# DisplayPort-HDCP Specification Compliance Test Specification

Revision 1.0

10 September, 2007

## Notice



## 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.
3855 SW 153rd Drive
Beaverton, OR 97006 USA

Email: info@digital-cp.com

Web: www.digital-cp.com

## Revision History

10 September, 2007 – 1.0 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 1.3 – Amendment for DisplayPort Revision 1.0.

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

## Normative References

Digital Content Protection LLC, "HDCP Specification 1.3 – Amendment for DisplayPort", Revision 1.0

# Definitions

## Acronyms and Abbreviations

| | |
|---|---|
| DUT | Device Under Test |
| PCP | Product Capability Parameter |
| TE | Test Equipment |
| 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 | No error(s) were detected in the DUT's operation, although the DUT may have WARNING item(s) |
| FAIL | Error(s) were detected in the DUT's operation |

## Product Capability Parameter (PCP)

The PCP provides information about the behavior of the product under certain conditions and is requested from HDCP Adopters who wish to have their products tested. Information contained in the PCP is necessary to ensure accurate test reports.

### Source Capability

| | |
|---|---|
| Source_FieldCPIRQ_R0' | Does the source field CP_IRQ interrupt to read R0' during the first phase of authentication? (Y/N) |
| Source_FieldCPIRQ_READY | Does the source field CP_IRQ interrupt to read Bstatus:READY bit during the second phase of authentication? (Y/N) |

| | |
|---|---|
| Source_Out_OnlyRep | Does DUT output HDCP Content to a repeater that has no active downstream HDCP Devices connected to it (i.e. Repeater whose DEVICE_COUNT is zero is connected to the DUT's downstream port)? (Y/N) |
| Source_EncDisableBootstrapping | Does the DUT implement encryption disable bootstrapping when encryption is temporarily disabled? (Y/N) |

**Repeater Capability**

| | |
|---|---|
| Repeater_Out_OnlyRep | Does DUT output HDCP Content to a repeater that has no active downstream HDCP Devices connected to it (i.e. Repeater whose DEVICE_COUNT is zero is connected to the DUT's downstream port)? (Y/N) |
| Repeater_MultipleOutputs | Does DUT have more than one output port? (Y/N) |

# DisplayPort-HDCP Specification Compliance Test Specification

The DisplayPort-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

Transmitters (Source DUTs) are tested for compliance with the DisplayPort-HDCP Specification by connecting them to Receivers (Sink TEs) and Repeaters (Repeater TEs).

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

## 1A. With Receiver

In this test, a DisplayPort Receiver (TE) is connected to the Transmitter (DUT).

The operations of the DUT under 1, 2 and 4-lane Main Link configurations are tested.

# 1A-01. Regular Procedure: With Receiver

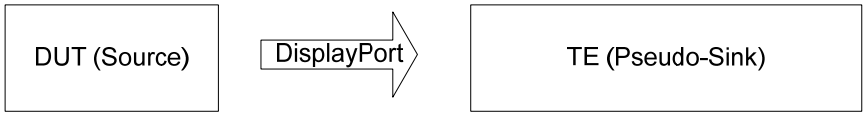
## Test Objective

Verify the Transmitter's implementation of the HDCP Protocol when an HDCP Receiver is connected to it

## Required Test Method

**<Connection Setup>**

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




**<Configuration of TE>**

| | |
|---|---|
| Initial Setting | |
| Bcaps:HDCP_CAPABLE | 1 |
| Bcaps:REPEATER | 0 |
| First Part of Authentication | |
| Bksv | Valid |
| R0' | Valid |
| Link Integrity Check | |
| Ciphers are synchronized and link integrity check is successful | |

**<Test Case>**

[Before Starting Authentication]

**(STEP 1A01-1)**

- ☐ TE asserts HPD

**(STEP 1A01-2)**

- ☐ DUT reads EDID and DPCD, determines that the attached sink device is a DisplayPort sink device and begins sending unencrypted video signal with HDCP Encryption disabled
  - ➢ If DUT begins the first part of authentication without sending unencrypted video signal, then FAIL (Ref-1A-1)
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-1)

**(STEP 1A01-3)**

- ☐ DUT reads the HDCP_CAPABLE bit in the TE's Bcaps register. This bit is set to 1

in the TE

- If DUT does not read the HDCP_CAPABLE bit before beginning the first part of authentication, then FAIL (Ref-1A-2)

[First Part of Authentication]

**(STEP 1A01-4)**

- ☐ During the first part of authentication, the DUT
  - Reads Bksv
  - Reads Bcaps (REPEATER)
  - Writes An
  - Writes Aksv

  Note: The DUT can initiate authentication by first reading the receiver's Bksv and Bcaps register before sending its An and Aksv. Alternatively, the DUT may first send its An and Aksv before reading Bksv and Bcaps
    - If DUT does not initiate the first part of authentication, then FAIL (Ref-1A-3)
    - If DUT writes Aksv before writing An, then FAIL (Ref-1A-3)
    - If Aksv is the same as facsimile Aksv, then FAIL

**(STEP 1A01-5)**

- ☐ TE calculates R0'
- ☐ If Source_FieldCPIRQ_R0' = Y, TE generates CP_IRQ interrupt and sets the R0'_AVAILABLE bit in the Bstatus register. DUT reads the R0'_AVAILABLE bit
  - If DUT does not read the R0'_AVAILABLE bit, then FAIL (Ref-1A-4)
- ☐ DUT reads R0'
  - If Source_FieldCPIRQ_R0' = N and DUT reads R0' sooner than 100ms after writing Aksv, then FAIL (Ref-1A-4)
  - If Source_FieldCPIRQ_R0' = N and DUT does not read R0' after 100ms after writing Aksv, then FAIL (Ref-1A-4)
  - If Source_FieldCPIRQ_R0' = Y and DUT does not read R0' after CP_IRQ was generated, then FAIL (Ref-1A-4)

**(STEP 1A01-6)**

- ☐ DUT enables HDCP Encryption after successful comparison of R0' against R0
  - If DUT does not enable HDCP Encryption, then FAIL (Ref-1A-1)
  - If DUT enables HDCP Encryption before reading R0', then FAIL (Ref-1A-1)

[Link Integrity Check]

**(STEP 1A01-7)**

- ☐ DUT transmits encrypted LINK_VERIFICATION_PATTERN one bit at a time. TE checks the correctness of the LINK_VERIFICATION_PATTERN within the first 48 VB-ID transmissions after encryption is enabled. If an incorrect

LINK_VERIFICATION_PATTERN is detected, the TE attempts re-authentication four additional times and performs Step 1A01-1 through Step 1A01-7

- If an incorrect LINK_VERIFICATION_PATTERN is detected within the first 48 VB-ID transmissions on all five attempts (it is assumed that the LINK_VERIFICATION_PATTERN transmitted by the DUT is incorrect), then FAIL (Ref-1A-5)
- If DUT does not restart authentication after the link integrity check failure, then FAIL (Ref-1A-5)

☐ If DUT completes the authentication and link integrity check process successfully, then PASS

## 1A-02. Regular Procedure: HPD After Writing Aksv

### Test Objective

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

### Required Test Method

**<Connection Setup>**

Same as '1A-01 Regular Procedure: With Receiver'

**<Configuration of TE>**

Same as '1A-01 Regular Procedure: With Receiver'

**<Test Case>**

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

[First Part of Authentication]

(STEP 1A01-4) and (STEP 1A01-5) described under [First Part of Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

- ☐ TE pulses HPD of the upstream HDCP-protected Interface Port to DUT
- ☐ DUT re-starts the first part of authentication
  - ➢ If the DUT does not re-start the first part of authentication and perform (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver', then FAIL (Ref-1A-6)
  - ➢ If DUT performs (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver' while TE is de-assserting HPD, then WARNING (Ref-1A-6)
  - ➢ If DUT enables HDCP Encryption and keeps encryption enabled, then FAIL (Ref-1A-6)
- ☐ If the DUT re-starts authentication on detecting HPD and performs (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver', then PASS

# 1A-03. Regular Procedure: HPD During Link Integrity Check Stage

## Test Objective

Verify that the Transmitter enters the No Receiver Attached state when HPD is de-asserted during the link integrity check stage and re-starts authentication after HPD is asserted by the downstream Receiver

## Required Test Method

### <Connection Setup>

Same as '1A-01 Regular Procedure: With Receiver'

### <Configuration of TE>

Same as '1A-01 Regular Procedure: With Receiver'

### <Test Case>

The steps described under [Before Starting Authentication] to [Link Integrity Check] in '1A-01 Regular Procedure: With Receiver' are performed

- TE pulses HPD of the upstream HDCP-protected Interface Port to DUT
- DUT re-starts the first part of authentication
  - If the DUT does not re-start the first part of authentication and perform (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver', then FAIL (Ref-1A-6)
  - If DUT performs (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver' while TE is de-assserting HPD, then WARNING (Ref-1A-6)
  - If DUT enables HDCP Encryption and keeps encryption enabled, then FAIL (Ref-1A-6)
- If the DUT re-starts authentication on detecting HPD and performs (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver', then PASS

# 1A-04. Irregular Procedure: (First Part of Authentication) Failure to Read Bcaps HDCP_CAPABLE Bit

## Test Objective

Verify that the Transmitter does not attempt to authenticate on failure to read Bcaps HDCP_CAPABLE bit

## Required Test Method

### <Connection Setup>

Same as '1A-01 Regular Procedure: With Receiver'

### <Configuration of TE>

Same as '1A-01 Regular Procedure: With Receiver' except for the following change

- Bcaps register is unavailable

### <Test Case>

[Before Starting Authentication]

- ☐ TE asserts HPD
- ☐ DUT reads EDID and DPCD, determines that the attached sink device is a DisplayPort sink device and begins sending unencrypted video signal with HDCP Encryption disabled
- ☐ DUT attempts to read the HDCP_CAPABLE bit in the TE's Bcaps register
  - ➢ If DUT does not attempt to read the Bcaps register after HPD is asserted, then FAIL (Ref-1A-2)
  - ➢ If DUT attempts to authenticate and performs (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver' after a failed Bcaps read attempt, then FAIL (Ref-1A-2)
- ☐ If DUT does not attempt to authenticate after a failed Bcaps read attempt, then PASS

# 1A-05. Irregular Procedure: (First Part of Authentication) Verify Bksv

## Test Objective

Verify that the Transmitter treats invalid Bksv read as an authentication failure

## Required Test Method

### <Connection Setup>

Same as '1A-01 Regular Procedure: With Receiver'

### <Configuration of TE>

Same as '1A-01 Regular Procedure: With Receiver' except for the following change

- Bksv does not contain 20 zeros and 20 ones

### <Test Case>

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

[First Part of Authentication]

- ☐ During the first part of authentication, the DUT
  - Reads Bksv
  - Reads Bcaps (REPEATER)
  - Writes An
  - Writes Aksv

  Note: The DUT can initiate authentication by first reading the receiver's Bksv and Bcaps register before sending its An and Aksv. Alternatively, the DUT may first send its An and Aksv before reading Bksv and Bcaps
    - If DUT aborts the authentication session without re-reading Bksv, then WARNING
    - If DUT reads R0' after reading invalid Bksv, then FAIL (Ref-1A-7)
    - If DUT enables HDCP Encryption and keeps encryption enabled after reading invalid Bksv, then FAIL (Ref-1A-7)
- ☐ If the DUT aborts the authentication session on reading an invalid Bksv, then PASS

Note: Authentication can be re-attempted with the transmission of new An and Aksv

# 1A-06. Irregular Procedure: (First Part of Authentication) Verify R0'

## Test Objective

Verify that the Transmitter treats invalid R0' read as an authentication failure

## Required Test Method

**<Connection Setup>**

Same as '1A-01 Regular Procedure: With Receiver'

**<Configuration of TE>**

Same as '1A-01 Regular Procedure: With Receiver' except for the following change

- R0' = invalid

**<Test Case>**

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

[First Part of Authentication]

