Migration Plan Review for the Dutch OV-Chipkaart

06.01.10

Executive Summary

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 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. VenW asked RHUL to carry out an independent review of the *migration plan* documentation and determine whether TLS and the PTOs have reached an acceptable state of "migration readiness", based upon a number of pre-defined VenW requirements aimed at determining technical and operational readiness for migration.

On the basis of the technical readiness review of the input documentation, 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 features 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 has therefore been 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[1].

The SmartMX card platform from NXP was selected based on reasoned arguments, although the choice was very restricted due to TLS requirements for legacy protocol (Mifare Classic) support. In the long term (when legacy mode is no longer needed) there is the potential to also use generic types of secured microcontrollers. 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 the *Preliminary* input documents for review. However, due to duplication of vendor effort and ambiguity in the decision framework for the start of migration, the plans were not regarded by RHUL as adequate to cope with the potential of a rapidly escalating threat. TLS had also identified the requirement for a faster response time, which resulted in a substantially revised set of *Final* plans being submitted for further review. The modified strategy within the *Final* plans was based on the principle that migration starts immediately in order to complete crucial technical preparation as soon as possible and avoid

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

duplication of effort. Migration would be "slow" unless a major fraud or attack was detected, in which case the migration speed would be accelerated sufficiently to cope with any rapidly escalating threat. If the *Final* plans start 1st February 2010 a "qualified" state of migration readiness could be reached by 1st November 2010. 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[2] from VenW, RHUL identified a number of recommendations for the improvement of the DFA, which 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 the revision of migration plans and associated documentation 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.

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