High-bandwidth Digital Content Protection Specification Compliance Test Specification

Revision 1.1

June 14, 2006

Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel Corporation disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

The cryptographic functions described in this specification may be subject to export control by the United States, Japanese, and/or other governments.

Acknowledgement

Matsushita Electric Industrial Co., Ltd., Philips Semiconductors and Silicon Image Inc. have contributed to the development of this guideline.

Intellectual Property

Implementation of this guideline requires a license from the Digital Content Protection LLC.

Contact Information

Digital Content Protection LLC
C/O Vital Technical Marketing, Inc.
5440 SW Westgate Drive, Suite 217
Portland, OR 97221

Email: info@digital-cp.com

Web: www.digital-cp.com

Revision History

31 May 06 – 1.0 Revision. Publication on DCP LLC web site

14 June 06 – 1.1 Revision. Publication on DCP LLC web site

Introduction

Purpose and Scope

This document specifies test procedures that will be used to test devices for compliance with the HDCP specification version 1.2.

Tests are specified for HDCP Source, HDCP Sink and HDCP Repeater devices.

Normative References

Digital Content Protection LLC, "High-bandwidth Digital Content Protection System Specification", Revision 1.2

In addition to the HDCP Compliance tests mentioned in this document, the Simplay HD Logo Program tests for interoperability between HDMI/HDCP devices and is highly recommended.

Definitions

Acronyms and Abbreviations

DUT	Device Under Test
PCP	Product Capability Parameter
TE	Test Equipment
PA	Protocol Analyzer
PG	Protocol Generator
TRF	Test Results Form
CDF	Capabilties Declaration Form. This is a questionnaire that the supplier of the DUT fills out prior to the testing phase. It provides additional information about the device, its modes, and its intended operation

Glossary of Terms

WARNING DUT's operation did not meet expectations, but because this test only tests for compliance with recommendations, it cannot be treated as a failure.

PASS The test result. No error(s) / problem(s) were detected in the DUT's operation, although the DUT may have WARNING item(s).

FAIL The test result. Error(s) / problem(s) were detected in the DUT's operation

Product Capability Parameter (PCP)

Source Capability

Source_Max_KSV Maximum number of downstream devices listed in KSV list which the DUT supports (1, 2 … up to 127)

Source_Authe_Count Number of times the DUT attempts authentication before it transitions into the authenticated state. The "Source_Authe_Count" number of authentications is verified (1, 2…or X)

Source_Out_OnlyRep Does DUT output contents to a repeater to which no downstream device is connected (ie. Repeater whose

DEVICE_COUNT is zero is connected to DUT's downstream port)? (Y/N)

Sink Capability

Sink_1.1Features_Supported Does DUT support ADVANCED_CIPHER mode and Enhanced Link Verification? (Y/N)

Sink_Audio_Supported Does DUT support the audio output? (Y/N)

Repeater Capability

Repeater_1.1Features_Supported Does DUT support ADVANCED_CIPHER mode and Enhanced Link Verification? (Y/N)

Repeater_Audio_Supported Does DUT support the audio output? (Y/N)

Repeater_HPD_pulse Does DUT have the capability to output HPD pulse by user operation? (Y/N)

Repeater_Max_KSV How many devices are supported by the size of the KSV FIFO? (1, 2 … up to 127)

Repeater_Out_OnlyRep Does DUT output contents to the downstream repeater to which no downstream device is connected (ie. Repeater whose DEVICE_COUNT is zero is connected to DUT's downstream port)? (Y/N)

HDCP Specification Compliance Test Specification

The HDCP Compliance Test Specification uses Pseudo-sinks, Pseudo-repeaters and Pseudo-source TEs to test corresponding source, sink and repeater DUTs. The TEs simulate the behavior of sources, sinks and repeaters and can be configured to test the behavior of the DUTs under normal and error conditions.

1. Transmitter Test

Transmitter's procedure is tested under the following two conditions of connection.

- Receiver is connected
- Repeater is connected

Note: The source is required to play protected content thus requiring HDCP to be enabled

1A. Downstream procedure with Receiver

Transmitter's downstream procedure with Receiver is tested under the following two conditions of connection.

- HDMI-capable Receiver is connected
- DVI Receiver is connected

□ With HDMI-capable Receiver

Transmitter's procedure is tested when it is connected to HDMI-capable Receiver.

- In this test, DUT should transmit one of the following video format signals with Data Island period in HDMI mode.
    - 640x480p@59.94/60Hz
    - 720x480p@59.94/60Hz
    - 720x576p@50Hz

1A-01. Regular procedure: With HDMI-capable Receiver

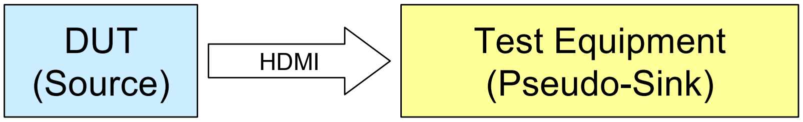
Test Objective

Verify that Transmitter performs the correct HDCP Authentication Protocol using production keys with the downstream HDMI-capable Receiver.

Required Test Method

<Connection Setup>

□ Connect TE to the downstream HDCP-protected Interface Port of DUT.



<Configuration of TE>

Initial Setting	
EDID	HDMI-capable
HDCP port	readable (i.e. it can be accessed)
Bcaps: REPEATER bit	0
First Part of Authentication	
Bcaps: 1.1_FEATURES bit	0
Bksv	valid value
R0’	correctly computed value
Third Part of Authentication	
Ri’	correctly computed value

<Test Case>

[Before starting authentication]

(STEP TP01)

□ TE asserts HPD. (TE’s Bstatus: HDMI_MODE is zero.)

(STEP TP02)

Confirm the video signal is transmitted to an unauthenticated Receiver

□ DUT reads EDID and begins sending unencrypted video signal (EESS: ENC_DIS) by HDMI protocol (i.e. one Data island at least once per two video fields).

➢ If DUT begins the first part of authentication before starting to send video signal, then FAIL. (Refer to ‘Ref-1A-1’)

(STEP TP03)

- □ TE sets Bstatus: HDMI_MODE after reception of a Data Island.

(STEP TP04)

- □ DUT begins the first part of authentication after successful transition to HDMI mode.
    - ➢ If DUT begins the first part of authentication before TE transitions to HDMI mode (i.e. before TE sets Bstatus: HDMI_MODE), then WARNING. (Refer to 'Ref-1A-2')

[First Part of Authentication]

(STEP T101)

- □ As the first part of authentication protocol, DUT performs the actions below.
    - ● Read Bcaps (REPEATER, 1.1_FEATURE)
    - ● Read Bksv
    - ● Write An
    - ● Write Aksv

Note: The order of the read access of Bksv and Bcaps does not matter. Bcaps and Bksv may be read after writing Aksv.

Note: DUT may start re-authentication at any time. If it happens, TE outputs the actual procedures in order but only uses the last-performed authentication to decide the test result.

(STEP T102)

- □ The following are considered as errors in the DUT's operation.

Verify the start of the authentication

- ➢ If DUT does not start the first part of authentication, then FAIL. (Refer to 'Ref-1A-3')

Verify the timing to write Aksv

- ➢ If Aksv was written before writing An, then FAIL. (Refer to 'Ref-1A-4')

Verify whether facsimile keys are being used

- ➢ If Aksv same as facsimile Aksv, then FAIL.

Verify Ainfo: ENABLE_1.1_FEATURES

- ➢ Ainfo: ENABLE_1.1_FEATURES bit was set to one after writing Aksv, then FAIL. (Refer to 'Ref-1A-5')

Note: TE does not support Advance Cipher and Enhanced Link Verification.

(STEP T103)

Verify the timing to read R0'

- □ TE calculates R0'.
- □ DUT reads R0'. This must be attempted later than 100 ms after writing Aksv.

- If DUT does not wait at least 100 ms to read R0' after writing Aksv, then FAIL. (Refer to 'Ref-1A-6')

(STEP T104)

Verify the timing of HDCP Encryption enabled

- □ DUT enables HDCP Encryption from disabled state (i.e. EESS: ENC_DIS -> ENC_EN) after reading R0'.
  - If DUT enables HDCP Encryption before reading the whole two bytes of R0', then FAIL. (Refer to 'Ref-1A-8')

[Third Part of Authentication]

(STEP T301)

- □ TE updates Ri' for every 128th frame from the first encrypted frame.

Verify the timing to read Ri'

- □ DUT reads Ri' at the authenticated state. This is made at the nominal rate of once every two seconds, plus one-half second.
  - If DUT does not read Ri' within 3.5 seconds after the previous reading, then FAIL. (Refer to 'Ref-1A-9')
  - If DUT does not read the whole two bytes of Ri', then FAIL.(Refer to 'Ref-1A-7')

(STEP TT01)

Verify CTLx, Keep-out period, Line Key Calc period

- □ The following are considered as errors in the DUT's operation.
  - If the encryption enable/disable value (EESS: ENC_DIS/ENC_EN) is not transmitted during the valid period, then FAIL. (Refer to 'Ref-1A-10')
  - If any Data Island, Video Data, or Guard Band is transmitted during keep-out period, then FAIL. (Refer to 'Ref-1A-11')
  - If any Data Island is transmitted during Line Key Calc period on the encrypted frame, then FAIL. (Refer to 'Ref-1A-12')

(STEP TT02)

Verify HDCP Encryption

- □ The following are checked to determine whether HDCP encryption is correctly applied. (Refer to 'Ref-1A-13')
  - Video: if the decrypted and shown image is not considered right visually, then FAIL.
  - Audio: if any error is detected by decrypting all packets which are transmitted in Data Island period and verifying their BCH ECC, then FAIL.

- □ Otherwise, if DUT completes the authentication, PASS.

1A-02. Regular procedure: HPD after writing Aksv

Test Objective

Verify that Transmitter enters the No Receiver Attached state when HPD is de-asserted after writing Aksv and then re-starts the authentication after HPD is asserted by the downstream Receiver.

Required Test Method

<Connection Setup>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver'.

<Configuration of TE>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver'.

<Test Case>

[Before starting authentication] described in '1A-01 Regular procedure: With HDMI-capable Receiver' is performed.

[First Part of Authentication]

(STEP T101) and **(STEP T102)** of [First Part of Authentication] described in '1A-01 Regular procedure: With HDMI-capable Receiver' are performed.

□ TE pulses HPD of the upstream HDCP-protected Interface Port to DUT more than 100 ms.

Verify the attempt of re-authentication

□ DUT attempts to re-start the first part of authentication.

- ➢ If DUT performs the procedures of **(STEP T101)** described in '1A-01 Regular procedure: With HDMI-capable Receiver' while TE is de-assserting HPD, then WARNING. (Refer to 'Ref-1A-14')
- ➢ If DUT enables and keeps HDCP Encryption, then FAIL. (Refer to 'Ref-1A-14')
- ➢ If DUT does not perform the procedures of **(STEP T101)** described in '1A-01 Regular procedure: With HDMI-capable Receiver' once again, then WARNING. (Refer to 'Ref-1A-14')

Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

□ Otherwise, PASS.

□ The following is an acceptable operation by the DUT.

- ➢ If DUT has no FAIL test results and DUT performs the procedures of **(STEP T101)** described in '1A-01 Regular procedure: With HDMI-capable Receiver' once again, then PASS. (Refer to 'Ref-1A-14')

1A-03. Regular procedure: HPD after starting third part of authentication

Test Objective

Verify that Transmitter enters the No Receiver Attached state when HPD is de-asserted during the third part of authentication and then re-starts the authentication after HPD is asserted by the downstream Receiver.

Required Test Method

<Connection Setup>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver'.

<Configuration of TE>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver'.

<Test Case>

The procedures from [Before starting authentication] to [Third Part of Authentication] described in '1A-01 Regular procedure: With HDMI-capable Receiver' are performed.

□ TE pulses HPD of the upstream HDCP-protected Interface Port to DUT more than 100 ms.

Verify the attempt of re-authentication

□ DUT attempts to re-start the first part of authentication.

- ➢ If DUT performs the procedures of **(STEP T101)** described in '1A-01 Regular procedure: With HDMI-capable Receiver' while TE is de-assserting HPD, then WARNING. (Refer to 'Ref-1A-14')
- ➢ If DUT keeps HDCP Encryption, then FAIL. (Refer to 'Ref-1A-14')
- ➢ If DUT does not perform the procedures of **(STEP T101)** described in '1A-01 Regular procedure: With HDMI-capable Receiver' once again, then WARNING. (Refer to 'Ref-1A-14')

Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

□ Otherwise, PASS.

□ The following is considered to be an acceptable operation by the DUT.

- If DUT has no FAIL test results and the DUT performs the procedures of **(STEP T101)** described in '1A-01 Regular procedure: With HDMI-capable Receiver' once again, then PASS. (Refer to 'Ref-1A-14')

1A-04. Irregular procedure: (First part of authentication) HDCP port access

Test Objective

Verify that Transmitter repeatedly attempts to start the authentication protocol whenever HPD is asserted and HDCP port is not acknowledged by the downstream Receiver.

Required Test Method

<Connection Setup>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver'.

<Configuration of TE>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver' except for the following.

- HDCP port is not readable (no acknowledge)

<Test Case>

[Before starting authentication]

□ TE asserts HPD. Its EDID is readable but HDCP port isn't.

□ DUT reads EDID and begins sending unencrypted video signal (EESS: ENC_DIS) by HDMI protocol (i.e. one Data island at least once per two video fields).

Verify the timing to access HDCP port

□ DUT attempts to read an HDCP register at least once every 2 seconds to start the first part of authentication.

- ➢ If DUT does not read an HDCP register at all after HPD is asserted, then FAIL. (Refer to 'Ref-1A-15')
- ➢ If DUT does not read an HDCP register past 4 seconds after the previous attempt, then FAIL. (Refer to 'Ref-1A-15')

Note: It does not matter for deciding PASS/FAIL whether DUT has accessed any other address space than HDCP register (e.g. EDID).

□ Otherwise, PASS.

1A-05. Irregular procedure: (First part of authentication) Verify Bksv

Test Objective

Verify that Transmitter considers it a failure of the first part of authentication protocol to read invalid Bksv from the downstream Receiver.

Required Test Method

<Connection Setup>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver'.

<Configuration of TE>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver' except for the following.

- Bksv does not contain 20 zeros and 20 ones

<Test Case>

[Before starting authentication] described in '1A-01 Regular procedure: With HDMI-capable Receiver' is performed.

[First Part of Authentication]

□ As the first part of authentication protocol, DUT performs the actions below.

- Read Bcaps (REPEATER, 1.1_FEATURE)
- Read Bksv (This Bksv is invalid. i.e. not containing 20 zeros and 20 ones)
- Write An
- Write Aksv

Note: The order of the read access of Bksv and Bcaps does not matter. Bcaps and Bksv may be read after writing Aksv.

(STEP T102) of [First Part of Authentication] described in '1A-01 Regular procedure: With HDMI-capable Receiver' is performed.

Verify the state after reading invalid Bksv

- ➢ If DUT reads invalid Bksv only once, then WARNING
- ➢ If DUT reads R0' after reading invalid Bksv and writing Aksv, then WARNING. (Refer to 'Ref-1A-16')

□ The following is considered as an error in the DUT's operation.

- ➢ If DUT enables and keeps HDCP Encryption after reading invalid Bksv and writing Aksv, then FAIL. (Refer to 'Ref-1A-16')

□ Otherwise, PASS.

□ The following is an acceptable operation by the DUT

- ➢ If DUT has no FAIL test results and the DUT performs the procedures of **(STEP T101)** described in '1A-01 Regular procedure: With HDMI-capable Receiver' once again, then PASS. (Refer to 'Ref-1A-16')

Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

1A-06. Irregular procedure: (First part of authentication) Verify R0'

Test Objective

Verify that Transmitter considers it a failure of the first part of authentication protocol to read invalid R0' from the downstream Receiver.