(STEP 1A01-4) and (STEP 1A01-5) described under [First Part of Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

- ☐ TE calculates R0' incorrectly
- ☐ If Source_FieldCPIRQ_R0' = Y, TE generates CP_IRQ interrupt and sets the R0'_AVAILABLE bit in the Bstatus register. DUT reads the R0'_AVAILABLE bit
  - ➢ If DUT does not read the R0'_AVAILABLE bit, then FAIL (Ref-1A-4)
- ☐ DUT reads R0'
  - ➢ If Source_FieldCPIRQ_R0' = N and DUT reads R0' sooner than 100ms after writing Aksv, then FAIL (Ref-1A-4)
  - ➢ If Source_FieldCPIRQ_R0' = N and DUT does not read R0' after writing Aksv, then FAIL (Ref-1A-4)
  - ➢ If Source_FieldCPIRQ_R0' = Y and DUT does not read R0' after CP_IRQ was generated, then FAIL (Ref-1A-4)
- ☐ On detecting a mismatch between R0 and R0', the DUT reads R0' two additional times. The DUT does not enable HDCP Encryption
  - ➢ If DUT does not re-read R0' two additional times (for a total of three consecutive times), then FAIL (Ref-1A-8). R0' is confirmed as invalid after the three consecutive mismatches
  - ➢ If DUT continues to read R0' even after the three R0' reads, then FAIL (Ref-1A-8)
  - ➢ If DUT enables HDCP Encryption and keeps encryption enabled after reading

invalid R0', then FAIL (Ref-1A-8)

- DUT re-starts the first part of authentication
  - If DUT does not perform (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver' once again, then WARNING
- If the DUT treats invalid R0' read as an authentication failure, then PASS

# 1A-07. Irregular Procedure: (Link Integrity Check) Link Integrity Failure

## Test Objective

Verify that the Transmitter fields CP_IRQ and restarts authentication on a link integrity failure

## Required Test Method

**<Connection Setup>**

Same as '1A-01 Regular Procedure: With Receiver'

**<Configuration of TE>**

Same as '1A-01 Regular Procedure: With Receiver' except for the following change

- Link Integrity Check: A link integrity failure is detected at the TE

**<Test Case>**

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

[Link Integrity Check]

- DUT transmits encrypted LINK_VERIFICATION_PATTERN one bit at a time
- TE asserts the LINK_INTEGRITY_FAILURE bit in the Bstatus register and generates a CP_IRQ interrupt
- DUT reads the LINK_INTEGRITY_FAILURE bit in the Bstatus register on receiving CP_IRQ
  - If DUT does not read the LINK_INTEGRITY_FAILURE bit, then FAIL (Ref-1A-5)
- On seeing the LINK_INTEGRITY_FAILURE bit set, the DUT disables encryption and restarts authentication
  - If the DUT continues to keep encryption enabled after reading the LINK_INTEGRITY_FAILURE bit, then FAIL (Ref-1A-5)
  - If DUT does not restart authentication and perform (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver', then FAIL (Ref-1A-5)
- If the DUT fields CP_IRQ, disables encryption and re-starts authentication on a link integrity failure, then PASS

# 1A-08. Irregular Procedure: SRM

## Test Objective

Verify that the Transmitter, which has capability to playback a DVD disc, aborts authentication when connected to a receiver whose Bksv is listed in the SRM

## Required Test Method

**<Connection Setup>**

Same as '1A-01 Regular Procedure: With Receiver'. In addition, the DUT has the capability to playback a DVD disc. An SRM which includes the Bksv of the TE is recorded in a DVD test disc. The DUT is required to playback the test disc during the test.

**<Configuration of TE>**

Same as '1A-01 Regular Procedure: With Receiver'

**<Test Case>**

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

[First Part of Authentication]

- ☐ During the first part of authentication, the DUT
  - Reads Bksv
  - Reads Bcaps (REPEATER)
  - Writes An
  - Writes Aksv

  Note: The DUT can initiate authentication by first reading the receiver's Bksv and Bcaps register before sending its An and Aksv. Alternatively, the DUT may first send its An and Aksv before reading Bksv and Bcaps
    - ➢ If DUT keeps HDCP Encryption enabled 1 minute after reading the Bksv, then FAIL (Ref-1A-9)
- ☐ If DUT aborts authentication within 1 minute after reading Bksv, then PASS

Note: Authentication can be re-attempted with the transmission of new An and Aksv

# 1A-09. Regular Procedure: Encryption Disable Bootstrapping

## Test Objective

Verify that the Transmitter correctly implements encryption disable bootstrapping when encryption is temporarily disabled

## Required Test Method

This test case is implemented only if Source_EncDisableBootstrapping = Y

**<Connection Setup>**

Same as '1A-01 Regular Procedure: With Receiver'

**<Configuration of TE>**

Same as '1A-01 Regular Procedure: With Receiver'

**<Test Case>**

The steps described under [Before Starting Authentication] to [Link Integrity Check] in '1A-01 Regular Procedure: With Receiver' are performed

- ☐ The flow of HDCP Content is stopped causing encryption to be disabled by the DUT
- ☐ TE performs encryption disable bootstrapping
- ☐ The flow of HDCP Content is started causing encryption to be enabled by the DUT

The steps described under [Link Integrity Check] in '1A-01 Regular Procedure: With Receiver' are performed

  - ➢ If a link integrity failure is detected within the initial two frames that are transmitted after encryption is re-enabled, then FAIL (Ref-1A-10)
- ☐ If a link integrity failure is not detected within the initial two frames that are transmitted after encryption is re-enabled, then PASS

# 1B. With Repeater

In this test, an HDCP Repeater (TE) is connected to the Transmitter (DUT).

The operations of the DUT under 1, 2 and 4-lane Main Link configurations are tested.

# 1B-01. Regular procedure: With Repeater

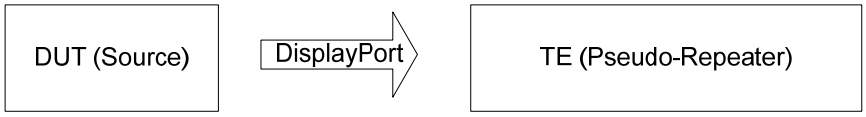
## Test Objective

Verify the Transmitter's implementation of the HDCP Protocol when an HDCP Repeater is connected to it

## Required Test Method

**<Connection Setup>**

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




**<Configuration of TE>**

| | |
|---|---|
| Initial Setting | |
| Bcaps:HDCP_CAPABLE | 1 |
| Bcaps:REPEATER | 1 |
| First Part of Authentication | |
| Bksv | Valid |
| R0' | Valid |
| Second Part of Authentication | |
| Binfo:DEPTH | 7 |
| Binfo:DEVICE_COUNT | 127 |
| Binfo:MAX_DEVS_EXCEEDED | 0 |
| Binfo:MAX_CASCADE_EXCEEDED | 0 |
| KSV FIFO | (DEVICE_COUNT * 5) bytes |
| Bstatus:READY | Assert before (DEPTH * 600)ms |
| V' | Valid |
| Link Integrity Check | |
| Ciphers are synchronized and link integrity check is successful | |

**<Test Case>**

The steps under [Before Starting Authentication] to [First Part of Authentication] described in '1A-01 Regular Procedure: With Receiver' are performed.

[Second Part of Authentication]

**(STEP 1B01-1)**

- ☐ TE sets Binfo:DEPTH and DEVICE_COUNT to the configured value, sets the KSVs

in the KSV FIFO and computes V'

- If Source_FieldCPIRQ_READY = Y, TE generates CP_IRQ interrupt and sets the READY bit in the Bstatus register
- If Source_FieldCPIRQ_READY = N, TE asserts Bstatus:READY bit at the configured period

**(STEP 1B01-2)**

- If Source_FieldCPIRQ_READY = Y, DUT reads the READY bit on receiving CP_IRQ
  - If DUT does not read READY bit, then FAIL (Ref-1B-1)
- If Source_FieldCPIRQ_READY = N, DUT polls downstream Bstatus:READY
  - If DUT does not read Bstatus:READY within five seconds after reading R0', then FAIL (Ref-1B-1)

**(STEP 1B01-3)**

- DUT reads the Binfo register
  - If DUT does not read the Binfo register, then FAIL (Ref-1B-2)

Two test cases must be performed when Source_Out_OnlyRep = Y

Case 1: DEVICE_COUNT and DEPTH are set to the configured value

- DUT reads the list of attached KSVs from the KSV FIFO in a single, auto-incrementing access. The size of KSVs to be read can be calculated from Binfo:DEVICE_COUNT
  - If DUT does not read the KSVs, then FAIL (Ref-1B-2)
  - If DUT does not read the correct size of KSVs, then FAIL (Ref-1B-2)

Case 2: DEVICE_COUNT is zero

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

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

**(STEP 1B01-4)**

- DUT reads V'.
  - If DUT does not read V' or DUT reads only a part of V', then FAIL (Ref-1B-2)

The steps under [Link Integrity Check] described in '1A-01 Regular Procedure: With Receiver' are performed

- If DUT completes the authentication and link integrity check process successfully, then PASS

## 1B-02. Irregular Procedure: Spurious CP_IRQ Interrupt

### Test Objective

Verify that the Transmitter ignores a spurious CP_IRQ interrupt

### Required Test Method

**<Connection Setup>**

Same as '1B-01 Regular procedure: With Repeater'

**<Configuration of TE>**

Same as '1B-01 Regular procedure: With Repeater'

**<Test Case>**

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

The steps described under [Second Part of Authentication] in '1B-01 Regular procedure: With Repeater' are performed

[Link Integrity Check]

- DUT transmits encrypted LINK_VERIFICATION_PATTERN one bit at a time
- TE generates a CP_IRQ interrupt without asserting any of the bits in the Bstatus register
  - If DUT does not read the LINK_INTEGRITY_FAILURE bit, then FAIL (Ref-1B-3)
  - If Source_FieldCPIRQ_READY = 'Y' and the DUT does not read the READY bit after reading the LINK_INTEGRITY_FAILURE bit, then FAIL (Ref-1B-3)
  - If Source_FieldCPIRQ_R0' = 'Y' and the DUT does not read the R0'_AVAILABLE bit after reading the READY bit, then FAIL (Ref-1B-3)
  - If the DUT aborts HDCP session or restarts authentication or reads R0', KSV FIFO, V' or Binfo as part of the CP_IRQ interrupt processing, then FAIL (Ref-1B-3)
- If the DUT ignores spurious CP_IRQ (i.e. DUT does not restart authentication, does not abort HDCP session, does not read R0', KSV FIFO, V' or Binfo), then PASS

# 1B-03. Regular Procedure: HPD After Reading R0'

## Test Objective

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

## Required Test Method

**<Connection Setup>**

Same as '1B-01 Regular procedure: With Repeater'

**<Configuration of TE>**

Same as '1B-01 Regular procedure: With Repeater'

**<Test Case>**

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

[Second Part of Authentication]

- TE pulses HPD of the upstream HDCP-protected Interface Port to DUT
- DUT re-starts the first part of authentication.
  - If the DUT does not re-start the first part of authentication and perform (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver', then FAIL (Ref-1A-6)
  - If DUT performs (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver' while TE is de-assserting HPD, then WARNING (Ref-1A-6)
  - If DUT enables HDCP Encryption and keeps encryption enabled, then FAIL (Ref-1A-6)
- If the DUT re-starts authentication on detecting HPD and performs (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver', then PASS

# 1B-04. Irregular Procedure: (Second Part of Authentication) Timeout of KSV List READY

## Test Objective

Verify that the Transmitter waits five seconds for the assertion of READY by the downstream Repeater

## Required Test Method

### <Connection Setup>

Same as '1B-01 Regular procedure: With Repeater'

### <Configuration of TE>

Same as '1B-01 Regular procedure: With Repeater' except for the following change

- Bstatus:READY bit is not asserted within 5 seconds

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

[Second Part of Authentication]

