Java Applet Installation Guide (V3.3)

Excelsecu Data Technology Co., Ltd.

Table of Contents

1. Overview

This document describes how to install an applet to JVM (Java virtual Machine). There are two methods provided to install applet.

2. Method 1: GP tool

The following describes how to install an applet by GP tool.

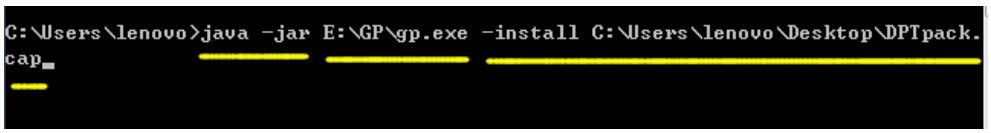
2.1. GlobalPlatformPro

Please refer to the website: https://github.com/martinpaljak/GlobalPlatformPro, and Download latest pre-built .JAR or .EXE from release area.

2.2. Install Applet

Install applet.cap (with AID information from the CAP) and go with GP command:

java -jar gp.jar -install applet.cap



3. Method 2: APDU Flow

The following describes how to install an applet by APDU flow.

3.1. Related Parameters

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

(1) Before installing the applet, you need to obtain the AID information set when the CAP package is compiled. The AID information used in the sample process is as follows:

Package AID: 0x113355770000

Applet AID: 0x113355770001

Instance AID: 0x113355770001

(2)Secure Channel

Supported Secure Channel Protocol is 'SCP 02', option i = 15: Initiation mode explicit, C-MAC on modified APDU, ICV set to zero, ICV encryption for CMAC session, 3 Secure Channel Keys

(3)Default Session Keys

KEYs	Default Value
S-MAC	404142434445464748494A4B4C4D4E4F
S-ENC	404142434445464748494A4B4C4D4E4F
DEK	404142434445464748494A4B4C4D4E4F

3.2. Installing the Applet

To install the applet:

