Evaluatie van de chip in reisdocumenten

Wojciech Mostowski, Ruben Muijers, Erik Poll en Roel Verdult
Sectie Digital Security
Radboud Universiteit Nijmegen

1 juli 2008

1 Samenvatting

Dit document is de rapportage over het testen van de chip in Nederlandse reisdocumenten, uitgevoerd in mei en juni 2008 in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

Zoals gevraagd is onderzocht of paspoorten van Nederland, Finland, Ierland en Slowakije, en de Nederlandse identiteitskaart (NIK) zich vóór de BAC-fase identiek gedragen. In kader hiervan is ook beoordeeld of de conclusies uit het rapport van Sdu Identification ('Sdu reactie op artikel fingerprinting Passports', v1.1, 9 april 2008) juist zijn.

Daarnaast is gekeken in hoeverre de resultaten en conclusies uit ons in 2006 verrichte onderzoek in opdracht van BZK nog geldig zijn, gezien de huidige kennis en de huidige stand van de techniek.

De volgende types documenten zijn getest: Nederlandse paspoorten en NIKs uit 2006 en 2008, Ierse paspoorten uit 2006 en 2008, Finse paspoorten uit 2006 en 2008 en een Slowaaks paspoort uit 2008.

Onze conclusies zijn:

- Alle reisdocumenten uit 2008 (Nederlandse, Ierse, Finse en Slowaakse) gedragen zich vóór de BAC-fase identiek.
- Alle reisdocumenten uit 2006 (Nederlandse, Ierse, en Finse) gedragen zich vóór de BAC-fase identiek.
- Er is te bepalen van welke generatie (2006 of 2008) een Nederlands, Iers, Fins of Slowaaks reisdocument behoort. Documenten van dezelfde generatie zijn niet te onderscheiden vóór de BAC-fase.
- De conclusies in het rapport van Sdu Identification ('Sdu reactie op artikel fingerprinting Passports', v1.1, 9 april 2008) zijn naar ons inzicht allemaal volledig correct.
- Er zijn verder geen fouten gevonden op het gebied van conformance, security, of privacy. De resultaten van ons onderzoek dat in 2006 in opdracht van het ministerie van BZK is uitgevoerd zijn dus nog steeds geldig.

2 Introductie

Dit document is de rapportage over het testen van de chip in Nederlandse reisdocumenten, uitgevoerd in mei en juni 2008 in opdracht van BZK.

Zoals gevraagd is onderzocht of paspoorten van Nederland, Finland, Ierland en Slowakije en de Nederlandse identiteitskaart (NIK) zich vóór de BAC-fase indentiek gedragen, ook op de lagere protocolniveaus van ISO14443. In kader hiervan is ook beoordeeld of de conclusies uit het rapport van Sdu Identification [6] juist zijn. Daarnaast is gekeken in hoeverre de resultaten en conclusies uit ons in 2006 verrichte onderzoek in opdracht van BZK (gerapporteerd in [2]) nog geldig zijn gezien de huidige kennis en de huidige stand van de techniek.

Er zijn verschillende niveaus waarop mogelijke verschillen in gedrag waar te nemen zijn: op het fysieke niveau, op niveau van het ISO14443 protocol voor draadloze chipkaarten of op niveau van het ISO7816 protocol voor chipkaarten. In Sectie 5 wordt een overzicht gegeven van de karakteristieken waarop documenten mogelijk te onderscheiden zouden zijn vóór de BAC-fase. In secties 6 t/m 12 wordt het onderzoek naar deze afzonderlijke karakteristieken beschreven. Sectie 13 re-evalueert de resultaten van ons onderzoek uit 2006, en Sectie 14 verzamelt alle conclusies.

Eerst wordt in Sectie 3 een opsomming gegeven van de reisdocumenten die getest zijn, en in Sectie 4 van de hardware die hierbij gebruikt is.

3 Geteste reisdocumenten

Voor de test kregen we de beschikking over specimina van

- het Ierse paspoort, generatie 2006 en 2008;
- het Finse paspoort, generatie 2006 en 2008;
- het Slowaakse paspoort, generatie 2008;
- het Nederlands paspoort en de NIK, generaties 2006 en 2008.

4 Gebruikte hardware

Voor de tests is gebruik gemaakt van de volgende hardware:

- standaard kaarlezers voor ISO14443, om precies te zijn een ACR122 van Advanced Card Systems (http://www.acs.com.hk/acr122.php) en een SDI 010 USB van SCM Microsystems (http://www.scmmicro.com/security/view_product_en.php?PID=19).
- een Proxmark test-instrument (http://www.proxmark.org) voor de analyse van ISO14443 gedrag op laag niveau.

5 Mogelijke karakteristieken vóór de BAC-fase

Het mechanisme van Basic Acces Control (BAC) is geïntroduceerd om de persoonsgegevens op de chip te beschermen tegen ongemerkt uitlezen: de persoonlijke gegevens die zijn opgeslagen op de chip worden enkel verstrekt aan een partij die aantoont de informatie in de Machine-Readable Zone (MRZ) gelezen te hebben.

Dit sluit niet uit dat er vóór de BAC-fase nog gedrag geobserveerd kan worden dat (i) uniek is voor één enkel reisdocument of (ii) karakteristiek is voor een bepaalde klasse reisdocumenten, bijvoorbeeld alle paspoorten van een bepaald land. Gedrag dat deze observaties mogelijk zou maken is duidelijk ongewenst voor reisdocumenten.

