Universal Serial Bus
Device Class Definition
for
Content Security Devices

Content Security Method 5
High-bandwidth Digital Content Protection 2.1
(HDCP 2.1) Implementation

Release 1.0

June 12, 2012
Scope of This Release
This document is the Release 1.0 of this Content Security Method 5 Definition.

Contributors
Jason Hawken  AMD
Jim Hunkins  AMD
Kenneth Ma  Broadcom Corporation
Alec Cawley  DisplayLink
Dan Ellis  DisplayLink
Trevor Hall  DisplayLink
Tom Burton  Fresco Logic
Jeff Foerster  Intel Corporation
Wey-Yi Guy  Intel Corporation
Steve McGowan  Intel Corporation
Abdul Rahman Ismail (Chair)  Intel Corporation
Barry O’Mahony (Editor)  Intel Corporation
Sridharan Ranganathan  Intel Corporation
Ygal Blum  Jungo
Yoav Nissim  Jungo
Joel Silverman  Kawasaki Microelectronics, Inc.
Geert Knapen  MCCI Corporation
Chris Yokum  MCCI Corporation
Richard Petrie  Nokia Corporation
Yoram Rimoni  Qualcomm, Inc
Shannon Cash  SMSC
Morgan Monks  SMSC
John Sisto  SMSC
Guy Stewart  SMSC
Mark Bohm  SMSC
Alexey Orishko  ST_Ericsson
Will Harris  Texas Instruments
Grant Ley  Texas Instruments
Paul Berg  USB-IF
A LICENSE IS HEREBY GRANTED TO REPRODUCE THIS SPECIFICATION FOR INTERNAL USE ONLY. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, IS GRANTED OR INTENDED HEREBY.

USB-IF AND THE AUTHORS OF THIS SPECIFICATION EXPRESSLY DISCLAIM ALL LIABILITY FOR INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS RELATING TO IMPLEMENTATION OF INFORMATION IN THIS SPECIFICATION. USB-IF AND THE AUTHORS OF THIS SPECIFICATION ALSO DO NOT WARRANT OR REPRESENT THAT SUCH IMPLEMENTATION(S) WILL NOT INFRINGE THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS.

THIS SPECIFICATION IS PROVIDED "AS IS" AND WITH NO WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE. ALL WARRANTIES ARE EXPRESSLY DISCLAIMED. USB-IF, ITS MEMBERS AND THE AUTHORS OF THIS SPECIFICATION PROVIDE NO WARRANTY OF MERCHANTABILITY, NO WARRANTY OF NON-INFRINGEMENT, NO WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE, AND NO WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE.

IN NO EVENT WILL USB-IF, MEMBERS OR THE AUTHORS BE LIABLE TO ANOTHER FOR THE COST OF PROCURING SUBSTITUTE GOODS OR SERVICES, LOST PROFITS, LOSS OF USE, LOSS OF DATA OR ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT, OR SPECIAL DAMAGES, WHETHER UNDER CONTRACT, TORT, WARRANTY, OR OTHERWISE, ARISING IN ANY WAY OUT OF THE USE OF THIS SPECIFICATION, WHETHER OR NOT SUCH PARTY HAD ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES.

All product names are trademarks, registered trademarks, or service marks of their respective owners.

Please send comments via electronic mail to cswg-chair@usb.org
# Table of Contents

Scope of This Release ............................................................................................................. 3
Contributors ............................................................................................................................. 3
Revision History ....................................................................................................................... Error! Bookmark not defined.

