Advanced Card Systems Ltd.
Card & Reader Technologies

ACOSJ
Sample Card

Applet Installation Manual V1.01

info@acs.com.hk
www.acs.com.hk

Table of Contents

List of Figures

1.0. Overview

This document describes how to install an applet to the ACOSJ sample card.

1.1. Technical Specifications

Before installing the applet, please take note of the following points:

1. The instance AID of the ISD (or Card Manager) is A000000151000000;

   The Executable Load File AID of ISD is A00000015101;

   The Executable Module AID of ISD is A000000151000000.

2. Supported Secure Channel Protocol is ’SCP 02 option 55’.

3. The Issuer Security Domain has three identical 16-byte initial static keys. The Key Version Numbers of these keys is set to '20' and the Key Identifiers are set to '01', '02' and '03' respectively. Unless otherwise requested by the Card Issuer, the value of any initial key is:

   '40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F'.

2.0. Installing the applet

To install the applet:

1. Open the reader.
2. Send SELECT to select ISD（AID= A000000151000000）
3. Initiate the Secure Channel (INITIALIZE UPDATE and EXTERNAL AUTHENTICATE).
4. Send INSTALL[for Load] (80 E6 02 00…).
5. Send LOAD (80 E8 00 00…).
6. Send INSTALL[for Install] (80 E6 0C 00…).

