Migration Plan Review for the Dutch OV-Chipkaart

06.01.10

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 that a Migration Planning Milestone (MPM) be set 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 reviewed and approved *migration plan* in place, prior to lifting the general obligation to accept the paper-based Strippenkaart in local and regional Dutch public transport. TLS and the PTOs have since developed a *migration plan* for the transition to a new card technology. VenW asked RHUL to carry out an independent review of the *migration plan* and determine whether TLS and the PTOs have reached an acceptable state of "migration readiness" based upon a number of VenW requirements. The findings of the review are summarised in this report.

It is important to note that RHUL defines migration readiness as a "go button" such that if migration conditions are reached the new technology is simply rolled-out. This does not mean that there is no work to be done after the button is pressed; but that all technical, planning and operation process related risks will have been taken care of before the MPM. Migration readiness can be characterised in two parts:

- Technical readiness for card migration.
- Organisational readiness for card migration.

Both parts must be fit-for-purpose to support an efficient migration to counter the potential of rapidly escalating attack and fraud scenarios. Therefore RHUL was instructed to include both technical readiness and organisational readiness aspects within its review. The criteria for the review were derived from the VenW requirements that are described in the following section.

The VenW Requirements

In preparation for the RHUL review assignment, VenW stated some key requirements for the MPM review. To validate these requirements, the RHUL review is guided towards several important subjects (listed below) for which RHUL has identified the primary practical goals.

- The system risk assessment.
    - This should ensure that all relevant risks are captured, understood and mitigation measures[1] are identified in the migration solution.
- The high-level security design/architecture.
    - This should provide a complete and detailed description of the migration security solution, including algorithms, keys, modes, protocols, messages sequences plus implementation aspects.
    - This migration solution design should demonstrate compliance with best practices for smart card, cryptographic and information security.
    - This should justify that the migration solution is reasonably future-proof.
- The replacement card/technology selection.
    - This should justify the card technology choice with respect to other candidate devices and approaches.
    - This should justify that the card technology choice meets all design criteria and fits the High Level Security Architecture (HLSA)[2].
- Design, building and testing of the security upgrade of all components of the system.
    - This should ensure that all upgrade tasks are identified.
    - It should be verifiable that all technical and design risks and/or product choice risks associated with upgrades of all relevant components of the system have been resolved.
    - This should ensure that the migration solution is practical from an implementation and performance viewpoint.
- The activity plan[3].
    - This should provide a realistic migration project plan[4], covering all main and important activities in the complete system.
    - The activity plan should consider timescale risks and provide confidence that migration would complete within the target timescale (i.e. six months from start[5]).

[1] From the new migration technology and not from short term remedial measures (that are out of scope for the review).
[2] The HLSA is sometimes referred to as the High Level Design (HLD).
[3] The Activity Plan in some documents is referred to as the Migration Plan.
[4] With dates referenced to "T0" i.e. the time at which the decision is taken to upgrade.
[5] This has been clarified to TLS as a target (rather than absolute limit) based on the need to counter a potentially rapidly escalating threat; and on our knowledge that a large PTO (outside of the Netherlands) is able to migrate within this period.

  - All main and important upgrade activities should be defined to sufficient detail that the actors (and RHUL) are convinced that there is sufficient information to understand, plan and resource the activities, and to be reasonably confident of successful execution within the overall activity plan.
  - It should be verifiable that TLS, all PTOs and Vendors are committed to and engaged within the activity plan and understand their respective responsibilities.

- The decision framework.
  - This should include description of the inputs to the framework including fraud reports from TLS, PTOs and any other parties.
  - It should define all models and metrics used to create triggers and alerts.
  - It should define the migration decision making process and associated actors.
  - It should be verifiable that migration would be triggered when stated conditions are met.

By proper review of these subjects the VenW expectation of the MPM (and the state of migration readiness) can be evaluated against the following statement[6] of scope and objective:

> *With this description of the subjects of the review, the technical and organisational migration readiness is well defined. At the start of the review all preparatory steps will have been professionally taken to minimise technical, security, project planning, process and decision making risks associated with the Migration Plan. For the avoidance of doubt the trigger for the start of the Migration Plan will be unambiguously defined taking into account both reasons of business economics and true client acceptance, and the plan as it affects the regional and national OVCK system will execute within a pre-defined maximum time period. Prior to the completion of the review all aspects of the Migration Plan shall be formally agreed upon by all actors, covering the complete current and future national OVCK system, as specified in the activity plan and the decision framework. These actors are the PTO's and TLS. Finally, the discipline of keeping the Migration Plan and associated documentation coherent and up to date is well organised and documented, and is formally agreed upon by all actors.*

NOTE: The VenW requirements and their practical interpretations were communicated to TLS prior to the start of the review and then incorporated within the review methodology and plans. However, during the review it became clear that the criteria affecting the Decision Framework would need to be revised, as described in the next section.

[6] Quote from VenW, included within MPM review planning documentation.

