Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2007–2008

23 645 Openbaar vervoer

Nr. 212

BRIEF VAN DE STAATSSECRETARIS VAN VERKEER EN WATERSTAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 juni 2008

Hierbij beantwoord ik de brief van de vaste commissie voor Verkeer en Waterstaat van 6 juni 2008 waarin mij in het kader van de contra-expertise van de Royal Holloway University of London (RHUL) OV-chipkaart het volgende is verzocht:

- Het doen toekomen van alle stukken die ik in het kader van de Wet openbaarheid bestuur (WOB) aan Trouw en Webwereld heb toegezonden;
- Een uiteenzetting van de gang van zaken rondom het RHUL-rapport;
- Een toelichting op wat de RHUL er toe heeft gebracht om wijzigingen in hun contra-expertise aan te brengen.

Bijgaand treft u de stukken aan zoals ik die aan het dagblad Trouw en Webwereld heb toegezonden.[1]

Voor een uiteenzetting van de gang van zaken rondom het RHUL-rapport verwijs ik u naar bijlage 1 bij deze brief waar een chronologische uiteenzetting van de feiten is opgenomen. Hieruit blijkt dat er in het opdrachtverleningsproces en bij de ontvangst van het rapport vanzelfsprekend contact is geweest met de RHUL. Het contact voorafgaande aan de opdrachtverlening was gericht op het maken van afspraken over de opdrachtformulering, de rollen van alle betrokkenen en het proces en de planning. Daarbij is door het departement expliciet de onafhankelijkheid van het RHUL benadrukt. Ook is besproken dat het rapport leesbaar en toegankelijk moet zijn voor het publiek en niet tot misverstanden mag leiden. Het departement heeft geen inhoudelijke bemoeienis met de totstandkoming van het rapport gehad.

De feitelijke gang van zaken rondom de ontvangst van het conceptrapport en het eindrapport toont aan dat er één keer overleg is geweest tussen vertegenwoordigers van het departement en de onderzoekers van de RHUL over het conceptrapport. Dat overleg was, conform de hiervoor genoemde afspraken, gericht op het begrijpen van het rapport en de

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

KST119392
0708tkkst23645-212
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2008

conclusies daaruit en bedoeld om foute interpretaties door de uiteindelijke lezer van het rapport te voorkomen. Door het departement is op geen enkele wijze geïntervenieerd gedurende het onderzoeksproces.

Er is geen causaal verband tussen de contacten van het departement en TLS enerzijds en de totstandkoming van het eindrapport anderzijds, zoals Trouw suggereert. Ook de bewering dat de door Trouw genoemde ambtenaar inhoudelijk met TLS heeft gesproken over het conceptrapport, is onjuist. TLS en TNO hebben mij laten weten dat zij op 30 maart 2008 de eerste vier pagina's van het concept eindrapport hebben ontvangen van de RHUL als onderdeel van de afgesproken review. Doel was om te beoordelen of de conceptversie geen conflicterende passages bevatte in verband met de geheimhoudingsverklaring (NDA). Deze vier pagina's bevatten de onderzoeksbevindingen van de RHUL, niet de conclusies en de aanbevelingen.

De RHUL heeft het rapport op eigen gezag en inzicht op punten verduidelijkt en aangescherpt ten opzichte van de conceptversie. Waarom de RHUL deze verduidelijkingen en aanscherpingen heeft doorgevoerd, kan ik dan ook niet beantwoorden. Ik citeer hierbij nogmaals (zie ook mijn brief van 5 juni 2008 (Kamerstuk 23 645, nr. 211)) dr. Mayes (verantwoordelijk voor het RHUL-rapport): «The first general point I would make is that any written report, book, paper or article starts as a «work-in-progress» and goes through many revisions before the authors judge it is ready for final release. Review of intermediate revisions is ill-advised as they are clearly not the final output/opinions of the authors».

In de media is gesuggereerd dat er grote inhoudelijke verschillen zijn tussen het conceptrapport en het eindrapport van de RHUL. Hoewel dat altijd nog een verantwoordelijkheid is van de RHUL, wil ik die suggestie wel wegnemen. De sleutelaanbeveling in beide versies is nagenoeg gelijk. Ik verwijs u hiervoor naar bijlage 2.

