Collis

Evaluatie van testen op chip in Nederlandse reisdocumenten

Evaluatie en testrapport

Auteur	Remko Muis, Paul van Leeuwen, Peter Kok, David Bakker
Versie	1.0
Datum	27 juni 2008
Status	Definitief

Document gegevens

Project Code	MinBZK_2008_120
Document Titel	Evaluatie van testen op chip in Nederlandse reisdocumenten
Bestandsnaam	MinBZK_2008_120 (review testen chip op Nederlandse reisdocumenten) v1.0.doc
Status	Definitief

Collis BV
De Heyderweg 1
2314 XZ LEIDEN
The Netherlands
Tel. +31-71 – 581 36 36
Fax +31-71 – 581 36 30
E-mail info@collis.nl
Web-site www.collis.nl

Versie historie

Versie	Date	Status	Auteur
1.0	27-06-2008	Definitief	R. Muis, P. van Leeuwen, P. Kok, D. J. Bakker

Wijzigingen

Versie	Datum	Reden van wijziging

INHOUDSOPGAVE

MANAGEMENTSAMENVATTING

In 2006 heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) het nieuwe Nederlandse electronische paspoort en de Nederlandse Identiteitskaart (NIK) ingevoerd. Voorafgaand aan de invoering heeft Collis, in opdracht van het ministerie, testen uit gevoerd op het elektronische paspoort en de NIK, om na te gaan of deze zich gedragen conform ISO-14443, ISO 7816 en ICAO Doc 9303 standaarden. Tevens heeft Collis onderzocht of er ongespecificeerd gedrag werd vertoond dat kon worden gebruikt om de authenticiteit en de vertrouwelijkheid van de gegevens in de chip van de genoemde reisdocumenten te schaden. Collis heeft toen gerapporteerd dat het electronisch paspoort en de NIK geschikt waren als elektronisch reisdocument.

In april 2008 heeft het ministerie Collis gevraagd of de toenmalige conclusies nog steeds van kracht zijn, of dat er in de achterliggende twee jaar ontwikkelingen zijn geweest die de beveiliging van de chip in een ander perspectief plaatsen. Indien de tests uit 2006 daarover onvoldoende uitsluitsel blijken te geven, werd Collis verzocht te beschrijven welke testen nog uitgevoerd moesten worden om de resultaten uit 2006 te actualiseren.

Daarnaast is Collis gevraagd vast te stellen of de paspoorten van Nederland, Finland, Slowakije en Ierland en de Nederlandse Identiteits Kaart (NIK) zich identiek gedragen tijdens het deel van de communicatie met de chip dat voorafgaat aan BAC (Basic Access Control). Hiervoor heeft het ministerie testdocumenten van Finland, Ierland en Nederland uit 2006 en Finse, Ierse, Nederlandse en Slowaakse testdocumenten uit 2008 aan Collis ter beschikking gesteld.

Dit document vormt het eindrapport voor deze opdracht. Het geeft achtereenvolgens:

a) een evaluatie van de in 2006 uitgevoerde testen en de rapportage daarvan.
b) de resultaten van een aantal testen waarin wordt nagegaan of de ter beschikking gestelde reisdocumenten zich, voorafgaande aan BAC, identiek gedragen, op de volgende niveaus:
    1) Electronisch niveau (ISO 14443-2)
    2) Datatransmissie-niveau (ISO 14443-3/4)
    3) Applicatie-niveau (ICAO layer 6-7)

De belangrijkste conclusies uit dit onderzoek zijn de volgende:

1. De resultaten van het onderzoek verricht in 2006 zijn nog steeds geldig. De vertrouwelijkheid en authenticiteit van de gegevens in de chip van de Nederlandse reisdocumenten is voldoende gewaarborgd. Het Nederlandse paspoort en de NIK worden geschikt geacht voor gebruik als elektronisch reisdocument.
2. Voor wat betreft de vraag of het mogelijk is om voorafgaande aan het BAC protocol gegevens aangaande de nationaliteit van het reisdocument te achterhalen, wordt het volgende geconcludeerd. Er is slechts één verschil aangetroffen tussen de onderzochte reisdocumenten: de documenten met uitgiftedatum in 2006 verzenden tijdens de uitvoering van het ISO 14443 protocol een zogeheten UID waarin een tweetal bits een vaste waarde heeft. De documenten die zijn uitgegeven in 2008 verzenden UIDs waarin alle bits willekeurig zijn. Binnen de groep documenten van 2006 en binnen de groep documenten van 2008 zijn geen verschillen gevonden. De Ierse, Finse en Nederlandse documenten uit 2006 laten voorafgaande aan BAC eenzelfde gedrag zien. Voor de

Ierse, Finse, Nederlandse en Slowaakse documenten uit 2008 geldt dat zij voor de BAC-fase niet van elkaar te onderscheiden zijn. Voor de BAC-fase is dus de generatie van de onderzochte testdocumenten te bepalen, maar niet de nationaliteit.