Revisions to the Decision Framework Requirements

It is important to note that the original VenW review criteria relating to the decision framework assumed a certain migration planning strategy i.e. the process and models that would ensure that a predefined and measureable level of attack activity would definitely trigger the start of migration which would complete within a fixed period[7]. However the planning strategy was revised during the RHUL review process so that the critical decision became whether to accelerate migration rather than when to start migration. This matter was raised with VenW and as a result the following formal revisions were made to the review criteria.

1) *The Decision Framework for the Start of Migration (DF) review, based on the original criteria, is no longer required in the report as TLS and the PTOs have taken the decision to start migration.*

2) *The Decision Framework for the Acceleration of Migration (DFA) document should be reviewed against the original DF criteria; except that the DFA does not need to be deterministic, but rather suitable for monitoring and control via an audit function.*

3) *To ensure that the DFA audit function is well defined, RHUL are asked to identify and propose any recommendations and improvements to the DFA document to ensure that it describes in adequate detail an effective decision making process that can be monitored and controlled via an auditor.*

4) *The Final plan (based on the revised strategy) will be the main subject of the review and only relevant parts of the Preliminary plan review (based on original strategy) should be included within the report.*

These criteria superseded the corresponding original requirements with respect to the RHUL review.

[7] Appropriate to counter a rapidly escalating threat/exploit.

The Adopted Methodology

Before describing the adopted methodology it is important to define the practical scope of the review to complement the high level objectives relating to the VenW requirements. The scope that was agreed following several discussions with TLS and VenW ensures that a migration security solution will be provided that satisfies the general requirement of *"overcoming the weaknesses of the Mifare Classic"*. RHUL is of the strong opinion that the migration security solution should be fit-for-purpose and in accordance with recognised best practices for smart cards, cryptography and information security in general.

Scope

RHUL and VenW recognise the TLS view that the majority of the system infrastructure was not directly affected by the published attacks. Therefore the scope and extent of the technical part of the review were agreed as follows:

- The security of the new card and reader-based infrastructure[8] as well as associated algorithms, key-sizes, protocols and management, must be "fit-for-purpose" and in accordance with best practices for cryptographic systems.
- The existing security levels of all other system infrastructure components must not be degraded by the introduction of the new card technology.

The review requirements clearly show that a technical design is only a part of an effective migration plan and so operational planning and decision making aspects (to reach technical and operational "readiness") are essential and included within the scope of the review.

Practical Steps

The practical steps in the methodology and review process were originally defined as follows:

- The input documentation set (see Appendix A) would undergo an initial review and the RHUL expert team would produce clarification questions for TLS and VenW[9], to be discussed and answered during meetings with TLS/VenW (in the Netherlands).
- Technical review.
  - The four detailed document reviews would run in parallel.
    - Risk Assessments.
    - Security Architecture.
    - Chip Card Selection.
    - Infrastructure Upgrades.
  - Performance demonstrations of the new technology.
- Operational and technical readiness.
  - Interviews with TLS/PTOs/Vendors.
  - The final three detailed document reviews would run in parallel.
    - Vendor Plans.
    - Activity Plan.
    - Decision Framework.

[8] For example, station entry/exit gates, ticket office machines, bus entry/exit validators etc.

[9] Note that at no time during the review process did VenW have access to the input documents. The VenW clarifications were related to review criteria and processes.

- An internal report would be drafted, reviewed and revised by the RHUL expert team.
- TLS would check the draft for inaccuracies and potential confidential information leakage.
- The report could then be revised, although there would be no obligation to do so and any changes would be at the sole discretion of the RHUL expert team.
- There would be a meeting in the Netherlands between the project leader and VenW and/or its representatives to clarify the progress and processes for translation and document release.
- Finally the document (in English) would be delivered to VenW.

Note that in following these steps (and with VenW permission) RHUL stated it would be happy to share intermediate findings, feedback and/or working notes with TLS when this would allow clarification and improvements to the quality of the input documents submitted for review. As a practical result of this feedback and TLS's own on-going work to improve responsiveness of the migration plans, there were in fact two sets of *Operation and Technical Readiness* documents presented for review, which will be referred to as *Preliminary* and *Final* respectively. RHUL reviewed both sets of documents and so the review findings from the *Preliminary* set are mentioned in this report, although RHUL recommendations are primarily based on the *Final* version. Most of the practical steps in the review should be self-explanatory; however some additional clarification is presented below.