Uit het voorgaande en de in de bijlage gepresenteerde feiten trek ik de conclusie dat het rapport onafhankelijk tot stand is gekomen. Ik herhaal hierbij het citaat van dr. Mayes uit mijn brief van 5 juni 2008:

«I emphasise once again that our review/report was totally independent and free from any outside pressure».

De staatssecretaris van Verkeer en Waterstaat,
J. C. Huizinga-Heringa

BIJLAGE 1

De opdracht aan het RHUL is verstrekt bij brief van 26 maart 2008. Op 13 maart 2008 is een voorbereidend overleg gevoerd tussen het departement, het HEC en de RHUL. Doel van dat gesprek was om de rollen van een ieder te expliciteren (zie schema in onder meer Wob-stuk nr. 8) en de onafhankelijkheid van het RHUL en het onderzoek te benadrukken (zie Wob-stuk nr. 9). De onafhankelijkheid van het RHUL wordt ook benadrukt in de toelichtende brief van 28 februari 2008 van het Het Expertise Centrum (HEC) aan het departement (Wob-stuk nr. 7).

Uit Wob-stuk nr. 8 en nr. 9 blijkt dat de RHUL vanzelfsprekend contact heeft met TNO en TLS. Zij moeten immers hun onderzoek toelichten, stukken tonen, etc. Het gaat hier ook om bedrijfsvertrouwelijke informatie van TNO, TLS en de toeleverancier NXP. Daarom moest de RHUL een geheimhoudingsverklaring (NDA) tekenen. Deze procedure is standaard binnen de onderzoekswereld en is noodzakelijk om gegevens van ondernemingen te verkrijgen. Uit deze geheimhoudingsverklaring volgt dat een uiteindelijke concept eindversie door TNO en TLS beoordeeld moest worden op de vraag of de RHUL in het rapport geen bedrijfsvertrouwelijke informatie heeft opgenomen. Daarnaast is in de opdrachtverlening aan RHUL afgesproken dat TLS en TNO de concept eindversie mochten beoordelen op feitelijke onjuistheden. Bij deze toetsen was het departement vanzelfsprekend niet betrokken. Het betrof immers een toets op het niet-verstrekken van geheime informatie en feitelijke onjuistheden.

Op 20 maart 2008 is het departement door Radboud Universiteit Nijmegen telefonisch geïnformeerd over het feit dat de Universiteit lijkt te slagen in verdere kraakpogingen. Deze informatie is op verzoek van het departement betrokken in de contra-expertise van de RHUL. Hiertoe heeft de Radboud Universiteit op 28 maart een presentatie gegeven aan vertegenwoordigers van HEC en TLS op het departement. Een vertegenwoordiger van het departement heeft de deelnemers welkom geheten en heeft daarna de bijeenkomst verlaten. Het HEC was aanwezig als vertegenwoordiger van de RHUL.

In de week van 28 maart 2008 wordt door ambtenaren de ontvangst van het rapport van het RHUL voorbereid. Hiervoor worden inhoudelijke scenario's van mogelijke aanbevelingen tegen het licht gehouden en wordt een mogelijke planning voorgesteld. Op dat moment beschikte het departement over geen enkel conceptrapport van het RHUL noch was men op een andere wijze bekend met mogelijke eindconclusies van het RHUL. WOB-stuk nr. 10 is dan ook de weergave van what-if scenario's van ambtenaren ter voorbereiding op de ontvangst van het conceptrapport. Het logisch gevolg van een professionele handelswijze waarin het departement zich voorbereidde op een zorgvuldig vervolgproces. Overigens bleek de praktijk anders dan in het WOB-stuk nr. 10 is geschetst. Niet alle in het stuk geplande overleggen hebben plaatsgevonden, aan de overleggen die wel plaatsvonden namen deels andere ambtenaren deel dan genoemd in Wob-stuk nr. 10, en ook het geschetste vervolgproces was in de praktijk een andere.

Ik heb begrepen dat op 30 maart 2008 de eerste vier pagina's van het concept eindrapport naar TLS en TNO zijn gestuurd om te beoordelen of er geen conflicterende passages met de geheimhoudingsverklaring (NDA) in staan. TLS en TNO hebben hier op 1 april 2008 gereageerd en aangegeven dat er geen conflict met de NDA is. Daarnaast hebben zij geen inhoudelijke opmerkingen kunnen maken, omdat een deel van het rapport nog miste.