- ☐ TE does not assert Bstatus:READY
- ☐ If Source_FieldCPIRQ_READY = Y, DUT waits for CP_IRQ
- ☐ If Source_FieldCPIRQ_READY = N, DUT polls downstream Bstatus:READY
  - ➢ If DUT does not read Bstatus:READY within five seconds after reading R0', then FAIL (Ref-1B-1)
- ☐ DUT waits five seconds for the assertion of READY after reading R0'. DUT disables HDCP Encryption after expiration of the five second timer
  - ➢ If DUT disables HDCP Encryption before the expiration of the five second timer, then FAIL (Ref-1B-1)
  - ➢ If DUT does not disable HDCP Encryption after the expiration of the five second timer, then FAIL (Ref-1B-1)
- ☐ DUT re-starts the first part of authentication.
  - ➢ If DUT does not perform (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver' once again, then WARNING
- ☐ If the DUT waits five seconds for the assertion of READY, then PASS

## 1B-05. Irregular Procedure: (Second Part of Authentication) Verify V'

### Test Objective

Verify that the Transmitter treats invalid V' read as an authentication failure

### Required Test Method

**<Connection Setup>**

Same as '1B-01 Regular procedure: With Repeater'

**<Configuration of TE>**

Same as '1B-01 Regular procedure: With Repeater' except for the following change

- V' = invalid

**<Test Case>**

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

(STEP 1B01-1) to (STEP 1B01-3) described under [Second Part of Authentication] in '1B-01 Regular procedure: With Repeater' are performed

[Second Part of Authentication]

- ☐ TE calculates V' incorrectly
- ☐ DUT reads V'
- ☐ On detecting a mismatch between V and V', the DUT reads V' two additional times. The DUT disables HDCP Encryption on three consecutive mismatches
  - ➢ If DUT does not re-read V' two additional times (for a total of three consecutive times), then FAIL (Ref-1B-2)
  - ➢ If DUT continues to read V' even after the three V' reads, then FAIL (Ref-1B-2)
  - ➢ If DUT does not disable HDCP Encryption after reading invalid V', then FAIL (Ref-1B-2)
- ☐ DUT re-starts the first part of authentication.
  - ➢ If DUT does not perform (STEP 1A01-4) described in '1A-01 Regular Procedure: With Receiver' once again, then WARNING
- ☐ If the DUT treats invalid V' read as an authentication failure, then PASS

# 1B-06. Irregular Procedure: (Second Part of Authentication) MAX_DEVS_EXCEEDED

## Test Objective

Verify that the Transmitter aborts the authentication protocol when Binfo:MAX_DEVS_EXCEEDED bit is asserted by the downstream Repeater

## Required Test Method

### <Connection Setup>

Same as '1B-01 Regular procedure: With Repeater'

### <Configuration of TE>

Same as '1B-01 Regular procedure: With Repeater' except for the following change

- Binfo:MAX_DEVS_EXCEEDED = 1
- Binfo:DEVICE_COUNT = 0

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

[Second Part of Authentication]

- ☐ TE sets Binfo:MAX_DEVS_EXCEEDED bit to one and asserts Bstatus:READY bit at the configured period
- ☐ If Source_FieldCPIRQ_READY = Y, DUT reads the READY bit on receiving CP_IRQ
  - ➢ If DUT does not read READY bit on receiving CP_IRQ, then FAIL (Ref-1B-1)
- ☐ If Source_FieldCPIRQ_READY = N, DUT polls downstream Bstatus:READY
  - ➢ If DUT does not read Bstatus:READY within five seconds after reading R0', then FAIL (Ref-1B-1)
- ☐ DUT reads Binfo and disables HDCP Encryption on seeing the MAX_DEVS_EXCEEDED bit set
  - ➢ If DUT does not read Binfo MAX_DEVS_EXCEEDED bit, then FAIL (Ref-1B-4)
  - ➢ If DUT does not disable HDCP Encryption on reading Binfo:MAX_DEVS_EXCEEDED, then FAIL (Ref-1B-4)
- ☐ If DUT aborts the authentication protocol when Binfo:MAX_DEVS_EXCEEDED bit is set, then PASS

# 1B-07. Irregular Procedure: (Second Part of Authentication) MAX_CASCADE_EXCEEDED

## Test Objective

Verify that the Transmitter aborts the authentication protocol when Binfo:MAX_CASCADE_EXCEEDED bit is asserted by downstream Repeater

## Required Test Method

### <Connection Setup>

Same as '1B-01 Regular procedure: With Repeater'

### <Configuration of TE>

Same as '1B-01 Regular procedure: With Repeater' except for the following change

- Binfo:MAX_CASCADE_EXCEEDED = 1
- Binfo:DEPTH = 0

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '1A-01 Regular Procedure: With Receiver' are performed

[Second Part of Authentication]

- ☐ TE sets Binfo:MAX_CASCADE_EXCEEDED bit to one and asserts Bstatus:READY bit at the configured period
- ☐ If Source_FieldCPIRQ_READY = Y, DUT reads the READY bit on receiving CP_IRQ
  - ➢ If DUT does not read READY bit on receiving CP_IRQ, then FAIL (Ref-1B-1)
- ☐ If Source_FieldCPIRQ_READY = N, DUT polls downstream Bstatus:READY
  - ➢ If DUT does not read Bstatus:READY within five seconds after reading R0', then FAIL (Ref-1B-1)
- ☐ DUT reads Binfo and disables HDCP Encryption on seeing the MAX_CASCADE_EXCEEDED bit set
  - ➢ If DUT does not read Binfo MAX_CASCADE_EXCEEDED bit, then FAIL (Ref-1B-4)
  - ➢ If DUT does not disable HDCP Encryption on reading Binfo:MAX_CASCADE_EXCEEDED, then FAIL (Ref-1B-4)
- ☐ If DUT aborts the authentication protocol when Binfo:MAX_CASCADE_EXCEEDED bit is set, then PASS

# 2. Receiver Test

Receivers (Sink DUTs) are tested for compliance with the DisplayPort-HDCP Specification by connecting them to Transmitters (Source TEs).

## 2A. With Transmitter

In this test, a DisplayPort Transmitter (TE) is connected to the Receiver (DUT).

The operations of the DUT under 1, 2 and 4-lane Main Link configurations are tested.

# 2A-01. Regular Procedure: With Transmitter

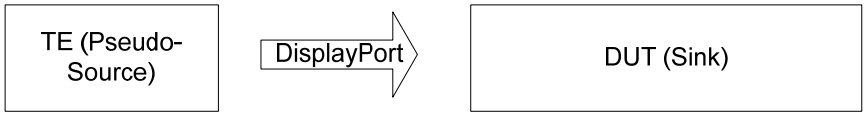
## Test Objective

Verify the Receiver's implementation of the HDCP Protocol when an HDCP Transmitter is connected to it

## Required Test Method

**<Connection Setup>**

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




**<Test Case>**

[Before Starting Authentication]

**(STEP 2A01-1)**

- ☐ TE detects HPD asserted by DUT.
  - ➢ If HPD is not asserted by DUT, then FAIL (Ref-1A-6)

**(STEP 2A01-2)**

- ☐ TE begins sending unencrypted video signal with HDCP Encryption disabled
- ☐ TE reads the HDCP_CAPABLE bit in the DUT's Bcaps register. This bit is set to 1 in the DUT
  - ➢ If Bcaps:HDCP_CAPABLE bit is zero in the DUT, then FAIL (Ref-1A-2)
  - ➢ If Bcaps:HDCP_CAPABLE bit is unavailable in the DUT, then FAIL (Ref-1A-2)

**(STEP 2A01-3)**

- ☐ TE reads all Reserved addresses. All bytes in the Reserved address space must be read as 0x00
  - ➢ If any byte in the Reserved address space is not zero, then FAIL (Ref-1B-7)

**(STEP 2A01-4)**

- ☐ TE reads fifteen bytes from the KSV FIFO in a single, auto-incrementing access
  - ➢ If all fifteen bytes are not read as 0x00, then FAIL (Ref-1B-8)
- ☐ TE begins the first part of authentication

[First Part of Authentication]

**(STEP 2A01-5)**

- ☐ During the first part of authentication, the TE
  - ● Reads Bksv
  - ● Reads Bcaps:REPEATER

- Writes An
- Writes Aksv
  - If Bcaps: REPEATER bit is one, then FAIL (Ref-1B-9)
  - If Bksv does not contain 20 zeros and 20 ones, then FAIL (Ref-1B-9)
  - If Bksv is the same as facsimile Bksv, then FAIL

**(STEP 2A01-6)**

- DUT calculates R0'
- TE reads R0' 100 ms after writing Aksv and compares R0' with R0. If there is a mismatch between R0 and R0', the TE reads R0' two additional times (for a total of three consecutive times)
  - If there are three consecutive mismatches between R0 and R0', then FAIL (Ref-1B-10)

**(STEP 2A01-7)**

- TE enables HDCP Encryption

[Link Integrity Check]

**(STEP 2A01-8)**

- TE transmits encrypted LINK_VERIFICATION_PATTERN one bit at a time
  - If a link integrity failure occurs, then FAIL (Ref-1A-5)
- If DUT completes the authentication and link integrity check process successfully, then PASS

# 2A-02. Irregular Procedure: (First Part of Authentication) New Authentication

## Test Objective

Verify that the Receiver re-authenticates when new An and Aksv are written by the Transmitter immediately after write of the first An and Aksv during the first part of authentication

## Required Test Method

**<Connection Setup>**

Same as '2A-01 Regular Procedure: With Transmitter'

**<Test Case>**

The steps described under [Before Starting Authentication] in '2A-01 Regular Procedure: With Transmitter' are performed

(STEP 2A01-5) described under [First Part of Authentication] in '2A-01 Regular Procedure: With Transmitter' is performed

- ☐ The TE once again
  - Reads Bksv
  - Reads Bcaps:REPEATER
  - Writes An
  - Writes Aksv
    - If Bcaps: REPEATER bit is one, then FAIL (Ref-1B-9)
    - If Bksv does not contain 20 zeros and 20 ones, then FAIL (Ref-1B-9)
    - If Bksv is the same as facsimile Bksv, then FAIL
- ☐ DUT calculates R0' using the new An
- ☐ TE reads R0' 100 ms after writing Aksv and compares R0' with R0. If there is a mismatch between R0 and R0', the TE reads R0' two additional times (for a total of three consecutive times)
  - If there are three consecutive mismatches between R0 and R0', then FAIL (Ref-1B-10)
- ☐ TE enables HDCP Encryption
- ☐ If DUT re-authenticates when a new An and Aksv is written by the TE immediately after write of the first An and Aksv, then PASS

## 2A-03. Irregular Procedure: (Link Integrity Check) New Authentication

### Test Objective

Verify that the Receiver re-authenticates when a new An and Aksv is written by the Transmitter during the link integrity check stage

### Required Test Method

**<Connection Setup>**

Same as '2A-01 Regular Procedure: With Transmitter'

**<Test Case>**

The steps described under [Before Starting Authentication] to [Link Integrity Check] in '2A-01 Regular Procedure: With Transmitter' are performed

- TE disables HDCP Encryption and sends unencrypted video signal
- The TE performs the first part of authentication once again by
  - Reading Bksv
  - Reading Bcaps:REPEATER
  - Writing An
  - Writing Aksv
    - If Bcaps: REPEATER bit is one, then FAIL (Ref-1B-9)
    - If Bksv does not contain 20 zeros and 20 ones, then FAIL (Ref-1B-9)
    - If Bksv is the same as facsimile Bksv, then FAIL
- DUT calculates R0' using the latest An
- TE reads R0' 100 ms after writing Aksv and compares R0' with R0. If there is a mismatch between R0 and R0', the TE reads R0' two additional times (for a total of three consecutive times)
  - If there are three consecutive mismatches between R0 and R0', then FAIL (Ref-1B-10)
- TE enables HDCP Encryption
- If DUT re-authenticates when a new An and Aksv is written by the TE during the link integrity check stage, then PASS

# 2A-04. Regular Procedure: Encryption Disable Bootstrapping

## Test Objective

Verify that the Receiver correctly implements encryption disable bootstrapping

## Required Test Method

### <Connection Setup>

Same as '2A-01 Regular Procedure: With Transmitter'

### <Test Case>

The steps described under [Before Starting Authentication] to [Link Integrity Check] in '2A-01 Regular Procedure: With Transmitter' are performed

- TE disables HDCP Encryption and sends unencrypted video signal
- TE performs encryption disable bootstrapping
- TE re-enables HDCP Encryption

The steps described under [Link Integrity Check] in '2A-01 Regular Procedure: With Transmitter' are performed

- If a link integrity failure occurs within the initial two frames that are transmitted after encryption is re-enabled, then FAIL (Ref-1A-10)

- If a link integrity failure does not occur within the initial two frames that are transmitted after encryption is re-enabled, then PASS

# 3. Repeater Test

Repeater DUTs are tested for compliance with the DisplayPort-HDCP Specification by connecting them to Transmitters (Source TEs), Receivers (Sink TEs) and Repeaters (Repeater TEs).