1. Introduction ......................................................................................................................... 11
  1.1. Scope ............................................................................................................................. 11
  1.2. Related Documents ....................................................................................................... 11
  1.3. Terms and Abbreviations ............................................................................................. 11

2. CSM-5 Content Security Class Additions .......................................................................... 13
  2.1. AKE USB Requests ....................................................................................................... 13
  2.2. Command and Response Requests Format .................................................................. 13
    2.2.1. PUT_COMMAND ................................................................................................. 13
    2.2.2. GET_RESPONSE ............................................................................................... 14
    2.2.3. GET_COMMAND .................................................................................................. 14
    2.2.4. PUT_RESPONSE .................................................................................................. 14
  2.3. HDCP 2.1 Commands and Responses ........................................................................ 14

3. CSM-5 Descriptors ............................................................................................................. 15
  3.1. Device Descriptor .......................................................................................................... 15
  3.2. Configuration Descriptor ............................................................................................. 15
  3.3. Content Security Interface Descriptor .......................................................................... 15
  3.4. Channel Descriptor ...................................................................................................... 15
  3.5. Content Security Method (CSM-5) Descriptor ............................................................. 15
  3.6. CSM-5 String Descriptor ............................................................................................ 15

4. HDCP 2.1 Packet Format ................................................................................................. 17

5. Example Sequence Diagrams .......................................................................................... 19
  5.1. AKE Sequence – Host is HDCP Transmitter ............................................................... 19
  5.2. AKE Sequence – Device is HDCP Transmitter ........................................................... 21
  5.3. Locality Check Sequence – Host is HDCP Transmitter ............................................... 22
  5.4. Locality Check Sequence – Device is HDCP Transmitter .......................................... 22
  5.5. Repeater Authentication Report Sequence – Host is HDCP Transmitter .................... 23
  5.6. Repeater Authentication Report Sequence – Device is HDCP Transmitter ................. 24

6. HDCP 2.1 Stream Parameters .......................................................................................... 25
List of Tables
Table 1-1: Terms and Abbreviations.................................................................................................................................................. 11
Table 2-1: General Request Layout.................................................................................................................................................. 13
Table 2-2: Command-Response Pairing......................................................................................................................................... 13
Table 2-3: PUT_COMMAND Request.............................................................................................................................................. 14
Table 2-4: GET_RESPONSE Request.............................................................................................................................................. 14
Table 2-5: GET_COMMAND Request.............................................................................................................................................. 14
Table 2-6: PUT_RESPONSE Request.............................................................................................................................................. 14
Table 3-1: CSM-5 Descriptor......................................................................................................................................................... 15
Table 3-2: CSM-5 String Descriptor.............................................................................................................................................. 15
List of Figures

Figure 4-1: HDCP 2.1 Packet Format......................................................................................................................... 17
Figure 5-1: Example AKE Sequence, previously paired HDCP Transmitter (Host) and HDCP Receiver (Device) ...... 20
Figure 5-2: Example AKE Sequence, previously paired HDCP Transmitter (Device) and HDCP Receiver (Host) .... 21
Figure 5-3: Example Locality Check (LC) Sequence, HDCP Transmitter (Host) and HDCP Receiver (Device) ......... 22
Figure 5-4: Example Locality Check (LC) Sequence, HDCP Transmitter (Device) and HDCP Receiver (Host) ......... 22
Figure 5-4: Example SKE Exchange Sequence, HDCP Transmitter (Host) and HDCP Receiver (Device) ............... 23
Figure 5-5: Example SKE Exchange Sequence, HDCP Transmitter (Device) and HDCP Receiver (Host) ............... 23
Figure 5-5: Example Repeater Authentication, HDCP Transmitter (Host) and HDCP Receiver (Device) ............... 24
Figure 5-6: Example Repeater Authentication, HDCP Transmitter (Device) and HDCP Receiver (Host) ............... 24
1. **Introduction**

This document describes the USB transport services and protocol formats that support High-bandwidth Digital Content Protection (HDCP) 2.1.

1.1. **Scope**

USB CSM5 describes the USB transport services, descriptors, and requests necessary to support HDCP2.1 protocols over USB. This document does not change or alter HDCP2.1 functionality.

The Content Security Class (CSC) specification allows Content Security Methods (CSM) to define additional requests as needed. CSM5 defines additional USB CSC requests in order to support HDCP2.1 AKE protocols between USB Host and Device. In addition, CSM5 implements the Content Security Notification Service and defines additional notifications that are needed to support HDCP2.1 protocols.

