM was described in the original CE report from RHUL.

> *"The CEB strongly recommends an earlier interim milestone referred to as the* migration planning ***Milestone****, set for January 2009 to coincide with the scheduled completion of the national roll out for the current system. This is to ensure that from the start of nation-wide usage there is a state of preparedness for the migration to a higher level of card security. The migration plan should define all necessary activities, involved parties, budgets and technology. Providing open communication on progress towards the milestone may have a deterrent effect on attackers and the independent review of draft versions of the plan should provide added confidence that migration will succeed. It would require significant activity prior to the milestone, such as conducting a structured risk analysis, identifying the new card technology, defining infrastructure upgrades, selecting suppliers, arranging budgets and all other normal logistic and project planning details. These steps, which are similar to those suggested by TNO, would stop short of any physical deployment. The final decision to start the migration could take place some time later, based on agreed processes and triggers (such as the measured level of fraud[2]) defined within the migration plan."*

According to the information in RHUL's current assignment from VenW, the MPM target date has regrettably (in RHUL's opinion) been shifted to June 30th 2009, by which time TLS is required to submit the formal *migration plan* to VenW for consideration. The *migration plan* will provide evidence that TLS and the PTOs have reached a state of readiness for migration to a new card technology.

There still appears to be some confusion over the interpretation of the MPM and a simple way to consider the milestone is as the first availability of a card migration "GO-Button". If the "GO-Button" is pressed, the *migration plan* simply *executes* and the transport systems are comprehensively upgraded to accommodate the new card technology. This is possible because all the activities requiring evaluation, selection, allocation, and general technical and business decision making must be finalised before the MPM. The only outstanding decision for a "GO-Button", is

[2] Attributed to the card security issue

when to press it and the conditions for this (including who has the authority to press the Go-Button) shall be unambiguously defined within the *migration plan*. The *migration plan* recommended by RHUL does not include any shorter term remedial measures (SRM). The use of a SRM is considered as part of normal day to day business and fraud management operations; and if a SRM is of significant value it should be implemented well before the MPM.

The *migration plan* delivered by the MPM should be referred to as the *baseline migration plan* and this will be used as the basis for the VenW decision on whether to approve the nationwide withdrawal of paper tickets. It is conceivable that the triggers for the "GO-Button" will not occur for some time and so there is a danger that elements of the plan become obsolete, if for example a supplier is no longer favoured or if improved technical components become available. The *migration plan* may therefore be revised and submitted for approval under a scheme acceptable to VenW[3]. At any given time after the MPM, it is the most current "approved" plan that would be *executed* by the "GO-Button".

As a further measure to avoid potential confusion, the withdrawal of Strippenkaarts from a network will be referred to as Paper Ticket Withdrawal (PTW) and not migration.

2.2. The VenW Criteria

The majority of the VenW criteria relate to the *migration plan* itself. They include:

- Risk Assessment
  - Is there an adequate assessment of the security risks associated with the current chip card technology?
- Security Architecture
  - Is the Security Architecture adequate[4] in light of the identified risks?
- Chip(card) selection
  - Has a chip been selected with an open cryptology[5]?
- Infrastructure upgrades
  - Is there a good overview of the required infrastructural changes needed to migrate?
- Vendor plans
  - Are adequate contingency plans agreed with the main (selected) vendors to execute their role in the overall plan?
- Activity plan
  - Is there a realistic activity plan in which the main activities have been identified and assigned to the main actors involved?
- Decision Framework[6]
  - Is there a Decision Framework with clear steps and fitting triggers and criteria to guide the decision making process with regard to short-term measures or migration, inclusive the decision making process itself?
- Budgets
  - (Declared out of scope for this review/assignment)

[3] VenW would not directly approve revisions to the *migration plan*, but would ensure a responsible process was in place

[4] It would be better to seek an optimal rather than adequate Security Architecture

[5] The meaning of this is discussed in section 4.2.1

[6] Although not explictly stated in the VenW criteria, it is critically important to define who has the authority to make the final migration decision.

The criterion for the *project plan* is.

- Whether it is reasonable to expect a compliant *migration plan* by June 2009

The above criteria could have been predicted from the original RHUL CE report: however, the request to abolish paper tickets creates new criteria.

- Do the measures set out in the ***regional fraud management plan*** form a good basis to manage fraud risks and supporting customer service processes with the present Mifare Classic OV-Chipkaart in Rotterdam in the period between transfer to an e-ticketing only situation and the MPM?

2.3. The Rotterdam System

Rotterdam has been a pioneering system for the use of the OV-Chipkaart. The following quote is taken from the official website http://www.ov-Chipkaart.nl

> *"The OV-Chipkaart launch is carried out in phases throughout the Netherlands. At the end of 2005, Rotterdam was the first to launch the use of the OV-Chipkaart. The OV-Chipkaart has been used to pay for journeys on the bus, train and metro owned by Connexxion, the NS (Dutch Railway Company) and RET since December 2006 and in the RET trams and busses since July 2007."*

Currently, the Rotterdam system supports both the OV-Chipkaart and the Strippenkaart paper tickets. Customers have been warned that the paper tickets are expected to be withdrawn (PTW) when VenW decides that the time is appropriate. TLS and RET[7] would like the PTW decision for Rotterdam to be made now.

[7] Note only RET was mentioned in the input documents and not the other companies mentioned in the website quote.

3. The *Project Plan*

The project plan describes the activities to reach the MPM. The version that was reviewed in this report was dated 1st August 2008 and its creation was a result of a request by TLS/RET to discontinue the use of paper tickets in Rotterdam. To consider the request, VenW asked for the *project plan* (and *regional fraud management plan*) to be provided for independent review.

The *project plan* would be expected to include activities from the 1st August 2008 until the MPM, but does not necessarily include all activities initiated by TLS and the PTOs. TLS have provided additional overview information on a "Security Program". The Security Program appears a positive response to the recent security problems and the information describes, in high level summary form, a number of projects and process initiatives. The main projects are listed below.

- Fraud Monitoring and Management
    - Optimisation of existing fraud management systems and processes
    - First deliverable: The Rotterdam *regional fraud management plan*
- Short Term measures
    - Assessment of short-term remedial measures that may improve security and fraud detection
    - Progress not yet reported
- Migration Plan
    - Work to reach the MPM
    - First deliverable: The *project plan*

Secondary projects included within the program are.