Er zijn verschillende niveaus waarop karakteristiek gedrag van een reisdocument of klasse van reisdocumenten herkend zou kunnen worden. Dit zou kunnen op basis van gedrag van de MRTD-applicatie zelf (d.w.z. de software op de chip in het reisdocument dat de functionaliteit zoals

gespecificeerd door ICAO implementeert), maar ook op basis van het gedrag van eventuele andere applicaties op de chip, het gedrag van het onderliggende operating system, of het gedrag van de daaronderliggende hardware. Wat andere applicaties betreft: omdat de chips in de Nederlandse reisdocumenten het Java Card platform gebruiken, is er naast de MRTD-applicatie in elk geval nog Global Platform-functionaliteit die geobserveerd kan worden. Voor communicatie met de chip in het reisdocument zijn twee protocollen van belang, namelijk het ISO7816 protocol, dat het standaard protocol is voor communicatie met chipkaarten, en het ISO14443 protocol, dat specifiek is voor de draadloze communicatie. Uit eerder, onafhankelijk onderzoek door onze groep was al gebleken dat paspoorten van sommige landen te onderscheiden zijn op basis van het gedrag van de MRTD-applicatie [8].

In dit onderzoek is gekeken naar de volgende mogelijkheden om de chips in de documenten te onderscheiden:

1. timing, d.w.z. de snelheid waarmee de chip in een reisdocument reageert;
2. het effect op het elektromagnetische veld van de lezer, oftewel hoeveel energie de chip in het reisdocument verbruikt;
3. de UIDs die de chip uitzendt in het anti-collision protocol als onderdeel van ISO14443;
4. de ATS (Answer To Reset), die de chip uitzendt als onderdeel van het ISO14443 protocol;
5. de reactie op niet-standaard ISO14443 sessies;
6. de BAC challenges die de MRTD-applicatie genereert als onderdeel van het ICAO protocol, en die ook willekeurig moeten zijn;
7. op APDU niveau volgens ISO7816, waar niet alleen gekeken is naar de reactie op reguliere ICAO instructies en Global Platform-instructies, maar naar de reactie op alle instructies waarop enige response te detecteren viel.

Deze onderzoeken worden in detail beschreven in de secties 6 t/m 12.

6 Timing Analyse

Doel van deze test was te ontdekken of er vóór de BAC-fase verschillen waren te ontdekken in het timing gedrag van de verschillende reisdocumenten.

Testopstelling

De Proxmark-antenne wordt tussen het reisdocument en de ACR-lezer geplaatst, en de lezer begint een standaard ISO14443 sessie. De Proxmark luistert alle communicatie af tussen lezer en chip en registreert ook timing-gegevens m.b.v. de `hi14asnoop` sniffing utility.

Resultaten

Bij deze test konden we geen verschillen detecteren in de reactiesnelheid van de chips in de verschillende documenten: de reactietijden van alle chips zijn identiek. Appendix A geeft enkele voorbeelden van traces incl. timing.

7 Analyse van de veldsterkte

Doel van deze test was om te ontdekken of er verschillen waren in de energieconsumptie van de chips, hetgeen waar te nemen is aan de sterkte van het veld dat de lezer genereert om de chips te activeren en ermee te communiceren. We hebben *niet* gekeken naar power consumption traces van prototocol sessies, d.w.z. naar variaties in de energieconsumptie in tijd, zoals bij zogenaamde SPA of DPA analyse gebeurt.

Testopstelling

De Proxmark wordt op de tafel geplaatst uit de buurt van mogelijke bronnen van elektromagnetische straling. De reisdocumenten worden in identieke positie op de Proxmark gelegd en met behulp van de Proxmark client utility wordt de invloed op het electromagnetische veld gemeten.

Resultaten

Bij alle paspoorten werd een waarde van 9.000 mV waargenomen; bij de NIK werd een waarde van 6000 mV waargenomen.

Dit betekent dus dat voor de activering van het paspoort een sterker veld nodig is dan voor de NIK. De voor de hand liggende verklaring is dat de verpakking van de chip in de paspoorten anders is dan in de NIK.

Uit onze ervaring met andere RFID-tags is een waarde in de range van 4.000 tot 7.000 mV normaal. In dit opzicht is het paspoort dus atypisch. Merk echter op dat de vereiste sterkte van het veld om een reisdocument te activeren sterk zal variëren, afhankelijk van de afstand tot de lezer en van de aanwezigheid van materialen tussen de chip en de lezer die de ontvangst bemoeilijken. Dit biedt dus geenszins een bruikbare manier om reisdocumenten op afstand te herkennen, laat staan van elkaar te onderscheiden.

Er is weliswaar niet geprobeerd om power consumption traces van verschillende reisdocumenten te vergelijken, maar het lijkt ons zeer onwaarschijnlijk dat hierbij verschillen te detecteren zouden zijn, aangezien alle andere experimenten erop wijzen dat er identieke software op identieke hardware wordt uitgevoerd, wat dus ook identieke power consumption traces zou produceren. Daarnaast zullen goede power consumption traces op afstand zeer lastig te verkrijgen zijn, door de eerdergenoemde factoren die de veldsterkte beinvloeden, dus dit lijkt geen bruikbare manier om reisdocumenten op afstand te herkennen, laat staan van elkaar te onderscheiden.

8 Mifare-emulatie

In deze test hebben we onderzocht of reisdocumenten Mifare ondersteunen, een RFID variant die nauw verwant is aan ISO14443. Het is natuurlijk *niet* de bedoeling dat de chips in reisdocumenten een dergelijke functionaliteit bieden. In het slechtste geval zou deze functionaliteit gebruikt kunnen worden om unieke kenmerken aan een reisdocument toe te voegen.

Testopstelling

Met een standaard kaartlezer (ACR122) beginnen we een Mifare Classic protocolsessie met de chip in het reisdocument, waarbij de Proxmark gebruikt wordt om gedetailleerde informatie over de reactie vast te leggen.