1.2. **Related Documents**


1.3. **Terms and Abbreviations**

This section defines terms used throughout this document. For additional terms that pertain to the Universal Serial Bus, see Chapter 2, “Terms and Abbreviations,” in [USB2.0] and [USB3.0].

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AKE</td>
<td>Authentication and Key Exchange</td>
</tr>
<tr>
<td>Content Security Device</td>
<td>Any USB Device that contains a Content Security Interface.</td>
</tr>
<tr>
<td>Channel</td>
<td>A logical path over which secure data can be transmitted or received.</td>
</tr>
<tr>
<td>Content Provider</td>
<td>The owner of the content.</td>
</tr>
<tr>
<td>CPM</td>
<td>Content Protection Method, refers to a content provider protection scheme.</td>
</tr>
<tr>
<td>CS</td>
<td>Content Security. USB terminology for content protection.</td>
</tr>
<tr>
<td>CSC</td>
<td>Content Security Class. Refers to USB Device Class Definition for Content Security Devices.</td>
</tr>
<tr>
<td>CSI</td>
<td>Content Security Interface.</td>
</tr>
<tr>
<td>CSM</td>
<td>Content Security Method.</td>
</tr>
<tr>
<td>CSNS</td>
<td>Content Security Notification Service.</td>
</tr>
<tr>
<td>HDCP</td>
<td>High-bandwidth Digital Content Protection</td>
</tr>
<tr>
<td>Sink</td>
<td>The target of secure data transfers.</td>
</tr>
<tr>
<td>Source</td>
<td>The source of secure data transfers.</td>
</tr>
</tbody>
</table>
2. **CSM-5 Content Security Class Additions**

The USB Device Class Definition for Content Security Devices (CSC) allows Content Security Methods to define additional services as needed. HDCP2.1 requires four USB Requests to transfer the Authentication Protocol commands and responses also referred to as Authentication Protocol Messages (APM). The CS Notification Service (CSNS) is used to allow USB devices to initiate HDCP2.1 Authentication Protocols.

HDCP Authentication Protocol transactions are performed in order to authenticate that the Device or Host that is receiving premium content, is a valid HDCP receiver. The keys exchanged during an Authentication session are used to protect the stream identified by the ChannelID. If there are multiple streams per Host/Device pair, then an Authentication session shall be established per ChannelID.

### 2.1. Authentication Protocol USB Requests

HDCP2.1 requires four USB requests to transfer the Authentication Protocol command frames and corresponding responses. This section details the structure of these requests. The General Request format for Authentication Protocol Command Response request is as follows:

#### Table 2-1: General Request Layout

<table>
<thead>
<tr>
<th>Offset</th>
<th>Field</th>
<th>Size</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>bmRequestType</td>
<td>1</td>
<td>Bitmap</td>
<td>D4..0: Recipient</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0b000001: Interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>D6..5: Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0b01: Class</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>D7: Data Transfer Direction</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0b0: Host to Device</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0b1: Device to Host</td>
</tr>
<tr>
<td>1</td>
<td>bRequest</td>
<td>1</td>
<td>Number</td>
<td>CSM-5 Requests:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>PUT_COMMAND, GET_RESPONSE, GET_COMMAND, PUT_RESPONSE.</td>
</tr>
<tr>
<td>2</td>
<td>wValue</td>
<td>2</td>
<td>Number</td>
<td>HByte: Reserved. Shall be set to zero.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LByte: CSM-5 Identifier. Shall be set to 0x05.</td>
</tr>
<tr>
<td>4</td>
<td>wIndex</td>
<td>2</td>
<td>Number</td>
<td>HByte: Channel ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LByte: CSI Interface Number</td>
</tr>
<tr>
<td>6</td>
<td>wLength</td>
<td>2</td>
<td>Number</td>
<td>Byte length of the Authentication Protocol Command or Response.</td>
</tr>
</tbody>
</table>

### 2.2. Command and Response Requests Format

The requests are paired together, one pair (PUT_COMMAND, GET_RESPONSE) is used to send Authentication Protocol commands to the Device and return the associated response. The other pair is used to retrieve an Authentication Protocol command from the Device and send the associated response.