- Life Cycle Management
    - Relevant to Security evolution and management, but also designed to improve general technical and business flexibility to support adaption to changing scenarios and conditions
    - Progress not yet reported
- Card Reader Solution
    - Evaluation of card reader options to provide secure, cost effective and future proof solutions for current and future business needs
    - Progress not yet reported
- Overall Security Management
    - To manage an overall and structured approach to organisational risk assessment.
    - Progress not yet reported

The Security Program is also intended to contribute a number of process initiatives

- International Co-operation
    - Information exchange and collaboration with similar international transport schemes
- Academic Exchange
    - Support for forums and investigation assignments
- Supplier Responsibility
    - To coordinate how suppliers will contribute to improved security solutions
- Stakeholder Management
    - Mentions the relationship with VenW
    - No other stakeholders explicitly mentioned

3.1. The Objective of the *Project Plan*

The stated objective of the *project plan* is to reach the MPM. The quoted requirement for the MPM is a reasonable, but not fully precise, interpretation of the original CE report, as the *project plan* mentions long distance travel or complete coverage in the Netherlands. The linkage to national coverage actually relates to the value of the assets that are protected i.e. the ticket values rather than the fact that a passenger is travelling a long distance (although the two are normally linked). Complete coverage of the Netherlands with standalone regional systems would not necessarily result in high ticket values.

3.2. Phasing and Deliverables

The project plan describes three phases of activity, which when fully detailed should address all the criteria required by VenW. Each phase produces some documented output allowing VenW or its nominees to carry out independent reviews if and when required.

- Phase 1 (July-October 2008) includes much of the technical/security evaluation, selection and design work
  - Deliverables
    - Structured Security Assessment
    - Card Selection
    - High Level Design of Security Architecture
- Phase 2 (Nov 2008 – January 2009) the core contribution is to define infrastructure upgrades, with secondary activity related to the Decision Framework (migration trigger)
  - Deliverables - TBA
- Phase 3 (Feb-June 2009) detailed planning and contractual/pricing activities
  - Deliverables - TBA

Detailed planning and deliverables are currently only defined for Phase 1. Outline plans are available for Phases 2 and 3.

3.3. Phase 1 of the *Project Plan*

Phase 1 of the project plan is shown as four sub-projects (listed below) each sub-divided further into a number of sub-tasks.

- "CC + Risk Analysis"
  - The main purpose of this task is to carry out and document a risk assessment according to a selected methodology and an associated workshop: and to then develop a Security Target based on a Common Criteria approach

- "Card Selection"
  - This is aimed at selecting a new card technology and runs in parallel with the CC + Risk Analysis task

- "HL Architecture"
    - The primary purpose of this task is to develop the high level design architecture and it starts after a draft ST document is available
- "Cost Estimates for Phase 2/3"
    - The meaning is self-explanatory

A first draft of the *migration plan* is made available at the end of Phase 1.

3.3.1. Phase 1 Deliverable Definition

The *project plan* describes three deliverables for Phase 1.

- Structured Security Assessment
- Card Selection
- High Level Design of Security Architecture

The deliverables are all assumed to be documents that would be available for review[5]. Each deliverable has a brief description and the remaining information is really relating to the task(s) and resources that created it. This information indicates some generic roles/resources, the activities to be carried out, relevant quality criteria and topics that are, or are not in scope.

3.4. High Level Project Organisation

The *project plan* is a deliverable from the Migration Plan project that is part of the broader Security Program. The Security Program is the responsibility of the Program Director who is a member of the TLS executive board. TLS state that there are sufficient resources to complete all envisaged projects and that there are weekly meetings between project leaders and the program management.

For changes at National level (involving PTOs) there is a pre-existing process for introducing changes to the transport scheme/systems. This is known as the National Change and Release management process. This involves the National Change Advisory Board (NCAB) and the National Release Board (NRB). NCAB handles the technical aspects of the request and NRB considers business aspects before giving final approval.

An overview of the normal (non MPM) process was provided with supporting information; however, the detail of who does what was not entirely clear. There is a "participant domain" although this term is not defined. The overview diagram shows change requests generated by PTOs although TLS and suppliers are not mentioned. There is a "national domain" that carries out a scheme compliance assessment and drafts a Change Note, but it is not stated who leads/resources this. The "combined domain" is the combination of the NCAB and NRB. Whilst it is mentioned that all "participants" have a seat on the NCAB, the representation on the NRB (that takes the final decision) is not stated.

[5] TLS should confirm this assumption

3.5. TLS Own Risk Evaluation for the *Project Plan*

TLS has quite rightly and responsibly tried to identify risks to the activities in the *project plan* and where necessary introduced mitigating measures. The main risks identified by TLS were lack of resources, lack of expertise, insufficient reviews and effective decision making by TLS/PTOs. TLS addresses the resource issue by planning to involve TLS and PTO staff. For added expertise and reviews, third party experts are involved including TNO, Thales and VenW nominees. According to TLS, the approach to motivating effective decision making appears to be milestone pressure created by external reviews, public deliverables and blocks on some business initiatives e.g. roll-out of OV-Chipkaarts or abolishment of Strippenkaarts.

4. *Project Plan* Review

4.1. Review of Planning

Only the planning for Phase 1 can be reviewed as the other phases are still at an outline stage. The first observation is that there is a lot of challenging activity in Phase 1 that is scheduled for completion by the end of October 2008. Although the time pressures are understood, the review and design of security systems never benefits from being rushed and so TLS has the responsibility to ensure that its plans and timescales are realistic and will not compromise quality.

