Author: rupp,scd
Project: Michigan Game Machine
Date: 01/06/13

PERSONALIZATION OF SIM CARDS

Index

Screens

1. Introduction

This document describes how to proceed with personalization of ACOS3 SIM cards.

2. Personalization

The sims comes without keys when they are bought from the manufacturer they are at *Manufacturing* lifetime (unless specific personalization is asked when ordered). [1] describes the process used to personalize the sim with the key pair K_T and K_C.

We will use the default PIN code (41 43 4F 53 54 45 53 54)

2.1. Data

We wish at least 3 data files , and encrypted IC code, encrypted AC1 code.

	byte1	byte2	byte3	byte4
record1	00	00	00	00
record2	00	00	00	00
record3	00	00	00	00

Personalization Stage

- [ ] Personalization Bit

Option Register

- [ ] ACCOUNT
- [ ] DEB_PIN
- [ ] 3-DES
- [ ] REV_DEB
- [ ] PIN_ALT
- [ ] TRNS_AUT
- [ ] DEB_MAC
- [ ] INQ_AUT

N_OF_FILE

Number of Data Files: 0 3 Hex

Security Option Register

- [x] Encrypted IC Code
- [ ] Encrypted PIN
- [ ] Encrypted AC5
- [ ] Encrypted AC4
- [ ] Encrypted AC3
- [ ] Encrypted AC2
- [x] Encrypted AC1

2.2. Security

	type	byte1	byte2	byte3	byte4	byte5	byte6	byte7	byte8
record1	*Issuer code IC*	48	3F	58	0E	EB	0F	A4	E4
record2	*PIN*	default	default	default	default	default	default	default	default
record3	*K_C*	0D	4F	11	CD	53	C1	BB	45
record4	*K_T*	E3	D4	45	B0	29	46	33	6C
record5	*Random generator seed*	default	default	default	default	default	default	default	default
record6	*Code AC1*	EE	3E	50	5E	35	AF	FA	D6

record7	*Code AC2*	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
record8	*Code AC3*	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
record9	*Code AC4*	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
record10	*Code AC5*	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
record11	~~*Key Try counter*~~	~~default~~	~~default~~	~~default~~	~~default~~	~~default~~	~~default~~	~~default~~	~~default~~
record12	*Backup Try counter*	default	default	default	default	default	default	default	default
record13	*Right-half of 3-DES K_C*	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
record14	*Right-half of 3-DES K_T*	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

3. Personalization workflow

This is the full personalization workflow for the ACOS3 card in manufacturing stage

Start of SIM Creation

- Authenticate with PIN:

  41 43 4F 53 54 45 53 54

- Select Personalization File 0xFF02 (TO READ FROM EXISTING SIM CARD)
- Write 4 Bytes in 1st record:

  00 82 03 80

- Write 4 Bytes in 2nd record:

  57 54 47 4C

- Write 4 Bytes in 3nd record:

  00 00 00 00

- Select Security File 0xFF03
- Write 8 Bytes in 1st record (PIN IC):

  48 3F 58 0E EB 0F A4 E4

- Write 8 Bytes in 2nd record ? (PIN To check):

41 43 4F 53 54 45 53 54

- Write 8 Bytes in 3nd record (K_C):

0D 4F 11 CD 53 C1 BB 45

- Write 8 Bytes in 4th record (K_T):

E3 D4 45 B0 29 46 33 6C

- Write 8 Bytes in 5th record (RANDOM GENERATOR SEED – ANY VALUE WILL DO):

11 22 33 44 11 22 33 44

- Write 8 Bytes in 6th record (PIN ACS1):

EE 3E 50 5E 35 AF FA D6

- Write 8 Bytes in 7th record (PIN ACS2):

41 43 4F 53 54 45 53 54

- Write 8 Bytes in 8th record (PIN ACS3):

41 43 4F 53 54 45 53 54

- Write 8 Bytes in 9th record (PIN ACS4):

41 43 4F 53 54 45 53 54

- Write 8 Bytes in 10th record (PIN ACS5):

41 43 4F 53 54 45 53 54

- Select User File Management File 0xFF04 (TO READ FROM EXISTING SIM CARD)
- Write 6 Bytes in 1st record:

20 03 82 82 F0 00

- Write 6 Bytes in 2nd record:

04 08 82 82 F0 01

- Write 6 Bytes in 3nd record:

F8 06 82 82 F0 02

- Lock Perso
- Select Manufacturer File 0xFF01
- Write 8 Bytes in 1st record:

00 00 00 00 00 00 00 00

(0x*80* =***1***0000000$_2$??)