- The review was dependent on the definition of an agreed input-document set (Appendix A).
    - The rationale was to ensure that RHUL received all relevant documents (in English) in good time for the review, by giving TLS adequate warning of delivery dates.
- The technical input document reviews would be supplemented by practical demonstration of the new working card and reader, allowing performance comparison with the existing Mifare Classic product.
    - The rationale was that there may be potential performance issues with the technical approach, and typical transactions with the new card should not be significantly slower than with the Mifare Classic; otherwise the approach may not be viable.
    - The tests and demonstrations were required to be as realistic as possible and convince the reviewer that the technical solutions could be rapidly deployed (and without further technical risk) on a live PTO network.
    - For the purpose of review, RHUL would compile a set of technical notes from observing the demonstrations and from technical discussions with the TLS experts responsible for the demonstration system. These notes should be of a standard that provides an "engineer" with the detailed factual information of the demonstrations and how they are representative of a live PTO network. This would include information on the protocol, data and APDU message sequences of relevant transactions[10] for both the new card and the Mifare Classic reference implementation. The document would also briefly describe the demonstration card and reader platform as well as the test equipment and test measurements.
- Interviews with representatives of TLS, PTOs, decision makers and significant vendors.
    - The rationale was to connect the reviewed documents with the real-life situation, ensuring that all parties have common understanding of responsibilities, commitments, plans, technical risks and activities.

[10] E.g. ticket validation, ticket purchase using the purse and purse top-up.

Review of the Migration Plan

From the presented input documentation and information provided during meetings, the RHUL expert team is convinced that TLS and its PTOs have committed significant time and resources to prepare for the migration planning milestone (MPM). Satisfying the MPM expectation requires attainment of a state of readiness for migration that is reliant on technical design aspects as well as technical and operational readiness, as evident from the *migration plan*.

Technical Review Stage

In terms of the technical aspects of the review, TLS provided four primary input documents and revised/improved some of them when requested to do so. TLS also provided secondary documents to help understanding of the primary documents and facilitated demonstrations and meetings requested by RHUL.

Risk Assessment Document: The risk assessment document was an extract from an existing TLS document and provided the information that was within the scope of the RHUL review. The supplied information addressed in competent technical detail the range of exploits that are possible against a Mifare Classic based OV-Chipkaart. The various attack scenarios were described and the likelihood of such attacks considered with respect to attacker skills, resources and motivation. A published methodology was used to try and quantify the risk although all such methods are based on subjective input. The subjective input provided by TLS classified many attacks as borderline medium risk (just below high risk) based on assumptions about the expertise and effort needed by attackers, whereas RHUL experts consider that the current level of activity and collaboration within the attacker community as well as developments within the related research communities means that copy-cat attacks could be very simple. The RHUL classification, which should be considered as no more than another subjective view, would characterise the majority of the attacks as high-risk. A residual risk matrix was created by TLS at the request of RHUL, showing that after technology migration all the medium/high risks were resolved. Therefore the proposed higher risk classification from RHUL should only remain a potential problem in the period until migration is finally completed.

The risk assessment document considered the impact on the system of a successful attack. However, the impact metric was expressed as a simple sum of money and did not explicitly relate to a time period or frequency of exploits, nor did it consider non-financial aspects such as reputational effects or effects on customers and their behaviour. Measuring the financial impact over a lengthy period and then reacting may be workable for a relatively slow and predictable growth in an attack, but it may not be adequate for a rapidly escalating problem. Such a problem might occur if sophisticated clones suddenly became available in large numbers, hence the need for a sensitive and/or early trigger and then the capability to carry out a swift migration.

A potential new risk that was not captured and dealt with in this document (nor in any supporting document) arises from the technical strategy (described under HLD) of issuing dual-mode cards and then sometime in the future invoking a process to copy information between legacy (Mifare Classic) and new technology modes. TLS was notified of this risk and stated that it would be investigated.

High Level Design: The High Level Design document described the migration solution in detailed technical terms, providing (along with input from question and answer sessions) all necessary information for reviewing the technical solution. The HLD contents primarily relate to the card and reader interaction and necessary supporting functions, such as card personalisation and key generation, distribution and management. Because of the problems with the Mifare Classic, TLS has stated that it does not wish to be restricted to vendor proprietary security solutions and has taken a decisive step to define and control its own protocol based on a well-known public algorithm. The algorithm is 2-key triple DES with a key size of 112 bits. This algorithm when properly implemented satisfies ECRYPT/NIST security recommendation, although AES would have been a more modern choice. Block cipher encryption is used to avoid some potential pit-falls with stream ciphers and a robust random number generation algorithm is used. An additional layer of security is provided by authenticating data using Message Authentication Codes (MAC).

Chip Card Selection: The TLS intention is to issue new cards to customers in advance of the entire national infrastructure having been upgraded. Therefore the cards also need to support the legacy (Mifare Classic) protocol mode. This decision restricts the initial choice of platform to either the NXP SmartMX or the NXP Mifare Plus. The latter product is still quite new and unproven, and it is a vendor proprietary product (albeit claiming to be based on an open algorithm); it therefore conflicts with the TLS decision to take full control of the solution. TLS also considered the possibility of using other platform types in future, the potential support for other algorithms/protocols and the possibility of internationally compatible (roaming support) ticket solutions. Based on these considerations, TLS decided to implement the new card solution as a Java applet on a SmartMX platform, with the potential to use alternative Java smart cards once the entire infrastructure is upgraded. The SmartMX is a reasonably mature product that is far more sophisticated than the Mifare Classic and has been successfully evaluated against Common Criteria security standards (to EAL4+) for use in other industry applications.