Required Test Method

<Connection Setup>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver'.

<Configuration of TE>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver' except for the following.

- R0' = incorrectly computed value

<Test Case>

[Before starting authentication] described in '1A-01 Regular procedure: With HDMI-capable Receiver' is performed.

[First Part of Authentication]

(STEP T101) and **(STEP T102)** of [First Part of Authentication] described in '1A-01 Regular procedure: With HDMI-capable Receiver' are performed.

Verify the timing to read R0'

□ TE calculates R0' incorrectly.

□ DUT reads R0'. This must be attempted later than 100 ms after writing Aksv.

➢ If DUT does not wait at least 100 ms to read R0' after writing Aksv, then FAIL. (Refer to 'Ref-1A-6')

Verify the comparison between R0 and R0'

□ After reading R0', DUT does not enable HDCP Encryption (i.e. keeps EESS: ENC_DIS).

➢ If DUT enables and keeps HDCP Encryption after reading invalid R0', then FAIL. (Refer to 'Ref-1A-17')

Verify the attempt of re-authentication

□ DUT attempts to re-start the first part of authentication.

If DUT does not perform the procedures of **(STEP T101)** described in '1A-01 Regular procedure: With HDMI-capable Receiver' once again, then WARNING. Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under <u>(STEP T101)</u>

- □ Otherwise, PASS.

1A-07. Irregular procedure: (Third part of authentication) Verify Ri’

Test Objective

Verify that Transmitter considers it a failure of the third part of authentication protocol to read invalid Ri’ from the downstream Receiver.

Required Test Method

<Connection Setup>

It is same as ‘1A-01 Regular procedure: With HDMI-capable Receiver’.

<Configuration of TE>

It is same as ‘1A-01 Regular procedure: With HDMI-capable Receiver’ except for the following.

- Ri’ = incorrectly computed value

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in ‘1A-01 Regular procedure: With HDMI-capable Receiver’ are performed.

[Third Part of Authentication]

□ TE updates invalid Ri’ for every 128th frame from the first encrypted frame.

Verify the comparison between Ri and Ri’

□ DUT reads Ri’. After this, DUT disables HDCP Encryption (i.e. EESS: ENC_EN -> ENC_DIS).

➢ If DUT does not disable HDCP Encryption after reading invalid Ri’, then FAIL. (Refer to ‘Ref-1A-18’)

Note: DUT may re-read the mismatched Ri’ before disabling HDCP Encryption.

Verify the attempt of re-authentication

□ DUT attempts to re-start the first part of authentication.

➢ If DUT does not perform the procedures of **(STEP T101)** of [First Part of Authentication] described in ‘1A-01 Regular procedure: With HDMI-capable Receiver’ once again, then WARNING

Note: Among the procedures of **(STEP T101)**, ‘Write An’ and ‘Write Aksv’ must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

- □ Otherwise, PASS.

1A-08. Irregular procedure: SRM

Test Objective

Verify that Transmitter, which has capability to playback DVD disc, considers it a failure of the first part of authentication protocol to read invalid Bksv listed in the SRM.

Required Test Method

<Connection Setup>

It is same as ‘1A-01 Regular procedure: With HDMI-capable Receiver’. In addition, The DUT has capability to playback a DVD disc. SRM which includes Bksv of TE is recorded in the Test disc. DUT starts to playback the Test disc before the test.

<Configuration of TE>

It is same as ‘1A-01 Regular procedure: With HDMI-capable Receiver’

<Test Case>

[Before starting authentication] described in ‘1A-01 Regular procedure: With HDMI-capable Receiver’ is performed.

[First Part of Authentication]

- □ As the first part of authentication protocol, DUT performs the actions below.
  - ● Read Bcaps (REPEATER, 1.1_FEATURE)
  - ● Read Bksv (This Bksv is listed in the SRM)
  - ● Write An
  - ● Write Aksv

  Note: The order of the read access of Bksv and Bcaps does not matter. Bcaps and Bksv may be read after writing Aksv.

(STEP T102) of [First Part of Authentication] described in ‘1A-01 Regular procedure: With HDMI-capable Receiver’ is performed.

Verify the state after reading invalid Bksv

- ➢ If DUT reads R0’ after reading invalid Bksv and writing Aksv, then WARNING. (Refer to ‘Ref-1A-19’)

- □ The following are considered as errors in the DUT’s operation.

- ➢ If DUT enables and keeps HDCP Encryption after reading invalid Bksv and writing Aksv, then FAIL. (Refer to 'Ref-1A-19')

- □ Otherwise, PASS.
- □ The following is an acceptable operation by the DUT.
  - ➢ If DUT has no FAIL test results and the DUT performs the procedures of **(STEP T101)** described in '1A-01 Regular procedure: With HDMI-capable Receiver' once again, then PASS. (Refer to 'Ref-1A-19')

Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

With DVI Receiver

Transmitter's procedure is tested when it is connected to DVI Receiver.

- In this test, DUT should transmit one of the following video format signals in DVI mode.
  - 640x480p@59.94/60Hz
  - 720x480p@59.94/60Hz
  - 720x576p@50Hz

1A-09. Regular procedure: With DVI Receiver

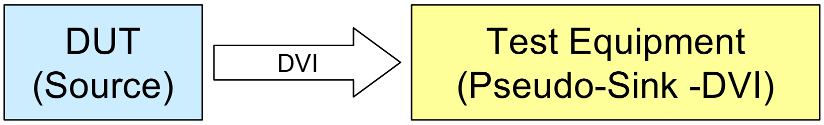
Test Objective

Verify that Transmitter performs the HDCP Authentication Protocol with the downstream DVI Receiver.

Required Test Method

<Connection Setup>

□ Connect TE to the downstream HDCP-protected Interface Port of DUT.



<Configuration of TE>

Initial Setting	
EDID	DVI (not HDMI-capable)
HDCP port	readable (i.e. it can be accessed)
Bcaps: REPEATER bit	0
First Part of Authentication	
Bcaps: 1.1_FEATURES bit	0
Bksv	valid value
R0'	correctly computed value
Third Part of Authentication	
Ri'	correctly computed value

<Test Case>

✧ In this test case, by viewing the decrypted image, it is only checked whether HDCP encryption is correctly applied. Regarding Authentication, TE does not output the test result. TE outputs only information about actually performed actions.

1B. Downstream procedure with Repeater

Transmitter's downstream procedure with Repeater is tested in HDMI protocol.

- In this test, DUT should transmit one of the following video signals with Data Island period in HDMI mode.
    - 640x480p@59.94/60Hz
    - 720x480p@59.94/60Hz
    - 720x576p@50Hz

1B-01. Regular procedure: With Repeater

Test Objective

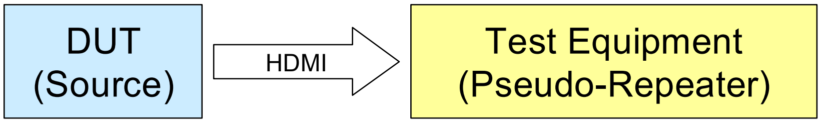
Verify that Transmitter performs the correct HDCP Authentication Protocol using production keys with the downstream HDMI-capable Repeater.

Required Test Method

If PCP Source_Out_OnlyRep == "Y", the following test must cover the case when DEVICE_COUNT is zero in addition to the case when DEVICE_COUNT is a non-zero value.

<Connection Setup>

- □ Connect TE to the downstream HDCP-protected Interface Port of DUT.



<Configuration of TE>

Initial Setting		
EDID		HDMI-capable
HDCP port		readable (i.e. it can be accessed)
Bcaps: REPEATER bit		1
First Part of Authentication		
Bcaps: 1.1_FEATURES bit		0
Bksv		valid value
R0'		correctly computed value
Second Part of Authentication		
Setting after Aksv written	Bstatus:	
	DEPTH	7 or fewer
	DEVICE_COUNT	127 or fewer
	MAX_DEVS_EXCEEDED bit	0
	MAX_CASCADE_EXCEEDED bit	0
	KSV FIFO	(DEVICE_COUNT*5) bytes

	Bcaps: READY bit	Assert before (DEPTH*600) ms
V’	correctly computed value	
Third Part of Authentication		
Ri’	correctly computed value	

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in ‘1A-01 Regular procedure: With HDMI-capable Receiver’ are performed.

[Second Part of Authentication]

(STEP T201)

□ TE sets Bstatus: DEPTH and DEVICE_COUNT to the configured value and asserts Bcaps: READY bit at the configured period after Aksv is written. At this point, TE already completes to set the configured size of valid KSVs in KSV FIFO and to set the correctly computed V’.

(STEP T202)

Verify the timing to read Bcaps: READY

□ DUT polls downstream Bcaps (READY).

➢ If DUT does not read Bcaps (READY) within five seconds after reading R0’, then FAIL. (Refer to ‘Ref-1B-1’)

Note: DUT may read Bcaps (READY) at any rate as it prefers within five seconds.

(STEP T203)

Verify to read KSVs

There are two test cases when PCP Source_Out_OnlyRep == “Y”

Case 1: DEVICE_COUNT is a non-zero value

□ DUT reads the list of attached KSVs from KSV FIFO in a single, auto-incrementing access. The size of KSVs to be read can be calculated from Bstatus: DEVICE_COUNT.

➢ If DUT does not read KSVs, then FAIL. (Refer to ‘Ref-1B-2’)

➢ If DUT does not read the correct size of KSVs, then FAIL. (Refer to ‘Ref-1B-2’)

Case 2: DEVICE_COUNT is zero

□ DUT need not read the list of attached KSVs from KSV FIFO

Note: If PCP Source_Out_OnlyRep == “N”, only Case 1 needs to be performed

(STEP T204)

Verify to read V’

- □ DUT reads V'.
  - ➢ If DUT does not read V' or DUT reads only a part of V', then FAIL. (Refer to 'Ref-1B-3' and 'Ref-1B-7')

  Note: Either KSVs or V' may be read in any order after Bcaps: READY bit is asserted.

As for the [Third Part of Authentication], the same procedures described in '1A-01 Regular procedure: With HDMI-capable Receiver' are performed.

- □ Otherwise, if DUT completes the authentication, PASS.

1B-02. Regular procedure: HPD after reading R0'

Test Objective

Verify that Transmitter enters the No Receiver Attached state when HPD is de-asserted after reading R0' and then re-starts the authentication after HPD is asserted by the downstream Repeater.

Required Test Method

<Connection Setup>

It is same as '1B-01 Regular procedure: With Repeater'.

<Configuration of TE>

It is same as '1B-01 Regular procedure: With Repeater'.

<Test Case>

The procedures from [Before starting authentication] to **(STEP T103)** of [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' are performed.

[Second Part of Authentication]

□ TE pulses HPD of the upstream HDCP-protected Interface Port to DUT more than 100 ms.

Verify the attempt of re-authentication

□ DUT attempts to re-start the first part of authentication.

- ➢ If DUT performs the procedures of **(STEP T201)** described in '1B-01 Regular procedure: With Repeater' while TE is de-assserting HPD, then WARNING. (Refer to 'Ref-1A-14')
- ➢ If DUT enables and keeps HDCP Encryption, then FAIL. (Refer to 'Ref-1A-14')
- ➢ If DUT does not perform the procedures of **(STEP T101)** of [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' once again, then WARNING

Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

□ Otherwise, PASS.

□ The following is an acceptable DUT operation.

- If DUT has no FAIL test results and the DUT performs the procedures of **(STEP T101)** of [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' once again, then PASS. (Refer to 'Ref-1A-14')

1B-03. Irregular procedure: (Second part of authentication) Timeout of KSV list READY

Test Objective

Verify that Transmitter waits at least five seconds polling for the assertion of READY from the downstream Repeater.

Required Test Method

<Connection Setup>

It is same as '1B-01 Regular procedure: With Repeater'.

<Configuration of TE>

It is same as 1B-01 Regular procedure: With Repeater' except for the following.

- Bcaps: READY bit never be asserted after Aksv is written.

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' are performed.

[Second Part of Authentication]

□ TE keeps Bcaps: READY zero.

Verify the timing to read Bcaps: READY

□ DUT polls downstream Bcaps (READY).

➢ If DUT does not read Bcaps (READY) within five seconds after reading R0', then FAIL. (Refer to 'Ref-1B-1')

Note: DUT may read Bcaps (READY) at any rate as it prefers within five seconds.

Verify the period of polling for Bcaps: READY

□ DUT waits at least five seconds polling for Bcaps (READY) after reading R0'. After this, DUT disables HDCP Encryption (i.e. EESS: ENC_EN -> ENC_DIS).

➢ If DUT does not disable HDCP Encryption past five seconds after reading R0' as the result of the polling for Bcaps (READY), then FAIL. (Refer to 'Ref-1B-4')

Verify the attempt of re-authentication

□ DUT attempts to re-start the first part of authentication.

➢ If DUT does not perform the procedures of **(STEP T101)** of [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' once again, then WARNING. (Refer to 'Ref-1B-8')

Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

- □ Otherwise, PASS.

1B-04. Irregular procedure: (Second part of authentication) Verify V'

Test Objective

Verify that Transmitter considers it a failure of the second part of authentication protocol to read invalid V' from the downstream Repeater.

Required Test Method

<Connection Setup>

It is same as '1B-01 Regular procedure: With Repeater'.

<Configuration of TE>

It is same as '1B-01 Regular procedure: With Repeater' except for the following.

- V' = incorrectly computed value

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' are performed.

The procedures from **(STEP T201)** to **(STEP T203)** of [Second Part of Authentication] described in '1B-01 Regular procedure: With Repeater' are performed.

[Second Part of Authentication]

Verify the comparison between V and V'

- □ TE calculates V' incorrectly.
- □ DUT reads V'. After this, DUT disables HDCP Encryption (i.e. EESS: ENC_EN -> ENC_DIS).
  - ➢ If DUT does not disable HDCP Encryption after reading invalid V', then FAIL. (Refer to 'Ref-1B-5')

Note: DUT may re-read Bstatus, KSVs and mismatched V' before disabling HDCP Encryption.

Verify the attempt of re-authentication

- □ DUT attempts to re-start the first part of authentication.
  - ➢ If DUT does not perform the procedures of **(STEP T101)** of [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' once again, then WARNING.

Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

- □ Otherwise, PASS.

1B-05. Irregular procedure: (Second part of authentication) MAX_DEVS_EXCEEDED

Test Objective

Verify that Transmitter considers it a failure of the second part of authentication protocol that Bstatus: MAX_DEVS_EXCEEDED bit is asserted by the downstream Repeater.

Required Test Method

<Connection Setup>

It is same as '1B-01 Regular procedure: With Repeater'.

<Configuration of TE>

It is same as '1B-01 Regular procedure: With Repeater' except for the followings.

- Bstatus: MAX_DEVS_EXCEEDED bit = 1

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' are performed.

[Second Part of Authentication]

There are two possible behaviors for TE[1]. Case 1 is performed as this test item.

Case 1:

□ TE sets Bstaus: MAX_DEVS_EXCEEDED bit to one and asserts Bcaps: READY bit at the configured period after Aksv is written.

Verify the timing to read Bcaps: READY

□ DUT polls downstream Bcaps (READY).

- ➢ If DUT does not read Bcaps (READY) within five seconds after reading R0', then FAIL. (Refer to 'Ref-1B-1')

Note: DUT may read Bcaps (READY) at any rate as it prefers within five seconds.

□ DUT reads Bstatus. After this, DUT disables HDCP Encryption (i.e. EESS: ENC_EN -> ENC_DIS).

[1] Refer to page 1 of Errata 1.1 "Section 2.2, append to paragraph 13: If either MAX_CASCADED_EXCEEDED or MAX_DEVS_EXCEEDED status bits are set, the READY bit may be set by the repeater, or it may not set the READY bit and simply let the timeout occur in the HDCP Transmitter."

