Beoordeling migratieplan voor de OV-chipkaart

06-01-10

Inleiding

Op basis van de contra-expertise (CE) van het TNO-rapport over de beveiligingsproblemen van de Mifare Classic-kaart en de OV-chipkaart heeft de Information Security Group/Smart Card Centre (ISG/SCC) van Royal Holloway, University of London (RHUL) geadviseerd voorafgaand aan landelijke invoering van de OV-chipkaart een mijlpaal voor migratieplanning (MPM) vast te stellen. De aanbeveling van RHUL om een *migratieplan* te ontwikkelen voor de overstap naar een nieuwe kaarttechnologie is door de openbaarvervoermaatschappijen overgenomen. In navolging van deze aanbeveling heeft het Nederlandse ministerie van Verkeer en Waterstaat (VenW) Trans Link Systems (TLS) en de exploitanten van openbaar vervoer (PTO's [Public Transport Operators]) verzocht een gecontroleerd en goedgekeurd *migratieplan* gereed te hebben voordat de algemene verplichting om de papieren strippenkaart in het lokale en regionale openbaar vervoer in Nederland te accepteren, wordt opgeheven. Inmiddels hebben TLS en de PTO's een *migratieplan* ontwikkeld voor de overstap naar een nieuwe kaarttechnologie. VenW heeft RHUL verzocht een onafhankelijke beoordeling van dit *migratieplan* uit te voeren en te bepalen of TLS en de PTO's op basis van een aantal eisen van VenW in voldoende mate gereed zijn om te migreren. In dit rapport worden de bevindingen van deze beoordeling samengevat.

Het is belangrijk hierbij op te merken dat gereedheid voor migratie door RHUL wordt gedefinieerd als een 'startknop', in die zin dat de nieuwe technologie wordt ingevoerd zodra aan de eisen voor migratie is voldaan. Dit betekent niet dat er niets meer gedaan hoeft te worden nadat deze knop is ingedrukt; wel dat alle technische risico's en risico's in de planning en het uitvoeringsproces vóór de MPM zijn aangepakt. De gereedheid voor migratie is op te splitsen in twee onderdelen:

- technische gereedheid voor migratie naar een andere kaarttechnologie
- organisatorische gereedheid voor migratie naar een andere kaarttechnologie.

Voor een effectieve migratie en om goed te kunnen reageren op eventuele serieuze, snel opkomende aanvallen op de kaart en fraudescenario’s, zijn beide vormen van gereedheid noodzakelijk. De opdracht aan RHUL was dan ook om zowel de technische als de organisatorische aspecten van de gereedheid in de beoordeling op te nemen. De bij de beoordeling gebruikte criteria komen voort uit de door VenW gestelde eisen die in de volgende paragraaf worden beschreven.

De eisen van VenW

Voorafgaand aan de beoordelingsopdracht voor RHUL stelde VenW de belangrijkste eisen voor de MPM-beoordeling vast. In verband met deze eisen is de RHUL-beoordeling gericht op verschillende belangrijke thema's die hieronder worden genoemd. Voor deze thema's heeft RHUL de voornaamste praktijkdoelstellingen bepaald.

- Risicoanalyse van het systeem
    - Deze moet ervoor zorgen dat alle relevante risico's worden onderkend en vastgelegd, en dat in het migratieprogramma maatregelen ter vermindering van de risico's[1] worden opgenomen.
- Globaal ontwerp van de beveiligingsarchitectuur
    - Dit moet een complete en gedetailleerde beschrijving geven van het beveiligingsprogramma voor de migratie, met inbegrip van de algoritmen, sleutels, modussen, protocollen en berichtreeksen, evenals de implementatieaspecten.
    - Dit ontwerp voor een migratieprogramma moet voldoen aan de geldende normen voor cryptografische beveiliging en de beveiliging van slimme kaarten en informatie.
    - Dit moet laten zien dat het migratieprogramma in voldoende mate toekomstbestendig is.
- Selectie van vervangende kaart/technologie
    - Deze moet de verantwoording leveren voor de keuze van de kaarttechnologie ten opzichte van andere kandidaat-apparaten en -systemen.
    - Deze moet aantonen dat de gekozen kaarttechnologie voldoet aan alle ontwerpcriteria en geschikt is voor het globale ontwerp van de beveiligingsarchitectuur (HLSA)[2].
- Ontwerp, uitvoering en toetsing van de verbetering van de beveiliging van alle componenten van het systeem
    - Dit moet de garantie bieden dat alle verbeteringstaken worden onderkend.
    - Alle technische en ontwerprisico's en/of productkeuzerisico's in verband met verbeteringen van alle relevante componenten van het systeem moeten verifieerbaar zijn opgelost.
    - Dit moet de garantie bieden dat het migratieprogramma zowel vanuit het oogpunt van implementatie als in de uitvoering praktisch is.
- Activiteitenplan[3]
    - Dit moet een realistisch migratieprojectplan[4] opleveren, waarin de belangrijkste activiteiten voor het gehele systeem zijn opgenomen.
    - In het activiteitenplan moet rekening worden gehouden met tijdsrisico's en het plan moet het vertrouwen bieden dat de migratie wordt voltooid binnen het gestelde tijdsbestek (d.w.z. zes maanden na het begin[5]).
    - De belangrijkste verbeteractiviteiten moeten tot in detail zijn vastgelegd, zodanig dat

[1] Van de nieuwe migratietechnologie en niet van herstelmaatregelen op korte termijn (die vallen buiten het bereik van de beoordeling)

[2] Het HLSA (*High Level Security Architecture*) wordt soms ook wel 'globaal ontwerp' genoemd (*High Level Design* of HLD).

[3] In sommige documenten wordt het activiteitenplan 'migratieplan' genoemd.

[4] Met data ten opzichte van 'T0', d.w.z. het moment waarop het besluit tot verbetering wordt genomen.

[5] Dit is aan TLS uitgelegd als een doelstelling (dus geen uiterste grens), gebaseerd op de noodzaak eventuele snel opkomende bedreigingen te verhinderen, en op onze wetenschap dat een grote PTO (buiten Nederland) in staat is binnen deze periode te migreren.

de partijen (en RHUL) ervan overtuigd zijn dat er voldoende informatie beschikbaar is om de activiteiten te begrijpen, te plannen en van middelen te voorzien, en ze er voldoende vertrouwen in hebben dat ze kunnen worden uitgevoerd binnen het algemene activiteitenplan.

- Het moet geverifieerd worden dat TLS en alle PTO's en leveranciers achter het plan staan, deelnemen aan het activiteitenplan, en hun respectieve verantwoordelijkheden begrijpen.

- Besluitvormingsmodel
  - Hierin moet een beschrijving zijn opgenomen van de informatie die is gebruikt voor de samenstelling van het model, waaronder frauderapporten van TLS, PTO's en eventuele andere partijen.
  - Hierin moeten alle modellen en variabelen die worden gebruikt bij het creëren van triggers en waarschuwingen, zijn vastgelegd.
  - Hierin moeten het besluitvormingsproces voor de migratie en de hierbij betrokken partijen zijn vastgelegd.
  - Het moet verifieerbaar zijn dat migratie in gang wordt gezet als aan bepaalde voorwaarden is voldaan.

De verwachting van VenW voor de MPM (en de mate van gereedheid voor migratie) kan met een gedegen inventarisatie van deze thema's worden beoordeeld, uitgaande van de volgende verklaring[6] betreffende bereik en doelstelling:

> *Met deze beschrijving van de onderwerpen van de beoordeling hebben we een goede definitie van technische en organisatorische gereedheid voor migratie. Als met de beoordeling wordt begonnen, zullen vakmatig alle voorbereidende stappen zijn genomen om de met het migratieplan verband houdende risico's op het gebied van techniek, beveiliging, proces, projectplanning en besluitvorming tot een minimum te beperken. Teneinde twijfel te voorkomen, wordt de trigger die het migratieplan in gang zet ondubbelzinnig gedefinieerd met inachtneming van zowel bedrijfseconomische factoren als de werkelijke acceptatie door de klant, en wordt het plan voor zowel het regionale als het nationale OVCK-systeem uitgevoerd binnen een vooraf vastgesteld maximaal tijdsbestek. Voor de beoordeling wordt afgerond, zal door alle partijen formeel worden ingestemd met alle aspecten van het migratieplan, dat het gehele huidige en toekomstige nationale OVCK-systeem bestrijkt, zoals vermeld in het activiteitenplan en het besluitvormingsmodel. Deze partijen zijn de PTO's en TLS. Ten slotte wordt de regeling voor het samenhangend en actueel houden van het migratieplan en alle bijbehorende documentatie goed georganiseerd en gedocumenteerd, en wordt deze formeel goedgekeurd door alle partijen.*

N.B.: De eisen van VenW en de praktische interpretatie daarvan zijn voorafgaand aan de beoordeling aan TLS meegedeeld en vervolgens opgenomen in de beoordelingsmethodiek en -plannen. Gedurende de beoordeling werd echter duidelijk dat de criteria met betrekking tot het besluitvormingsmodel moesten worden herzien, zoals wordt beschreven in de volgende paragraaf.

