HDCP Wireless Receiver Device Key Provisioning

Enabling Guide

April 2016

Revision 0.4

Intel Confidential

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. **No computer system can be absolutely secure.** Check with your system manufacturer or retailer or learn more at intel.com.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.

Contents

Figures

Revision History

Revision Number	Description	Revision Date
0.3	• Initial release.	March 2016
0.4	• Alpha Release	April 2016

§ §

1 Introduction

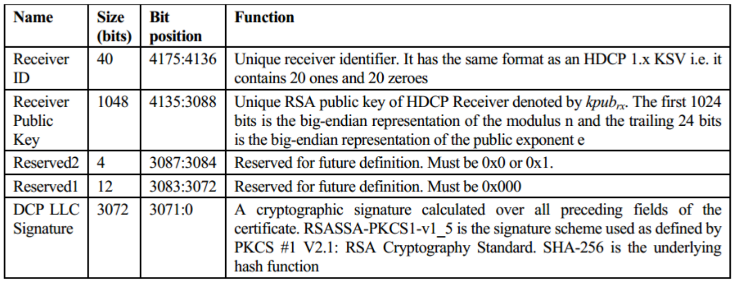
1.1 Purpose and Scope

This document describes the steps for an OEM to provision Kaby Lake platforms that runs Intel® Management Engine Firmware (Intel® ME) with HDCP Receiver support.

HDCP Receiver keys are required to enable Kaby Lake platform devices to play protected content while acting in the role of Miracast/Soft Sink Receiver.

1.2 Terminology

Term	Description
Crypto_lib	Cryptography program that is able to perform X.509 certificate verification and parsing and RSA encryption. OpenSSL is a popular crypto library.
FPT	Flash programming tool, an executable run on host
FW	Firmware
HDCP	High Bandwidth Digital Content Protection
IHV	Independent Hardware Vendor
Intel® ME	Intel's firmware-based Manageability Engine for Kaby Lake
Intel® MEI	Manageability Engine Interface
Kaby Lake	Intel® 10 Series Chipset Family SoC product name
Miracast	Miracast is a peer-to-peer wireless screen casting standard formed via Wi-Fi Direct connections. It enables wireless delivery of audio and video to or from desktops, tablets, mobile phones, and other devices.
Provisioning_cert.cer	HDCP provisioning X.509 certificate in DER format. This certificate contains the 2048-bit RSA public key (referred to as "provisioning_key" onwards in this document) that will be used by an OEM to encrypt HDCP device private key. This certificate is signed by Intel's root CA. The subject name of this certificate is referred to as "subject_name" onwards in this document. The size of the subject-name is 132 bytes

<table>
<tr><th>Term</th><th>Description</th></tr>
<tr><td>Receiver_cert.bin</td><td>Receiver certificate has the following format defined in HDCP specification. 522 bytes in size.

<table>
<tr><th>Name</th><th>Size (bits)</th><th>Bit position</th><th>Function</th></tr>
<tr><td>Receiver ID</td><td>40</td><td>4175:4136</td><td>Unique receiver identifier. It has the same format as an HDCP 1.x KSV i.e. it contains 20 ones and 20 zeroes</td></tr>
<tr><td>Receiver Public Key</td><td>1048</td><td>4135:3088</td><td>Unique RSA public key of HDCP Receiver denoted by $kpub_{rx}$. The first 1024 bits is the big-endian representation of the modulus n and the trailing 24 bits is the big-endian representation of the public exponent e</td></tr>
<tr><td>Reserved2</td><td>4</td><td>3087:3084</td><td>Reserved for future definition. Must be 0x0 or 0x1.</td></tr>
<tr><td>Reserved1</td><td>12</td><td>3083:3072</td><td>Reserved for future definition. Must be 0x000</td></tr>
<tr><td>DCP LLC Signature</td><td>3072</td><td>3071:0</td><td>A cryptographic signature calculated over all preceding fields of the certificate. RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function</td></tr>
</table>
</td></tr>
<tr><td>Receiver_private_key:</td><td>Device’s RSA private key “p” (device private CRT P), 64 bytes in size. Note that the HDCP LLC may provide other private key elements such as 64-byte q and 128-bytes d. For the purpose of provisioning, only p is required. Intel® ME FW will internally derive other private elements if necessary.</td></tr>
<tr><td>Root_cert.cer</td><td>Intel root CA’s (certificate authority) X.509 root certificate in DER format. This certificate contains Intel root CA’s RSA public key. It is self-signed.</td></tr>
<tr><td>SoC</td><td>System On Chip. Refers to Intel designs where the CPU, PCH and additional platform components are integrated into one package and/or silicon design</td></tr>
</table>