  - ➢ If DUT does not disable HDCP Encryption after reading Bstatus (MAX_DEVS_EXCEEDED), then FAIL. (Refer to 'Ref-1B-6')

Verify the attempt of re-authentication

- □ DUT attempts to re-start the first part of authentication.
  - ➢ If DUT does not perform the procedures of **(STEP T101)** of [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' once again, then WARNING.

Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

- □ Otherwise, PASS.

Case 2:

- □ TE sets Bstaus: MAX_DEVS_EXCEEDED bit to one and does not assert Bcaps: READY bit.

Note: The behavior of DUT is checked in '1B-03 Irregular procedure: (Second part of authentication) Timeout of KSV list READY' when TE does not assert Bcaps: READY bit.

1B-06. Irregular procedure: (Second part of authentication) MAX_CASCADE_EXCEEDED

Test Objective

Verify that Transmitter considers it a failure of the second part of authentication protocol that Bstatus: MAX_CASCADE_EXCEEDED bit is asserted by downstream Repeater.

Required Test Method

<Connection Setup>

It is same as '1B-01 Regular procedure: With Repeater'.

<Configuration of TE>

It is same as '1B-01 Regular procedure: With Repeater' except for the following.

- Bstatus: MAX_CASCADE_EXCEEDED bit = 1
- Bstatus: DEPTH = 7
- Bstatus: DEVICE_COUNT = 7

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' are performed.

[Second Part of Authentication]

There are two possible behaviors for TE[2]. Case 1 is performed as this test item.

Case 1:

□ TE sets Bstaus: MAX_CASCADE_EXCEEDED bit to one and asserts Bcaps: READY bit at the configured period after Aksv is written.

Verify the timing to read Bcaps: READY

□ DUT polls downstream Bcaps (READY).

➢ If DUT does not read Bcaps (READY) within five seconds after reading R0', then FAIL. (Refer to 'Ref-1B-1')

Note: DUT may read Bcaps (READY) at any rate as it prefers within five seconds.

[2] Refer to page 1 of Errata 1.1 "Section 2.2, append to paragraph 13: If either MAX_CASCADED_EXCEEDED or MAX_DEVS_EXCEEDED status bits are set, the READY bit may be set by the repeater, or it may not set the READY bit and simply let the timeout occur in the HDCP Transmitter."

- □ DUT reads Bstatus. After this, DUT disables HDCP Encryption (i.e. EESS: ENC_EN -> ENC_DIS).
  - ➢ If DUT does not disable HDCP Encryption after reading Bstatus: MAX_CASCADE_EXCEEDED bit, then FAIL. (Refer to 'Ref-1B-6')

Verify the attempt of re-authentication

- □ DUT attempts to re-start the first part of authentication.
  - ➢ If DUT does not perform the procedures of **(STEP T101)** of [First Part of Authentication] described in '1B-01 Regular procedure: With Repeater' once again, then WARNING.

Note: Among the procedures of **(STEP T101)**, 'Write An' and 'Write Aksv' must always be performed by the DUT, the DUT is not required to perform the other procedures outlined under **(STEP T101)**

- □ Otherwise, PASS.

Case 2:

- □ TE sets Bstaus: MAX_CASCADE_EXCEEDED bit to one and does not assert Bcaps: READY bit.

Note: The behavior of DUT is checked in '1B-03 Irregular procedure: (Second part of authentication) Timeout of KSV list READY' when TE does not assert Bcaps: READY bit.

2. Receiver Test

Receiver's procedure is tested.

2C. Upstream procedure with Transmitter

Receiver's upstream procedure with Transmitter is tested under the following two conditions of connection.

- HDMI-capable Transmitter is connected
- DVI Transmitter is connected

Make sure that DUT keeps HPD asserted unless HPD pulse is needed during each test.

□ With HDMI-capable Transmitter

Receiver's procedure is tested when it is connected to HDMI-capable Transmitter.

- In this test, TE transmits 640x480p video signal with Data Island period in HDMI mode. If PCP for Sink_Audio_Supported == Y, video signal with audio is transmitted. Otherwise, video signal without audio is transmitted.

2C-01. Regular procedure: With HDMI-capable Transmitter

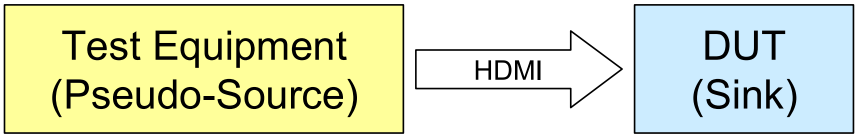
Test Objective

Verify that Receiver performs the correct Authentication Protocol using production keys with the upstream HDMI-capable Transmitter.

Required Test Method

<Connection Setup>

□ Connect TE to the upstream HDCP-protected Interface Port of DUT.



<Configuration of TE>

Initial Setting		
Output signal	640x480p video signal with Data Island period in HDMI mode	
First Part of Authentication		
Ainfo: ENABLE_1.1_FEATURES bit	write one	no write (i.e. zero)
	By switching, each case is verified.	
	However, if PCP for Sink_1.1Features_Supported == N, only [no write] case is performed.	
R0 and Ri read	short format	combined format
	By switching, each case is verified	

* When TE sets Ainfo: ENABLE_1.1_FEATURES bit to one, TE performs Enhanced Link Verification.

<Test Case>

[Before starting authentication]

(STEP SP01)

□ TE detects HPD asserted by DUT.

➢ If HPD is not asserted by DUT, then FAIL. (Refer to 'Ref-2C-1')

(STEP SP02)

Verify HDMI_MODE

□ TE reads Bstatus: HDMI_MODE.

➢ If Bstatus: HDMI_MODE bit is one, then FAIL. (Refer to 'Ref-2C-4')

Note: It is not considered a failure when DUT does not respond to the read access of Bstatus at this time.

(STEP SP03)

□ TE begins sending unencrypted video signal (EESS: ENC_DIS) by HDMI protocol (i.e. one Data island at least once per two video fields).

□ After DUT detects a Data Island, it sets Bstatus: HDMI_MODE to one.

Verify HDCP port access

□ TE reads Bksv.

➢ If DUT does not respond to the read access of Bksv, then WARNING. (Refer to 'Ref-2C-1')

(STEP SP04)

Verify Reserved ports/bits

□ TE reads all Reserved ports and bits.

➢ If any Reserved port or bit is not zero, then FAIL. (Refer to 'Ref-2C-2')

(STEP SP05)

Verify KSV FIFO values of Receiver

□ TE reads five bytes from KSV FIFO in a single, auto-incrementing access.

➢ If all five bytes are not 0x00, then FAIL. (Refer to 'Ref-2C-3')

(STEP SP06)

Verify HDMI_MODE again

□ TE reads Bstatus: HDMI_MODE.

➢ If Bstatus: HDMI_MODE bit is still zero, then FAIL. (Refer to 'Ref-2C-4')

□ TE begins the first part of authentication.

[First Part of Authentication]

(STEP S101)

□ As the first part of authentication protocol, TE performs the actions below.

● Read Bcaps (REPEATER, 1.1_FEATURE)

● Read Bksv

● Write Ainfo (ENABLE_1.1_FEATURES)

(If DUT's Bcaps: 1.1_FEATURES bit == 1, this may be done)

● Write An

● Write Aksv

(STEP S102)

□ The followings are considered as errors in the DUT's operation.

Verify REPEATER

- ➢ If Bcaps: REPEATER bit is one, then FAIL. (Refer to 'Ref-2C-5')

Verify 1.1_FEATURE

- ➢ If Bcaps: 1.1_FEATURE bit does not correspond to PCP for Sink_1.1Features_Supported, then FAIL.(Refer to 'Ref-2C-7')

- PCP for Sink_1.1Features_Supported == Y and Bcaps: 1.1_FEATURE bit == 0, then FAIL.
- PCP for Sink_1.1Features_Supported == N and Bcaps: 1.1_FEATURE bit == 1, then FAIL.

Verify Bksv

- ➢ If Bksv does not contain 20 zeros and 20 ones, then FAIL. (Refer to 'Ref-2C-6')
- ➢ If Bksv is the same as facsimile Bksv, then FAIL

(STEP S103)

Verify R0' compared with R0

- □ DUT calculates R0'.
- □ TE reads R0' after 100 ms from the time that TE finished writing Aksv. This read is made in short read format or in the combined-format byte read. TE compares R0' with R0.
  - ➢ If DUT does not support short read format access to R0', then FAIL. (Refer to 'Ref-2C-9')

Note: This is verified only when TE performs short read format access.

- ➢ If R0' does not equal to its own calculation R0, then FAIL. (Refer to 'Ref-2C-8')

(STEP S104)

- □ TE enables HDCP Encryption. (i.e. EESS: ENC_DIS -> ENC_EN)

[Third Part of Authentication]

(STEP S301)

Verify Ri' compared with Ri

- □ DUT updates Ri' for every 128th frame from the first encrypted frame.
- □ TE reads Ri' for every 128th frame from the first encrypted frame. This read is made in short read format or in the combined-format byte read.
  - ➢ If DUT does not support short read format access to Ri', then FAIL. (Refer to 'Ref-2C-9')

Note: This is verified only when TE performs short read format access.

- ➢ If read Ri' does not equal to its own calculation Ri, then FAIL. (Refer to 'Ref-2C-10')

Note: As TE continues to output video frames for which encryption is enabled, it reads

Ri' for every 128th frame regardless of whether ADVANCE_CIPHER mode is used or not. TE reads Ri' at least after 128 pixel clocks following the Encryption Enable detection (ENC_EN) of the 128th frame.

(STEP S302)

Note: This step is performed if PCP for Sink_1.1Features_Supported == Y and TE sets Ainfo: ENABLE_1.1_FEATURES bit to one.

Verify Pj' compared with Pj

- □ DUT updates Pj' for every 16th frame from the first encrypted frame.
- □ TE reads Pj' for every 16th frame from the first encrypted frame.
  - ➢ If read Pj' does not equal to its own calculation Pj, then FAIL. (Refer to 'Ref-2C-10')

Note: As TE continues to output video frames for which encryption is enabled, it reads Pj' for every 16th frame. TE reads Pj' after it outputs the first video pixel of the 16th frame.

- □ Otherwise, PASS.

2C-02. Irregular procedure: (First part of authentication) New Authentication

Test Objective

Verify that Receiver accepts re-authentication, when new An and Aksv is written by Transmitter right after An and Aksv is written in the unauthenticated state

Required Test Method

<Connection Setup>

It is same as '2C-01 Regular procedure: With HDMI-capable Transmitter'.

<Configuration of TE>

Initial Setting	
Output signal	640x480p video signal with Data Island period in HDMI mode
First Part of Authentication	
Ainfo: ENABLE_1.1_FEATURES bit	no write (i.e. zero)

<Test Case>

[Before starting authentication] described in '2C-01 Regular procedure: With HDMI-capable Transmitter' is performed.

(STEP S101) and **(STEP S102)** of [First Part of Authentication] described in '2C-01 Regular procedure: With HDMI-capable Transmitter' are performed.

- □ TE performs the actions below right after **(STEP S102)**.
  - ● Read Bcaps (REPEATER, 1.1_FEATURE)
  - ● Read Bksv
  - ● Write An (different from the previously written one)
  - ● Write Aksv

(STEP S102) is performed again.

Verify R0' compared with R0

- □ DUT calculates R0' using the latest An.
- □ TE reads R0' after 100 ms from the time that TE finished writing the latest Aksv and compares R0' with R0.
  - ➢ If R0' does not equal to its own calculation R0, then FAIL. (Refer to 'Ref-2C-11')
- □ TE enables HDCP Encryption. (i.e. EESS: ENC_DIS -> ENC_EN).

As for the [Third Part of Authentication], the same procedures described in '2C-01 Regular procedure: With HDMI-capable Transmitter' are performed.

- □ Otherwise, PASS.

2C-03. Irregular procedure: (Third part of authentication) New Authentication

Test Objective

Verify that Receiver accepts re-authentication if new An and Aksv is written by Transmitter during the third part of authentication.

Required Test Method

<Connection Setup>

It is same as '2C-01 Regular procedure: With HDMI-capable Transmitter'.

<Configuration of TE>

It is same as '2C-02 Irregular procedure: (First part of authentication) New Authentication'.

<Test Case>

The procedures from [Before starting authentication] to [Third Part of Authentication] described in '2C-01 Regular procedure: With HDMI-capable Transmitter' are performed.

- □ TE disables HDCP Encryption and sends unencrypted video signal (EESS: ENC_DIS) by HDMI protocol (i.e. one Data island at least once per two video fields).
- □ Then, as the first part of authentication protocol, TE performs the actions below.
  - ● Read Bcaps (REPEATER, 1.1_FEATURE)
  - ● Read Bksv
  - ● Write An (different from the previously written one)
  - ● Write Aksv

(STEP S102) is performed again.

Verify R0' compared with R0

- □ DUT calculates R0' using the latest An.
- □ TE reads R0' after 100 ms from the time that TE finished writing the latest Aksv and compares R0' with R0.
  - ➢ If R0' does not equal to its own calculation R0, then FAIL. (Refer to 'Ref-2C-12')
- □ TE enables HDCP Encryption. (i.e. EESS: ENC_DIS -> ENC_EN).

As for the [Third Part of Authentication], the same procedures described in '2C-01 Regular procedure: With HDMI-capable Transmitter' are performed.

□ Otherwise, PASS.

□ With DVI Transmitter

Receiver's procedure is tested when it is connected to DVI Transmitter.

- In this test, TE transmits 640x480p video signal in DVI mode.

2C-04. Regular procedure: With DVI Transmitter

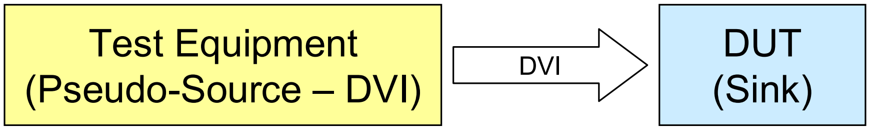
Test Objective

Verify that Receiver performs the HDCP Authentication Protocol with the upstream DVI Transmitter.

Required Test Method

<Connection Setup>

□ Connect TE to the upstream HDCP-protected Interface Port of DUT.



<Configuration of TE>

Initial Setting	
Output signal	640x480p video signal in DVI mode
First Part of Authentication	
Ainfo: ENABLE_1.1_FEATURES bit	no write (i.e. zero)

<Test Case>

✧ In this test case, the image displayed at the monitor of the DUT is only checked visually. Regarding Authentication, TE does not output the test result. TE outputs only information about actually performed actions.

✧ In this test, with respect to the position of OESS: ENC_EN signal asserted during the permitted period of the vertical blanking interval, the three cases below are possible. DUT is verified whether it can cope with each case.

1. OESS: ENC_EN signal is positioned in the leading part.
   (i.e. 8 pixel clocks starting at the active edge of VSYNC)
2. OESS: ENC_EN signal is positioned in the trailing part.
   (i.e. 8 pixel clocks ending no closer than 128 pixel clocks from the end of the vertical blank interval)
3. OESS: ENC_EN signal is positioned in the center part.
   (i.e. 8 pixel clocks around in the middle point between the above 1. and 2.)

3. Repeater Test

Repeater's procedure is tested regarding to the following three procedures.

- Downstream procedure with Receiver
- Downstream procedure with Repeater
- Upstream procedure with Transmitter

3A. Downstream procedure with Receiver

Repeater's downstream procedure with Receiver is tested under the following two conditions of connection.

- Repeater is located between HDMI-capable Transmitter and HDMI-capable Receiver (TE)
- Repeater is located between HDMI-capable Transmitter and DVI Receiver (TE)

- In this test, HDMI-capable Transmitter should transmit one of the following video format signal with Data Island period in HDMI mode.
    - 640x480p@59.94/60Hz
    - 720x480p@59.94/60Hz
    - 720x576p@50Hz

□ Between HDMI-capable Transmitter and HDMI-capable Receiver

Repeater's downstream procedure with HDMI-capable Receiver is tested when HDMI-capable Transmitter is connected to the upstream HDCP-protected Interface Port of Repeater.