[6] Citaat van VenW uit documentatie voor beoordelingsplanning MPM

Wijzigingen in de eisen voor het besluitvormingsmodel

Het is belangrijk op te merken dat bij de oorspronkelijke beoordelingscriteria van VenW voor het besluitvormingsmodel werd uitgegaan van een bepaalde migratieplanningsstrategie, d.w.z. het proces en de modellen die ervoor zouden zorgen dat een vooraf gedefinieerd en meetbaar niveau van aanvalsactiviteiten zeker de migratie in gang zou zetten, die dan zou worden voltooid binnen een bepaalde, vastgelegde periode[7]. De planningsstrategie werd echter herzien tijdens de beoordeling door RHUL, en de cruciale beslissing veranderde van 'Wanneer beginnen we met de migratie?' in 'Moeten we de migratie versnellen?'. Deze kwestie werd opgenomen met VenW en als gevolg hiervan werden de volgende wijzigingen aangebracht in de beoordelingscriteria.

1) *In het rapport is geen beoordeling meer nodig van het besluitvormingsmodel voor het beginmoment van de migratie (Decision Framework for the Start of Migration, DF), op basis van de oorspronkelijke criteria, aangezien TLS en de PTO's al hebben besloten te beginnen met de migratie.*

2) *Het DFA-document (*Decision Framework for the Acceleration of Migration, *oftewel Besluitvormingsmodel voor versnelling van de migratie) dient te worden beoordeeld op basis van de oorspronkelijke DF-criteria, met dien verstande dat het DFA niet determinerend hoeft te zijn, maar eerder geschikt moet zijn voor toezicht en controle via een auditfunctie.*

3) *Met het oog op een goed gedefinieerde DFA-auditfunctie wordt RHUL verzocht aanbevelingen te doen voor eventuele verbeteringen in het DFA-document, zodat dit voldoende gedetailleerd een effectief besluitvormingsproces beschrijft dat kan worden gemonitord en gecontroleerd door een auditor.*

4) *Het definitieve plan (gebaseerd op de herziene strategie) wordt het voornaamste onderwerp van de beoordeling en alleen de relevante onderdelen van de beoordeling van het voorlopige plan (gebaseerd op de oorspronkelijke strategie) dienen in het rapport te worden opgenomen.*

Deze criteria vervangen de overeenkomstige oorspronkelijke eisen met betrekking tot de beoordeling door RHUL.

De gehanteerde methodiek

Voordat we een beschrijving geven van de gehanteerde methodiek, is het van belang de praktische omvang van de beoordelingsopdracht vast te stellen in aanvulling op de globale doelstellingen die voortkomen uit de eisen van VenW. Na verschillende gesprekken met TLS en VenW werd overeengekomen dat de beoordeling erop diende te zijn gericht dat een migratiebeveiligingsprogramma wordt geleverd dat voldoet aan de algemene vereiste dat *"de zwakke punten van de Mifare Classic worden opgelost"*. RHUL is sterk van mening dat het migratiebeveiligingsprogramma geëigend moet zijn voor het vastgestelde doel en moet overeenstemmen met de erkende 'beste praktijken' voor slimme kaarten, cryptografie en informatiebeveiliging in het algemeen.

Reikwijdte

RHUL en VenW onderschrijven de visie van TLS dat het grootste deel van de infrastructuur van het systeem geen directe gevolgen heeft ondervonden van de gepubliceerde aanvallen. De reikwijdte en de omvang van het technische deel van de beoordeling werden dan ook als volgt overeengekomen:

[7] Geschikt om snel opkomende bedreigingen/vormen van misbruik te verhinderen.

- de beveiliging van de nieuwe kaart en de infrastructuur van kaartlezers[8], evenals de bijbehorende algoritmen, sleutelformaten, protocollen en het beheer, moeten geschikt zijn voor het vastgestelde doel en overeenstemmen met de 'beste praktijken' voor cryptografische systemen;
- de bestaande beveiligingsniveaus van geen van de onderdelen van de systeeminfrastructuur mogen door de introductie van de nieuwe kaarttechnologie worden verlaagd.

Uit de vereisten voor de beoordeling blijkt duidelijk dat het technisch ontwerp slechts één onderdeel is van een effectief migratieplan. De operationele planning en de besluitvorming vormen cruciale factoren in het bereiken van technische en operationele gereedheid en maken dan ook deel uit van de beoordeling.

Praktische stappen

Oorspronkelijk waren de volgende praktische stappen in de methodiek en het beoordelingsproces gespecificeerd.

- De aangeleverde documenten (zie bijlage A) zouden aan een eerste kritische blik worden onderworpen en het team deskundigen van RHUL zou vragen ter verheldering opstellen voor TLS en VenW[9], die vervolgens zouden worden besproken en beantwoord in gesprekken met TLS/VenW (in Nederland).
- Technische beoordeling
  - Er zouden tegelijkertijd vier gedetailleerde documentbeoordelingen plaatsvinden:
    - risicoanalyses
    - beveiligingsarchitectuur
    - selectie van de chipkaart
    - verbetering van de infrastructuur
  - Demonstratie van de prestaties van de nieuwe technologie.
- Operationele en technische gereedheid
  - Gesprekken met TLS/PTO's/leveranciers.
  - De laatste drie gedetailleerde documentbeoordelingen zouden tegelijkertijd plaatsvinden:
    - leverancierspla nnen
    - activiteitenplan
    - besluitvormingsmodel
- Er zou een intern rapport worden opgesteld, beoordeeld en gereviseerd door het team deskundigen van RHUL.
- TLS zou de concepttekst controleren op onjuistheden en de aanwezigheid van potentiële lekken van vertrouwelijke informatie.
- Het rapport zou vervolgens kunnen worden herzien, hoewel hiertoe geen verplichting bestond, en de wenselijkheid van eventuele wijzigingen zou volledig ter beoordeling zijn van het team deskundigen van RHUL.
- Er zou in Nederland een ontmoeting plaatsvinden tussen de projectleider en VenW en/of hun vertegenwoordigers om de voortgang toe te lichten en de processen voor vertaling en publicatie van het document duidelijk te maken.
- Uiteindelijk zou het document (in het Engels) worden geleverd aan VenW.

RHUL heeft aangegeven dat het bij het volgen van deze stappen (en met toestemming van VenW) bereid was voorlopige bevindingen, feedback en/of aantekeningen met TLS te delen als dit de duidelijkheid ten goede zou komen, en de kwaliteit van de documenten die ter beoordeling werden voorgelegd, zou kunnen verbeteren. Deze feedback en de voortdurende inspanningen van TLS zelf om de migratieplannen zo transparant mogelijk te maken, resulteerden erin dat uiteindelijk twee sets documenten inzake de operationele en technische gereedheid ter beoordeling werden ingediend, waarnaar respectievelijk zal worden verwezen met de benamingen 'voorlopig' en 'definitief'. RHUL heeft

[8] Bijvoorbeeld in-/uitgangspoortjes op stations, kaartjesautomaten, in-/uitcheckzuilen in bussen

[9] Op geen enkel moment tijdens het beoordelingsproces had VenW toegang tot de te beoordelen documenten. De verhelderingen van VenW hadden betrekking op de beoordelingscriteria en -processen.

beide sets documenten beoordeeld, en de beoordelingsresultaten voor de voorlopige documenten worden dan ook genoemd in dit rapport, hoewel de aanbevelingen van RHUL voornamelijk zijn gebaseerd op de definitieve versie. Het grootste deel van de praktische stappen in de beoordeling zou voor zich moeten spreken, maar we geven hieronder toch een korte toelichting.