1.3 Prerequisite

The following materials must be ready before the provisioning:

Item	Provided By
Root_cert.cer	***Intel® ME FW Kit*** Location: …/Intel(R)_ME_11.5_xx_xx/Image Components/Certificates/HDCP
Provisioning_cert.cer	
Intel® FPT[Flash Programming Tool]	***Intel® ME FW Kit*** Location: …/Intel(R)_ME_11.5_xx_xx/Tools/System Tools
Receiver_private_key	***OEM*** Keys purchased from HDCP LLC
Receiver_cert.bin	
Crypto_lib	This is an open Source that OEMs use or their own custom tools for encryption

§ §

2 Provisioning HDCP Receiver Keys

2.1 HDCP Keys Receiver Provisioning Steps

Exercise the following steps below to perform provisioning.

Note: Abort the flow if any step fails.

Disclaimer:

- Provisioning keys are stored in flash. The following scenarios will result in keys getting lost/wiped:
  - Flash Corruption
  - RE-programming the entire Intel® ME region
- In case of key loss, systems will need to be returned to OEM for re-provisioning.

2.1.1 Disable Intel® Content Protection HECI Service (CPHS):

Note: You will need to follow this step if you provisioning the system after booting to OS [Windows]. Please ignore this step otherwise.

The Intel® Content Protection HECI Service is used to enable premium video playback (such as Blu-ray) for Intel® HD Graphics.

- Boot to OS [Windows]
- From an admin open a command prompt
- Type the command to disable Intel® CPHS

```
•   $ sc config cphs start=disabled
```

Disclaimer: Disabling the Intel® Content Protection HECI Service will prevent certain types of premium video from playing on the system; however, unprotected video such as user-generated content and YouTube* videos will continue to play.

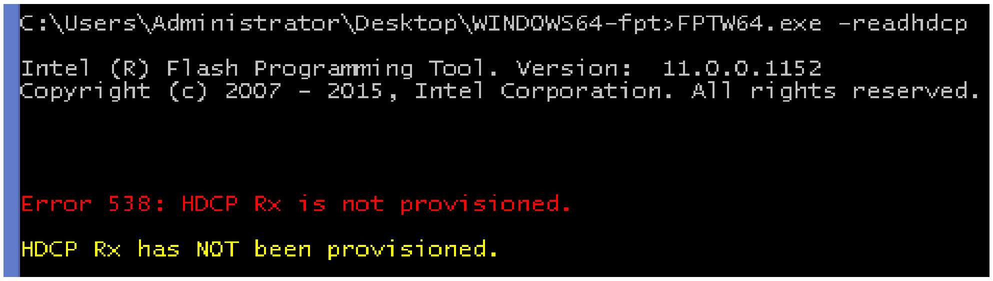
2.1.2 Verify Device Status:

a. Open a command prompt (Admin) and issue the read status command using Intel® FPT

```
$ fpt.exe -readhdcp
```

b. Intel® FPT reports status of provisioning:

Figure 2-1: Checking Provisioning Status



```
C:\Users\Administrator\Desktop\WINDOWS64-fpt>FPTW64.exe -readhdcp

Intel (R) Flash Programming Tool. Version:  11.0.0.1152
Copyright (c) 2007 - 2015, Intel Corporation. All rights reserved.



Error 538: HDCP Rx is not provisioned.

HDCP Rx has NOT been provisioned.
```

2.1.3 Encrypting Device Private Key using OpenSSL

- To parse Provisioning_cert.cer and extract subject_name and provisioning_key, run the following on OpenSSL command line.

```
$ openssl x509 -in provisioning_cert.cer -inform DER -text
```

- To verify the Intel CA's signature on Provisioning_cert.cer, run the following on OpenSSL command line.

```
$ openssl x509 -in Provisioning_cert.cer -inform DER -out
Provisioning_cert.pem

$ openssl x509 -in Root_cert.cer -inform DER -out
Root_cert.pem

$ openssl verify -CAfile Root_cert.pem
Provisioning_cert.pem
```

