DESFire EV1 Communication Examples

Brought from: https://github.com/sotechcllc/RFDoorLock

What you find here is a follow up for Ridrix Blog.
Sadly his blog is the only place in internet where you find some Desfire data examples.
A lot of people wrote their problems there while developing code for Desfire cards.
But mostly when they solved their problem they were too LAZY to post the solution.
How can people be so egoistic that they ask for help in a blog but when they found the solution the do NOT post it?

After spending several weeks with Desfire EV1 development I decided to post some examples for all those who need input data for checking the complex cryprography.

Here you find some Debug output from the most important Desfire EV1 operations.
Currently you cannot find this information in internet.
This data is extremely helpfull when you develop a Desfire EV1 project.
If I would have had these examples I would have saved a LOT of time developing my code.

Even if you have the Desfire EV1 documentation, you will need more than that.
A documentation is only theory. But what is the cause when your card returns an Authentication Error or an Integrity Error or an unexpected CMAC?
Is the Session key OK ?
Is CBC working in the correct mode ?
Is the CMAC calculated correctly ?
Is the CRC32 correct ?
Is the IV of the session key correct before / after a function call ?

Without examples you are completely lost.

Pitfalls for ISO and AES authenticated sessions

In ISO and AES mode EVERY encryption/decryption goes through **CBC**.
The **IV** of the session key is reset to zero only ONCE when the key is created after authentication.
The IV of the authentication key is reset only ONCE when authentication starts.

During authentication:
1. Random B is received from the card with RECEIVE + DECIPHER
2. Random AB is sent to the card with SEND + ENCIPHER
3. Random A is received with RECEIVE + DECIPHER

The **CMAC** is a copy of the IV of the session key.
The CMAC must mostly be calculated for data sent to the card and for data returned from the card.
But all commands that do a CBC encryption (e.g. ChangeKeySettings) differ from that scheme.
Commands that send/receive multiple frames (e.g. GetApplicationIDs) must calculate the CMAC over the data of all frames that have been sent/received (not including the 0xAF status byte).
For TX data the CMAC is calculated over the command byte + all parameter bytes.
For RX data the CMAC is calculated over all response bytes + the last status byte (always 00 = Success) that must be appended at the end!

The authentication is **invalidated**:
- when an error occures (status != 00 and != AF),
- when SelectApplication is executed,
- after the same key has been changed that was used for authentication,
- when another card comes into the RF field (don't forget to reset your variables).
In these cases the session key is no longer valid and so a CMAC must not be calculated.

The **CRC32** of the new key is calculated only over the key data itself.
The CRC32 of the cryptogram is calculated over command, key number and the not yet encrypted cryptogram.

The following debug output has been generated by my code running in a Teensy 3.2 with a PN532 board from Adafruit.
For further details see my **source code**.
The source code has been written for Arduino/Teensy, but it has been designed **multiplatform** so that it requires only changing a few lines to compile it on Visual Studio, Linux or other platforms.

Red: In the following example all keys have key version 0x10, except the default keys full of zeroes which have version 0x00.
Green: Data sent to the card (first byte = command).
Blue: Data received from the card (first byte = status).
Magenta: The PN532 INDATAEXCHANGE command (0x40) and it's response (0x41).
Black: The other bytes sent/received are the framing bytes of the PN532.