## 3A. Downstream Procedure With Receiver

In this test, a DisplayPort Receiver (TE) is connected to the downstream HDCP-protected Interface Port of the Repeater. A DisplayPort Transmitter is connected to the upstream HDCP-protected Interface Port of the Repeater.

The operations of the DUT under 1, 2 and 4-lane Main Link configurations are tested.

# 3A-01. Regular procedure: With Receiver

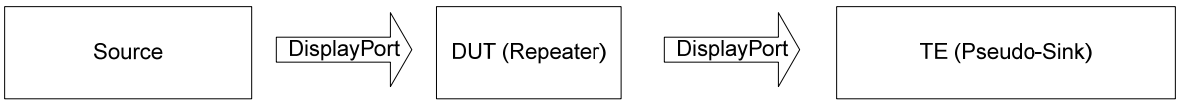
## Test Objective

Verify the Repeater's implementation of the HDCP Protocol when an HDCP Receiver is connected to the downstream Repeater port

## Required Test Method

### <Connection Setup>

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




Note: A device that has already passed the Transmitter test is used as the Source device

### <Configuration of TE>

Same as '1A-01 Regular Procedure: With Receiver'

### <Test Case>

Same as '1A-01 Regular Procedure: With Receiver'

# 3A-02. Irregular Procedure: (First Part of Authentication) Failure to Read Bcaps HDCP_CAPABLE Bit

## Test Objective

Verify that the Repeater does not attempt to authenticate on failure to read Bcaps HDCP_CAPABLE bit

## Required Test Method

### <Connection Setup>

Same as '3A-01 Regular procedure: With Receiver'

### <Configuration of TE>

Same as '1A-04 Irregular Procedure: (First Part of Authentication) Failure to Read Bcaps HDCP_CAPABLE Bit'

### <Test Case>

Same as '1A-04 Irregular Procedure: (First Part of Authentication) Failure to Read Bcaps HDCP_CAPABLE Bit'

## 3A-03. Irregular Procedure: (First Part of Authentication) Verify Bksv

### Test Objective

Verify that the Repeater treats invalid Bksv read as an authentication failure

### Required Test Method

**<Connection Setup>**

Same as '3A-01 Regular procedure: With Receiver'

**<Configuration of TE>**

Same as '1A-05 Irregular Procedure: (First Part of Authentication) Verify Bksv'

**<Test Case>**

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 the Repeater treats invalid R0' read as an authentication failure

### Required Test Method

**<Connection Setup>**

Same as '3A-01 Regular procedure: With Receiver'

**<Configuration of TE>**

Same as '1A-06 Irregular Procedure: (First Part of Authentication) Verify R0"

**<Test Case>**

Same as '1A-06 Irregular Procedure: (First Part of Authentication) Verify R0"

# 3B. Downstream Procedure with Repeater

In this test, a DisplayPort Repeater (TE) is connected to the downstream HDCP-protected Interface Port of the Repeater (DUT). A DisplayPort Transmitter is connected to the upstream HDCP-protected Interface Port of the Repeater.

The operations of the DUT under 1, 2 and 4-lane Main Link configurations are tested.

## 3B-01. Regular procedure: With Repeater

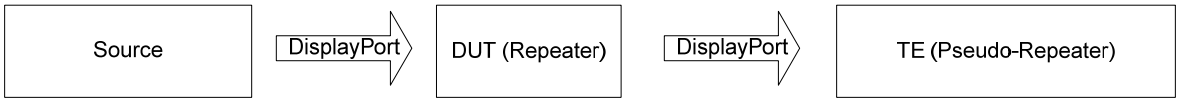
### Test Objective

Verify the Repeater's implementation of the HDCP Protocol when an HDCP Repeater is connected to the downstream Repeater port

### Required Test Method

**<Connection Setup>**

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




Note: A device that has already passed the Transmitter test is used as the Source device

**<Configuration of TE>**

Same as '1B-01 Regular procedure: With Repeater' except for the following change

- Binfo:DEVICE_COUNT = 126
- Binfo:DEPTH = 6

**<Test Case>**

Same as '1B-01 Regular procedure: With Repeater' except for the following change to (STEP 1B01-3)

**(STEP 1B01-3)**

- ☐ DUT reads the Binfo register
  - ➢ If DUT does not read the Binfo register, then FAIL (Ref-1B-2)

Two test cases must be performed when Repeater_Out_OnlyRep = Y

Case 1: DEVICE_COUNT and DEPTH are set to the configured value

- ☐ DUT reads the list of attached KSVs from the KSV FIFO in a single, auto-incrementing access. The size of KSVs to be read can be calculated from Binfo:DEVICE_COUNT
  - ➢ If DUT does not read the KSVs, then FAIL (Ref-1B-2)
  - ➢ If DUT does not read the correct size of KSVs, then FAIL (Ref-1B-2)
  - ➢ If DUT sets Binfo:MAX_DEVS_EXCEEDED or Binfo:MAX_CASCADE_EXCEEDED, then FAIL (Ref-3B-1)

Case 2: DEVICE_COUNT is zero

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

Note: If Repeater_Out_OnlyRep = N, only Case 1 needs to be performed

# 3B-02. Irregular Procedure: (Second Part of Authentication) Timeout of KSV List READY

## Test Objective

Verify that the Repeater (DUT) waits five seconds for the assertion of READY by the downstream Repeater (TE)

## Required Test Method

### <Connection Setup>

Same as '3B-01 Regular procedure: With Repeater'

### <Configuration of TE>

Same as '3B-01 Regular procedure: With Repeater' except for the following change

- Bstatus:READY bit is not asserted within 5 seconds

### <Test Case>

Same as '1B-04 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 the Repeater (DUT) treats invalid V' read from the downstream Repeater (TE) as an authentication failure

### Required Test Method

**<Connection Setup>**

Same as '3B-01 Regular procedure: With Repeater'

**<Configuration of TE>**

Same as '3B-01 Regular procedure: With Repeater' except for the following change

- V' = invalid

**<Test Case>**

Same as '1B-05 Irregular Procedure: (Second Part of Authentication) Verify V"

# 3B-04. Irregular Procedure: (Second Part of Authentication) MAX_DEVS_EXCEEDED

## Test Objective

Verify that the Repeater (DUT) aborts the authentication protocol when Binfo:MAX_DEVS_EXCEEDED bit is asserted by the downstream Repeater (TE)

## Required Test Method

### <Connection Setup>

Same as '3B-01 Regular procedure: With Repeater'

### <Configuration of TE>

Same as '3B-01 Regular procedure: With Repeater' except for the following change

- Binfo:MAX_DEVS_EXCEEDED = 1
- Binfo:DEVICE_COUNT = 128

### <Test Case>

Same as '1B-06 Irregular Procedure: (Second Part of Authentication) MAX_DEVS_EXCEEDED'

# 3B-05. Irregular Procedure: (Second Part of Authentication) MAX_CASCADE_EXCEEDED

## Test Objective

Verify that the Repeater (DUT) aborts the authentication protocol when Binfo:MAX_CASCADE_EXCEEDED bit is asserted by downstream Repeater (TE)

## Required Test Method

### <Connection Setup>

Same as '3B-01 Regular procedure: With Repeater'

### <Configuration of TE>

Same as '3B-01 Regular procedure: With Repeater' except for the following change

- Binfo:MAX_CASCADE_EXCEEDED = 1
- Binfo:DEPTH = 8

### <Test Case>

Same as '1B-07 Irregular Procedure: (Second Part of Authentication) MAX_CASCADE_EXCEEDED'

# 3C. Upstream Procedure with Transmitter

In this test, the DisplayPort Repeater is tested under the following two connection setups.

- A DisplayPort Transmitter (TE) is connected to the upstream HDCP-protected Interface Port and a DisplayPort Receiver is connected to the downstream port of the Repeater (DUT)
- A DisplayPort Transmitter (TE) is connected to the upstream HDCP-protected Interface Port and a DisplayPort Repeater is connected to the downstream port of the Repeater (DUT)

## ☐ Repeater (DUT) Connected to Transmitter (TE) and Receiver

In this test, a DisplayPort Transmitter (TE) is connected to the upstream HDCP-protected Interface Port of the Repeater (DUT). A DisplayPort Receiver is connected to the downstream HDCP-protected Interface Port of the Repeater (DUT).

The operations of the DUT under 1, 2 and 4-lane Main Link configurations are tested.

# 3C-01. Regular Procedure: Transmitter – DUT – Receiver

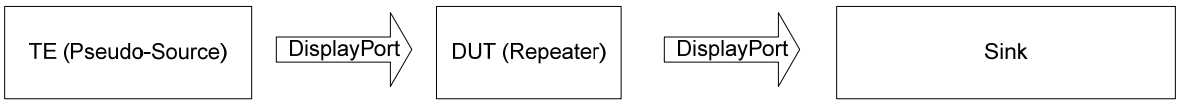
## Test Objective

Verify the Repeater's implementation of the HDCP Protocol when an HDCP Transmitter is connected to the upstream Repeater port and an HDCP Receiver is connected to the downstream Repeater port

## Required Test Method

**<Connection Setup>**

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




Note: A device that has already passed the Receiver test is used as the Sink device

**<Test Case>**

The steps under [Before Starting Authentication] described in '2A-01 Regular Procedure: With Transmitter' are performed except for (STEP 2A01-4). (STEP 2A01-4) is not performed in this test

The steps under [First Part Authentication] described in '2A-01 Regular Procedure: With Transmitter' are performed except for the following change to (STEP 2A01-5)

**(STEP 2A01-5)**

- ☐ During the first part of authentication, the TE
  - Reads Bksv
  - Reads Bcaps:REPEATER
  - Writes An
  - Writes Aksv
    - If Bcaps:REPEATER bit is not one, then FAIL (Ref-1B-9)
    - If Bstatus:READY bit is one, then FAIL (Ref-3C-1)
    - If Bksv does not contain 20 zeros and 20 ones, then FAIL (Ref-1B-9)
    - If Bksv is the same as facsimile Bksv, then FAIL

[Second Part of Authentication]

**(STEP 3C01-1)**

- ☐ DUT successfully completes the first part of authentication protocol with the downstream Sink

- TE waits for assertion of CP_IRQ interrupt
  - If DUT does not assert Bstatus:READY and generate CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-1B-1)

**(STEP 3C01-2)**

- TE reads Bstatus.
  - If Binfo:MAX_DEVS_EXCEEDED bit is one, then FAIL (Ref-3B-1)
  - If Binfo:MAX_CASCADE_EXCEEDED bit is one, then FAIL (Ref-3B-1)
  - If Binfo:DEPTH is not one, then FAIL (Ref-3C-2)
  - If Binfo:DEVICE_COUNT is not one, then FAIL (Ref-3C-2)

