High-bandwidth Digital Content Protection

Revision 2.3 on DisplayPort

Compliance Test Specification

Revision 1.1

4 March 2019

Notice

Acknowledgement

Teledyne Lecroy Inc. contributed to the development of the HDCP 2.2 CTS.

Intellectual Property

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

Contact Information

Digital Content Protection, LLC
C/O VTM Group
3855 SW 153rd Dr.
Beaverton, OR 97006

Email: info@digital-cp.com
Web: www.digital-cp.com

Revision History

25 August 2016 – Version 1.0. Adapting for DisplayPort.

4 November 2016 – Version 1.1 Updating as per the other contributors comments.

March 2019 - Version

Table of Contents

Introduction

Purpose and Scope

This document specifies test procedures that will be used to test devices for compliance with the HDCP2.3 DisplayPort Specification Revision 2.3.

Tests are specified for HDCP2.3 DP Source, HDCP2.3 DP Sink, and HDCP2.3 DP Repeater devices.

Normative References

Digital Content Protection, LLC, “High-bandwidth Digital Content Protection System – DisplayPort”, Revision 2.3.

Definitions

Acronyms and Abbreviations

CDF	Capabilities 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. The CDF will be maintained on the DCP Website (www.digital-cp.com/compliance).
DUT	Device Under Test
PCP	Product Capability Parameter
TE	Test Equipment
TRF	Test Results Form
HPD assert	Hot plug, CONNECTION_STATUS_NOTIFY and IRQ_HPD are collectively referred to as Receiver Connected Indication in this specification.
HPD de-assert	Hot Unplug is referred to as Receiver Disconnected Indication in this Specification.

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 Parameters (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_MultipleOutputs	Does the DUT support transmission of HDCP-protected content to more than one downstream device at the same time? (Y/N)
MST_Capable	Does the DUT support MST configuration. (Y/N)
SST	Does the DUT support SST configuration. (Y/N)
CP_IRQ	Does source support processing of CP_IRQ as per the HDCP2.2 spec. (Y/N)

Repeater Capability

Repeater_MultipleOutputs	Does the DUT support transmission of HDCP-protected content to more than one downstream device at the same time? (Y/N)

HDCP2.3 DisplayPort Compliance Test Specification

The HDCP DisplayPort 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 specification by connecting them to Receivers (TE pseudo-Sink) and Repeaters (TE pseudo-Repeater).

> Note: The source is required to play protected content; thus requiring HDCP to be enabled. The Content Stream to be played does not have any output restrictions (Type = 0).

1A. Downstream procedure with Receiver

In these tests, a DisplayPort HDCP2.3 Receiver (TE pseudo-Sink) 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 previously connected Receiver (With stored k_m)

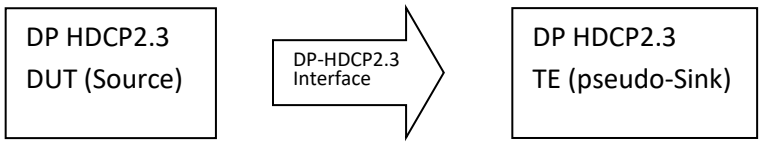
Test Objective

Verify the Transmitter's implementation of the HDCP protocol when an HDCP Receiver (that was previously connected) is attached.

Required Test Method

<Connection Setup>

☐ Connect TE (pseudo-Sink) to the downstream HDCP-protected Interface Port of DUT



Note: Upon initial connection, TE should authenticate and complete pairing with the DUT before proceeding

<Configuration of TE>

Message:	Parameter:	Value:
Authentication and Key Exchange		
AKE_Send_Cert	RxCaps:REPEATER	FALSE(0)
	RxCaps:HDCP_CAPABLE	TRUE(1)
	$cert_{rx}$	Valid (within 100ms timeout)
	r_{rx}	Valid (within 100ms timeout)
AKE_Send_H_prime	H'	Valid (within 200ms timeout)
Pairing		
AKE_Send_Pairing_Info	E_{kh}_k_m	Valid (used only for first time)
Locality Check		
LC_Send_L_prime	L'	Valid (within 16ms timeout)

<Test Case>

[Before Starting Authentication]

(STEP 1A-01-1)

- ☐ TE transmits Receiver Connected Indication(Hot plug, CONNECTION_STATUS_NOTIFY and IRQ_HPD) (Ref-1A-1)
- ☐ DUT Should read HDCP_CAPABLE bit RxCaps register. (Ref-1A-1)
- ☐ DUT may begin transmitting low value, unencrypted signal with HDCP Encryption disabled
  - ➢ If DUT begins the Authentication and Key Exchange without sending unencrypted video signal, then WARNING (Ref-1A-2)
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)

[Authentication and Key Exchange]

(STEP 1A-01-2)

- ☐ DUT initiates authentication by transmitting AKE_Init
  - ➢ If DUT does not write AKE_Init within 10 seconds of TE transmitting Receiver Connected Indication, then FAIL (Ref-1A-3)
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)

(STEP 1A-01-3)

- ☐ TE makes AKE_Send_Cert message available.
- ☐ If DUT attempts to read AKE_Send_Cert sooner than 100ms after writing the AKE_Init message, then WARNING(Ref-1A-3)
- ☐ DUT sends AKE_Stored_km message or AKE_No_Stored_Km message
  - ➢ If DUT sends AKE_No_Stored_km message,
    - NOTE (“DUT does not appear to implement persistent pairing for faster authentication”)
    - TE computes H’ and sends AKE_Send_H_Prime message with 1sec
    - TE generates Ekh(Km) and sends AKE_Send_pairing_Info message within 200ms.
  - ➢ If DUT sends AKE_Stored_km message
    - TE computes H’ and sets H’_AVAILABLE status bit in RxStatus register and creates the CP_IRQ interrupt to send AKE_Send_H_Prime message within 200ms timeout at the transmitter.