Risk analysis via workshops can be quite time consuming because of the need to collect opinions/information from various parties and there is often an iterative approach used to refine and document the findings. If RHUL were considering such an exercise then at least two workshops (as opposed to the one in the plan) would be scheduled, as typically there can be significant discussion and input after the draft from the first workshop is circulated. To complete this task in one month and during the August 2008 holiday period seems quite ambitious. The risk could be either that the milestone slips or perhaps that not all relevant inputs and views are captured in the analysis.
It is not clear how the risk analysis fits with the Fraud Monitoring and Management project (under the Security Program) that delivered the *regional fraud management plan* for Rotterdam. Typically a risk assessment will initially focus on the risks to the system, assets to be protected, attack methods and existing detective and corrective measures. The deficient areas will then generate recommendations for optimisations, short term improvements and the initial requirements for improved security solutions (migration). According to the *project plan* the risk assessment will not complete until the end of August 2008, whereas the regional *fraud management plan* is dated 1st August 2008. This raises a concern that there may be independent or duplicate regional/national risk assessments and if so are the results and decisions consistent? TLS should be asked to clarify the following anomalies.

- If there is a single risk assessment, who is in charge of it (and makes the decisions) and on what basis was the *regional fraud management plan* issued before the risk assessment was due to complete?
- If multiple risk assessments are performed who is in overall charge of them and how is consistency of output maintained?

Following the risk assessment[9] there are tasks to define a Common Criteria (CC) Security Target (ST). This is usually a precursor to the formal CC evaluation of a system. Evaluations to recognised levels can be very positive from a security perspective, but can also be very time consuming and will rely on a precisely defined ST. Although no mention is given of a planned CC evaluation it is questionable whether the ST could actually be completed in one month bearing in mind that the card selection task is running in parallel and the work on the High level design does not start until the draft ST is available. TLS would be advised to re-check with their CC advisors that the time available is adequate to produce a quality ST and how it would be used in the Phases that follow.

The Card selection activity is shown as a span task in the planning chart so no timing details are provided for detailed sub-tasks; the task should be expanded further. Within the text of the *project plan* it indicates that the activities will involve identifying card replacement candidates and

[9] Note there was no explicit mention of Mifare Light cards being considered in the assessment.

developing a scoring process for structured comparison. It also appears to use input from other tasks (although the references are not consistent with the planning chart), timing and cost issues, residual risks and the decision document (relates to migration triggers). The start of the card selection task seems to pre-date all other tasks, but unexpectedly appears close to completion before the risk assessment and ST work has completed and before the HL architecture work has started.

The HL architecture task is compressed to within one month and does not start until the card selection task is almost finished. This phasing is unexpected as the HL work would have been expected to run in parallel with the card selection task. The reason is that the two designs are critically linked. For example if another symmetric key algorithm approach is chosen (as used for Mifare Classic) that may have the least effect on the infrastructure architecture and dictate a certain set of candidate cards, whereas if a PKI approach (as noted to be within scope of the security assessment) is used, this would have more impact on the architecture, card choice, KMS and performance issues.

The last part of Phase 1 is for quotations for the work in Phase 2 and 3. Whilst this is the least technically demanding of the tasks, two working weeks may be overly ambitious if quotes are based on detailed specifications.

The general impression is that the time allocated to complete Phase1 seems too short and the phasing of the sub-tasks is puzzling.

4.2. Review of Deliverables

The "Structured Security Assessment" deliverable records a structured risk assessment of the OV-Chipkaart system, focussing mainly on the card (L0) the access devices/readers (L1) and the TLS back office systems (L4), with respect to particular issues arising from the Mifare Classic attacks. The execution of the task appears to be outsourced to Thales CEACI[10], which may have influenced the selection of the EBIOS methodology, although it is not clear which organisation is providing the "Risk Expert" to lead the task. Given that risk assessment benefits from interaction with many internal staff and experts, TLS would be expected to lead and facilitate the task, using Thales expertise as appropriate. Interestingly, under the deliverable definition the ST work is described as a parallel activity, although it is shown as sequential within the plan. It is unclear if the deliverable is just the output from the risk assessment or whether it will also include the Security Target. Most relevant technical aspects are defined to be within the scope of the task/deliverable although organisational aspects and IT/Website issues are excluded.

The "HL Design of the Security Architecture" deliverable is described as a reference for the card selection and for developing the Specifications Document Open Architecture (SDOA) and should also detail work package requirements. It mentions that the HL and card selection will interact to ensure a fitting combination; however, the phasing of the work plan does not seem to reflect this, with the HL work starting after most of the card selection activity. In the activities list it states that the HL design is based on the selected smart card and the risk assessment work, which adds weight to the suggestion that the card is selected before the HL design is considered. It is not clear which organisation leads the task although PTO technical experts and Thales Transport are involved in the

[10] This is a respected lab that carried out the CC evaluation on the ITSO Security Application Module (ISAM)

project execution along with security and smart card specialists. The quality criteria are mainly to ensure that there is adequate detail to redefine the SDOA and begin some prototyping.
The "Card Selection" deliverable/task is a structured and documented procedure for selecting a new card technology as part of the overall security architecture. The activities appear typical for a systematic product scoring and selection process. It is not clear which organisation leads the task, although it is noted that PTO experts are involved as well as security and smart card experts. New business requirements are declared out of scope, which seems rather short-sighted. The quality criteria correctly notes that the requirements from the security assessment should be accommodated, but it is difficult to see how the HL design can be satisfied when the related tasks seem to happen after the card selection task. The quality criteria also include "Open Cryptology". This is an ambiguous term and not defined within the *project plan*. It is therefore necessary to explore the possible meaning of this term and how it relates to security and commercial issue.

4.2.1. What is Meant by Open Cryptology?

Cryptology is a term used for the combination of cryptography (code making/use) and cryptanalysis (code breaking). Our interpretation of the VenW criterion is that it is really "Open Cryptography" that is of primary interest. The following description will therefore focus on cryptography, although we are of course looking for a solution that will render cryptanalysis ineffective.

From a security perspective we would like to see a card technology based on cryptography that can be seen to be fit for purpose i.e. it is available for critical review, it satisfies all requirements identified from design, risk assessment and aggressive testing viewpoints. In helping to find an appropriate solution we recall the following principles.

a) The security of the solution should not rely on the secrecy of the algorithm
b) The key size should be in accordance with international recommendations
c) The algorithm implementation should resist attacks made against implementations

It is reasonable to assume that some published algorithms (such as AES/RSA) are considered fit-for-purpose because they have survived rigorous review by international experts. We also know that it is possible to implement such algorithms in a manner designed to resist attacks and that this attack resistance can be rigorously tested by commercial laboratories.