1 INLEIDING

In het kader van de continue aandacht die van de zijde van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) wordt besteed aan de beveiliging van de Nederlandse reisdocumenten is Collis gevraagd of,Collis sinds de onderzoeken die Collis in 2006 in opdracht van het ministerie van BZK heeft uitgevoerd, nieuwe ontwikkelingen, risico's cq dreigingen onderkent die voor de beveiliging van de chip in de reisdocumenten en/of de daarin opgeslagen gegevens van belang kunnen zijn.

In de eerste plaats wil het ministerie graag weten in welke mate de tests die Collis in 2006 (Ref. [1]) reeds heeft uitgevoerd, nog altijd garanderen dat de authenticiteit en de vertrouwelijkheid van gegevens voldoende is gewaarborgd.

In de tweede plaats is recent door onderzoekers bekend gemaakt dat zij de nationaliteit van een aantal electronische paspoorten konden achterhalen, buiten het Basic Access Control (BAC) mechanisme om, dus zonder dat het nodig is de MRZ (Machine Readable Zone) gegevens van het paspoort zelf te lezen. Het ministerie wil graag weten in hoeverre dit ook voor de ter beschikking gestelde reisdocumenten het geval is.

1.1 Scope van dit Document

Dit document bevat de evaluatie van de tests die Collis al in 2006 heeft uitgevoerd, alsmede analyse van het gedrag van elf ter beschikking gestelde testdocumenten voordat het Basic Access Control mechanisme in werking treedt.

1.2 Doelgroep

Dit document is bedoeld voor het Nederlandse Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

1.3 Referenties

Ref.	Titel	Auteur	Status	Versie	Datum
[1]	Evaluatie van testen op chip in Nederlandse reisdocumenten	Collis (E. Reid en A. Geluk)	Concept	0.94	29-09-2006
[2]	Fingerprinting Passports	Radboud Universiteit (H. Richter, W. Mostowski en E. Poll)	-	-	Maart 2008
[3]	ISO 14443: Identification cards – Contactless integrated circuit(s) cards – Proximity cards	ISO	Final		01-02-2001
[4]	ICAO 9303: Machine Readable Travel Documents – Part 1: Machine Readable Passports, Vol. 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability	ICAO	Draft		20-07-2005

2 EVALUATIE 2006-TESTEN

2.1 Samenvatting van het onderzoek

2.1.1 Uitgevoerde testen en resultaten

In verband met de invoering van het elektronische paspoort en de Nederlandse identiteitskaart (NIK) had het Nederlandse ministerie van BZK Collis gevraagd om verschillende testen uit te voeren op twintig testdocumenten gepersonaliseerd als elektronische paspoorten en op twintig testdocumenten gepersonaliseerd als Nederlandse Identiteitskaarten.

Het doel van de testen was om vast te stellen dat:

1) De testdocumenten zich gedragen conform de ISO en ICAO standaarden.
2) De testdocumenten geen ongespecificeerd gedrag vertonen wat kan worden misbruikt om de authenticiteit en de vertrouwelijkheid van de gegevens op het reisdocument te schaden
3) De door het testdocument gegenereerde “Unique Identifier” (UID) geschikt is voor het gebruik in een elektronisch reisdocument.

Ten overvloede: het vaststellen of het Nederlandse paspoort kan worden onderscheiden van paspoorten met een andere nationaliteit viel destijds niet binnen het bereik van het onderzoek.

De volgende testen werden uitgevoerd op de testdocumenten:

- Testen volgens de ISO test specificatie voor elektronische reisdocumenten.
- Extra testen om gebreken in de dekking van de ISO-testspecificatie aan te vullen
- Extra testen om onbekende of invalide commando’s op te sporen die kunnen worden gebruikt om de beveiliging en de functionaliteit van het elektronische paspoort aan te tasten.
- Een statistische analyse van de willekeurige waarde van de ‘Unique Identifier’ bytes die worden verzonden gedurende het opzetten van de communicatie tussen de reisdocumenten en de reisdocumentlezers.

De 38 testgevallen die door ISO zijn gespecificeerd voor de logische data structuur werden op alle veertig testdocumenten uitgevoerd. Daarbij werden geen problemen gevonden.

Met betrekking tot de 120 door ISO gespecificeerde testgevallen voor veiligheid en commando’s werden twee waarnemingen gerapporteerd. Collis heeft in zijn rapportage aangegeven dat het verwachtte dat het waargenomen gedrag geen impact had op de juiste werking van de elektronische reisdocumenten.

Met betrekking tot de 81 testen die door Collis zijn ontworpen om de ISO testen aan te vullen en om commando’s op te sporen welke niet door de ICAO standaarden zijn gespecificeerd werden zeven waarnemingen gerapporteerd. Collis heeft in zijn rapportage aangeven dat het verwachtte dat het aan deze waarnemingen gerelateerde gedrag geen impact zou hebben op de juiste werking van de elektronische reisdocumenten.

Er werd één waarneming gedaan tijdens de statistische analyse van de “Unique Identifiers” die worden aangemaakt door de testdocumenten.

Collis concludeerde dat de testdocumenten geschikt waren voor gebruik als elektronische reisdocumenten.