- Reset

Card is personalized

Data files 0xF0 00 , 0xF0 01 and 0xF0 02 have been created

- Do Mutual Authentication
- Verify IC
- VERIFY ACS1 PINs
- Write to data files
- Select file 0xF000
- Write 4 bytes in 1st record:
- Select file 0xF000
- Write 20 bytes in 1st record:

  6D 6F 74 6F 72 20 63 69 74 79 20 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

- Write 20 bytes in 2nd record:
- 57 6F 72 6C 64 20 54 6F 75 63 68 20 47 61 6D 69
  6E 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00
- Write 20 bytes in 3nd record:
- 5E 17 AA 21 A1 31 D8 23 CE 1A 4B 71 29 0F 3D 17
  E4 48 77 49 99 6D 50 1C C3 58 D7 3B C8 32 1C 71
- Select file 0xF001
- Write 4 bytes in 1st record:

  04 00 00 00

- Write 4 Bytes in 2nd record:

  04 00 00 00

- Write 4 Bytes in 3nd record:

  02 00 00 00

- Write 4 Bytes in 4th record:

  D1 1B 01 00

- Write 4 Bytes in 5th record:

  DD 07 00 00

- Write 4 Bytes in 6th record:

  01 00 00 00

- Write 4 Bytes in 7th record:

```
12 00 00 00
```

- Write 4 Bytes in 8th record:

```
08 02 00 00
```

- Select file 0xF002
- Write 0xF8 bytes in 1st record:

```
47 1E 00 00 02 00 00 00 41 41 00 02 80 25 4B 00
42 42 00 02 80 25 4B 00 42 4C 46 02 80 25 4B 00
43 4B 00 02 80 25 4B 00 43 4C 43 02 80 25 4B 00
43 4C 44 02 80 25 4B 00 43 4E 4C 02 80 25 4B 00
43 52 43 02 80 25 4B 00 46 4C 46 02 80 25 4B 00
46 54 53 02 80 25 4B 00 47 49 47 02 80 25 4B 00
47 53 44 02 80 25 4B 00 4A 4F 42 02 80 25 4B 00
4C 42 00 02 80 25 4B 00 4C 4E 46 02 80 25 4B 00
4D 4D 00 02 80 25 4B 00 4D 4E 52 02 80 25 4B 00
4D 54 4D 02 80 25 4B 00 50 45 4E 02 80 25 4B 00
52 48 44 02 80 25 4B 00 52 4E 52 02 80 25 4B 00
52 4E 57 02 80 25 4B 00 52 52 00 02 80 25 4B 00
53 42 4B 02 80 25 4B 00 53 43 00 02 80 25 4B 00
53 4F 53 02 80 25 4B 00 54 4A 4D 02 80 25 4B 00
55 42 4B 02 80 25 4B 00 56 43 4C 02 80 25 4B 00
57 54 52 02 80 25 4B 00
```

- Write 0xF8 bytes in 2nd record:

```
47 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00

- Write 0xF8 bytes in 3->6th record:
  same data as record 2

4. **End of SIM Creation**

5. FileStructure

5.1. Template for System file 0xFF02

a) Record 1

0x04 bytes:

57 54 47 4C

5.2. Template for data file 0xF000

a) Record 0

6D 6F 74 6F 72 20 63 69 74 79 20 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

b) Record 1

57 6F 72 6C 64 20 54 6F 75 63 68 20 47 61 6D 69
6E 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00

c) Record 2

5E 17 AA 21 A1 31 D8 23 CE 1A 4B 71 29 0F 3D 17
E4 48 77 49 99 6D 50 1C C3 58 D7 3B C8 32 1C 71

5.3. Template for data file 0xF001

a) Record 0

0x04 bytes:

04 00 00 00

b) Record 1

0x04 bytes:

```
04 00 00 00
```

c) Record 2

0x04 bytes:

```
02 00 00 00
```

d) Record 3

0x04 bytes:

```
D1 1B 01 00
```

e) Record 4

0x04 bytes:

```
DD 07 00 00
```

f) Record 5

0x04 bytes:

```
01 00 00 00
```

g) Record 6

0x04 bytes:

```
12 00 00 00
```

h) Record 7

0x04 bytes:

```
08 02 00 00
```

5.4. Template for data file 0xF002

a) Record 0

0xF8 bytes:

```
47 1E 00 00 01 00 00 00 41 41 00 02 00 1A 4F 00
 42 42 00 02 00 1A 4F 00 42 4C 46 02 00 1A 4F 00
 43 4B 00 02 00 1A 4F 00 43 4C 43 02 00 1A 4F 00
```

```
43 4C 44 02 00 1A 4F 00 43 4E 4C 02 00 1A 4F 00
43 52 43 02 00 1A 4F 00 46 4C 46 02 00 1A 4F 00
46 54 53 02 00 1A 4F 00 47 49 47 02 00 1A 4F 00
47 53 44 02 00 1A 4F 00 4A 4F 42 02 00 1A 4F 00
4C 42 00 02 00 1A 4F 00 4C 4E 46 02 00 1A 4F 00
4D 4D 00 02 00 1A 4F 00 4D 4E 52 02 00 1A 4F 00
4D 54 4D 02 00 1A 4F 00 50 45 4E 02 00 1A 4F 00
52 48 44 02 00 1A 4F 00 52 4E 52 02 00 1A 4F 00
52 4E 57 02 00 1A 4F 00 52 52 00 02 00 1A 4F 00
53 42 4B 02 00 1A 4F 00 53 43 00 02 00 1A 4F 00
53 4F 53 02 00 1A 4F 00 54 4A 4D 02 00 1A 4F 00
55 42 4B 02 00 1A 4F 00 56 43 4C 02 00 1A 4F 00
57 54 52 02 00 1A 4F 00
```

b) Record 1

0xF8 bytes:

```
47 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00
```

Record 2

Same as record1

Record 3

Same as record1

c) Record 4

Same as record1

d) Record 5

Same as record1

6. Tool for personalization

6.1. APDU Script

Apdu script will be used with ACS APDU tool script execution

[1] ACOS3 Reference Manual