A concern for any new smart card ticket technology and especially one based on Java is the operational performance. Transport ticketing applications are very sensitive to transaction speed as this effects customer interaction at reader devices and the overall speed of customer throughput at access gates. Java applets run on a virtual machine for flexibility and security, but are typically slower than native software applications and custom hardware. For this reason, TLS was requested to provide practical performance demonstrations of representative transactions, compared with a Mifare Classic reference. TLS complied with this request and made available all details of the demonstrated transactions as well as message traces and permitted RHUL to independently capture its own traces for subsequent review. Various measurements were taken and as a rough rule of thumb, computation/transaction time with the new card technology and protocol solution increases by 50%-80% compared to the Mifare Classic for an equivalent and typical gate transaction. This is considered by TLS (and not disputed by RHUL) to be just within the target of practicality and there is scope for further improvement e.g. from a new version of the SmartMX platform and Secure Application Module (SAM) optimisation. It should be noted that the current level of performance has only been possible by using function calls specific to the platform API, without which the transaction time would have been much longer. The implication is that the applet might need to be modified if implemented on other chip platforms in future. Furthermore, the transaction time then becomes platform dependent and the choice of suitable platforms may need to be restricted to those offering similar function calls to achieve acceptable performance.

The demonstration was regarded by RHUL as a functional proof of concept. It involved a new card/ticket plus a similar card configured as a SAM. A real gate was not used, but instead a laptop PC mimicked the missing functionality to the extent necessary to stress the performance aspects. Further work would be required on functional and security testing before the card and SAM would be fit-for-purpose for deployment within the Dutch networks. It is not clear whether a single type of SAM will be used throughout the Dutch network (RHUL preferred option) or if there will eventually be multiple variants and legacy devices from various vendors. No major hurdle would be anticipated for finalising the card itself and a common SAM should also be feasible; however the practicality of integrating multiple SAMs into existing infrastructure plus supporting management functionality and legacy modes is unclear and RHUL regards this as a remaining area of technical risk.

Infrastructure Upgrades: The major and necessary upgrades to the infrastructure were identified in the TLS documentation, along with the involved parties e.g. TLS, PTOs and Vendors. Each upgrade was considered with respect to its potential impact on the overall migration. The documented rating mechanism was initially unclear, however discussions with TLS clarified that an upgrade was considered to have a potential impact if it affected the timescale or cost of the entire migration, or if there was significant uncertainty in the assessment of the effect on timescale and cost. An upgrade with significant impact was justification for providing a corresponding vendor or activity plan for review. The input document showed various parties (PTOs/Vendors/TLS) associated with upgrade items, yet TLS asked relatively few parties to submit plans. TLS provided some clarifying information describing the relative size and importance of the various parties and how TLS had adopted an 80:20 rule i.e. the plans provided should cover 80% of the migration system. RHUL does not consider this approach unrealistic, although the impact rating would have been more informative and verifiable if split into categories such as relating to technical, resourcing and timescale risks. Using costs (which were not disclosed to RHUL as they are out of scope for review) as an impact category means that RHUL cannot verify any upgrade that is or is not flagged as significant by virtue of this category. Furthermore, as only a functional prototype of the new protocol has been demonstrated (as opposed to a realistic mock-up on real equipment and systems) RHUL considers that some of the reported impacts are partly due to technical implementation risks.

Aside from using independent judgement to check that the most notable upgrades identified in the HLD appear in the infrastructure upgrades document and checking that all flagged upgrades are accompanied by vendor and/or activity plans, there is little additional verification that RHUL can carry out on the input infrastructure upgrade document. Therefore greater emphasis was placed on the treatment of various impact categories within the operational readiness review.

Operational Readiness (Planning) Review

In terms of the operational readiness aspects of the review, TLS initially provided three primary input documents and clarifying statements. During the initial review activities and informal working feedback to VenW and TLS, it became clear that there were some major bottlenecks in the plans as well as duplication of effort, which required a significant change to planning strategy. Following subsequent discussions between VenW and TLS, a significantly revised set of documents was supplied by TLS and then reviewed by RHUL. In this section we will refer to the original and subsequent reviews, as *Preliminary* and *Final* respectively.

Preliminary Review

The Preliminary document set was based around a phased approach, with the first phase being triggered by a decision to migrate based on models and processes described in a decision framework. The TLS migration/activity plan is based around four phases:

- Phase 1: Migration preparation
    - Phase 1 is aimed at first synchronising the PTO/Vendor approach and getting to a stage where dual mode cards may be issued. This requires the card applet to be completed as well as the back office card issuing systems. There is apparently a minor change needed for the L1 (reader) devices to accept the emulation of Mifare Classic on the new cards. From the end of Phase 1 onwards the new dual mode cards would be issued to new customers.
- Phase 2: Development and Issuance
    - Phase 2 is aimed at upgrading the infrastructure so that the new card solution may be used.
- Phase 3: Conversion
    - During Phase 3 dual mode cards will be converted to the new solution, although legacy (Mifare Classic) cards will still be supported.
- Phase 4: Migrated
    - At the start of Phase 4 (i.e. end of Phase 3), only the new solution will be used.