Selftest

```
*** SelectApplication(0x000000)
Sending:  00 00 FF 07 F9 <D4 40 01 5A 00 00 00> 91 00
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00

*** GetKeyVersion()
Sending:  00 00 FF 05 FB <D4 40 01 64 00> 87 00
Response: 00 00 FF 05 FB <D5 41 00 00 00> EA 00 AA AA AA AA AA AA AA AA
Version: 0x00

*** Authenticate(KeyNo= 0, Key= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 0C F4 <D5 41 00 AF 5D 99 4C E0 85 F2 40 89> D9 00 AA AA AA AA AA AA AA AA
* RndB_enc:  5D 99 4C E0 85 F2 40 89
* RndB:      4F D1 B7 59 42 A8 B8 E1
* RndB_rot:  D1 B7 59 42 A8 B8 E1 4F
* RndA:      84 9B 36 C5 F8 BF 4A 09
* RndAB:     84 9B 36 C5 F8 BF 4A 09 D1 B7 59 42 A8 B8 E1 4F
* RndAB_enc: 21 D0 AD 5F 2F D9 74 54 A7 46 CC 80 56 7F 1B 1C
Sending:  00 00 FF 14 EC <D4 40 01 AF 21 D0 AD 5F 2F D9 74 54 A7 46 CC 80 56 7F 1B 1C> 2A 00
Response: 00 00 FF 0C F4 <D5 41 00 00 91 3C 6D ED 84 22 1C 41> C0 00
* RndA_enc:  91 3C 6D ED 84 22 1C 41
* RndA_dec:  9B 36 C5 F8 BF 4A 09 84
* RndA_rot:  9B 36 C5 F8 BF 4A 09 84
* SessKey:   84 9A 36 C4 4E D0 B6 58 84 9A 36 C4 4E D0 B6 58 (DES)

NOTE: This session key is a simple DES key where the first 8 bytes and the second 8 bytes are equal.
NOTE: DES encryption ignores bit 0 of all bytes. In these bits the 8 bit key version is stored.

*** GetCardVersion()
TX CMAC:  50 20 EC 82 60 86 DF 12
Sending:  00 00 FF 04 FC <D4 40 01 60> 8B 00
Response: 00 00 FF 0B F5 <D5 41 00 AF 04 01 01 01 00 1A 05> 15 00 AA AA AA AA AA AA AA AA
```

```
Sending:  00 00 FF 04 FC <D4 40 01 AF> 3C 00
Response: 00 00 FF 0B F5 <D5 41 00 AF 04 01 01 01 04 1A 05> 11 00 AA AA AA AA AA AA AA AA
Sending:  00 00 FF 04 FC <D4 40 01 AF> 3C 00
Response: 00 00 FF 1A E6 <D5 41 00 00 04 06 3F 72 63 34 80 BA 45 19 E3 20 49 13 CD C8 10 BA FA 40 17 59> 98 00
RX CMAC:  CD C8 10 BA FA 40 17 59
--- Desfire Card Details ---
Hardware Version: 1.0
Software Version: 1.4
EEPROM size:      8192 byte
Production:       week 49, year 2013
UID no:           04 06 3F 72 63 34 80
Batch no:         BA 45 19 E3 20

*** FormatCard()
TX CMAC:  0D 89 CA 4B FB E6 90 72
Sending:  00 00 FF 04 FC <D4 40 01 FC> EF 00
Response: 00 00 FF 0C F4 <D5 41 00 00 9C 2C 81 3A 06 5C 45 F7> C9 00
RX CMAC:  9C 2C 81 3A 06 5C 45 F7

*** CreateApplication(App= 0x00DE16, KeyCount= 2, Type= 3DES)
TX CMAC:  EE E9 BE 10 51 A4 06 F3
Sending:  00 00 FF 09 F7 <D4 40 01 CA 16 DE 00 0F 02> 1C 00
Response: 00 00 FF 0C F4 <D5 41 00 00 0A 13 79 B0 1D 85 AD 47> 0E 00
RX CMAC:  0A 13 79 B0 1D 85 AD 47

*** CreateApplication(App= 0x00DE24, KeyCount= 2, Type= 3K3DES)
TX CMAC:  EE 60 B2 1A CA 1A 5B 1A
Sending:  00 00 FF 09 F7 <D4 40 01 CA 24 DE 00 0F 42> CE 00
Response: 00 00 FF 0C F4 <D5 41 00 00 5D 73 AE 52 87 A1 BB E4> 53 00
RX CMAC:  5D 73 AE 52 87 A1 BB E4

*** CreateApplication(App= 0x00AE16, KeyCount= 2, Type= AES)
TX CMAC:  75 F0 4D 6F F8 74 2D CA
Sending:  00 00 FF 09 F7 <D4 40 01 CA 16 AE 00 0F 82> CC 00
Response: 00 00 FF 0C F4 <D5 41 00 00 3B 68 D7 2A 3B E0 D2 0C> 4D 00
RX CMAC:  3B 68 D7 2A 3B E0 D2 0C

*** CreateApplication(App= 0xAABBCC, KeyCount= 1, Type= 3DES)
TX CMAC:  CD DE 90 47 66 39 58 1F
Sending:  00 00 FF 09 F7 <D4 40 01 CA CC BB AA 0F 01> E0 00
Response: 00 00 FF 0C F4 <D5 41 00 00 F1 1A C0 73 8E F8 38 78> 76 00
RX CMAC:  F1 1A C0 73 8E F8 38 78

*** GetApplicationIDs()
TX CMAC:  D0 56 6D 1B DB 78 8A C3
Sending:  00 00 FF 04 FC <D4 40 01 6A> 81 00
Response: 00 00 FF 18 E8 <D5 41 00 00 16 DE 00 24 DE 00 16 AE 00 CC BB AA 27 39 15 4E 26 30 D6 50> C0 00 AA AA AA AA AA AA AA AA AA AA A
RX CMAC:  27 39 15 4E 26 30 D6 50
Application  0: 0x00DE16
Application  1: 0x00DE24
Application  2: 0x00AE16
Application  3: 0xAABBCC

*** DeleteApplication(0xAABBCC)
TX CMAC:  07 C6 E3 9E 38 77 96 79
Sending:  00 00 FF 07 F9 <D4 40 01 DA CC BB AA> E0 00
Response: 00 00 FF 0C F4 <D5 41 00 00 A9 AF 19 05 22 92 F6 62> 68 00
RX CMAC:  A9 AF 19 05 22 92 F6 62

*** GetApplicationIDs()
TX CMAC:  D9 46 56 FD BE 75 AD 08
Sending:  00 00 FF 04 FC <D4 40 01 6A> 81 00
Response: 00 00 FF 15 EB <D5 41 00 00 16 DE 00 24 DE 00 16 AE 00 52 0E 51 E0 0A F0 6D 5E> DA 00 AA AA AA AA AA AA AA AA AA AA AA AA AA A
RX CMAC:  52 0E 51 E0 0A F0 6D 5E
Application  0: 0x00DE16
Application  1: 0x00DE24
Application  2: 0x00AE16

*** SelectApplication(0x00DE16)
Sending:  00 00 FF 07 F9 <D4 40 01 5A 16 DE 00> 9D 00
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00

*** Authenticate(KeyNo= 0, Key= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 0C F4 <D5 41 00 AF 84 76 D1 CF 30 24 B7 C7> CF 00 AA AA AA AA AA AA AA AA
* RndB_enc:  84 76 D1 CF 30 24 B7 C7
* RndB:      3B 3D FE 62 81 64 BF DA
* RndB_rot:  3D FE 62 81 64 BF DA 3B
* RndA:      49 EC 63 DE CD E0 07 72
* RndAB:     49 EC 63 DE CD E0 07 72 3D FE 62 81 64 BF DA 3B
* RndAB_enc: DA C6 7A B7 43 76 3D C9 FA F8 A0 AE 50 4E 80 C5
Sending:  00 00 FF 14 EC <D4 40 01 AF DA C6 7A B7 43 76 3D C9 FA F8 A0 AE 50 4E 80 C5> 89 00
Response: 00 00 FF 0C F4 <D5 41 00 00 13 E9 E4 FA 43 88 BF 16> 70 00
* RndA_enc:  13 E9 E4 FA 43 88 BF 16
* RndA_dec:  EC 63 DE CD E0 07 72 49
* RndA_rot:  EC 63 DE CD E0 07 72 49
* SessKey:   48 EC 62 DE 3A 3C FE 62 48 EC 62 DE 3A 3C FE 62 (DES)

*** GetKeySettings()
TX CMAC:  D9 C6 E0 63 74 01 B7 52
Sending:  00 00 FF 04 FC <D4 40 01 45> A6 00
Response: 00 00 FF 0E F2 <D5 41 00 00 0F 02 25 DD 8D 77 31 B1 CF D5> 4D 00
RX CMAC:  25 DD 8D 77 31 B1 CF D5
Settings: 0x0F, KeyCount: 2, KeyType: 3DES

*** ChangeKeySettings(0x0D)
* Sess Key IV: 25 DD 8D 77 31 B1 CF D5
* New Settg:   0D ED 09 40 1E 00 00 00