Resultaten

Geen van de reisdocumenten reageerden op het Mifare protocol. Er is dus geen sprake van ondersteuning van dit protocol door de gebruikte chips.

9 UIDs

Als onderdeel van de eerste fase van het ISO 14443 protocol, de zgn. anti-collision fase, stuurt de chip een UID van 4 bytes naar de lezer. Het ISO14443 protocol laat de mogelijkheid open of een chip altijd een vaste UID stuurt of een willekeurige (random) UID. Random UIDs beginnen met 08 als eerste byte, gevolgd door 3 bytes met willekeurige waarden. Om het herkennen van een uniek reisdocument onmogelijk te maken, dienen de chips in de Nederlandse reisdocumenten een willekeurige UID te versturen.

Resultaten

In de rapportage over ons eerdere onderzoek in 2006 hadden we al opgemerkt dat in de toenmalige testexemplaren van Nederlandse reisdocumenten de random number generator voor verbetering vatbaar was, omdat 2 van de 24 bits in de random UIDs een vaste waarde hadden. We observeerden dit gedrag opnieuw bij alle reisdocumenten uit 2006, d.w.z. voor het Nederlandse paspoort en de NIK uit 2006, en voor het Finse en het Ierse paspoort uit 2006. Voor al deze documenten hadden de 1ste en het 5de bit van de eerste random byte in de UID altijd een vaste waarde. Welke waarden dit zijn verschilt per reisdocument, en hieraan is dus niet te zien welke nationaliteit een reisdocument heeft.

Bij de reisdocumenten uit 2008 treedt dit fenomeen niet op. We hebben enkele verzamelingen van opeenvolgende UIDs die een document verstuurde geanalyseerd maar konden hier geen eigenaardigheden in herkennen: de verzamelingen lijken echt random. In testsets van 2000 tot 3000 samples waren individuele bits ongeveer even vaak 0 als 1: tussen de 49 en 51%, om precies te zijn. De verdeling van de UIDs was zoals te verwachten vrij uniform, ook als we elk van de drie bytes afzonderlijk beschouwen. De aantallen collisions waren zoals verwacht, nl. nul. Ter illustratie geeft Appendix B een voorbeeld van een waargenomen verdeling.

Op basis van dit gedrag is het dus mogelijk om reisdocumenten van de 2006 generatie te onderscheiden van de 2008 generatie.

We hadden binnen dit project geen tijd om erg uitgebreide tests op de willekeurigheid van de UIDs uit te voeren. Het zou wellicht nuttig zijn om voor de zekerheid standaardtests op randomness, zoals gedefiniëerd in NIST FIPS 140, op de UIDs uit te voeren.

10 BAC challenges

Na de anti-collision fase van ISO14443 produceert de chip in het reisdocument desgevraagd een random challenge, als de eerste stap van het BAC-protocol. Dit random getal is 8 bytes lang.

In de series willekeurige waarden die een reisdocument als BAC-challenge produceert konden we geen patronen of eigenaardigheden ontdekken: de series lijken echt random. In grote sample sets (meer dan 2 millioen random challenges) kwamen de bits 0 en 1 met een frequentie van 50.0 % voor, en was de distributie van challenges zoals verwacht, vrij vlak. Ter illustratie geeft Appendix C een voorbeeld van een waargenomen verdeling.

Bij het testen van de BAC challenges en de UIDs hebben we ook geëxperimenteerd met misvormde boodschappen van de lezer naar de chip, namelijk misvormde APDU's (die zich niet aan correcte 'format' voor APDU's houden) en misvormde boodschappen als onderdeel van het anti-collision protocol. Hierop kregen we geen interessante reacties: de chips stopten de communicatie.

11 APDU vingerafdruk

Op ISO7816-niveau communiceren de chip en de lezer met series bytes, oftewel APDU's (Application Protocol Data Units). Op elk bericht van de lezer naar de chip, met een zogenaamde command APDU, antwoordt de chip met een zogenaamde response APDU. Er is een zeer grote verzameling van mogelijke commando's, en voor elk ervan kan de applicatie op de chip kiezen uit een grote verzameling van mogelijke antwoorden. Het algemene idee is om de antwoorden (response APDU's) van de chip in het reisdocument op een grote collectie verschillende commando's (command APDU's) vast te leggen, een zogenaamde APDU vingerafdruk, om hierin mogelijke verschillen te ontdekken.

Uit eerder onderzoek [8] bleek reeds dat het mogelijk is op basis van APDU vingerafdrukken om paspoorten van sommige landen te onderscheiden, maar hierbij waren destijds geen Ierse, Slowaakse of Finse paspoorten bekeken.

11.1 Testmethode

In het eerdere onderzoek [8] konden we op een ad-hoc manier vrij eenvoudig verschillen tussen de APDU vingerafdrukken van reisdocumenten uit de verschillende landen ontdekken. Voor de reisdocumenten in de huidige test was het niet mogelijk om op zo'n manier verschillen te vinden; dit was ook te verwachten, aangezien alle reisdocumenten van dezelfde leverancier komen en de software op de chips naar verwachting vrijwel of helemaal identiek is.

Het testen van *alle* mogelijke commando's is niet mogelijk, omdat het aantal mogelijkheden hiervoor veel te groot is. Command ADPU's zijn minstens 4 bytes lang, en enkel deze eerste 4 bytes geven al meer dan 4 miljard combinaties. Testen van alle mogelijke APDUs zou jaren duren. We hebben daarom een teststrategie ontwikkeld om zeer grondig op zoek te gaan naar mogelijke verschillen. Het idee is dat we een 'interessante' verzameling APDU's bepalen om te testen, uitgaande van aannames over de gebruikelijke, systematische manier waarop smartcardapplicaties APDUs verwerken.