2.1.2 Evaluatie

Tijdens het huidige onderzoek hebben we opnieuw gekeken naar de dekkingsgraad van de testen die in 2006 zijn uitgevoerd. Uit deze evaluatie blijkt dat er onder andere volledige scans zijn gedaan op de Instructie, Class, P1 en P2 bytes van een commando (APDU) dat naar een reisdocument kan worden gestuurd. Dit betekent dat alle mogelijke waarden voor deze bytes zijn uitgeprobeerd om te zien wat de reactie van het reisdocument is. In feite zijn daarmee alle mogelijkheden voor een ‘aanval’ op het reisdocument vóór authenticatie (BAC) afgedekt.

Wanneer de kaartlezer zich heeft geauthentiseerd bij het reisdocumentt, zijn er veel meer mogelijke commando’s die naar het reisdocument kunnen worden gestuurd. We constateren dat de overwegingen die toen hebben geleid tot de keuze welke tests uitgevoerd zouden worden en welke niet, nog onverminderd van kracht zijn. Er hebben zich sinds 2006 geen ontwikkelingen voorgedaan die naar de overtuiging van Collis aanleiding zijn tot het doen van aanvullende tests.

Op basis van deze resultaten en overwegingen zijn wij van mening dat de conclusies die Collis destijds getrokken heeft ten aanzien van de veiligheid van de Nederlandse elektronische reisdocumenten nog steeds geldig zijn. De nieuwe ontwikkelingen op chipkaartgebied sinds 2006 brengen in deze conclusie geen verandering.

2.2 Nieuwe ontwikkelingen sinds 2006

Het ministerie van BZK heeft aan Collis gevraagd om haar werk uit 2006 opnieuw te evalueren. Meer specifiek heeft het ministerie van BZK gevraagd of Collis sinds de in 2006 uitgevoerde onderzoeken nieuwe ontwikkelingen, risico’s cq. dreigingen onderkent die voor de beveiliging van de chip in de reisdocumenten en/of daarin opgeslagen gegevens van belang kunnen zijn. Hierbij wordt door Collis bijzonder aandacht geschonken aan mogelijke dreigingen op het gebied van het data-transmissieprotocol (ISO 14443) en ook op het gebied van brute-force attacks en ‘hackers gedrag’. In deze paragraaf vatten we daarom de ontwikkelingen sinds 2006 samen en geven aan welke implicaties die kunnen hebben voor de veiligheid van het Nederlandse elektronische reisdocument.

2.2.1 Beveiliging van de chip

De chip in een Nederlands reisdocument is in feite een mini-computer: hij bevat een processor (CPU), werkgeheugen (RAM) en een harde schijf (EEPROM). De chip in het Nederlandse reisdocument is daarom in staat cryptografische berekeningen uit te voeren, en kan daarmee de data in zijn geheugen beschermen tegen ongeauthoriseerde toegang of afluisteraars.

Voor de elektronische reisdocumenten geldt dat de cryptografische algoritmes die gebruikt worden openbaar zijn. Het grote voordeel hiervan is dat deze algoritmes daarom het voorwerp zijn van voortdurend wetenschappelijk onderzoek naar de betrouwbaarheid ervan. De sleutels die het reisdocument gebruikt in combinatie met deze algoritmes, zijn volgens de huidige wetenschappelijke normen lang genoeg om ervoor te zorgen dat de authenticiteit van de

informatie in het reisdocument voldoende gewaarborgd is. De confidentialiteit van persoonsgegevens die verstuurd worden van chip naar lezer wordt beschermd door het Basic Access Control (BAC) mechanisme. Van BAC is al langer bekend dat het niet bestand is tegen een serieuze cryptografische aanval, hoewel het in de praktijk voldoende bescherming biedt tegen het ongemerkt 'inbreken' in een reisdocument.

De chip in de Nederlandse reisdocumenten beschikt wel over een CPU en RAM, kan daarom zelfstandig cryptografische berekeningen uitvoeren, en maakt daarbij gebruik van publieke, goed onderzochte algoritmes en lange sleutels. Dat maakt het kraken van de chip in de Nederlandse reisdocumenten uitermate lastig.

2.2.2 Achterhalen nationaliteit reisdocumenten zonder authenticatie

In maart 2008 maakten onderzoekers van de Radboud Universiteit in Nijmegen bekend dat zij de nationaliteit van (de houder van) een elektronisch paspoort konden achterhalen zonder daarvoor de inhoud van het paspoort uit te hoeven lezen. Dit betekent dat deze informatie te achterhalen is zonder dat de 'aanvaller' zich geauthenticeerd heeft bij het paspoort.

Collis heeft het rapport van deze onderzoekers gelezen en geprobeerd hun resultaten te reproduceren. Hiervan doen we in paragraaf 3.4.2.7 kort verslag. Onze belangrijkste conclusie is dat hun beweringen hoogstwaarschijnlijk kloppen, maar dat niet alle paspoorten op deze wijze kunnen worden onderscheiden. Zo kan tussen Finse, Ierse, Slowaakse en Nederlandse paspoorten en de NIK op deze wijze geen onderscheid gemaakt worden.