3A-01. Regular procedure: With HDMI-capable Receiver

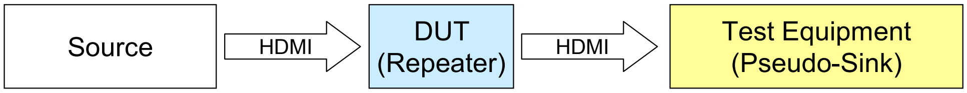
Test Objective

Verify that Repeater (DUT) performs the correct HDCP Authentication Protocol using production keys between the upstream HDMI-capable Transmitter and the downstream HDMI-capable Receiver. Downstream procedure of Repeater is verified.

Required Test Method

<Connection Setup>

- □ Connect a Source device to the upstream HDCP-protected Interface Port of DUT.
- □ Connect TE to the downstream HDCP-protected Interface Port of DUT.



* A Source device is the one that has already passed the Transmitter Test.

<Configuration of TE>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver'.

<Test Case>

It is same as '1A-01 Regular procedure: With HDMI-capable Receiver'.

3A-02. Irregular procedure: (First part of authentication) HDCP port access

Test Objective

Verify that Repeater (DUT) repeatedly attempts to start the authentication protocol whenever HPD is asserted and HDCP port is not acknowledged by the downstream Receiver.

Required Test Method

<Connection Setup>

It is same as '3A-01 Regular procedure: With HDMI-capable Receiver'.

<Configuration of TE>

It is same as '1A-04 Irregular procedure: (First part of authentication) HDCP port access'.

<Test Case>

It is same as '1A-04 Irregular procedure: (First part of authentication) HDCP port access'.

3A-03. Irregular procedure: (First part of authentication) Verify Bksv

Test Objective

Verify that Repeater (DUT) considers it a failure of the first part of authentication protocol to read invalid Bksv from the downstream Receiver.

Required Test Method

<Connection Setup>

It is same as '3A-01 Regular procedure: With HDMI-capable Receiver'.

<Configuration of TE>

It is same as '1A-05 Irregular procedure: (First part of authentication) Verify Bksv'.

<Test Case>

It is same as '1A-05 Irregular procedure: (First part of authentication) Verify Bksv'.

3A-04. Irregular procedure: (First part of authentication) Verify R0’

Test Objective

Verify that Repeater (DUT) considers it a failure of the first part of authentication protocol to read invalid R0’ from the downstream Receiver.

Required Test Method

<Connection Setup>

It is same as ‘3A-01 Regular procedure: With HDMI-capable Receiver’.

<Configuration of TE>

It is same as ‘1A-06 Irregular procedure: (First part of authentication) Verify R0”.

<Test Case>

It is same as ‘1A-06 Irregular procedure: (First part of authentication) Verify R0”.

□ Between HDMI-capable Transmitter and DVI Receiver

Repeater's downstream procedure with DVI Receiver is tested when HDMI-capable Transmitter is connected to the upstream HDCP-protected Interface Port of Repeater.

3A-05. Regular procedure: With DVI Receiver

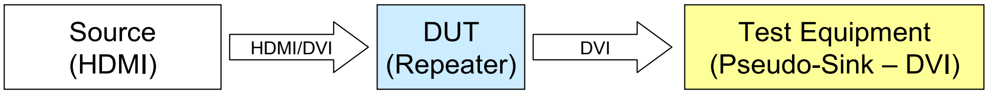
Test Objective

Verify that Repeater (DUT) performs the HDCP Authentication Protocol between the upstream HDMI-capable Transmitter and the downstream DVI Receiver. Downstream procedure of Repeater is verified.

Required Test Method

<Connection Setup>

- □ Connect a Source device (HDMI-capable) to the upstream HDCP-protected Interface Port of DUT.
- □ Connect TE to the downstream HDCP-protected Interface Port of DUT.



* A Source device is the one that has already passed the Transmitter Test.

<Configuration of TE>

It is same as '1A-09 Regular procedure: With DVI Receiver'

<Test Case>

- ✧ In this test case, by viewing the decrypted image, it is only checked whether HDCP encryption is correctly applied. Regarding Authentication, TE does not output the test result. TE outputs only information about actually performed actions.

3B. Downstream procedure with Repeater

Repeater's downstream procedure with Repeater is tested when HDMI-capable Transmitter is connected to the upstream HDCP-protected Interface Port of Repeater.

- In this test, HDMI-capable Transmitter transmits one of the following video format signal with Data Island period in HDMI mode.
  - 640x480p@59.94/60Hz
  - 720x480p@59.94/60Hz
  - 720x576p@50Hz

3B-01. Regular procedure: With Repeater

Test Objective

Verify that Repeater (DUT) performs the correct HDCP Authentication Protocol using production keys between the upstream HDMI-capable Transmitter and the downstream HDMI-capable Repeater. Downstream procedure of Repeater is verified.

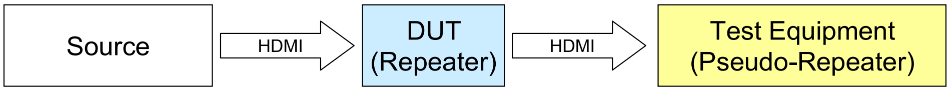
Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

□ Connect a Source device to the upstream HDCP-protected Interface Port of DUT.

□ Connect TE to the downstream HDCP-protected Interface Port of DUT.



* A Source device is the one that has already passed the Transmitter Test.

<Configuration of TE>

It is same as '1B-01 Regular procedure: With Repeater' except for the following.

Second Part of Authentication		
Setting after Aksv written	Bstatus:	
	DEPTH	6 or fewer
	DEVICE_COUNT	126 or fewer

<Test Case>

It is same as '1B-01 Regular procedure: With Repeater'.

Note that PCP Repeater_Out_OnlyRep is used instead of Source_Out_OnlyRep

3B-02. Irregular procedure: (Second part of authentication) Timeout of KSV list READY

Test Objective

Verify that Repeater (DUT) waits at least five seconds polling for the assertion of READY from the downstream Repeater.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3B-01 Regular procedure: With Repeater'.

<Configuration of TE>

It is same as '3B-01 Regular procedure: With Repeater' except for the following.

- Bcaps: READY bit never be asserted after Aksv is written.

<Test Case>

It is same as '1B-03 Irregular procedure: (Second part of authentication) Timeout of KSV list READY'.

3B-03. Irregular procedure: (Second part of authentication) Verify V'

Test Objective

Verify that Repeater (DUT) considers it a failure of the second part of authentication protocol to read invalid V' from the downstream Repeater.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3B-01 Regular procedure: With Repeater'.

<Configuration of TE>

It is same as '3B-01 Regular procedure: With Repeater' except for the following.

- V' = incorrectly computed value

<Test Case>

It is same as '1B-04 Irregular procedure: (Second part of authentication) Verify V''.

3B-04. Irregular procedure: (Second part of authentication) MAX_DEVS_EXCEEDED

Test Objective

Verify that Repeater (DUT) considers it a failure of the second part of authentication protocol that Bstatus: MAX_DEVS_EXCEEDED bit is asserted by the downstream Repeater.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3B-01 Regular procedure: With Repeater'.

<Configuration of TE>

It is same as '3B-01 Regular procedure: With Repeater' except for the following.

- Bstatus: MAX_DEVS_EXCEEDED bit = 1

<Test Case>

It is same as '1B-05 Irregular procedure: (Second part of authentication) MAX_DEVS_EXCEEDED'.

3B-05. Irregular procedure: (Second part of authentication) MAX_CASCADE_EXCEEDED

Test Objective

Verify that Repeater (DUT) considers it a failure of the second part of authentication protocol that Bstatus: MAX_CASCADE_EXCEEDED bit is asserted by downstream Repeater.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3B-01 Regular procedure: With Repeater'.

<Configuration of TE>

It is same as '3B-01 Regular procedure: With Repeater' except for the followings.

- Bstatus: MAX_CASCADE_EXCEEDED bit = 1
- Bstatus: DEPTH = 7
- Bstatus: DEVICE_COUNT = 7

<Test Case>

It is same as '1B-06 Irregular procedure: (Second part of authentication) MAX_CASCADE_EXCEEDED'.

3C. Upstream procedure with Transmitter

Repeater's upstream procedure with HDMI-capable Transmitter is tested under the following two conditions of connection.

- HDMI-capable Receiver is connected to the downstream HDCP-protected Interface Port of Repeater (DUT)
- HDMI-capable Repeater is connected to the downstream HDCP-protected Interface Port of Repeater (DUT)

Make sure that DUT keeps HPD asserted unless HPD pulse is needed during each test.

□ Between HDMI-capable Transmitter and HDMI-capable Receiver

Repeater's upstream procedure with HDMI-capable Transmitter is tested when HDMI-capable Receiver is connected to the downstream HDCP-protected Interface Port of Repeater (DUT).

The attached Receiver supports the audio output.

● In this test, TE transmits 640x480p video signal with Data Island period in HDMI mode. If PCP for Repeater_Audio_Supported == Y, video signal with audio is transmitted. Otherwise, video signal without audio is transmitted.

3C-I-01. Regular procedure: Transmitter – DUT - Receiver

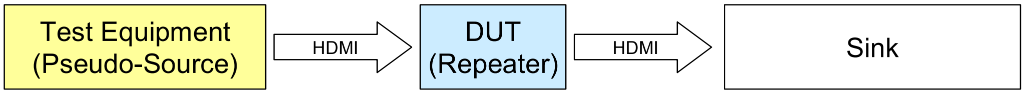
Test Objective

Verify that Repeater (DUT) performs the correct HDCP Authentication Protocol using production keys between the upstream HDMI-capable Transmitter and the downstream HDMI-capable Receiver. Upstream procedure of Repeater is verified.

Required Test Method

<Connection Setup>

- □ Connect TE to the upstream HDCP-protected Interface Port of DUT.
- □ Connect a Sink device to the downstream HDCP-protected Interface Port of DUT.



* A Sink device is the one that has already passed the Receiver Test.

<Configuration of TE>

Initial Setting		
Output signal	640x 480p video signal with Data Island period in HDMI mode	
First Part of Authentication		
Ainfo: ENABLE_1.1_FEATURES bit	write one	no write (i.e. zero)
	By switching, each case is verified	
	However, if PCP for Repeater_1.1Features_Supported == N, only [no write] case is performed.	
R0 and Ri read	short format	combined format
	By switching, each case is verified	

* When TE sets Ainfo: ENABLE_1.1_FEATURES bit to one, TE performs Enhanced Link Verification.

<Test Case>

[Before starting authentication] described in '2C-01 Regular procedure: With HDMI-capable Transmitter' is performed except for (STEP SP05). (STEP SP05) is not performed in this test.

[First Part Authentication] described in '2C-01 Regular procedure: With HDMI-capable Transmitter' is performed except for **(STEP S102)**.

Instead of **(STEP S102)**, TE performs the actions below.

(STEP S102S)

□ The followings are considered as errors in the DUT's operation.

Verify Bcaps: REPEATER

- If Bcaps: REPEATER bit is not one, then FAIL. (Refer to 'Ref-3C-1')

Verify Bcaps: 1.1_FEATURE

- If Bcaps: 1.1_FEATURE bit does not correspond to PCP for Repeater_1.1Features_Supported, then FAIL. (Refer to 'Ref-2C-7')
- PCP for Repeater_1.1Features_Supported == Y and Bcaps: 1.1_FEATURE bit == 0, then FAIL.
- PCP for Repeater_1.1Features_Supported == N and Bcaps: 1.1_FEATURE bit == 1, then FAIL.

Verify Bcaps: READY

- If Bcaps: READY bit is one, then FAIL. (Refer to 'Ref-3C-2')

Verify Bksv

- If Bksv does not contain 20 zeros and 20 ones, then FAIL. (Refer to 'Ref-2C-6')
- If Bksv is the same as facsimile Bksv, then FAIL

[Second Part of Authentication]

(STEP S201S)

Verify the timing to assert Bcaps: READY

□ DUT successfully completes the first part of authentication protocol with the downstream Sink device that has valid Bksv.

□ TE reads Bcaps (READY) from DUT at a rate of once every 100 ms after TE confirms R0' of DUT. DUT asserts Bcaps: READY bit within 600 ms after TE writes Aksv.

- If DUT does not assert Bcaps: READY bit within 600 ms after Aksv is written, then FAIL. (Refer to 'Ref-3C-3')

(STEP S202S)

Verify Bstatus

□ TE reads Bstatus.

- If Bstatus: MAX_DEVS_EXCEEDED bit is one, then FAIL. (Refer to 'Ref-3C-4')
- If Bstatus: MAX_CASCADE_EXCEEDED bit is one, then FAIL. (Refer to 'Ref-3C-5')

- If Bstatus: DEPTH is not one, then FAIL. (Refer to 'Ref-3C-6')
- If Bstatus: DEVICE_COUNT is not one, then FAIL. (Refer to 'Ref-3C-7')

(STEP S203S)

Verify KSV list

□ TE reads five bytes KSV from KSV FIFO in a single, auto-incrementing access.

- If DUT does not output Bksv of attached Sink device from KSV FIFO, then FAIL. (Refer to 'Ref-3C-8')

(STEP S204S)

Verify V' compared with V

□ TE reads V'.

- If read V' does not equal to its own calculation V, then FAIL. (Refer to 'Ref-3C-9')

As for the [Third Part of Authentication], the same procedures described in '2C-01 Regular procedure: With HDMI-capable Transmitter' are performed. Among the procedures of the [Third Part of Authentication], **(STEP S302)** is performed if PCP for Repeater_1.1Features_Supported == Y and TE sets Ainfo: ENABLE_1.1_FEATURES bit to one.

□ Otherwise, PASS.

3C-I-02. Regular procedure: HPD pulse output caused by user operation

Test Objective

Verify that Repeater (DUT) pulses HPD of the upstream HDCP-protected Interface Port more than 100 ms when the Repeater (DUT) is operated manually to output HPD pulse to the upstream connection during the third part of authentication.

Required Test Method

This test is performed if PCP for Repeater_HPD_pulse == Y.

<Connection Setup>

It is same as '3C-I-01 Regular procedure: Transmitter – DUT - Receiver'.

<Configuration of TE>

Initial Setting	
Output signal	640x480p video signal with Data Island period in HDMI mode
First Part of Authentication	
Ainfo: ENABLE_1.1_FEATURES bit	no write (i.e. zero)

<Test Case>

The procedures from [Before starting authentication] to [Third Part of Authentication] described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

Verify HPD

□ By the manual operation, let the DUT output HPD pulse to the upstream connection. For example, connect another Sink device to the open downstream HDCP-protected Interface Port of DUT.

□ DUT pulses HPD for more than 100ms.

- ➢ If HPD is not de-asserted, then FAIL. (Refer to 'Ref-3C-10')
- ➢ If HPD is not de-asserted more than 100ms, then FAIL. (Refer to 'Ref-3C-10')]
- ➢ If HPD is not asserted again, then FAIL. (Refer to 'Ref-3C-10')

□ Otherwise, PASS.

3C-I-03. Irregular procedure: (First part of authentication) New Authentication

Test Objective

Verify that Repeater (DUT) accepts re-authentication when new An and Aksv is written by Transmitter right after An and Aksv is written in the unauthenticated state.

Required Test Method

<Connection Setup>

It is same as '3C-I-01 Regular procedure: Transmitter – DUT - Receiver'.

<Configuration of TE>

It is same as '3C-I-02 Regular procedure: HPD pulse output caused by user operation'.

<Test Case>

[Before starting authentication] described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' is performed.

(STEP S101) and **(STEP S102S)** of [First Part of Authentication] described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

- □ TE performs the actions below right after **(STEP S102S)**.
  - ● Read Bksv
  - ● Write An (different from the previously written one)
  - ● Write Aksv
  - ● Read Bcaps (REPEATER, 1.1_FEATURE, READY)

(STEP S102S) is performed again.