There may well be unpublished/proprietary algorithms that are just as good (as published algorithms), having been expertly designed, reviewed and tested in a rigorous manner, however there will always be greater scepticism when an algorithm is kept secret. It is a general recommendation of RHUL that cryptography used in systems of national importance be based on algorithms that have been made available for public/expert scrutiny.

One definition of the "Open Cryptography" criterion could be the use of published algorithms that have been successfully evaluated by the expert community. The term "Open" can also relate to Intellectual Property and Licensing. Ideally the algorithm should be free to use and not bound to restrictive licences or mandatory fees. Whilst this is primarily a commercial issue that affects the costs of cards, infrastructure and choice of supplier it could become a security issue if commercial licence requirements create a market for counterfeit products. It is also possible to have an "Open Framework" for cryptography, whereby one or more of a range of algorithms could be used because the interface conforms to an Open Standard. This would allow systems to use either "free" or licensed algorithms depending on security and commercial choice.

4.3. Review of High Level Management

In the normal change management process of TLS/PTOs, once a change has been approved there is an obligation for all participants to implement it (although the permitted timescale for implementation was not defined in the input documentation). In the case of the *migration plan* we require the process to approve the *migration plan*, but not begin implementation until the Decision Framework (still work in progress) triggers execution of the *migration plan*. It is thought likely that the Decision Framework itself will also result in scheme changes prior to migration as it requires a new operational and decision making process plus supporting tests, trials and statistics gathering.

Whilst the national organisation and change control processes appear quite typical and claim to involve senior decisions makers within the appropriate organisations, they risk introduction of delay into the migration planning process as the NCAB and NRB will need adequate time to review and discuss the technical and business aspects of the proposed *migration plan*. It is also important to avoid duplicating the discussion process once the trigger conditions are met. The only activity should be then to confirm that the trigger conditions are indeed correct and then to publish the associated Change Note(s) for mandatory execution of the *migration plan*.

Greater clarity is required regarding who actually makes the change note decisions within the NRB and in particular who will approve the *migration plan* and decide when the migration trigger conditions are met.

4.4. Review of TLS own Risk Evaluation for the *Project Plan*

There are a few risk reduction decisions that should be noted from TLS's own work on risk identification and mitigation for the *project plan*.

- Because of the time pressure on HL Security Architecture and Card Selection tasks, the mitigating measure is not to consider new business requirements. This could be a mistake that has significant business impact in the future. Smart Card systems often suffer because "legacy" problems are designed in due to time and cost pressures. Whilst there may be insufficient time to consider particular new business initiatives in detail, it is recommended that some reasonable efforts are used to ensure that migration technologies will have flexible security and application enablers to support future products and services.

- The Chip Selection is described as starting from an existing short-list supplied by TNO. The criteria used to search for products and compile this initial selection are unknown. Clearly the list should be as comprehensive as possible and any significant filtering should be confined to the Chip Selection task. The list was not provided as an input document for this review.

- There is a risk that not all infrastructure upgrades can be identified adequately. The mitigating measure proposed by TLS (to cope with time pressures), is to deal with the major suppliers to ensure that at least 80% of the upgrades are covered. This is only a reasonable compromise if the 80% includes all security critical upgrades and does not leave a "weak link" in the system. TLS should confirm that all security critical upgrades are being addressed.

- Another concern voiced by TLS is being able to define upgrades in sufficient detail that suppliers will be able to provide quotations/offers for the work. The mitigating measure is to prioritise the writing of specifications on the critical upgrade path. Whilst this is a way of optimising the time available within the *project plan* it does not alter the fact that all the specifications/offers are required to be finalised before the MPM.

- The Decision Framework discussion mentions a risk to do with "not knowing about alternatives to migration and lack of knowledge of threshold values to put into the trigger process". However the requirement for a trigger mechanism in the *migration plan* is quite simple; if a certain combination of factors occurs then the "GO-Button" is pressed and the *migration plan* is executed; migrating to the new card type/technology. Any useful SRMs may be introduced earlier as normal day-to-day business in order to delay migration by keeping the *migration plan* trigger factors below tolerable thresholds. An additional risk not mentioned by TLS is uncertainty over who makes the final decision to press the "Go-Button".

- Monitoring of back office reports and statistics is important both in determining factors to contribute to migration triggers and the thresholds to apply. The factors should not only be the level of revenue lost to relevant fraud, but also the costs of remedial measures and processes, the frequency of exploits and the detection and classification of exploit types.

- Quality Controls for the three sub-projects are mainly ensured by internal and external reviews. Regarding a statement with the High Level design under quality it says that "the HL design should be highly compatible with the existing infrastructure". Whilst the desire for this is understandable it seems to conflict with the less restrictive scope of the HL tasks.

4.5. Summary and Review with Respect to VenW Criteria

The criterion for the *project plan* itself is simply whether it is reasonable to expect a compliant *migration plan* by June 2009. VenW has confirmed that "compliant" means addressing all the VenW criteria (for the *migration plan*) and being a detailed "execution-only" plan, with all decisions, comparisons, selections, negotiations, costing, budgeting and detailed planning and contracts having been completed during the *project plan* period. The *migration plan* will include the main execution plan (changeover to a new card/technology) and an unambiguous definition of the decision factors and authorised parties that trigger it. Any SRMs should be described within the appropriate *regional fraud management plans* and not within the *migration plan*.

Based on the documentation received from TLS, it is evident that TLS has embraced the VenW requirements and the recommendations from the original CE report. Considerable resource appears to have been committed to the project plan, and wider initiatives (Security Program) have been introduced which extend beyond the requirements for the MPM. The initiatives should help improve risk management and the handling of fraud and security issues for the future benefit of TLS, the PTOs and the confidence of the travelling public. Considering the current version of the *project plan* it would appear that all the VenW criteria are being addressed within the planned tasks, although the answers to the VenW questions are still unknown; being work in progress. The contributions and responsibilities of the various parties to tasks addressing the VenW questions are not fully defined; and this is a cause for concern, although the skill sets and expert third parties are defined for some initial tasks.

