Sdu reactie op artikel fingerprinting Passports

Versie: v1.1
Datum: 9 april 2008

INHOUDSOPGAVE

VERSIEBEHEER

Dit document staat onder versiebeheer bij Sdu Identification en staat als configuratie item geregistreerd onder nummer: 8828/20080409/RBL/011.

Versie

Versie	***Datum***	***Korte beschrijving aanpassing***
0.1 Draft	2008-04-08	Initiële versie
1.0	2008-04-08	Aangepast naar aanleiding van review
1.1	2008-04-08	Toevoeging testresultaten

INTRODUCTIE

Dit document bevat een analyse van Sdu Identification m.b.t. de bevindingen genoemd in het artikel D[4] “Fingerprinting Passports” opgesteld door Henning Richter, Wojciech Mostowski en Erik Poll. Henning Richter is student aan de Lausitz University of Applied Sciences in Duitsland. Wojtek Mostowski and Erik Poll zijn onderzoekers bij de Digital Security group aan de Radboud Universiteit van Nijmegen.

1 DOCUMENTEN

Naar onderstaande documenten wordt verwezen in deze rapportage.

1.1 Normen

D[1] *ICAO 9303: Machine Readable Travel Documents Part 1: Machine readable passport, Vol. 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability – 6th Edition 2006 - International Civil Aviation Organization (ICAO)*

D[2] *ISO 7816 – 4, Inter industry commands for interchange*

D[3] *ISO 7816 – 8, Security Related Inter industry commands*

1.2 Overige documenten

D[4] *Fingerprinting Passports - Henning Richter, Wojciech Mostowski en Erik Poll (source: http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf)*

2 Inleiding

De huidige generatie paspoorten bieden de paspoorthouder bescherming tegen het ongemerkt uitlezen van de persoonsgegevens. Deze bescherming wordt geboden door het Basic Access Control mechanisme gespecificeerd in de ICAO standaard D[1].

Henning Richter, Wojciech Mostowski en Erik Poll beschrijven in hun artikel D[4] “Fingerprinting Passports” een methode om de nationaliteit van een ICAO ePassport van een 10-tal landen vast te stellen zonder dat hiervoor het Basic Access Control beveiligingprotocol is doorlopen. Deze aanval vindt plaats op logisch niveau. Daarnaast worden in het artikel ook nog andere methoden genoemd op basis waarvan een classificatie van paspoorten kan worden uitgevoerd.

Dit rapport bevat een analyse met betrekking tot de bevindingen genoemd in het artikel. Daarnaast bevat rapport de resultaten van testen op de paspoorten die Sdu Identification levert aan Nederland, Finland, Slowakije en Ierland. Deze testen zijn uitgevoerd om te bepalen of nationaliteiten gekoppeld aan deze paspoorten onderscheidbaar zijn op basis van de methoden beschreven in D[2] “Fingerprinting Passports”.

3 Probleemanalyse artikel "Fingerprinting Passports"

3.1 Probleemstelling

De huidige generatie paspoorten bieden de paspoorthouder bescherming tegen het ongemerkt uitlezen van de persoonsgegevens. Deze bescherming wordt geboden door het Basic Access Control mechanisme gespecificeerd in de ICAO standaard D[1].

Henning Richter, Wojciech Mostowski en Erik Poll beschrijven in hun artikel D[4] "Fingerprinting Passports" een methode om de nationaliteit van een ICAO ePassport van een 10-tal landen vast te stellen zonder dat hiervoor het Basic Access Control beveiligingprotocol is doorlopen.

3.2 Probleemanalyse

Het artikel D[4] geeft aan dat paspoorten op basis van de volgende eigenschappen onderscheidbaar zijn:

1. Diversiteit aan ISO7816 foutmeldingen op bewust incorrect ingegeven ISO7816 APDU commando's.
2. Het wel of niet afgegeven ISO7816 File Control Information en de inhoud hiervan.
3. Random/Fixed UID
4. ATS
5. Side channel karakteristieken

3.2.1 Diversiteit aan ISO7816 foutmeldingen (ISO7816 layer)

De ISO7816 norm biedt geen éénduidig en consistent raamwerk voor wat betreft de te retourneren foutcodes. De ICAO norm D[1] biedt aanvullende specificaties met betrekking tot foutcodes en foutafhandeling. Echter ook de combinatie van de twee normen biedt nog steeds ruimte voor verschillende ISO7816/ICAO conforme paspoort implementaties.