Verify R0' compared with R0

- □ DUT calculates R0' using the latest An.
- □ TE reads R0' after 100 ms from the time that TE finished writing the latest Aksv and compares R0' with R0.
  - ➢ If R0' does not equal to its own calculation R0, then FAIL. (Refer to 'Ref-3C-11')
- □ TE enables HDCP Encryption. (i.e. EESS: ENC_DIS -> ENC_EN).

As for the [Second Part of Authentication] and [Third Part of Authentication], the same procedures described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

- □ Otherwise, PASS.

3C-I-04. Irregular procedure: (Second part of authentication) New Authentication

Test Objective

Verify that Repeater (DUT) accepts re-authentication if new An and Aksv is written by Transmitter during second part of authentication.

Required Test Method

<Connection Setup>

It is same as '3C-I-01 Regular procedure: Transmitter – DUT - Receiver'.

<Configuration of TE>

It is same as '3C-I-02 Regular procedure: HPD pulse output caused by user operation'.

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

(STEP S201S) of [Second Part of Authentication] described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' is performed.

- □ TE disables HDCP Encryption and sends unencrypted video signal (EESS: ENC_DIS) by HDMI protocol (i.e. one Data island at least once per two video fields).
- □ Then, as the first part of authentication protocol, TE performs the actions below.
  - ● Read Bksv
  - ● Write An (different from the previously written one)
  - ● Write Aksv
  - ● Read Bcaps (REPEATER, 1.1_FEATURE, READY)

(STEP S102S) is performed again.

Verify R0' compared with R0

- □ DUT calculates R0' using the latest An.
- □ TE reads R0' after 100 ms from the time that TE finished writing the latest Aksv and compares R0' with R0.
  - ➢ If R0' does not equal to its own calculation R0, then FAIL. (Refer to 'Ref-3C-12')
- □ TE enables HDCP Encryption. (i.e. EESS: ENC_DIS -> ENC_EN).

As for the [Second Part of Authentication] and [Third Part of Authentication], the same procedures described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

□ Otherwise, PASS.

3C-I-05. Irregular procedure: (Third part of authentication) New Authentication

Test Objective

Verify that Repeater (DUT) accepts re-authentication if new An and Aksv is written by Transmitter during third part of authentication.

Required Test Method

<Connection Setup>

It is same as '3C-I-01 Regular procedure: Transmitter – DUT - Receiver'.

<Configuration of TE>

It is same as '3C-I-02 Regular procedure: HPD pulse output caused by user operation'.

<Test Case>

The procedures from [Before starting authentication] to [Third Part of Authentication] described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

- □ TE disables HDCP Encryption and sends unencrypted video signal (EESS: ENC_DIS) by HDMI protocol (i.e. one Data island at least once per two video fields).
- □ Then, as the first part of authentication protocol, TE performs the actions below.
  - ● Read Bksv
  - ● Write An (different from the previously written one)
  - ● Write Aksv
  - ● Read Bcaps (REPEATER, 1.1_FEATURE, READY)

(STEP S102S) is performed again.

Verify R0' compared with R0

- □ DUT calculates R0' using the latest An.
- □ TE reads R0' after 100 ms from the time that TE finished writing the latest Aksv and compares R0' with R0.
  - ➢ If R0' does not equal to its own calculation R0, then FAIL. (Refer to 'Ref-3C-12')
- □ TE enables HDCP Encryption. (i.e. EESS: ENC_DIS -> ENC_EN).

As for the [Second Part of Authentication] and [Third Part of Authentication], the same procedures described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

□ Otherwise, PASS.

3C-I-06. Irregular procedure: (Second part of authentication) Verify Bksv

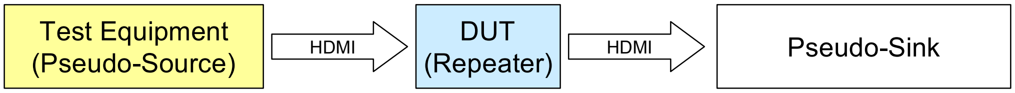
Test Objective

Verify that Repeater (DUT) considers it a failure of authentication protocol to read invalid Bksv from the downstream Receiver and does not assert Bcaps: READY bit to the upstream Transmitter as a failure of the second part of authentication protocol.

Required Test Method

<Connection Setup>

- □ Connect TE to the upstream HDCP-protected Interface Port of DUT.
- □ Connect Pseudo-Sink to the downstream HDCP-protected Interface Port of DUT.



* Pseudo-Sink is the device that has Sink (Receiver) function.

<Configuration of TE>

It is same as ‘3C-I-02 Regular procedure: HPD pulse output caused by user operation’.

<Configuration of Pseudo-Sink>

Initial Setting	
EDID	HDMI-capable
HDCP port	readable (can be accessed)
Bcaps: REPEATER bit	0
First Part of Authentication	
Bcaps: 1.1_FEATURES bit	0
Bksv	invalid value (does not containing 20 zeros and 20 ones)
R0’	correctly computed value
Third Part of Authentication	
Ri’	correctly computed value

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

[Second Part of Authentication]

Verify Bcaps: READY

- □ DUT reads invalid Bksv from downstream Pseudo-Sink and considers it a failure of the first part of authentication protocol with Pseudo-Sink.
- □ TE reads Bcaps (READY) from DUT at a rate of once every 100 ms after TE confirms the R0' of DUT for a maximum-permitted time of five seconds.
  - ➢ If DUT asserts Bcaps: READY bit within five seconds, then FAIL. (Refer to 'Ref-3C-13')

- □ Otherwise, PASS.

3C-I-07. Irregular procedure: (Second part of authentication) Verify R0'

Test Objective

Verify that Repeater (DUT) considers it a failure of authentication protocol to read invalid R0' from the downstream Receiver and does not assert Bcaps: READY bit to the upstream Transmitter as a failure of the second part of authentication protocol.

Required Test Method

<Connection Setup>

It is same as '3C-I-06 Irregular procedure: (Second part of authentication) Verify Bksv'.

<Configuration of TE>

It is same as '3C-I-06 Irregular procedure: (Second part of authentication) Verify Bksv'.

<Configuration of Pseudo-Sink>

Initial Setting	
EDID	HDMI-capable
HDCP port	readable (can be accessed)
Bcaps: REPEATER bit	0
First Part of Authentication	
Bcaps: 1.1_FEATURES bit	0
Bksv	valid value
R0'	incorrectly computed value
Third Part of Authentication	
Ri'	correctly computed value

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

[Second Part of Authentication]

Verify Bcaps: READY

□ Pseudo-Sink sets R0' incorrectly.

□ DUT reads invalid R0' from downstream Pseudo-Sink and considers it a failure of the first part of authentication protocol with Pseudo-Sink.

□ TE reads Bcaps (READY) from DUT at a rate of once every 100 ms after TE confirms the R0' of DUT for a maximum-permitted time of five seconds.

- ➢ If DUT asserts Bcaps: READY bit within five seconds, then FAIL. (Refer to

‘Ref-3C-13’)

- □ Otherwise, PASS.

□ Between HDMI-capable Transmitter and Repeater

Repeater's upstream procedure with HDMI-capable Transmitter is tested when Repeater is connected to the downstream HDCP-protected Interface Port of Repeater (DUT).

The attached Repeater supports the audio output.

- In this test, TE transmits 640x480p video format signal with Data Island period in HDMI mode. If PCP for Repeater_Audio_Supported == Y, video signal with audio is transmitted. Otherwise, video signal without audio is transmitted.

3C-II-01. Regular procedure: Transmitter - DUT - Repeater+Receiver

Test Objective

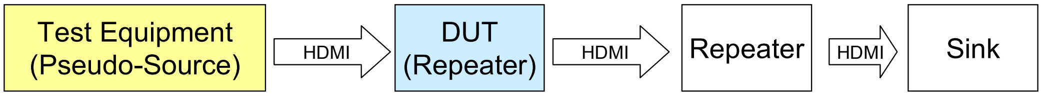
Verify that Repeater (DUT) performs the correct HDCP Authentication Protocol using production keys between the upstream HDMI-capable Transmitter and the downstream HDMI-capable Repeater. Upstream procedure of Repeater is verified.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

- □ Connect TE to the upstream HDCP-protected Interface Port of DUT.
- □ Connect a Repeater device which is connected with a Sink device to the downstream HDCP-protected Interface Port of DUT.



* A Sink device is the one that has already passed the Receiver Test.

* A Repeater device is the one that has already passed the Repeater Test.

<Configuration of TE>

Initial Setting		
Output signal	640x480p video signal with Data Island period in HDMI mode	
First Part of Authentication		
Ainfo: ENABLE_1.1_FEATURES bit	write one	no write (i.e. zero)
	By switching, each case is verified	
	However, if PCP for Repeater_1.1Features_Supported == N, only [no write] case is performed.	
R0 and Ri read	short format	combined format
	By switching, each case is verified	

* When TE sets Ainfo: ENABLE_1.1_FEATURES bit to one, TE performs Enhanced Link Verification.

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

[Second Part of Authentication]

(STEP S201R)

Verify the timing to assert Bcaps: READY

- □ DUT successfully completes the first part of authentication protocol with the downstream Repeater device that has valid Bksv.
- □ The downstream Repeater successfully completes the first part of authentication protocol with the downstream Sink device that has valid Bksv.
- □ The downstream Repeater sets Bstatus: DEPTH and DEVICE_COUNT to one and asserts Bcaps: READY bit. At this point, the Repeater already completes to set the configured size of valid KSVs in KSV FIFO and to calculate the correct V'.
- □ DUT successfully completes the second part of authentication with the downstream Repeater.
- □ TE reads Bcaps (READY) from DUT at a rate of once every 100 ms after TE confirms the R0' of DUT. DUT asserts Bcaps: READY bit within 1.2 seconds.
  - ➢ If DUT does not assert Bcaps: READY bit within 1.2 seconds after Aksv is written, then FAIL. (Refer to 'Ref-3C-14')

(STEP S202R)

Verify Bstatus

- □ TE reads Bstatus.
  - ➢ If Bstatus: MAX_DEVS_EXCEEDED bit is one, then FAIL. (Refer to 'Ref-3C-4')
  - ➢ If Bstatus: MAX_CASCADE_EXCEEDED bit is one, then FAIL. (Refer to 'Ref-3C-5')
  - ➢ If Bstatus: DEPTH is not two, then FAIL. (Refer to 'Ref-3C-6')
  - ➢ If Bstatus: DEVICE_COUNT is not two, then FAIL. (Refer to 'Ref-3C-7')

(STEP S203R)

Verify KSV list

- □ TE reads the KSVs from KSV FIFO in a single, auto-incrementing access. The size of KSVs is 10 bytes.
  - ➢ If DUT does not output the KSV list which consists of the downstream Repeater's Bksv and Sink's Bksv, then FAIL. (Refer to 'Ref-3C-15')

(STEP S204R)

Verify V' compared with V

- □ TE reads V'.
  - ➢ If read V' does not equal to its own calculation V, then FAIL. (Refer to 'Ref-3C-9')

As for the [Third Part of Authentication], the same procedures described in '3C-I-01 Regular procedure: Transmitter – DUT - Receiver' are performed.

□ Otherwise, PASS.

3C-II-02. Regular procedure: HPD after writing Aksv

Test Objective

Verify that Repeater (DUT) pulses HPD of the upstream HDCP-protected Interface Port more than 100 ms when the attached downstream Repeater pulses HPD of the upstream HDCP-protected Interface Port more than 100 ms during the first part of authentication.

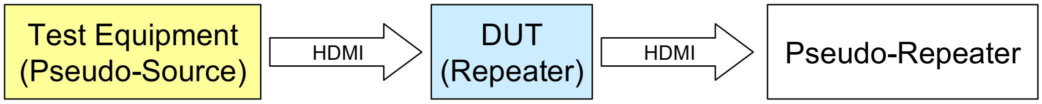
Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

□ Connect TE to the upstream HDCP-protected Interface Port of DUT.

□ Connect Pseudo-Repeater to the downstream HDCP-protected Interface Port of DUT.



* Pseudo-Repeater is the device that has both functions of Repeater and Sink connected to the Repeater.

<Configuration of TE>

It is same as '3C-I-02 Regular procedure: HPD pulse output caused by user operation'.

<Configuration of Pseudo-Repeater>

Initial Setting	
EDID	HDMI-capable
HDCP port	readable (can be accessed)
Bcaps: REPEATER bit	1
First Part of Authentication	
Bcaps: 1.1_FEATURES bit	0
Bksv	valid value
R0'	correctly computed value

Second Part of Authentication		
Setting after Aksv written	Bstatus:	
	DEPTH	6 or fewer
	DEVICE_COUNT	126 or fewer
	MAX_DEVS_EXCEEDED bit	0
	MAX_CASCADE_EXCEEDED bit	0
	KSV FIFO	(DEVICE_COUNT*5) bytes
	Bcaps: READY bit	Assert before (DEPTH*600) ms
V’	correctly computed value	
Third Part of Authentication		
Ri’	correctly computed value	

<Test Case>

[Before starting authentication] described in ‘3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver’ is performed.

(STEP S101) and **(STEP S102S)** of [First Part of Authentication] described in ‘3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver’ is performed.

Verify HPD

- □ Pseudo-Repeater pulses HPD of the upstream HDCP-protected Interface Port to DUT more than 100 ms after Aksv is written by DUT.
- □ Then, DUT pulses HPD of the upstream HDCP-protected Interface Port to TE for more than 100ms.
  - ➢ If HPD is not de-asserted, then FAIL. (Refer to ‘Ref-3C-10’)
  - ➢ If HPD is not de-asserted more than 100ms, then FAIL. (Refer to ‘Ref-3C-10’)]
  - ➢ If HPD is not asserted again, then FAIL. (Refer to ‘Ref-3C-10’)

- □ Otherwise, PASS.

3C-II-03. Regular procedure: HPD after reading R0'

Test Objective

Verify that Repeater (DUT) pulses HPD of the upstream HDCP-protected Interface Port more than 100 ms when the attached downstream Repeater pulses HPD of the upstream HDCP-protected Interface Port more than 100 ms during the second part of authentication.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of TE>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of Pseudo-Repeater>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver' are performed.

Verify HPD

□ Pseudo-Repeater pulses HPD of the upstream HDCP-protected Interface Port to DUT more than 100 ms after R0' is read by DUT.

□ Then, DUT pulses HPD of the upstream HDCP-protected Interface Port to TE for more than 100ms.

- ➢ If HPD is not de-asserted, then FAIL. (Refer to 'Ref-3C-10')
- ➢ If HPD is not de-asserted more than 100ms, then FAIL. (Refer to 'Ref-3C-10')]
- ➢ If HPD is not asserted again, then FAIL. (Refer to 'Ref-3C-10')

□ Otherwise, PASS.

3C-II-04. Regular procedure: HPD after starting third part of authentication

Test Objective

Verify that Repeater (DUT) pulses HPD of the upstream HDCP-protected Interface Port more than 100 ms when the attached downstream Repeater pulses HPD of the upstream HDCP-protected Interface Port more than 100 ms during the third part of authentication.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of TE>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of Pseudo-Repeater>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver' are performed.

[Second Part of Authentication]

(STEP S201PR)

Verify the timing to assert Bcaps: READY

- □ DUT successfully completes the first part of authentication protocol with Pseudo-Repeater that has valid Bksv.
- □ Pseudo-Repeater sets Bstatus: DEPTH and DEVICE_COUNT to the configured value and asserts Bcaps: READY bit. At this point, Pseudo-Repeater already completes to set the configured size of valid KSVs in KSV FIFO and to calculate the correct V'.
- □ DUT successfully completes the second part of authentication with Pseudo-Repeater.
- □ TE reads Bcaps (READY) from DUT at a rate of once every 100 ms after TE confirms

the R0' of DUT. DUT asserts Bcaps: READY bit within 600ms after Pseudo-Repeater asserts Bcaps: READY bit.