- Voor de beoordeling moest een set te beoordelen documenten (bijlage A) worden vastgesteld.
    - Uitgangspunt was ervoor te zorgen dat RHUL alle relevante documenten (in het Engels) ruim op tijd voor de beoordeling zou ontvangen, door TLS tijdig te informeren over leveringsdata.
- De beoordelingen van de technische documenten zouden worden aangevuld met een praktische demonstratie van de nieuwe, werkende kaart en kaartlezer, wat vergelijking met het bestaande Mifare Classic-product mogelijk zou maken.
    - De achterliggende gedachte was dat het technische systeem mogelijk prestatieproblemen zou geven, en dat veelvoorkomende transacties met de nieuwe kaart niet veel langzamer zouden mogen zijn dan met de Mifare Classic, omdat het systeem anders mogelijk niet werkbaar is.
    - De tests en demonstraties moesten zo realistisch mogelijk zijn en de onderzoeker de overtuiging geven dat de technische oplossingen snel zouden kunnen worden ingevoerd (zonder verdere technische risico's) in een actief PTO-netwerk.
    - RHUL zou met het oog op de beoordeling technische aantekeningen maken bij de demonstraties en bij technische besprekingen met de deskundigen van TLS die verantwoordelijk waren voor het demonstratiesysteem. Deze aantekeningen zouden van dusdanige aard moeten zijn dat ze een technicus gedetailleerde feitelijke informatie verschaften over de demonstraties en de mate waarin deze representatief zijn voor een actief PTO-netwerk. Ze zouden informatie moeten bevatten over het protocol, data en APDU-berichtreeksen van relevante transacties[10], voor zowel de nieuwe kaart als de reeds geïmplementeerde Mifare Classic-referentiekaart. In dit document met aantekeningen zou ook een korte beschrijving worden gegeven van de voor de demonstratie gebruikte kaart en het lezerplatform, evenals van de testapparatuur en testmetingen.
- Gesprekken met vertegenwoordigers van TLS, PTO's, beslissingsbevoegden en belangrijke leveranciers.
    - Het idee was om de beoordeelde documenten en de werkelijke situatie met elkaar in verband te brengen, en er zorg voor te dragen dat alle partijen gelijkelijk op de hoogte waren van de verantwoordelijkheden, verplichtingen, plannen, technische risico's en activiteiten.

[10] Bijv. controle vervoerbewijzen, verkoop vervoerbewijzen op saldo en opladen saldo.

Beoordeling van het migratieplan

Na bestudering van de aangeleverde documenten en de informatie die tijdens bijeenkomsten werd gegeven, is het team van RHUL ervan overtuigd dat TLS en de PTO's voldoende tijd en middelen hebben besteed aan de voorbereiding op de mijlpaal voor migratieplanning (MPM). Zoals blijkt uit het *migratieplan*, moet, om te kunnen voldoen aan de verwachting met betrekking tot de MPM, een bepaald niveau van gereedheid worden bereikt dat niet alleen wordt bepaald door operationele en technische gereedheid, maar tevens afhankelijk is van technische ontwerpaspecten.

Technische beoordeling

In verband met de technische aspecten van de beoordeling heeft TLS vier hoofddocumenten geleverd en een aantal hiervan op verzoek herzien/verbeterd. TLS heeft daarnaast secundaire documenten geleverd voor een beter begrip van de primaire documenten en ter ondersteuning van de demonstraties en bijeenkomsten waarom RHUL heeft verzocht.

Document voor risicoanalyse: Het document voor risicoanalyse was een gedeelte van een bestaand TLS-document en leverde de informatie die van belang was voor het onderzoek van RHUL. De verschafte informatie gaf een voldoende gedetailleerde technische beschrijving van de manieren waarop misbruik gemaakt kan worden van een Mifare Classic OV-chipkaart. De verschillende aanvalsscenario's werden beschreven en er werd een inschatting gemaakt van de waarschijnlijkheid van dergelijke aanvallen gezien de benodigde vaardigheden, middelen en motivatie van de aanvaller. Aan de hand van een gepubliceerde methodiek was geprobeerd het risico te kwantificeren, hoewel dergelijke methodieken altijd zijn gebaseerd op subjectieve uitgangsgegevens. In de subjectieve gegevens die door TLS werden geleverd, waren veel aanvallen geclassificeerd als 'borderline medium risk' (net onder 'high risk') op basis van aannamen over de benodigde expertise en inspanningen van de aanvallers. Deskundigen van RHUL zijn echter van mening dat het huidige niveau van activiteit en samenwerking binnen de gemeenschap van aanvallers, en de ontwikkelingen binnen de eraan gerelateerde onderzoeksgemeenschappen, inhouden dat er zeer eenvoudig een aanval kan worden uitgevoerd door die van een ander te imiteren. In de classificatie van RHUL, die overigens net zo goed subjectief is, zou het grootste deel van de aanvallen gelden als 'high risk'. Op verzoek van RHUL maakte TLS een matrix van restrisico's. Deze liet zien dat na de technologiemigratie alle 'medium risks' en 'high risks' zouden zijn opgelost. De door RHUL voorgestelde hogere risicoindeling zou dan ook alleen een probleem kunnen vormen in de periode voorafgaand aan de uiteindelijke voltooiing van de migratie.

In het risicoanalysedocument werd bekeken wat het effect van een succesvolle aanval op het systeem zou zijn. Dit effect werd echter alleen uitgedrukt in termen van geld, en werd niet expliciet gerelateerd aan een periode in de tijd of het aantal gevallen van misbruik. Ook werd niet naar niet-financiële aspecten gekeken, zoals reputatieschade of de gevolgen voor klanten en invloed op hun gedrag. Misschien is het, als er een relatief langzame en voorspelbare groei in aanvallen plaatsvindt, werkbaar om de financiële gevolgen over een langere periode te meten en vervolgens te reageren. Voor een zich snel uitbreidend probleem is het mogelijk geen geschikte benadering. Een dergelijk probleem kan bijvoorbeeld optreden als er plotseling grote aantallen geavanceerde klonen beschikbaar komen. Er is dan ook een gevoelige en/of vroege trigger nodig, en de mogelijkheid vervolgens een snelle migratie uit te voeren.

Een potentieel nieuw risico dat niet in dit document (of een ondersteunend document) werd behandeld, komt voort uit de technische strategie (zoals beschreven in het HLD, oftewel globaal ontwerp) om kaarten uit te geven die geschikt zijn voor twee soorten technologie, en vervolgens in de toekomst met een methode te komen voor het kopiëren van informatie van de oude (Mifare Classic) naar de nieuwe technologie. TLS is op de hoogte gebracht van dit risico en heeft verklaard dat het zal worden onderzocht.

Globaal ontwerp: Het document voor het globale ontwerp (HLD) gaf een technisch gedetailleerde beschrijving van het migratieprogramma. In combinatie met informatie uit vraag- en antwoordsessies verschafte dit alle benodigde informatie voor de beoordeling van de technische oplossing. Het HLD heeft

voornamelijk betrekking op de interactie tussen kaart en lezers, en op de noodzakelijke ondersteunende functies, zoals personalisering van de kaart en generatie, distributie en beheer van sleutels. Naar aanleiding van de problemen met de Mifare Classic heeft TLS verklaard dat het bedrijf zich niet wil beperken tot beveiligingsoplossingen die door leveranciers worden aangeboden, en het heeft de beslissende stap genomen om zelf een protocol te ontwikkelen en te beheren dat is gebaseerd op een bekend openbaar algoritme. Het gaat om het algoritme 3DES met twee sleutels, met een sleutellengte van 112 bits. Als dit algoritme op de juiste manier wordt geïmplementeerd, beantwoordt het aan het beveiligingsadvies van ECRYPT/NIST, hoewel AES een actuelere keuze zou zijn geweest. Er wordt gebruikgemaakt van blokvercijfering, waardoor een aantal valkuilen van stroomvercijfering worden vermeden, en er wordt een solide algoritme voor het genereren van willekeurige getallen gebruikt. Tevens wordt een extra beveiligingslaag toegevoegd door data met behulp van 'Message Authentication Codes' (MAC) te authenticeren.

Selectie van de chipkaart: TLS is voornemens nieuwe kaarten uit te geven aan klanten voordat de landelijke infrastructuur volledig is vernieuwd. Daarom moet de kaart ook het oude protocol (Mifare Classic) ondersteunen. Deze beslissing beperkt de aanvankelijke keuze voor een platform tot een keuze tussen de NXP SmartMX en de NXP Mifare Plus. Het laatste product is nog tamelijk nieuw en heeft zich nog niet bewezen. Bovendien is het een particulier product van een leverancier (al zou het zijn gebaseerd op een openbaar algoritme). Dit levert dan ook een conflict op met de beslissing van TLS om het systeem volledig in eigen hand te nemen. TLS heeft tevens rekening gehouden met de mogelijkheid in de toekomst andere typen platforms te gaan gebruiken of andere algoritmen/protocollen te ondersteunen, en met de mogelijkheid van internationaal compatibele systemen voor vervoerbewijzen ('roaming support'). Op basis van deze overwegingen besloot TLS het nieuwe kaartsysteem te implementeren als Java-applet op een SmartMX-platform, met de mogelijkheid alternatieve op Java gebaseerde slimme kaarten te gebruiken wanneer de volledige infrastructuur is vernieuwd. De SmartMX is een redelijk volwassen product dat veel geavanceerder is dan de Mifare Classic en voor gebruik in andere industriële toepassingen met succes is getoetst aan de Common Criteria-veiligheidsnormen (niveau EAL4+).