* Settg_enc:   27 88 28 05 FC 3F D4 9D
Sending:  00 00 FF 0C F4 <D4 40 01 54 27 88 28 05 FC 3F D4 9D> 0F 00
Response: 00 00 FF 0C F4 <D5 41 00 00 A6 28 37 83 74 27 0A CD> F0 00
RX CMAC:  A6 28 37 83 74 27 0A CD

*** GetKeySettings()
```

```
TX CMAC:  03 0B A6 6F E3 62 06 00
Sending:  00 00 FF 04 FC <D4 40 01 45> A6 00
Response: 00 00 FF 0E F2 <D5 41 00 00 0D 02 61 3F B2 D3 F4 53 D2 E4> B9 00
RX CMAC:  61 3F B2 D3 F4 53 D2 E4
Settings: 0x0D, KeyCount: 2, KeyType: 3DES

------------------------------------------------------------
---------------------- 2K3DES ------------------------------
------------------------------------------------------------

*** SelectApplication(0x00DE16)
Sending:  00 00 FF 07 F9 <D4 40 01 5A 16 DE 00> 9D 00
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00

*** Authenticate(KeyNo= 0, Key= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 0C F4 <D5 41 00 AF DE 50 F9 23 10 CA F5 A5> 7D 00 AA AA AA AA AA AA AA AA
* RndB_enc:  DE 50 F9 23 10 CA F5 A5
* RndB:      4C 64 7E 56 72 E2 A6 51
* RndB_rot:  64 7E 56 72 E2 A6 51 4C
* RndA:      C9 6C E3 5E 4D 60 87 F2
* RndAB:     C9 6C E3 5E 4D 60 87 F2 64 7E 56 72 E2 A6 51 4C
* RndAB_enc: E0 06 16 66 87 04 D5 54 9C 8D 6A 13 A0 F8 FC ED
Sending:  00 00 FF 14 EC <D4 40 01 AF E0 06 16 66 87 04 D5 54 9C 8D 6A 13 A0 F8 FC ED> FF 00
Response: 00 00 FF 0C F4 <D5 41 00 00 1D 9D 29 54 69 7D E7 60> 86 00
* RndA_enc:  1D 9D 29 54 69 7D E7 60
* RndA_dec:  6C E3 5E 4D 60 87 F2 C9
* RndA_rot:  6C E3 5E 4D 60 87 F2 C9
* SessKey:   C8 6C E2 5E 4C 64 7E 56 C8 6C E2 5E 4C 64 7E 56 (DES)

*** ChangeKey(KeyNo= 0)
* SessKey IV:  00 00 00 00 00 00 00 00
* New Key:     00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 (2K3DES)
* CRC Crypto:  0x5001FFC5
* Cryptogram:  00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 C5 FF 01 50 00 00 00 00
* CryptogrEnc: BE DE 0F C6 ED 34 7D CF 0D 51 C7 17 DF 75 D9 7D 2C 5A 2B A6 CA C7 47 9D
Sending:  00 00 FF 1D E3 <D4 40 01 C4 00 BE DE 0F C6 ED 34 7D CF 0D 51 C7 17 DF 75 D9 7D 2C 5A 2B A6 CA C7 47 9D> 97 00
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00 AA AA AA AA AA AA AA AA

*** Authenticate(KeyNo= 0, Key= 00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 (2K3DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 0C F4 <D5 41 00 AF B2 95 57 99 26 15 5A E3> 8C 00 AA AA AA AA AA AA AA AA
* RndB_enc:  B2 95 57 99 26 15 5A E3
* RndB:      BC D8 29 97 47 33 2D AF
* RndB_rot:  D8 29 97 47 33 2D AF BC
* RndA:      53 0E 3D 90 F7 A2 01 C4
* RndAB:     53 0E 3D 90 F7 A2 01 C4 D8 29 97 47 33 2D AF BC
* RndAB_enc: 70 F3 49 74 0C 94 5D AE 15 9B A9 FE DB CC 46 1A
Sending:  00 00 FF 14 EC <D4 40 01 AF 70 F3 49 74 0C 94 5D AE 15 9B A9 FE DB CC 46 1A> 13 00
Response: 00 00 FF 0C F4 <D5 41 00 00 B8 FD 7F E5 6B 24 1F C4> 5F 00
* RndA_enc:  B8 FD 7F E5 6B 24 1F C4
* RndA_dec:  0E 3D 90 F7 A2 01 C4 53
* RndA_rot:  0E 3D 90 F7 A2 01 C4 53
* SessKey:   52 0E 3C 90 BC D8 28 96 F6 A2 00 C4 46 32 2C AE (2K3DES)

*** ChangeKey(KeyNo= 0)
* SessKey IV:  00 00 00 00 00 00 00 00
* New Key:     10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 (2K3DES)
* CRC Crypto:  0x630E72C9
* Cryptogram:  10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 C9 72 0E 63 00 00 00 00
* CryptogrEnc: 94 E4 F7 09 DC 2A 2B 07 55 26 10 A1 96 6E 5C 49 EC 90 F6 16 ED EC A5 5B
Sending:  00 00 FF 1D E3 <D4 40 01 C4 00 94 E4 F7 09 DC 2A 2B 07 55 26 10 A1 96 6E 5C 49 EC 90 F6 16 ED EC A5 5B> 41 00
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00 AA AA AA AA AA AA AA AA

*** Authenticate(KeyNo= 0, Key= 10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 (2K3DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 0C F4 <D5 41 00 AF 94 14 81 9C C8 BB 62 C3> CE 00 AA AA AA AA AA AA AA AA
* RndB_enc:  94 14 81 9C C8 BB 62 C3
* RndB:      A4 0E 79 E0 F5 2F 63 AF
* RndB_rot:  0E 79 E0 F5 2F 63 AF A4
* RndA:      DD B0 97 C2 A1 E4 7B 96
* RndAB:     DD B0 97 C2 A1 E4 7B 96 0E 79 E0 F5 2F 63 AF A4
* RndAB_enc: 93 7E 6B 18 54 A6 D9 2E 0F D9 75 D9 90 90 01 E8
Sending:  00 00 FF 14 EC <D4 40 01 AF 93 7E 6B 18 54 A6 D9 2E 0F D9 75 D9 90 90 01 E8> 68 00
Response: 00 00 FF 0C F4 <D5 41 00 00 E0 55 D1 1D D9 53 50 60> EB 00
* RndA_enc:  E0 55 D1 1D D9 53 50 60
* RndA_dec:  B0 97 C2 A1 E4 7B 96 DD
* RndA_rot:  B0 97 C2 A1 E4 7B 96 DD
* SessKey:   DC B0 96 C2 A4 0E 78 E0 A0 E4 7A 96 F4 2E 62 AE (2K3DES)

*** GetKeyVersion()
TX CMAC:  8C B2 4F 61 B8 14 A9 56
Sending:  00 00 FF 05 FB <D4 40 01 64 00> 87 00
Response: 00 00 FF 0D F3 <D5 41 00 00 10 33 45 AA 95 F2 D9 56 CF> 33 00
RX CMAC:  33 45 AA 95 F2 D9 56 CF
Version: 0x10

*** ChangeKey(KeyNo= 0)
* SessKey IV:  33 45 AA 95 F2 D9 56 CF
* New Key:     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (DES)
* CRC Crypto:  0x87AA7155
* Cryptogram:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 71 AA 87 00 00 00 00
* CryptogrEnc: FC 9E 20 FD 77 19 1E 2A AB 0C FD 53 D9 99 99 84 BC 59 E8 86 BF EB 42 D0
Sending:  00 00 FF 1D E3 <D4 40 01 C4 00 FC 9E 20 FD 77 19 1E 2A AB 0C FD 53 D9 99 99 84 BC 59 E8 86 BF EB 42 D0> C3 00
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00 AA AA AA AA AA AA AA AA

*** Authenticate(KeyNo= 0, Key= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 0C F4 <D5 41 00 AF 53 A6 70 D7 8C 0D FF D6> 8D 00 AA AA AA AA AA AA AA AA
* RndB_enc:  53 A6 70 D7 8C 0D FF D6
* RndB:      CB E9 52 5F B7 DF 5C 3A
* RndB_rot:  E9 52 5F B7 DF 5C 3A CB
* RndA:      CB A6 75 E8 EF BA B9 9C
* RndAB:     CB A6 75 E8 EF BA B9 9C E9 52 5F B7 DF 5C 3A CB