For review purposes we considered reaching the end of Phase 3 as the critical milestone as before this point it is not possible to use the new solution anywhere in the Dutch transport system. A brief summary of comments on the *Preliminary* plans are listed below:

- The migration has no definite start or end.
- If a rapidly escalating threat was detected, the subsequent migration would take at least four years, which is incompatible with the criteria of providing a *"swift response to a rapidly escalating threat"*.
- There is significant and sequential duplication of critical Vendor tasks.
- There is a significant speed difference between Vendor plans.

The findings from the preliminary review were discussed with TLS and VenW and this resulted in a revised planning strategy and some changes to the formal review criteria. The revised document set (*Final* set) was reviewed against the criteria as described in the following section.

Final Review

The preliminary operational readiness feedback contributed to a significant and positive change to the migration planning strategy. The main points may be summarised as:

- The migration will "start" as soon as the TLS plans are accepted by VenW.
- The initial work will establish migration readiness as quickly as possible, by centralising critical tasks and avoiding duplication of effort identified in the preliminary review.
- The overall migration will be achieved within a pre-defined maximum time period.
- The overall migration will be "slow" (natural replacement of assets) unless there are significant measured frauds/attacks.
- In case of significant exploits the migration will be accelerated to complete within X months[11] of the acceleration decision.
- The Decision Framework is now focused on the decision framework to accelerate migration (DFA) rather than the decision to start migration.

Other changes and additional activities included direct discussions between VenW and TLS on possible processes for the monitoring of migration acceleration decisions. Furthermore, TLS facilitated interviews for RHUL with a number of PTOs and Vendors for verification of the new strategy and plans.

Phase 1: The *Final* Plans (which kept to the four phase approach) were presented, including a Phase 1 in which TLS would take the lead in managing technical activities involving vendors, to achieve the following:

- Bring the new card solution to product readiness (ready for deployment).
- Develop a new/common SAM approach for use by all Vendors and PTOs.
- Ensure minor changes are made to reader devices to accept Mifare Classic Emulation on new cards.
- Enable PTOs to issue the new cards, initially in legacy (Mifare Classic) mode.

Note that Phase 1 requires TLS to have direct contractual relationships with some vendors (normally this is handled by PTOs).

The plan for Phase 1 shows a completion of the critical activities within nine months from the start date (T0). Because of TLS leadership in this phase, confidence in the plan's execution is largely dependent on TLS and the vendors. Interviews with the vendors were reasonably positive. The detailed nature of their tasks is dependent on release of specifications in March 2010, however there was confidence that the scope of work was within the available skills and resources. The plans also require a degree of co-operation and collaboration between competing vendors. The vendor interviews suggested that this would happen and interviews with PTOs confirmed that they would also use contractual pressure to ensure that the necessary vendor collaboration would occur.

Completion of Phase 1 is effectively equivalent to the migration planning milestone suggested by RHUL and required by VenW. For example, this means that assuming a start date of 1st February 2010 the system will have reached the milestone by 1st November 2010. However, this alone does not guarantee migration readiness as there is a need to demonstrate sufficient speed of migration, should a rapidly escalating attack/exploit occur, such as could be triggered by the widespread

[11] The exact period will not be disclosed due to security/confidentiality restrictions.

availability and use of cloned cards. Completing migration requires execution of Phases 2 and 3. There were two sets of *Final* plans for these phases; the first showing rapid migration to respond to a rapidly escalating attack and the second showing a slower migration based on phased replacement of card and system assets.

Rapid Migration Phase 2/3: The earliest that this plan could execute would be at the end of Phase 1, assuming that the decision to rapidly migrate was made during Phase 1. For this to be considered adequate it should be swift enough to counter a rapidly escalating exploit. The growth rate of such an exploit cannot be precisely estimated although RHUL has considered a number of escalation models, and the speed of response from the rapid migration plan is within the acceptable range of these models. The exact speed of migration is security sensitive and TLS-Confidential, however having considered the rapid migration plan, RHUL can suggest no further optimisation and considers it the fastest achievable in practice. On the basis of the *Final* plans and associated verification interviews, the completion of Phase 1 should be regarded as "migration readiness", providing an effective decision making process is in place.