De operationele prestaties vormen een bron van zorg bij iedere nieuwe technologische ontwikkeling voor vervoerbewijzen op basis van slimme kaarten, maar dit geldt nog meer als het systeem op Java is gebaseerd. Toepassingen voor vervoerbewijzen zijn zeer afhankelijk van de transactiesnelheid; deze beïnvloedt namelijk de communicatie van gebruikers met de leesapparatuur en de gemiddelde snelheid van de reizigersdoorstroming bij toegangspoortjes. Java-applets draaien vanwege de flexibiliteit en veiligheid op een virtuele machine, maar zijn over het algemeen langzamer dan ingebouwde toepassingen en gebruikersspecifieke hardware. Dit is waarom TLS werd verzocht om praktische prestatiedemonstraties te geven van representatieve transacties, waarbij de nieuwe kaart werd vergeleken met een Mifare Classic-referentiekaart. TLS voldeed aan dit verzoek en stelde alle gegevens van de gedemonstreerde transacties en de berichttraces beschikbaar. Tevens werd aan RHUL toestemming verleend om zelf onafhankelijk traces ter beoordeling vast te leggen. Er werden verschillende metingen verricht en de berekenings-/transactiesnelheid laat met de nieuwe kaarttechnologie en het nieuwe protocol een verbetering zien van grofweg 50-80% in vergelijking met de Mifare Classic (voor een vergelijkbare, veelvoorkomende transactie aan een poortje). Volgens TLS valt dit nog net binnen de doelstelling voor praktische bruikbaarheid (wat door RHUL wordt onderschreven) en is er ruimte voor verdere verbetering, bv. door het gebruik van een nieuwe versie van het SmartMX-platform en optimalisering van de 'Secure Application Module' (SAM). Hierbij dient wel te worden opgemerkt dat het huidige prestatieniveau alleen haalbaar was doordat gebruik werd gemaakt van specifiek op de platform-API toegespitste function calls. Anders zou de transactiesnelheid veel lager zijn geweest. Hieruit is de conclusie te trekken dat de applet mogelijk moet worden aangepast als deze in de toekomst op andere chipplatforms wordt geïmplementeerd. Bovendien betekent dit dat de transactietijd afhankelijk is van het gebruikte platform. Bij het kiezen van een geschikt platform moeten, om tot acceptabele prestaties te komen, de opties misschien worden beperkt tot die platforms die gebruikmaken van vergelijkbare function calls.

De demonstratie werd door RHUL beschouwd als een functionele test van de validiteit van het concept. Er werd gebruikgemaakt van een nieuwe kaart (vervoerbewijs) en een vergelijkbare kaart in de vorm van

een SAM. In plaats van een echt poortje werd een laptop gebruikt die de ontbrekende functies en de belasting simuleerde die nodig waren om de prestatieaspecten te testen. De functionaliteit en veiligheid moeten verder worden getest voordat de kaart en SAM geschikt zijn voor gebruik in de Nederlandse netwerken. Het is niet duidelijk of in het gehele netwerk in Nederland één type SAM zal worden gebruikt (RHUL geeft de voorkeur aan deze optie), of dat er uiteindelijk meerder varianten en oudere apparaten zullen zijn van verschillende leveranciers. Er worden geen grote obstakels voorzien voor de voltooiing van de kaart zelf en een gemeenschappelijke SAM zou ook haalbaar moeten zijn. De praktische haalbaarheid van het combineren van meerdere SAM's in de bestaande infrastructuur en het ondersteunen van beheerfuncties en oudere systemen is echter niet duidelijk. RHUL beschouwt dit dan ook als een onderdeel waar nog een technisch risico bestaat.

Verbetering van de infrastructuur: In de documentatie van TLS waren de belangrijkste noodzakelijke verbeteringen van de infrastructuur aangegeven, evenals de betrokken partijen zoals TLS, PTO's en leveranciers. Van iedere verbetering was afgewogen wat de mogelijke gevolgen voor het gehele migratieproces zouden zijn. De in de documenten gebruikte waarderingsstructuur was aanvankelijk niet duidelijk, maar tijdens besprekingen met TLS bleek dat verbeteringen een mogelijk effect werden geacht te hebben als deze invloed zouden hebben op de tijdsduur of de kosten van de gehele migratie, of als de gevolgen voor de tijdsduur en kosten slechts met grote onzekerheid konden worden bepaald. Als een verbetering aanzienlijke gevolgen zou hebben, werd de leverancier in kwestie of het betreffende activiteitenplan ter beoordeling voorgelegd. In het geleverde document kwamen verschillende partijen voor die betrokken zijn bij verbeteringsonderdelen (PTO's/leveranciers/TLS), maar TLS heeft in verhouding maar aan weinig partijen gevraagd om plannen te overleggen. TLS verschafte helderheid door informatie te geven over de relatieve grootte en het belang van de verschillende partijen, en over de 80/20-regel die door TLS was toegepast: de geleverde plannen moesten betrekking hebben op 80% van het migratiesysteem. RHUL vindt dit geen onrealistische benadering, maar de effectbeoordeling zou meer informatie hebben opgeleverd en beter verifieerbaar zijn geweest als deze was opgesplitst in categorieën, zoals risico's op het gebied van techniek, middelen, of tijdsbestek. Dat kosten een effectcategorie vormen (RHUL beschikte niet over gegevens van de kosten, aangezien deze buiten het bestek van dit onderzoek vallen), betekent dat RHUL geen verbeteringen kon controleren die met betrekking tot deze categorie als belangrijk of niet belangrijk zijn aangemerkt. Bovendien is RHUL van mening dat, gezien het feit dat alleen een functioneel prototype van het nieuwe protocol is gedemonstreerd (in plaats van een realistische simulatie met echte apparatuur en systemen), een aantal van de gerapporteerde effecten voor een deel samenhangen met technische implementatierisico's.

RHUL kan weliswaar met een onafhankelijke blik nagaan of de voornaamste verbeteringen uit het HLD ook voorkomen in het document over de verbeteringen van de infrastructuur, en controleren of alle gemarkeerde verbeteringen zijn voorzien van leverancier en/of activiteitenplannen, maar verder kan RHUL niet veel meer controles uitvoeren op het ter beoordeling geleverde document voor de verbeteringen van de infrastructuur. Er is dan ook meer nadruk gelegd op de behandeling van verschillende effectcategorieën binnen de beoordeling van de operationele gereedheid.

Beoordeling operationele gereedheid (planning)

Voor de beoordeling van de operationele gereedheid leverde TLS aanvankelijk drie hoofddocumenten en toelichtingen aan. Gedurende de beginfase van onze beoordeling, en tijdens de informele feedback over onze werkzaamheden aan VenW en TLS, werd duidelijk dat de plannen een aantal grote knelpunten bevatten en dat er sprake was van dubbel geplande activiteiten. Dit betekende dat de planningsstrategie aanmerkelijk moest worden gewijzigd. Na een reeks gesprekken tussen VenW en TLS werd door TLS een set documenten met aanmerkelijke wijzigingen aangeleverd, die vervolgens werd beoordeeld door RHUL. In deze paragraaf verwijzen we naar de oorspronkelijke en de daaropvolgende beoordeling met de respectieve benamingen 'voorlopig' en 'definitief'.