Wij willen benadrukken dat de authenticiteit van de gegevens op het reisdocument op geen enkele manier in het geding is gekomen door deze aanval. Datzelfde geldt ook voor de confidentialiteit van deze gegevens. Bij dit laatste wordt wel aangetekend dat het mogelijk is de fabrikant van het reisdocument te identificeren en zo een indicatie van de nationaliteit van de houder te verkrijgen. Alle overige gegevens op het reisdocument zijn op deze manier niet te achterhalen. De reden hiervoor is dat deze aanval uitsluitend gebaseerd is op het *gedrag* van de diverse reisdocumenten, en niet op de *inhoud* ervan. De nationaliteit van een reisdocument heeft invloed op zijn gedrag, omdat de meeste landen een eigen applicatie hebben ontwikkeld voor hun reisdocumenten. Was dat niet geval geweest, dan had ook de nationaliteit van een reisdocument niet op deze wijze achterhaald kunnen worden.

2.3 Conclusie

Op grond van het bovenstaande concluderen wij dat de resultaten van de tests die Collis in 2006 heeft uitgevoerd nog steeds geldig zijn, en dat de conclusies die wij destijds trokken nog steeds valide zijn.

Verder concluderen we dat het moeilijk voorstelbaar is de chip in de Nederlandse elektronische reisdocumenten zal worden gekraakt. Bovendien stellen wij dat het achterhalen van de fabrikant van een reisdocument op basis van zijn gedrag voor BAC geen gevolgen heeft voor de authenticiteit van de data op een reisdocument of voor de confidentialiteit van de overige data op het reisdocument.

3 TESTEN VOOR DETECTIE VAN NATIONALITEIT

3.1 Introductie

Een eigenschap van het gebruik van contactloze chips is dat het in principe mogelijk is dat onbevoegden met de chip communiceren zonder fysiek over de chip te beschikken en zonder toestemming of medeweten van de eigenaar. Om het uitlezen van persoonsgegevens uit het electronisch reisdocument zonder toestemming van de houder onmogelijk te maken, heeft ICAO een toegangsmechanisme ontworpen. Dit 'Basic Access Control' (BAC) protocol houdt in dat de chip in het reisdocument ter controle vraagt om een aantal gegevens die op de houderpagina van het reisdocument zijn afgedrukt, voordat het zijn persoonsgegevens prijsgeeft.

Recent hebben onderzoekers van de Radboud Universiteit in Nijmegen aangekondigd (Ref. [2]) dat ze, buiten BAC om, door bepaalde berichten naar een paspoort te sturen de nationaliteit van een tiental paspoorten van verschillende nationaliteiten konden achterhalen. Dit leidt tot de algemene vraag in hoeverre reisdocumenten van verschillende nationaliteiten verschillend reageren op berichten die ernaar toe gestuurd worden voordat de kaartlezer zich heeft geauthenticeerd door middel van het BAC mechanisme.

Het ministerie van BZK heeft Collis een aantal reisdocumenten (paspoorten van Finland, Ierland, Nederland en Slowakije en de NIK) ter beschikking gesteld, en gevraagd of deze zich vóór de BAC fase identiek gedragen.

In dit hoofdstuk wordt een aantal tests beschreven die moeten uitwijzen of de reisdocumenten die door het ministerie aan Collis zijn verstrekt voor de BAC fase verschillen in gedrag vertonen.

Dit hoofdstuk is als volgt ingedeeld:

- Paragraaf 3.2 beschrijft de wijze waarop de verschillende tests zijn uitgevoerd.
- Paragraaf 3.3 geeft de resultaten van de tests op het niveau van datatransmissie (Ref. [3]).
- Paragraaf 3.4 geeft de resultaten van de tests op applicatie-niveau (Ref. [4]).
- Paragraaf 3.5 geeft tenslotte de resultaten van een korte hertest van de willekeurigheid van de unieke identificator (UID) waarmee het reisdocument zich aandient bij een lezer. In feite is hier een test uitgevoerd die ook in 2006 al uitgebreid is gedaan, maar ditmaal op de nu beschikbare documenten.

3.2 Testoverzicht

3.2.1 Testomgeving

Om het gedrag van de documenten te testen zijn berichten naar het document gestuurd en zijn de reacties van de diverse documenten vergeleken. Hierbij is gebruik gemaakt van het door Collis ontwikkelde Conclusion® Test Platform. Ter ondersteuning bij het testproces is gebruik gemaakt van en doorgebouwd op de functionaliteit van de door Collis ontwikkelde 'e-Passport

Toolkit'. De gebruikte kaartlezer is van het merk Integrated Engineering, type 'SmartID/CCID 0'.

3.2.2 Testobjecten

De testen zijn uitgevoerd op elf verschillende testdocumenten die zijn gepersonaliseerd als elektronisch paspoort en als elektronische identiteitskaart. De testdocumenten zijn gepersonaliseerd met verschillende data (voor verschillende landen en personen) en verschillen qua type. We onderzoeken of de reisdocumenten verschillend gedrag vertonen wanneer berichten worden verstuurd naar het reisdocument, nog voordat BAC heeft plaatsgevonden. In Tabel 1 geven we een overzicht van de ontvangen testdocumenten en de verder in dit document gebruikte identificaties hiervan.