```

```
* RndAB_enc: B3 08 40 8B 57 5A 20 25 25 3D 49 D6 93 CC C2 9C
Sending:  00 00 FF 14 EC <D4 40 01 AF B3 08 40 8B 57 5A 20 25 25 3D 49 D6 93 CC C2 9C> 82 00
Response: 00 00 FF 0C F4 <D5 41 00 00 52 5B B0 1E 5B 70 B7 94> 59 00
* RndA_enc:  52 5B B0 1E 5B 70 B7 94
* RndA_dec:  A6 75 E8 EF BA B9 9C CB
* RndA_rot:  A6 75 E8 EF BA B9 9C CB
* SessKey:   CA A6 74 E8 CA E8 52 5E CA A6 74 E8 CA E8 52 5E (DES)

*** ChangeKey(KeyNo= 1)
* SessKey IV:  00 00 00 00 00 00 00 00
* New Key:     00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 (2K3DES)
* Cur Key:     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (DES)
* CRC Crypto:  0xD7A73486
* CRC New Key: 0xC4EF3A3A
* Cryptogram:  00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 86 34 A7 D7 3A 3A EF C4
* CryptogrEnc: 4E B6 69 E4 8D CA 58 47 49 54 2E 1B E8 9C B4 C7 84 5A 38 C5 7D 19 DE 59
Sending:  00 00 FF 1D E3 <D4 40 01 C4 01 4E B6 69 E4 8D CA 58 47 49 54 2E 1B E8 9C B4 C7 84 5A 38 C5 7D 19 DE 59> 52 00
Response: 00 00 FF 0C F4 <D5 41 00 00 2E AD 04 DC F1 21 E0 FE> 3F 00
RX CMAC:  2E AD 04 DC F1 21 E0 FE

*** ChangeKey(KeyNo= 1)
* SessKey IV:  2E AD 04 DC F1 21 E0 FE
* New Key:     10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 (2K3DES)
* Cur Key:     00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 (2K3DES)
* CRC Crypto:  0x3303371A
* CRC New Key: 0xF7E0B736
* Cryptogram:  10 08 00 18 70 68 20 38 D0 C8 C0 D8 C0 D8 10 08 1A 37 03 33 36 B7 E0 F7
* CryptogrEnc: FA 7B EF A6 78 2C 93 E8 D6 9C F7 35 2C FD 33 DF 5B C8 AC 4F BA 49 06 FC
Sending:  00 00 FF 1D E3 <D4 40 01 C4 01 FA 7B EF A6 78 2C 93 E8 D6 9C F7 35 2C FD 33 DF 5B C8 AC 4F BA 49 06 FC> 01 00
Response: 00 00 FF 0C F4 <D5 41 00 00 CB 0A 50 64 05 51 28 93> 50 00
RX CMAC:  CB 0A 50 64 05 51 28 93

*** Authenticate(KeyNo= 1, Key= 10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 (2K3DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 01> D0 00
Response: 00 00 FF 0C F4 <D5 41 00 AF 87 D3 AC 1E 09 57 0A AD> 00 00 AA AA AA AA AA AA AA AA
* RndB_enc:  87 D3 AC 1E 09 57 0A AD
* RndB:      60 8B EC D6 0A 7E 49 34
* RndB_rot:  8B EC D6 0A 7E 49 34 60
* RndA:      F7 A2 01 C4 DB 76 05 38
* RndAB:     F7 A2 01 C4 DB 76 05 38 8B EC D6 0A 7E 49 34 60
* RndAB_enc: D8 2E 8C 09 26 31 FE 15 25 7D 67 62 9F C9 29 D5
Sending:  00 00 FF 14 EC <D4 40 01 AF D8 2E 8C 09 26 31 FE 15 25 7D 67 62 9F C9 29 D5> 66 00
Response: 00 00 FF 0C F4 <D5 41 00 00 C4 13 2C EF 0D 13 F8 12> CE 00
* RndA_enc:  C4 13 2C EF 0D 13 F8 12
* RndA_dec:  A2 01 C4 DB 76 05 38 F7
* RndA_rot:  A2 01 C4 DB 76 05 38 F7
* SessKey:   F6 A2 00 C4 60 8A EC D6 DA 76 04 38 0A 7E 48 34 (2K3DES)

------------------------------------------------------------
---------------------- 3K3DES ------------------------------
------------------------------------------------------------

*** SelectApplication(0x00DE24)
Sending:  00 00 FF 07 F9 <D4 40 01 5A 24 DE 00> 8F 00
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00

*** Authenticate(KeyNo= 0, Key= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (3K3DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 14 EC <D5 41 00 AF BC 1C 57 0B C9 48 15 61 87 13 23 64 E4 DC E1 76> 42 00
* RndB_enc:  BC 1C 57 0B C9 48 15 61 87 13 23 64 E4 DC E1 76
* RndB:      31 6E 6D 76 A4 49 F9 25 BA 30 4F B2 65 36 56 A2
* RndB_rot:  6E 6D 76 A4 49 F9 25 BA 30 4F B2 65 36 56 A2 31
* RndA:      36 C5 F8 BF 4A 09 AC 23 9E 8D A0 C7 32 51 D4 AB
* RndAB:     36 C5 F8 BF 4A 09 AC 23 9E 8D A0 C7 32 51 D4 AB 6E 6D 76 A4 49 F9 25 BA 30 4F B2 65 36 56 A2 31
* RndAB_enc: DD DC 9A 77 59 7F 03 A4 0C 7F AA 36 2F 45 A8 EA DB E4 6A 11 5D 98 19 8C BF 36 A6 E5 1B 39 D8 7C
Sending:  00 00 FF 24 DC <D4 40 01 AF DD DC 9A 77 59 7F 03 A4 0C 7F AA 36 2F 45 A8 EA DB E4 6A 11 5D 98 19 8C BF 36 A6 E5 1B 39 D8 7C> 8
Response: 00 00 FF 14 EC <D5 41 00 00 72 44 D9 35 ED 9A 13 06 CD 8C 84 1A 7C 1D E3 9A> 79 00
* RndA_enc:  72 44 D9 35 ED 9A 13 06 CD 8C 84 1A 7C 1D E3 9A
* RndA_dec:  C5 F8 BF 4A 09 AC 23 9E 8D A0 C7 32 51 D4 AB 36
* RndA_rot:  C5 F8 BF 4A 09 AC 23 9E 8D A0 C7 32 51 D4 AB 36
* SessKey:   36 C4 F8 BE 30 6E 6C 76 AC 22 9E 8C F8 24 BA 30 32 50 D4 AA 64 36 56 A2 (3K3DES)

*** ChangeKey(KeyNo= 0)
* SessKey IV:  00 00 00 00 00 00 00 00
* New Key:     00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 70 60 50 40 30 20 10 00 (3K3DES)
* CRC Crypto:  0xA2003ED6
* Cryptogram:  00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 70 60 50 40 30 20 10 00 D6 3E 00 A2 00 00 00 00
* CryptogrEnc: F4 F8 65 F3 18 CB 9D E8 0B 2B 16 51 45 02 1F 4F 3A FE F1 24 4F EA 42 FC 99 77 26 FD E7 50 74 1D
Sending:  00 00 FF 25 DB <D4 40 01 C4 00 F4 F8 65 F3 18 CB 9D E8 0B 2B 16 51 45 02 1F 4F 3A FE F1 24 4F EA 42 FC 99 77 26 FD E7 50 74 1D
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00 AA AA AA AA AA AA AA AA

*** Authenticate(KeyNo= 0, Key= 00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 70 60 50 40 30 20 10 00 (3K3DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 14 EC <D5 41 00 AF FA 2F B9 A1 7B 35 9D 03 4D F3 EB 1C 41 79 20 7E> C9 00
* RndB_enc:  FA 2F B9 A1 7B 35 9D 03 4D F3 EB 1C 41 79 20 7E
* RndB:      F4 D6 56 42 AE EB 3D 12 FB 8A C6 FE 46 CE 7A 2F
* RndB_rot:  D6 56 42 AE EB 3D 12 FB 8A C6 FE 46 CE 7A 2F F4
* RndA:      03 FE 6D 00 A7 92 31 34 8B 66 35 A8 AF 7A 79 5C
* RndAB:     03 FE 6D 00 A7 92 31 34 8B 66 35 A8 AF 7A 79 5C D6 56 42 AE EB 3D 12 FB 8A C6 FE 46 CE 7A 2F F4
* RndAB_enc: 7B F9 E1 AC 2D 7C 28 36 11 2E 64 2D 39 8F BA EF 5C A6 1C C3 A6 29 FA 8B D5 2F 43 F9 D9 31 C0 43
