Advanced Card Systems Ltd.
Card & Reader Technologies

# ACOSJ
# 样卡

应用安装说明手册 V1.01



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

# 目录



# 图目录

# 1.0. 概述

本文介绍如何将小应用程序（Applet）安装到 ACOSJ 样卡中。

## 1.1. 技术要求

安装 Applet 前，请确认以下几点：

1. ISD（或卡片管理器）的实例 AID 是 A000000151000000；

   ISD 的可执行加载文件 AID 是 A00000015101；

   ISD 的可执行模块 AID 是 A000000151000000；

2. 所支持的安全通道协议是‘SCP 02 option 55’。

3. 发卡方安全域有 3 个相同的 16 字节初始静态密钥。这些密钥的密钥版本号设为‘20’，密钥标识符分别设为‘01’、‘02’和‘03’。除非发卡方另有要求，初始密钥的值都是：

   ‘40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F’。

# 2.0. 安装 applet

安装 Applet：

1. 打开读写器。
2. 发送 SELECT 命令选择 ISD（AID= A000000151000000）。
3. 初始化安全通道（INITIALIZE UPDATE 命令和 EXTERNAL AUTHENTICATE 命令）。
4. 发送 INSTALL[for Load]命令(80 E6 02 00…)。
5. 发送 LOAD 命令(80 E8 00 00…)。
6. 发送 INSTALL[for Install]命令(80 E6 0C 00…)。

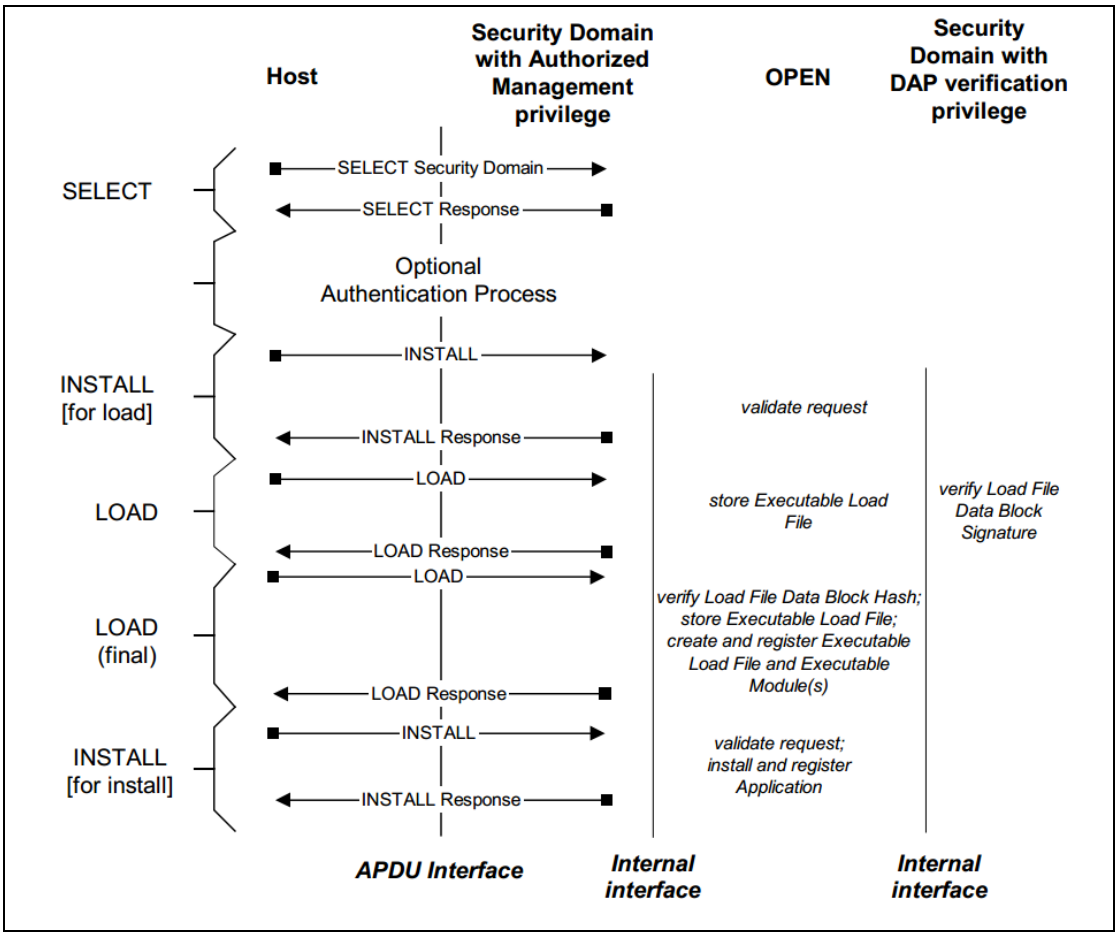



**图1**：Applet 安装流程图

下面是待发送给读写器，用于 Applet 安装的示例脚本。

```
;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 05A0112233440000000
=> 00(9000)

;send INSTALL[for Load]
;send  1st  LOAD
<= 80E80000FF
C482011D010014DECAFFED020204000105A011223344047041707002002100140021000A001
5002E000E0058000A00100000006A01F40000000000002010004001502030107A000000062
0101030107A00000006201020300 0A0106A0112233440100 0F06000E000000800301000107 0
1000000230700580002101 88C000118058D000287007A05308F00033D8C0004181D0441181D
258B00057A0422188B000660037A198B00072D1A0725321A0425730019FF84FF840009AD001
A081F8B000819081F8B00097008116D008D000A7A08000A0000000000000000000005002E00
0B020002000680030006810E0001000200060000010380030203800303 03
=> 00(9000)

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

;send INSTALL[FOR INSTALL]
<= 80E60C001A 05A01122334406A0112233440106A0112233440101000 2C90000(9000)
=> 00(9000)
```