1. Open the Card reader.

2. Send SELECT to select ISD APDU (00A4040000).

3. Initiate the Secure Channel (INITIALIZE UPDATE and EXTERNAL AUTHENTICATE).

4. Send INSTALL [for Load] (80/84 E6 02 00…).

5. Send LOAD (80/84 E8 00 00…).

6. Send INSTALL [for Install] (80/84 E6 0C 00…).

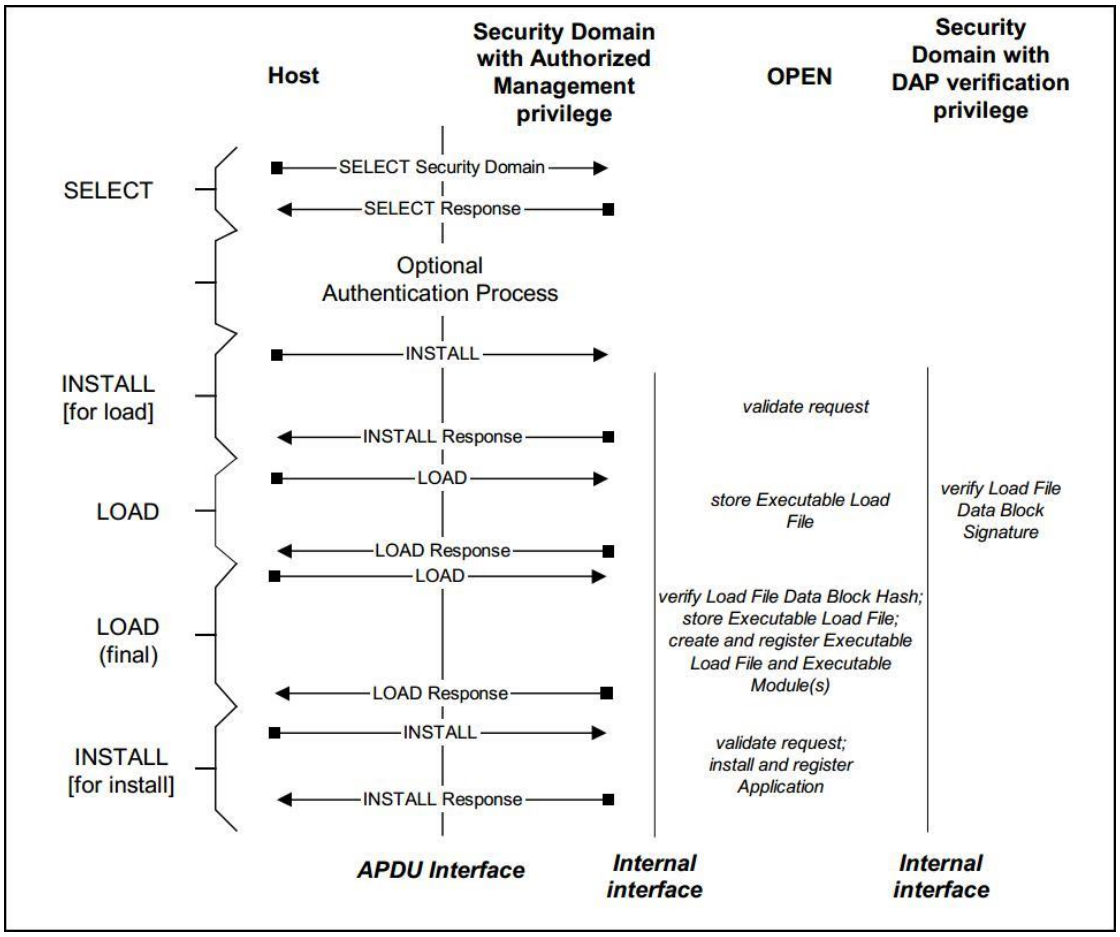


Figure 1: Applet Installation Flow

3.3. APDU Flow for Sample Applet Installation

（1）Select ISD

-> 00A4040000

<- 6F1B8408A000000003000000A50F730906072A864886FC6B019F6501FF（9000）

（2）Send INITIALIZE UPDATE

(with 8 bytes random number as Host Challenge)

-> 8050000008 D6B4BDC3B619EB02

<- 00006180123456780001FF0200040843E81CC9FFF3DB2F2420584EEA（9000）

（3）Send EXTERNAL AUTHENTICATE

(Host cipher: 6886B6F095B1DD10 C-MAC: 0BA974CA77E2DEF8)

-> 8482000010 6886B6F095B1DD10 0BA974CA77E2DEF8

<-（9000）

（4）INSTALL[for load]

-> 80E6020013 0611335577000008A0000000030000000000000

<- 00（9000）

（5）LOAD

-> 80E80000C0

C482017D010015DECAFFED020204000106113355770000047261 6E6402002100150021000
A00150042000E0098000A001B0000009E02E60000000000000201000400150202010 7A000
0000620101020107A0000000620102030 00A0106113355770001001706000E00000080030
2000207010000002B07009800031 0188C00071807058D000B870018058D000E87017A0530
8F00063D8C000F181D0441181D258B00087A0221188B000560037A198B000C2D1A032560
08116E008D000A1A0425

<- 00（9000）

-> 80E80001C0

7500140002FF84000D0001001A18198C00027008116D008D000A7A0522198B000C2D1A07
2532181F8C00093BAD00031A081F8D000D3B19081F8B00037A0420181D900B8700AD01AD
00031D8B0004AD007708000A0000000000000000000000500420010020002010200020006 0
0006203800A0803810E0103800303010002000680030003800302060000840680070106 80
080D03800A010680100206810E0006000001090 01B00070E075F170202070010050607080
40A07070C1508070A0A07

<- 00（9000）

-> 80E8800201 12

<- 00（9000）

（6）INSTALL[for install]

-> 80E60C001B 0611335577000006113355770001061133557700010100002C90000

<- 00（9000）

3.4. Removing Executable Load Files

(1) Detail for APDU: (DELETE)

Format: 80 E4 00 00 Lc Data

Example: 80/84 E4 00 00/80 Lc 4F AIDlen AID

(2) For the applet installed in step 3.0, the removing APDU is following:

-> 80E4008008 4F06113355770000

<- 00（9000）