- If DUT does not send AKE_Stored_km or AKE_No_Stored_km message within 5 Seconds, then FAIL (Ref-1A-4)

[Locality Check]

(STEP 1A-01-4)

- ☐ DUT sends LC_Init message
  - If DUT does not send LC_Init message within 5seconds of AKE_Send_H_prime or AKE_Send_Pairing_Info message, then FAIL (Ref-1A-5)
- ☐ TE computes L' and sends LC_Send_L_prime message within the 16ms timeout to the transmitter.

[Session Key Exchange]

(STEP 1A-01-5)

- ☐ DUT sends SKE_Send_Eks message
  - If DUT does not send SKE_Send_Eks message within 5 seconds of transmission of LC_Send_L_prime message, then FAIL (Ref-1A-6)
- ☐ DUT writes Valid Type Value message
  - If DUT fails to write valid Type Value corresponding to the Content Stream, then FAIL.

(STEP 1A-01-6)

- ☐ DUT enables HDCP encryption 200ms after transmission of SKE_Send_Eks and TYPE message
  - If DUT enables HDCP encryption in less than 200ms, then FAIL (Ref-1A-6)
  - If DUT does not enable HDCP encryption between 200ms and 10 seconds of transmission of SKE_Send_Eks message, then FAIL (Ref-1A-6)

[Link Integrity Check]

(STEP 1A-01-7)

- ☐ DUT transmits encrypted LINK_VERIFICATION_PATTERN one bit at a time. TE checks the correctness of the LINK_VERIFICATION_PATTERN within the first 48VB-ID transmission

after encryption is enabled. If and incorrect LINK_VERIFICATION_PATTERN is detected, the TE attempts re-authentication four additional times and performs (STEP 1A-01-1) through (STEP 1A-01-7).

- If an incorrect LINK_VERIFICATION_PATTERN is detected within the first(16*3=48 VB-ID transmissions) 48 VB-ID transmission on all five attempts(It is assumed that the LINK_VERIFICATION_PATTERN transmitted by the DUT is incorrect), then FAIL (Ref-1A-11)
- If DUT does not restart authentication after the link integrity check failure is detected at TE and subsequently TE requesting re-authentication by setting LINK_INTEGRITY_FAILURE bit in RxStatus and generating CP_IRQ, then FAIL (Ref-1A-11)

☐ If DUT successfully completes the authentication and link integrity process and the image on TE looks valid as expected, then PASS.(Ref-1A-10)

1A-02. Regular Procedure – With newly connected Receiver (Without stored k_m)

Test Objective

Verify the Transmitter's implementation of the HDCP protocol when an HDCP Receiver (not previously connected) is attached.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)' except for following change:

- ☐ TE utilizes *Receiver ID* not paired to DUT and does not complete pairing

<Test Case>

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication and Key Exchange]

(STEP 1A-01-2) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

- ☐ TE sends AKE_Send_Cert message

(STEP 1A-02-1)

- ☐ DUT transmits AKE_No_Stored_km message
  - ➢ If DUT does not transmit AKE_No_Stored_km message within 5 seconds, then FAIL (Ref-1A-3)
  - ➢ If DUT sends AKE_Stored_km message, then FAIL (Ref-1A-3)
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
- ☐ If DUT sends AKE_No_Stored_km message, then PASS

  Note: TE does not complete pairing.

1A-03. Regular Procedure – Receiver disconnect after AKE_Init

Test Objective

Verify the Source DUT restarts authentication after the receiver is disconnected and reconnected following the write of AKE_Init with a new r_{tx} value.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

<Test Case>

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication and Key Exchange]

(STEP 1A-01-2) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

- ☐ TE transmits Receiver Disconnected Indication after AKE_Init message
- ☐ TE waits 500ms
- ☐ TE transmits Receiver Connected Indication

(STEP 1A-03-1)

- ☐ DUT restarts Authentication and Key Exchange
  - If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then FAIL (Ref-1A-7)
  - If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
- ☐ If DUT re-starts Authentication and Key Exchange on detecting Receiver Connected Indication and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS

1A-04. Regular Procedure – Receiver disconnect after k_m

Test Objective

Verify the Source DUT restarts authentication after the receiver is disconnected and reconnected following the exchange of k_m.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Test Case>

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication and Key Exchange]

(STEP 1A-01-2) and (STEP 1A-01-3) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

- ☐ TE transmits Receiver Disconnected Indication after AKE_Stored_km message
- ☐ TE waits for 500ms
- ☐ TE transmits Receiver Connected Indication (duration of disconnect is interface dependent)

(STEP 1A-04-1)

- ☐ DUT restarts Authentication and Key Exchange
  - ➢ If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then FAIL (Ref-1A-7)
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
- ☐ If DUT re-starts Authentication and Key Exchange on detecting Receiver Connected Indication and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS

1A-05. Regular Procedure – Receiver disconnect after locality check

Test Objective

Verify the Source DUT restarts authentication after the receiver is disconnected and reconnected after locality check is initiated.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Test Case>

The steps described under [Before Starting Authentication] and [Authentication and Key Exchange] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Locality Check]