The completion of the Phase 1 work in a manner that will adequately meet all objectives appears extremely ambitious (especially with respect to timescales). Risk assessment workshops are advisably iterative over multiple workshops and the availability of key personnel (TLS/PTOs and third party experts), the time for documentation, reviewing and responding mean that conclusion within a month (especially August/holiday time) would be difficult. The HL architecture work does not start until mid September 2008 and includes a demanding set of tasks related to documenting designs and defining detailed work packages. The HL task should be iterative with the card selection process (although card selection sub-tasks and intermediate milestones are not defined). In summary, RHUL would not be surprised if the end of Phase 1 slipped or that the delivered draft of the migration plan was not as comprehensive as anticipated.

However, TLS clearly states that it has adequate resource to complete all the projects in the Security Program (and thereby reach the MPM) and has carried out some risk review of project time-scales and activities to pre-empt potential planning and progress problems. It was not possible to review the Phase 2 and 3 activities in any detail as the tasks were not fully defined and presented in an overview form. Therefore it was not possible to determine whether potential slippage in Phase 1 will affect meeting the MPM date.

It should also be noted that whilst the delivered migration plan may be on time and "compliant" it can only be considered "compliant" in VenW decision-making once it has being independently checked/verified. This will add some further months of delay beyond the MPM and so the VenW decision point on the *migration plan* will likely be sometime between September to December 2009.

5. Review of the *Regional Fraud Management Plan* – for Rotterdam

The *regional fraud management plan* (dated 1st August 2008) is described by TLS as an output from the Fraud Monitoring and Management project within the Security Program. The plan was presented for review in order to satisfy the VenW request to justify the early (pre MPM) withdrawal of the Strippenkaart (PTW) in Rotterdam by demonstrating that the risks to cardholders and the transport business were well managed and controlled. Bearing in mind that RET/TLS would suffer if there were security and fraud problems in the Rotterdam system, the fact that they wish to make progress before the MPM is an indication of their belief and confidence to manage any issues that may arise.

The title of the supplied document is rather misleading as the content is not restricted to managing fraud, but also relates to security attacks/exploits where there is no direct attempt to gain a monetary advantage. The recent action of some researchers is included in the report as "Academic Abuse" and described as "academic community investigation of weaknesses in the OV-Chipkaart system". The meaning may have been changed in translation from Dutch to English, but the word "abuse" often suggests a dark, serious and criminal nature of an action and implying that a whole academic community is involved in this way is inaccurate and not conducive to amicable co-operation.
It could be better to re-title the types of "abuse" as types of "exploit". The academic exploit could then be renamed as a "proof-of-concept" exploit as this type of attack may be carried out by any curious and reasonably skilled individual who may have no association with academic institutions or their ideals.

The document is "high level" and does not include the detail that would be expected from a risk assessment on the types of exploits and the back office detection and correction actions. This may be in line with the expectation of VenW, and/or the need to safeguard security sensitive information and/or the fact that the detailed risk assessment had not completed by the 1st August 2008 (according to the *project plan*). The document does however describe the typical principles and processes that would be used for management of such a system.

The document attempts to classify the types of exploit based on the motivation/objective of the perpetrator. There are five types (described in tables and text).

- Proof-of-concept
- Denial-of-service
- Criminal scheme/business
- Individual fare evasion
- False claims

The card attacks are broken into three groups

- Card manipulation
- Card copying
- Card cloning/emulation

We consider that the description of card copying is just a sub-set of card cloning/emulation where there is a blank Mifare Classic with a fixed (and invalid) ID, so in our opinion only two major attack groups are described; manipulation and cloning. The different characteristics of clone types need to be well understood (and better described than in the report) as their effective detection by back office systems is relevant to not only management of the system, but also to the *migration plan* triggers.

There is a statement that "at this moment" card clones are likely to be implemented only on emulators. This is probably correct, however the plan has to safeguard the Rotterdam system for perhaps a year before the MPM is reached and the *migration plan* is approved; and then for at least as long as it takes to migrate the system (assuming an immediate trigger). It is quite feasible to expect counterfeit/clone card platforms to appear during this time window and so it is very important that the MPM date does not slip further.

There is an overview of back office monitoring. It mentions that indicators, exceptions and patterns are monitored, but as no detail is given, there is no way of verifying if these are appropriate or effective. It is claimed that card manipulation is detected as a content (unspecified) mis-match with the back office system and clones are detected by analysis (unspecified) of impossible travel patterns as well as card manipulation exceptions.

There is a little more detail given on the timing cycle of detection, analysis and control, which basically confirms the general cycle time mentioned in the TNO report. The split between automatic and human analysis is not clearly defined, although there is certainly some human analysis of the exception reports. The principle control is the blacklist which prevents a card of a particular ID from being used in the system.

The report describes an approach to blacklisting, depending on whether card manipulation or cloning is suspected. More care is given to the latter case as it is claimed that a real/innocent customer is more likely to be inconvenienced. Depending on the type of exploit and card/clone, blacklisting may be temporary or permanent. Permanent black-listing is subject to some capacity constraints although the report claims that the capacity is sufficient for permanent black-listing on the Rotterdam system and identifies some measures to optimise the use of the black-list.

As part of a targeted response to general exploits and suspected fraud, the PTO can put a card ID on a hotlist rather than a blacklist. This would alert local security enforcement when a particular card was used so that conventional policing action (perhaps backed up by CCTV) could be taken.

Additional visual inspections of cards are also mentioned. To be effective this would also need to be combined with reading of the card, otherwise when challenged an attacker could simply present a legitimate card instead of his attack card/emulator. The CE report also recommends some anti-counterfeit measures that could be consistently checked by inspection staff regardless of the various artworks used/planned for OV-Chipkaarts.

An enforcement process is also mentioned, but it is still work in progress. This is an important activity and TLS/PTOs (and their legal advisors) need to be absolutely clear on the crimes and potential punishments associated with the various types of exploit and the powers and responsibilities of local security enforcement when confronting suspected perpetrators. As the report states, communicating the potential penalties to travellers can have a deterrent effect. Whilst some travellers may risk a penalty fare, they may be less inclined to risk prosecution for a deliberate attempt to mis-use the system.