**(STEP 3C01-3)**

- TE reads five bytes of the KSV from the KSV FIFO in a single, auto-incrementing access
  - If DUT does not output Bksv of the attached Sink device from the KSV FIFO, then FAIL (Ref-3C-3)

**(STEP 3C01-4)**

- TE reads V'
  - If V' does not match TE's calculation of V, then FAIL (Ref-1B-2)

The steps described under [Link Integrity Check] in '2A-01 Regular Procedure: With Transmitter' are performed

- If DUT completes the authentication and link integrity check process successfully, then PASS

# 3C-02. Regular Procedure: HPD Propagation when an Active Receiver is Disconnected and Reconnected Downstream

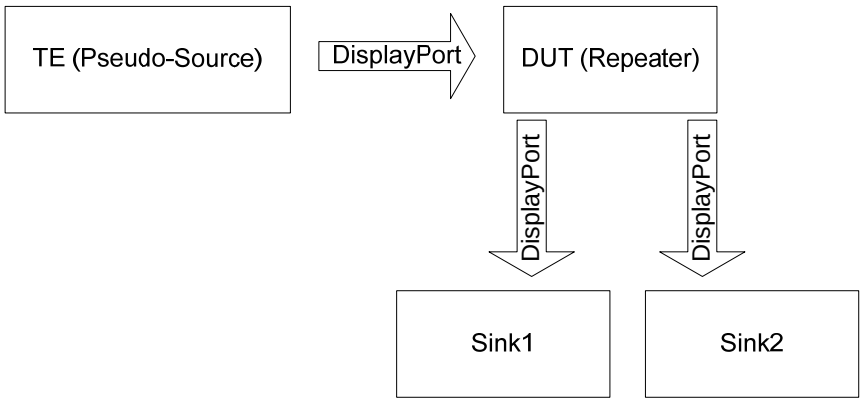
## Test Objective

Verify that the Repeater does not propagate HPD upstream when an active downstream Receiver is disconnected and reconnected when HDCP Content is flowing. Also verify that the Repeater propagates HPD upstream when the flow of HDCP Content stops

## Required Test Method

This test is performed if Repeater_MultipleOutputs = Y

**<Connection Setup>**




**<Test Case>**

The steps performed under [Before Starting Authentication] and [First Part of Authentication] are the same as those described in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' [Second Part of Authentication]

**(STEP 3C02-1)**

- ☐ DUT successfully completes the first part of authentication protocol with the downstream Sinks
- ☐ TE waits for assertion of CP_IRQ interrupt
  - ➢ If DUT does not assert Bstatus:READY and generate CP_IRQ interrupt within 5 seconds after reading R0', then FAIL (Ref-1B-1)

**(STEP 3C02-2)**

- ☐ TE reads Bstatus.
  - ➢ If Binfo:MAX_DEVS_EXCEEDED bit is one, then FAIL (Ref-3B-1)
  - ➢ If Binfo:MAX_CASCADE_EXCEEDED bit is one, then FAIL (Ref-3B-1)
  - ➢ If Binfo:DEPTH is not one, then FAIL (Ref-3C-2)
  - ➢ If Binfo:DEVICE_COUNT is not two, then FAIL (Ref-3C-2)

**(STEP 3C02-3)**

- TE reads ten bytes of the KSV from the KSV FIFO in a single, auto-incrementing access
  - If DUT does not output Bksvs of the attached Sink devices from the KSV FIFO, then FAIL (Ref-3C-3)

**(STEP 3C02-4)**

- TE reads V'
  - If V' does not match TE's calculation of V, then FAIL (Ref-1B-2)

The steps performed under [Link Integrity Check] are the same as those described in '3C-01 Regular Procedure: Transmitter – DUT – Receiver'

[Reconnect of Downstream Sink]

**(STEP 3C02-5)**

- Disconnect and reconnect Sink1 when HDCP Content is flowing
  - If the DUT pulses HPD upstream, then FAIL (Ref-3C-4)
- TE stops the flow of HDCP Content and disables encryption
  - If the DUT does not pulse HPD upstream once the flow of HDCP Content stops, then FAIL (Ref-3C-4)
- If the DUT does not propagate HPD upstream when an active downstream Sink is disconnected and reconnected when HDCP Content is flowing and propagates HPD upstream when the flow of HDCP Content stops, then PASS

# 3C-03. Regular Procedure: HPD Propagation when an Active Receiver is Disconnected Downstream

## Test Objective

Verify that the Repeater does not propagate HPD upstream when an active downstream Receiver is disconnected when HDCP Content is flowing. Also verify that the Repeater propagates HPD upstream when the flow of HDCP Content stops

## Required Test Method

This test is performed if Repeater_MultipleOutputs = Y

**<Connection Setup>**

Same as '3C-02 Regular Procedure: HPD Propagation when an Active Receiver is Disconnected and Reconnected Downstream'

**<Test Case>**

The steps performed under [Before Starting Authentication] to [Link Integrity Check] are the same as those described in '3C-02 Regular Procedure: HPD Propagation when an Active Receiver is Disconnected and Reconnected Downstream'

[Disconnect of Downstream Sink]

**(STEP 3C03-1)**

- Disconnect Sink1 when HDCP Content is flowing
  - If the DUT pulses HPD upstream, then FAIL (Ref-3C-4)
- TE stops the flow of HDCP Content and disables encryption
  - If the DUT does not pulse HPD upstream once the flow of HDCP Content stops, then FAIL (Ref-3C-4)
- If the DUT does not propagate HPD upstream when the active downstream Sink is disconnected when HDCP Content is flowing and propagates HPD upstream when the flow of HDCP Content stops, then PASS

# 3C-04. Regular Procedure: HPD Propagation when an Active Receiver is Connected Downstream

## Test Objective

Verify that the Repeater immediately propagates HPD upstream when an active Receiver is connected downstream when HDCP Content is flowing

## Required Test Method

This test is performed if Repeater_MultipleOutputs = Y

**<Connection Setup>**

Same as '3C-01 Regular Procedure: Transmitter – DUT – Receiver'

**<Test Case>**

The steps performed under [Before Starting Authentication] to [Link Integrity Check] are the same as those described in '3C-02 Regular Procedure: HPD Propagation when an Active Receiver is Disconnected and Reconnected Downstream'

[Connect Active Downstream Sink]

**(STEP 3C04-1)**

- Connect Sink2 when HDCP Content is flowing
  - If the DUT does not pulse HPD upstream, then FAIL (Ref-3C-5)
- If the DUT propagates HPD upstream when Sink2 is connected, then PASS

# 3C-05. Irregular Procedure: (First Part of Authentication) New Authentication

## Test Objective

Verify that the Repeater re-authenticates when new An and Aksv are written by the Transmitter immediately after write of the first An and Aksv during the first part of authentication

## Required Test Method

**<Connection Setup>**

Same as '3C-01 Regular Procedure: Transmitter – DUT – Receiver'

**<Test Case>**

The steps described under [Before Starting Authentication] in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' are performed

(STEP 2A01-5) described under [First Part of Authentication] in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' is performed

- ☐ The TE once again
  - Reads Bksv
  - Reads Bcaps:REPEATER
  - Writes An
  - Writes Aksv
    - If Bcaps: REPEATER bit is not one, then FAIL (Ref-1B-9)
    - If Bksv does not contain 20 zeros and 20 ones, then FAIL (Ref-1B-9)
    - If Bksv is the same as facsimile Bksv, then FAIL
- ☐ DUT calculates R0' using the new An
- ☐ TE reads R0' 100 ms after writing Aksv and compares R0' with R0. If there is a mismatch between R0 and R0', the TE reads R0' two additional times (for a total of three consecutive times)
  - If there are three consecutive mismatches between R0 and R0', then FAIL (Ref-1B-10)
- ☐ TE enables HDCP Encryption
- ☐ If DUT re-authenticates when a new An and Aksv is written by the TE immediately after write of the first An and Aksv, then PASS

# 3C-06. Irregular Procedure: (Second Part of Authentication) New Authentication

## Test Objective

Verify that the Repeater re-authenticates when new An and Aksv are written by the Transmitter during the second part of authentication

## Required Test Method

### <Connection Setup>

Same as '3C-01 Regular Procedure: Transmitter – DUT – Receiver'

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' are performed

(STEP 3C01-1) described under [Second Part of Authentication] in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' is performed

- ☐ TE disables HDCP Encryption and sends unencrypted video signal
- ☐ The TE performs the first part of authentication once again by
  - Reading Bksv
  - Reading Bcaps:REPEATER
  - Writing An
  - Writing Aksv
    - If Bcaps: REPEATER bit is not one, then FAIL (Ref-1B-9)
    - If Bksv does not contain 20 zeros and 20 ones, then FAIL (Ref-1B-9)
    - If Bksv is the same as facsimile Bksv, then FAIL
- ☐ DUT calculates R0' using the latest An
- ☐ TE reads R0' 100 ms after writing Aksv and compares R0' with R0. If there is a mismatch between R0 and R0', the TE reads R0' two additional times (for a total of three consecutive times)
  - If there are three consecutive mismatches between R0 and R0', then FAIL (Ref-1B-10)
- ☐ TE enables HDCP Encryption
- ☐ If DUT re-authenticates when a new An and Aksv is written by the TE during the second part of authentication, then PASS

# 3C-07. Irregular Procedure: (Link Integrity Check) New Authentication

## Test Objective

Verify that the Repeater re-authenticates when a new An and Aksv is written by the Transmitter during the link integrity check stage

## Required Test Method

**<Connection Setup>**

Same as '3C-01 Regular Procedure: Transmitter – DUT – Receiver'

**<Test Case>**

The steps described under [Before Starting Authentication] to [Link Integrity Check] in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' are performed

- ☐ TE disables HDCP Encryption and sends unencrypted video signal
- ☐ The TE performs the first part of authentication once again by
  - Reading Bksv
  - Reading Bcaps:REPEATER
  - Writing An
  - Writing Aksv
    - If Bcaps: REPEATER bit is not one, then FAIL (Ref-1B-9)
    - If Bksv does not contain 20 zeros and 20 ones, then FAIL (Ref-1B-9)
    - If Bksv is the same as facsimile Bksv, then FAIL
- ☐ DUT calculates R0' using the latest An
- ☐ TE reads R0' 100 ms after writing Aksv and compares R0' with R0. If there is a mismatch between R0 and R0', the TE reads R0' two additional times (for a total of three consecutive times)
  - If there are three consecutive mismatches between R0 and R0', then FAIL (Ref-1B-10)
- ☐ TE enables HDCP Encryption
- ☐ If DUT re-authenticates when a new An and Aksv is written by the TE during the link integrity check stage, then PASS

# 3C-08. Irregular procedure: (Second part of authentication) Verify Bksv

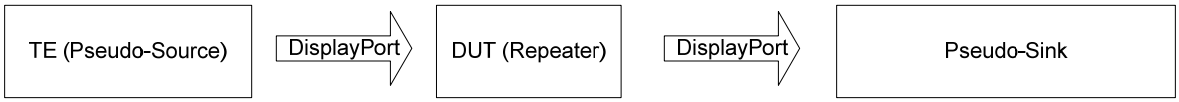
## Test Objective

Verify that the Repeater treats invalid Bksv read as an authentication failure and does not assert Bstatus:READY to the upstream transmitter

## 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




**<Configuration of Pseudo-Sink>**

| | |
|---|---|
| Initial Setting | |
| Bcaps:HDCP_CAPABLE | 1 |
| Bcaps:REPEATER | 0 |
| First Part of Authentication | |
| Bksv | Invalid (does not contain 20 ones and 20 zeroes) |
| R0' | Valid |
| Link Integrity Check | |
| Ciphers are synchronized and link integrity check is successful | |

**<Test Case>**

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' are performed

[Second Part of Authentication]