Motivatie van de testprocedure

Een command ADPU bestaat uit tenminste 4 bytes, waaronder de volgende velden:

- CLAss byte,
- INStruction byte,
- P1 en P2 parameter bytes,
- een optioneel data veld, bestaande uit 1 byte met de lengte (LC) gevolgd door LC bytes data,
- optioneel een byte met de verwachte lengte van het antwoord, LE.

In een normale smartcard-applicatie wordt gevalsonderscheid gedaan naar de individuele bytes van de command APDU, in eerste instantie de CLA en INS bytes (waarbij meestal eerst naar CLA gekeken wordt en vervolgens naar INS). Als een applicatie antwoordt dat een bepaalde waarde van CLA niet acceptabel is, zullen de waarden van andere bytes (INS, P1, P2, etc.) daar waarschijnlijk geen invloed op hebben. Op basis hiervan is te verwachten dat niet alle combinaties van bytes nodig zijn om al het gedrag van een applicatie te bepalen.

In bepaalde situaties kunnen afhankelijkheden tussen verschillende bytes van belang zijn. Bijvoorbeeld bij zogenaamde chaining commands kan er gedrag zijn dat enkel optreedt bij een bepaalde combinatie van CLA en INS bytes. Het ontdekken van dit gedrag zou een uitputtende test van alle combinaties vereisen. Maar gelukkig is het niet te verwachten dat zoiets zich vóór de BAC-fase voordoet.

Het is ook niet te verwachten dat vóór de BAC-fase de inhoud van het APDU-dataveld invloed zal hebben op het gedrag: het reisdocument verwacht in deze fase geen data, en het zou daarom hoogstmerkwaardig zijn als een MRTD-applicatie vóór de BAC fase ook maar naar de inhoud van dat veld zou kijken. Als mogelijke inhoud van het dataveld hebben we daarom gewoon een rij nullen uitgeprobeerd. De enige uitzondering hierop is de Select Application' APDU, die de applicatie wel kan verwachten vóór de BAC-fase. Voor dit geval hebben we een aparte testprocedure gemaakt (zie 11.3).

Tot slot, in onze eerdere ervaring met reisdocumenten van allerlei nationaliteiten reageren reisdocumenten heel verschillend op het wel of niet aanwezig zijn van een LE byte. In onze testverzameling hebben we daarom zowel een nul als niet-nul waarde voor LE meegenomen (LE=0 betekent dat er geen LE wordt verstuurd). Voor alle zekerheid hebben we dit ook met de LC byte gedaan.

11.2 Testomgeving

De applicatie voor het uitvoeren van deze test is geschreven in Java, gebruik makend van de SmartcardIO bibliotheek van de Java Development Kit 1.6. Voor het testen is gebruik gemaakt van een SCM SDI 010 USB lezer.

11.3 De APDU testprocedure

Gebaseerd op de bovengenoemde aannames en onze ervaring over hoe de code van een smartcard-applicatie er meestal uitziet, zijn we met de onderstaande testprocedure gekomen. In de eerste stappen van de procedure worden 'interessante' waarden voor de CLA, INS, P1, P2, LC en LE bytes verzameld – d.w.z. waarden die voorkomen als onderdeel van APDU's die resulteren in verschillende response APDU's – en in de laatse stap worden alle combinaties van deze waarden uitgeprobeerd. In meer detail, is de procedure als volgt:

1. De MRTD-applicatie wordt geselecteerd met een 'Select Application' APDU.
2. We proberen een verzameling APDU's uit door combinaties van
   - alle mogelijke waarden voor CLA (0–255), met
   - een interessante verzameling waarden voor de INS, waaronder alle instructies die een MRTD-applicatie volgens de ICAO standaard moet kennen: {`A4`, `B0`, `B1`, `82`, `84`, `88`, `44`} [4, 5, 7]
   - P1=0, P2=0, en LC en LE allebei variërend over de verzameling $\{0, 1\}$.

   Voor deze verzameling APDU's bepalen we de verzameling status words die de chip produceert als antwoord. Voor elk van deze status words kiezen we een waarde van CLA die het status word kon veroorzaken.
3. Vervolgens nemen we CLA=0 (de CLA waarde voor de MRTD-applicatie) en proberen we alle mogelijke waarden voor INS uit, waarbij we P1, P2, LC en LE allemaal 0 nemen.

   Als het antwoord niet 'INStruction Not Supported' is, doen we voor deze waarde van INS:

   (a) een volledige iteratie over alle waarden van P1 en P2, in combinatie met LC en LE uit {0,1}.
   Alle verschillende status words die dit oplevert worden verzameld en voor elke waarde wordt een waarde van P1/P2 gekozen die dit status word kan veroorzaken.

   (b) een volledige iteratie over LC en LE, in combinatie met P1 en P2 steeds 0.
   Alle verschillende status words die dit oplevert worden verzameld en voor elke waarde wordt een waarde van LC/LE gekozen die dit status word kan veroorzaken.
4. Tot slot worden alle combinaties van de verzamelde waardes van CLA, P1/P2, en LC/LE uitgeprobeerd als command APDU's. In een log file worden al deze command APDU's en de b.b.h. responses opgeslagen.

Het is eenvoudig na te gaan of de geproduceerde log files identiek zijn voor verschillende reisdocumenten. In de laatste stap, stap 4, werden ongeveer 65 duizend combinaties geprobeerd.