(STEP 1A-01-4) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

- ☐ TE transmits Receiver Disconnected Indication after LC_Init message
- ☐ TE waits for 500ms
- ☐ TE transmits Receiver Connected Indication (duration of disconnect is interface dependent)

(STEP 1A-05-1)

- ☐ DUT restarts Authentication and Key Exchange
  - ➢ If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then FAIL (Ref-1A-7)
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
- ☐ If DUT re-starts Authentication and Key Exchange on detecting Receiver Connected Indication and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS

1A-06. Regular Procedure – Receiver disconnect after k_s

Test Case

Verify the Source DUT restarts authentication after the receiver is disconnected and reconnected following the exchange of k_s.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Test Case>

The steps described under [Before Starting Authentication] through [Locality Check] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Session Key Exchange]

(STEP 1A-01-5) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

- ☐ TE transmits Receiver Disconnected Indication, within 100ms after SKE_Send_Eks message
- ☐ TE waits for 500ms
- ☐ TE transmits Receiver Connected Indication (duration of disconnect is interface dependent)

(STEP 1A-06-1)

- ☐ DUT restarts Authentication and Key Exchange
  - If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then FAIL (Ref-1A-7)
  - If DUT has enabled HDCP Encryption, then it should disable it before starting authentication else FAIL (Ref-1A-2)

- ☐ If DUT re-starts Authentication and Key Exchange on detecting Receiver Connected Indication and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS

1A-07. Regular Procedure – Receiver sends REAUTH_REQ after Ks

Test Objective

Verify the Source DUT restarts authentication after the receiver sends REAUTH_REQ following the exchange of Ks.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Test Case>

The steps described under [Before Starting Authentication] through [Locality Check] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Session Key Exchange]

(STEP 1A-01-5) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

- ☐ TE Sends REAUTH_REQ by setting REAUTH_REQ bit of the RxStatus and causing CP_IRQ after SKE_Send_Eks message is read by TE

(STEP 1A-07-1)

- ☐ DUT restarts Authentication and Key Exchange
  - If DUT does not restart Authentication and Key Exchange and (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then FAIL (Ref-1A-7)
  - If DUT has enabled HDCP Encryption, then it should disable it before re-starting authentication else FAIL (Ref-1A-2)
- ☐ If DUT re-starts Authentication and Key Exchange on detecting REAUTH_REQ and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS

1A-08. Irregular Procedure – Verify Receiver Certificate

Test Objective

Verify the Source DUT considers it a failure of authentication when verification of Receiver Certificate fails.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m) except for following change:

- TE provides invalid value for $cert_{rx}$

<Test Case>

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication and Key Exchange]

(STEP 1A-01-2) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

(STEP 1A-08-1)

☐ TE provides invalid $cert_{rx}$ as part of AKE_Send_Cert

- If DUT enables HDCP Encryption, then FAIL (Ref-1A-1)
- If DUT transmits AKE_No_Stored_km or AKE_Stored_km, then FAIL (Ref-1A-8)

☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS

- If DUT does not attempt to restart authentication by performing (STEP 1A-01-2) after receipt of invalid $cert_{rx}$, then FAIL (Ref-1A-1)

1A-09. Irregular Procedure – SRM

Test Objective

Verify the Source DUT considers it a failure of authentication when the *Receiver ID* is on the revocation list.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Test Case>

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication and Key Exchange]

(STEP 1A-01-2) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

(STEP 1A-09-1)

- ☐ TE provides revoked *Receiver ID* as part of AKE_Send_Cert
  - If DUT enables HDCP Encryption, then FAIL (Ref-1A-1)
  - If DUT transmits AKE_No_Stored_km or AKE_Stored_km, then FAIL (Ref-1A-8)
- ☐ If DUT aborts Authentication and Key Exchange within 2 seconds of receipt of revoked *Receiver ID*, then PASS. Otherwise, FAIL(Ref-1A-2) (Ref-1A-8)

  Note: DUT may alternatively re-start Authentication and Key Exchange and perform (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', by transmitting a new r_{tx} as part of AKE_Init.

1A-10. Irregular Procedure – Invalid H'

Test Objective

Verify the Source DUT considers it a failure of authentication if the Receiver provides a value for H' that does not match H, or does not respond with H' in the allotted time.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

- Exception in Test Case 3 – TE utilizes unpaired *Receiver ID*.

<Test Case>

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication and Key Exchange]

(STEP 1A-01-2) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

Three test cases; all are performed

[Test Case 1 – Invalid H']

(STEP 1A-10-1)

- ☐ TE sends AKE_Send_Cert message (with previously paired *Receiver ID*)
- ☐ DUT sends AKE_Stored_km or AKE_No_Stored_Km message
  - ➢ If DUT does not send AKE_Stored_km or AKE_No_Stored_Km message, then FAIL (Ref-1A-4)
- ☐ TE provides invalid *H'* as part of AKE_Send_H_prime
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
  - ➢ If DUT transmits LC_Init, then FAIL (Ref-1A-8)

- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS
    - ➢ If DUT does not attempt to restart authentication by performing (STEP 1A-01-2) after receipt of invalid H' , then FAIL (Ref-1A-1)

[Test Case 2 – H'_AVAILABLE timeout after AKE_Stored_km]

(STEP 1A-10-2)