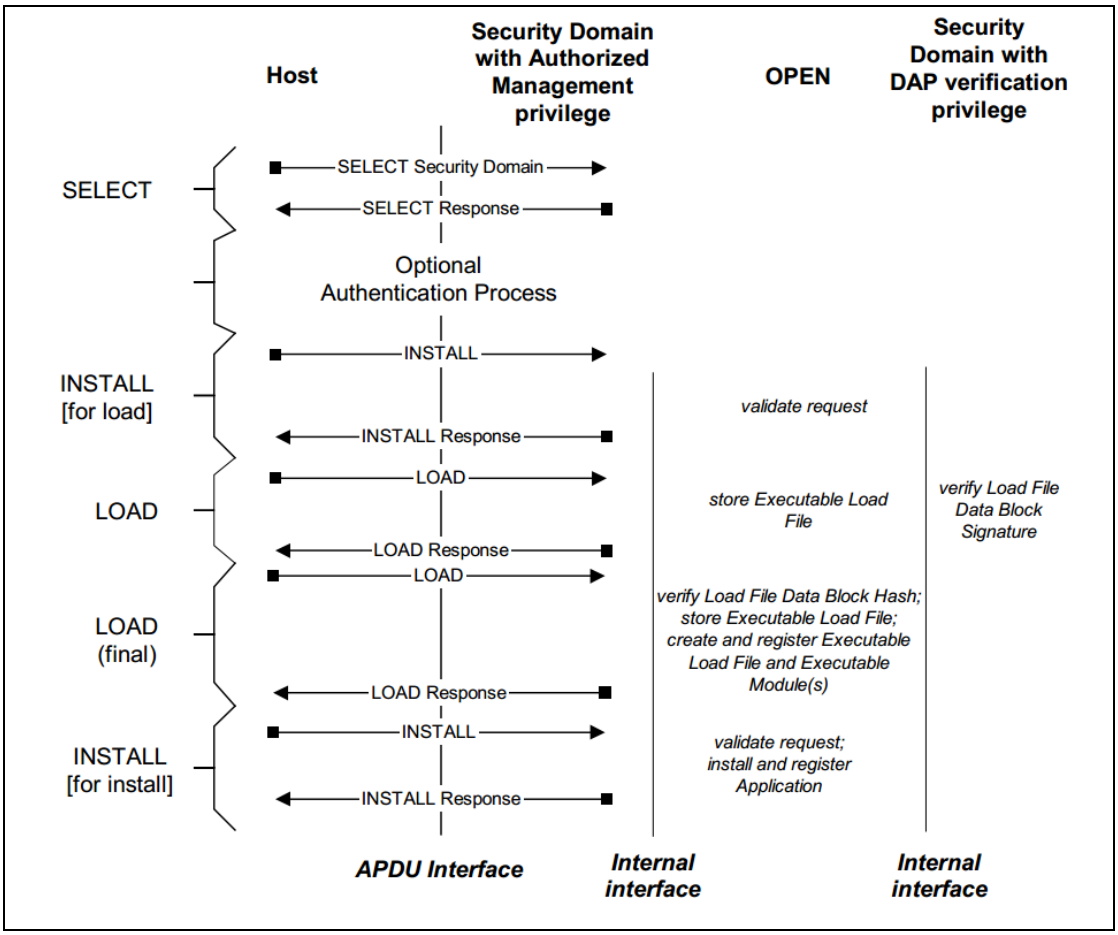


Figure 1: Applet Installation Flow

Below is the applet installation's sample script to be sent to the reader:

```
;Select issure secure domain
<= 00A4040008A000000151000000
=>
6F5C8408A000000151000000A550734A06072A864886FC6B01600C060A2A864886FC6B02020
201630906072A864886FC6B03640B06092A864886FC6B040255650B06092A864886FC6B0201
03660C060A2B060104012A026E01039F6501FF(9000)

;send INITIALIZE UPDATE
<= 8050000008 1122334455667788
=> 000002650183039536622002000A72BB2775E0D3610D90424829CEB5(9000)
```

```
Session Key(Enc) : 339F1D7F5D5841EB034F5CE234557894
Session Key(Cmac): C6713F31B8DC1F8905DFECB4065CB81E
Session Key(Dek) : 06E72D52EEFBD1D8DB5C230C3F2B56E9

;send EXTERNAL AUTHENTICATE
<= 84820000103CA4BC00FAD9D1434F4086C4959E26B5
=> (9000)


;start upload cap file
<= 80E602000A 05A01122334400000000
=> 00(9000)

;send INSTALL[for Load]
;send  1st  LOAD
<= 80E80000FF
C482011D010014DECAFFED020204000105A011223344047041707002002100140021000A001
5002E000E0058000A00100000006A01F40000000000000201000400150203010 7A000000062
0101030107A0000000620102030 00A0106A01122334401000F06000E000000800301000107 0
1000000230700580002101 88C000118058D000287007A05308F00033D8C0004181D0441181D
258B00057A0422188B000660037A198B00072D1A0725321A0425730019FF84FF840009AD001
A081F8B000819081F8B00097008116D008D000A7A08000A0000000000000000000000005002E00
0B020002000680030006810E0001000200060000010380030203800303 03
=> 00(9000)

;send  2st  LOAD
<= 80E8800122
800A0103810E0103800A0806800701090010000 20D35000A050508040A0707190608
=> 00(9000)

;send INSTALL[FOR INSTALL]
<= 80E60C001A 05A01122334406A0112233440106A01122334401010002C90000(9000)
=> 00(9000)
```

Below is the procedure on how to initiate the Secure Channel:

1. Host send: INITIALIZE UPDATE, with level 0, with key version '0xFF' (or other key version added through PUT KEY)
   =>80 50 00 00 08 1122334455667788 (9000)
   <=0000026501830395366 2 2002 000A 72BB2775E0D3 610D90424829CEB5

2. Generate session keys.
   S-ENC:
   Using the default Key '4041424344454647 48494A4B4C4D4E4F' to encrypt the data '0182000A00000000 0000000000000000' with DES-CBC: then you will get the session key(S-ENC): 339F1D7F5D5841EB 034F5CE234557894

   S-MAC:
   Using the default Key '4041424344454647 48494A4B4C4D4E4F' to encrypt the data '0101000A00000000 0000000000000000' with DES-CBC: then you will get the session key(S- MAC): C6713F31B8DC1F89 05DFECB4065CB81E

DEK:

Using the default Key '4041424344454647 48494A4B4C4D4E4F' to encrypt the data '0181000A00000000 0000000000000000' with DES-CBC: then you will get the session key(DEK): 06E72D52EEFBD1D8 DB5C230C3F2B56E9

3. Verify Card Authentication Cryptogram: concatenating the 8-byte host challenge and 8-byte card challenge resulting in a 16-byte block.

   Using S-ENC '339F1D7F5D5841EB 034F5CE234557894' to sign the data '1122334455667788 + 000A + 72BB2775E0D3 + 8000000000000000' with DES_MAC4_ISO9797_M1, ICV=0, the result of signature will be 610D90424829CEB5, and should be equal to the cryptogram sent by the card.