Sending:  00 00 FF 24 DC <D4 40 01 AF 7B F9 E1 AC 2D 7C 28 36 11 2E 64 2D 39 8F BA EF 5C A6 1C C3 A6 29 FA 8B D5 2F 43 F9 D9 31 C0 43> 7
Response: 00 00 FF 14 EC <D5 41 00 00 1E 30 51 B5 9B A3 1E 4C EF 64 BB E8 72 1B 7B D6> 1A 00
* RndA_enc:  1E 30 51 B5 9B A3 1E 4C EF 64 BB E8 72 1B 7B D6
* RndA_dec:  FE 6D 00 A7 92 31 34 8B 66 35 A8 AF 7A 79 5C 03
* RndA_rot:  FE 6D 00 A7 92 31 34 8B 66 35 A8 AF 7A 79 5C 03
* SessKey:   02 FE 6C 00 F4 D6 56 42 30 34 8A 66 3C 12 FA 8A AE 7A 78 5C 46 CE 7A 2E (3K3DES)

*** ChangeKey(KeyNo= 0)
* SessKey IV:  00 00 00 00 00 00 00 00
* New Key:     10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 90 98 A0 A8 B0 B8 C0 C8 (3K3DES)
* CRC Crypto:  0xD810C41E
* Cryptogram:  10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 90 98 A0 A8 B0 B8 C0 C8 1E C4 10 D8 00 00 00 00
* CryptogrEnc: 0A 9B E7 7E 72 03 CD 8D 3E B1 3D 5F 2C 1F 11 FF E8 97 EC AC 1F E0 54 CE 42 87 68 5F 3C E2 16 2E
Sending:  00 00 FF 25 DB <D4 40 01 C4 00 0A 9B E7 7E 72 03 CD 8D 3E B1 3D 5F 2C 1F 11 FF E8 97 EC AC 1F E0 54 CE 42 87 68 5F 3C E2 16 2E
```

```
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00 AA AA AA AA AA AA AA AA

*** Authenticate(KeyNo= 0, Key= 10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 90 98 A0 A8 B0 B8 C0 C8 (3K3DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 14 EC <D5 41 00 AF ED FA C0 76 F7 F7 5F 3F A9 30 D8 36 5A 7C 92 06> 3D 00
* RndB_enc:  ED FA C0 76 F7 F7 5F 3F A9 30 D8 36 5A 7C 92 06
* RndB:      58 14 D2 51 3D 9E C0 66 68 C0 CC 1B 59 23 7A FD
* RndB_rot:  14 D2 51 3D 9E C0 66 68 C0 CC 1B 59 23 7A FD 58
* RndA:      D1 54 2B 86 D5 C8 4F 9A 19 7C B3 EE 9D 70 57 82
* RndAB:     D1 54 2B 86 D5 C8 4F 9A 19 7C B3 EE 9D 70 57 82 14 D2 51 3D 9E C0 66 68 C0 CC 1B 59 23 7A FD 58
* RndAB_enc: B4 F5 26 6D BF 4B F9 39 70 BC 38 6E 94 F4 FA 59 88 4E 94 F9 F1 13 B1 BF B5 A5 4E 5A 1B A0 88 92
Sending:  00 00 FF 24 DC <D4 40 01 AF B4 F5 26 6D BF 4B F9 39 70 BC 38 6E 94 F4 FA 59 88 4E 94 F9 F1 13 B1 BF B5 A5 4E 5A 1B A0 88 92> 6
Response: 00 00 FF 14 EC <D5 41 00 00 65 F4 F5 DA DE 89 E1 2E 24 05 FC E1 4D 5C D7 98> 2E 00
* RndA_enc:  65 F4 F5 DA DE 89 E1 2E 24 05 FC E1 4D 5C D7 98
* RndA_dec:  54 2B 86 D5 C8 4F 9A 19 7C B3 EE 9D 70 57 82 D1
* RndA_rot:  54 2B 86 D5 C8 4F 9A 19 7C B3 EE 9D 70 57 82 D1
* SessKey:   D0 54 2A 86 58 14 D2 50 4E 9A 18 7C C0 66 68 C0 9C 70 56 82 58 22 7A FC (3K3DES)

*** GetKeyVersion()
TX CMAC:  54 BF 79 31 E5 18 1A 08
Sending:  00 00 FF 05 FB <D4 40 01 64 00> 87 00
Response: 00 00 FF 0D F3 <D5 41 00 00 10 AD 4A 52 B1 E3 1C C7 41> D9 00
RX CMAC:  AD 4A 52 B1 E3 1C C7 41
Version: 0x10

*** ChangeKey(KeyNo= 0)
* SessKey IV:  AD 4A 52 B1 E3 1C C7 41
* New Key:     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (3K3DES)
* CRC Crypto:  0xEC987837
* Cryptogram:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 37 78 98 EC 00 00 00 00
* CryptogrEnc: E6 D4 F3 40 95 49 F6 38 36 4D 6E 64 69 4E C0 51 D6 08 47 15 9E 10 40 C1 6B 61 36 18 C7 97 F7 07
Sending:  00 00 FF 25 DB <D4 40 01 C4 00 E6 D4 F3 40 95 49 F6 38 36 4D 6E 64 69 4E C0 51 D6 08 47 15 9E 10 40 C1 6B 61 36 18 C7 97 F7 07
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00 AA AA AA AA AA AA AA AA

*** Authenticate(KeyNo= 0, Key= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (3K3DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 14 EC <D5 41 00 AF 8F 31 54 AF A8 6D A5 33 EA BE 28 85 9E 5D 57 42> A2 00
* RndB_enc:  8F 31 54 AF A8 6D A5 33 EA BE 28 85 9E 5D 57 42
* RndB:      E5 94 26 66 6D 90 09 A7 15 8E DE 04 43 6B DA 5E
* RndB_rot:  94 26 66 6D 90 09 A7 15 8E DE 04 43 6B DA 5E E5
* RndA:      02 E1 24 BB D6 E5 98 DF EA 29 4C 43 3E AD 40 E7
* RndAB:     02 E1 24 BB D6 E5 98 DF EA 29 4C 43 3E AD 40 E7 94 26 66 6D 90 09 A7 15 8E DE 04 43 6B DA 5E E5
* RndAB_enc: 1D D9 8B 71 B9 00 61 98 B8 B8 00 43 FF 29 63 86 77 5E D2 C2 DB C8 77 BB D9 52 FD 06 F5 F8 73 61
Sending:  00 00 FF 24 DC <D4 40 01 AF 1D D9 8B 71 B9 00 61 98 B8 B8 00 43 FF 29 63 86 77 5E D2 C2 DB C8 77 BB D9 52 FD 06 F5 F8 73 61> A
Response: 00 00 FF 14 EC <D5 41 00 00 AE CD 47 04 21 0B CA AF E1 53 3D 48 3F BE F3 F8> DE 00
* RndA_enc:  AE CD 47 04 21 0B CA AF E1 53 3D 48 3F BE F3 F8
* RndA_dec:  E1 24 BB D6 E5 98 DF EA 29 4C 43 3E AD 40 E7 02
* RndA_rot:  E1 24 BB D6 E5 98 DF EA 29 4C 43 3E AD 40 E7 02
* SessKey:   02 E0 24 BA E4 94 26 66 98 DE EA 28 08 A6 14 8E 3E AC 40 E6 42 6A DA 5E (3K3DES)

*** ChangeKey(KeyNo= 1)
* SessKey IV:  00 00 00 00 00 00 00 00
* New Key:     00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 70 60 50 40 30 20 10 00 (3K3DES)
* Cur Key:     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (3K3DES)
* CRC Crypto:  0x078BAED8
* CRC New Key: 0x12A6733E
* Cryptogram:  00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 70 60 50 40 30 20 10 00 D8 AE 8B 07 3E 73 A6 12
* CryptogrEnc: 01 70 A4 72 13 42 A8 C4 C5 C4 DB 5B A1 F1 AE DF E9 CE F7 3B B4 6B AC 44 B8 C1 14 98 CA 17 D9 45
Sending:  00 00 FF 25 DB <D4 40 01 C4 01 01 70 A4 72 13 42 A8 C4 C5 C4 DB 5B A1 F1 AE DF E9 CE F7 3B B4 6B AC 44 B8 C1 14 98 CA 17 D9 45
Response: 00 00 FF 0C F4 <D5 41 00 00 DC 85 C9 A5 A7 53 B1 7A> F6 00
RX CMAC:  DC 85 C9 A5 A7 53 B1 7A

*** ChangeKey(KeyNo= 1)
* SessKey IV:  DC 85 C9 A5 A7 53 B1 7A
* New Key:     10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 90 98 A0 A8 B0 B8 C0 C8 (3K3DES)
* Cur Key:     00 10 20 31 40 50 60 70 80 90 A0 B0 B0 A0 90 80 70 60 50 40 30 20 10 00 (3K3DES)
* CRC Crypto:  0x330312F1
* CRC New Key: 0x68B689F6