- ☐ TE sends AKE_Send_Cert message (with previously paired *Receiver ID*)
- ☐ DUT sends AKE_Stored_km message
    - ➢ If DUT send AKE_No_Stored_km message, then NOTE ("NOT JUDGED-DUT does not appear to implement persistent pairing for faster authentication"); TE ends test
    - ➢ If DUT does not send AKE_Stored_km message or AKE_No_Stored_km message, then FAIL (Ref-1A-4)
- ☐ TE does not respond with setting H'_AVAILABLE in RxStatus and not setting the CP_IRQ within the 200ms timeout at the transmitter
    - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-1)
    - ➢ If DUT transmits LC_Init, then FAIL (Ref-1A-8)
- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS
    - ➢ If DUT does not attempt to restart authentication by performing (STEP 1A-01-2) after expiry of the 200ms timeout , then FAIL (Ref-1A-1)

[Test Case 3 – H'_AVAILABLE timeout after AKE_No_Stored_km]

(STEP 1A-10-3)

- ☐ TE sends AKE_Send_Cert message (with unpaired *Receiver ID*)
- ☐ DUT sends AKE_No_Stored_km message
    - ➢ If DUT does not send AKE_No_Stored_km message, then FAIL (Ref-1A-3)

- ☐ TE does not respond with setting H'_AVAILABLE in RxStatus and not setting the CP_IRQ within the 1 second timeout at the transmitter
  - If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
  - If DUT transmits LC_Init, then FAIL (Ref-1A-8)
- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS
  - If DUT does not attempt to restart authentication by performing (STEP 1A-01-2) after expiry of the 1second timeout , then FAIL (Ref-1A-1)

1A-11. Irregular Procedure – Pairing Failure

Test Objective

Verify the Source DUT considers it a failure of authentication if the Receiver does not send AKE_Send_Pairing_Info.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m) except for following change:

- ☐ TE utilizes *Receiver ID* not paired to DUT

<Test Case>

The steps described under [Before Starting Authentication] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication and Key Exchange]

(STEP 1A-01-2) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

(STEP 1A-11-1)

- ☐ TE sends AKE_Send_Cert message
- ☐ DUT sends AKE_No_Stored_km message
  - If DUT does not transmit AKE_No_Stored_km message, then FAIL (Ref-1A-3)
  - If DUT sends AKE_Stored_km message, then FAIL (Ref-1A-3)
  - If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)

(STEP 1A-11-2)

- ☐ TE computes *H'* and respond with setting H'_AVAILABLE in RxStatus and setting the CP_IRQ within the 1 second and sends valid AKE_Send_H_prime message

(STEP 1A-11-3)

- ☐ TE does not send AKE_Send_Pairing_Info message within 200ms of the reception of AKE_Send_H_prime
- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS
  - ➢ If DUT does not attempt to restart authentication by performing (STEP 1A-01-2) after expiry of the 200ms timeout , then FAIL (Ref-1A-1)

Note: TE does not complete pairing.

1A-12. Irregular Procedure – Locality Failure

Test Objective

Verify the Source DUT considers it a failure of authentication if the Receiver provides a value for L' that does not match L.

Required Test Method

<Connection Setup>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)

<Test Case>

The steps described under [Before Starting Authentication] and [Authentication and Key Exchange] in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Locality Check]

(STEP 1A-01-4) described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' is performed.

(STEP 1A-12-1)

- ☐ TE provides invalid *L'* as part of LC_Send_L_prime message for first and subsequent 1023 re-attempts

(STEP 1A-12-2)

- ☐ DUT reattempts locality check with the transmission of LC_Init 1023 additional times (for a total max of 1024 attempts) with new Rn
  - ➢ If Rn is not different in each attempt then FAIL

(STEP 1A-12-3)

- ☐ DUT restarts Authentication and Key Exchange
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS

- If DUT does not attempt to restart authentication by performing (STEP 1A-01-2) after receipt of invalid L' , then FAIL (Ref-1A-1)

1B. Downstream procedure with Repeater

In these tests, an HDCP Repeater (TE pseudo-Repeater) is connected to the Transmitter (DUT).

1B-01. Regular Procedure – With Repeater

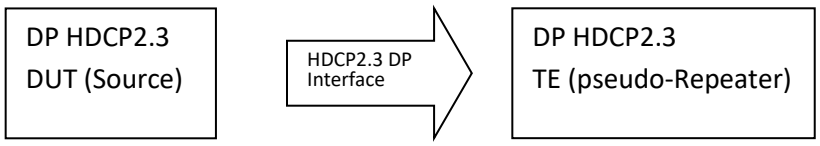
Test Objective

Verify the Source DUT works with a repeater attached under nominal circumstances

Required Test Method

<Connection Setup>

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



<Configuration of TE>

Message:	Parameter:	Value:
Authentication and Key Exchange		
AKE_Send_Cert	RxCaps:REPEATER	TRUE(1)
	RxCaps:HDCP_CAPABLE	TRUE(1)
	r_{rx}	Valid
	$cert_{rx}$	Valid
AKE_Send_H_prime	H’	Valid (within 200ms timeout)
Pairing		
AKE_Send_Pairing_Info	E_{kh}_k_m	Valid (used only for first time)
Locality Check		
LC_Send_L_prime	L’	Valid (within 16ms timeout)
Authentication with Repeater		
RepeaterAuth_Send_ReceiverID_List	RxInfo:MAX_DEVS_EXCEEDED	FALSE
	RxInfo:MAX_CASCADE_EXCEEDED	FALSE
	RxInfo:HDCP2_0_REPEATER_DOWNSTREAM	FALSE
	RxInfo:HDCP1_DEVICE_DOWNSTREAM	FALSE
	RxInfo:DEVICE_COUNT	31
	RxInfo:DEPTH	4
	Receiver ID List	(DEVICE_COUNT * 5) bytes
	V’	16 bytes, Valid (within 3 second timeout)
	seq_num_V	Valid