- ➢ If DUT does not assert Bcaps: READY bit within 'Pseudo-Repeater's configured period to assert Bcaps: READY' plus 600ms after Aksv is written, then FAIL. (Refer to 'Ref-3C-14')

(STEP S202PR)

Verify Bstatus

- □ TE reads Bstatus.
  - ➢ If Bstatus: MAX_DEVS_EXCEEDED bit is one, then FAIL. (Refer to 'Ref-3C-4')
  - ➢ If Bstatus: MAX_CASCADE_EXCEEDED bit is one, then FAIL. (Refer to 'Ref-3C-5')
  - ➢ If Bstatus: DEPTH is not 'Pseudo-Repeater's configured value' plus one, then FAIL. (Refer to 'Ref-3C-6')
  - ➢ If Bstatus: DEVICE_COUNT is not 'Pseudo-Repeater's configured value' plus one, then FAIL. (Refer to 'Ref-3C-7')

(STEP S204PR)

Verify V' compared with V

- □ TE reads V'.
  - ➢ If read V' does not equal to its own calculation V, then FAIL. (Refer to 'Ref-3C-9')

As for the [Third Part of Authentication], the same procedures described in '3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver' are performed.

Verify HPD

- □ Pseudo-Repeater pulses HPD of the upstream HDCP-protected Interface Port to DUT more than 100 ms.
- □ Then, DUT pulses HPD of the upstream HDCP-protected Interface Port to TE for more than 100ms.
  - ➢ If HPD is not de-asserted, then FAIL. (Refer to 'Ref-3C-10')
  - ➢ If HPD is not de-asserted more than 100ms, then FAIL. (Refer to 'Ref-3C-10')]
  - ➢ If HPD is not asserted again, then FAIL. (Refer to 'Ref-3C-10')

- □ Otherwise, PASS.

3C-II-05. Irregular procedure: (Second part of authentication) Verify V'

Test Objective

Verify that Repeater (DUT) considers it a failure of the second part of authentication protocol to read invalid V' from the downstream Repeater and does not assert Bcaps: READY bit to the upstream Transmitter.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of TE>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of Pseudo-Repeater>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv' except for the following.

- V' = incorrectly computed value

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver' are performed.

[Second Part of Authentication]

Verify Bcaps: READY

□ Pseudo-Repeater calculates V' incorrectly.

□ DUT reads invalid V' from Pseudo-Repeater and considers it a failure of the second part of authentication protocol with Pseudo-Repeater.

□ TE reads Bcaps (READY) from DUT at a rate of once every 100 ms after TE confirms the R0' of DUT for a maximum-permitted time of five seconds.

- ➢ If DUT asserts Bcaps: READY bit within five seconds, then FAIL. (Refer to 'Ref-3C-16')

□ Otherwise, PASS.

3C-II-06. Irregular procedure: (Second part of authentication) DEVICE_COUNT

Test Objective

Verify that Repeater (DUT) asserts Bstatus: MAX_DEVS_EXCEEDED bit if the computed DEVICE_COUNT for it exceeds the size or the KSV FIFO.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of TE>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of Pseudo-Repeater>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv' except for the following.

- DEVICE_COUNT = Repeater_Max_KSV

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver' are performed.

[Second Part of Authentication]

□ Pseudo-Repeater sets Bstatus: DEPTH and DEVICE_COUNT to the configured value and asserts Bcaps: READY bit at the configured period after Aksv is written.

□ TE reads Bcaps (READY) from DUT at a rate of once every 100 ms after TE confirms the R0' of DUT.

There are two possible behaviors for DUT.

Verify	Bstatus

Case 1:

□ DUT asserts Bcaps: READY bit within 'Pseudo-Repeater's configured period' plus 600ms.

□ TE reads Bstatus.

- ➢ If Bstatus: MAX_DEVS_EXCEEDED bit is not one, then FAIL. (Refer to 'Ref-3C-17')

Case 2:

□ DUT does not assert Bcaps: READY bit.

□ TE polls downstream Bcaps (READY) at least five seconds.

□ TE reads Bstatus.

- ➢ If Bstatus: MAX_DEVS_EXCEEDED bit is not one, then FAIL. (Refer to 'Ref-3C-17')

□ Otherwise, PASS.

3C-II-07. Irregular procedure: (Second part of authentication) DEPTH

Test Objective

Verify that Repeater (DUT) asserts Bstatus: MAX_CASCADE_EXCEEDED bit if the computed DEPTH for it exceeds seven.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of TE>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of Pseudo-Repeater>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv' except for the following.

- Bstatus: DEPTH = 7
- Bstatus: DEVICE_COUNT = 7

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver' are performed.

[Second Part of Authentication]

□ Pseudo-Repeater sets Bstatus: DEPTH and DEVICE_COUNT to the configured value and asserts Bcaps: READY bit at the configured period after Aksv is written.

□ TE reads Bcaps (READY) from DUT at a rate of once every 100 ms after TE confirms the R0' of DUT.

There are two possible behaviors for DUT.

Verify Bstatus

Case 1:

□ DUT asserts Bcaps: READY bit within 'Pseudo-Repeater's configured period' plus

600ms.

□ TE reads Bstatus.

- ➢ If Bstatus: MAX_CASCADE_EXCEEDED bit is not one, then FAIL. (Refer to 'Ref-3C-18')

Case 2:

□ DUT does not assert Bcaps: READY bit.

□ TE polls downstream Bcaps (READY) at least five seconds.

□ TE reads Bstatus.

- ➢ If Bstatus: MAX_CASCADE_EXCEEDED bit is not one, then FAIL. (Refer to 'Ref-3C-18')

□ Otherwise, PASS.

3C-II-08. Irregular procedure: (Second part of authentication) MAX_DEVS_EXCEEDED

Test Objective

Verify that Repeater (DUT) asserts Bstatus: MAX_DEVS_EXCEEDED bit when it receives a MAX_DEVS_EXCEEDED status from a downstream Repeater.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of TE>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of Pseudo-Repeater>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv' except for the following.

- Bstatus: MAX_DEVS_EXCEEDED bit = 1

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver' are performed.

[Second Part of Authentication]

□ Pseudo-Repeater sets Bstaus: MAX_DEVS_EXCEEDED bit to one and asserts Bcaps: READY bit at the configured period after Aksv is written.

□ TE reads Bcaps (READY) from DUT at a rate of once every 100 ms after TE confirms the R0' of DUT.

There are two possible behaviors for DUT.

Verify Bstatus

Case 1:

□ DUT asserts Bcaps: READY bit within 'Pseudo-Repeater's configured period' plus 600ms.

□ TE reads Bstatus.

- ➢ If Bstatus: MAX_DEVS_EXCEEDED bit is not one, then FAIL. (Refer to 'Ref-3C-19')

Case 2:

□ DUT does not assert Bcaps: READY bit.

□ TE polls downstream Bcaps (READY) at least five seconds.

□ TE reads Bstatus.

- ➢ If Bstatus: MAX_DEVS_EXCEEDED bit is not one, then FAIL. (Refer to 'Ref-3C-19')

□ Otherwise, PASS.

3C-II-09. Irregular procedure: (Second part of authentication) MAX_CASCADE_EXCEEDED

Test Objective

Verify that Repeater (DUT) asserts Bstatus: MAX_CASCADE_EXCEEDED bit when it receives a MAX_ CASCADE _EXCEEDED status from a downstream Repeater.

Required Test Method

This test is performed if PCP for Repeater_Max_KSV >= 2.

<Connection Setup>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of TE>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv'.

<Configuration of Pseudo-Repeater>

It is same as '3C-II-02 Regular procedure: HPD after writing Aksv' except for the following.

- Bstatus: MAX_CASCADE_EXCEEDED bit = 1
- Bstatus: DEPTH = 7
- Bstatus: DEVICE_COUNT = 7

<Test Case>

The procedures from [Before starting authentication] to [First Part of Authentication] described in '3C-II-01 Regular procedure: Transmitter - DUT - Repeater+Receiver' are performed.

[Second Part of Authentication]

□ Pseudo-Repeater sets Bstaus: MAX_CASCADE_EXCEEDED bit to one and asserts Bcaps: READY bit at the configured period after Aksv is written.

□ TE polls downstream Bcaps (READY) at a rate of once every 100 ms after TE confirms the R0' of DUT.

There are two possible behaviors for DUT.

Verify Bstatus

Case 1:

- □ DUT asserts Bcaps: READY bit within 'Pseudo-Repeater's configured period' plus 600ms.
- □ TE reads Bstatus.
  - ➢ If Bstatus: MAX_CASCADE_EXCEEDED bit is not one, then FAIL. (Refer to 'Ref-3C-19')

Case 2:

- □ DUT does not assert Bcaps: READY bit.
- □ TE polls downstream Bcaps (READY) at least five seconds.
- □ TE reads Bstatus.
  - ➢ If Bstatus: MAX_CASCADE_EXCEEDED bit is not one, then FAIL. (Refer to 'Ref-3C-19')

- □ Otherwise, PASS.

Recommended Tests

This section of the HDCP Compliance Test Specification uses Protocol Analyzers and Protocol Generators to test corresponding Source and Sink devices.

In general, Source devices are tested using a Sink emulator and/or Protocol Analyzer (PA). These Sink emulators may have a variety of EDID structures used to encourage certain behavior by the Source DUT and they are capable of measuring a variety of parameters or attributes of the signals delivered by the Source DUT. The measurement may be performed using the facilities of the Sink emulator itself or using standard test equipment such as digital oscilloscopes, logic analyzers or spectrum analyzers.

Likewise, Sink devices are tested using a variety of Source emulators or Protocol Generators (PG) capable of generating a variety of test signals or examining a variety of Sink characteristics indicated via DDC.

4. Source Tests

4A. Audio/Video Format Switching

Test Objective

If the DUT has the ability to change audio and/or video formats, this function is checked to verify proper HDCP operation during the change

Test Conditions and Setup

Setup: Source Standard PA

Test Method

- Turn off DUT, connect DUT to PA
- Power on and configure PA
- Power on DUT
- Verify initial authentication and transmission of correct audio and video content
- Attempt, through menus, buttons, etc., to force the DUT to change video formats (e.g. 480p, 1080i, 720p…) while playing same content (same DVD or channel). Force at least 5 such changes
    - If the above operations caused a non-recovered failure, then FAIL
- Attempt, through menus, buttons, etc. to force the DUT to change audio formats (e.g. “Stream”, “Dolby Digital”, “PCM”…) while playing same content (same DVD or channel). Force at least 5 such changes
    - If the above operations caused a non-recovered failure, then FAIL
- If the audio / video format changes were completed successfully with proper HDCP operation during the change, then PASS
- Record any warnings or errors detected in the TRF

4B. Media Switching

Test Objective

If the DUT has the ability to change source media (DVDs, channel changing, input sources, etc.), this test will verify proper HDCP operation during the change

Test Conditions and Setup

Setup: Source Standard PA

Test Method

- Turn off DUT, connect DUT to ready PA
- Power on DUT
- Verify initial authentication and transmission of correct audio and video content
- If DUT contains a DVD player or other pre-recorded content player, change the media while leaving the DUT powered on and active. Repeat for 4 changes, alternating between two different DVDs (or other media)
- If DUT contains a satellite, off-air or cable decoder function, change the channel while leaving the DUT powered on and active. Repeat at least 20 times
    - If some channels are HD and others are standard, perform the channel changing through as many SD -> HD -> SD transitions as feasible
- If DUT contains multiple sources of content (e.g. combo DVD and VCR, or DVD with up-converted analog input, or STB with 1394 input from D-VHS, etc.), switch between each of the content sources. For each source, perform any appropriate media switching test such as DVD changing or channel changing
    - If any of the operations caused a non-recovered failure, then FAIL
- If the media switching was completed successfully with proper HDCP operation during the change, then PASS
- Record on the TRF whether any failure conditions were found, whether AVMUTE was used during changes, and PASS/FAIL/WARNING

4C. Force AVMUTE

Test Objective

Verify behavior of AVMUTE for any other cause not already covered

Test Conditions and Setup

Setup: Source Standard PA

Test Method

If CDF field AVMUTE_usage indicates a condition that has not already been tested in the previous two tests, perform this test. SKIP if the indicated AVMUTE cause has already been tested

- Turn off DUT, connect DUT to ready PA
- Power on DUT
- Verify initial authentication and transmission of correct audio and video content
- Cause the DUT to activate AVMUTE using the CDF recommended procedures
- For each listed cause, perform the operation 5 times
  - If the above operation(s) caused a non-recovered failure in authentication or content delivery, then FAIL, “AVMUTE not effective”
- If the above operation(s) were completed successfully, then PASS
- Record on the TRF whether any re-authentications were performed, any failure conditions, whether AVMUTE was used during changes, and PASS/FAIL/WARNING

If the audio and video data contains protected content, it must be blocked in some way at the DUT, so that it is not possible to observe “plaintext” while muted.

Note that it is acceptable for the DUT to block all content while muted, whether or not the content needs to be protected

4D. Link Integrity (Pj) Check Repeat Rate

Test Objective

Are the Pj checks performed at the proper rate?

Test Conditions and Setup

Setup: Source Standard PA

Test Method

- The DUT is configured to send a recognizable audio/video stream, with HDCP enabled.
- The PA will produce the expected Pj' results
- The DUT shall perform the Pj checks within the prescribed time limits
  - If the DUT does not perform Pj checks within the prescribed time limits (every 16th encrypted frame or every 16th frame if ADVANCE_CIPHER is enabled), then FAIL
- If DUT performs Pj checks within prescribed time limits, then PASS

Note that it MAY do this whether or not 1.1 features are supported, but that it MUST do this when supported and enabled

4E. Pj Mismatch Response

Test Objective

Does the system respond properly when there is a Pj mismatch?

Test Conditions and Setup

Setup: Source Standard PA

Test Method

- The DUT is configured to send a recognizable audio/video stream, with HDCP enabled
- The PA will intentionally garble the Pj' sequence after approximately 30 seconds of proper encryption
- The DUT shall detect this as a link failure within 1 second of the first garbled Pj' read. The DUT shall then re-authenticate and re-enable the link
  - If the DUT does not re-authenticate within 1 second of the first garbled Pj' read, then FAIL

5. Reference

Ref-1A-1. Video signal

Reference	Requirement
Transition H1:H3. in page 17	**Transition H1:H3.** Immediately after transitioning to HDMI mode, the transmitter should begin sending a video signal. This signal may be required before the registers of the HDCP Receiver are visible to the HDCP Transmitter.
Transition P1:P3. in page 23	**Transition P1:P3.** Immediately after transitioning to HDMI mode, the transmitter should begin sending a video signal. This signal may be required before the registers of the HDCP Receiver are visible to the HDCP Repeater.

Ref-1A-2. The transition to HDMI mode

Reference	Requirement
5th paragraph in page 33	The reception of a Data Island preamble followed by a Data Island Guard Band will transition the HDCP Receiver to HDMI mode. The successful transition to HDMI mode by the HDCP Receiver is indicated by setting Bstatus bit HDMI_MODE. After this, the authentication protocol is started and EESS assumed regardless of the setting of Bcaps bit 1.1_FEATURES or Ainfo bit ENABLE_1.1_FEATURES.

Ref-1A-3. The start of the authentication

Reference	Requirement
State A0 in page 17	For this reason, a valid video screen should at all times be transmitted whenever HPD is asserted and authentication should be started immediately after detecting a valid Bksv (Transition A0: A1).

Ref-1A-4. Write An, Aksv

Reference	Requirement
State A1 in page 17	**State A1: Exchange KSVs.** In this state, the HDCP Transmitter generates a 64-bit pseudorandom value (An) and writes that value to the HDCP Receiver.
An of Table2-2 in page 28	This multi-byte value must be written by the HDCP Transmitter before the KSV is written.

