Ministerie van Verkeer en Waterstaat

Mobiliteit

RET
tav dhr P. Peters
Postbus
Rotterdam

Contactpersoon	Doorkiesnummer
Datum 30 september 2008	Bijlage(n) -
Ons kenmerk VENW/DGMo-2008/3018	Uw kenmerk -
Onderwerp Review RHUL	

Geachte heer Peters,

De stadsregio Rotterdam heeft bij de staatssecretaris van Verkeer en Waterstaat bij brief van 26 oktober 2007 het verzoek ingediend om het NVB in de Rotterdamse metro uit te zetten. De staatssecretaris heeft in haar brief van 25 augustus 2008 nogmaals het overzicht van eisen gegeven, waaraan voldaan moet zijn voordat aan het verzoek van de stadsregio Rotterdam voldaan kan worden.

Eén van deze criteria betreft het aspect beveiliging. De beoordeling door V&W van dit aspect vindt in dit stadium plaats door review van (1) het regionaal migratieplan (fraudebeheersing) en (2) het plan van aanpak voor de realisatie van het bereiken van migratiegereedheid conform de RHUL contra-expertise van april 2008. V&W stelt goedkeuring van uw aanvraag afhankelijk van zowel de voortgang op het landelijke vlak als in de regio Rotterdam.

Beide plandocumenten zijn inmiddels door Royal Holloway University London (RHUL) getoetst. TLS en RET hebben tijdens de review door RHUL een reeks vragen van RHUL beantwoord. Deze antwoorden heeft RHUL betrokken bij het finaliseren van haar rapportage 'Review of the Project Plan and Regional Fraud management Plan by RHUL' van 8 september 2008. Op dinsdag 23 september heeft VenW de inhoud van dit rapport met TLS besproken en op vrijdag 26 september is de rapportage van RHUL onderdeel van bespreking geweest die ik met mevrouw Baljeu (SRR) en de heer Peters (RET) heb gehad.

Om tot een afrondend oordeel te komen over het criterium beveiliging, leg ik het volgende aan TLS en RET voor.

De conclusies en aanbevelingen uit de rapportage van het RHUL komen er in hoofdlijnen op neer dat de plannen in lijn liggen met de criteria die door VenW zijn gesteld en die in het rapport van de contra-expertise zijn benoemd. RHUL adviseert daarbij een viertal zekerheden te vragen. Ik neem dit advies over en verzoek u mij zekerheid te geven omtrent onderstaande punten, door mij een gezamenlijke schriftelijke reactie te sturen waarin:

1) Herbevestigd wordt dat het migratieplan niet later dan juni 2009 gereed is en ter toetsing aan RHUL kan worden aangeboden.
2) Bevestigd wordt dat de door u gehanteerde kernbegrippen zoals MPM, SRM, project plan en migration plan inhoudelijk overeenkomen met de definities en verduidelijkingen die RHUL geeft in het contra-expertise rapport (april 2008) en haar review (september 2008).
3) Bevestigd wordt dat de periode tussen Rotterdamse beëindiging van het NVB en het opleveren van het migratieplan niet langer dan zes maanden zal bedragen.
4) Bevestigd wordt dat het fraudemanagement conform het regionale fraudemanagement plan operationeel zal zijn voordat het NVB daadwerkelijk zal worden uitgezet, inclusief de desbetreffende 'obligations' die in de review zijn beschreven overeenkomstig uw antwoord in Appendix A.

Gezien de door u gevraagde termijn verzoek ik TLS en RET in een gezamenlijke reactie mij voor 7 oktober 2008 de gevraagde zekerheden te verschaffen. Ik verzoek u daarbij tevens aan te geven welke controlemechanismen binnen uw en de overige betrokken organisaties worden gehanteerd om te verzekeren dat blijvend aan de gestelde eisen zal worden voldaan. Om deze reden stuur ik deze brief ook aan de heer Kok van Trans Link Systems.

Voor 15 oktober 2008 zal ik u vervolgens laten weten of uw inhoudelijke reactie mij voldoende zekerheid geeft om het uitzetten van het NVB in de Rotterdamse metro niet uit te stellen om redenen van beveiliging.

Een afschrift van deze brief stuur ik aan de Stadsregio Rotterdam.

Met vriendelijke groe

DE DIRECTEUR-GENERAAL MOBILITEIT,

drs. S. Riedstra

Appendix A

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.