Speciale gevallen

Een paar speciale gevallen worden bij de tests overgeslagen:

- De INStruction byte `70` wordt overgeslagen, omdat de gebruikte SmartcardIO library (onderdeel van Java 1.6) APDU's met INS=70 weigert.

- De instructie 'Get Challenge' command (INS=84) wordt overgeslagen. Dit is een toegestane instructie - het is de eerste instructie van een normale BAC-sessie - maar omdat deze een random getal als antwoord oplevert verschilt het antwoord hierop steeds. Deze instructie is apart getest (zie Sectie 10).
- De 'Select Application' APDU wordt overgeslagen, omdat dit resultaten van volgende APDU's beinvloed. Daarom wordt een aparte test voor Application Selection gedaan, zoals hieronder beschreven.

Additionele Tests

ATR/ATS Voor elk reisdocument word de ATR/ATS (Answer To Reset/Answer To Select) bytes opgeslagen ter vergelijking.

Application Selection De 'Select Application' instructie vereist speciale aandacht:

- Deze instructie kan voorkomen zelfs vóór de reisdocument applicatie op de chip actief (d.w.z. geselecteerd) wordt. Hierdoor kan de instructie gebruikt worden om verschillen in het onderliggende platform (bijv. Java Card/Global Platform) te ontdekken.
- Deze instructie kan gebruikt worden om de 'default selectable application' op de chip te bepalen. Op de geteste chips is dit *niet* de MRTD-applicatie, maar het Global Platform Security Domain.
- Met een goede keuze voor de LE byte in een 'Select Application' instructie is het mogelijk de FCI (File Control Information) gegevens voor een applicatie op te vragen. Verschillen in deze FCI data zouden het onderscheiden van reisdocumenten mogelijk maken.

Daarom is een speciale testprocedure voor de 'Select Application' instructie toegevoegd. Eerst wordt geprobeerd de default application te selecteren (door geen AID op te geven) met alle mogelijke waardes van LE. Daarna wordt de MRTD-applicatie geselecteerd, eveneens met alle mogelijke waardes van LE in een poging de reisdocument FCI te verkrijgen.

Al deze command APDU's en bijbehorende response APDU's worden gelogd om vergelijking van reisdocumenten mogelijk te maken.

11.4 Testresultaten

Het draaien van deze APDU test duurt iets minder dan 6 uur. Bij de test worden in de orde van anderhalf millioen APDU's verstuurd.

In de tests gedroegen alle reisdocumenten zich hetzelfde: de geproduceerde log files zijn identiek. Er zijn hierbij dus geen mogelijkheden gevonden om de documenten te onderscheiden door verschillen in antwoorden op APDU commando's vóór de BAC-fase.

12 De Global Platform test

In ons eerdere onderzoek van Nederlandse reisdocumenten in 2006 hadden we het gedrag van de Global Plaform Security Domain al getest. Omdat het Nederlandse paspoort en NIK op een Java Card smartcard geïmplementeerd zijn is er een Global Platform Security Domain dat geselecteerd kan worden. De test in 2006 was er vooral op gericht om te zien of toegang tot het Security Domain goed geblokkeerd was, d.w.z. alle pogingen om een Global Plaform operatie uit te voeren moeten geweigerd worden met het status word 'Conditions Not Satisfied' (`6985`) als antwoord.

We hebben deze test nu herhaald op alle documenten, om mogelijke verschillen in de implementatie van het Global Platform Security Domain te detecteren.

12.1 Testresultaten

Het uitvoeren van deze test van de Global Platform-functionaliteit duurt in de orde van 11 uur. Bij de test worden ruim 3 millioen APDU's verstuurd.

Alle reisdocumenten gedragen zich identiek bij het testen van de Global Platform functionaliteit. Er waren geen verschillen waar te nemen en er is geen functionaliteit van het Global Platform Security Domain die nog gebruikt kan worden.

In tegenstelling tot de ICAO specificaties is de Global Plaform documentatie [3] zeer precies over welke status words er als foutmelding geantwoord moeten worden onder welke omstandigheden. Het is daardoor minder waarschijnlijk dat er verschillen tussen verschillende implementaties van Global Plaform te ontdekken dan tussen verschillende implementaties van de ICAO standaard voor de MRTD-applicatie.

13 Re-evaluatie van ons onderzoek in 2006

In ons onderzoek in opdracht van BZK in 2006 was gekeken naar potentiële zwakheden vanuit oogpunt van conformance, security en privacy:

- *Conformance.* De chip in het reisdocument moet zich conform de specificaties van ICAO gedragen.
- *Security.* De chip moet afdoende beveiligd zijn:
  - Het BAC mechanisme moet correct geïmplementeerd zijn, d.w.z. de inhoud van de datagroepen moet geheim blijven (totdat BAC succesvol is uitgevoerd), en zelfs nadat BAC succesvol is uitgevoerd door een partij die vertrouwd wordt door de kaarthouder, dan mogen andere partijen nog steeds niet de inhoud van de datagroepen achterhalen.
  - De confidentialiteit van de cryptografische sleutels op de chip moet gewaarborgd zijn, d.w.z. de BAC sleutels zelf moeten geheim blijven (totdat BAC succesvol is uitgevoerd) en de AA privé sleutel moet geheim blijven.
  - De confidentialiteit en integriteit van de bytecode van de applet moeten gegarandeerd zijn.
  - De integriteit van de persoonsgegevens (datagroepen) moet gegarandeerd zijn, d.w.z. de persoonsgegevens mogen niet te veranderen zijn.
  - De chip kan niet geblokkeerd kan worden waardoor hij niet meer functioneert.
- *Privacy.* Het moet onmogelijk zijn een elektronisch reisdocument uniek te identiceren zonder het uitvoeren van BAC.