Diverse landen hebben hun implementaties gebaseerd op bestaande, of in een vergevorderd stadium van ontwikkeling verkerende chip/operating system combinaties. ICAO heeft daarom rekening gehouden met de daardoor reeds bestaande verschillende interpretaties van ISO7816.

3.2.2 ISO7816 File Control Information (ISO7816 layer)

De ISO7816 biedt optioneel de mogelijkheid om als response op een incorrecte of niet toegestane SELECT FILE commando aanvullende informatie aan de terminal te verschaffen inzake het de reden van het weigeren of correct accepteren van het SELECT FILE commando.

De ICAO ePassport oplossing van Sdu Identification ondersteunt om beveiligingsredenen geen File Control Information (FCI).

3.2.3 Random/Fixed UID (ISO 14443 layer)

Het artikel bericht over (niet nader genoemde) landen die een statisch Unique Identifier (UID) hebben geconfigureerd. Hierdoor wordt een paspoort traceerbaar en is deze onderscheidbaar van andere paspoortuitgevers die een random UID configureren.

Alle door Sdu Identification uitgeleverde paspoorten hebben een random UID geconfigureerd. Dit geldt voor alle 4 de landen die het Sdu ePassport platform gebruiken, d.w.z. Nederland, Finland, Slowakije en Ierland.

Daarnaast is het mogelijk op basis van type-A of type-B ISO14443 protocol een onderscheid te maken.

3.2.4 ATS (ISO 14443-4 layer)

De Answer To Select (ATS) is gespecificeerd in ISO14443-4. Deze bevat communicatie parameters die de chip ondersteunt, zoals maximum frame size, maximum baudrate, etc. Daarnaast kan de ATS historical bytes bevatten die meestal statische data bevatten.

Sdu Identification verwijdert alle historical bytes tijdens het initialisatie proces. Dit geldt voor alle landen aan wie Sdu levert. Het is niet mogelijk om de overige ATS bytes te verwijderen, omdat deze noodzakelijk zijn voor de reader bij het opzetten van de communicatie met de kaart. Deze overige ATS bytes bevatten per definitie platform (chip/operating systeem) specifieke data. Het is nimmer mogelijk de ATS voor alle paspoorten in de wereld vast te leggen, waardoor op basis van de ATS altijd een mogelijkheid tot onderscheid mogelijk zal zijn.

3.2.5 Side channel karakteristieken

Voor side channel monitoring is meer geavanceerde apparatuur nodig dan voor de logische aanvallen op ISO7816 level.

Side channel attacks zoals Differential Power Analysis (DPA) en Differential Frequency Analysis (DFA) zijn er op gericht om de waarde van het cryptografisch sleutelmateriaal in de kaart te achterhalen. Resistentheid tegen dergelijke aanvallen is getest tegen AVA_VLA.2 niveau in de Common Criteria certificering van de Sdu ePassport oplossing. Dit neemt echter niet weg dat de power consumptie gedurende een bepaalde transactie met de kaart mogelijk een platform specifiek beeld of spectrum kan opleveren.

Ook door het meten van response tijden is het altijd mogelijk om platform specifieke kenmerken vast te stellen op basis waarvan een platform geïdentificeerd kan worden.

4 Testen

De testen die zijn uitgevoerd komen overeen met de ‘aanvallen’ op logisch niveau zoals beschreven in het artikel D[4] ‘Fingerprinting Passports’. Daarnaast zijn aanvullende testen uitgevoerd waarbij andere vergelijkbare foutcodes worden opgewerkt.
Onderstaand de resultaten van de testen zoals beschreven in het artikel D[4].

	44	82	84	88	A4	B0	B1		
	Rehab.CHV	**Ext.Auth.**	**Get Chall.**	**Int.Auth.**	**Select File**	**Read Binary**	**Read Binary**	**FCI**	**ATS**
Nederland	6D00	6700	6700	6982	6A86	6982	6982	Geen	043833B1
Finland	6D00	6700	6700	6982	6A86	6982	6982	Geen	043833B1
Ierland	6D00	6700	6700	6982	6A86	6982	6982	Geen	043833B1
Slowakije	6D00	6700	6700	6982	6A86	6982	6982	Geen	043833B1

De bovenstaande testresultaten voor Nederland komen overeen met de testresultaten in artikel D[4] ‘Fingerprinting Passports’.