#### Table 2-2: Command-Response Pairing

<table>
<thead>
<tr>
<th>Command</th>
<th>Associated Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUT_COMMAND</td>
<td>GET_RESPONSE</td>
</tr>
<tr>
<td>GET_COMMAND</td>
<td>PUT_RESPONSE</td>
</tr>
</tbody>
</table>

### 2.2.1. PUT_COMMAND

The PUT_COMMAND request is used to transfer an Authentication Protocol Command from the Host to the Device.
Table 2-3: PUT_COMMAND Request

<table>
<thead>
<tr>
<th>bmRequestType</th>
<th>bRequest</th>
<th>wValue</th>
<th>wIndex</th>
<th>wLength</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0b00100001</td>
<td>PUT_COMMAND</td>
<td>HByte: 0x00</td>
<td>HByte: Channel ID</td>
<td>Length of Command (in bytes)</td>
<td>HDCP 2.1 Command</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LByte: 0x05</td>
<td>LByte: CSI interface number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.2.2. GET_RESPONSE

The GET_RESPONSE request is used to transfer an Authentication Protocol Response from the Device to the Host.

Table 2-4: GET_RESPONSE Request

<table>
<thead>
<tr>
<th>bmRequestType</th>
<th>bRequest</th>
<th>wValue</th>
<th>wIndex</th>
<th>wLength</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0b10100001</td>
<td>GET_RESPONSE</td>
<td>HByte: 0x00</td>
<td>HByte: Channel ID</td>
<td>Length of Response (in bytes)</td>
<td>HDCP 2.1 Response</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LByte: 0x05</td>
<td>LByte: CSI interface number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.2.3. GET_COMMAND

The GET_COMMAND request is used to transfer an Authentication Protocol Command from the Device to the Host.

Table 2-5: GET_COMMAND Request

<table>
<thead>
<tr>
<th>bmRequestType</th>
<th>bRequest</th>
<th>wValue</th>
<th>wIndex</th>
<th>wLength</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0b10100001</td>
<td>GET_COMMAND</td>
<td>HByte: 0x00</td>
<td>HByte: Channel ID</td>
<td>Length of Command (in bytes)</td>
<td>HDCP 2.1 Command</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LByte: 0x05</td>
<td>LByte: CSI interface number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.2.4. PUT_RESPONSE

The PUT_RESPONSE request is used to transfer an Authentication Protocol Response from the Host to the Device.

Table 2-6: PUT_RESPONSE Request

<table>
<thead>
<tr>
<th>bmRequestType</th>
<th>bRequest</th>
<th>wValue</th>
<th>wIndex</th>
<th>wLength</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0b00100001</td>
<td>PUT_RESPONSE</td>
<td>HByte: 0x00</td>
<td>HByte: Channel ID</td>
<td>Length of Response (in bytes)</td>
<td>HDCP 2.1 Response</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LByte: 0x05</td>
<td>LByte: CSI interface number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3. HDCP 2.1 Commands and Responses

HDCP messages are exchanged between Host and Device or vice-versa according to Authentication Protocol procedures specified in [HDCP2.1], using a USB request specified in Section 2.2, "Command and Response Requests Format". HDCP Messages sent from an HDCP Transmitter to an HDCP Receiver are designated as Commands for the purposes of this document. Messages sent from an HDCP Receiver to an HDCP Transmitter are designated as Responses. Both USB Hosts and USB Devices may act as either HDCP Transmitters or HDCP Receivers.
3. **CSM-5 Descriptors**

This section describes information relevant to the CSM-5 instantiation and the use of CSC descriptors. Each subsection corresponds to a CSC descriptor and only values pertinent to CSM-5 are listed in each subsection. Note that some subsections may not have any data and therefore the definition and use of the descriptor as specified in CSC is sufficient.

3.1. **Device Descriptor**

No additional definition needed.