* Cryptogram:  10 08 00 18 70 68 20 38 D0 C8 C0 D8 C0 D8 10 08 E0 F8 F0 E8 80 98 D0 C8 F1 12 03 33 F6 89 B6 68
* CryptogrEnc: E3 E2 DD 9F 1E 2C 8D B5 78 65 2F 78 C3 0C 53 3E AD E1 E6 63 62 5E 0F 74 DD 13 D4 F9 B9 B3 E4 3C
Sending:  00 00 FF 25 DB <D4 40 01 C4 01 E3 E2 DD 9F 1E 2C 8D B5 78 65 2F 78 C3 0C 53 3E AD E1 E6 63 62 5E 0F 74 DD 13 D4 F9 B9 B3 E4 3C
Response: 00 00 FF 0C F4 <D5 41 00 00 FA 14 2D EB A3 08 01 91> 87 00
RX CMAC:  FA 14 2D EB A3 08 01 91

*** Authenticate(KeyNo= 1, Key= 10 18 20 29 30 38 40 48 50 58 60 68 70 78 80 88 90 98 A0 A8 B0 B8 C0 C8 (3K3DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 01> D0 00
Response: 00 00 FF 14 EC <D5 41 00 AF 66 0B 0E 97 E2 3B 9C 0F 93 FD 82 D0 F0 69 C2 98> C8 00
* RndB_enc:  66 0B 0E 97 E2 3B 9C 0F 93 FD 82 D0 F0 69 C2 98
* RndB:      41 C4 0C 7F 0E 89 71 0D 08 A3 94 E3 04 D1 15 E8
* RndB_rot:  C4 0C 7F 0E 89 71 0D 08 A3 94 E3 04 D1 15 E8 41
* RndA:      7F 0A C9 6C E3 5E 4D 60 87 F2 11 94 6B C6 15 08
* RndAB:     7F 0A C9 6C E3 5E 4D 60 87 F2 11 94 6B C6 15 08 C4 0C 7F 0E 89 71 0D 08 A3 94 E3 04 D1 15 E8 41
* RndAB_enc: 46 D1 82 F6 B3 C5 C4 58 EC 1E C8 BD 43 F0 CA 89 8C C9 CD 77 F9 BB C8 7F 4E 60 61 7C 1F F9 42 66
Sending:  00 00 FF 24 DC <D4 40 01 AF 46 D1 82 F6 B3 C5 C4 58 EC 1E C8 BD 43 F0 CA 89 8C C9 CD 77 F9 BB C8 7F 4E 60 61 7C 1F F9 42 66> 2
Response: 00 00 FF 14 EC <D5 41 00 00 80 18 B8 0E 22 46 BD 1C 1C 05 A0 67 CD 8E 6E 17> 43 00
* RndA_enc:  80 18 B8 0E 22 46 BD 1C 1C 05 A0 67 CD 8E 6E 17
* RndA_dec:  0A C9 6C E3 5E 4D 60 87 F2 11 94 6B C6 15 08 7F
* RndA_rot:  0A C9 6C E3 5E 4D 60 87 F2 11 94 6B C6 15 08 7F
* SessKey:   7E 0A C8 6C 40 C4 0C 7E 4C 60 86 F2 70 0C 08 A2 6A C6 14 08 04 D0 14 E8 (3K3DES)

------------------------------------------------------
---------------------- AES ---------------------------
------------------------------------------------------

*** SelectApplication(0x00AE16)
Sending:  00 00 FF 07 F9 <D4 40 01 5A 16 AE 00> CD 00
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00

*** Authenticate(KeyNo= 0, Key= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (AES))
Sending:  00 00 FF 05 FB <D4 40 01 AA 00> 41 00
Response: 00 00 FF 14 EC <D5 41 00 AF B9 69 FD FE 56 FD 91 FC 9D E6 F6 F2 13 B8 FD 1E> ED 00
* RndB_enc:  B9 69 FD FE 56 FD 91 FC 9D E6 F6 F2 13 B8 FD 1E
* RndB:      C0 5D DD 71 4F D7 88 A6 B7 B7 54 F3 C4 D0 66 E8
* RndB_rot:  5D DD 71 4F D7 88 A6 B7 B7 54 F3 C4 D0 66 E8 C0
```

```
* RndA:      F4 4B 26 F5 68 6F 3A 39 1C D3 8E BD 10 77 22 81
* RndAB:     F4 4B 26 F5 68 6F 3A 39 1C D3 8E BD 10 77 22 81 5D DD 71 4F D7 88 A6 B7 B7 54 F3 C4 D0 66 E8 C0
* RndAB_enc: 36 AA D7 DF 6E 43 6B A0 8D 18 61 38 30 A7 0D 5A D4 3E 3D 3F 4A 8D 47 54 1E EE 62 3A 93 4E 47 74
Sending:  00 00 FF 24 DC <D4 40 01 AF 36 AA D7 DF 6E 43 6B A0 8D 18 61 38 30 A7 0D 5A D4 3E 3D 3F 4A 8D 47 54 1E EE 62 3A 93 4E 47 74> 2
Response: 00 00 FF 14 EC <D5 41 00 00 80 0D B6 80 BC 14 6B D1 21 D6 57 8F 2D 2E 20 59> 6A 00
* RndA_enc:  80 0D B6 80 BC 14 6B D1 21 D6 57 8F 2D 2E 20 59
* RndA_dec:  4B 26 F5 68 6F 3A 39 1C D3 8E BD 10 77 22 81 F4
* RndA_rot:  4B 26 F5 68 6F 3A 39 1C D3 8E BD 10 77 22 81 F4
* SessKey:   F4 4B 26 F5 C0 5D DD 71 10 77 22 81 C4 D0 66 E8 (AES)

*** ChangeKey(KeyNo= 0)
* SessKey IV:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
* New Key:     00 10 20 30 40 50 60 70 80 90 A0 B0 B0 A0 90 80 (AES)
* CRC Crypto:  0x6BE6C6D2
* Cryptogram:  00 10 20 30 40 50 60 70 80 90 A0 B0 B0 A0 90 80 10 D2 C6 E6 6B 00 00 00 00 00 00 00 00 00 00 00
* CryptogrEnc: E9 F8 5E 21 94 96 C2 B5 8C 10 90 DC 39 35 FA E9 E8 40 CF 61 B3 83 D9 53 19 46 25 6B 1F 11 0C 10
Sending:  00 00 FF 25 DB <D4 40 01 C4 00 E9 F8 5E 21 94 96 C2 B5 8C 10 90 DC 39 35 FA E9 E8 40 CF 61 B3 83 D9 53 19 46 25 6B 1F 11 0C 10
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00 AA AA AA AA AA AA AA AA

*** Authenticate(KeyNo= 0, Key= 00 10 20 30 40 50 60 70 80 90 A0 B0 B0 A0 90 80 (AES))
Sending:  00 00 FF 05 FB <D4 40 01 AA 00> 41 00
Response: 00 00 FF 14 EC <D5 41 00 AF CC C8 31 6C 2B 26 13 FE 9A 18 9B AC 9C C8 9D 03> AB 00
* RndB_enc:  CC C8 31 6C 2B 26 13 FE 9A 18 9B AC 9C C8 9D 03
* RndB:      27 10 47 12 5A 2A A5 81 78 F5 C5 1B 11 77 A1 9B
* RndB_rot:  10 47 12 5A 2A A5 81 78 F5 C5 1B 11 77 A1 9B 27
* RndA:      C2 A1 E4 7B 96 A5 58 9F AA E9 0C 03 FE 6D 00 A7
* RndAB:     C2 A1 E4 7B 96 A5 58 9F AA E9 0C 03 FE 6D 00 A7 10 47 12 5A 2A A5 81 78 F5 C5 1B 11 77 A1 9B 27
* RndAB_enc: C0 2E 06 1E 72 E1 77 26 48 9C AE EC 99 7C 52 37 58 BF 86 3E FE 76 71 C5 5B 46 65 D0 6A CC D9 7B
Sending:  00 00 FF 24 DC <D4 40 01 AF C0 2E 06 1E 72 E1 77 26 48 9C AE EC 99 7C 52 37 58 BF 86 3E FE 76 71 C5 5B 46 65 D0 6A CC D9 7B> 3
Response: 00 00 FF 14 EC <D5 41 00 00 72 AC CC 0B DE A4 82 B5 31 85 BB 5A D0 08 62 46> F1 00
* RndA_enc:  72 AC CC 0B DE A4 82 B5 31 85 BB 5A D0 08 62 46
* RndA_dec:  A1 E4 7B 96 A5 58 9F AA E9 0C 03 FE 6D 00 A7 C2
* RndA_rot:  A1 E4 7B 96 A5 58 9F AA E9 0C 03 FE 6D 00 A7 C2
* SessKey:   C2 A1 E4 7B 27 10 47 12 FE 6D 00 A7 11 77 A1 9B (AES)

*** ChangeKey(KeyNo= 0)
* SessKey IV:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
* New Key:     10 18 20 28 30 38 40 48 50 58 60 68 70 78 80 88 (AES)
* CRC Crypto:  0x62638574
* Cryptogram:  10 18 20 28 30 38 40 48 50 58 60 68 70 78 80 88 10 74 85 63 62 00 00 00 00 00 00 00 00 00 00 00
* CryptogrEnc: 29 45 E3 76 0E 60 F4 A4 04 6B B8 A5 05 B3 1C F5 59 A3 A2 E0 52 13 BC 82 94 2C A6 AB 5D BC EC F5
Sending:  00 00 FF 25 DB <D4 40 01 C4 00 29 45 E3 76 0E 60 F4 A4 04 6B B8 A5 05 B3 1C F5 59 A3 A2 E0 52 13 BC 82 94 2C A6 AB 5D BC EC F5