Uit de testresultaten blijkt voorts dat de Nederlandse, Finse, Ierse en Slowaakse reisdocumenten niet van elkaar te onderscheiden zijn op basis van de methode zoals beschreven in het artikel D[4] ‘Fingerprinting Passports’. Ook op basis van de door Sdu Identification uitgevoerde aanvullende testen is geen onderscheid te maken naar de Nederlandse, Finse, Ierse en Slowaakse reisdocumenten.

Voor details wordt verwezen naar de bijlage waarin het volledige testrapport is opgenomen.

5 Samenvatting resultaten

De resultaten worden als volgt samengevat. De methoden beschreven in het artikel zijn altijd uitvoerbaar en leiden inderdaad tot een classificatie van paspoorten. Deze classificatie is platform (chip/operating systeem) specifiek en niet (zoals het artikel beweert) landspecifiek. Deze veronderstelling zou alleen correct zijn indien ieder land zijn eigen chip/operating system platform toepast. Zodra dezelfde technologie aan meer dan één land wordt geleverd zijn de paspoorten op basis van de methoden beschreven in D[2] “Fingerprinting Passports” niet onderscheidbaar. Zo is het Nederlandse paspoort op basis van methoden beschreven in het artikel niet onderscheidbaar van het Finse, het Ierse en het Slowaakse paspoort.

Het is technisch en organisatorisch ondoenlijk om alle mogelijkheden om het platform specifiek categoriseren van paspoorten te voorkomen. Teneinde ongevoelig te zijn voor alle mogelijke methoden beschreven in D[4] “Fingerprinting Passports” biedt uitsluitend het aanbrengen van een afscherming van het RF-veld (“shielding”) een haalbare en afdoende oplossing.

Appendix: Testrapport

A.1. Samenvatting

De testen die zijn uitgevoerd komen overeen met de ‘aanvallen’ op logisch niveau zoals beschreven in het onderzoek ‘Fingerprinting Passports’. Daarnaast zijn aanvullende testen uitgevoerd waarbij andere vergelijkbare foutcodes worden opgewerkt.
De testen bestaan uit het opwekken van foutcodes en het opvragen van FCI en ATS. Onderstaand de resultaten van de testen zoals beschreven in het onderzoekrapport.

	44 Rehab.CHV	82 Ext.Auth.	84 Get Chall.	88 Int.Auth.	A4 Select File	B0 Read Binary	B1 Read Binary	FCI	ATS
Nederland	6D00	6700	6700	6982	6A86	6982	6982	Geen	043833B1
Finland	6D00	6700	6700	6982	6A86	6982	6982	Geen	043833B1
Ierland	6D00	6700	6700	6982	6A86	6982	6982	Geen	043833B1
Slowakije	6D00	6700	6700	6982	6A86	6982	6982	Geen	043833B1

Uit de testen blijkt dat, met behulp van de RFID chip in het reisdocument, de Nederlandse, Finse, Ierse en Slowaakse reisdocumenten niet van elkaar te onderscheiden zijn op basis van de methode zoals beschreven in het artikel ‘Fingerprinting Passports’. Ook op basis van de aanvullende testen is geen onderscheid te maken naar de Nederlandse, Finse, Ierse en Slowaakse reisdocumenten.

A.2. Testbeschrijving

Dit testrapport beschrijft de testen en de daarbij behorende resultaten die uitgevoerd zijn op de reisdocumenten van Nederland (NLD), Finland (FIN), Ierland (IRL) en Slowakije (SVK).

Met deze testen wordt aangetoond dat de chips in deze reisdocumenten op logisch niveau identiek reageren en niet van elkaar te onderscheiden zijn.

De testen zijn verdeeld in vier onderdelen:
1. Testen op APDU's;
2. Testen op FCI;
3. Testen op ATS;
4. Testen op default selected.

A.3. Testen op APDU's

In het onderzoek 'Fingerprinting Passports' wordt gesproken over alle mogelijke 256 instructie bytes en vervolgens over 7 specifieke instructies:
1. REHABILITATE CHV;
2. EXTERNAL AUTHENTICATE;
3. GET CHALLENGE;
4. INTERNAL AUTHENTICATE;
5. SELECT FILE:
6. READ BINARY (B0);
7. READ BINARY (B1).