Voorlopige beoordeling

In de oorspronkelijke set documenten is uitgegaan van een gefaseerd traject, waarbij de eerste fase zou worden geïnitieerd als het besluit hiertoe werd genomen op basis van modellen en processen die in een besluitvormingsmodel werden beschreven. Het migratie-/activiteitenplan van TLS bestaat uit vier fasen:

- Fase 1: Voorbereiding op de migratie
  - Fase 1 is erop gericht om eerst de benadering van PTO's en leveranciers te synchroniseren en te komen tot een stadium waarin kaarten kunnen worden uitgegeven die geschikt zijn voor twee soorten systemen ('dual mode cards'). Hiervoor moet de ontwikkeling van de kaartapplet en de kaartuitgiftesystemen in de backoffice zijn voltooid. Er lijkt een kleine aanpassing nodig te zijn om ervoor te zorgen dat de L1-apparaten (lezers) de emulatie van Mifare Classic op de nieuwe kaarten accepteren. De nieuwe 'dual mode cards' zouden vanaf het einde van fase 1 aan nieuwe klanten worden verstrekt.
- Fase 2: Ontwikkeling en uitgifte
  - Fase 2 is gericht op het verbeteren van de infrastructuur teneinde gebruik van het nieuwe kaartsysteem mogelijk te maken.
- Fase 3: Conversie
  - Tijdens fase 3 zullen 'dual mode cards' geconverteerd naar het nieuwe systeem, hoewel de oude Mifare worden -kaarten nog steeds zullen worden ondersteund.
- Fase 4: Migratie voltooid
  - Aan het begin van fase 4 (d.w.z. het einde van fase 3) wordt alleen nog het nieuwe systeem gebruikt.

Voor deze beoordeling hebben we het einde van fase 3 als kritieke mijlpaal aangehouden, aangezien het eerder niet mogelijk is het nieuwe systeem in het gehele Nederlandse vervoerssysteem te gebruiken. Hieronder geven we een kort overzicht van onze aanmerkingen op de voorlopige plannen:

- het migratieproces heeft geen welomschreven begin en einde;
- als er een bedreiging zou worden geconstateerd die zich snel uitbreidt, zou de hierop volgende migratie minstens vier jaar duren, wat niet verenigbaar is met het criterium dat het systeem een *"snelle reactie op een zich snel uitbreidende bedreiging"* mogelijk dient te maken;
- een aantal cruciale leverancierstaken wordt dubbel uitgevoerd;
- er bestaat een aanzienlijk verschil in snelheid tussen de verschillende leveranciersplannen.

De bevindingen van de voorlopige beoordeling werden besproken met TLS en VenW. Dit resulteerde in een herziene planningsstrategie en een aantal aanpassingen van de formele beoordelingscriteria. De herziene set documenten (set 'definitief') werd beoordeeld aan de hand van de criteria die worden beschreven in de volgende paragraaf.

Definitieve beoordeling

De voorlopige feedback met betrekking tot de operationele gereedheid leidde tot een aanmerkelijke positieve wijziging in de migratieplanningsstrategie. De belangrijkste punten kunnen als volgt worden samengevat:

- de migratie 'begint' zodra de plannen van TLS door VenW zijn goedgekeurd;
- er zal allereerst zo snel mogelijk voor migratiegereedheid worden gezorgd, door cruciale taken te centraliseren en de dubbele uitvoering van activiteiten die bij de voorlopige beoordeling werd geconstateerd, te voorkomen;
- de volledige migratie wordt voltooid binnen een vooraf bepaald maximaal tijdsbestek;
- de volledige migratie is een geleidelijk proces (natuurlijke vervanging van bedrijfsmiddelen), tenzij er belangrijke fraudegevallen/aanvallen worden geconstateerd;
- als er in belangrijke mate misbruik van het systeem wordt gemaakt, wordt het migratieproces versneld en afgerond binnen X maanden[11] na het nemen van de beslissing tot versnelling;
- het besluitvormingsmodel (DFA) is nu gericht op de beslissing om de migratie te versnellen en niet langer op de beslissing om het migratieproces in gang te zetten.

Er vonden meer wijzigingen en aanvullende activiteiten plaats, waaronder directe besprekingen tussen VenW en TLS over mogelijke methoden voor het toezicht op de beslissingen tot versnelling van de migratie. Ook zorgde TLS ervoor dat RHUL gesprekken kon voeren met een aantal PTO's en leveranciers ter verificatie van de nieuwe strategie en plannen.

Fase 1: De definitieve plannen (waarbij de vierfasenbenadering werd aangehouden) werden gepresenteerd, inclusief een fase 1 waarin TLS de leiding zou nemen bij de technische activiteiten waarbij leveranciers betrokken zijn, en met de volgende doelstellingen:

- het nieuwe kaartsysteem gereed te maken voor invoering;
- een nieuw algemeen SAM-systeem te ontwikkelen dat door alle leveranciers en PTO's kan worden gebruikt;
- ervoor te zorgen dat leesapparaten een kleine aanpassing ondergaan waardoor ze de Mifare Classic-emulatie op nieuwe kaarten accepteren;
- de PTO's in staat te stellen de nieuwe kaarten uit te geven, in eerste instantie met gebruikmaking van het oude Mifare Classic-systeem.

In fase 1 dient TLS dus rechtstreeks contractuele relaties aan te gaan met een aantal leveranciers (dit is normaal gesproken voorbehouden aan PTO's).

In de planning voor fase 1 worden de essentiële activiteiten afgerond binnen negen maanden na de begindatum (T0). Vanwege de leidende rol van TLS in deze fase is het vertrouwen in de uitvoering van dit plan in hoge mate afhankelijk van TLS en de leveranciers. De gesprekken met leveranciers waren redelijk positief. Voor hun taken zijn ze wegens de gedetailleerde aard afhankelijk van de uitgifte van specificaties in maart 2010. Het vertrouwen werd echter gewekt dat de voor de werkzaamheden benodigde vaardigheden en middelen aanwezig waren. De plannen vereisen tevens dat de concurrerende leveranciers in zekere mate met elkaar samenwerken. Uit de gesprekken met leveranciers ontstond de indruk dat dit zou gebeuren, en gesprekken met PTO's bevestigden dat zij tevens contractueel druk zouden uitoefenen om ervoor te zorgen dat de vereiste samenwerking tussen leveranciers plaatsvindt.

De voltooiing van fase 1 komt in wezen overeen met de mijlpaal voor migratieplanning die door RHUL werd voorgesteld en waarom door VenW werd gevraagd. Dit betekent bijvoorbeeld dat, als we uitgaan van 1 februari 2010 als begindatum, de mijlpaal voor het systeem wordt bereikt op 1 november 2010. Dit garandeert echter op zich geen migratiegereedheid, aangezien de migratie tevens voldoende snel moet kunnen worden uitgevoerd als er zich aanvallen of misbruikgevallen voordoen die zich snel uitbreiden. Dit zou bijvoorbeeld het geval kunnen zijn als er een groot aantal gekloonde kaarten beschikbaar komt en

[11] De exacte lengte van deze periode wordt niet openbaar gemaakt wegens veiligheids-/vertrouwelijkheidsbepalingen.

wordt gebruikt. Voor de voltooiing van de migratie moeten fasen 2 en 3 worden uitgevoerd. Voor deze fasen bestonden twee sets definitieve plannen; de eerste voor een snelle migratie in antwoord op een zich snel uitbreidend aanval, en de tweede voor een geleidelijker migratie die is gebaseerd op de gefaseerde vervanging van de kaarten en systeemonderdelen.

Snelle migratie, fase 2/3: Dit plan zou op zijn vroegst kunnen worden uitgevoerd aan het einde van fase 1, ervan uitgaande dat het besluit tot een snelle migratie wordt genomen tijdens fase 1. Het kan worden beschouwd als een geschikte optie als de migratie snel genoeg is om een snel toenemend aantal gevallen van misbruik te verhinderen. De snelheid waarmee een dergelijk misbruik toeneemt, is niet exact te bepalen, hoewel RHUL een aantal escalatiemodellen heeft onderzocht, en de reactiesnelheid in het plan voor snelle migratie binnen de grenzen valt van wat in deze modellen geldt als aanvaardbaar. De exacte migratiesnelheid is vertrouwelijke informatie en om veiligheidsredenen alleen bekend bij TLS. Na bestudering van het plan voor snelle migratie heeft RHUL echter geen voorstellen voor verdere optimalisatie en we beschouwen dit plan als het in de praktijk snelst mogelijke. Op basis van de definitieve plannen en de hiermee verband houdende verificatiegesprekken, moet voltooiing van fase 1 worden beschouwd als 'migratiegereedheid', op voorwaarde dat er een effectief besluitvormingsproces van kracht is.