- To encrypt key_n_subjectName.bin with provisioning_key and result in encrypted_key_n_subjectName.bin.

```
$ openssl rsautl -encrypt -certin -inkey
Provisioning_cert.pem -in key_n_subjectName.bin -out
encrypted_key_n_subjectName.bin
```

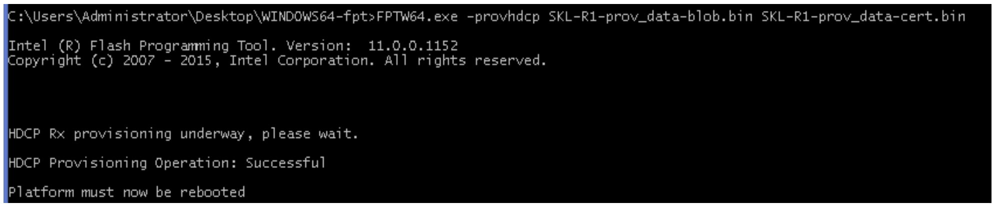
2.1.4 Provisioning the Device

a. From command prompt(Admin) issue the provision command:

```
$ fpt.exe -provhdcp encrypted_key_n_subjectName.bin
Receiver_cert.bin
```

b. Intel® FPT indicates device is provisioned.

Figure 2-2: Provisioning Platform using Intel® FPT



```
C:\Users\Administrator\Desktop\WINDOWS64-fpt>FPTW64.exe -provhdcp SKL-R1-prov_data-blob.bin SKL-R1-prov_data-cert.bin

Intel (R) Flash Programming Tool. Version:  11.0.0.1152
Copyright (c) 2007 - 2015, Intel Corporation. All rights reserved.



HDCP Rx provisioning underway, please wait.

HDCP Provisioning Operation: Successful

Platform must now be rebooted
```

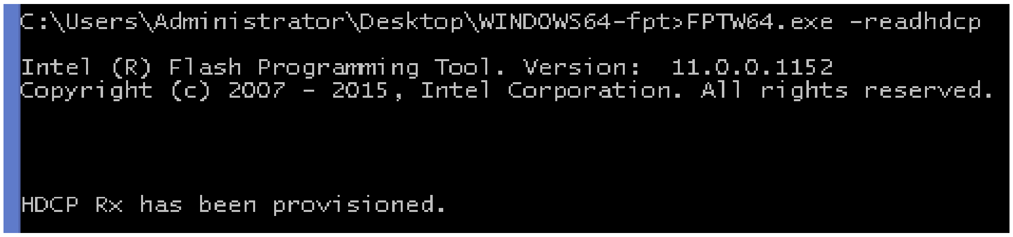
2.1.5 Verify Provisioning Status

a. Open a command prompt (Admin) and issue the read status command using Intel® FPT

```
$ fpt.exe -readhdcp
```

b. Intel® FPT indicates device is provisioned:

Figure 2-3: Verify HDCP Rx Provisioning using Intel(R) FPT



```
C:\Users\Administrator\Desktop\WINDOWS64-fpt>FPTW64.exe -readhdcp

Intel (R) Flash Programming Tool. Version:  11.0.0.1152
Copyright (c) 2007 - 2015, Intel Corporation. All rights reserved.



HDCP Rx has been provisioned.
```

2.1.6 Enable Intel® Content Protection HECI Service (CPHS):

Note: You will need to follow this step if you provisioning the system after booting to OS [Windows]. Please ignore this step otherwise.

From an admin command prompt

```
$ sc config cphs start=auto
$ sc start cphs
$ sc query cphs
```

§ §

3 Troubleshooting

1. FPT command – ‘fpt.exe –readhdcp ’tool gets hung during reading HDCP port
   a. Check if Intel® CPHS is running by running the following query and disable it:

```
$ sc query cphs
```

   b. Ensure latest MEI Driver is installed.

2. FPT Commands Status/Error Codes

Table 3-1: Verify HDCP Rx Provisioning using Intel(R) FPT

FPT Command	Status/Error Code	Comment
fpt.exe –readhdcp	0x0	Success. HDCP Rx is provisioned
	0x538	HDCP Rx not provisioned
	0x535	Reading HDCP Rx Failure
fpt –provhdcp <xx.bin> <Rxx.bin>	0x0	Success. HDCP Rx provisioning successful
	0x536	Cannot provision after closed Manuf.
	0x537	Provisioning with invalid certificate

§ §