Voor alle instructies wordt een minimale APDU test uitgevoerd, de test zoals deze waarschijnlijk ook is uitgevoerd in het 'Fingerprinting Passports' onderzoek. Een minimale APDU heeft de volgende specificatie:

CLA	**INS**	**P1**	**P2**
00	XX	00	00

Voor de 7 specifieke instructies wordt naast de minimale APDU ook nog de mogelijke foutcodes opgewekt. Bij alle testen wordt voor het uitvoeren van de APDU eerst de MRTD applicatie geselecteerd.

A.3.1 REHABILITATE CHV

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	44	00	00	-	-	-	Minimale APDU

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	6D00	6D00	6D00	6D00

Conclusie:
Met behulp van het uitvoeren van het REHABILITATE CHV commando is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.3.2 EXTERNAL AUTHENTCATE

A.3.2.1 Voordat GET CHALLENGE uitgevoerd is

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	82	00	00	-	-	-	Minimale APDU
2	00	82	00	00	28	data	28	Correcte APDU
3	00	82	00	01	28	data	28	P1/P2 incorrect
4	00	82	00	00	-	-	28	Lengte incorrect

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	6700	6700	6700	6700
2	6300	6300	6300	6300
3	6A86	6A86	6A86	6A86
4	6700	6700	6700	6700

Conclusie:
Met behulp van het uitvoeren van het EXTERNAL AUTHENTICATE commando voordat het GET CHALLENGE commando uitgevoerd is, is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.3.2.2 Nadat GET CHALLENGE uitgevoerd is

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur een correct GET CHALLENGE commando naar de chip van het reisdocument;
- Ontvang de challenge van de chip van het reisdocument;
- Stuur de volgende APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	82	00	00	-	-	-	Minimale APDU
2	00	82	00	00	28	data	28	Correcte APDU
3	00	82	00	01	28	data	28	P1/P2 incorrect
4	00	82	00	00	-	-	28	Lengte incorrect

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	6700	6700	6700	6700
2	6300	6300	6300	6300
3	6A86	6A86	6A86	6A86
4	6700	6700	6700	6700

Conclusie:
Met behulp van het uitvoeren van het EXTERNAL AUTHENTICATE commando nadat het GET CHALLENGE commando uitgevoerd is, is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.3.3 GET CHALLENGE

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	84	00	00	-	-	-	Minimale APDU
2	00	84	00	00	-	-	08	Correcte APDU, 8 bytes random gevraagd
3	00	84	00	00	-	-	10	Correcte APDU, 16 bytes random gevraagd
4	00	82	00	01	-	-	08	P1/P2 incorrect

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	6700	6700	6700	6700
2	9000 (8 bytes random)	9000 (8 bytes random)	9000 (8 bytes random)	9000 (8 bytes random)
3	9000 (16bytes random)	9000 (16bytes random)	9000 (16bytes random)	9000 (16bytes random)
4	6A86	6A86	6A86	6A86

Conclusie:
Met behulp van het uitvoeren van het GET CHALLENGE commando is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.3.4 INTERNAL AUTHENTICATE

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	88	00	00	-	-	-	Minimale APDU
2	00	88	00	00	08	data	00	Correcte APDU
3	00	88	00	01	08	data	00	P1/P2 incorrect
4	00	88	00	00	-	-	08	Lengte incorrect

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	6982	6982	6982	6982
2	6982	6982	6982	6982
3	6982	6982	6982	6982
4	6982	6982	6982	6982

Conclusie:
Met behulp van het uitvoeren van het INTERNAL AUTHENTICATE commando is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.3.5 SELECT FILE

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	A4	00	00	-	-	-	Minimale APDU
2	00	A4	04	0C	07	A0000 2471001	-	Selecteer DF, geen FCI opvragen
3	00	A4	04	00	07	A0000 2471001	00	Selecteer DF, wel FCI opvragen
4	00	A4	02	0C	02	0101	-	Selecteer bestaande EF, geen FCI opvragen
5	00	A4	02	0C	02	0104	-	Selecteer niet bestaande EF
6	00	A4	02	00	02	0101	00	Selecteer bestaande EF, wel FCI opvragen
7	00	A4	82	0C	02	0101	-	P1/P2 incorrect
8	00	A4	02	0C	08	0101	-	Lengte incorrect