Op 3 april 2008 ontvangt het departement via HEC de concept eindversie V1.0. Dezelfde dag is het conceptrapport door een aantal ambtenaren

gelezen. Overigens niet tijdens een gezamenlijke sessie zoals WOB-stuk nr. 10 suggereert. Op 3 april 2008 heeft er 's middags geen inhoudelijk overleg met TLS plaatsgehad over de inhoud van het rapport. Wel is er kort met vertegenwoordigers van TLS gesproken over het proces rondom het verschijnen van de contra-expertise. TLS is die dag door het departement niet op de hoogte gebracht van de ontvangst van het conceptrapport.

Met de RHUL was al op 13 maart afgesproken dat op 4 april 2008 's morgens het conceptrapport door de onderzoekers zou worden gepresenteerd aan vertegenwoordigers van het departement met als doel opzet, conclusies en aanbevelingen toe te lichten (Wob-stuk nr. 9). Daarbij was het vooral van belang dat de weergave in het rapport niet tot interpretatieverschillen zou kunnen leiden en dat het rapport voldoende toegankelijk was voor niet-materiedeskundigen.

Tijdens de presentatie op 4 april 2008 hebben vertegenwoordigers van het departement en HEC toelichtende vragen en vragen ter verduidelijking gesteld. Hiervan zijn geen notulen gemaakt, omdat het immers niet de bedoeling was afspraken te maken over de inhoud van het rapport.

TLS en TNO hebben op 4 april 2008 's middags de gelegenheid gekregen om het conceptrapport versie V1.0 in te zien. Op verzoek van het departement is het conceptrapport aan het einde van de middag elektronisch en beveiligd door RHUL naar TLS gestuurd ter informatie. Daarbij is expliciet meegedeeld dat de RHUL de volledige vrijheid had om eventuele opmerkingen van TLS wel of niet te verwerken. TLS heeft per e-mail op zaterdag 5 april 2008 een reactie gestuurd naar RHUL. Het departement heeft daar geen inhoudelijke bemoeienis mee gehad.

Op maandag 7 april 2008 ontvangt het HEC van het RHUL de eindversie. Het HEC heeft in opdracht van het departement getoetst of de eindversie aan de in de opdracht gestelde eisen voldeed en of het RHUL decharge kon worden verleend. Dat bleek het geval (Wob-stuk nr. 13), zodat de eindversie op dinsdag 8 april 2008 aan het einde van de middag aan het departement is gestuurd. De strekking en conclusies van het rapport zijn naar aanleiding van de reacties van betrokken partijen ongemoeid gebleven.

Vervolgens is besloten om het rapport te laten vertalen. Op 10 april 2008 zijn de stukken naar de vertaler gestuurd. Op 12 april 2008 zijn de vertalingen door het vertaalbureau aangeleverd. Op 14 april 2008 zijn die stukken met een begeleidende brief aan de Tweede Kamer gestuurd.

BIJLAGE 2

	Concepteindrapport V1.0	Eindrapport V1.00
Pagina 5, 1e alinea	«The CEB concurs with TNO that the Mifare Classic 4k used in the OV-chipkaart will need to be replaced. The CEB would go further and recommend that any replacement should be based on an algorithm that has been rigorously assessed by the cryptographic expert community, that does not rely on secrecy of the algorithm for security and uses a key length in accordance with cryptographic key length recommendations».	«The CEB concurs with TNO that the Mifare Classic 4k used in the OV-chipkaart will need to be replaced. The CEB would go further and recommend that any replacement should be based on an algorithm that has been rigorously assessed by the cryptographic expert community, that does not rely on secrecy of the algorithm for security and uses a key length in accordance with cryptographic key length recommendations».
Pagina 7, 2e alinea	«The remedial measures suggested by TNO could protect against some attack scenario's, however their practicality is not yet well proven and the effort to introduce them might be better directed towards migrating to a better card technology solution».	«The remedial measures suggested by TNO could protect against some attack scenario's, however their practicality is not yet well proven and this should be investigated as a matter of urgency». Zie verder pagina 5 eerste
Pagina 7, 4e alinea	«The CEB recommends an earlier interim milestone referred to as the Migration Planning Milestone set for January 2009 to coincide with the completion of the national system and the escalation of the OV-chipkaart as an attack target. By this time, the transport companies would be required to present a complete plan for how they would roll out an upgrated/ migration solution».	«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 form the start of nation-wide usage there is a state of preparedness for the migration to a higher level of card security».