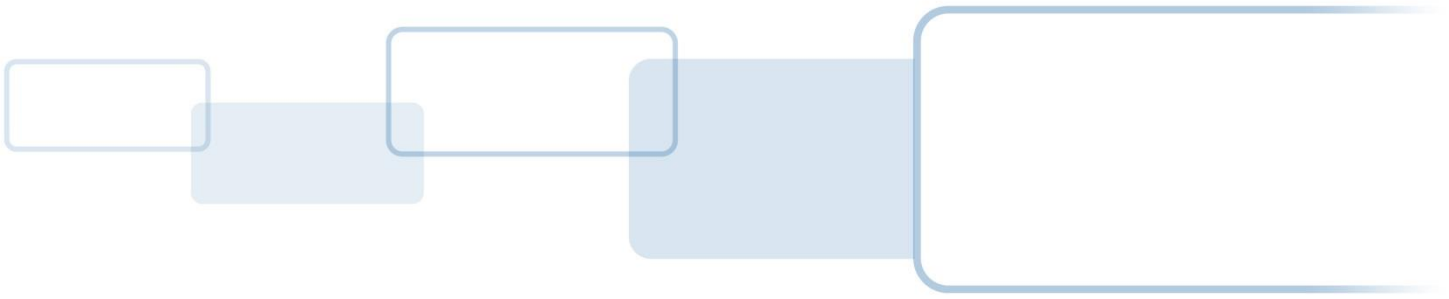
HID Partner Services - APDU Guide

Crescendo Low Level Access - Minidriver Profile Update

v 1.1 | November 13, 2017



Document Control

Document Contributor(s)

Name	Department
Adrian Castillo	HID Product Management
Ravikumara Siddappa	Center of Integration

Document Reviewer(s)

Name	Department
Lynn Chien	HID Partner Services
Ankur Gupta	Center of Integration

Document Approver(s)

Name	Department	Date Approved
Zahid Johar	HID Partner Services & COI	

Document Revision(s)

Date	Author	Version	Revision Description
May 16, 2017	Adrian Castillo	0.1	Document creation
September 12, 2017	Lynn Chien	0.2	Placed original document into template and review
October 26, 2017	Ravikumara Siddappa	0.3	Removed PIV card info and added applet info
October 27,2017	Ravikumara Siddappa	1.0	Review comments incorporation
November 13, 2017	Ravikumara Siddappa	1.1	Removed Proprietary section

Related Document(s)

Reference	Author	Version	Revision Description

Table of Contents

1 Introduction

This is a quick guide that describes the low level APDU Commands that are required to use the keys and certificates in Crescendo cards after they have been personalized by ActivID CMS or by manually using the Minidriver or ActivClient middleware.

1.1 Overview

Crescendo cards can be issued in one of two modes:

- A Minidriver card edge, that is used by the plug and play Windows Minidriver and by ActivClient middleware that is available for Windows, Linux and Mac OS
- A PIV card edge, compatible with NIST SP 800-73

HID recommends that a client application supports both modes and that it includes a discovery mechanism where it tries first the Minidriver plug-and-play AID as described below and, if that fails, then tries the PIV card edge configuration.

The card ATR is: 3B F9 96 00 00 80 31 FE 45 53 43 45 37 20 03 00 20 46 42

2 Using the Crescendo Low Level Access - Minidriver Profile Update

Crescendo cards can be issued in one of two modes:

- A Minidriver card edge, that is used by the plug and play Windows Minidriver and by ActivClient middleware that is available for Windows, Linux and Mac OS
- A PIV card edge, compatible with NIST SP 800-73

This document covers APDU's for Cresendo Minidriver based card only.

Important: HID recommends that a client application supports both modes and that it includes a discovery mechanism where it tries first the Minidriver plug-and-play AID as described below and, if that fails, then tries the PIV card edge configuration.

.

2.1 Applet versions and instances

- ACA Applet instance
  - Version 2.7.3.6
  - AID: A0000000791000
- PKI Applet instance
  - Version 2.7.3.6
  - AID: A0000000790101

2.2 Crescendo Minidriver

The steps required to identify a minidriver card, read certificates, and use the associated private keys for signatures are the following:

1. In the Crescendo Minidriver profile, select the ACA instance and verify the PIN. See the "Important" call-out below about PIN encoding. The default PIN of Crescendo cards is the ASCII code of 0 eight times, that appears highlighted in the example below:

```
00A4040007A0000000791000
< 6F0B8407A0000000791000A5009000
> 00200000083030303030303030
< 9000 (or 63CX with X number of remaining tries)
```

Important: A Crescendo card stores the value of the PIN internally in 8 bytes, which is always the data length for the Verify command. When doing PIN verification:

- If the PIN length is less than the effective PIN length (8 bytes), pad it with 0xFF
- If the PIN length is longer than the effective PIN length (8 bytes), pad it with zero to next multiple of 8 and DES CBC encrypt it using "30h.30h.30h.30h.30h.30h.30h.30h" for key and initial value. Use the last 8 bytes of the result as the hashed value of the PIN.