Slow/Natural Migration Phase 2/3: The speed of migration has a very significant impact on cost. Although detailed cost information was not part of the RHUL review, it is obvious that assets such as card and SAM infrastructure have a normal lifetime (e.g. about five years) and early replacement will erode asset value. Therefore TLS/PTOs would like to migrate in a slower (compared to the "rapid" plans) more natural way. This is a reasonable approach providing there is readiness to switch to rapid migration should a major problem occur. While the slow migration is in progress all newly issued cards will be dual-mode operating in legacy mode, and SAMs due for replacement will be substituted with new versions, which should make it progressively easier to "accelerate" should the need occur. The duration of the overall "slow" plan is long and it would take in excess of an additional five years from the end of Phase1 to complete the full migration.

An important question is whether it is possible to switch from slow to rapid migration, when vendors and PTOs may not have advance information for resource reservation and planning. The answers from interviews with PTOs and vendors were consistent, suggesting that normal business activity required significant peaks in resource requirements, often at short-notice and so migration was no different in this respect.

Planning in General: It does appear that the important activities have been considered in the *Final* plans and that the various parties have a reasonably common view and confidence that the plans are realistic. The interviews have provided a reasonable level of assurance that the various parties understand their roles and responsibilities and are committed to the migration planning process.

Decision Framework for Acceleration of Migration (DFA): The revised migration planning strategy inherently satisfies two of the original stated VenW requirements.

- *The start of the Migration Plan will be unambiguously defined.*
- *The plan as it affects the regional and national OVCK system will execute within a pre-defined maximum time period.*

However, acceleration of the migration is now the critical "decision" and the relevant review requirements applied to the acceleration decision, and the RHUL comments are summarised below.

- *This should include description of the inputs to the framework including fraud reports from TLS, PTOs and any other parties.*
    - The inputs are described in high-level terms.
    - Further inputs are advisable to ensure that a broader range of potential issues are considered within the DFA.
- *It should define all models and metrics used to create triggers and alerts.*
    - There are no models.
    - Models should be added to help predict potential problem escalation.
    - There is only one trigger metric (and this is a process rather than direct "acceleration" trigger).
        - The metric is computed as a percentage of transactions over the entire national network, however RHUL suggests that the metric should be computed for each network and/or PTO so that local issues are visible to the decision making process rather than being averaged out on a national scale.
        - Further trigger metrics are advisable to better include customer acceptance, IT systems loading and cost indications.
- *It should define the migration decision making process and associated actors.*
    - Defined at high level.

The view of RHUL is that the description of the DFA is not yet sufficiently detailed and clear to be easily and independently monitored, and the lack of models and triggers means that a significant level of expertise is required to interpret and understand developments (as opposed to a simple/conventional audit function). Therefore, RHUL has identified and proposed improvements to the DFA (listed in the Summary and Recommendations section) and VenW is strongly advised to require TLS to adopt these recommendations as post-review obligations.

Summary and Recommendations

On the basis of the technical readiness review of the first four primary input documents, it appears that the new card technology solution supports an architecture that is designed to be flexible, offers a reasonable degree of future-proofing and minimises reliance on vendor specific proprietary implementations. The protocol makes use of a public algorithm with a key-size in accordance with international recommendations. Further positive aspects include the use of block cipher encryption instead of a stream cipher for confidentiality and an additional layer of security from data authentication. The performance of the solution (at least from the card end) appears to be adequate for the intended application. Based on its brief review, RHUL could find no obvious major faults in the design approach (for the protocol and card solution), although it is of course well known from open reviews that expanding the set of reviewers increases the security assurance. TLS is therefore advised to seek further assurance on the security of its protocol design and final implementation either using an "open" approach or via expert/commercial labs. The quality of the security implementation is still unknown (apart from performance indicators) and TLS has been advised that the application and its implementation on the SmartMX card platform should be evaluated by a commercial test-lab[12], with instructions to evaluate and test against all known attacks e.g. logical, physical, side-channel and fault attacks. It was determined that the major risks in the infrastructure upgrade had been identified and for each one, a vendor plan was produced as part of the overall activity plan. Although technical readiness has not yet been reached, it is believed to be achievable if the planned activities are carried out.

To determine operational readiness, TLS initially provided three more primary documents (*Preliminary* set) for review and made their own key personnel available for meetings and interviews. Following feedback during the review process TLS provided revised documentation (*Final* set) and facilitated verification interviews with some vendors and PTOs. In general the plans were reviewed bearing in mind the need for a PTO to be able to counter a rapidly escalating threat such as from the widespread availability of sophisticated clone tickets or a major surge in the usage of current attack methods. Phase 1 of the plans described a number of preparation activities and Phase 2 addressed the infrastructure upgrade. However the end of Phase 3 was considered as the critical performance milestone, being the earliest time when the new card security solution can be used on any PTO network in the Netherlands.