Ministerie van Verkeer en Waterstaat

Mobiliteit

Trans Link Systems
tav dhr J
Stationsplein
Amersfoort

Contactpersoon	Doorkiesnummer
Datum 30 september 2008	Bijlage(n) 1
Ons kenmerk VENW/DGMo-2008/3018	Uw kenmerk -
Onderwerp Review RHUL	

Geachte heer Kok,

De stadsregio Rotterdam heeft bij de staatssecretaris van Verkeer en Waterstaat bij brief van 26 oktober 2007 het verzoek ingediend om het NVB in de Rotterdamse metro uit te zetten. De staatssecretaris heeft in haar brief van 25 augustus 2008 nogmaals het overzicht van eisen gegeven, waaraan voldaan moet zijn voordat aan het verzoek van de stadsregio Rotterdam voldaan kan worden.

Eén van deze criteria betreft het aspect beveiliging. De beoordeling door V&W van dit aspect vindt in dit stadium plaats door review van (1) het regionaal migratieplan (fraudebeheersing) en (2) het plan van aanpak voor de realisatie van het bereiken van migratiegereedheid conform de RHUL contra-expertise van april 2008. V&W stelt goedkeuring van uw aanvraag afhankelijk van zowel de voortgang op het landelijke vlak als in de regio Rotterdam.

Beide plandocumenten zijn inmiddels door Royal Holloway University London (RHUL) getoetst. TLS en RET hebben tijdens de review door RHUL een reeks vragen van RHUL beantwoord. Deze antwoorden heeft RHUL betrokken bij het finaliseren van haar rapportage 'Review of the Project Plan and Regional Fraud management Plan by RHUL' van 8 september 2008. Op dinsdag 23 september heeft VenW de inhoud van dit rapport met TLS besproken en op vrijdag 26 september is de rapportage van RHUL onderdeel van bespreking geweest die ik met mevrouw Baljeu (SRR) en de heer Peters (RET) heb gehad

Om tot een afrondend oordeel te komen over het criterium beveiliging, leg ik het volgende aan TLS en RET voor.

De conclusies en aanbevelingen uit de rapportage van het RHUL komen er in hoofdlijnen op neer dat de plannen in lijn liggen met de criteria die door VenW zijn gesteld en die in het rapport van de contra expertise zijn benoemd. RHUL adviseert daarbij een viertal zekerheden te vragen. Ik neem dit advies over en verzoek u mij zekerheid te geven omtrent onderstaande punten, door mij een gezamenlijke schriftelijke reactie te sturen waarin:

1) Herbevestigd wordt dat het migratieplan niet later dan juni 2009 gereed is en ter toetsing aan RHUL kan worden aangeboden.
2) Bevestigd wordt dat de door u gehanteerde kernbegrippen zoals MPM, SRM, project plan en migration plan inhoudelijk overeenkomen met de definities en verduidelijkingen die RHUL geeft in het contra-expertise rapport (april 2008) en haar review (september 2008).
3) Bevestigd wordt dat de periode tussen Rotterdamse beëindiging van het NVB en het opleveren van het migratieplan niet langer dan zes maanden zal bedragen.
4) Bevestigd wordt dat het fraudemanagement conform het regionale fraudemanagement plan operationeel zal zijn voordat het NVB daadwerkelijk zal worden uitgezet, inclusief de desbetreffende 'obligations' die in de review zijn beschreven overeenkomstig uw antwoord in Appendix A.

Gezien de door u gevraagde termijn verzoek ik TLS en RET in een gezamenlijke reactie mij voor 7 oktober 2008 de gevraagde zekerheden te verschaffen. Ik verzoek u daarbij tevens aan te geven welke controlemechanismen binnen uw en de overige betrokken organisaties worden gehanteerd om te verzekeren dat blijvend aan de gestelde eisen zal worden voldaan. Om deze reden stuur ik deze brief ook aan de heer Peters van RET.

Voor 15 oktober 2008 zal ik u vervolgens laten weten of uw inhoudelijke reactie mij voldoende zekerheid geeft om het uitzetten van het NVB in de Rotterdamse metro niet uit te stellen om redenen van beveiliging.

Een afschrift van deze brief stuur ik aan de Stadsregio Rotterdam

Met vriendelijke groet

DE DIRECTEUR-GENERAAL MOBILITEIT,

drs. S. Riedstra

Appendix A

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-à-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.