There is a discussion on handling fraud from a customer and customer-services viewpoint. This includes proposed communication with the customers about the handling of suspected fraud and provides assurances that the customer will not incur any financial damage. The report claims that there is already a fraud FAQ for use by PTO/OV-Chipkaart service desk personnel. Although this section clearly addresses fraud it also seems applicable to proof-of-concept and possibly denial-of-service exploits.

Suspicion of fraud can be reported by the cardholder, TLS and/or PTOs. Ultimately, blacklisting is controlled by TLS and TLS is also responsible for any follow-up activities with specially trained staff. In the case of the cardholder suspecting fraud (presumably because of unexpected ticket charges) there is a well defined sequence of steps that handle both anonymous and personalised OV-Chipkaarts. A critical step within this sequence (that is not described in detail) is the analysis leading to the decision of whether fraud has taken place. This is usually not trivial to determine in cloning scenarios and requires further explanation. TLS and PTO suspected fraud handling is also described quite precisely, although the events and measures that lead to the suspicion are not described.

A reporting mechanism is briefly described for communication of exploits and fraudulent activity. The PTOs will receive a monthly overview from TLS with further details available on request. It is mentioned that comparisons can be made with Strippenkaart statistics, although it is not always easy to get a true measure from old technologies as card technologies and gated stations may identify frauds/exploits that could have been undetectable with paper tickets. The PTOs will provide "Stadtsregio" and VenW reports on a quarterly basis or more often if required. These reports should be to a level of detail acceptable to the recipients.

6. Summary Review of the *Regional Fraud Management Plan*

The *regional fraud management plan* is a reasonable basis for managing fraud and other security exploits and attacks on the Rotterdam system. However, the document is not sufficiently detailed for a rigorous review and more precise information should be added to subsequent revisions before PTW, even if this means appendix material that must remain TLS confidential. The plan is most precise in the area of process sequences for cardholder and customer service use-cases for suspected fraud. A similar level of precision/detail could be added to the local enforcement measures so that the triggers and processes associated with visual inspections and hotlisting are unambiguous. There appears an assumption that card manipulation is an "own card" exploit, however there may be scenarios where this is not the case and this should be considered within the customer-service processes. The plan is weakest in its description of back office monitoring and exception generation and differentiating between the various clone types and exploits that may threaten the system. The back office monitoring is critical not only for combating fraud/exploits but also generating the triggers and statistics that can ultimately invoke the *migration plan*. Nothing is said about the number of incidents or suspected exploits that can be handled by the back office processes and systems, although this can probably only be determined by operational experience.

Practical fraud management often results in requirements for a range of SRMs and so it is recommended that all SRMs are detailed within *regional fraud management plans* and not within the *migration plan*.

Further information is provided in section 7, which provides conclusions and recommendations, by considering both the *regional fraud management plan* and *the project plan*.

7. Conclusions and Recommendations

The *project plan* and *regional fraud management plan* were presented for review as two separate documents although the reality is that they are inextricably linked by addressing some overlapping issues.

The measures in the *regional fraud management plan* would be expected to have arisen from the structured risk assessments in the *project plan* and be revised as further assessments were carried out and additional mitigating measures identified. The operational monitoring reports capable of being generated by the Rotterdam system could provide the inputs to the decision making framework for the *migration plan* and the operational statistics including fraud level, frequency and type of exploits could be the "trigger" for execution of the *migration plan*.

The decision to withdraw the paper tickets (PTW) provides an opportunity to gather a useful statistic: the comparative fraud of the Strippenkaart and OV-Chipkaart systems. The business information gathered by careful monitoring during the PTW period would be useful for the Rotterdam system, but also for other regions considering the future of their paper tickets.

The *project plan* does not give much emphasis to collecting reports and statistics from a live operational network and so the Rotterdam system could assist in that respect. This would help with currently unanswered questions concerning the number of potential exploits that will be flagged and the ability of the back office processes to cope. Furthermore it will be difficult to be confident in the *migration plan* if critical infrastructure elements and cards have not been tried on a fully operational system. The Rotterdam system could be used as a test-bed for tests and trials which could be of particular interest if cards with a legacy mode are used. In this case "new" cards could be issued and used on the system in advance of infrastructure upgrade.

The critical question is of course whether VenW should permit the Rotterdam system to discontinue the paper Strippenkaart prior to the MPM and if so whether this introduces unacceptable added risk to customers, PTOs and TLS.

The CE report made no definite recommendation aimed at legacy tickets on low fare regional systems prior to the MPM. For regional OV-Chipkaart infrastructure it is of course advisable to carry out a risk review and optimise back office detective and corrective controls as are included in the *project plan* and the *regional fraud management plan*. This is good practice in any case, but of increased importance due to the Mifare Classic problems.

If Rotterdam is permitted to discontinue paper tickets in advance of the MPM then the increased window of potential risk for Rotterdam is between the PTW and the *migration plan* approval date (MPM + review/approval time). This is likely to be in the region of 6-12 months. A longer time period would not be advised due to the potential development of clone cards and so the earliest PTW date should be January 2009; assuming that the MPM remains fixed at June 2009. It should be noted that paper tickets do not represent an ideal practical or fraud/counterfeit resistant solution to ticketing and indeed that is one of the reasons why they are being increasingly phased out in transport systems. What they do offer is familiar option for the customer and a guarantee not to spend more than the ticket face value. For the ticket inspection staff they offer a simple visual check of validity.

Despite the reported Mifare Classic problems, smart card ticketing with gated infrastructure offers an effective way to manage travel systems, avoiding fare dodging and other frauds that are possible with paper tickets. Customers who currently still use Strippenkaarts will need to adapt to the new system, but users of such systems normally find that the cards are convenient and cost effective. Additionally if customers can be assured/convinced that they will not suffer financial or personal data loss from any security/fraud problem (as is proposed in the TLS plans) and are offered best value fares, then the OV-Chipkaart should be accepted. These assurances need to be fully clarified and communicated to customers. TLS/RET should confirm that customers will not suffer financial loss because of PTW.

Losing some aspects of visual inspection could present a security weakness, however this may be overcome via a number of measures. Firstly an inspector needs to determine (to a reasonable extent) that the presented card is "genuine", without the need for inspection equipment. Because smart card artwork may be duplicated, the cards should incorporate at least one anti-counterfeiting measure. Laser engraving should be considered as the minimum initial measure with a planned upgrade to a more sophisticated solution such as a hologram. Secondly, inspectors should be equipped with portable card reading equipment and trained in the examination of card contents and how to react to and report anomalies.