<Test Case>

The steps under [Before Starting Authentication] to [Session Key Exchange] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication with Repeaters]

(STEP 1B-01-1)

- ☐ TE clears MAX_CASCADE_EXCEEDED, MAX_DEVS_EXCEEDED, HDCP2_0_REPEATER_DOWNSTREAM, and HDCP1_DEVICE_DOWNSTREAM flags, sets DEPTH and DEVICE_COUNT to the configured values, initializes *seq_num_V* to 0, generates the ReceiverID_List and computes V'; in the RepeaterAuth_Send_ReceiverID_List message
- ☐ TE sets the READY bit in RxStatus and asserts CP_IRQ interrupt RepeaterAuth_Send_ReceiverID_List within the 3 second timeout of the receipt of SKE_Send_Eks
- ☐ DUT transmits 128 least significant bits of V to TE in the RepeaterAuth_Send_Ack message
  - ➢ If DUT does not transmit RepeaterAuth_Send_Ack message within 2 seconds from the time the READY status was set and the CP_IRQ interrupt was asserted by the TE, then FAIL (Ref-1B-2)
  - ➢ If 128 least significant bits of V transmitted by DUT do not match the 128 least significant bits of V' computed by the TE, then FAIL (Ref-1B-2)

(STEP 1B-01-2)

Note: The Transmitter DUT must complete Content Stream Management at least 100ms before transmitting the reference stream. Content Stream Management may be implemented in parallel with Authentication with Repeaters. The TE will support either method of Content Stream Management implemented in the DUT.

- ☐ DUT Transmits RepeaterAuth_Stream_Manage message
  - ➢ If DUT does not transmit RepeaterAuth_Stream_Manage message within 5sec of TE receiving SKE_Send_Eks, then FAIL
  - ➢ If DUT does not start with seq_num_M equal to 0, then FAIL
  - ➢ If K is not 31 then FAIL

- All StreamID values should be distinct else FAIL
- If Type is other than 0 or 1 then Warning

☐ TE responds with RepeaterAuth_Stream_Ready message within 100ms

(STEP 1B-01-3)

☐ DUT begins transmitting Content Stream within 10 seconds of completion of Content Stream Management and Authentication with Repeater

- If DUT begins transmitting Content Stream before 100ms after completion of Content Stream Management, then FAIL (Ref-1B-5)

☐ If DUT successfully completes the authentication process, then PASS

1B-02. Irregular Procedure – Timeout of Receiver ID list

Test Objective

Verify that the Source DUT considers it a failure of authentication if the downstream repeater does not respond with RepeaterAuth_Send_ReceiverID_List prior to expiration of watchdog timer.

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:

- ☐ TE does not respond with READY bit in RxStatus and does not send CP_IRQ interrupt within the 3 second timeout of the receipt of SKE_Send_Eks.

<Test Case>

The steps under [Before Starting Authentication] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication and Key Exchange]

(STEP 1B-02-1)

- ☐ TE does not respond with READY bit in RxStatus and does not send CP_IRQ interrupt within the 3 second timeout of the receipt of SKE_Send_Eks.
- ☐ DUT waits 3 seconds for the reception of Ready bit in RxStatus and CP_IRQ

(STEP 1B-02-2)

- ☐ DUT disables encryption, if enabled, after the expiration of the 3 second timer.
  - ➢ If DUT disables encryption, if enabled, before the timer expires, then FAIL(Ref-1B-2)
  - ➢ If DUT does not disable encryption, if enabled, after the timer expires, then FAIL (Ref-1B-2)
- ☐ If DUT restarts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – with previously connected Receiver (With stored km)', then PASS

- If DUT does not attempts to re-start authentication by performing (STEP 1A-01-2) after expiration of the 3 second timeout, then FAIL(Ref-1A-1)

1B-03. Irregular Procedure – Verify V'

Test Objective

Verify that the Source considers it a failure of authentication if the repeater provides a value for V' that does not match V.

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:

- ☐ TE provides an incorrect value for V'

<Test Case>

The steps under [Before Starting Authentication] to [Session Key Exchange] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

(STEP 1B-03-1)

- ☐ TE clears MAX_CASCADE_EXCEEDED, MAX_DEVS_EXCEEDED, HDCP2_0_REPEATER_DOWNSTREAM and HDCP1_DEVICE_DOWNSTREAM flags, sets DEPTH and DEVICE_COUNT to the configured value, initializes *seq_num_V* to 0, generates the ReceiverID_List and computed invalid V' in the RepeaterAuth_Send_ReceiverID_List message
- ☐ TE responds with READY bit in RxStatus and asserts CP_IRQ interrupt within the 3 second timeout of the receipt of SKE_Send_Eks

(STEP 1B-03-2)

- ☐ DUT disables encryption, if enabled, after receiving invalid V'
  - ➢ If DUT does not disables encryption, if enabled, then FAIL(Ref-1B-2)
- ☐ If DUT restarts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – with previously connected Receiver (With stored km), then PASS
  - ➢ If DUT does not attempts to re-start authentication by performing (STEP 1A-01-2) after receipt of invalid V', then FAIL(Ref-1B-2)

1B-04. Irregular Procedure – MAX_DEVS_EXCEEDED

Test Objective

Verify the Source DUT considers it a failure of authentication if the repeater sets the MAX_DEVS_EXCEEDED bit in the RepeaterAuth_Send_ReceiverID_List message.