Ref. ID	Nationaliteit	Type	Jaar v. uitgifte	Documentnummer
FIN_P_642	FIN	elektronisch paspoort	2006	XP9285642
FIN_P_264	FIN	elektronisch paspoort	2008	PP3353264
IRL_P_632	IRL	elektronisch paspoort	2006	XP9996632
IRL_P_763	IRL	elektronisch paspoort	2008	PB0015763
NLD_I_3G7	NLD	elektronische identiteitskaart	2008	XI85003G7
NLD_I_3F4	NLD	elektronische identiteitskaart	2008	XI85003F4
NLD_P_BF0	NLD	elektronisch paspoort	2008	XN5003BF0
NLD_P_BJ2	NLD	elektronisch paspoort	2008	XN5003BJ2
NLD_P_2F4	NLD	elektronische identiteitskaart	2006	XI85902F4
NLD_P_BC3	NLD	elektronisch paspoort	2006	XN5902BC3
SVK_P_000	SVK	elektronisch paspoort	2008	XB0000000

Tabel 1 Identificatie testobjecten

3.3 Resultaten van tests op datatransmissie-niveau

Bij het zoeken naar verschillen in gedrag van de testdocumenten op datatransmissie-niveau is ervoor gekozen om een aantal protocolparameters te controleren: bij het initialiseren van de communicatie tussen reisdocument en lezer worden tussen de chip en de lezer 'protocolparameters' uitgewisseld. Deze parameters schrijven onder andere voor wat de maximale grootte van de berichten mag zijn, en welke velden in de berichten aanwezig mogen zijn.

3.3.1 Protocolparameters

Bij de verstrekte testdocumenten is de werking van de volgende protocolparameters getest:

a. ATS (Answer To Select): deze is voor alle documenten gelijk.
b. FSDI (Frame Size Device Integer): de documenten werken correct met waarden in de range van '0' tot en met '8'. Dit zijn de waarden die in ISO 14443-4 zijn gespecificeerd. De ISO specificaties schrijven geen specifiek gedrag voor bij waarden van '9' tot en met 'F'. Het waargenomen gedrag heeft geen kwetsbaarheden of verschillen tussen de testdocumenten aan het licht gebracht. Het waargenomen gedrag is voor alle documenten gelijk.
c. Het gebruik van de CID (Card Identifier) in de berichten tussen lezer en paspoort: de documenten gedragen zich correct indien een CID wordt gebruikt in de range van '0'

tot en met ‘E’ (14). Met deze waarden voor de CID kan het reisdocument probleemloos communiceren met de reader. De CID waarde ‘F’ wordt niet gebruikt in het ISO 14443 protocol. Deze waarde wordt niet geaccepteerd door de reisdocumenten. Het gedrag dat we hebben waargenomen leidt niet tot kwetsbaarheden of verschillen tussen de testdocumenten. Het waargenomen gedrag is voor alle documenten gelijk.

d. Geen van de documenten ondersteunt het gebruik van een NAD (Node Address). Berichten met een NAD veld worden door de documenten genegeerd. Dit gedrag is correct. Het gedrag dat we hebben waargenomen heeft geen kwetsbaarheden of verschillen tussen de testdocumenten aan het licht gebracht.
e. Frame Size: De grootte van de berichten van lezer naar reisdocument-chip is getest voor waarden tussen 0 en 255 bytes. Hierbij zijn geen kwetsbaarheden of verschillen tussen de testdocumenten aan het licht gekomen. De documenten gedragen zich correct volgens ISO 14443-4. Het waargenomen gedrag is voor alle documenten gelijk.
f. Chaining van berichten: er is getest of de documenten bestand zijn tegen het ontvangen van grote berichten (>10.000 bytes) door deze met behulp van ‘chaining’ als één commando aan te bieden. In veel gevallen bleek het sturen van extra ‘00’ bytes de communicatie niet te verstoren. Bij geen enkele test zijn de documenten onbruikbaar geworden. Kwetsbaarheden of verschillen tussen de testdocumenten zijn niet aan het licht gekomen.

3.3.2 Conclusie

Op basis van de testen op datatransmissie-niveau zijn geen verschillen tussen de geteste reisdocumenten aan het licht gekomen. Ook zijn geen kwetsbaarheden ontdekt.

3.4 Resultaten van tests op applicatie-niveau

Op applicatie-niveau is een aantal tests uitgevoerd met het oogmerk onderscheidend gedrag op te sporen waarmee de nationaliteit van een paspoort zou kunnen worden achterhaald voordat BAC heeft plaatsgevonden. Er is een lijst met mogelijke aandachtspunten opgesteld, waarin we onderscheid maken tussen twee verschillende uitgangssituaties. We beschouwen de situatie nadat de chip in het reisdocument gereset is en de situatie nadat de reisdocument oftewel ICAOapplicatie geselecteerd is. Het gedrag van de chip in deze situaties (eigenlijk: fasen in de communicatie tussen paspoort en lezer) kan verschillen. Deze aandachtspunten staan in tabel 2 opgesomd en worden in deze paragraaf nader uitgewerkt. Bij al deze situaties gaat het erom verschillen te vinden in respons van de testdocumenten, ten einde op basis van deze verschillen een uitspraak te doen over de nationaliteit of het type van het document.