One might suggest that the risk averse strategy is to keep the Strippenkaart until the MPM. Indeed in the opinion of RHUL this is the simplest and recommended strategy for networks that have not yet deployed OV-Chipkaart infrastructure. However for the Rotterdam network that already supports both smartcard and paper tickets, no one can be certain if this really is a "risk averse" strategy, as there are insufficient published statistics comparing fraud/exploits on Strippenkaart and OV-Chipkaart ticketing. Neither are there statistics on the volume and impact of "exploits" on OV-Chipkaarts and the capacity of back office systems to deal with them.

Another factor to consider is that pressing the *migration plan* "Go-button" will almost certainly require some statistical inputs based on network reports. If we wait until the MPM before gathering this information then this may introduce a further period of delay and uncertainty until we can be confident that the button should be pressed (or not). The Rotterdam system could therefore be a useful source of operational statistics as well as a live system to test new technologies needed in the *migration plan*.

The time window for the Rotterdam concession is the same period as for the completion and approval of the *migration plan* and so it would seem sensible to include it as part of the *project plan* in order to gain experience and information that may help reduce risks associated with the *migration plan*.

There is risk in any endeavour and it normally cannot be completely removed, so risk analysis and management is about identifying, understanding and measuring risks and taking reasonable mitigating and contingency measures to deal with them. From a fraud risk perspective there is currently insufficient tangible evidence to prevent TLS/RET from proceeding with their business strategy; for the early withdrawal of the Strippenkaart (PTW) in Rotterdam. In particular, TLS/RET appear to provide assurance that customers will not suffer financial or data loss and have given attention to the monitoring of fraud and other exploits and associated customer-service procedures. What could change this logic is if the time window between the Rotterdam PTW and the *migration plan* approval, becomes extended as this may allow or indeed encourage evolution of card based fraud[11].

To ensure that some added defensive measures are in place for the Rotterdam system and that there is significant benefit for the *project plan* (and eventually the *migration plan*) it is recommended that the Rotterdam Strippenkaart concession from VenW should be associated with the following obligations for TLS/RET.

Table 1 Obligations and Relevance for the *regional fraud management plan* and *project plan*

Obligation		***Regional Fraud Mgmt Plan***	***Project Plan***
1.	Provide clear assurance that customers will not suffer financial loss because of PTW	Yes	
2.	Provide clear guidance to customers on aspects of security, privacy and suspected fraud	Yes	
3.	Clearly identify the decision making parties in all plans and in the Decision Framework	Yes	Yes
4.	Improve the level of detail in the next revision of the *regional fraud management plan* and including SRM information	Yes	
5.	Reassess and if necessary revise the *project plan* timescales and project phasing		Yes
6.	Provide detail on the card selection sub-tasks within the *project plan*		Yes
7.	Ensure that there is an effective visual anti counterfeit measure on the card	Yes	
8.	Ensure that ticket inspectors have portable reader devices and are trained in their usage	Yes	
9.	Ensure that the enforcement situation is clearly understood and communicated	Yes	
10.	Identify and implement the attack type/frequency detection reports and statistical reports that will eventually feed into the Decision Framework	Yes	Yes
11.	Collect these reports and deliver to PTOs and VenW as proposed in the reporting section of the *regional fraud management plan*	Yes	
12.	Analyse the reports as input into the *migration plan* and migration triggers		Yes
13.	Make a quantitative comparison between OV-Chipkaart and paper ticket fraud at PTW	Yes	
14.	Measure the time/cost of handling various stages of an exploit-report and predict handling capacities and best response times	Yes	Yes
15.	Ensure there are adequate facilities to trial, test and evaluate critical elements of the new card technology and infrastructure prior to the MPM	Yes	Yes
16.	Provide clarification for any other issues highlighted in this report	Yes	Yes

[11] Specifically exploitation of Mifare Classic vulnerabilities

In accordance with VenW instructions for the RHUL assignment, TLS/RET were shown the preliminary findings of this review and invited to provide any initial response; particularly with respect to the proposed obligations listed above. Their draft response is included within Appendix A. Subject to final confirmation of the content of the response by TLS (after discussion with PTOs) it would appear that all the proposed obligations are accepted in principle and are being acted upon to some extent.

As a final part of the assignment, the practicalities of PTW were discussed with VenW. It appears that there are significant logistical, contractual and legal tasks that would need to be started before the actual PTW for Rotterdam. It is at this earlier start point that VenW would need to be finally convinced by direct assurances from TLS/RET that all information, measures and timing to support critical assumptions were in place. RHUL recommends that the direct assurances should include the following.

a) Reconfirmation or revision of the MPM date in the light of this review. (TLS has confirmed June 2009 within the review input documents (not yet seen by VenW), although RHUL has voiced some doubts and added *project plan* obligations in Table 1).
b) Confirmation that the TLS/RET understanding of all critical terms used in this review such as MPM, SRM, *project plan* and *migration plan* matches the definitions and clarifications given in this review.
c) Confirmation that the Rotterdam PTW would not occur more than 6 months before the MPM (to minimise the window of potential risk; as suggested by RHUL).
d) Confirmation that the obligations[12] in Table 1, relevant to the *regional fraud management plan*, would be completed prior to VenW beginning its PTW preparation work.

As the timing of activities is very challenging, it is suggested that these assurances could be provided first in a formal letter to VenW and then discussed in a sequence of regular meetings between VenW and TLS, rather than relying solely on reviews of major *project plan* milestones.

Please note that the opinions offered in this review are for the Rotterdam network alone and should not be used as a general guide for other regional networks.

This concludes the review by RHUL.

[12] Obligation 1 is recommended as the first priority.