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	6A86	6A86	6A86	6A86
2	9000 (geen FCI)	9000 (geen FCI)	9000 (geen FCI)	9000 (geen FCI)
3	9000 (geen FCI)	9000 (geen FCI)	9000 (geen FCI)	9000 (geen FCI)
4	6982	6982	6982	6982
5	6982	6982	6982	6982
6	6982	6982	6982	6982
7	6A86	6A86	6A86	6A86
8	6700	6700	6700	6700

Conclusie:
Met behulp van het uitvoeren van het SELECT FILE commando is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.3.6 READ BINARY (B0)

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	B0	00	00	-	-	-	Minimale APDU
2	00	B0	00	00	-	-	00	Correcte APDU
3	00	B0	9E	00	-	-	00	Correcte APDU met impliciete selectie van EF
4	00	B0	01	00	-	-	00	P1/P2 incorrect

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	6982	6982	6982	6982
2	6982	6982	6982	6982
3	6982	6982	6982	6982
4	6982	6982	6982	6982

Conclusie:
Met behulp van het uitvoeren van het READ BINARY (B0) commando is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.3.7 READ BINARY (B1)

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	B1	00	00	-	-	-	Minimale APDU
2	00	B1	00	00	03	540100	00	Correcte APDU
3	00	B1	00	1E	03	540100	00	Correcte APDU met impliciete selectie van EF
4	00	B1	01	00	03	540100	00	P1/P2 incorrect

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	6982	6982	6982	6982
2	6982	6982	6982	6982
3	6982	6982	6982	6982
4	6982	6982	6982	6982

Conclusie:
Met behulp van het uitvoeren van het READ BINARY (B0) commando is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.3.8 Minimale APDU

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende APDU naar de chip van het reisdocument:

CLA	**INS**	**P1**	**P2**
00	XX	00	00

  Hierbij wordt XX oplopend ingevuld van 00 naar FF
- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

XX	**NLD**	**FIN**	**IRL**	**SVK**	**XX**	**NLD**	**FIN**	**IRL**	**SVK**
00	6D00	6D00	6D00	6D00	**80**	6D00	6D00	6D00	6D00
01	6D00	6D00	6D00	6D00	**81**	6D00	6D00	6D00	6D00
02	6D00	6D00	6D00	6D00	**82**	6700	6700	6700	6700
03	6D00	6D00	6D00	6D00	**83**	6D00	6D00	6D00	6D00
04	6D00	6D00	6D00	6D00	**84**	6700	6700	6700	6700
05	6D00	6D00	6D00	6D00	**85**	6D00	6D00	6D00	6D00
06	6D00	6D00	6D00	6D00	**86**	6D00	6D00	6D00	6D00
07	6D00	6D00	6D00	6D00	**87**	6D00	6D00	6D00	6D00
08	6D00	6D00	6D00	6D00	**88**	6982	6982	6982	6982
09	6D00	6D00	6D00	6D00	**89**	6D00	6D00	6D00	6D00
0A	6D00	6D00	6D00	6D00	**8A**	6D00	6D00	6D00	6D00
0B	6D00	6D00	6D00	6D00	**8B**	6D00	6D00	6D00	6D00
0C	6D00	6D00	6D00	6D00	**8C**	6D00	6D00	6D00	6D00
0D	6D00	6D00	6D00	6D00	**8D**	6D00	6D00	6D00	6D00
0E	6D00	6D00	6D00	6D00	**8E**	6D00	6D00	6D00	6D00
0F	6D00	6D00	6D00	6D00	**8F**	6D00	6D00	6D00	6D00
10	6D00	6D00	6D00	6D00	**90**	6D00	6D00	6D00	6D00
11	6D00	6D00	6D00	6D00	**91**	6D00	6D00	6D00	6D00
12	6D00	6D00	6D00	6D00	**92**	6D00	6D00	6D00	6D00
13	6D00	6D00	6D00	6D00	**93**	6D00	6D00	6D00	6D00
14	6D00	6D00	6D00	6D00	**94**	6D00	6D00	6D00	6D00
15	6D00	6D00	6D00	6D00	**95**	6D00	6D00	6D00	6D00
16	6D00	6D00	6D00	6D00	**96**	6D00	6D00	6D00	6D00
17	6D00	6D00	6D00	6D00	**97**	6D00	6D00	6D00	6D00
18	6D00	6D00	6D00	6D00	**98**	6D00	6D00	6D00	6D00
19	6D00	6D00	6D00	6D00	**99**	6D00	6D00	6D00	6D00
1A	6D00	6D00	6D00	6D00	**9A**	6D00	6D00	6D00	6D00
1B	6D00	6D00	6D00	6D00	**9B**	6D00	6D00	6D00	6D00
1C	6D00	6D00	6D00	6D00	**9C**	6D00	6D00	6D00	6D00
1D	6D00	6D00	6D00	6D00	**9D**	6D00	6D00	6D00	6D00
1E	6D00	6D00	6D00	6D00	**9E**	6D00	6D00	6D00	6D00