4. Send EXTERNAL AUTHENTICATE with level =0.

   a. Host Authentication Cryptogram:

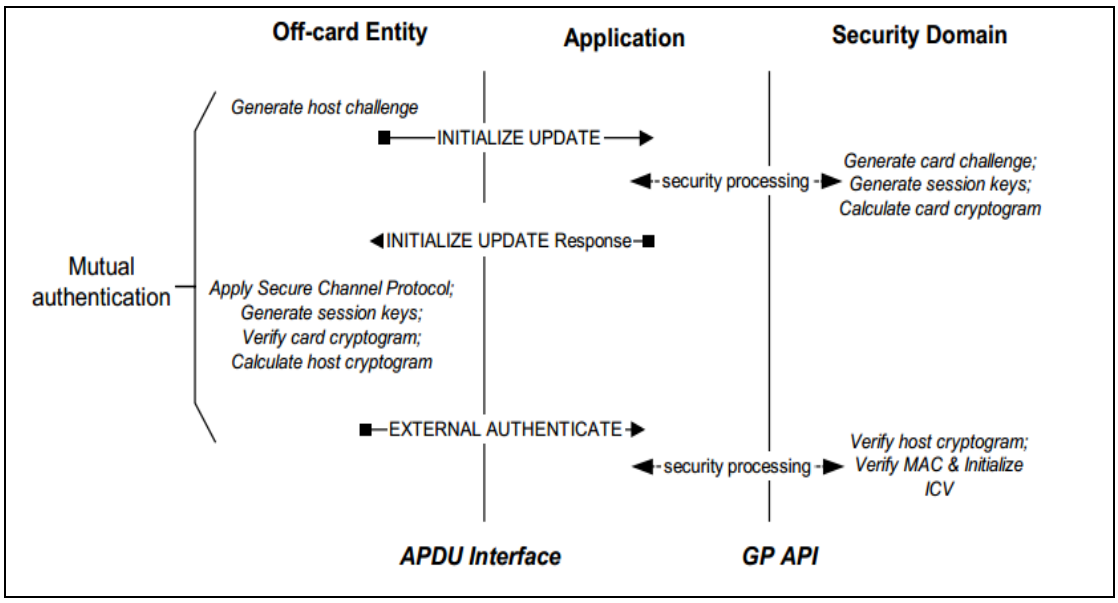
      Concatenating the 8-byte card challenge and 8-byte host challenge resulting in a 16-byte block using S-ENC'339F1D7F5D5841EB 034F5CE234557894' to sign the data '000A + 72BB2775E0D3 + 1122334455667788 + 8000000000000000' with DES_MAC4_ISO9797_M1, ICV=0, the result of signature will be 3CA4BC00FAD9D143.

   b. Calculate the MAC with S-MAC ' C6713F31B8DC1F89 05DFECB4065CB81E' to sign the data '8482000010 3CA4BC00FAD9D143' with single DES plus final triple DES, the result of MAC will be 4F4086C4959E26B5.

   c. Concatenate EXTERNAL AUTHENTICATE:

      =>8482000010 3CA4BC00FAD9D143 4F4086C4959E26B5

      <=9000



3.0. Removing executable load files

An executable load file contains executable modules from which the applications have been installed. This optional feature removes the executable load file an all other application-related files.

Detail for APDU:

80 E4 00 00 Lc Data

Data field consists of the format of TLV beginning with tag 4F, followed by the length and the AID of the applet to be removed.

That is:

80 E4 00 00 Lc 4F + AIDlen + AID

If successful, you will get 00 and SW = 9000.

Appendix A. Instruction Set

CLA	INS	Command
80h/84h	E4h	Delete
80h/84h	F2h	Get Status
00h/80h/84h	CAh	Get Data
80h/84h	E6h	Install
80h/84h	E8h	LOAD
00h	70h	Manage Channel
80h/84h	D8h	Put Key
00h	A4h	Select
80h/84h	F0h	Set Status
80h/84h	E2h	Store Data
80h	50h	INITIALIZE UPDATE
84h	82h	EXTERNAL AUTHENTICATE