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00 AA AA AA AA AA AA AA AA

*** Authenticate(KeyNo= 0, Key= 10 18 20 28 30 38 40 48 50 58 60 68 70 78 80 88 (AES))
Sending:  00 00 FF 05 FB <D4 40 01 AA 00> 41 00
Response: 00 00 FF 14 EC <D5 41 00 AF 3E 2B E6 26 C0 5E 77 98 EE 51 83 55 A7 51 64 8E> 98 00
* RndB_enc:  3E 2B E6 26 C0 5E 77 98 EE 51 83 55 A7 51 64 8E
* RndB:      91 03 68 45 7E 2E 9A A1 67 35 5B FB 54 4B 99 31
* RndB_rot:  03 68 45 7E 2E 9A A1 67 35 5B FB 54 4B 99 31 91
* RndA:      90 F7 A2 01 C4 DB 76 05 38 FF 8A 49 EC 63 DE CD
* RndAB:     90 F7 A2 01 C4 DB 76 05 38 FF 8A 49 EC 63 DE CD 03 68 45 7E 2E 9A A1 67 35 5B FB 54 4B 99 31 91
* RndAB_enc: FA BF 71 BB 0D C4 5B 8F 31 BA ED DF F7 F3 43 96 52 D4 09 4D F1 2C 17 EF 0C 94 35 3E 6D 77 70 C8
Sending:  00 00 FF 24 DC <D4 40 01 AF FA BF 71 BB 0D C4 5B 8F 31 BA ED DF F7 F3 43 96 52 D4 09 4D F1 2C 17 EF 0C 94 35 3E 6D 77 70 C8> 5
Response: 00 00 FF 14 EC <D5 41 00 00 1C E6 C5 74 E2 49 23 D4 04 E1 8B 6A 24 0C 1B 08> 60 00
* RndA_enc:  1C E6 C5 74 E2 49 23 D4 04 E1 8B 6A 24 0C 1B 08
* RndA_dec:  F7 A2 01 C4 DB 76 05 38 FF 8A 49 EC 63 DE CD 90
* RndA_rot:  F7 A2 01 C4 DB 76 05 38 FF 8A 49 EC 63 DE CD 90
* SessKey:   90 F7 A2 01 91 03 68 45 EC 63 DE CD 54 4B 99 31 (AES)

*** GetKeyVersion()
TX CMAC:  25 7F C5 38 61 8A 94 4A 3A 20 96 7B 6F 31 43 48
Sending:  00 00 FF 05 FB <D4 40 01 64 00> 87 00
Response: 00 00 FF 0D F3 <D5 41 00 00 10 8A 8F A3 6F 55 CD 21 0D> 5F 00
RX CMAC:  8A 8F A3 6F 55 CD 21 0D D8 05 46 58 AC 70 D9 9A
Version: 0x10

*** ChangeKey(KeyNo= 0)
* SessKey IV:  8A 8F A3 6F 55 CD 21 0D D8 05 46 58 AC 70 D9 9A
* New Key:     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (AES)
* CRC Crypto:  0x1B860F0A
* Cryptogram:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A 0F 86 1B 00 00 00 00 00 00 00 00 00 00 00
* CryptogrEnc: 63 53 75 E4 91 9F 8A F2 E9 E8 6B 1C 1B A5 5B 0C 08 07 EA F4 84 D7 A7 EF 6E 0C 30 84 16 0F 5A 61
Sending:  00 00 FF 25 DB <D4 40 01 C4 00 63 53 75 E4 91 9F 8A F2 E9 E8 6B 1C 1B A5 5B 0C 08 07 EA F4 84 D7 A7 EF 6E 0C 30 84 16 0F 5A 61
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00 AA AA AA AA AA AA AA AA

*** Authenticate(KeyNo= 0, Key= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (AES))
Sending:  00 00 FF 05 FB <D4 40 01 AA 00> 41 00
Response: 00 00 FF 14 EC <D5 41 00 AF ED DA F0 C5 D9 A7 CF 42 B8 80 8B E2 01 38 99 A1> 16 00
* RndB_enc:  ED DA F0 C5 D9 A7 CF 42 B8 80 8B E2 01 38 99 A1
* RndB:      D8 10 00 44 4B 97 6F 48 34 0D CD E3 4D 7A B1 7C
* RndB_rot:  10 00 44 4B 97 6F 48 34 0D CD E3 4D 7A B1 7C D8
* RndA:      C2 A1 E4 7B 96 A5 58 9F AA E9 0C 03 FE 6D 00 A7
* RndAB:     C2 A1 E4 7B 96 A5 58 9F AA E9 0C 03 FE 6D 00 A7 10 00 44 4B 97 6F 48 34 0D CD E3 4D 7A B1 7C D8
* RndAB_enc: D8 10 5F 87 4E 2C A5 7B 76 C3 54 A8 06 6B 0D 78 80 B0 C4 EC 39 9D BF 25 34 38 DB 46 D7 5F 8F 60
Sending:  00 00 FF 24 DC <D4 40 01 AF D8 10 5F 87 4E 2C A5 7B 76 C3 54 A8 06 6B 0D 78 80 B0 C4 EC 39 9D BF 25 34 38 DB 46 D7 5F 8F 60> 5
Response: 00 00 FF 14 EC <D5 41 00 00 45 9C 76 B7 1A B9 F1 73 64 13 F5 AC D7 3E 7D F9> 02 00
* RndA_enc:  45 9C 76 B7 1A B9 F1 73 64 13 F5 AC D7 3E 7D F9
* RndA_dec:  A1 E4 7B 96 A5 58 9F AA E9 0C 03 FE 6D 00 A7 C2
* RndA_rot:  A1 E4 7B 96 A5 58 9F AA E9 0C 03 FE 6D 00 A7 C2
* SessKey:   C2 A1 E4 7B D8 10 00 44 FE 6D 00 A7 4D 7A B1 7C (AES)

*** ChangeKey(KeyNo= 1)
* SessKey IV:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
* New Key:     00 10 20 30 40 50 60 70 80 90 A0 B0 B0 A0 90 80 (AES)
* Cur Key:     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (AES)
* CRC Crypto:  0x84B47033
* CRC New Key: 0x1979E3BF
* Cryptogram:  00 10 20 30 40 50 60 70 80 90 A0 B0 B0 A0 90 80 10 33 70 B4 84 BF E3 79 19 00 00 00 00 00 00 00
* CryptogrEnc: E7 EC CB 6B D1 CA 64 BC 16 1A 12 B1 C0 24 F7 14 30 33 74 08 C8 A8 7E AC AB 7A 1F F1 89 51 FC A3
Sending:  00 00 FF 25 DB <D4 40 01 C4 01 E7 EC CB 6B D1 CA 64 BC 16 1A 12 B1 C0 24 F7 14 30 33 74 08 C8 A8 7E AC AB 7A 1F F1 89 51 FC A3
Response: 00 00 FF 0C F4 <D5 41 00 00 21 28 D3 CD 9C 9A CF FF> FD 00
RX CMAC:  21 28 D3 CD 9C 9A CF FF F6 EB 95 46 AD F3 5E 17
```

```
*** ChangeKey(KeyNo= 1)
* SessKey IV:  21 28 D3 CD 9C 9A CF FF F6 EB 95 46 AD F3 5E 17
* New Key:     10 18 20 28 30 38 40 48 50 58 60 68 70 78 80 88 (AES)
* Cur Key:     00 10 20 30 40 50 60 70 80 90 A0 B0 B0 A0 90 80 (AES)
* CRC Crypto:  0xE0E6EA29
* CRC New Key: 0x2A766EB3
* Cryptogram:  10 08 00 18 70 68 20 38 D0 C8 C0 D8 C0 D8 10 08 10 29 EA E6 E0 B3 6E 76 2A 00 00 00 00 00 00 00
* CryptogrEnc: 28 41 93 8C 40 A4 BC 2C 33 06 44 82 FE AD A5 F4 3E C5 35 D3 42 55 B0 28 6C 23 52 CD 17 38 63 C7
Sending:  00 00 FF 25 DB <D4 40 01 C4 01 28 41 93 8C 40 A4 BC 2C 33 06 44 82 FE AD A5 F4 3E C5 35 D3 42 55 B0 28 6C 23 52 CD 17 38 63 C7
Response: 00 00 FF 0C F4 <D5 41 00 00 CA F3 BF 0B 28 36 E9 DE> 3E 00
RX CMAC:  CA F3 BF 0B 28 36 E9 DE 80 B1 FD 6F B4 5E 93 80

*** Authenticate(KeyNo= 1, Key= 10 18 20 28 30 38 40 48 50 58 60 68 70 78 80 88 (AES))
Sending:  00 00 FF 05 FB <D4 40 01 AA 01> 40 00
Response: 00 00 FF 14 EC <D5 41 00 AF B3 51 CB 24 65 D4 F3 3A C6 27 FD 6E 87 A1 68 F2> 08 00
* RndB_enc:  B3 51 CB 24 65 D4 F3 3A C6 27 FD 6E 87 A1 68 F2
* RndB:      62 6F FB D4 5C AF 33 4A CC A4 55 99 30 4F 5B 17
* RndB_rot:  6F FB D4 5C AF 33 4A CC A4 55 99 30 4F 5B 17 62
* RndA:      40 E7 D2 71 74 CB A6 75 E8 EF BA B9 9C 53 0E 3D
* RndAB:     40 E7 D2 71 74 CB A6 75 E8 EF BA B9 9C 53 0E 3D 6F FB D4 5C AF 33 4A CC A4 55 99 30 4F 5B 17 62