The *Preliminary* activity and vendor plans did not meet the review criteria. Simply stated it would have taken more than four years from the time migration is triggered (due to a major/immediate problem) to complete the switch to the new technology. In RHUL's opinion this was completely inadequate to counter a rapidly escalating threat. The *Final* plans were, in RHUL's opinion, a significant improvement, and were based on the principle that the migration starts immediately in order to complete crucial technical preparation as soon as possible and avoid duplication of effort. Migration would be "slow" unless a major threat was detected, in which case the migration speed would be accelerated sufficiently to match the pace of a rapidly escalating threat model. If the plans were started 1st February 2010 a "qualified" state of migration readiness would have been reached by 1st November 2010.

[12] From interviews there is evidence that TLS is already working with expert/commercial labs on the security assurance.

It is a qualified state because it relies on an effective decision framework (DFA) to trigger the accelerated plan. In accordance with the revised review requirements[13] from VenW, RHUL identified a number of recommendations for improvement of the DFA, including metrics that would allow for the practical monitoring and control of the acceleration decision via an audit function. The recommendations are summarised as follows:

- The number of trigger metrics is increased to also include customer acceptance, IT systems loading and cost issues.
- Models are defined for predicting the potential escalation trends for trigger metrics.
- Trigger metrics are computed for each network and/or PTO rather than as national averages.
- A full set of initial trigger thresholds is defined.
- A process for the potential adaption of trigger thresholds is defined.
- A process for keeping the migration plans and associated documentation coherent and up-to-date is included within the DFA document.

On the conditions that the *Final* plans are adopted and that TLS will accept and adopt the RHUL recommendations for the DFA within two months from the start of the *Final* plans, the RHUL conclusion is that TLS and its PTOs should be able to reach a state of migration readiness by 1st November 2010, if work commences on 1st February 2010.

Appendix B provides review comments against the various VenW criteria.

This concludes the review from RHUL.

[13] The revisions were necessary as migration "acceleration" was not considered in the original review criteria.

Appendix A
Input Document Set

The document set consisted of primary documents and secondary (support) documents. Each of the seven review sub-tasks were based on the review of a single primary document. Secondary documents were only used to supplement the data and understanding of the primary documents and were not reviewed themselves. TLS was encouraged to provide all primary documents by the start of the project to benefit from the initial document clarification task. In any case a primary document could not arrive later than the scheduled start of the corresponding review task. During the review process some revised plans and decision framework documents were provided. The original set (*Preliminary*) and the subsequent set (*Final*) were both reviewed, with the main emphasis placed on the *Final* set.

Note that only documents supplied in English were considered as "delivered" for review. The initial agreed document set is defined below; however during the preparation for, and execution of the review, further secondary documents were allowed to be added if mutually agreed by TLS and RHUL. The status of the documents was required to be definitive and agreed upon by TLS, the PTOs and (where necessary) the Vendors.

Technical Readiness Primary Document Set

- *MPM1: The Security Risk Assessment (SRA)->task 8*
- *MPM2: The High Level Design (HLD)*[14] *->task 9*
- *MPM3: The Chip Selection (CS) ->task 10*
- *MPM4: The Infrastructure Upgrades (IU) ->task 11*

Operational Readiness Primary Document Set

- *MPM5: Vendor Plans (VP) ->task 13*
- *MPM6: Activity Plan (AP)*[15] *->task 14*
- *MPM7: Decision Framework (DF)*[16] *->task 15*

Supporting Documents

- Requirements specification
- The Protection Profile (PP)
- The Demonstration Notes (DN)[17]
- Card/Reader demo/trials report/results
- Regional Fraud Management Plans (RFMPs) from previous reviews
- Product datasheets
- Original CE review

[14] This document is required to include full and detailed description, of the new security solution including but not restricted to the algorithm, keys, modes, protocols and implementation security features.

[15] The Activity Plan should also include TLS's own attempts to identify and mitigate risks associated with execution of the plan to achieve migration.

[16] To include (a) the input flows from fraud reporting, (b) trigger calculations/ models and (c) the migration decision making process.

[17] This was not a supplied document, but a set of notes compiled by RHUL during demonstrations.

Appendix B

The table below provides a summary review of the *Final* plans against the VenW criteria. Note that the original Decision Framework (DF) review criteria were intended for a "start" migration decision rather than "acceleration", and so during the review it was necessary to formally revise some review criteria relevant to the Decision Framework for Acceleration (DFA).

Table 1: Review comments applied to VenW criteria

Criteria	**Comment**	**Status**
System risk assessment.		
This should ensure that all relevant risks are captured, understood and mitigation measures[18] are identified in the migration solution.	Technical risks[19] were identified. A potential risk from conversion was not covered in the input documents.	Pass (assuming risk will be addressed by TLS).
The high-level security design/architecture.		
This should provide a complete and detailed description of the migration security solution, including algorithms, keys, modes, protocols, messages sequences plus implementation aspects.	This was a detailed document providing the information necessary for review.	Pass.
This migration solution design should demonstrate compliance with best practices for smart card, cryptographic and information security.	A public algorithm was selected and key-sizes were in compliance with best practice recommendations. The protocol was based on standard open algorithms. We note that TLS must also take added steps to ensure the design and implementation security.	Pass.
This should justify that the migration solution is reasonably future-proof.	TLS has chosen an approach that is ultimately suitable for implementation on a variety of secured microprocessor platforms found in smart cards, but also possibly in mobile phones and other devices. This is a flexible approach that is probably the most flexible and future-proof of the options that were available to TLS.	Pass.

