brightsight®
your partner in security approval

delftechpark 1
2628 xj delft
the netherlands

p (+31) 15 269 2500
f (+31) 15 269 2555
info@brightsight.com

www.brightsight.com

kvk 30105045

07-RPT-005

Testen van de UID (random) generator in testdocumenten van de Nederlandse reisdocumenten

Datum	15 juli 2008
Auteur(s)	Paul Szulc Monique Bakker
Projectmanager	Jan Blonk
Exemplaarnummer	
Oplage	3
Aantal pagina's	10
Aantal bijlagen	
Opdrachtgever	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Versie	1.0
Rapport ID	
Certificatie ID	
Projectnaam	
Projectnummer	06098

Samenvatting

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft Brightsight (voormalig TNO ITSEF) gevraagd om te onderzoeken of de “randomness” van de UID parameter in de implementatie van twee testsamples van de Nederlandse reisdocumenten voldoet aan de FIPS 140-2 eisen. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft ook gevraagd om een correlatie test uit te voeren.

Uit de uitgevoerde testen is gebleken dat de UID (Uid1 tot Uid3), zoals verzonden door de chip in de reisdocumenten van de Nederlandse reisdocumenten, voldoet aan de FIPS 140-2 eisen voor random nummers en ook aan de eisen van de correlatietest.

Inhoudsopgave

1 Inleiding 4
1.1 Vraagstelling 4
1.2 Geleverde monsters en referenties 4
1.3 Gevolgde methode 5

2 De UID zoals beschreven in ISO 14443 6

3 Praktische testen 7
3.1 Opstelling voor testen 7
3.2 Test resultaten 7

4 Conclusie 10

1 Inleiding

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft Brightsight gevraagd om de “randomness” van het UID uitgezonden door twee testdocumenten van de Nederlandse reisdocumenten te onderzoeken.

1.1 Vraagstelling

Het Ministerie van BZK heeft TNO ITSEF (nu Brightsight) in concreto verzocht een FIPS 140-2 onderzoek en een correlatietest uit te voeren op de randomgenerator in twee testsamples van Nederlandse reisdocumenten. Het Ministerie van BZK heeft hiertoe twee testdocumenten met chip geleverd aan Brightsight.

1.2 Geleverde monsters en referenties

Het Ministerie van BZK heeft de volgende testsamples van reisdocumenten aangeleverd:

Monster nummer	Omschrijving
4487-1	Testdocument van Nederlands reisdocument
4487-2	Testdocument van Nederlands reisdocument

Bij de testen zijn de volgende referenties gebruikt:

Referentie	Omschrijving
[1]	ISO/IEC FDIS 14443-3:2000(E) Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 3: Initialization and anticollision.

De chip in beide testdocumenten communiceert volgens de ISO 14443 type A standaard.

1.3 Gevolgde methode

Teneinde antwoord te geven op de gestelde vraag zijn praktische testen uitgevoerd op de beide geleverde testdocumenten.

2 De UID zoals beschreven in ISO 14443

De chips in de geleverde testdocumenten van de reisdocumenten werken volgens de ISO 14443 type A standaard. De UID wordt gebruikt om een kaart in een RF veld uniek te kunnen selecteren om een communicatie kanaal op te kunnen zetten. De chips hanteren een ‘single format’ UID, hetgeen inhoudt dat de geretourneerde UID uit vier bytes bestaat waarvan drie willekeurig zijn (random). De volledige specificatie is in [1] beschreven. De UID is hieronder beschreven:

Uid0	Uid1	Uid2	Uid3
08	00…FF	00…FF	00…FF

De waarde van de eerste byte (Uid0 = 08) geeft aan dat de volgende bytes (Uid1 tot Uid3) willekeurig (random) en dynamisch gegenereerd zijn.
Het doel van de random waarde is tweeledig:

- Het verkrijgen van een dynamische kaartidentificatie die uniek is in het RF veld van de kaartlezer waarin ook andere kaarten kunnen voorkomen;
- Het verkrijgen van een bitpatroon dat voor collision detection kan worden gebruikt (zie [1]).

De ISO 14443 standaard bevat geen kwaliteitseis t.a.v. de mate van de “randomness” van de byte waarden in de UID.

3 Praktische testen

De praktische testen bestaan uit het uitvoeren van testen op de random waarden verstuurd door de chips in de UID (alleen Uid1 tot Uid3). Er zijn verschillende mogelijkheden om de random waarden te testen. Voor deze tests werden de door FIPS 140-2 gedefinieerde random testen gebruikt. FIPS 140-2 testen bestaan uit de volgende random testen:

- Monobit;
- Poker;
- Runs;
- Long runs.