3.2. **Configuration Descriptor**

No additional definition needed.

3.3. **Content Security Interface Descriptor**

No additional definition needed.

3.4. **Channel Descriptor**

Depending on the transport resource that needs content protection services, the appropriate Channel descriptor shall be selected (Interface, Endpoint, or AVData Channel descriptor).

The Channel descriptor shall indicate at least CSM-5 as one of the supported Content Security Methods, i.e. one of the bMethod[i] fields shall be set to 0x05.

Other Content Security Methods may be supported on the same Channel.

3.5. **Content Security Method (CSM-5) Descriptor**

**Table 3-1: CSM-5 Descriptor**

<table>
<thead>
<tr>
<th>Offset</th>
<th>Field</th>
<th>Size</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>bLength</td>
<td>1</td>
<td>Number</td>
<td>Size of this descriptor, in bytes: 6.</td>
</tr>
<tr>
<td>1</td>
<td>bDescriptorType</td>
<td>1</td>
<td>Constant</td>
<td>CSM. See Appendix A.2 in [USBCS].</td>
</tr>
<tr>
<td>2</td>
<td>bMethodID</td>
<td>1</td>
<td>Number</td>
<td>Method ID of a Content Security Method. Shall be set to 0x05.</td>
</tr>
<tr>
<td>3</td>
<td>iCSMDescriptor</td>
<td>1</td>
<td>Index</td>
<td>Index of the String descriptor that describes the Content Security Method. See Section 3.6, &quot;CSM-5 String Descriptor&quot;.</td>
</tr>
<tr>
<td>4</td>
<td>bcdVersion</td>
<td>2</td>
<td>BCD</td>
<td>CSM Descriptor Version number in Binary-Coded Decimal. This filed identifies the version of the HDCP that is supported. Shall be set to 0x0210.</td>
</tr>
</tbody>
</table>

The CSMData field is not used and shall therefore not be present.

3.6. **CSM-5 String Descriptor**

**Table 3-2: CSM-5 String Descriptor**

<table>
<thead>
<tr>
<th>Offset</th>
<th>Field</th>
<th>Size</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>bLength</td>
<td>1</td>
<td>Number</td>
<td>Size of this descriptor, in bytes: 108.</td>
</tr>
<tr>
<td>1</td>
<td>bDescriptorType</td>
<td>1</td>
<td>Constant</td>
<td>STRING. See Table 9-5 in [USB2.0] or [USB3.0].</td>
</tr>
<tr>
<td>2</td>
<td>bString</td>
<td>106</td>
<td>UTF-16LE</td>
<td>This field shall contain the following string (without the square brackets): [High-bandwidth Digital Content ProtectionRevision 2.1]</td>
</tr>
</tbody>
</table>
4. **HDCP 2.1 Packet Format**

The contents and structure of the APM Data are detailed in [HDCP2.1].

As defined in Section 4.2 of the reference, the first byte, APM[1], is the *msg_id* field of the AKE message, with the remaining bytes in the field as defined for the particular message. Preceding the *msg_id* field is the *N* field, indicating the length in bytes of the APM data field, APM[1..N].

The N/R bit of the *msg_id* field shall be set to one when the USB Device is not yet ready to supply the data for the APM in question. Otherwise, the N/R bit shall be set to zero.

When the N/R bit is set to one then:

- If there is a pending Command or Response being processed, the *msg_id* field shall be set to the value of the pending Command or Response; otherwise it shall be set to zero.
- The *N* field shall be set to one.

The USB device shall not transition to the next step in the sequence diagrams (see Section 195) unless the entire command/response has been successfully sent.
5. **Authentication Sequence Diagrams**

All of these are normative examples.

5.1. **AKE Sequence – Host is HDCP Transmitter**

Figure 5-1 shows an example Authentication and Key Exchange (AKE) sequence diagram for the case where the USB Host is the HDCP Transmitter and the USB Device is the HDCP Receiver. It is assumed that the Host and Device have been previously paired. See Figure 2.2 of [HDCP2.1] for an illustration of this transaction.