XX	NLD	FIN	IRL	SVK	XX	NLD	FIN	IRL	SVK
1F	6D00	6D00	6D00	6D00	**9F**	6D00	6D00	6D00	6D00
20	6D00	6D00	6D00	6D00	**A0**	6D00	6D00	6D00	6D00
21	6D00	6D00	6D00	6D00	**A1**	6D00	6D00	6D00	6D00
22	6D00	6D00	6D00	6D00	**A2**	6D00	6D00	6D00	6D00
23	6D00	6D00	6D00	6D00	**A3**	6D00	6D00	6D00	6D00
24	6D00	6D00	6D00	6D00	**A4**	6A86	6A86	6A86	6A86
25	6D00	6D00	6D00	6D00	**A5**	6D00	6D00	6D00	6D00
26	6D00	6D00	6D00	6D00	**A6**	6D00	6D00	6D00	6D00
27	6D00	6D00	6D00	6D00	**A7**	6D00	6D00	6D00	6D00
28	6D00	6D00	6D00	6D00	**A8**	6D00	6D00	6D00	6D00
29	6D00	6D00	6D00	6D00	**A9**	6D00	6D00	6D00	6D00
2A	6D00	6D00	6D00	6D00	**AA**	6D00	6D00	6D00	6D00
2B	6D00	6D00	6D00	6D00	**AB**	6D00	6D00	6D00	6D00
2C	6D00	6D00	6D00	6D00	**AC**	6D00	6D00	6D00	6D00
2D	6D00	6D00	6D00	6D00	**AD**	6D00	6D00	6D00	6D00
2E	6D00	6D00	6D00	6D00	**AE**	6D00	6D00	6D00	6D00
2F	6D00	6D00	6D00	6D00	**AF**	6D00	6D00	6D00	6D00
30	6D00	6D00	6D00	6D00	**B0**	6982	6982	6982	6982
31	6D00	6D00	6D00	6D00	**B1**	6982	6982	6982	6982
32	6D00	6D00	6D00	6D00	**B2**	6D00	6D00	6D00	6D00
33	6D00	6D00	6D00	6D00	**B3**	6D00	6D00	6D00	6D00
34	6D00	6D00	6D00	6D00	**B4**	6D00	6D00	6D00	6D00
35	6D00	6D00	6D00	6D00	**B5**	6D00	6D00	6D00	6D00
36	6D00	6D00	6D00	6D00	**B6**	6D00	6D00	6D00	6D00
37	6D00	6D00	6D00	6D00	**B7**	6D00	6D00	6D00	6D00
38	6D00	6D00	6D00	6D00	**B8**	6D00	6D00	6D00	6D00
39	6D00	6D00	6D00	6D00	**B9**	6D00	6D00	6D00	6D00
3A	6D00	6D00	6D00	6D00	**BA**	6D00	6D00	6D00	6D00
3B	6D00	6D00	6D00	6D00	**BB**	6D00	6D00	6D00	6D00
3C	6D00	6D00	6D00	6D00	**BC**	6D00	6D00	6D00	6D00
3D	6D00	6D00	6D00	6D00	**BD**	6D00	6D00	6D00	6D00
3E	6D00	6D00	6D00	6D00	**BE**	6D00	6D00	6D00	6D00
3F	6D00	6D00	6D00	6D00	**BF**	6D00	6D00	6D00	6D00
40	6D00	6D00	6D00	6D00	**C0**	6D00	6D00	6D00	6D00
41	6D00	6D00	6D00	6D00	**C1**	6D00	6D00	6D00	6D00
42	6D00	6D00	6D00	6D00	**C2**	6D00	6D00	6D00	6D00
43	6D00	6D00	6D00	6D00	**C3**	6D00	6D00	6D00	6D00
44	6D00	6D00	6D00	6D00	**C4**	6D00	6D00	6D00	6D00
45	6D00	6D00	6D00	6D00	**C5**	6D00	6D00	6D00	6D00
46	6D00	6D00	6D00	6D00	**C6**	6D00	6D00	6D00	6D00
47	6D00	6D00	6D00	6D00	**C7**	6D00	6D00	6D00	6D00
48	6D00	6D00	6D00	6D00	**C8**	6D00	6D00	6D00	6D00
49	6D00	6D00	6D00	6D00	**C9**	6D00	6D00	6D00	6D00
4A	6D00	6D00	6D00	6D00	**CA**	6D00	6D00	6D00	6D00
4B	6D00	6D00	6D00	6D00	**CB**	6D00	6D00	6D00	6D00