Als onderdeel van dit onderzoek was een reference implementatie van de MRTD-applicatie gemaakt en waren specimina van Nederlandse reisdocumenten getest, zowel op een ad-hoc manier als modelgebaseerd. Er was hierbij gekeken naar drie aspecten: de anti-collision fase van ISO14443, het Global Platform gedrag en het gedrag van de MRTD-applicatie zelf.

In het kader van het huidige onderzoek zijn deze drie aspecten opnieuw getest. Het gedrag van de MRTD-applicatie is hierbij nu uitgebreider getest voor zover het gedrag vóór de BAC-fase betrof (zie Sectie 11). Het gedrag van de MRTD-applicatie na de BAC-fase is niet opnieuw getest, omdat dit voor de huidige onderzoeksvraag (onderscheidbaarheid vóór de BAC-fase) niet relevant was, en omdat naar ons inzicht het gedrag van de MRTD-applicatie na de BAC-fase niet onderheving is aan nieuwe dreigingen sinds 2006.

Er waren in ons onderzoek in 2006 geen fouten gevonden op gebied van conformance, security of privacy. Wel werd de onvolkomenheid in de random number generation voor UIDs in de toenmalige generatie van reisdocumenten gevonden; deze is reeds besproken in Sectie 9, en is nu dus verbeterd in de 2008 generatie reisdocumenten.

In de conclusie van het rapport over het onderzoek in 2006 [2] werden een paar punten genoemd die nog vragen opriepen. Het betrof hier scenario's waar de ICAO standaarden enigszins ondergespecificeerd waren. Er is inmiddels duidelijk geworden [8] dat ten gevolge van de niet eenduidigheid van de ICAO standaarden variaties kunnen ontstaan in het gedrag van verschillende MRTD-applicaties waardoor chips in reisdocumenten van verschillende fabrikanten mogelijk te onderscheiden zijn. De vragen voor verder onderzoek die in [2] werden genoemd zijn hiermee beantwoord.

Het bovenstaande in acht genomen zijn onze conclusies uit 2006 volgens ons nog steeds geldig. Er zijn sinds 2006 geen nieuwe ontwikkelingen, risico's of bedreigingen geweest die voor de beveiliging van de chip in reisdocumenten van belang zijn.

In ons onderzoek hebben wij niet gekeken naar zogenaamde (semi)invasive aanvallen. In onze optiek vormt de voortschrijdende techniek voor (semi)invasive aanvallen echter geen echte bedreiging voor reisdocumenten; de gegevens die hiermee achterhaald zouden kunnen worden (de geheime sleutel voor het Actieve Authenticatie mechanisme van een enkel paspoort) staan in geen enkele verhouding tot de kosten.

14 Conclusies

Uit onze tests concluderen we het volgende:

- Alle reisdocumenten uit 2008 (Nederlandse paspoort en NIK, Ierse paspoort, Finse paspoort en Slowaakse paspoort) gedragen zich vóór de BAC-fase identiek.
- Alle reisdocumenten uit 2006 (Nederlandse paspoort en NIK, Ierse paspoort en Finse paspoort) gedragen zich vóór de BAC-fase identiek.
- Er is te bepalen tot welke generatie (2006 of 2008) een Nederlands, Iers, Fins of Slowaaks reisdocument behoort; reisdocumenten uit 2006 zijn te onderscheiden van de reisdocumenten uit 2008, aan de verdeling van de UIDs (zie Sectie 9), maar hierin is geen onderscheid naar nationaliteit mogelijk. Documenten van dezelfde generatie zijn niet van elkaar te onderscheiden vóór de BAC-fase.

De conclusies in het rapport van Sdu Identification [6] zijn naar ons inzicht allemaal volledig correct.

We concluderen verder dat de resultaten van ons onderzoek in 2006 in opdracht van het ministerie van BZK nog steeds geldig zijn. Er zijn geen fouten gevonden op het gebied van conformance, security of privacy. In Sectie 13 wordt uitgelegd wat er onder conformance, security en privacy wordt verstaan. Wel is het mogelijk paspoorten van verschillende fabrikanten te onderscheiden, zoals reeds gemeld in [8] en bevestigd in het rapport van Sdu Identification [6], door verschillen in het platfrom (chip en operating system) en verschillen in de software (de MRTD-applicatie). De vragen voor eventueel nader onderzoek die in de conclusies van het rapport [2] werden gesignaleerd zijn inmiddels beantwoord.

Zoals reeds opgemerkt aan het eind van Sectie 9, hebben we binnen dit project geen tijd gehad om erg uitgebreide tests op de willekeurigheid van de UIDs uit te voeren. Het zou nuttig zijn de random number generatie voor de UIDs aan uitgebreidere tests te onderwerpen, bijvoorbeeld de statistische tests voor pseudo-random nummer generatoren beschreven door NIST als onderdeel van FIPS 140 [1].

Indien het onderscheid tussen reisdocumenten van verschillende fabrikanten bezwaarlijk wordt gevonden (ondanks de zeer beperkte afstand waarop dit mogelijk te detecteren is), is het aanscherpen van de specificaties van ICAO (m.n. over toegestane/voorgeschreven foutmeldingen) een optie, maar dat zou aanpassingen in alle bestaande implementaties van paspoort-software vereisen. Maar zoals ook geconcludeerd in het Sdu rapport [6], is het technisch en organisatorisch ondoenlijk alle mogelijke verschillen in de onderliggende platformen uit te bannen. Een handigere tegenmaatregel, zeker voor het paspoort, lijkt het opnemen van metaalfolie in het paspoortomslag als een zgn. Faraday kooi. Dit is een goed voorbeeld van ‘defense-in-depth’.