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:

- ☐ TE sets MAX_DEVS_EXCEEDED to 'TRUE' in RepeaterAuth_Send_ReceiverID_List message

<Test Case>

The steps under [Before Starting Authentication] to [Session Key Exchange] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

(STEP 1B-04-1)

- ☐ TE clears MAX_CASCADE_EXCEEDED, DEPTH, DEVICE_COUNT, HDCP2_0_REPEATER_DOWNSTREAM, and HDCP1_DEVICE_DOWNSTREAM flags, sets MAX_DEVS_EXCEEDED to 'TRUE' and does not generate the ReceiverID_List, *seq_num_V* or compute V' in the RepeaterAuth_Send_ReceiverID_List message
- ☐ TE responds with READY bit in RxStatus and asserts CP_IRQ interrupt within the 3 second timeout of the receipt of SKE_Send_Eks

(STEP 1B-04-2)

- ☐ DUT disables HDCP encryption after receiving MAX_DEVS_EXCEEDED error
  - ➢ If DUT does not disable encryption after receiving MAX_DEVS_EXCEEDED error, then FAIL (Ref-1B-3)
- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored Km)', then PASS
  - ➢ If DUT does not attempt to re-start authentication by performing (STEP 1A-01-2) after receipt of the MAX_DEVS_EXCEEDED error, then FAIL (Ref-1A-1)

1B-05. Irregular Procedure – MAX_CASCADE_EXCEEDED

Test Objective

Verify the Source DUT considers it a failure of authentication if the repeater sets the MAX_CASCADE_EXCEEDED bit in the RepeaterAuth_Send_ReceiverID_List message.

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:

- ☐ TE sets MAX_CASCADE_EXCEEDED to 'TRUE' in RepeaterAuth_Send_ReceiverID_List message

<Test Case>

The steps under [Before Starting Authentication] to [Session Key Exchange] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

(STEP 1B-05-1)

- ☐ TE clears MAX_DEVS_EXCEEDED, DEPTH, DEVICE_COUNT, HDCP2_0_REPEATER_DOWNSTREAM, and HDCP1_DEVICE_DOWNSTREAM flags, sets MAX_CASCADE_EXCEEDED to 'TRUE' and does not generate the ReceiverID_List, *seq_num_V* or compute V' in the RepeaterAuth_Send_ReceiverID_List message
- ☐ TE responds with READY bit in RxStatus and asserts CP_IRQ interrupt within the 3 second timeout of the receipt of SKE_Send_Eks

(STEP 1B-05-2)

- ☐ DUT disables HDCP encryption, if enabled, after receiving MAX_CASCADE_EXCEEDED error
  - ➢ If DUT does not disable encryption, if enabled, after receiving MAX_CASCADE_EXCEEDED error, then FAIL (Ref-1B-3)
- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored Km)', then PASS
  - ➢ If DUT does not attempt to re-start authentication by performing (STEP 1A-01-2) after receipt of the MAX_CASCADE_EXCEEDED error, then FAIL (Ref-1A-1)

1B-06. Irregular Procedure – Incorrect *seq_num_V*

Test Objective

Verify the Source DUT considers it a failure of authentication if the repeater provides a non-zero value in *seq_num_V* in the first RepeaterAuth_Send_ReceiverID_List message after AKE_Init.

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:

- ☐ TE sets non-zero value for *seq_num_V* in first RepeaterAuth_Send_ReceiverID_List message

<Test Case>

The steps under [Before Starting Authentication] to [Session Key Exchange] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

(STEP 1B-06-1)

- ☐ TE clears MAX_CASCADE_EXCEEDED , MAX_DEVS_EXCEEDED, HDCP2_0_REPEATER_DOWNSTREAM and HDCP1_DEVICE_DOWNSTREAM flags, sets DEPTH, DEVICE_COUNT to configured value and set *seq_num_V* to a non-zero value and computes V' in the RepeaterAuth_Send_ReceiverID_List message
- ☐ TE responds with READY bit in RxStatus and asserts CP_IRQ interrupt within the 3 second timeout of the receipt of SKE_Send_Eks

(STEP 1B-06-2)

- ☐ DUT disables HDCP encryption, if enabled, after receiving a non-zero *seq_num_V*
  - ➢ If DUT does not disable encryption, if enabled, after receiving a non-zero *seq_num_V*, then FAIL (Ref-3C-7)
- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored Km)', then PASS
  - ➢ If DUT does not attempt to re-start authentication by performing (STEP 1A-01-2) after receipt of a non-zero *seq_num_V*, then FAIL (Ref-1B-4)

1B-07. Regular Procedure – Re-authentication on HPD

Test Objective

Verify the Source DUT initiates re-authentication when a HPD is received from 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 under [Before Starting Authentication] to [Session Key Exchange] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

The steps under [Authentication with Repeaters] described in '1B-01 Regular Procedure – With Repeater' are performed.

(STEP 1B-07-1)

- ☐ TE de-asserts HPD after RepeaterAuth_Send_ReceiverID_List message
- ☐ TE asserts HPD after 500ms

(STEP 1B-07-2)

- ☐ DUT restarts Authentication and Key Exchange
  - ➢ If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver(With stored Km)', then FAIL (Ref-1A-7)
- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored Km)', then PASS

1B-08. Regular Procedure – Re-authentication on REAUTH_REQ

Test Objective

Verify that the Source DUT initiates re-authentication when a REAUTH_REQ is received from 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 under [Before Starting Authentication] to [Session Key Exchange] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

The steps under [Authentication with Repeaters] described in '1B-01 Regular Procedure – With Repeater' are performed.