XX	NLD	FIN	IRL	SVK	XX	NLD	FIN	IRL	SVK
4C	6D00	6D00	6D00	6D00	**CC**	6D00	6D00	6D00	6D00
4D	6D00	6D00	6D00	6D00	**CD**	6D00	6D00	6D00	6D00
4E	6D00	6D00	6D00	6D00	**CE**	6D00	6D00	6D00	6D00
4F	6D00	6D00	6D00	6D00	**CF**	6D00	6D00	6D00	6D00
50	6D00	6D00	6D00	6D00	**D0**	6D00	6D00	6D00	6D00
51	6D00	6D00	6D00	6D00	**D1**	6D00	6D00	6D00	6D00
52	6D00	6D00	6D00	6D00	**D2**	6D00	6D00	6D00	6D00
53	6D00	6D00	6D00	6D00	**D3**	6D00	6D00	6D00	6D00
54	6D00	6D00	6D00	6D00	**D4**	6D00	6D00	6D00	6D00
55	6D00	6D00	6D00	6D00	**D5**	6D00	6D00	6D00	6D00
56	6D00	6D00	6D00	6D00	**D6**	6D00	6D00	6D00	6D00
57	6D00	6D00	6D00	6D00	**D7**	6D00	6D00	6D00	6D00
58	6D00	6D00	6D00	6D00	**D8**	6D00	6D00	6D00	6D00
59	6D00	6D00	6D00	6D00	**D9**	6D00	6D00	6D00	6D00
5A	6D00	6D00	6D00	6D00	**DA**	6D00	6D00	6D00	6D00
5B	6D00	6D00	6D00	6D00	**DB**	6D00	6D00	6D00	6D00
5C	6D00	6D00	6D00	6D00	**DC**	6D00	6D00	6D00	6D00
5D	6D00	6D00	6D00	6D00	**DD**	6D00	6D00	6D00	6D00
5E	6D00	6D00	6D00	6D00	**DE**	6D00	6D00	6D00	6D00
5F	6D00	6D00	6D00	6D00	**DF**	6D00	6D00	6D00	6D00
60	6D00	6D00	6D00	6D00	**E0**	6D00	6D00	6D00	6D00
61	6D00	6D00	6D00	6D00	**E1**	6D00	6D00	6D00	6D00
62	6D00	6D00	6D00	6D00	**E2**	6D00	6D00	6D00	6D00
63	6D00	6D00	6D00	6D00	**E3**	6D00	6D00	6D00	6D00
64	6D00	6D00	6D00	6D00	**E4**	6D00	6D00	6D00	6D00
65	6D00	6D00	6D00	6D00	**E5**	6D00	6D00	6D00	6D00
66	6D00	6D00	6D00	6D00	**E6**	6D00	6D00	6D00	6D00
67	6D00	6D00	6D00	6D00	**E7**	6D00	6D00	6D00	6D00
68	6D00	6D00	6D00	6D00	**E8**	6D00	6D00	6D00	6D00
69	6D00	6D00	6D00	6D00	**E9**	6D00	6D00	6D00	6D00
6A	6D00	6D00	6D00	6D00	**EA**	6D00	6D00	6D00	6D00
6B	6D00	6D00	6D00	6D00	**EB**	6D00	6D00	6D00	6D00
6C	6D00	6D00	6D00	6D00	**EC**	6D00	6D00	6D00	6D00
6D	6D00	6D00	6D00	6D00	**ED**	6D00	6D00	6D00	6D00
6E	6D00	6D00	6D00	6D00	**EE**	6D00	6D00	6D00	6D00
6F	6D00	6D00	6D00	6D00	**EF**	6D00	6D00	6D00	6D00
70	6C01	6C01	6C01	6C01	**F0**	6D00	6D00	6D00	6D00
71	6D00	6D00	6D00	6D00	**F1**	6D00	6D00	6D00	6D00
72	6D00	6D00	6D00	6D00	**F2**	6D00	6D00	6D00	6D00
73	6D00	6D00	6D00	6D00	**F3**	6D00	6D00	6D00	6D00
74	6D00	6D00	6D00	6D00	**F4**	6D00	6D00	6D00	6D00
75	6D00	6D00	6D00	6D00	**F5**	6D00	6D00	6D00	6D00
76	6D00	6D00	6D00	6D00	**F6**	6D00	6D00	6D00	6D00
77	6D00	6D00	6D00	6D00	**F7**	6D00	6D00	6D00	6D00
78	6D00	6D00	6D00	6D00	**F8**	6D00	6D00	6D00	6D00