Aandachtspunten per uitgangssituatie	
Direct na document reset / initialisatie (paragraaf 3.4.1)	
	Selecteren van de Master File op diverse manieren
	Selecteren en lezen van een bestand
	Selecteren van een bestand met vaste parameters
	Selecteren van alle ‘bekende’ bestanden met alle mogelijke parameters
	Selecteren van een applicatie
	Opvragen van diverse toevalsgetallen
ICAO-applicatie geselecteerd (paragraaf 3.4.2)	
	Selecteren van de Master File op diverse manieren
	Selecteren en lezen van een bestand

	Selecteren van een bestand met vaste parameters
	Selecteren van alle ‘bekende’ bestanden met alle mogelijke parameters
	Opvragen van diverse toevalsgetallen
	Sturen van incorrecte MRZ data
	Reproduceren van de bevindingen Nijmegen

Tabel 2 Aandachtspunten op applicatieniveau

Uit de tabel volgt de opbouw van deze paragraaf. Paragraaf 3.4.1 bevat de resultaten van de tests die zijn uitgevoerd direct na een reset van de chip in de documenten. Paragraaf 3.4.2 bevat de resultaten van de tests die zijn uitgevoerd nadat de ICAO applicatie is geselecteerd.

3.4.1 Tests uitgevoerd direct na document reset / initialisatie

Onderstaande acties zijn uitgevoerd direct na reset / initialisatie van het document.

3.4.1.1 Selecteren van de Master File op diverse manieren

De specificaties laten ruimte voor meerdere valide manieren om de Master File te selecteren. Per testdocument zijn verschillende manieren toegepast om de Master File te selecteren. Er is nagegaan of de verschillende documenten verschillen in gedrag vertonen. Er zijn geen verschillen gevonden.

3.4.1.2 Selecteren en lezen van een bestand

Alle testdocumenten antwoorden op ieder Select commando met de respons ‘6A 86’ (Security Status Not Satisfied), ongeacht of het bestand bestaat of niet. Als na zo’n Select commando vervolgens geprobeerd wordt het betreffende bestand te lezen met een Read Binary commando, dan reageren de documenten alle met ‘6E 00’ (Class not supported). Op basis van de antwoorden op deze commando’s kan dus geen onderscheid gemaakt worden tussen de elf documenten.

3.4.1.3 Selecteren van een bestand met vaste parameters

Bestanden op een ISO 7816-chip hebben een File ID van twee bytes. We hebben het Select commando met vaste waarden voor de parameters P1 en P2 (‘02 00’ met Le ‘00’ en ‘02 0C’ zonder Le) uitgevoerd voor alle mogelijke File ID’s (dat wil zeggen ‘00 00’ tot en met ‘FF FF’) en de responses van de diverse documenten vergeleken. We hebben geen verschillen gevonden in de responses van de diverse documenten.

3.4.1.4 Selecteren van alle ‘bekende’ bestanden met alle mogelijke parameters

Tijdens een scan hebben we zes File ID’s gevonden die positief reageren *na* authenticatie middels BAC: '01 00', '01 01', '01 02', '01 0F', '01 1D' en '01 1E'. Van deze File ID’s viel op dat ’01 00’ na BAC alleen reageerde bij het Finse paspoort, maar niet bij de andere documenten.

Op basis van deze zes File ID’s zijn er tests uitgevoerd *voor* authenticatie. We hebben het Select commando uitgevoerd voor alle zes File ID’s voor alle mogelijke waarden van P1 en P2 (dat wil zeggen ‘00 00’ tot en met ‘FF FF’). We hebben geen verschillen gevonden in de responses van de diverse documenten. Onafhankelijk van de vraag of een bestand aanwezig is op een document of niet, reageren de documenten altijd met hetzelfde statusword. Dit betekent dus dat de observatie in de eerste alinea in deze sectie geen mogelijkheden biedt om de nationaliteit van een reisdocument voor de BAC-fase te bepalen.

3.4.1.5 Selecteren van een applicatie

Naast de reisdocument applicatie met AID ‘A0 00 00 02 47 10 01’ (deze is door ICAO gespecificeerd) kan op elk van de documenten ook een applicatie met AID ‘A0 00 00 00 03 00 00 00’ worden gevonden. Bij het selecteren van deze applicatie geven de documenten informatie vrij die voldoet aan het formaat van de FCI (File Control Information) zoals gespecificeerd voor Global Platform chips. Deze informatie (de FCI data) is identiek voor alle documenten. Bovendien blijkt de FCI data overeen te komen met de FCI data die de documenten geven bij het selecteren van de Master File (de Master File is door ICAO gedefinieerd als een optioneel element in de reisdocument chip). In een eerder onderzoek zijn reeds testen uitgevoerd op het gedrag van de Nederlandse reisdocumenten bij het selecteren van de Master File. De resultaten van dit onderzoek zijn nog steeds geldig. Het blijkt dat voor alle documenten de default applicatie (de applicatie die actief is voor enig Select commando) gelijk is. Naast deze default applicatie en de ICAO-applicatie zijn er geen andere applicaties aangetroffen. Hierbij dient te worden opgemerkt dat er ook niet uitputtend naar andere applicaties is gezocht, omdat het aantal mogelijke AID’s erg groot is.