[18] From the new migration technology and not from short term remedial measures that are out of scope for the review.
[19] Other risk types were considered when reviewing the operational readiness documents

The replacement card/technology selection.		
This should justify the card technology choice with respect to other candidate devices and approaches.	The card choice was justified, although there were few candidates given the strategy to offer dual-mode cards, with 4K Mifare Classic emulation.	Pass.
This should justify that the card technology choice meets all design criteria and the High Level Security Architecture (HLSA/HLD).	The card choice did match the requirements in the HSLA/HLD.	Pass.
Design, building and testing of the security upgrade of all components of the system.		
This should ensure that all upgrade tasks are identified.	It seems that the major upgrade items were identified.	Pass.
It should be verifiable that all technical and design risks and/or product choice risks associated with upgrades of all relevant components of the system have been resolved.	This could not be fully verified although a functional demonstrator of a card and SAM interaction was shown working. This should be effectively addressed in the Phase 1 activities.	Anticipated by 1st Nov 2010.
This should prove that the migration solution is practical from an implementation and performance viewpoint.	The performance of the card solution appears practical (which was in doubt beforehand). The practicality of all the systems upgrades is not known. This should be effectively addressed in the Phase 1 activities.	Anticipated by 1st Nov 2010.
The activity plan[20].		
This should provide a realistic Migration project plan, covering all main and important activities in the complete system, with dates referenced to "T0" i.e. the time at which the decision is taken to upgrade.	The accelerated (fast) plan is realistic in terms of speed and verified by interviewees. The slow migration plan is likely to be realistic in terms of minimising asset replacement costs.	Pass.
The activity plan should consider timescale risks and provide confidence that migration would complete within the target timescale.	The acceleration option allows for reaction to major risks and rapid mode is within reasonable bounds of escalation models	Pass.

[20] The Activity Plan in some documents is referred to as the Migration Plan.

All main and important upgrade activities should be defined to sufficient detail that the actors (and RHUL) are convinced that there is sufficient information to understand, plan and resource the activities, and to be reasonably confident of successful execution within the overall activity plan.	A reasonable (rather than comprehensive) level of detail was provided at this stage and interviewees seem well informed.	Pass.
It should be verifiable that TLS, all PTOs and Vendors are committed to and engaged within the activity plan and understand their respective responsibilities.	Interviews took place and all interviewees seemed committed and informed.	Pass.
The decision framework (for acceleration)		
This should include description of the inputs to the framework including fraud reports from TLS, PTOs and any other parties.	Description in high-level terms. Description detail should be improved and more data included so that additional trigger metrics may be constructed.	Anticipated by 1st April 2010.
It should define all models and metrics used to create triggers and alerts.	Insufficient detail or information. Models should be added to predict escalating problems. Further triggers should be added to include customer acceptance, IT systems loading and cost issues.	Anticipated by 1st April 2010.
It should define the migration decision making process and associated actors.	Described in high-level terms.	Pass.
It should be verifiable that migration would be triggered when stated conditions are met	The start is certain. The acceleration decision framework needs to be verifiable, which should be possible once post-review improvements to the DFA have been made.	Pass for start of migration. Improved DFA Anticipated by 1st April 2010.

Criteria form VenW Requirements paragraph		
At the start of the review all preparatory steps will have been professionally taken to minimise technical, security, project planning, process and decision making risks associated with the Migration Plan	Some significant steps have been taken and the remainder should complete during Phase 1.	Anticipated by 1st Nov 2010.
For the avoidance of doubt the trigger for the start of the Migration Plan will be unambiguously defined taking into account both reasons of business economics and true client acceptance	The start is certain. The acceleration decision according to the improved DFA will be dependent on a precise and expanded set of trigger metrics including business and customer acceptance indicators.	Pass for start of migration. Improved DFA Anticipated by 1st April 2010.
The plan as it affects the regional and national OVCK system will execute within a pre-defined maximum time period.	The plan has a maximum duration in both fast and slow modes.	Pass.
Prior to the completion of the review all aspects of the Migration Plan shall be formally agreed upon by all actors, covering the complete current and future national OVCK system, as specified in the activity plan and the decision framework.	TLS has confirmed to VenW that the *Final* plans are those agreed by TLS and the PTOs.	Pass.
Finally, the discipline of keeping the Migration Plan and associated documentation coherent and up to date is well organised and documented, and is formally agreed upon by all actors.	This was not covered in detail within the input documents. The RHUL recommendation is that this be described within the DFA document.	Anticipated by 1st April 2010.

This concludes the RHUL summary review of the *Final* plans against the VenW criteria.