Lijst van gebruikte afkortingen

- ATS: Answer to Reset
- BAC: Basic Access Control
- MRTD: Machine Readable Travel Document
- MRZ: Machine Readable Zone
- NIK: Nederlandse Identiteitskaart
- PRNG: Pseudo Random Number Generation
- RFID: Radio Frequency IDentification
- UID: Unique IDentifier

Appendix A: Low level traces

Hieronder 4 voorbeelden van de low-level traces verkregen bij de timing analyse beschreven in Sectie 6, voor achtereenvolgens Nederlands paspoort (2008), NIK (2008), Iers paspoort (2006) en Slowaaks paspoort (2008). De traces geven het begin van een ISO14443 sessie, namelijk de anti-collision fase en het versturen van de ATS.

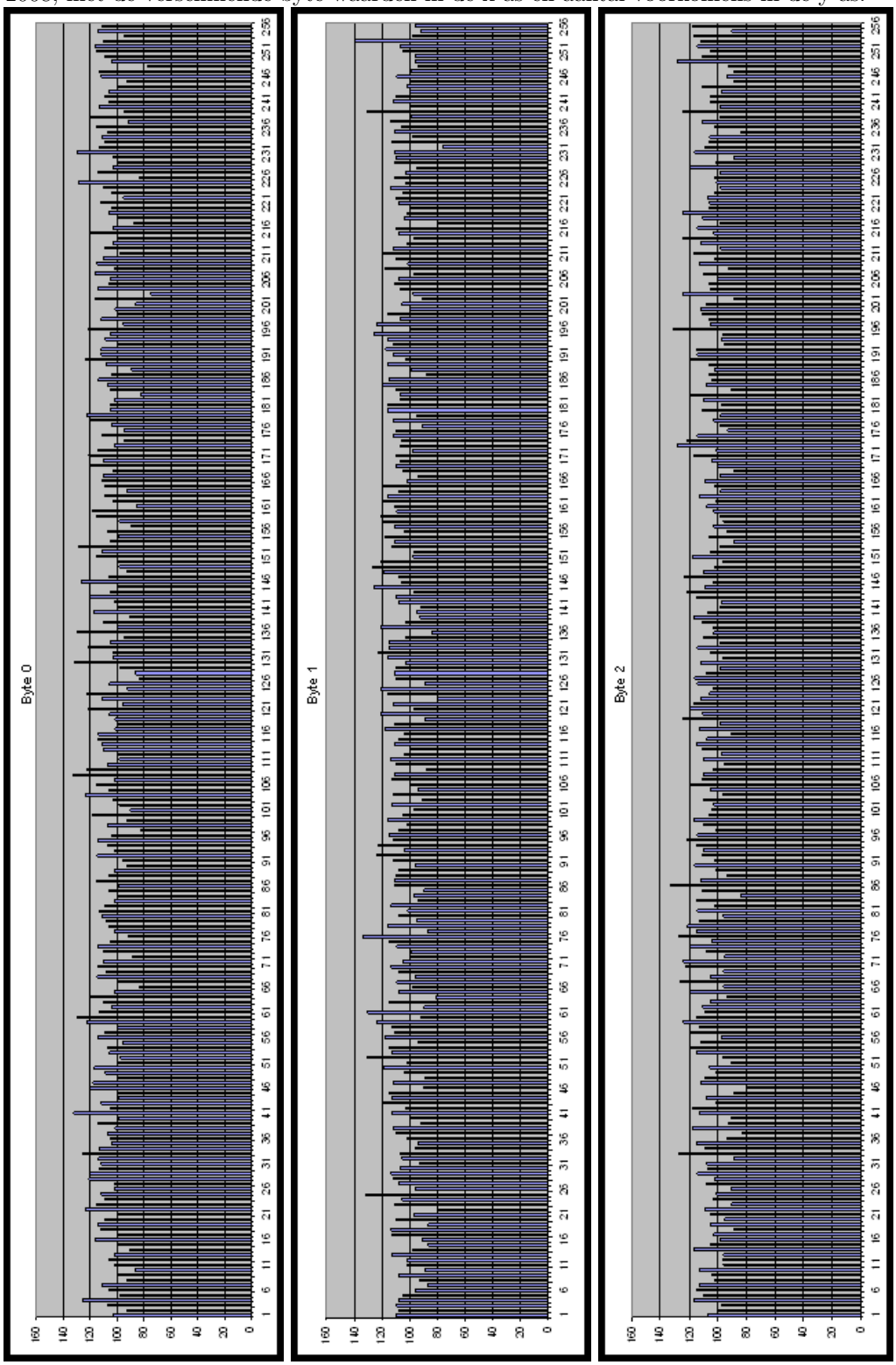
De tweede kolom geeft de timing in Proxmark ticks; een Proxmark tick is 1/8 van de bit-period (etu) zoals beschreven in ISO14443A. (Een etu = 128 / carrier frequency = 128 / 13.56 MHz $\approx 9,439\mu s$, 1 proxmark-tick = etu / 8 $\approx 1,179\mu s$.)