3.4.1.6 Opvragen van diverse toevalsgetallen

Er is nagegaan hoe de documenten reageren op het opvragen van toevalsgetallen van alle toegestane lengtes. We hebben dat gedaan door middel van het Get Challenge commando (‘00 84’), met parameters P1 en P2 gelijk aan ‘00’ en Le variabel (‘00 84 00 00 XX’, met XX = ‘00’ t/m ‘FF’) De default-applicatie kent het commando Get Challenge niet en reageert voor alle documenten voor alle toegestane lengtes (0 t/m 255) met de status words ‘6E 00’ (Class not supported).

3.4.2 Tests uitgevoerd nadat ICAO-applicatie is geselecteerd

Onderstaande acties zijn uitgevoerd na het selecteren van de ICAO-applicatie.

3.4.2.1 Selecteren van de Master File op diverse manieren

Er is nagegaan of de verschillende documenten verschillend reageren op een aantal toegestane berichten die de Master File beogen te selecteren. Er zijn geen verschillen aangetroffen.

3.4.2.2 Selecteren en lezen van een bestand

Indien de BAC authenticatie nog niet gedaan is, antwoorden alle testdocumenten op ieder Select commando met de respons ‘69 82’ (Security Status Not Satisfied), ongeacht of het bestand bestaat of niet. Als na zo’n Select commando vervolgens geprobeerd wordt het betreffende bestand te lezen met een Read Binary commando, dan reageren de documenten alle wederom met ‘69 82’. Op basis van de responses op deze berichten kan dus geen onderscheid gemaakt worden tussen de elf documenten.

3.4.2.3 Selecteren van een bestand met vaste parameters

We hebben het Select commando met vaste waarden voor de parameters P1 en P2 (‘02 00’ met Le ‘00’ en ‘02 0C’ zonder Le) uitgevoerd voor alle mogelijke File ID’s (dat wil zeggen ‘00 00’ tot en met ‘FF FF’) en de responses van de diverse documenten vergeleken (ditmaal uiteraard na het selecteren van de ICAO-applicatie). We hebben geen verschillen gevonden in de responses van de diverse documenten.

3.4.2.4 Selecteren van alle 'bekende' bestanden met alle mogelijke parameters

We hebben het Select commando uitgevoerd voor de zes File ID's '01 00', '01 01', '01 02', '01 0F', '01 1D' en '01 1E' voor alle mogelijke waardes van P1 en P2 (dat wil zeggen '00 00' tot en met 'FF FF'). We hebben geen verschillen gevonden in de responses van de diverse documenten.

3.4.2.5 Opvragen van diverse toevalsgetallen

Het Get Challenge commando kan worden gebruikt om een toevalsgetal te vragen aan de paspoortchip. De ICAO-applicatie reageert voor alle documenten voor alle toegestane lengtes (0 t/m 255) hetzelfde op een Get Challenge commando. Ook in de tijdsduur die nodig is om een toevalsgetal op te vragen, zijn geen significante verschillen aangetroffen.

3.4.2.6 Sturen van incorrecte MRZ data

Bij het sturen van onjuiste MRZ data tijdens de BAC authenticatie zijn er geen verschillen gevonden in de responses van de verschillende documenten.

3.4.2.7 Reproduceren van de bevindingen van de Radboud Universiteit

Gebaseerd op de recente publicatie uit Nijmegen (Ref. [2]) hebben we geprobeerd de berichten te achterhalen waar de Nijmeegse onderzoekers hun bevindingen op hebben gebaseerd. Omdat ze

a) expliciet spreken van 'ill-formed requests',
b) zorgvuldig uitleggen hoe een correct gevormde APDU eruit ziet, en
c) niet aangeven welke waarden ze meesturen voor de parameters P1 en P2,

lijkt het aannemelijk dat de onderzoekers uitsluitend een class byte en een instruction byte naar de door hen onderzochte paspoorten hebben gestuurd. Wij hebben eenzelfde test gedaan met de door het ministerie verstrekte documenten, en daaruit blijkt dat de resultaten van de Nijmeegse onderzoekers exact konden worden gereproduceerd voor de Nederlandse reisdocumenten. Tevens bleek dat de andere testdocumenten identiek reageren; er zijn dus geen verschillen gevonden. Onderstaande tabel geeft een overzicht van de responses van de testdocumenten op het commando '00 XX', waarin XX de instructie-byte is.