下面是初始化安全通道的过程：

1. 主机发送：INITIALIZE UPDATE，级别为 0，密钥版本号为‘0xFF’（或者其他

   通过 PUT KEY 命令增加的密钥版本）

   =>80 50 00 00 08 1122334455667788 (9000)

   <=0000026501830395366220020 00A 72BB2775E0D3 610D90424829CEB5

2. 生成过程密钥。

   S-ENC：

   使用默认密钥‘4041424344454647 48494A4B4C4D4E4F’以 DES-CBC 的模式加密数据‘0182000A00000000 0000000000000000’：然后会获得过程密钥(S-ENC)：339F1D7F5D5841EB 034F5CE234557894

   S-MAC：

   使用默认密钥‘4041424344454647 48494A4B4C4D4E4F’以 DES-CBC 的模式加密

数据‘0101000A00000000 0000000000000000’：然后会获得过程密钥(S-MAC)：
C6713F31B8DC1F89 05DFECB4065CB81E

DEK：

使用默认密钥‘4041424344454647 48494A4B4C4D4E4F’以 DES-CBC 的模式加密数据‘0181000A00000000 0000000000000000’：然后会获得过程密钥(DEK)：
06E72D52EEFBD1D8 DB5C230C3F2B56E9

3. 校验卡片认证密文：将 8 字节主机随机数和 8 字节卡片随机数相连接组合成 16 字节块。

   使用 S-ENC‘339F1D7F5D5841EB 034F5CE234557894’，并采用 DES_MAC4_ISO9797_M1 和 0 作为 ICV 对数据‘1122334455667788 + 000A + 72BB2775E0D3 + 8000000000000000’进行签名，生成的签名结果会是‘610D90424829CEB5’，与卡片发送过来的密文相同。

4. 发送 EXTERNAL AUTHENTICATE，级别为 0。

   a. 主机认证密文

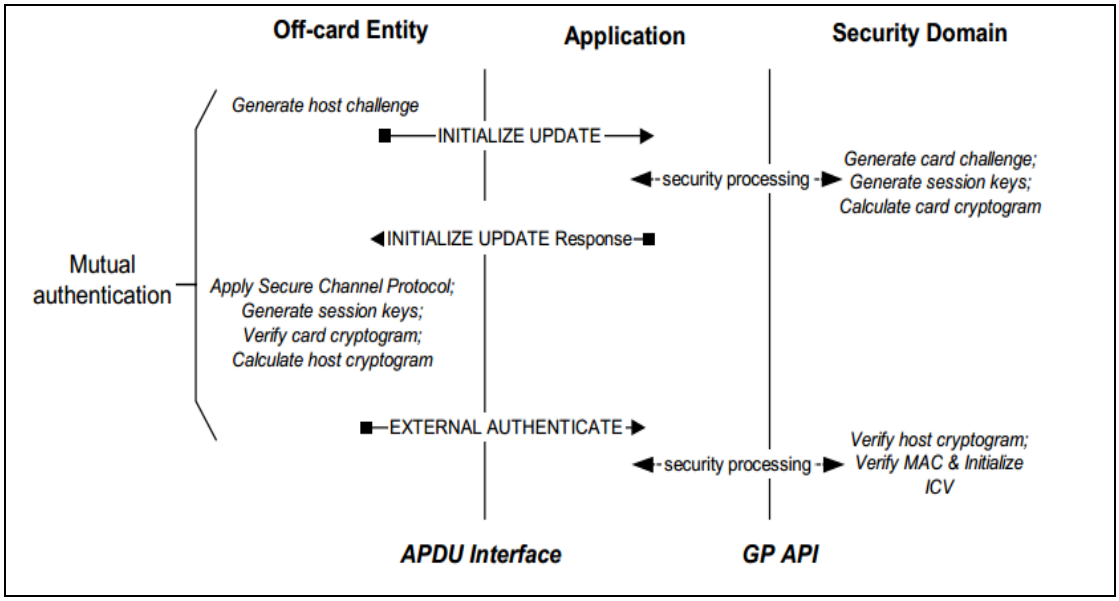
      将 8 字节卡片随机数和 8 字节主机随机数相连接组合成 16 字节块。使用 S-ENC‘339F1D7F5D5841EB 034F5CE234557894’，并采用 DES_MAC4_ISO9797_M1 和 0 作为 ICV 对数据‘000A + 72BB2775E0D3 + 1122334455667788 + 8000000000000000’进行签名，生成的签名结果会是 3CA4BC00FAD9D143。

   b. 计算 MAC，方法是采用 S-MAC‘C6713F31B8DC1F89 05DFECB4065CB81E’，以单一 DES 加最终 3DES MAC 的模式对数据‘8482000010 3CA4BC00FAD9D143’进行签名，生成的 MAC 结果会是‘4F4086C4959E26B5’。

   c. 连接 EXTERNAL AUTHENTICATE：

      =>8482000010 3CA4BC00FAD9D143 4F4086C4959E26B5

      <=9000



# 3.0. 删除可执行加载文件

一个可执行加载文件中包含多个可执行模块，应用会从可执行模块中安装。此附加功能删除可执行加载文件和其他与应用相关的所有文件。

APDU 详细信息：

80 E4 00 00 Lc Data

Data 数据域包括以标签 4F 开头的 TLV 的格式，后面跟随着待删除 Applet 的长度及 AID。

即：

80 E4 00 00 Lc 4F + AIDlen + AID

命令成功后返回 00 和 SW = 9000。

# 附录A 指令集

| CLA | INS | 命令 |
|---|---|---|
| 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 |