- Authentication of the DUT with the downstream Pseudo-Sink fails on reading invalid Bksv
- TE waits for assertion of CP_IRQ interrupt for a maximum permitted time of 5 seconds after R0' of the DUT has been read
  - If DUT asserts Bstatus:READY and generates CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-3C-6)

- If the DUT treats invalid Bksv read as an authentication failure and does not assert Bstatus:READY to the upstream TE, then PASS

# 3C-09. Irregular Procedure: (Second Part of Authentication) Verify R0'

## Test Objective

Verify that the Repeater treats invalid R0' read as an authentication failure and does not assert Bstatus:READY to the upstream transmitter

## Required Test Method

### <Connection Setup>

Same as '3C-08 Irregular procedure: (Second part of authentication) Verify Bksv'

### <Configuration of Pseudo-Sink>

| | |
|---|---|
| Initial Setting | |
| Bcaps:HDCP_CAPABLE | 1 |
| Bcaps:REPEATER | 0 |
| First Part of Authentication | |
| Bksv | Valid |
| R0' | Invalid |
| Link Integrity Check | |
| Ciphers are synchronized and link integrity check is successful | |

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' are performed

[Second Part of Authentication]

- Authentication of the DUT with the downstream Pseudo-Sink fails on reading invalid R0'
- TE waits for assertion of CP_IRQ interrupt for a maximum permitted time of 5 seconds after R0' of the DUT has been read
  - If DUT asserts Bstatus:READY and generates CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-3C-7)
- If the DUT treats invalid R0' read as an authentication failure and does not assert Bstatus:READY to the upstream TE, then PASS

## ☐ Repeater (DUT) Connected to Transmitter (TE) and Repeater

In this test, a DisplayPort Transmitter (TE) is connected to the upstream HDCP-protected Interface Port of the Repeater (DUT). A DisplayPort Repeater is connected to the downstream HDCP-protected Interface Port of the Repeater (DUT).

The operations of the DUT under 1, 2 and 4-lane Main Link configurations are tested.

# 3C-10. Regular Procedure: Transmitter – DUT – Repeater

## Test Objective

Verify the Repeater's (DUT) implementation of the HDCP Protocol when an HDCP Transmitter (TE) is connected to the upstream Repeater port and an HDCP Repeater is connected to the downstream Repeater port

## Required Test Method

**<Connection Setup>**

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


Note: Devices that have already passed the Repeater and Receiver tests are used as the Repeater and Sink devices respectively

**<Test Case>**

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' are performed

[Second Part of Authentication]

**(STEP 3C10-1)**

- DUT successfully completes the first part of authentication protocol with the downstream Repeater
- The downstream Repeater successfully completes the first part of authentication protocol with the downstream Sink device
- The downstream Repeater sets Binfo:DEPTH and Binfo:DEVICE_COUNT to one, sets the appropriate size of KSVs in the KSV FIFO, calculates V' and asserts Bstatus:READY bit
- DUT successfully completes the second part of authentication with the downstream Repeater
- TE waits for assertion of CP_IRQ interrupt
  - If DUT does not assert Bstatus:READY and generate CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-1B-1)

**(STEP 3C10-2)**

- TE reads READY bit on receiving CP_IRQ and then reads Binfo
  - If Binfo:MAX_DEVS_EXCEEDED bit is one, then FAIL (Ref-3B-1)
  - If Binfo:MAX_CASCADE_EXCEEDED bit is one, then FAIL (Ref-3B-1)
  - If Binfo:DEPTH is not two, then FAIL (Ref-3C-2)
  - If Binfo:DEVICE_COUNT is not two, then FAIL (Ref-3C-2)

**(STEP 3C10-3)**

- TE reads the KSVs from KSV FIFO in a single, auto-incrementing access
  - If the KSVs read from the KSV FIFO do not contain the downstream Repeater's Bksv and Sink's Bksv, then FAIL (Ref-3C-3)

**(STEP 3C10-4)**

- TE reads V'
  - If V' does not match TE's calculation of V, then FAIL (Ref-1B-2)

The steps described under [Link Integrity Check] in '3C-01 Regular Procedure: Transmitter – DUT – Receiver' are performed

- If DUT completes the authentication and link integrity check process successfully, then PASS

# 3C-11. Regular Procedure: HPD After Writing Aksv

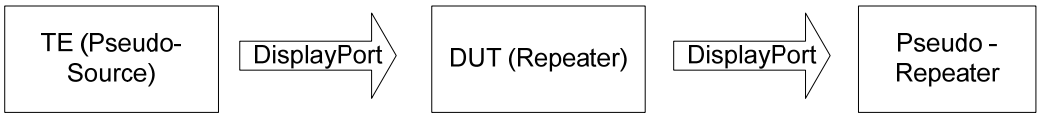
## Test Objective

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

## Required Test Method

**<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




**<Configuration of Pseudo-Repeater>**

| | |
|---|---|
| Initial Setting | |
| Bcaps:HDCP_CAPABLE | 1 |
| Bcaps:REPEATER | 1 |
| First Part of Authentication | |
| Bksv | Valid |
| R0' | Valid |
| Second Part of Authentication | |
| Binfo:DEPTH | 6 |
| Binfo:DEVICE_COUNT | 126 |
| Binfo:MAX_DEVS_EXCEEDED | 0 |
| Binfo:MAX_CASCADE_EXCEEDED | 0 |
| KSV FIFO | (DEVICE_COUNT * 5) bytes |
| Bstatus:READY | Assert before (DEPTH * 600)ms |
| V' | Valid |
| Link Integrity Check | |
| Ciphers are synchronized and link integrity check is successful | |

**<Test Case>**

The steps described under [Before Starting Authentication] in '3C-10 Regular Procedure: Transmitter – DUT – Repeater' are performed

(STEP 2A01-5) described under [First Part of Authentication] in '3C-10 Regular Procedure:

Transmitter – DUT – Repeater' is performed.

- Pseudo-Repeater pulses HPD of the upstream HDCP-protected Interface Port to DUT after Aksv is written by DUT.
- DUT pulses HPD of the upstream HDCP-protected Interface Port to TE
  - If DUT does not pulse HPD upstream, FAIL (Ref-3C-8)
- If DUT pulses HPD of the upstream HDCP-protected Interface Port when the attached downstream Repeater pulses HPD during the first part of authentication, then PASS

# 3C-12. Regular Procedure: HPD After Reading R0'

## Test Objective

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

## Required Test Method

### <Connection Setup>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv'

### <Configuration of Pseudo-Repeater>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv'

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-10 Regular Procedure: Transmitter – DUT – Repeater' are performed

- Pseudo-Repeater pulses HPD of the upstream HDCP-protected Interface Port to DUT after R0' is read by DUT.
- DUT pulses HPD of the upstream HDCP-protected Interface Port to TE
  - If DUT does not pulse HPD upstream, FAIL (Ref-3C-8)
- If DUT pulses HPD of the upstream HDCP-protected Interface Port when the attached downstream Repeater pulses HPD during the second part of authentication, then PASS

# 3C-13. Regular Procedure: HPD After Starting Third Part of Authentication

## Test Objective

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

## Required Test Method

**<Connection Setup>**

Same as '3C-11 Regular Procedure: HPD After Writing Aksv'

**<Configuration of Pseudo-Repeater>**

Same as '3C-11 Regular Procedure: HPD After Writing Aksv'

**<Test Case>**

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-10 Regular Procedure: Transmitter – DUT – Repeater' are performed

[Second Part of Authentication]

**(STEP 3C13-1)**

- ☐ DUT successfully completes the first part of authentication protocol with the Pseudo-Repeater
- ☐ Pseudo-Repeater sets Binfo:DEPTH and Binfo:DEVICE_COUNT to the configured value, sets the appropriate size of KSVs in the KSV FIFO, calculates V' and asserts Bstatus:READY bit
- ☐ DUT successfully completes the second part of authentication with the Pseudo-Repeater
- ☐ TE waits for assertion of CP_IRQ interrupt
  - ➢ If DUT does not assert Bstatus:READY and generate CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-1B-1)

**(STEP 3C13-2)**

- ☐ TE reads READY bit on receiving CP_IRQ and then reads Binfo
  - ➢ If Binfo:MAX_DEVS_EXCEEDED bit is one, then FAIL (Ref-3B-1)
  - ➢ If Binfo:MAX_CASCADE_EXCEEDED bit is one, then FAIL (Ref-3B-1)
  - ➢ If Binfo:DEPTH is not the configured value in the Pseudo-Repeater plus one, then FAIL (Ref-3C-2)
  - ➢ If Binfo:DEVICE_COUNT is not the configured value in the Pseudo-Repeater plus one, then FAIL (Ref-3C-2)

**(STEP 3C13-3)**

- TE reads the KSVs from KSV FIFO in a single, auto-incrementing access
  - If the KSVs read from the KSV FIFO do not contain the KSVs from the downstream Pseudo-Repeater's FIFO, then FAIL (Ref-3C-3)

**(STEP 3C13-4)**

- TE reads V'
  - If V' does not match TE's calculation of V, then FAIL (Ref-1B-2)

The steps described under [Link Integrity Check] in '3C-10 Regular Procedure: Transmitter – DUT – Repeater' are performed

- Pseudo-Repeater pulses HPD of the upstream HDCP-protected Interface Port to DUT
- DUT pulses HPD of the upstream HDCP-protected Interface Port to TE
  - If DUT does not pulse HPD upstream, FAIL (Ref-3C-8)
- If DUT pulses HPD of the upstream HDCP-protected Interface Port when the attached downstream Repeater pulses HPD during the third part of authentication, then PASS

# 3C-14. Irregular Procedure: (Second Part of Authentication) Verify V'

## Test Objective

Verify that Repeater (DUT) treats invalid V' read from the downstream Repeater as an authentication failure and does not assert Bstatus:READY bit to the upstream Transmitter

## Required Test Method

### <Connection Setup>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv'

### <Configuration of Pseudo-Repeater>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv' except for the following change

- V' = incorrectly computed value

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-10 Regular Procedure: Transmitter – DUT – Repeater' are performed

[Second Part of Authentication]

- ☐ Pseudo-Repeater calculates V' incorrectly.
- ☐ DUT reads invalid V' from Pseudo-Repeater and treats it as an authentication failure
- ☐ TE waits for the assertion of CP_IRQ interrupt
  - ➢ If DUT asserts Bstatus:READY and generates CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-3C-9)
- ☐ If the DUT treats invalid V' read from the downstream Repeater as an authentication failure and does not assert Bstatus:READY bit to the upstream Transmitter, then PASS

# 3C-15. Irregular Procedure: (Second Part of Authentication) DEVICE_COUNT

## Test Objective

Verify that the Repeater (DUT) asserts Binfo:MAX_DEVS_EXCEEDED bit if the computed DEVICE_COUNT for it exceeds 127

## Required Test Method

### <Connection Setup>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv'

### <Configuration of Pseudo-Repeater>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv' except for the following change

- Binfo:DEVICE_COUNT = 127

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-10 Regular Procedure: Transmitter – DUT – Repeater' are performed

[Second Part of Authentication]

- ☐ Pseudo-Repeater sets Binfo:DEPTH and Binfo:DEVICE_COUNT to the configured value and asserts Bstatus:READY bit at the configured period after its R0' has been read by the DUT
- ☐ TE waits for the assertion of CP_IRQ interrupt
  - ➢ If DUT does not asserts Bstatus:READY and generates CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-1B-1)
- ☐ TE reads READY bit on receiving CP_IRQ and then reads Binfo
  - ➢ If Binfo:MAX_DEVS_EXCEEDED bit is not one, then FAIL (Ref-3B-1)
- ☐ If the DUT asserts Binfo:MAX_DEVS_EXCEEDED bit if the computed DEVICE_COUNT for it exceeds 127, PASS

# 3C-16. Irregular Procedure: (Second Part of Authentication) DEPTH

## Test Objective

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

## Required Test Method

### <Connection Setup>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv'

### <Configuration of Pseudo-Repeater>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv' except for the following change