Geleidelijke/natuurlijke migratie, fase 2/3: De snelheid van de migratie is van grote invloed op de kosten. Hoewel gedetailleerde gegevens over de kosten niet binnen het bestek van de beoordeling door RHUL vielen, spreekt het voor zich dat zaken als kaarten en de SAM-infrastructuur normaal gesproken een levensduur hebben van een aantal jaren (bijv. vijf jaar) en dat er waardevernietiging plaatsvindt als deze vroegtijdig worden vervangen. TLS en de PTO's willen dan ook liever migreren op een geleidelijker, meer natuurlijke manier (ten opzichte van de 'snelle' plannen). Dit is aanvaardbaar, mits men bereid is op een snelle migratie over te schakelen als er zich een ernstig probleem voordoet. Gedurende de periode dat de geleidelijke migratie wordt uitgevoerd, zullen alle nieuwe kaarten geschikt zijn voor twee systemen, maar nog werken op basis van het oude systeem. SAM's die moeten worden vernieuwd, zullen worden vervangen door nieuwe versies. Dit moet het steeds eenvoudiger maken om te versnellen als dit nodig mocht zijn. De uitvoering van het gehele geleidelijke plan kost veel tijd; na afloop van fase 1 duurt het nog meer dan vijf jaar voor de migratie geheel is afgerond.

Een belangrijke vraag is of het mogelijk is over te schakelen van een geleidelijke op een snelle migratie, aangezien leveranciers en PTO's misschien niet tijdig over de benodigde informatie beschikken om middelen te kunnen reserveren en een planning te maken. In de gesprekken met PTO's en leveranciers werden echter steeds dezelfde antwoorden gegeven, waaruit kon worden opgemaakt dat in een normale bedrijfssituatie altijd pieken voorkomen waarin veel meer middelen nodig zijn, vaak op korte termijn, en dat de migratie dus geen uitzonderlijke eisen stelt.

Planning in het algemeen: In de definitieve plannen lijken de belangrijkste activiteiten te zijn opgenomen, en bij de verschillende partijen bestaan redelijk overeenkomende ideeën en is het vertrouwen aanwezig dat de plannen realistisch zijn. De gesprekken hebben ons voldoende vertrouwen gegeven dat de verschillende partijen hun rol en verantwoordelijkheden kennen en zich zullen inzetten voor het migratieplanningsproces.

Besluitvormingsmodel voor versnelling van de migratie (DFA): De herziene migratieplannings-strategie voldoet automatisch aan twee van de oorspronkelijk door VenW gesteld eisen:

- *de trigger die het migratieplan in gang zet, wordt ondubbelzinnig gedefinieerd;*
- *het plan voor zowel het regionale als het nationale OVCK-systeem wordt uitgevoerd binnen een vooraf vastgesteld maximaal tijdsbestek.*

De cruciale beslissing is nu echter wanneer de migratie moet worden versneld, en de relevante beoordelingseisen, toegepast op de beslissing tot versnelling, en het commentaar van RHUL zijn hieronder kort weergegeven.

- *Hierin moet een beschrijving zijn opgenomen van de informatie die is gebruikt voor de samenstelling van het model, waaronder frauderapporten van TLS, PTO's en eventuele andere partijen.*
    - De aangeleverde informatie wordt beschreven in globale termen.
    - Er zou bij voorkeur meer informatie moeten worden aangeleverd, zodat in het DFA met een groter aantal potentiële problemen rekening kan worden gehouden.
- *Hierin moeten alle modellen en variabelen die worden gebruikt bij het creëren van triggers en waarschuwingen, zijn vastgelegd.*
    - Er worden geen modellen gegeven.
    - Er moeten modellen worden toegevoegd, zodat beter kan worden voorspeld of en wanneer problemen zullen escaleren.
    - Er wordt slechts één kwantiteit of variabele genoemd als basis voor een trigger (en dit is eerder een proces dan een directe trigger voor versnelling).
        - Deze variabele betreft een percentage van het totale aantal transacties in het gehele landelijke netwerk. RHUL stelt voor dit percentage voor ieder netwerk en/of iedere PTO apart te berekenen, zodat voor het besluitvormingsproces ook lokale problemen zichtbaar zijn en deze niet 'verdwijnen' in een landelijk gemiddelde.
        - Het is aan te raden meerdere variabelen als basis voor triggers te gebruiken, zodat beter rekening kan worden gehouden met kosten, acceptatie door de klant, en de belasting van IT-systemen.
- *Hierin moeten het besluitvormingsproces voor de migratie en de hierbij betrokken partijen zijn vastgelegd.*
    - Globaal gedefinieerd.

RHUL is van oordeel dat het DFA nog niet voldoende is uitgewerkt en niet voldoende duidelijk is om op een eenvoudige en onafhankelijke manier te kunnen worden gemonitord. Het gebrek aan modellen en triggers betekent tevens dat er een aanzienlijk niveau van deskundigheid vereist is om ontwikkelingen te kunnen interpreteren (wat in een eenvoudige/gebruikelijke auditfunctie niet nodig zou moeten zijn). RHUL doet dan ook voorstellen ter verbetering van het DFA (deze worden genoemd in de paragraaf Samenvatting en aanbevelingen) en raadt VenW sterk aan om van TLS te verlangen deze aanbevelingen over te nemen als zijnde uit de beoordelingen voortvloeiende verplichtingen.

Samenvatting en aanbevelingen

Uit de beoordeling van de technische gereedheid, op basis van de eerste vier geleverde primaire documenten, komt het beeld naar voren dat de nieuwe kaarttechnologie een architectuur ondersteunt die ontworpen is voor flexibiliteit, voldoende toekomstbestendig is, en de afhankelijkheid van leverancierspecifieke implementaties vermindert. Voor het protocol wordt gebruikgemaakt van een openbaar algoritme met een sleutelformaat dat beantwoordt aan internationale aanbevelingen. Positieve aspecten zijn verder het gebruik van blokvercijfering in plaats van stroomvercijfering, wat een betere beveiliging biedt, en een extra beveiligingslaag in de vorm van gegevensauthenticatie. De prestaties van het systeem (in ieder geval aan de kant van de kaart) lijken voldoende te zijn voor de bedoelde toepassing. Op basis van deze bondige beoordeling heeft RHUL geen opvallende, grote gebreken gevonden in het ontwerp (voor het protocol en het kaartsysteem), hoewel natuurlijk van openbare beoordelingen bekend is dat de veiligheid met meer zekerheid kan worden vastgesteld naarmate er meer beoordelaars bij worden betrokken. TLS wordt daarom aangeraden meer zekerheid te verkrijgen over de veiligheid van het protocolontwerp en de uiteindelijke implementatie aan de hand van een 'open' benadering of door inschakeling van commerciële of universiteitslabs. Het is nog niet bekend wat de kwaliteit is van de implementatie van de beveiligingsmaatregelen (afgezien van prestatie-indicatoren), en TLS heeft het advies gekregen om het systeem en de implementatie op het SmartMX-kaartplatform te laten evalueren door een commercieel testlaboratorium[12], en dit opdracht te geven om te toetsen op alle bekende mogelijke aanvallen, te weten logische en fysieke aanvallen en *side-channel* en *fault attacks*. Vastgesteld werd dat de belangrijkste risico's met betrekking tot de verbetering van de infrastructuur zijn onderkend en dat voor elk van deze risico's als onderdeel van het algemene activiteitenplan een leverancierspplan is opgesteld. Hoewel technische gereedheid nog niet is bereikt, wordt verondersteld dat dit zal gebeuren als de geplande activiteiten zijn uitgevoerd.

Teneinde de operationele gereedheid vast te kunnen stellen, werden door TLS in eerste instantie nog drie primaire documenten ('voorlopige' set) ter beoordeling geleverd. Ook werden belangrijke medewerkers beschikbaar gesteld voor bijeenkomsten en gesprekken. Nadat tijdens het beoordelingsproces feedback was geleverd, verschafte TLS een set herziene documenten ('definitieve' set) en maakte het bedrijf verificatiegesprekken mogelijk met een aantal leveranciers en PTO's. Bij de beoordeling van de plannen werd er vanuit gegaan dat PTO's in staat zouden moeten zijn een plotseling toenemende bedreiging snel te pareren, bijvoorbeeld wanneer er op grote schaal geavanceerde gekloonde kaarten beschikbaar zouden komen, of wanneer er steeds meer gebruik zou worden gemaakt van reeds bestaande aanvalsmethoden. In fase 1 van de plannen werd een aantal voorbereidende activiteiten beschreven, terwijl in fase 2 de verbetering van de infrastructuur werd behandeld. Het einde van fase 3 werd echter beschouwd als de cruciale prestatiemijlpaal, omdat dit het vroegst mogelijke moment is waarop het nieuwe kaartbeveiligingssysteem kan worden gebruikt in PTO-netwerken in heel Nederland.