For example, if the PIN value was "Applez1995" with length 10 characters, it would first be padded to the next 8 bytes block:

```
4170706C657A31393935000000000000
```

The DES CBC result would be

```
6766E7DB89ECFACB5F067CE52BE7FC21
```

And the verify PIN APDU is

```
00200000085F067CE52BE7FC21
```

2. Select the PKI instance and get the properties to see which keys are initialized. The response to the Get Properties command (INS 0x56) has the TLV structure shown below, with the tag 0x40 indicating the number of PKI slots in the card and then a tag 0x51 with the state of each one of those keys. The value 0x0101 highlighted below is the ID of a key that is initialized. The value 0x07 indicates the key size is 2048 bits; that byte takes the value 0x06 for 1024 keys. The 0x01 at the end shows that this particular public key is initialized. The second byte from the end shows the particular private key is initialized.

```
> 00A4040007A0000000790101
< 6F0B8407A0000000790101A5009000
> 8056010000
< 01 05 10 02 07 03 06
40 01 09
51 11 41 02 01 01 42 05 00 20 00 C4 09 43 04 07 20 01 01
51 11 41 02 01 02 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 03 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 04 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 05 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 06 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 07 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 08 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 09 42 05 00 20 00 C4 09 43 04 07 20 01 00
90 00
```

3. If the key and certificate being used are those in the first slot, as the example above, then it is already selected. However, if we are using any other key, the corresponding object needs to be selected first instead of the default selected 0101, for example to select the second slot 0102 the command would be:

```
> 00A4020002 0102
< 9000
```

4. In Crescendo Minidriver cards, there are two types of buffers that contain data associated to each PKI slot. There is a T-Buffer that contains the tags and lengths of the elements and a V-Buffer with the actual values. First we need to get the length of the T-Buffer that is stored in the first two bytes of it. Then we read the number of bytes obtained in the response (0x0A in the example below) starting at offset 0x0002

```
> 80520000020102
< 0A009000
> 8052000202010A
< 6799710170FF6404FE009000
```

   From the response, we see that the V-Buffer will contain the values for tag 67 with length 0x99, tag 71 with length 01, tag 70 with length 0x0464, tag FE with length 0x00. Note that when the length is more than 254 bytes, then the length is indicated little-endian in three bytes with the first byte with the value 0xFF.

5. Send several Read Buffer commands to read tag 71 (to check if the certificate is deflated) and the certificate (tag 70) starting at the correct offset (skipping tag 67 and the first two bytes of the V-buffer that contains its total length)

```
> 8052009b0202FF
< 255 bytes | 9000
> 8052019a0202FF
< 255 bytes | 9000
> 805202990202FF
< 255 bytes | 9000
> 805203980202FF
< 255 bytes | 9000
> 80520497020269
< 105 bytes | 9000
```

6. If Tag 71 has value 0x01 indicating that the certificate is deflated, use zlib/gzip to inflate it, otherwise the certificate is already the raw ASN.1 bytes

7. To generate a signature, send one (for 1024 bit keys) or two (for 2048 bit keys) commands containing the PKCS#1 encoded hash to sign. Input data has to be the same length as the key. For a 2048 bit key (key type 07 from step 4) the commands would be the following. The first command has P1 = 0x80 to indicate that more blocks follow.

```
> 80428000FF | first 255 bytes of PKCS#1 signature block
< 9000
> 8042000001 | last byte to complete 256 bytes = 2048 bits
< 256 bytes signature | 9000
```

   The same command is used to decrypt data, except that the input is the PKCS#1 encrypted message (the first byte of the decrypted plaintext block will be 0x02) rather than a signature block, where the first byte is 0x01

NOTE: Smartcards communicate with ISO7816 T=0/T=1 protocols in contact mode. The SCardConnect API will return card supported protocol during initialization.

2.3 Difference b/w NIPR-ALT card and other CAC cards

The main difference between NIPR-ALT card and other cards is the presence of card capability container (CCC). NIPR-ALT cards will not have CCC.

The mechanism to identify NIPR-ALT card by checking CCC container, if container is not available then it can be identified based on version in applet properties

```
#Select PKI instance
> 00 A4 04 00 07 A0 00 00 00 79 01 01
< 6F 0B 84 07 A0 00 00 00 79 01 01 A5 00 90 00
#Get properties
> 80 56 01 00 00
< 01 05 10 02 07 03 06
40 01 09
51 11 41 02 01 01 42 05 00 20 00 C4 09 43 04 07 20 01 01
51 11 41 02 01 02 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 03 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 04 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 05 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 06 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 07 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 08 42 05 00 20 00 C4 09 43 04 07 20 00 00
51 11 41 02 01 09 42 05 00 20 00 C4 09 43 04 07 20 01 00
90 00
```

3 Glossary

Acronym	Description
ACA	Access Control Applet
AID	Application Identifier
API	Application Programming Interface
APDU	Smart Card Application Protocol Data Unit
CMS	HID Card Management System
NIST SP	National Institute of Standards and Technology Special Publication
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
TLV	Type Length Value

4 Trademarks

HID GLOBAL, HID, the HID logo, 4TRESS, ActivIdentity and ActivID are the trademarks or registered trademarks of HID Global Corporation, or its licensors, in the U.S. and other countries.

The absence of a mark, product, service name or logo from this list does not constitute a waiver of the HID Global trademark or other intellectual property rights concerning that name or logo. The names of actual companies, trademarks, trade names, service marks, images and/or products mentioned herein are the trademarks of their respective owners. Any rights not expressly granted herein are reserved.

Americas	+1 510.574.0100
US Federal	+1 571.522.1000
Europe	+33 (0) 1.42.04.84.00
Asia Pacific	+61 (0) 3.9809.2892

Corporate Headquarters

611 Center Ridge Drive
Austin, TX 78753
U.S.A.

www.hidglobal.com