XX	NLD	FIN	IRL	SVK	XX	NLD	FIN	IRL	SVK
79	6D00	6D00	6D00	6D00	**F9**	6D00	6D00	6D00	6D00
7A	6D00	6D00	6D00	6D00	**FA**	6D00	6D00	6D00	6D00
7B	6D00	6D00	6D00	6D00	**FB**	6D00	6D00	6D00	6D00
7C	6D00	6D00	6D00	6D00	**FC**	6D00	6D00	6D00	6D00
7D	6D00	6D00	6D00	6D00	**FD**	6D00	6D00	6D00	6D00
7E	6D00	6D00	6D00	6D00	**FE**	6D00	6D00	6D00	6D00
7F	6D00	6D00	6D00	6D00	**FF**	6D00	6D00	6D00	6D00

Conclusie:
Met behulp van het uitvoeren van alle mogelijke minimale instructies is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.4. Testen op FCI

Test beschrijving:
- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende SELECT FILE APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	A4	04	0C	07	A0000 2471001	-	Selecteer DF, geen FCI opvragen
2	00	A4	04	00	07	A0000 2471001	00	Selecteer DF, wel FCI opvragen

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	9000 (geen FCI)	9000 (geen FCI)	9000 (geen FCI)	9000 (geen FCI)
2	9000 (geen FCI)	9000 (geen FCI)	9000 (geen FCI)	9000 (geen FCI)

Conclusie:
Met behulp van FCI informatie is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.5. Testen op ATS

Test beschrijving:
- Plaatst het reisdocument op de kaartlezer;
- Vraag de ATS op van het reisdocument.

Resultaat:

	NLD	FIN	IRL	SVK
ATS	043833B1	043833B1	043833B1	043833B1

Conclusie:
Met behulp van het opvragen van de ATS is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.

A.6. Testen op default selected

De reisdocumenten van Sdu Identification maken gebruik van Java Card waarbij de MRTD applicatie niet als default geselecteerd is.

Bij onderstaande test wordt **niet** eerst de MRTD applicatie geselecteerd.

Test beschrijving:

- Plaatst het reisdocument op de kaartlezer;
- Stuur de volgende GET CHALLENGE APDU naar de chip van het reisdocument:

Test	CLA	INS	P1	P2	Lc	Data	Le	Omschrijving
1	00	84	00	00	-	-	08	Correcte APDU, 8 bytes random gevraagd

- Ontvang het resultaat van de chip van het reisdocument.

Resultaat:

Test	NLD	FIN	IRL	SVK
1	6E00	6E00	6E00	6E00

Conclusie:
Met behulp van het niet default selected zijn van de MRTD applicatie is geen onderscheid te maken tussen de reisdocumenten van Nederland, Finland, Ierland en Slowakije.