De voorlopige activiteiten- en leverancierspplannen voldeden niet aan de beoordelingscriteria. Eenvoudig gezegd zou het vanaf het moment dat de migratie in gang zou worden gezet (door een groot en/of urgent probleem) meer dan vier jaar duren om geheel over te schakelen op de nieuwe technologie. Naar het oordeel van RHUL is dit volstrekt ontoereikend om een zich snel uitbreidende bedreiging het hoofd te bieden. De definitieve plannen lieten volgens RHUL belangrijke verbeteringen zien. Deze plannen waren gebaseerd op het uitgangspunt dat meteen met de migratie zou worden begonnen, zodat de cruciale technische voorbereidingen zo snel mogelijk zouden kunnen worden afgerond, en bepaalde inspanningen niet dubbel zouden worden verricht. De migratie zou geleidelijk worden uitgevoerd, tenzij er een grote bedreiging zou worden geconstateerd. In een dergelijk geval zou de migratie worden versneld in overeenstemming met de snelheid volgens een escalatiemodel voor toenemende bedreigingen. Wanneer op 1 februari 2010 met de plannen zou worden begonnen, zou op 1 november 2010 een 'gekwalificeerd' stadium van gereedheid worden bereikt.

[12] Uit gesprekken is naar voren gekomen dat er door TLS waarschijnlijk al met commerciële of universiteitslabs wordt gewerkt aan meer zekerheid betreffende de beveiliging.

We noemen dit een gekwalificieerd stadium omdat het alleen wordt bereikt als het versnelde plan in werking treedt naar aanleiding van een effectief besluitvormingsmodel (DFA). Op grond van de herziene beoordelingsvereisten[13] van VenW heeft RHUL een aantal aanbevelingen gedaan voor verbetering van het DFA, zoals de toevoeging van meetgegevens waardoor de beslissing tot versnelling in de praktijk zou kunnen worden gemonitord en gecontroleerd via een auditfunctie. De aanbevelingen kunnen als volgt worden samengevat:

- het aantal triggervariabelen wordt uitgebreid met kwantiteiten die verband houden met acceptatie door de klant, de belasting van IT-systemen en kostengerelateerde kwesties;
- er worden modellen gedefinieerd waarmee potentiële escalatietrends voor triggervariabelen kunnen worden voorspeld;
- er wordt niet uitgegaan van landelijke gemiddelden, maar voor ieder netwerk en/of iedere PTO worden de triggervariabelen apart berekend;
- er wordt een volledige set aanvankelijke drempelwaarden voor triggers gedefinieerd;
- er wordt een procedure vastgelegd voor mogelijke aanpassing van de drempelwaarden voor triggers;
- in het DFA-document wordt een procedure opgenomen die de samenhang en actualisering van de migratieplannen en de bijbehorende documenten garandeert.

Vooropgesteld dat de definitieve plannen worden goedgekeurd en dat TLS de aanbevelingen van RHUL voor het DFA binnen twee maanden na aanvang van de definitieve planning aanvaardt en overneemt, is de conclusie van RHUL dat TLS en de PTO's op l november 2010 gereed zouden moeten zijn voor migratie, als met de werkzaamheden wordt begonnen op 1 februari 2010.

In bijlage B wordt voor de verschillende criteria van VenW ons beoordelingscommentaar weergegeven.

Tot zover de beoordeling van RHUL.

[13] Deze herzieningen waren nodig omdat in de oorspronkelijke beoordelingscriteria geen rekening was gehouden met een versnelling van de migratie.

Bijlage A

Ter beoordeling geleverde documenten

De documentatie bestond uit een set primaire en secundaire (ondersteunende) documenten. De zeven subtaken van de beoordeling werden elk uitgevoerd op basis van één primair document. De secundaire documenten werden niet beoordeeld. Deze werden alleen gebruikt voor aanvullende gegevens en voor een beter begrip van de primaire documenten. TLS werd aangemoedigd alle primaire documenten aan het begin van het project te verschaffen, zodat kon worden geprofiteerd van het eerste stadium waarin eventuele vragen zouden kunnen worden opgehelderd. Een primair document mocht in geen geval later worden ontvangen dan de geplande begindatum van de bijbehorende beoordelingstaak. Tijdens het beoordelingsproces werd een aantal herziene plannen en documenten betreffende besluitvormingsmodellen geleverd. De oorspronkelijke set ('voorlopig') en de daaropvolgende set ('definitief') werden beide beoordeeld, waarbij de nadruk lag op de definitieve set.

Hierbij moet worden opgemerkt dat alleen documenten die in het Engels waren aangeleverd, werden beschouwd als 'ter beoordeling geleverd'. De oorspronkelijk overeengekomen set documenten is hieronder weergegeven. Tijdens de voorbereiding op en de uitvoering van de beoordeling werd het echter toegestaan om meer secundaire documenten toe te voegen als TLS en RHUL hier beide mee instemden. De documenten moesten als definitief zijn aangemerkt met instemming van TLS, de PTO's en, waar nodig, de leveranciers.

Technische gereedheid – primaire set documenten

- *MPM1: Security Risk Assessment (SRA* – Analyse van veiligheidsrisico's*)* → *taak 8*
- *MPM2: High Level Design (HLD* – Globaal ontwerp*)*[14] → *taak 9*
- *MPM3: Chip Selection (CS* – Selectie van de chip*)* → *taak 10*
- *MPM4: Infrastructure Upgrades (IU* – Verbeteringen van de infrastructuur*)* → *taak 11*

Operationele gereedheid – primaire set documenten

- *MPM5: Vendor Plans (VP* – Leveranciersplannen*)* → *taak 13*
- *MPM6: Activity Plan (AP* – Activiteitenplan*)*[15] → *taak 14*
- *MPM7: Decision Framework (DF* – Besluitvormingsmodel*)*[16] → *taak 15*

Ondersteunende documenten

- Specificatie van vereisten
- Beveiligingsprofiel (*Protection Profile*, PP)
- Demonstratieaantekeningen (*Demonstration Notes*, DN)[17]
- Rapporten/resultaten van kaart- en kaartlezerdemonstraties en -tests
- Regionale fraudemanagementplannen (RFMP) die eerder zijn beoordeeld
- Datasheets van producten
- Origineel CE-rapport

[14] Dit document moet een volledige en gedetailleerde beschrijving bevatten van de nieuwe beveiligingstechnologie, met onder meer het algoritme, de sleutels, de modussen, de protocollen en de implementatiebeveiligingsfuncties.

[15] In het activiteitenplan moeten tevens de inspanningen zijn opgenomen die TLS zelf heeft verricht om risico's in verband met de uitvoering van het migratieplan op te sporen en te verkleinen.

[16] Dient te bevatten: a) de gegevens van de frauderapporten, b) de triggerberekeningen/-modellen, en c) het migratiebesluitvormingsproces.

[17] Dit is geen aangeleverd document, maar een serie aantekeningen die door RHUL zijn gemaakt tijdens demonstraties.

Bijlage B

Onderstaande tabel geeft in het kort ons oordeel over de definitieve plannen weer aan de hand van de criteria van VenW. De oorspronkelijke criteria voor beoordeling van het besluitvormingsmodel (DF) waren gericht op een beslissing over het beginmoment van de migratie en niet over een versnelling. Tijdens het beoordelingsproces bleek het dan ook noodzakelijk voor het besluitvormingsmodel voor versnelling (DFA) een aantal beoordelingscriteria formeel te herzien.

Tabel 1: Commentaar na beoordeling op grond van de criteria van VenW

Criterium	**Commentaar**	**Status**
Risicoanalyse van het systeem		
Deze moet ervoor zorgen dat alle relevante risico's worden onderkend en begrepen, en dat in het migratie-programma maatregelen ter vermindering van de risico's[18] worden opgenomen.	Er zijn technische risico's[19] vastgesteld. In de geleverde documenten is geen aandacht besteed aan een potentieel conversierisico.	Voldoende (mits TLS aandacht besteedt aan dit risico).
Globaal ontwerp van de beveiligingsarchitectuur		
Dit moet een complete en gedetailleerde beschrijving geven van het beveiligingsprogramma voor de migratie, met inbegrip van de algoritmen, sleutels, modussen, protocollen en berichtreeksen, evenals de implementatieaspecten.	Dit was een gedetailleerd document met voldoende informatie om de beoordeling te kunnen uitvoeren.	Voldoende
Dit ontwerp voor een migratie-programma moet voldoen aan de geldende normen voor crypto-grafische beveiliging en de beveiliging van slimme kaarten en informatie.	Er is gekozen voor een openbaar algoritme en de sleutelformaten zijn in overeenstemming met aanbevelingen voor 'beste praktijken'. Het protocol is gebaseerd op openbare standaard-algoritmen. We willen opmerken dat TLS aanvullende maatregelen moet nemen om de veiligheid van het ontwerp en de implementatie te garanderen.	Voldoende
Dit moet laten zien dat het migratieprogramma in voldoende mate toekomst-bestendig is.	TLS heeft gekozen voor een systeem dat uiteindelijk kan worden geïmplementeerd op een ruim aantal beveiligde micro-processorplatforms die worden gebruikt in slimme kaarten, maar mogelijk ook in mobiele telefoons en andere apparaten. Het is een flexibel systeem dat waarschijnlijk van alle opties waaruit TLS de keuze had, het meest flexibel en toekomstbestendig is.	Voldoende

[18] Van de nieuwe migratietechnologie en niet van herstelmaatregelen op korte termijn (die vallen buiten het bereik van de beoordeling)

[19] Aan andere risico's is aandacht besteed bij het beoordelen van de documenten voor operationele gereedheid.