Ref-1A-5. Write Ainfo: ENABLE_1.1_FEATURES

Reference	Requirement
State A1 in page 17	If necessary, it sets Ainfo in the HDCP Receiver to determine the options that will be in effect prior to writing its KSV (Aksv) to the HDCP Receiver.
Ainfo of Table 2-2. in page 28	Bit 1: ENABLE_1.1_FEATURES. This bit enables the Advance Cipher option.

Ref-1A-6. Read R0'

Reference	Requirement
4th paragraph in page 10	The HDCP Transmitter must not read the R0' value sooner than 100ms after writing Aksv
State A3 in page 17	The HDCP Transmitter must allow the HDCP Receiver up to 100 ms to make R0' available from the time that Aksv is written.
State F3 in page 23	The HDCP Transmitter must not attempt to read R0' sooner than this 100 ms. The HDCP Receiver's Bksv is added to the KSV list for this HDCP Repeater.

Ref-1A-7. Ri' Size

Reference	Requirement
Ri of Table 2-2. in page 28	Ri' = 2 (size in Bytes)

Ref-1A-8. Enable Encryption

Reference	Requirement
last paragraph in page 10	The HDCP Transmitter enables HDCP Encryption when the first part of the authentication protocol successfully completes
State A3 in page 17	The HDCP Transmitter reads *R0* from the HDCP Receiver and compares it with the corresponding *R0* produced by the HDCP Transmitter during the computations of State A2. If *R0* is equal to *R0*, then HDCP Encryption is immediately enabled.
State F3 in page 23	State F3: Validate Receiver. The downstream (HDCP Transmitter) side reads R0' from the HDCP Receiver and compares it with the corresponding R0 produced by itself during the computations of State F2, then immediately enables data encryption if R0' is equal to R0.

Ref-1A-9. Read Ri’

Reference	Requirement
Figure 2-4. in page 13	Read: R’i every 2 seconds Verify Ri == Ri’ every 2 seconds
Figure 2-4. – footnotes in page 13	Reading Ri synchronously every 128th frame is also acceptable in lieu of asynchronous polling every 2 seconds

First paragraph in page 14	R*i* is a 16-bit value used for link integrity verification, and is updated for every 128th frame counter increment, starting with the 128th. The HDCP Transmitter verifies *Ri'* against its own calculations to insure that the video receiver is still able to correctly decrypt the information. This verification is made at a minimum rate of once every two seconds
First paragraph in page 14	Synchronous reading of Ri every time it changes (every 128th frame) is also acceptable in lieu of asynchronous polling. (Synchronous reading in the frame prior to Ri update and shortly after 1 millisecond of the Ri update also provides a method of detecting frame counter mismatch between HDCP transmitter and HDCP receiver when either device does not support Enhanced Link Verification.)
State A5 in page 18	**State A5: Link Integrity Check.** In this state, the HDCP Transmitter reads Ri' from the HDCP Receiver and compares that value against its value Ri. If the values are not equal, then the HDCP Receiver is incorrectly decrypting the transmitted stream. The Ri' value may be reread to allow for synchronization and I2C bus errors.
State A3 in page 17	**State A3: Validate Receiver**. The HDCP Transmitter reads *R0'* from the HDCP Receiver and compares it with the corresponding *R0* produced by the HDCP Transmitter during the computations of State A2. If *R0* is equal to *R0'*, then HDCP Encryption is immediately enabled. The verification timer is set up to generate timer events at the nominal rate of once every two seconds, plus or minus one-half second.
State F4 in page 23	**State F4: Authenticated**. At this time, and at no prior time, the downstream (HDCP Transmitter) side has completed the authentication protocol and is fully operational, able to deliver HDCP Content. The verification timer is set up to generate timer events at the nominal rate of once every two seconds, plus or minus one-half second.
State F5 in page 24	**State F5: Link Integrity Check.** In this state, the downstream (HDCP Transmitter) side reads *Ri'* from the HDCP Receiver and

	compares that value against its value *Ri*. If the values are equal, then the HDCP Receiver is correctly decrypting the transmitted stream. The *Ri'* value may be re-read to allow for synchronization and I2C bus errors.

Ref-1A-10. CTLx

Reference	Requirement
Page 32, Section 2.7, first paragraph	However, since an HDCP Transmitter may become unauthenticated with no immediate downstream indication, an HDCP Receiver may not be aware of this change and will continue to expect encryption signaling. Therefore it is highly recommended that the HDCP Transmitter not signal frame encryption while in the unauthenticated state. In the case of prior EESS signaling, it is recommended that the encryption-disabled signaling continue (rather than no encryption signaling), ensuring that the HDCP receiver properly displays the blue screen, informative display, or low value content which is sent while the HDCP Transmitter is in an unauthenticated state and the HDCP Receiver is still in an authenticated state.
Last paragraph in page 33	The CTLx signals described in Table 2-5 are only valid within a 16-clock window of opportunity starting at 512 pixel clocks following the active edge of VSYNC.

Ref-1A-11. Keep-out period

Reference	Requirement
Last paragraph in page 34	It is required that no Data Island or Video Data, nor any Guard Band, be transmitted during a keep-out period that starts 508 pixels past the active edge of VSYNC and ends 650 pixels past the active edge of VSYNC.

Ref-1A-12. Line Key Calc

Reference	Requirement
State G3 in page 41	No data period may begin until at least 58 pixel clocks following the fall of videoData.

Ref-1A-13. Authenticated/Encryption

Reference	Requirement
State A4. in page 18	**State A4: Authenticated**. The HDCP Transmitter has completed the authentication protocol. At this time, and at no time prior, the HDCP System makes available to the Upstream Content Control Function upon request, information that indicates that the HDCP System is fully engaged and able to deliver HDCP Content, which means (a) HDCP Encryption is operational on each downstream HDCP-protected Interface Port attached to an HDCP Receiver, (b) processing of valid received SRMs, if any, has occurred, as defined in this Specification, and (c) there are no HDCP Receivers on HDCP-protected Interface Ports, or downstream, with KSVs in the current revocation list.
State F4. in page 23	**State F4: Authenticated**. At this time, and at no prior time, the downstream (HDCP Transmitter) side has completed the authentication protocol and is fully operational, able to deliver HDCP Content.

Ref-1A-14. Loss of HPD

Reference	Requirement
Transition Any State:H0. in page 16	**Transition Any State:H0.** Reset conditions at the HDCP Transmitter or loss of Hot Plug Detect (HPD) cause the HDCP Transmitter to enter the No Receiver Attached state.

Ref-1A-15. HDCP Port Access

Reference	Requirement
First paragraph in page 15	The HDCP transmitter should not attempt to authenticate until it has successfully obtained an acknowledged read of an HDCP I2C register. Should the I2C register read or the authentication fail, the HDCP Transmitter must retry periodically, with a period of no more than 2 seconds (preferably much more often).
State A0 in page 17	The transmitter must repeatedly attempt to read an HDCP register, at least once every 2 seconds and preferably much more often.

Ref-1A-16. Verify Bksv

Reference	Requirement
the last paragraph in page 9	The HDCP Transmitter verifies that the HDCP Receiver's KSV has not been revoked (section 5), and that the received KSV contains 20 ones and 20 zeros.
State A1 in page 17	The HDCP Transmitter also reads the HDCP Receiver's KSV (*Bksv*) and the REPEATER status bit necessary for cipher initialization.
Transition A1:A0 in page 17	Transition A1:A0. Failure to read Bksv containing 20 zeros and 20 ones is considered a protocol failure and causes this state transition to State A0.
State A0. in page 17	For this reason, a valid video screen should at all times be transmitted whenever HPD is asserted and authentication should be started immediately after detecting a valid Bksv (Transition A0: A1).
Transition A3:A0 in page 18	Transition A3:A0. The link integrity message R0 received from the HDCP Receiver does not match the value calculated by the HDCP Transmitter, or Bksv is in the current revocation list.
Transition F1:F2 in page 23	The downstream (HDCP Transmitter) side is required to validate that Bksv contains 20 ones and 20 zeros.

Ref-1A-17. Verify R0’

Reference	Requirement
last paragraph in page 10	The HDCP Transmitter enables HDCP Encryption when the first part of the authentication protocol successfully completes
Transition A3:A0 in page 18	Transition A3:A0. The link integrity message R0 received from the HDCP Receiver does not match the value calculated by the HDCP Transmitter, or Bksv is in the current revocation list.
State A0. in page 17	For this reason, a valid video screen should at all times be transmitted whenever HPD is asserted and authentication should be started immediately after detecting a valid Bksv (Transition A0: A1).
Transition F3:F0 in page 23	Transition F3:F0. The link integrity message R0' received from the HDCP Receiver does not match the value calculated by the downstream (HDCP Transmitter) side.
State F0. in page 23	For this reason, a valid video screen should at all times be transmitted whenever Hot Plug Detect is asserted, and downstream authentication should be started immediately after detecting a valid Bksv (Transition F0: F1).

Ref-1A-18. Verify Ri’

Reference	Requirement
Transition A5:A0. in page 18	Transition A5:A0. Ri' from the HDCP Receiver does not match the expected value, Ri, or the value was not returned to the HDCP Transmitter within 1 millisecond from the initiation of the read operation, or the loss of synchronization was detected using the Ri or Pj values.
State A0. in page 17	For this reason, a valid video screen should at all times be transmitted whenever HPD is asserted and authentication should be started immediately after detecting a valid Bksv (Transition A0: A1).
Transition F5:F0. in page 24	Transition F5:F0. Ri’ from the HDCP Receiver does not match the expected value, Ri, or the value was not returned to the downstream (HDCP Transmitter) side within 1 millisecond from the initiation of the read operation, or the loss of synchronization was detected using the Ri or Pj values.
State F0. in page 23	For this reason, a valid video screen should at all times be transmitted whenever Hot Plug Detect is asserted, and downstream authentication should be started immediately after detecting a valid Bksv (Transition F0: F1).

Ref-1A-19. SRM

Reference	Requirement
the last paragraph in page 12	Authentication fails if the topology maximums are exceeded. The top-level HDCP Transmitter checks to see if the KSV of any attached device is found in the current revocation list, and, if present, the authentication fails. The HDCP Transmitter verifies the integrity of the current revocation list by checking the signature of the system renewability message (SRM) using the Digital Content Protection LLC public key. Failure of this integrity check constitutes an authentication failure.
State A4, in page 18	State A4: Authenticated. The HDCP Transmitter has completed the authentication protocol. At this time, and at no time prior, the HDCP System makes available to the Upstream Content Control Function upon request, information that indicates that the HDCP System is fully engaged and able to deliver HDCP Content, which means (a) HDCP Encryption is operational on each downstream HDCP-protected Interface Port attached to an HDCP Receiver, (b) processing of valid received SRMs, if any, has occurred, as defined in this Specification, and (c) there are no HDCP Receivers on HDCP-protected Interface Ports, or downstream, with KSVs in the current revocation list.
Section 5 - Renewability	The HDCP Transmitter is required to manage system renewability messages (SRMs) carrying the KSV revocation list. These messages are delivered with content and must be checked when available. The validity of an SRM is established by verifying the integrity of its signature with the Digital Content Protection LLC public key, which is specified by the Digital Content Protection LLC.

Ref-1B-1. KSV list READY

Reference	Requirement
1st paragraph in page 11	The HDCP Transmitter executes the second part of the protocol only when the REPEATER bit is set, indicating that the attached HDCP Receiver is an HDCP Repeater.
The 4th paragraph in page 11	The HDCP Transmitter, having determined that the REPEATER bit read earlier in the protocol is set, sets a five-second watchdog timer and polls the HDCP Repeater's READY status bit.
1st paragraph in page 13	Table 2–1 specifies HDCP Repeater timing requirements that bound the worst-case propagation time for the KSV list. Note that because each HDCP Repeater does not know the number of downstream HDCP Repeaters, it must use the same five-second timeout used by the upstream HDCP Transmitter when polling for downstream READY.
State A8 in page 18	State A8: Wait for Ready. The HDCP Transmitter sets up a five-second watchdog timer and polls the HDCP Receiver's READY bit.
State F8 in page 24	State F8: Wait for Ready. The downstream (HDCP Transmitter) side sets up a five-second watchdog timer and polls the HDCP Receiver's READY bit.

Ref-1B-2. Read KSV FIFO

Reference	Requirement
KSV_FIFO of Table2-2 in page 29	All bytes (DEVICE_COUNT * 5) must be read in a single, auto-incrementing access.
State A9 in page 18	The HDCP Transmitter reads the list of attached KSVs from the KSV FIFO, reads *V'*, computes *V*, and verifies *V* == *V'*, and the KSVs from the list are compared against the current revocation list.
State F9 in page 24	The downstream (HDCP Transmitter) side reads the list of attached KSVs through the KSV FIFO, reads *V'*, computes *V*, and verifies *V*== *V'*, and the KSVs from this port are added to the KSV list for this HDCP Repeater.

Ref-1B-3. Read V’

Reference	Requirement
4th paragraph in page 11	The HDCP Transmitter verifies the integrity of the KSV list by computing the SHA–1 hash value V and comparing this value to V'.
State A9 in page 18	The HDCP Transmitter reads the list of attached KSVs from the KSV FIFO, reads V’, computes V, and verifies V == V', and the KSVs from the list are compared against the current revocation list.
Transition A9:A4. in page 19	**Transition A9:A4.** If *V*== *V'*, the SRM is valid, none of the reported KSVs are in the current revocation list, and the downstream topology does not exceed specified maximums.
State F9 in page 24	The downstream (HDCP Transmitter) side reads the list of attached KSVs through the KSV FIFO, reads *V'*, computes *V*, and verifies *V*== *V'*, and the KSVs from this port are added to the KSV list for this HDCP Repeater.
Transition F9:F4. in page 24	**Transition F9:F4.** This transition is made if *V*== *V'* and the downstream topology does not exceed specified maximums.

Ref-1B-4. Timeout of KSV list READY

Reference	Requirement
Last paragraph in page 12	If the asserted READY status is not received within a maximum-permitted time of five seconds, authentication of the HDCP Repeater fails.
Transition A8:A0 in page 18	Transition A8:A0. The watchdog timer expires before the READY indication is received.
State A0. in page 17	For this reason, a valid video screen should at all times be transmitted whenever HPD is asserted and authentication should be started immediately after detecting a valid Bksv (Transition A0: A1).
Transition F8:F0 in page 24	Transition F8:F0. The watchdog timer expires before the READY indication is received.
State F0. in page 23	For this reason, a valid video screen should at all times be transmitted whenever Hot Plug Detect is asserted, and downstream authentication should be started immediately after detecting a valid Bksv (Transition F0: F1).

Ref-1B-5. Verify V’

Reference	Requirement
4th paragraph in page 11	If *V* is not equal to *V'*, then the authentication protocol is aborted.
State A9 in page 18	State A9: Read KSV List. The watchdog timer is cleared. The HDCP Transmitter reads the list of attached KSVs from the KSV FIFO, reads V’, computes V, and verifies V == V', and the KSVs from the list are compared against the current revocation list.
Transition A9:A0 in page 19	**Transition A9:A0.** This transition is made if *V* != *V'*, [verification of the SRM fails,] or if any of the KSVs in the list are found in the current revocation list. A retry of the entire KSV FIFO read operation may be implemented if V != V’.
State A0. in page 17	For this reason, a valid video screen should at all times be transmitted whenever HPD is asserted and authentication should be started immediately after detecting a valid Bksv (Transition A0: A1).
State F9 in page 24	The downstream (HDCP Transmitter) side reads the list of attached KSVs through the KSV FIFO, reads *V'*, computes *V*, and verifies *V* == *V'*, and the KSVs from this port are added to the KSV list for this HDCP Repeater.
Transition F9:F0 in page 24	**Transition F9:F0.** This transition is made if *V* != *V'*. A retry of the entire KSV FIFO read operation may be implemented if V != V’.
State F0. in page 23	For this reason, a valid video screen should at all times be transmitted whenever Hot Plug Detect is asserted, and downstream authentication should be started immediately after detecting a valid Bksv (Transition F0: F1).