* RndAB_enc: 04 4B 6C AC 34 3A 08 65 89 51 49 64 9C A8 DD E1 F5 AC 4E C6 7B D2 08 90 0A F0 2F 04 9E 05 F0 B0
Sending:  00 00 FF 24 DC <D4 40 01 AF 04 4B 6C AC 34 3A 08 65 89 51 49 64 9C A8 DD E1 F5 AC 4E C6 7B D2 08 90 0A F0 2F 04 9E 05 F0 B0> 6
Response: 00 00 FF 14 EC <D5 41 00 00 A2 EE 14 4B 10 12 FB EB 7B 2F 11 13 2D 95 A4 54> 6B 00
* RndA_enc:  A2 EE 14 4B 10 12 FB EB 7B 2F 11 13 2D 95 A4 54
* RndA_dec:  E7 D2 71 74 CB A6 75 E8 EF BA B9 9C 53 0E 3D 40
* RndA_rot:  E7 D2 71 74 CB A6 75 E8 EF BA B9 9C 53 0E 3D 40
* SessKey:   40 E7 D2 71 62 6F FB D4 9C 53 0E 3D 30 4F 5B 17 (AES)

----------------------------------------------------------------
----------------------------------------------------------------
----------------------------------------------------------------

*** CreateStdDataFile(ID= 5, Size= 80)
TX CMAC:  F2 3B 03 68 57 8C 65 AD 70 5C 52 AF E7 62 61 B6
Sending:  00 00 FF 0B F5 <D4 40 01 CD 05 00 11 00 50 00 00> B8 00
Response: 00 00 FF 0C F4 <D5 41 00 00 A7 53 16 AD 15 96 B9 53> 76 00
RX CMAC:  A7 53 16 AD 15 96 B9 53 74 EE F5 5F B7 FA 00 EC

*** GetFileIDs()
TX CMAC:  F6 9B 3B AD A9 9A 58 AA 2B D7 36 66 2E 32 D4 B0
Sending:  00 00 FF 04 FC <D4 40 01 6F> 7C 00
Response: 00 00 FF 0D F3 <D5 41 00 00 05 2D 5F F6 7F FE C9 D2 D3> 78 00 AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA A
RX CMAC:  2D 5F F6 7F FE C9 D2 D3 60 87 21 15 88 EA C2 D7
File ID's: 05

*** GetFileSettings(ID= 5)
TX CMAC:  63 65 D3 B1 98 DC A8 40 43 DF 6D F8 FE 76 DF D6
Sending:  00 00 FF 05 FB <D4 40 01 F5 05> F1 00
Response: 00 00 FF 13 ED <D5 41 00 00 00 00 11 00 50 00 00 2A AC 75 17 02 4E 09 DC> F2 00 AA AA AA AA AA AA AA AA AA AA AA AA AA
RX CMAC:  2A AC 75 17 02 4E 09 DC 45 28 57 D5 D5 6F D2 13
Type: 0, Encrypt: 0, Access Read: 0x0, Write: 0x0, Rd+Wr: 0x1, Change: 0x1
FileSize: 80

*** WriteFileData(ID= 5, Offset= 0, Length= 80)
TX CMAC:  5F 7B CA 26 9F 97 49 5C 64 BC FB 3D B4 14 49 CA
Sending:  00 00 FF 3F C1 <D4 40 01 3D 05 00 00 00 34 00 00 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19
Response: 00 00 FF 0C F4 <D5 41 00 00 76 5C 9D AA 50 EC B6 2F> B0 00
RX CMAC:  76 5C 9D AA 50 EC B6 2F 59 BA CA 81 F2 EF 80 F9
TX CMAC:  ED F3 2C B9 09 97 15 5F 8C 0A 15 BB CA 11 8D A1
Sending:  00 00 FF 27 D9 <D4 40 01 3D 05 34 00 00 1C 00 00 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D
Response: 00 00 FF 0C F4 <D5 41 00 00 3E 0A ED 98 6B 8B 0F 37> E1 00
RX CMAC:  3E 0A ED 98 6B 8B 0F 37 F6 4D 79 B9 11 A5 A6 C9

*** ReadFileData(ID= 5, Offset= 0, Length= 80)
TX CMAC:  43 33 03 AB 3C FF A7 58 BF 7E B1 6F FE C4 7A 70
Sending:  00 00 FF 0B F5 <D4 40 01 BD 05 00 00 00 30 00 00> F9 00
Response: 00 00 FF 3C C4 <D5 41 00 00 00 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20
RX CMAC:  4C 65 F1 F8 42 26 2B AC 65 FF BF 61 CF 71 FD 06
TX CMAC:  C2 6B DE 4E B9 65 BC 3C 83 1C 07 71 C4 2F D5 B9
Sending:  00 00 FF 0B F5 <D4 40 01 BD 05 30 00 00 20 00 00> D9 00
Response: 00 00 FF 2C D4 <D5 41 00 00 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F F0
RX CMAC:  F0 22 05 CF 91 3C 03 C9 35 4C 8F F4 3D 1C 9E 61

*** DeleteFile(ID= 5)
TX CMAC:  16 91 88 F6 17 AE 87 D4 AB EF D4 D0 58 36 1B FD
Sending:  00 00 FF 05 FB <D4 40 01 DF 05> 07 00
Response: 00 00 FF 0C F4 <D5 41 00 00 1B EF 0D 32 B6 D1 D7 F9> 4A 00
RX CMAC:  1B EF 0D 32 B6 D1 D7 F9 E6 A8 32 32 09 19 CE 67

*** GetFileIDs()
TX CMAC:  34 06 A8 4E 41 14 31 A2 92 ED 8E F9 D8 3C 5E D6
Sending:  00 00 FF 04 FC <D4 40 01 6F> 7C 00
Response: 00 00 FF 0C F4 <D5 41 00 00 FC 19 4E A9 3E 3E F8 E7> 83 00 AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA A
RX CMAC:  FC 19 4E A9 3E 3E F8 E7 A4 C1 A9 82 15 F7 A7 EF
No files.

*** SelectApplication(0x000000)
Sending:  00 00 FF 07 F9 <D4 40 01 5A 00 00 00> 91 00
Response: 00 00 FF 04 FC <D5 41 00 00> EA 00

*** Authenticate(KeyNo= 0, Key= 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (DES))
Sending:  00 00 FF 05 FB <D4 40 01 1A 00> D1 00
Response: 00 00 FF 0C F4 <D5 41 00 AF 44 15 93 9B 21 D8 EE E8> E5 00 AA AA AA AA AA AA AA AA
* RndB_enc:  44 15 93 9B 21 D8 EE E8
* RndB:      14 4A 72 D2 5B 22 70 62
* RndB_rot:  4A 72 D2 5B 22 70 62 14
* RndA:      6D 00 A7 92 31 34 8B 66
* RndAB:     6D 00 A7 92 31 34 8B 66 4A 72 D2 5B 22 70 62 14
* RndAB_enc: 89 D6 11 80 9D 60 5F 8C 91 7A 18 BF 26 DE 2D 6F
Sending:  00 00 FF 14 EC <D4 40 01 AF 89 D6 11 80 9D 60 5F 8C 91 7A 18 BF 26 DE 2D 6F> E2 00
Response: 00 00 FF 0C F4 <D5 41 00 00 21 69 62 14 FD DA 25 04> EA 00
* RndA_enc:  21 69 62 14 FD DA 25 04
* RndA_dec:  00 A7 92 31 34 8B 66 6D
* RndA_rot:  00 A7 92 31 34 8B 66 6D
```

```
* SessKey:   6C 00 A6 92 14 4A 72 D2 6C 00 A6 92 14 4A 72 D2 (DES)

*** FormatCard()
TX CMAC:  1E A2 9F 16 4F 15 19 8D
Sending:  00 00 FF 04 FC <D4 40 01 FC> EF 00
Response: 00 00 FF 0C F4 <D5 41 00 00 3C 28 C1 12 18 2E 3B E8> 4A 00
RX CMAC:  3C 28 C1 12 18 2E 3B E8

Selftest success
```

CMAC Calculation for AES 128

From: NIST

```
AES Key: 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
SubKey1: fb ee d6 18 35 71 33 66 7c 85 e0 8f 72 36 a8 de
SubKey2: f7 dd ac 30 6a e2 66 cc f9 0b c1 1e e4 6d 51 3b

Message: <empty>
CMAC:    bb 1d 69 29 e9 59 37 28 7f a3 7d 12 9b 75 67 46

Message: 6b c1 be e2 2e 40 9f 96 e9 3d 7e 11 73 93 17 2a
CMAC:    07 0a 16 b4 6b 4d 41 44 f7 9b dd 9d d0 4a 28 7c

Message: 6b c1 be e2 2e 40 9f 96 e9 3d 7e 11 73 93 17 2a ae 2d 8a 57 1e 03 ac 9c 9e b7 6f ac 45 af 8e 51 30 c8 1c 46 a3 5c e4 11
CMAC:    df a6 67 47 de 9a e6 30 30 ca 32 61 14 97 c8 27
```

Elmü