Tevens is een correlatietest uitgevoerd.

3.1 Opstelling voor testen

De opstelling bestond uit een contactloze kaartlezer die volgens het ISO 14443 type A protocol kan communiceren en een PC om de kaartlezer aan te sturen en de ontvangen UID bytes op te slaan in een bestand met random bits.

Om een UID uit een chip op te kunnen vragen, wordt een anticollision protocol uitgevoerd, gebruikmakend van het REQA commando. Na het REQA commando geeft de kaart de UID als antwoord.

3.2 Test resultaten

Voor de random testen volgens FIPS 140-2 is een totaal van 20.000 bits noodzakelijk. Om dit aantal te halen, werd het REQA commando meerdere malen uitgevoerd op de twee geleverde monsters. Het resultaat, bestaande uit twee bestanden met random bits, werd onderworpen aan de FIPS 140-2 en correlatie tests. Hieronder zijn de resultaten beschreven:

Resultaten op monster 4487-1

```
Monobit  : X   = 10029  ( 9725 < X < 10275)  Passed
Poker    : X   = 11.45  ( 2,16 < X < 46,17)  Passed
Runs     : R1-0=  2565  ( 2343 < R1 < 2657)  Passed
         : R1-1=  2516                       Passed
         : R2-0=  1212  ( 1135 < R2 < 1365)  Passed
         : R2-1=  1261                       Passed
         : R3-0=   586  (  542 < R3 <  708)  Passed
         : R3-1=   612                       Passed
         : R4-0=   323  (  251 < R4 <  373)  Passed
         : R4-1=   279                       Passed
         : R5-0=   168  (  111 < R5 <  201)  Passed
         : R5-1=   158                       Passed
         : R6-0=   152  (  111 < R6 <  201)  Passed
         : R6-1=   181                       Passed
Long Runs: R-0 =     0  ( X = 0 )            Passed
         : R-1 =     0  ( X = 0 )            Passed


Correlation test:
In AIS 312505 bytes used in tests
In AIS 3120040 bits used in tests
 number of 1's= 10029
 number of 0's= 7989971
Autocorrelation test is 1 times performed

Maximum Z_tau-deviation from 2500:  139
occurred at shifts:
 Shift: 2151a
Repetition of the autocorrelation test with Shift: 2151 on Bits
10.000 to 14.999
Z_2151 = 2467
Autocorrelation test: Passed
```

Resultaten op monster 4487-2

```
Monobit  : X   =  9993  ( 9725 < X < 10275)  Passed
Poker    : X   = 14.88  ( 2,16 < X < 46,17)  Passed
Runs     : R1-0=  2564  ( 2343 < R1 < 2657)  Passed
         : R1-1=  2527                       Passed
         : R2-0=  1289  ( 1135 < R2 < 1365)  Passed
         : R2-1=  1308                       Passed
         : R3-0=   606  (  542 < R3 <  708)  Passed
         : R3-1=   648                       Passed
         : R4-0=   300  (  251 < R4 <  373)  Passed
         : R4-1=   305                       Passed
         : R5-0=   149  (  111 < R5 <  201)  Passed
         : R5-1=   136                       Passed
         : R6-0=   159  (  111 < R6 <  201)  Passed
         : R6-1=   144                       Passed
Long Runs: R-0 =     0  ( X = 0 )            Passed
         : R-1 =     0  ( X = 0 )            Passed


Correlation test:
In AIS 312505 bytes used in tests
In AIS 3120040 bits used in tests
 number of 1's= 10054
 number of 0's= 7989946
Autocorrelation test is 1 times performed

Maximum Z_tau-deviation from 2500:  120
occurred at shifts:
 Shift: 3856
 Shift: 4398a
Repetition of the autocorrelation test with Shift: 3856 on Bits
10.000 to 14.999
Z_3856 = 2501

Autocorrelation test: Passed
```

Uit de resultaten van deze testen is gebleken dat de UID in de twee Nederlandse testdocumenten voldoet aan de FIPS 140-2 eisen voor random nummers en aan de eisen van de correlatietest.

4 Conclusie

Uit de uitgevoerde testen is gebleken dat de UID (Uid1 tot Uid3) zoals verzonden door de chip in de testdocumtenten van de Nederlandse reisdocumenten voldoet aan de FIPS 140-2 eisen voor random nummers en ook aan de eisen van de correlatietest.