Ref-1B-6. MAX_CASCADE_EXCEEDED / MAX_DEVS_EXCEEDED

Reference	Requirement
Transition A9:A0. in page 19	Two additional status bits cause this transition when asserted. These are MAX_CASCADE_EXCEEDED and MAX_DEVS_EXCEEDED.
State A0. in page 17	For this reason, a valid video screen should at all times be transmitted whenever HPD is asserted and authentication should be started immediately after detecting a valid Bksv (Transition A0: A1).
Transition F9:F0 in page 24	It is also made if either MAX_CASCADE_EXCEEDED or MAX_DEVS_EXCEEDED are asserted.
State F0. in page 23	For this reason, a valid video screen should at all times be transmitted whenever Hot Plug Detect is asserted, and downstream authentication should be started immediately after detecting a valid Bksv (Transition F0: F1).

Ref-1B-7. DEVICE_COUNT = 0

Reference	Requirement
2nd paragraph in Page 21	NOTE: HDCP Repeaters that have no active downstream HDCP devices must be considered. The HDCP Repeater may authenticate as an HDCP Receiver with Bcaps REPEATER bit set to 0 if it wishes to receive HDCP Content, but may not pass HDCP Content to downstream devices. If an HDCP Transmitter encounters a downstream HDCP Repeater reporting zero DEVICE_COUNT and sends it HDCP Content, it must complete the second phase of authentication successfully, computing V over an empty KSV list.

Ref-1B-8. Re-authentication after timeout of READY

Reference	Requirement
1st paragraph in Page 12	If the asserted READY status is not received within a maximum-permitted time of five seconds, authentication of the HDCP Repeater fails. With this failure, the HDCP Transmitter abandons the authentication protocol with the HDCP Repeater. Authentication can be reattempted with the transmission of a new value An and the Aksv.

Ref-2C-1. HDCP port access

Reference	Requirement
State B0 in page 19	**State B0: Unauthenticated**. The HDCP Receiver is idle, awaiting the reception of *An* and *Aksv* from the HDCP Transmitter to trigger the authentication protocol.

Ref-2C-2. Reserved port/bit

Reference	Requirement
Table 2-2 in page 28 and 29	All bytes read as 0x00 Reserved zeros.

Ref-2C-3. KSV FIFO of Receiver

Reference	Requirement
KSV FIFO of Table 2-2 in page 29	All bytes read as 0x00 for HDCP Receivers that are not HDCP Repeaters (REPEATER == 0).

Ref-2C-4. HDMI_MODE bit

Reference	Requirement
HDMI_MODE of Table 2-4 in page 31	HDMI Mode. When set to one, the HDCP Receiver has transitioned from DVI Mode to HDMI Mode. This has occurred because the HDCP Receiver has detected HDMI bus conditions on the link. This bit must not be cleared when the HDCP Transmitter and HDCP Receiver are connected and both are operating in an active HDMI mode. This bit must be cleared upon power-up, reset, unplug or plug of an HDCP Transmitter or anytime that the HDCP Receiver has not seen at least one Data Island within 30 video frames.
3rd paragraph in page 33	Transition to HDMI protocol must then be initiated by the HDCP Transmitter (or downstream side of an HDCP Repeater) by the transmission of a Data Island period. The reception of a Data Island preamble followed by a Data Island Guard Band will transition the HDCP Receiver to HDMI mode. The successful transition to HDMI mode by the HDCP Receiver is indicated by setting Bstatus bit HDMI_MODE.

Ref-2C-5. REPEATER bit

Reference	Requirement
1st paragraph in Page11	The HDCP Transmitter executes the second part of the protocol only when the REPEATER bit is set, indicating that the attached HDCP Receiver is an HDCP Repeater.
Transition A6:A4. in page 18	The REPEATER bit is not set (the HDCP Receiver is not an HDCP Repeater).
Bcaps of Table 2-2 in page 29	Bit 6: REPEATER, HDCP Repeater capability. When set to one, this HDCP Receiver supports downstream connections as permitted by the Digital Content Protection LLC license. This bit does not change while the HDCP Receiver is active.

Ref-2C-6. Bksv

Reference	Requirement
Bksv of Table 2-2 in page 28	Valid KSVs contain 20 ones and 20 zeros, a characteristic that must be verified by HDCP Transmitters before encryption is enabled. This value must be available any time the HDCP Receiver's HDCP hardware is ready to operate.

Ref-2C-7. Bcaps: 1.1_FEATURE

Reference	Requirement
Bcaps of Table 2-2 in page 29	Bit 1: 1.1_FEATURES. When set to one, this HDCP Receiver supports Enhanced Encryption Status Signaling (EESS), Advance Cipher, and Enhanced Link Verification options. For the HDMI protocol, Enhanced Encryption Status Signaling (EESS) capability is assumed regardless of this bit setting. This bit does not change while the HDCP Receiver is active.

Ref-2C-8. R0' calculation

Reference	Requirement
3rd paragraph from the bottom in page 10	*R0*' must be available for the HDCP Transmitter to read within 100milliseconds from the time that the HDCP Transmitter finishes writing *Aksv* to the video receiver. The HDCP Transmitter must not read the *R0*' value sooner than 100ms after writing *Aksv*.
State B1 in page 20	State B1: Computations. In this state, the HDCP Receiver calculates the values Km', Ks', M0', and R0' using the HDCP Receiver's Device Private Keys and the received values of An and Aksv. The HDCP Receiver must complete the computations within 100 milliseconds and make R0' available to the HDCP Transmitter.

Ref-2C-9. Short read format

Reference	Requirement
2nd paragraph in page 32	In order to minimize the number of bits that must be transferred for the link integrity check, a second read format must be supported by all HDCP Receivers and by HDCP Transmitters that do not implement a hardware I2C master. This access, shown in Figure 2-13, has an implicit offset address equal to 0x08, the starting location for Ri'. The short read format may be uniquely differentiated from combined reads by tracking STOP conditions (P) on the bus. Short reads must be supported with auto-incrementing addresses.

Ref-2C-10. Update Ri'/Pj'

Reference	Requirement
State B3 in page 20	The Ri' value is updated when (i mod 128 == 0). The updated *Ri'* value must be available through the HDCP-protected Interface Port no more than 128 pixel clocks from the time that encryption enable is indicated for the next frame over the CTLx signals. Section 2.7 specifies encryption enable signaling. Also, if the HDCP Receiver indicates it is capable of the Enhanced Link Verification option, it will similarly make a new Pj available if (j mod 16 == 0) within 128 pixel clocks after it receives the first pixel of the frame.
Ri' of Table 2-2 in page 28	Link verification response. Upon completion of the authentication computations, this register contains the *R0* value. Following that, it is updated upon completion of HDCPBlockCipher if (i mod 128) == 0 It is recommended that HDCP Transmitters protect against errors in the I2C transmission by re-reading this value when unexpected values are received, though care must be taken to avoid missing legitimate mismatch conditions. This value must be available at all times between updates. *R0* must be available less than 100 ms after *Aksv* is received. Subsequent *Ri'* values must be available a maximum of 128 pixel clocks following the Encryption Enable detection (ENC_EN).
Pj' of Table 2-2 in page 28	Enhanced Link Verification Response. Updated upon receipt of first video pixel received when frame counter value (j mod 16) == 0. The value is the XOR of the decrypted byte on channel zero of the first video pixel with the least significant byte of Rj. Rj is derived from the output function in the same manner as Ri, but is captured every 16th counted frame (rather than every 128th counted frame).

Ref-2C-11. New Authentication in the unauthenticated state

Reference	Requirement
Transition B1:B1 in page 20	Should the HDCP Transmitter write the Aksv while the HDCP Receiver is in State B1, the HDCP Receiver abandons intermediate results and restarts the computations.

Ref-2C-12. New Authentication in the authenticated state

Reference	Requirement
Transition B2:B1 in page 20	A new authentication is forced any time the Aksv is written by the attached HDCP Transmitter.

Ref-3C-1. REPEATER bit

Reference	Requirement
1st paragraph in Page11	The HDCP Transmitter executes the second part of the protocol only when the REPEATER bit is set, indicating that the attached HDCP Receiver is an HDCP Repeater.
Bcaps of Table 2-2 in page 29	Bit 6: REPEATER, HDCP Repeater capability. When set to one, this HDCP Receiver supports downstream connections as permitted by the Digital Content Protection LLC license. This bit does not change while the HDCP Receiver is active.

Ref-3C-2. READY bit in the unauthenticated state

Reference	Requirement
State C0 in page 25	The READY status bit, in the HDCP-protected Interface Port, is de-asserted.
Bit 5: READY, KSV FIFO ready of Table 2-2 in page 29	See states C0 and C2.

Ref-3C-3. READY bit (Timing Requirements)

Reference	Requirement
Table 2–1. in page 12-13	From AKSV1 To AKSV2 Max Delay:100 ms Downstream propagation time. To latest *Aksv* transmission when more than one HDCP Receiver is attached.
Table 2–1. in page 12-13	From AKSV3 To RDY1 Max Delay:500 ms Upstream propagation time when no downstream HDCP Repeaters are attached.(no downstream KSV lists to process).
State C2 in page 24	The READY status bit is asserted.
Bit 5: READY, KSV FIFO ready of Table 2-2 in page 29	See states C0 and C2.

Ref-3C-4. MAX_DEVS_EXCEEDED

Reference	Requirement
MAX_DEVS_EXCEEDED of Table 2-4 in page 31	Topology error indicator. When set to one, more than 127 downstream devices, or the capacity of the KSV FIFO, are attached.

Ref-3C-5. MAX_CASCADE_EXCEEDED

Reference	Requirement
MAX_CASCADE_EXCEEDED of Table 2-4 in page 31	Topology error indicator. When set to one, more than seven levels of video repeater have been cascaded together.

Ref-3C-6. DEPTH

Reference	Requirement
DEPTH of Table 2-4 in page 31	Three-bit repeater cascade depth. This value gives the number of attached levels through the connection topology.

Ref-3C-7. DEVICE_COUNT

Reference	Requirement
DEVICE_COUNT of Table 2-4 in page 31	Total number of attached downstream devices. Always zero for HDCP Receivers. This count does not include the HDCP Repeater itself, but only downstream devices downstream from the HDCP Repeater.

Ref-3C-8. KSV List

Reference	Requirement
State C6 in page 26	A downstream HDCP-protected Interface Port that arrives in State F4 that has an HDCP Receiver that is not an HDCP Repeater attached, adds the *Bksv* of the attached HDCP Receiver to the list.

Ref-3C-9. Upstream V’

Reference	Requirement
State C6 in page 26	When the KSV list for all downstream HDCP Receivers has been assembled, the HDCP Repeater computes the upstream *V’*.

Ref-3C-10. HPD

Reference	Requirement
Last paragraph in page 20	The HDCP Repeater signals the detection of an active downstream HDCP Receiver to the upstream HDCP Transmitter by pulsing the Hot Plug Detect signal of the upstream HDCP-protected Interface Port. The pulse width must be greater than 100 ms.

Ref-3C-11. New Authentication in the unauthenticated state

Reference	Requirement
Transitions Any State:C0. in page 25	Re-authentication is forced any time the Aksv is written by the attached HDCP Transmitter, with a transition through the unauthenticated state.

State C1 in page 25	Should the HDCP Transmitter write the Aksv while the HDCP Repeater is in this state (State C1), the HDCP Repeater abandons intermediate results and restarts the computations.

Ref-3C-12. New Authentication in the authenticated state

Reference	Requirement
Transitions Any State:C0. in page 25	Re-authentication is forced any time the Aksv is written by the attached HDCP Transmitter, with a transition through the unauthenticated state.

Ref-3C-13. Timeout of KSV list READY

Reference	Requirement
State C5. in page 26	**State C5: Wait for Downstream**. The upstream (HDCP Receiver) state machine waits for all downstream HDCP-protected Interface Ports of the HDCP Repeater to enter either the unconnected (State P0), inactive (State F0), or the authenticated state (State F4).
Transition C5:C0. in page 26	Transition C5:C0. The watchdog timer expires before all downstream HDCP-protected Interface Ports enter the authenticated or unconnected state.

Ref-3C-14. READY bit (Timing Requirement)

Reference	Requirement
Table 2–1. in page 12-13	From AKSV1 To AKSV2 Max Delay:100 ms Downstream propagation time. To latest *Aksv* transmission when more than one HDCP Receiver is attached.
Table 2–1. in page 12-13	From AKSV3 To RDY1 Max Delay:500 ms Upstream propagation time when no downstream HDCP Repeaters are attached.(no downstream KSV lists to process).
Table 2–1. in page 12-13	From RDY1 To RDY2 Max Delay:500 ms Upstream propagation time when one or more HDCP Repeaters are attached. From latest downstream READY. (downstream KSV lists must be processed)
State C2 in page 25	The READY status bit is asserted.
Bit 5: READY, KSV FIFO ready of Table 2-2 in page 29	See states C0 and C2.

Ref-3C-15. KSV List

Reference	Requirement
State C6 in page 26	Downstream HDCP-protected Interface Ports that arrive in State F4 that have an HDCP Repeater attached will cause the KSV list read from the attached HDCP Repeater, plus the Bksv of the attached HDCP Repeater itself, to be added to the list.

Ref-3C-16. Verify Downstream V’

Reference	Requirement
State C6 in page 26	The HDCP Repeater must verify the integrity of the downstream HDCP Repeater’s list by computing V and checking this value against V' received from the attached HDCP Repeater. If V does not equal V', the downstream KSV list integrity check fails. A retry of the entire KSV FIFO read operation should be performed if V != V’.

Ref-3C-17. Assert MAX_DEVS_EXCEEDED by DEVICE_COUNT

Reference	Requirement
2nd paragraph in page 12	If the computed DEVICE_COUNT for an HDCP Repeater exceeds 127 or the maximum number of devices supported by the size of the KSV FIFO, the HDCP Repeater must assert the MAX_DEVS_EXCEEDED status bit.
State C6 in page 26	If the computed DEVICE_COUNT for an HDCP Repeater exceeds 127 or the size of the KSV_FIFO, the HDCP Repeater must assert the MAX_DEVS_EXCEEDED status bit.
2nd paragraph in page 12	If either MAX_CASCADED_EXCEEDED or MAX_DEVS_EXCEEDED status bits are set, the READY bit may be set by the repeater, or it may not set the READY bit and simply let the timeout occur in the HDCP Transmitter.

Ref-3C-18. Assert MAX_CASCADE_EXCEEDED by DEPTH

Reference	Requirement
2nd paragraph in page 12	If the computed DEPTH for an HDCP Repeater exceeds seven, the HDCP Repeater must assert the MAX_CASCADE_EXCEEDED status bit.
State C6 in page 26	If the computed DEPTH for an HDCP Repeater exceeds seven, the DCP Repeater must assert the MAX_CASCADE_EXCEEDED status bit.
2nd paragraph in page 12	If either MAX_CASCADED_EXCEEDED or MAX_DEVS_EXCEEDED status bits are set, the READY bit may be set by the repeater, or it may not set the READY bit and simply let the timeout occur in the HDCP Transmitter.

Ref-3C-19. Assert MAX_DEVS_EXCEEDED or MAX_CASCADE_EXCEEDED from Downstream

Reference	Requirement
2nd paragraph in page 12	When an HDCP Repeater receives a MAX_DEVS_EXCEEDED or a MAX_CASCADE_EXCEEDED status from a downstream HDCP Repeater, it is required to assert the corresponding status bits to the upstream HDCP Transmitter.
State C6 in page 27	When an HDCP Repeater receives a MAX_DEVS_EXCEEDED or a MAX_CASCADE_EXCEEDED status from a downstream HDCP Repeater, it is required to assert its corresponding upstream status bit.
2nd paragraph in page 12	If either MAX_CASCADED_EXCEEDED or MAX_DEVS_EXCEEDED status bits are set, the READY bit may be set by the repeater, or it may not set the READY bit and simply let the timeout occur in the HDCP Transmitter.