Appendix A

Draft response to the RHUL review of the Project Plan and the Rotterdam Fraud Management Plan

3 September 2008

General remarks

This response concerns the RHUL report "Review of the *Project Plan* and *Regional Fraud Management Plan*" and taking into account the remarks made in a clarifying telephone conference of 1 September 2008. This response does not seek to comment the RHUL review, but outlines where and how the Project Plan and the Fraud Management Plan will be improved in response to the review. This draft response has been prepared by TLS and RET and is made available to RHUL as an 'addendum' to be included in the final assessment of the plans with regard to the criteria agreed with the Ministry of Transport. The final response will be co-ordinated with PTOs and confirmed as soon as possible.

For the *regional fraud management plan* the criterion is as follows:

> *Do the measures set out in the regional fraud management plan form a good basis to manage fraud risks and supporting customer service processes with the present Mifare Classic OV-Chipkaart in Rotterdam (vis-á-vis current fraud levels) in the period between transfer to an e-ticketing only situation and the Migration Planning Milestone (mid 2009)?*

For the *project plan* the criterion is:

> *Is it reasonable to expect a compliant migration plan by June 2009?*

The agreement with the Ministry of Transport foresees that, if the plans do not meet the criteria, TLS and RET will have the opportunity to assess the recommendations made by RHUL and indicate whether and how such recommendations will be accepted. Both will be made part of the RHUL review and final report.

As agreed with RHUL this response focuses on the first 15 points of page 21 of the draft report, which summarize the most important recommendations with respect to the envisaged withdrawal of paper tickets in Rotterdam. We will provide comments for each of these points.

1. Provide clear assurance that customers will not suffer financial loss because of PTW

This recommendation does not regard the documents as such. We confirmed that customers would not suffer financial loss due to potential security/fraud issues. We have informed RHUL of the agreement between the Ministry of Transport and the PTOs with regard to 'revenue neutrality', meaning that on average customers will pay the same for the kilometre-based *OV-Chipkaart* as they would for the zone-based *strippenkaart*.

2. *Provide clear guidance to customers on aspects of security, privacy and suspected fraud*

We will take up this recommendation on two levels:

- As part of the overall security program TLS will make available such information to the public on her website.
- A folder with information will be made available for customers at the point-of-sales and service locations of RET.

3. *Clearly identify the decision making parties in all plans and in the Decision Framework*

We will clarify the plans where necessary and follow this through in later deliverables as well (such as the Decision Framework).

4. *Improve the level of detail in the next revision of the regional fraud management plan and including SRM information*

In the overall security project we will report to PTOs in detail with regard to fraud and Short-term Remedial Measures in October 2008. Findings and decision will be included in our Fraud Management Plans (both regional and national), which will be updated every three months.

5. *Reassess and if necessary revise the project plan timescales and project phasing*

We acknowledge the fact that the timescales are ambitious, especially in the light of the need to involve various parties in the decisions that must be taken. After each phase the project plan will be updated, and detailed for the next phase. When necessary we will propose additional resources or changes to the contents of the plan. We note that the first migration plan will focus on the security requirements while keeping the functional specifications constant. For future instances of the migration plan we foresee that changing business requirements can be taken into account. This approach is described in our letter of 1 August where we submitted our documents for review.

6. *Provide detail on the card selection sub-tasks within the project plan*

We recognize the shortcomings of the phasing of this task and have made the adjustments set out below.

We have taken the following steps to come to a shortlist of three potential successors:

- TNO has provided us with a long-list of cards based on an open cryptography, taking into account the newest insights from the Mifare Classic hack.
- With internal and external experts we have set out knock-out criteria, evaluation criteria and a weighting of these criteria.
- We have scored the cards on the long-list and made a shortlist of three cards.
- This methodology has been reviewed by TNO and comments will be taken into account.

The next steps are the following:

- Taking into account current functional specifications as well as the 'new' assessment of security risks, a High Level design of the security architecture for each of these three potential successors is made by experts from Thales Transport and Thales security, and with substantial assistance of potential chip-supplier under supervision of TLS.
- Evaluation of the three solutions (card plus high level design) by internal and external experts.
- Recommendation on the solution to DOC (the directors of TLS and PTOs) by TLS, again reviewed by TNO.
- Review of deliverable by RHUL as agreed with the Ministry of Transport.

7. Ensure that there is an effective visual anti counterfeit measure on the card

As discussed in our telephone conference, the cards all have a laser engraved ID. We are currently assessing whether we can issue all our new cards with holographic foil as part of the project for the Short Term Remedial Measures. In certain fraud scenarios we may also replace cards already issued.

8. Ensure that ticket inspectors have portable reader devices and are trained in their usage

This has been done and will be continued on a regular basis.

9. Ensure that the enforcement situation is clearly understood and communicated

This will be done and continued on a regular basis, amongst others as part of the abovementioned folder with relevant information. RET is of the opinion that fraud with the OV-Chipkaart is similar to manipulation of existing paper based tickets.

10. Identify and implement the attack type/frequency detection reports and statistical reports that will eventually feed into the Decision Framework

This is part of the Fraud monitoring project. Substantial results are planned for October 2008, after which the results will feed into our updated (regional and national) fraud management plans.

11. Collect these reports and deliver to PTOs and VenW as proposed in the reporting section of the regional fraud management plan

This will be done as described in the Rotterdam fraud management plan.

12. Analyse the reports as input into the migration plan and migration triggers

This is indeed our intent and we will include it explicitly in the update of the project plan for the next phase (due in October).

13. Make a quantitative comparison between OV-Chipkaart and paper ticket fraud at PTW

This will be done as described in the Rotterdam fraud management plan.

14. Measure the time/cost of handling various stages of an exploit-report and predict handling capacities and best response times

Currently there is an overcapacity for analysis. But this may change as the system is rolled out across the Netherlands and the abilities of fraudsters increase. We will include a specific evaluation as part of the National Fraud Management Plan (January 2009).

15. Ensure there are adequate facilities to trial, test and evaluate critical elements of the new card technology and infrastructure prior to the MPM

We will include prototyping of critical elements in our planning for the third phase. We will use our extensive experience and facilities that we have built up with regard to acceptance tests, integration tests and certification tests in the regular *OV-Chipkaart* programme.

16. Remaining points.

We appreciate the review as a whole and will integrate the remaining points where they are applicable in the future deliverables of the programme.

* * *

We trust that this addendum to our plans meets your requirements. Should there be any misunderstanding in this respect, we are available for further clarification.