Selectie van vervangende kaart/technologie		
Deze moet de verantwoording leveren voor de keuze van de kaarttechnologie ten opzichte van andere kandidaat-apparaten en -systemen.	De keuze voor de kaart is verantwoord, hoewel er, gezien de strategie om 'dual mode'-kaarten aan te bieden die tevens emulatie van de Mifare Classic 4K ondersteunen, weinig andere kandidaten waren.	Voldoende
Deze moet aantonen dat de gekozen kaarttechnologie voldoet aan alle ontwerpcriteria en geschikt is voor het globale ontwerp van de beveiligings-architectuur (HLSA/HLD).	De gekozen kaart voldoet aan de in het HSLA/HLD gestelde eisen.	Voldoende
Ontwerp, uitvoering en toetsing van de verbetering van de beveiliging van alle componenten van het systeem		
Dit moet de garantie bieden dat alle verbeteringstaken zijn vastgesteld.	De belangrijkste verbeterpunten lijken te zijn onderkend.	Voldoende
Alle technische en ontwerprisico's en/of productkeuzerisico's in verband met verbeteringen van alle relevante componenten van het systeem moeten verifieerbaar zijn opgelost.	Hoewel bij een functionele demonstratie de kaart en SAM-communicatie bleken te werken, kon dit punt niet volledig worden geverifieerd. Tijdens de activiteiten in fase 1 moet hierover dan ook uitsluitsel worden verkregen.	Verwacht voor 1 nov. 2010
Dit moet aantonen dat het migratie-programma zowel vanuit het oogpunt van implementatie als in de uitvoering praktisch is.	Het kaartsysteem lijkt functioneel in de uitvoering te zijn (vooraf werd hieraan getwijfeld). Het is niet bekend hoe functioneel alle systeemverbeteringen zijn. Hierover moet uitsluitsel worden verkregen tijdens de activiteiten in fase 1.	Verwacht voor 1 nov. 2010
Activiteitenplan[20]		
Dit moet een realistisch migratie-projectplan opleveren, waarin de belangrijkste activiteiten voor het gehele systeem zijn opgenomen, met data ten opzichte van 'T0', d.w.z. het moment waarop het besluit tot verbetering wordt genomen.	Het 'snelle' plan is realistisch waar het de snelheid betreft, en is geverifieerd door de personen met wie is gesproken. Het geleidelijke migratieplan is waarschijnlijk realistisch waar het de minimalisering van de vervangingskosten voor bedrijfsmiddelen betreft.	Voldoende
In het activiteitenplan moet rekening worden gehouden met tijdsrisico's en het plan moet het vertrouwen bieden dat de migratie wordt voltooid binnen het gestelde tijdsbestek.	De versnellingsoptie maakt het mogelijk te reageren op belangrijke bedreigingen. De snelle procedure valt binnen de grenzen die volgens escalatiemodellen als aanvaardbaar gelden.	Voldoende

[20] In sommige documenten wordt het activiteitenplan 'migratieplan' genoemd.

De belangrijkste verbeteractiviteiten moeten tot in detail zijn vastgelegd, zodanig dat de partijen (en RHUL) ervan overtuigd zijn dat er voldoende informatie beschikbaar is om de activiteiten te begrijpen, te plannen en van middelen te voorzien, en ze er in voldoende mate vertrouwen in hebben dat ze kunnen worden uitgevoerd binnen het algemene activiteitenplan.	De geleverde gegevens zijn voor dit stadium voldoende gedetailleerd (maar niet echt uitgebreid). De personen met wie is gesproken, leken goed geïnformeerd.	Voldoende
Het moet geverifieerd worden dat TLS en alle PTO's en leveranciers achter het plan staan, deelnemen aan het activiteitenplan, en hun respectieve verantwoordelijkheden begrijpen.	Er hebben gesprekken plaatsgevonden en alle gesprekspartners leken gemotiveerd en goed geïnformeerd.	Voldoende
Het besluitvormingsmodel (voor versnelling)		
Hierin moet een beschrijving zijn opgenomen van de informatie die heeft bijgedragen aan de samenstelling van het model, waaronder frauderapporten van TLS, PTO's en eventuele andere partijen.	Beschrijving in algemene termen. De beschrijvingen moeten worden uitgebreid, zodat aanvullende triggervariabelen kunnen worden vastgesteld.	Verwacht voor 1 april 2010
Hierin moeten alle modellen en variabelen die worden gebruikt bij het creëren van triggers en waarschuwingen, zijn vastgelegd.	Deze zijn onvoldoende gedetailleerd of bevatten niet genoeg gegevens. Er moeten modellen worden toegevoegd waarmee zich snel uitbreidende problemen kunnen worden voorspeld. Er moeten triggers worden toegevoegd op het gebied van acceptatie door de klant, de belasting van IT-systemen en kostengerelateerde kwesties.	Verwacht voor 1 april 2010
Hierin moeten het besluitvormings-proces voor de migratie en de hierbij betrokken partijen zijn vastgelegd.	In algemene termen beschreven.	Voldoende
Het moet verifieerbaar zijn dat migratie in gang wordt gezet als aan bepaalde voorwaarden is voldaan.	Het beginmoment is al bepaald. Het besluitvormingsmodel voor versnelling moet verifieerbaar zijn op het moment dat de verbeteringen naar aanleiding van deze beoordeling zijn aangebracht in het DFA.	Voldoende voor begin van migratie. Verbeterd DFA verwacht voor 1 april 2010.

Criteria uit paragraaf *De eisen van VenW*		
Als met de beoordeling wordt begonnen, zullen vakmatig alle voorbereidende stappen zijn genomen om de met het migratieplan verband houdende risico's op het gebied van techniek, beveiliging, proces, projectplanning en besluitvorming tot een minimum te beperken.	Er is een aantal belangrijke stappen genomen. De overige moeten worden afgerond tijdens fase 1.	Verwacht voor 1 nov. 2010.
Teneinde twijfel te voorkomen, wordt de trigger die het migratieplan in gang zet ondubbelzinnig gedefinieerd met inachtneming van zowel bedrijfseconomische factoren als de werkelijke acceptatie door de klant.	Het beginmoment is al bepaald. De beslissing tot versnellen wordt op grond van het verbeterde DFA genomen naar aanleiding van een precieze en uitgebreide serie triggervariabelen, waaronder indicatoren voor bedrijfseconomische factoren en acceptatie door de klant.	Voldoende voor begin van migratie. Verbeterd DFA verwacht voor 1 april 2010.
Het plan voor zowel het regionale als het nationale OVCK-systeem wordt uitgevoerd binnen een vooraf vastgesteld maximaal tijdsbestek.	Voor uitvoering van het plan geldt zowel in de snelle als in de geleidelijke versie een maximale tijdsduur.	Voldoende
Voor de beoordeling wordt afgerond, zal door alle partijen formeel worden ingestemd met alle aspecten van het migratieplan, dat het gehele huidige en toekomstige nationale OVCK-systeem bestrijkt, zoals vermeld in het activiteitenplan en het besluitvormingsmodel.	TLS heeft aan VenW bevestigd dat de definitieve plannen de plannen zijn die door TLS en de PTO's zijn goedgekeurd.	Voldoende
Ten slotte wordt de regeling voor het samenhangend en actueel houden van het migratieplan en alle bijbehorende documentatie goed georganiseerd en gedocumenteerd, en wordt deze formeel goedgekeurd door alle partijen.	Dit is in de aangeleverde documentatie niet gedetailleerd beschreven. De RHUL raadt aan om een beschrijving hiervan op te nemen in het DFA.	Verwacht voor 1 april 2010.

Tot zover het overzicht van de beoordelingen van RHUL betreffende de definitieve plannen, op grond van de criteria van VenW