- Binfo:DEPTH = 7

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-10 Regular Procedure: Transmitter – DUT – Repeater' are performed

[Second Part of Authentication]

- ☐ Pseudo-Repeater sets Binfo:DEPTH and Binfo:DEVICE_COUNT to the configured value and asserts Bstatus:READY bit at the configured period after its R0' has been read by the DUT
- ☐ TE waits for the assertion of CP_IRQ interrupt
  - ➢ If DUT does not asserts Bstatus:READY and generates CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-1B-1)
- ☐ TE reads READY bit on receiving CP_IRQ and then reads Binfo
  - ➢ If Binfo:MAX_CASCADE_EXCEEDED bit is not one, then FAIL (Ref-3B-1)
- ☐ If the DUT asserts Binfo:MAX_CASCADE_EXCEEDED bit if the computed DEPTH for it exceeds seven, PASS

# 3C-17. Irregular Procedure: (Second Part of Authentication) MAX_DEVS_EXCEEDED

## Test Objective

Verify that the Repeater (DUT) asserts Binfo:MAX_DEVS_EXCEEDED bit when it receives a MAX_DEVS_EXCEEDED status from the downstream Pseudo-Repeater

## Required Test Method

### <Connection Setup>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv'

### <Configuration of Pseudo-Repeater>

Same as '3C-11 Regular Procedure: HPD After Writing Aksv' except for the following change

- Binfo:MAX_DEVS_EXCEEDED = 1

### <Test Case>

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-10 Regular Procedure: Transmitter – DUT – Repeater' are performed

[Second Part of Authentication]

- ☐ Pseudo-Repeater sets Binfo:MAX_DEVS_EXCEEDED bit to one and asserts Bstatus:READY bit at the configured period after its R0' has been read by the DUT
- ☐ TE waits for the assertion of CP_IRQ interrupt
  - ➢ If DUT does not asserts Bstatus:READY and generates CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-1B-1)
- ☐ TE reads READY bit on receiving CP_IRQ and then reads Binfo
  - ➢ If Binfo:MAX_DEVS_EXCEEDED bit is not one, then FAIL (Ref-3C-10)
- ☐ If the DUT asserts Binfo:MAX_DEVS_EXCEEDED bit when it receives a MAX_DEVS_EXCEEDED status from the downstream Pseudo-Repeater, PASS

# 3C-18. Irregular Procedure: (Second Part of Authentication) MAX_CASCADE_EXCEEDED

## Test Objective

Verify that the Repeater (DUT) asserts Binfo:MAX_CASCADE_EXCEEDED bit when it receives a MAX_CASCADE_EXCEEDED status from the downstream Pseudo-Repeater

## Required Test Method

**<Connection Setup>**

Same as '3C-11 Regular Procedure: HPD After Writing Aksv'

**<Configuration of Pseudo-Repeater>**

Same as '3C-11 Regular Procedure: HPD After Writing Aksv' except for the following change

- Binfo:MAX_CASCADE_EXCEEDED = 1

**<Test Case>**

The steps described under [Before Starting Authentication] to [First Part of Authentication] in '3C-10 Regular Procedure: Transmitter – DUT – Repeater' are performed

[Second Part of Authentication]

- ☐ Pseudo-Repeater sets Binfo:MAX_CASCADE_EXCEEDED bit to one and asserts Bstatus:READY bit at the configured period after its R0' has been read by the DUT
- ☐ TE waits for the assertion of CP_IRQ interrupt
  - ➢ If DUT does not asserts Bstatus:READY and generates CP_IRQ interrupt within 5 seconds after its R0' has been read by TE, then FAIL (Ref-1B-1)
- ☐ TE reads READY bit on receiving CP_IRQ and then reads Binfo
  - ➢ If Binfo:MAX_CASCADE_EXCEEDED bit is not one, then FAIL (Ref-3C-10)
- ☐ If the DUT asserts Binfo:MAX_CASCADE_EXCEEDED bit when it receives a MAX_CASCADE_EXCEEDED status from the downstream Pseudo-Repeater, PASS

# 4. Reference

Refer to the "HDCP Specification 1.3 – Amendment for DisplayPort, Revision 1.0" specification.

### Ref-1A-1.

| Reference | Requirement |
|---|---|
| State H2: Transmit DisplayPort, Page 17 | **State H2: Transmit DisplayPort.** In this state the transmitter should begin sending an unencrypted signal with HDCP Encryption disabled after the receiver is made active. In some types of transmitters, the transmitted signal can be a low value content or informative on-screen display, and it could be available immediately, while in other types of transmitters, there may be an additional step of making the connected receiver active before any content is displayed. If video signal is being transmitted by the HDCP Transmitter, this will ensure that a valid video signal is displayed to the user before and during authentication. |
| State A4: Authenticated, 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. |

### Ref-1A-2.

| Reference | Requirement |
|---|---|
| State A0: Determine Rx HDCP Capable, Page 17 | **State A0: Determine Rx HDCP Capable.** In this state, the transmitter reads the HDCP_CAPABLE bit in the receiver's *Bcaps* register. If this bit is set to 1, it indicates that the receiver is HDCP capable. Since state A0 is reached when content protection is desired by the Upstream Content Control Function, authentication must be started immediately by the transmitter. If video signal is being transmitted by the HDCP Transmitter, a valid video screen is displayed to the user with encryption disabled during this time. |

### Ref-1A-3.

| Reference | Requirement |
|---|---|
| Transition H2:A0, Page 17 | **Transition H2:A0.** If content protection is desired by the Upstream Content Control Function, then the HDCP Transmitter should immediately attempt to determine whether the receiver is HDCP capable. |

| | |
|---|---|
| Table 2-2, Page 28 | An: Session random number. This multi-byte value must be written by the HDCP Transmitter before the KSV is written. |

## Ref-1A-4.

| Reference | Requirement |
|---|---|
| Paragraph 5, Page 10 | The HDCP Transmitter can optionally choose to ignore the CP_IRQ interrupt and read $R_0'$ after 100ms. It must not read $R_0'$ sooner than 100ms in this case. |
| Paragraph 5, Page 10 | As soon as $R_0'$ is available, the HDCP Receiver must set the $R_0$'_AVAILABLE bit in the *Bstatus* register and generate CP_IRQ interrupt. If the HDCP Transmitter chooses to field the CP_IRQ interrupt, it must read the $R_0$'_AVAILABLE bit in the *Bstatus* register. If this bit is set, it must read $R_0'$. |

## Ref-1A-5.

| Reference | Requirement |
|---|---|
| Paragraph 2, Page 15 | A link integrity failure is determined to have occurred if three consecutive pattern mismatches at the receiver (in 16 * 3 = 48 VB-ID transmissions) are detected within two successive frame periods. Two successive frame periods are checked to enable recovery from simple transient synchronization errors (e.g., random bit error bursts). If a failure is detected within two successive frames then the receiver has experienced a non-recoverable loss of cipher synchronization. |
| Paragraph 3, Page 15 | On receiving a CP_IRQ interrupt, the HDCP Transmitter is required to read the *Bstatus* register to determine the cause of the interrupt.The HDCP Transmitter must disable HDCP Encryption at the CPSR/SR transmission boundary as soon as feasible after receiving the CP_IRQ interrupt from the HDCP Receiver if the LINK_INTEGRITY_FAILURE bit is set and must initiate re-authentication with the transmission of a new *An* and *Aksv*. |

## Ref-1A-6.

| Reference | Requirement |
|---|---|
| Transition Any State:H0, Page 17 | **Transition Any State:H0.** Reset conditions at the HDCP Transmitter or hot unplug of all HDCP capable receivers cause the HDCP Transmitter to enter the No Receiver Attached state. |
| Transition H0:H1, Page 17 | **Transition H0:H1.** The detection of a sink device (through Hot Plug Detect) indicates to the transmitter that a sink device is attached and that the EDID ROM and DPCD are available for reading. Reception of an HPD is sufficient indication to the transmitter that the receiver is available and active (ready to display received content). When the receiver is no longer active, the transmitter is notified through hot unplug. |
| State H2: Transmit DisplayPort, Page 17 | **State H2: Transmit DisplayPort.** In this state the transmitter should begin sending an unencrypted signal with HDCP Encryption disabled after the receiver is made active. In some types of transmitters, the transmitted signal can be a low value content or informative on-screen display, and it could be available immediately, while in other types of transmitters, there may be an additional step of making the connected |

| | |
|---|---|
| | receiver active before any content is displayed. If video signal is being transmitted by the HDCP Transmitter, this will ensure that a valid video signal is displayed to the user before and during authentication. |

## Ref-1A-7.

| Reference | Requirement |
|---|---|
| State A1:Exchange KSVs, Page 17 | **State A1:Exchange KSVs.** In this state, the HDCP Transmitter generates a 64-bit pseudo-random value (*An*) and writes that value to the HDCP Receiver. The transmitter also writes its KSV (*Aksv*). It reads the HDCP Receiver's KSV (*Bksv*) and the REPEATER status bit necessary for cipher initialization. Generation of *An* using the HDCP Cipher is described in Section 4.5. |
| Transition A1:H2, Page 17 | **Transition A1:H2.** Failure to read *Bksv* containing 20 zeros and 20 ones is considered a protocol failure and causes this state transition to State H2. |

## Ref-1A-8.

| Reference | Requirement |
|---|---|
| Paragraph 6, Page 10 | If authentication was successful, then $R_0'$ will be equal to $R_0$. If there is a mismatch between $R_0$ and $R_0'$, the HDCP Transmitter must re-read $R_0'$ for comparison against $R_0$ two additional times (for a total of three consecutive comparisons) in order to account for the possibility of link errors. The authentication protocol is deemed to have failed on three consecutive mismatches between $R_0$ and $R_0'$. Authentication can be reattempted with the transmission of new *An* and *Aksv* on failure of the first part of authentication. |
| Paragraph 2, Page 11 | The HDCP Transmitter enables HDCP Encryption when the first part of the authentication protocol successfully completes. |

## Ref-1A-9.

| Reference | Requirement |
|---|---|
| Paragraph 5, Page 13 | 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. |
| Paragraph 6, Page 11 | The top-level HDCP Transmitter must complete the second phase of authentication within 1 minute after the assertion of READY by the downstream HDCP Repeater. |

## Ref-1A-10.

| Reference | Requirement |
|---|---|
| Paragraph 2, Page 50 | Encryption disable bootstrapping must be implemented by HDCP Receivers on detection of an SR. In the case of HDCP Transmitters, encryption disable bootstrapping must not be implemented if encryption was disabled due to the detection of a hot plug, hot unplug, link errors (e.g. link integrity check failure) or any other event that causes the link to be unauthenticated. In all other cases where encryption is disabled while the link is still active and authenticated, encryption disable bootstrapping can be implemented by |

| | |
|---|---|
| | the HDCP Transmitter. |
| Paragraph 5, Page 50 | In both these cases, encryption disable bootstrapping operation enables HDCP Encryption to be applied seamlessly when it is re-enabled by the HDCP Transmitter without requiring any re-authentication. |
| Paragraph 2, Page 15 | A link integrity failure is determined to have occurred if three consecutive pattern mismatches at the receiver (in 16 * 3 = 48 VB-ID transmissions) are detected within two successive frame periods. Two successive frame periods are checked to enable recovery from simple transient synchronization errors (e.g., random bit error bursts). If a failure is detected within two successive frames then the receiver has experienced a non-recoverable loss of cipher synchronization. |

## Ref-1B-1.

| Reference | Requirement |
|---|---|
| Paragraph 1, Page 12 | The HDCP Transmitter, having determined that the REPEATER bit read earlier in the protocol is set, sets a five-second watchdog timer. It may either poll the HDCP Repeater's READY status bit or alternatively check the READY bit when a CP_IRQ interrupt is received. |
| Paragraph 2, Page 12 | If the asserted READY status is not received by the HDCP Transmitter within a maximum-permitted time of five seconds, authentication of the HDCP Repeater fails. |