Note that in some cases, the Device returns a NOT_YET_READY (i.e. the device sets the N/R bit set to one in the msg_id field) in response to a GET_COMMAND or GET_RESPONSE request. The Host then attempts the request again at a later time.
Figure 5-1: Example AKE Sequence, previously paired HDCP Transmitter (Host) and HDCP Receiver (Device)

Note: If the Host requests the AKE_Send_H_prime Response less than 200 ms after the AKE_Stored_km Command, the Device may return NOT_YET_READY. The AKE_Send_H_prime Response in a successful HDCP AKE transaction shall be returned no later than 200 ms after the AKE_Stored_km Command, but may be returned sooner.
5.2. **AKE Sequence – Device is HDCP Transmitter**

Figure 5-2 shows an example Authentication and Key Exchange (AKE) sequence diagram for the case where the USB Host is the HDCP Receiver and the USB Device is the HDCP Transmitter. It is assumed that the Host and Device have been previously paired. See Figure 2.2 of [HDCP2.1] for an illustration of this transaction.

![Diagram](image)

**Figure 5-2**: Example AKE Sequence, previously paired HDCP Transmitter (Device) and HDCP Receiver (Host)
5.3. **Locality Check Sequence – Host is HDCP Transmitter**

Figure 5-3 shows an example Locality Check (LC) sequence diagram for the case where the USB Host is the HDCP Transmitter and the USB Device is the HDCP Receiver. See Figure 2.5 of [HDCP2.1] for an illustration of this transaction.

![Diagram of Locality Check Sequence - Host is HDCP Transmitter]

5.4. **Locality Check Sequence – Device is HDCP Transmitter**

Figure 5-4 shows an example Locality Check (LC) sequence diagram for the case where the USB Host is the HDCP Receiver and the USB Device is the HDCP Transmitter. See Figure 2.5 of [HDCP2.1] for an illustration of this transaction.

![Diagram of Locality Check Sequence - Device is HDCP Transmitter]
5.5. **SKE Exchange Sequence – Host is HDCP Transmitter**

Figure 5-5 shows an example SKE sequence diagram for the case where the USB Host is the HDCP Transmitter and the USB Device is the HDCP Receiver.

![Figure 5-5: Example SKE Exchange Sequence, HDCP Transmitter (Host) and HDCP Receiver (Device)](image)

5.6. **SKE Exchange Sequence – Device is HDCP Transmitter**

Figure 5-6 shows an example SKE sequence diagram for the case where the USB Host is the HDCP Receiver and the USB Device is the HDCP Transmitter.

![Figure 5-6: Example SKE Exchange Sequence, HDCP Transmitter (Device) and HDCP Receiver (Host)](image)
5.7. **Repeater Authentication Report Sequence – Host is HDCP Transmitter**

Figure 5-7 shows an example Repeater Authentication Report sequence diagram for the case where the USB Host is the HDCP Transmitter and the USB Device is the HDCP Receiver. See Figure 2.6 of [HDCP2.1] for an illustration of this transaction.

![Diagram](image)

Figure 5-7: Example Repeater Authentication, HDCP Transmitter (Host) and HDCP Receiver (Device)

5.8. **Repeater Authentication Report Sequence – Device is HDCP Transmitter**

Figure 5-8 shows an example Repeater Authentication Report sequence diagram for the case where the USB Host is the HDCP Receiver and the USB Device is the HDCP Transmitter. See Figure 2.6 of [HDCP2.1] for an illustration of this transaction.

![Diagram](image)

Figure 5-8: Example Repeater Authentication, HDCP Transmitter (Device) and HDCP Receiver (Host)
6. **HDCP 2.1 Stream Parameters**

Each stream protected by HDCP2.1 shall contain parameters to indicate real-time encryption state (enabled or disabled), and to maintain encryption synchronization between HDCP Transmitter and HDCP Receiver. As described in [HDCP2.1], each stream has an associated 4-byte parameter `streamCtr` and an 8-byte parameter `inputCtr`.