Data voorafgegaan door `TAG` worden verstuurd door de chip naar de lezer; andere data zijn van de lezer naar de chip. Merk op dat de timing van alle responses van de chip identiek is (64 of 80 ticks). De responses zelf zijn ook identiek, met uitzondering natuurlijk van de random UIDs (voorafgegaan door `08`).

```
Low level trace NL
 +      0:    :     26
 +     64:   0: TAG 08  00
 +    856:    :     93  20
 +     64:   0: TAG 08  c8  19  c1  18
 +   2367:    :     93  70  08  c8  19  c1  18  8d  0b
 +     64:   0: TAG 20  fc  70
 +   1047:    :     e0  50  bc  a5
 +     80:   0: TAG 04  38  33  b1  48  5c

Low level trace NIK
 +      0:    :     26
 +     64:   0: TAG 08  00
 +    855:    :     93  20
 +     64:   0: TAG 08  0e  77  77  06
 +   2366:    :     93  70  08  0e  77  77  06  d9  f9
 +     64:   0: TAG 20  fc  70
 +   1048:    :     e0  50  bc  a5
 +     80:   0: TAG 04  38  33  b1  48  5c

Low level trace IRL:
 +      0:    :     26
 +     64:   0: TAG 08  00
 +    847:    :     93  20
 +     64:   0: TAG 08  50  00  ef  b7
 +   2367:    :     93  70  08  50  00  ef  b7  cf  fd
 +     64:   0: TAG 20  fc  70
 +   1046:    :     e0  50  bc  a5
 +     80:   0: TAG 04  38  33  b1  48  5c

Low level trace SVK:
 +      0:    :     26
 +     64:   0: TAG 08  00
 +    855:    :     93  20
 +     64:   0: TAG 08  09  2c  d1  fc
 +   2366:    :     93  70  08  09  2c  d1  fc  47  a7
 +     64:   0: TAG 20  fc  70
 +   1048:    :     e0  50  bc  a5
 +     80:   0: TAG 04  38  33  b1  48  5c
```

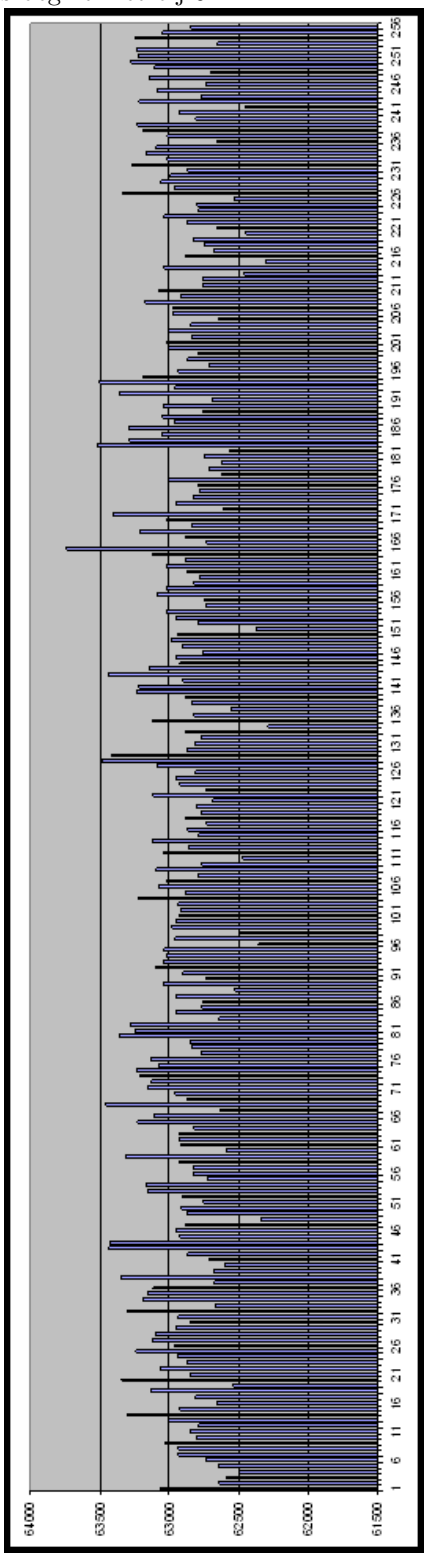
Appendix B: Distributies van UID bytes

Hieronder distributies van de drie bytes van de UIDs gegenereerd door een Nederlands paspoort uit 2008, met de verschillende byte-waarden in de x-as en aantal voorkomens in de y-as.



Appendix C: Distributies van BAC challenges

Hieronder de distributie van de bytes in BAC challenges gegenereerd door een Nederlands paspoort uit 2008, met de verschillende byte-waarden in de x-as en aantal voorkomens in de y-as. NB de y-as begint niet bij 0.



Referenties

[1] A statistical test suite for random and pseudorandom number generators for cryptographic applicatiions, 2001. NIST Special Publication 800-22.

[2] Cees-Bart Breunesse, Engelbert Hubbers, Pieter Koopman, Wojciech Mostowski, Martijn Oostdijk, Vlad Rusu, René de Vries, Arjen van Weelden, Ronny Wichers Schreur, and Tim Willemse. Het testen van de Nederlandse elektronische reisdocumenten, 2006.

[3] Global Platform Organization. *Card Specification, Version 2.1.1*, March 2003. `http://www.globalplaform.org`.

[4] Development of a logical data structure - LDS for optional capacity expansion technologies, revision 1.7. Technical report, ICAO, May 2004. Available from `http://mrtd.icao.int/images/stories/Doc/ePassports/Logical%AC%AC_Data_Structure(LDS)_version1.7.pdf`.

[5] PKI for machine readable travel documents offering ICC read-only access, version 1.1. Technical report, ICAO, Oct 2004. Available from `http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf`.

[6] Sdu identification. Sdu reactie op artikel fingerprinting Passports, version 1.1, april 9, 2008.

[7] ISO 7816. ISO/IEC 7816 Identification cards – Integrated circuit(s) cards, Part 4: Organization, security and commands for interchange. Technical report, ISO JTC 1/SC 17, 2005.

[8] Henning Richter, Wojciech Mostowski, and Erik Poll. Fingerprinting passports. In *NLUUG Spring Conference on Security*, pages 21–30, May 2008.