(STEP 1B-08-1)

- ☐ TE responds with REAUTH_REQ bit in RxStatus and asserts CP_IRQ interrupt

(STEP 1B-08-2)

- ☐ DUT disables HDCP encryption, if enabled, after receiving REAUTH request
  - ➢ If DUT does not disable encryption, if enabled, after receiving REAUTH request, then FAIL (Ref-1A-7)
- ☐ If DUT re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored Km)', then PASS
  - ➢ If DUT does not attempt to re-start authentication by performing (STEP 1A-01-2) after receipt of the REAUTH_REQ, then FAIL (Ref-1A-7)

1B-09. Irregular Procedure – Rollover of *seq_num_V*

Test Objective

Verify that the Source DUT initiates re-authentication when a rollover of *seq_num_V* is detected from 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 under [Before Starting Authentication] to [Session Key Exchange] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

The steps under [Authentication with Repeaters] described in '1B-01 Regular Procedure – With Repeater' are performed.

(STEP 1B-09-1)

- ☐ TE sets *seq_num_V* to 0xFFFFFFh
- ☐ TE simulates disconnect of an active downstream device by decrementing DEVICE_COUNT and adjusting the ReceiverID_List and transmits RepeaterAuth_Send_ReceiverID_List message
- ☐ DUT transmits 128 least significant bits to TE in the RepeaterAuth_Send_Ack message
  - ➢ If DUT does not transmit RepeaterAuth_Send_Ack message within one second, then FAIL (Ref-1B-2)
  - ➢ If 128 least significant bits transmitted by DUT do not match the 128 least significant bits computed by the TE, then FAIL (Ref-1B-2)

(STEP 1B-09-2)

- ☐ TE sets *seq_num_V* to 0x000000h (indicating rollover of *seq_num_V*)
- ☐ TE simulates connection of an active downstream device (same device that disconnected in STEP 1B-09-1) by incrementing DEVICE_COUNT and adjusting the ReceiverID_List and transmits RepeaterAuth_Send_ReceiverID_List message

(STEP 1B-09-3)

- ☐ DUT restarts Authentication and Key Exchange upon detecting rollover of *seq_num_V*
  - ➢ If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then FAIL (Ref-1A-7)
- ☐ If DUT detects the rollover of *seq_num_V* as a failure of authentication, and re-starts Authentication and Key Exchange and performs (STEP 1A-01-2) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS

1B-10. Irregular Procedure – Failure of Content Stream Management

Test Objective

Verify that the Source DUT re-attempts Content Stream Management following a failure of Content Stream Management.

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 following change:

- ☐ TE provides an incorrect value for *M'*

<Test Case>

The steps under [Before Starting Authentication] to [Session Key Exchange] described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)' are performed.

[Authentication with Repeaters]

(STEP 1B-01-1) described in '1B-01 Regular Procedure – With Repeater' is performed.

Two test cases; both are performed

[Test Case 1 – Incorrect value for *M'*]

(STEP 1B-10-1)

- ☐ DUT transmits RepeaterAuth_Stream_Manage message
  - ➢ If DUT does not transmit RepeaterAuth_Stream_Manage message within 5 sec, then FAIL (Ref-1B-5)
- ☐ TE responds with RepeaterAuth_Stream_Ready message within 100 ms with incorrect value for *M'*

(STEP 1B-10-2)

- ☐ DUT transmits RepeaterAuth_Stream_Manage message with incremented *seq_num_M*
  - ➢ If DUT transmits content stream without resending RepeaterAuth_Stream_Manage message, then FAIL (Ref-1B-5)

- If DUT transmits RepeaterAuth_Stream_Manage message with same *seq_num_M*, then FAIL (Ref-1B-5)
- If DUT does not transmit new RepeaterAuth_Stream_Manage message, then WARNING (Ref-1B-5)

☐ If DUT transmits new valid RepeaterAuth_Stream_Manage message after failure of *M'* comparison, then PASS

[Test Case 2 – Timeout of RepeaterAuth_Stream_Ready message]

(STEP 1B-10-3)

☐ DUT transmits RepeaterAuth_Stream_Manage message

- If DUT does not transmit RepeaterAuth_Stream_Manage message within 5 second, then FAIL (Ref-1B-5)

☐ TE does not respond with RepeaterAuth_Stream_Ready message within 100ms

(STEP 1B-10-4)

☐ DUT transmits RepeaterAuth_Stream_Manage message with incremented *seq_num_M*

- If DUT transmits content stream without resending RepeaterAuth_Stream_Manage message, then FAIL (Ref-1B-5)
- If DUT transmits RepeaterAuth_Stream_Manage message with same *seq_num_M*, then FAIL (Ref-1B-5)
- If DUT does not transmit new RepeaterAuth_Stream_Manage message, then WARNING (Ref-1B-5)

☐ If DUT transmits new RepeaterAuth_Stream_Manage message after timeout of 100ms timer, then PASS

2. Receiver Tests

Receivers (Sink DUTs) are tested for compliance with the DisplayPort-HDCP2.3 specification by connecting them to Transmitters (TE pseudo-Source).

2C. Upstream procedure with Transmitter

Receiver's upstream procedure with Transmitter is tested with an HDCP2.3-capable Transmitter. Make sure that the DUT maintains "connection" during the test, unless "receiver disconnect" is needed during the test.