## Ref-1B-2.

| Reference | Requirement |
|---|---|
| Paragraph 5, Page 11 | When constructing the byte stream for the SHA-1 input, the KSV list is in the same little-endian byte order in which it is transmitted over the link, *Binfo* is appended in little-endian order, and $M_0$ is also appended in little-endian order. When both the KSV list and *V'* are available, the HDCP Repeater asserts its READY status indicator and asserts the CP_IRQ interrupt. |
| Paragraph 2, Page 12 | When READY is set, the HDCP Transmitter reads the KSV list and *V'* from the HDCP Repeater. The HDCP Transmitter verifies the integrity of the KSV list by computing the SHA–1 hash value *V* and comparing this value to *V'*. If *V* is not equal to *V'*, the HDCP Transmitter must re-read the KSV list, *Binfo* and *V'* two additional times (for a total of three consecutive *V'* checks) to account for the possibility of link errors. The authentication protocol is aborted on three consecutive mismatches between *V* and *V'* and authentication can be reattempted with the transmission of new *An* and the *Aksv*. |
| Paragraph 4, Page 11 | The total length of the KSV list is five bytes times the total number of attached and active downstream HDCP Devices, including downstream HDCP Repeaters. |

## Ref-1B-3.

| Reference | Requirement |
|---|---|
| Paragraph 5, Page 30 | The HDCP Transmitter uses the following steps when processing HPD interrupts:<br>1. If CP_IRQ is not set, process the interrupt as specified in DisplayPort Specification |

| | |
|---|---|
| | and exit<br><br>2. Read *Bstatus* register<br><br>3. If LINK_INTEGRITY_FAILURE, abort HDCP session<br><br>4. If the transmitter is not relying on CP_IRQ for READY and $R_0'$ check, it can exit the interrupt service routine at this time<br><br>5. If (READY bit is set)<br><br>a. Read *Binfo* register<br><br>b. If MAX_DEVS_EXCEEDED, abort authentication<br><br>c. If MAX_CASCADE_EXCEEDED, abort authentication<br><br>d. Continue with the second part of authentication: process the KSV_FIFO, compute V and verify whether $V = V'$<br><br>6. If ($R_0$'_AVAILABLE bit is set)<br><br>a. Read $R_0'$<br><br>b. Verify whether $R_0 = R_0'$<br><br>7. Else ignore interrupt and continue HDCP session without aborting |

## Ref-1B-4.

| Reference | Requirement |
|---|---|
| State F7: Read KSV List, Page 25 | **State F7: Read KSV List**. The watchdog timer is cleared. The downstream 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. Additional status bits (MAX_CASCADE_EXCEEDED and MAX_DEVS_EXCEEDED) from the downstream HDCP Repeater are read and if asserted, cause the HDCP Repeater to also assert them upstream. |
| Transition F7:P2, Page 25 | **Transition F7:P2.** This transition is made if $V' != V$'. It is also made if either MAX_CASCADE_EXCEEDED or MAX_DEVS_EXCEEDED are asserted. |

### Ref-1B-5.

| Reference | Requirement |
|---|---|
| Transition H0:H1, Page 17 | **Transition H0:H1.** The detection of a sink device (through Hot Plug Detect) indicates to the transmitter that a sink device is attached and that the EDID ROM and DPCD are available for reading. Reception of an HPD is sufficient indication to the transmitter that the receiver is available and active (ready to display received content). When the receiver is no longer active, the transmitter is notified through hot unplug. |

### Ref-1B-6.

| Reference | Requirement |
|---|---|
| Table 2-2, Page 28 | Bcaps: Bit 0: HDCP_CAPABLE. When set to 1, indicates that the receiver is HDCP capable. This bit does not change while the HDCP Receiver is active. |
| State A0: Determine Rx HDCP Capable., Page 17 | **State A0: Determine Rx HDCP Capable.** In this state, the transmitter reads the HDCP_CAPABLE bit in the receiver's *Bcaps* register. If this bit is set to 1, it indicates that the receiver is HDCP capable. Since state A0 is reached when content protection is desired by the Upstream Content Control Function, authentication must be started immediately by the transmitter. If video signal is being transmitted by the HDCP Transmitter, a valid video screen is displayed to the user with encryption disabled during this time. |

### Ref-1B-7.

| Reference | Requirement |
|---|---|
| Table 2-2, Page 28 | Rsvd: All bytes read as 0x00 |

### Ref-1B-8.

| Reference | Requirement |
|---|---|
| Table 2-2, Page 28 | KSV FIFO: Key selection vector FIFO. Used to pull downstream KSVs from HDCP Repeaters using auto-incrementing access. All bytes read as 0x00 for HDCP Receivers that are not HDCP Repeaters (REPEATER == 0). |

### Ref-1B-9.

| Reference | Requirement |
|---|---|
| Table 2-2, Page 28 | Bksv: HDCP Receiver KSV. 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. |
| Table 2-2, Page | Bcaps: Bit 1: REPEATER, HDCP Repeater capability. When set to one, this HDCP Receiver supports |

| | |
|---|---|
| 28 | downstream connections as permitted by the Digital Content Protection LLC license. This bit does not change while the HDCP Receiver is active. |

### Ref-1B-10.

| Reference | Requirement |
|---|---|
| Paragraph 6, Page 10 | If authentication was successful, then $R_0'$ will be equal to $R_0$. If there is a mismatch between $R_0$ and $R_0'$, the HDCP Transmitter must re-read $R_0'$ for comparison against $R_0$ two additional times (for a total of three consecutive comparisons) in order to account for the possibility of link errors. The authentication protocol is deemed to have failed on three consecutive mismatches between $R_0$ and $R_0'$. |

### Ref-3B-1.

| Reference | Requirement |
|---|---|
| Paragraph 2, Page 13 | HDCP Repeaters must be capable of supporting DEVICE_COUNT values less than or equal to 127 and DEPTH values less than or equal to 7. If the computed DEVICE_COUNT for an HDCP Repeater exceeds 127, the HDCP Repeater must assert the MAX_DEVS_EXCEEDED status bit. If the computed DEPTH for an HDCP Repeater exceeds seven, the HDCP Repeater must assert the MAX_CASCADE_EXCEEDED status bit. |

### Ref-3C-1.

| Reference | Requirement |
|---|---|
| Table 2-3, Page 29 | READY: When set to one, this HDCP Repeater has built the list of attached KSVs and computed the verification value $V'$. This value must be reset by the HDCP Repeater as soon as *Binfo* has been read by the HDCP Transmitter. This value is always zero during the computation of $V'$. |

### Ref-3C-2.

| Reference | Requirement |
|---|---|
| Paragraph 3, Page 12 | An HDCP Repeater reports the topology status variables DEVICE_COUNT and DEPTH. The DEVICE_COUNT for an HDCP Repeater is equal to the total number of attached downstream HDCP Receivers and HDCP Repeaters. The value is calculated as the sum of the number of attached downstream HDCP Receivers and HDCP Repeaters plus the sum of the DEVICE_COUNT read from all attached HDCP Repeaters. The DEPTH status for an HDCP Repeater is equal to the maximum number of connection levels below any of the downstream HDCP-protected Interface Ports. The value is calculated as the maximum DEPTH reported from downstream HDCP Repeaters plus one (accounting for the attached downstream HDCP Repeater). |

### Ref-3C-3.

| Reference | Requirement |
|---|---|
| Paragraph 4, Page 11 | An HDCP-protected Interface Port with no active device attached adds nothing to the list. Also, the KSV of the HDCP Repeater itself at any level is not included in its own KSV list. An HDCP-protected Interface Port connected to an HDCP Receiver that is not an HDCP Repeater adds the *Bksv* of the attached HDCP Receiver to the list. HDCP-protected Interface Ports that have an HDCP Repeater attached add the KSV list read from the attached downstream HDCP Repeater, plus the *Bksv* of the attached downstream HDCP Repeater itself. |

### Ref-3C-4.

| Reference | Requirement |
|---|---|
| Paragraph 5, Page 21 | Unplug or re-connect of an active, authenticated HDCP Receiver attached to the downstream HDCP Repeater connection must not result in an HPD pulse to the upstream HDCP Transmitter when HDCP Content is flowing. The HPD pulse must be propagated to the upstream HDCP Transmitter once the flow of HDCP Content stops. |

### Ref-3C-5.

| Reference | Requirement |
|---|---|
| Paragraph 3, Page 21 | When an active HDCP Receiver is connected to a downstream HDCP Repeater connection that previously had no active downstream HDCP Receivers, the generated HPD must immediately be propagated to the upstream HDCP Transmitter. The pulse width must comply with the HPD Interrupt Event Signaling pulse width specification provided in the DisplayPort specification.. On detecting HPD, the upstream HDCP Transmitter must initiate re-authentication. When an HDCP Repeater receives an HPD propagated by the downstream HDCP Repeater, it must immediately propagate the HPD upstream. |

### Ref-3C-6.

| Reference | Requirement |
|---|---|
| Transition F1:P2, Page 24 | **Transition F1:P2.** Failure to read *Bksv* containing 20 zeros and 20 ones is considered a protocol failure and causes this state transition to State P2. |
| Transition C5:C0, Page 27 | **Transition C5:C0.** If any downstream HDCP-protected Interface Port should transition to the unauthenticated state, the upstream connection transitions to the unauthenticated state. This transition is also made when any downstream HDCP-protected Interface Ports becomes unauthenticated, or when the |

| | |
|---|---|
| | KSV list integrity check for a downstream HDCP Repeater fails. |

### Ref-3C-7.

| Reference | Requirement |
|---|---|
| Transition F3:P2, Page 24 | **Transition F3:P2.** The link integrity message $R_0'$ received from the HDCP Receiver does not match the value calculated by the downstream side. |
| Transition C5:C0, Page 27 | **Transition C5:C0.** If any downstream HDCP-protected Interface Port should transition to the unauthenticated state, the upstream connection transitions to the unauthenticated state. This transition is also made when any downstream HDCP-protected Interface Ports becomes unauthenticated, or when the KSV list integrity check for a downstream HDCP Repeater fails. |

### Ref-3C-8.

| Reference | Requirement |
|---|---|
| Paragraph 3, Page 21 | When an HDCP Repeater receives an HPD propagated by the downstream HDCP Repeater, it must immediately propagate the HPD upstream. |

### Ref-3C-9.

| Reference | Requirement |
|---|---|
| Transition F7:P2, Page 25 | **Transition F7:P2.** This transition is made if $V' != V'$. It is also made if either MAX_CASCADE_EXCEEDED or MAX_DEVS_EXCEEDED are asserted. |
| Transition C5:C0, Page 27 | **Transition C5:C0.** If any downstream HDCP-protected Interface Port should transition to the unauthenticated state, the upstream connection transitions to the unauthenticated state. This transition is also made when any downstream HDCP-protected Interface Ports becomes unauthenticated, or when the KSV list integrity check for a downstream HDCP Repeater fails. |

### Ref-3C-10.

| Reference | Requirement |
|---|---|
| Paragraph 2, Page 13 | HDCP Repeaters must be capable of supporting DEVICE_COUNT values less than or equal to 127 and DEPTH values less than or equal to 7. If the computed DEVICE_COUNT for an HDCP Repeater exceeds 127, the HDCP Repeater must assert the MAX_DEVS_EXCEEDED status bit. If the computed DEPTH for an HDCP Repeater exceeds seven, the HDCP Repeater must assert the MAX_CASCADE_EXCEEDED status bit. When an HDCP Repeater receives a MAX_DEVS_EXCEEDED or a |

| | |
|---|---|
| | MAX_CASCADE_EXCEEDED status from a downstream HDCP Repeater, it must assert the corresponding status bits to the upstream HDCP Transmitter, assert the READY bit and assert the CP_IRQ interrupt. |