	Instructie byte						
Document	**44**	**82**	**84**	**88**	**A4**	**B0**	**B1**
FIN_P_642	6D00	6700	6700	6982	6A86	6982	6982
FIN_P_264	6D00	6700	6700	6982	6A86	6982	6982
IRL_P_632	6D00	6700	6700	6982	6A86	6982	6982
IRL_P_763	6D00	6700	6700	6982	6A86	6982	6982
NLD_I_3G7	6D00	6700	6700	6982	6A86	6982	6982
NLD_I_3F4	6D00	6700	6700	6982	6A86	6982	6982
NLD_P_BF0	6D00	6700	6700	6982	6A86	6982	6982
NLD_P_BJ2	6D00	6700	6700	6982	6A86	6982	6982
NLD_I_2F4	6D00	6700	6700	6982	6A86	6982	6982
NLD_P_BC3	6D00	6700	6700	6982	6A86	6982	6982
SVK_P_000	6D00	6700	6700	6982	6A86	6982	6982

Tabel 3 Reacties documenten op verschillende instructie bytes

Uit deze tabel blijkt dat binnen de geteste groep alle documenten op identieke wijze reageren op deze 'commando's'. Binnen deze groep is het dus niet mogelijk de nationaliteit van de documenthouder op deze wijze te achterhalen. Dit laat uiteraard de resultaten van de Radboud Universiteit onverlet, omdat deze andere paspoorten hebben getest.

De Nijmeegse onderzoekers laten doorschemeren dat de door hen geteste paspoorten identiek reageren op andere commando's dan degene die in Tabel 3 zijn genoemd. Er is niet geprobeerd dit te reproduceren.

3.4.3 Conclusie

Op basis van de testen op applicatie-niveau zijn geen verschillen tussen de geteste reisdocumenten aan het licht gekomen vóór authenticatie met BAC. Ook zijn geen kwetsbaarheden ontdekt.

3.5 Resultaten van de willekeurigheidstesten van de UID

3.5.1 Resultaten van het onderzoek in 2006

Tijdens het in 2006 uitgevoerde onderzoek is gebleken dat bij Nederlandse paspoorten en Nederlandse identiteitskaarten niet alle bits van de UID (Unique Identifier) ook werkelijk willekeurig waren. De bits 4 en 8 van het 2^{e} byte van de UID bleken voor elk document een constante, maar niet voor alle documenten identieke, waarde te hebben.

3.5.2 Resultaten van het huidige onderzoek

Deze test is nogmaals uitgevoerd met de elf testdocumenten die aan Collis ter beschikking zijn gesteld.

De testdocumenten kunnen op basis het jaar van uitgifte worden verdeeld in twee groepen, namelijk de documenten die zijn uitgegeven in 2006 en die welke zijn uitgegeven in 2008.

De documenten die in 2006 zijn uitgegeven vertonen het in 2006 gevonden gedrag: bits 4 en 8 van het 2^{e} byte uit de UID zijn constant. Bij de documenten die in 2008 zijn uitgegeven zijn alle bits in de UID variabel.

De toevalswaarde die de UID bevat is niet verder onderzocht om na te gaan of dit werkelijk een 'true random' is. De UIDs zijn voldoende willekeurig voor gebruik in het ISO 14443 protocol.

3.5.3 Conclusie

Op grond van het waargenomen gedrag van de elf testdocumenten kan afgeleid worden of het document van generatie 2006 of van generatie 2008 is.

4 CONCLUSIES

Collis is gevraagd of de paspoorten van Finland, Ierland, Nederland en Slowakije en de Nederlandse Identititeitskaart (NIK) zich identiek gedragen voorafgaand aan de Basic Access Control (BAC) fase. Van alle nationaliteiten zijn testdocumenten ter beschikking gesteld uit 2006 én 2008, met uitzondering van Slowakije: het Slowaakse paspoort is uitgegeven in 2008. In de communicatie voor BAC is slechts één verschil aangetroffen tussen de onderzochte reisdocumenten: de oudere documenten (met uitgiftedatum in 2006) verzenden tijdens de uitvoering van het ISO 14443 protocol een zogeheten UID waarin een tweetal bits een vaste waarde heeft. De overige documenten zijn uitgegeven in 2008 en verzenden UIDs waarin alle bits willekeurig zijn. Documenten uit 2006 zijn dus (binnen de groep van elf geteste documenten) voor BAC te onderscheiden van documenten uit 2008. Het is niet mogelijk om Finse, Ierse en Nederlandse documenten uit 2006 voor BAC van elkaar te onderscheiden. Ierse, Finse, Nederlandse en Slowaakse documenten uit 2008 laten voor BAC eenzelfde gedrag zien. Er vallen uiteraard geen conclusies te trekken ten aanzien van de onderscheidbaarheid van de geteste reisdocumenten met reisdocumenten buiten de onderzochte groep.

Collis is verder gevraagd of het sinds de in 2006 uitgevoerde onderzoeken nieuwe ontwikkelingen onderkent die voor de beveiliging van de chip in de Nederlandse reisdocumenten van belang kunnen zijn. Collis concludeert dat de vertrouwelijkheid en authentictiteit van de gegevens in de chip in de Nederlandse reisdocumenten voldoende beschermd is. Bovendien concludeert Collis dat de chip in de Nederlandse reisdocumenten zich gedraagt conform de van toepassing zijnde ISO en ICAO standaarden. Collis acht het Nederlandse paspoort en NIK geschikt voor gebruik als elektronisch reisdocument.