In these tests, an HDCP2.3 Transmitter (TE Pseudo-source) is connected to the Receiver (DUT).

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

2C-01. Regular Procedure – With transmitter

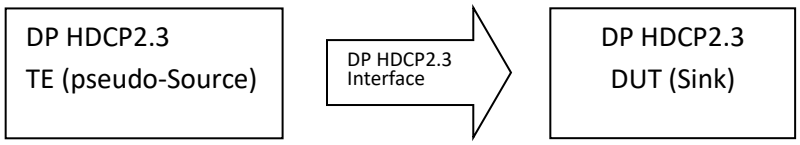
Test Objective

Verify the Receiver DUT works with an attached source under nominal circumstances.

Required Test Method

<Connection Setup>

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



<Test Case>

[Before Starting Authentication]

(STEP 2C-01-1)

☐ TE detects Receiver Connected Indication

- If DUT does not send Receiver Connected Indication (Hot plug, CONNECTION_STATUS_NOTIFY and IRQ_HPD) within 10 seconds, then FAIL (Ref-2C-1.)

[Authentication and Key Exchange]

(STEP 2C-01-2)

☐ TE begins sending unencrypted video signal with HDCP Encryption disabled

☐ TE transmits AKE_Init message

☐ DUT transmits AKE_Send_Cert message

- If DUT does not make AKE_Send_Cert message available within 100ms, then FAIL (Ref-2C-2)
- If AKE_Send_Cert:RxCaps:REPEATER is 'TRUE', then FAIL (Ref-2C-3)

Two test cases; both are performed

[Test Case 1 – Not previously connected *Receiver ID*]

(STEP 2C-01-3)

- ☐ TE transmits AKE_No_Stored_km message

(STEP 2C-01-4)

- ☐ DUT set H'_AVAILABLE status bit in RxStatus and generates CP_IRQ and makes AKE_Send_H_prime message available
  - If DUT does not set H'_AVAILABLE status bit in RxStatus and generates CP_IRQ and makes valid AKE_Send_H_prime message available within 1second from the time the transmitter finishes writing the AKE_No_Stored_Km, then FAIL (Ref-2C-2)
  - If *H'* is not equal to *H*, then FAIL (Ref-2C-2)

[Pairing]

(STEP 2C-01-5)

- ☐ DUT set PAIRING_AVAILABLE status bit in RxStatus and generates CP_IRQ and makes AKE_Send_Pairing_Info message available
  - If DUT does not set PAIRING_AVAILABLE status bit in RxStatus and generates CP_IRQ and makes AKE_Send_Pairing_Info message available within 200ms of AKE_Send_H_prime message, then FAIL (Ref-1A-4)

[Test Case 2 – Previously connected *Receiver ID*]

(STEP 2C-01-6)

- ☐ TE transmits AKE_Stored_km message

(STEP 2C-01-7)

- ☐ DUT set H'_AVAILABLE status bit in RxStatus and generates CP_IRQ and makes AKE_Send_H_prime message available
  - If DUT does not set H'_AVAILABLE status bit in RxStatus and generates CP_IRQ and makes valid AKE_Send_H_prime message available within 200ms from the time the transmitter finishes writing the AKE_Stored_Km, then FAIL (Ref-2C-2)
  - If *H'* is not equal to *H*, then FAIL (Ref-2C-2)
  - If DUT transmits AKE_Send_Pairing_Info, then FAIL (Ref-1A-4**Error! Reference source not found.**)

[Both test cases]

[Locality Check]

(STEP 2C-01-8)

- ☐ TE transmits LC_Init message
- ☐ DUT sends LC_Send_L_prime message
  - ➢ If DUT does not make valid LC_Send_L_prime message available within 16ms of transmission of LC_Init message, then FAIL(Ref-2C-4)
  - ➢ If L' does not match L, then FAIL (Ref-2C-4)

[Session Key Exchange]

(STEP 2C-01-9)

- ☐ TE transmits SKE_Send_Eks and Type message
- ☐ TE enables HDCP Encryption 200ms after transmitting SKE_Send_Eks and Type message
- ☐ TE transmits visible test pattern to DUT
- ☐ If DUT completes the authentication process and test pattern is viewed successfully, then PASS

2C-02. Irregular Procedure – New Authentication after AKE_Init

Test Objective

Verify the Receiver DUT restarts authentication when a new AKE_Init and r_{tx} is transmitted right after the transmission of AKE_Init in the unauthenticated state.

Required Test Method

<Connection Setup>

Same as '2C-01 Regular Procedure – With Transmitter'

<Test Case>

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

[Authentication and Key Exchange]

(STEP 2C-01-1) described in '2C-01 Regular Procedure – With Transmitter' is performed.

(STEP 2C-02-1)

☐ TE transmits AKE_Init message

(STEP 2C-02-2)

☐ DUT transmits AKE_Send_Cert message

- If DUT does not transmit AKE_Send_Cert message, then FAIL (Ref-2C-2)
- If AKE_Send_Cert:REPEATER is 'TRUE', then FAIL (Ref-2C-3)

The steps under [Test Case 2 – Previously connected *Receiver ID*] described in '2C-01 Regular Procedure – With Transmitter' are performed.

☐ If DUT successfully completes authentication with the new r_{tx} value provided in the second AKE_Init message, then PASS

2C-03. Irregular Procedure – New Authentication during Locality Check

Test Objective

Verify the Receiver DUT restarts authentication when a new AKE_Init and r_{tx} is transmitted right after the reception of LC_Init.

Required Test Method

<Connection Setup>

Same as '2C-01 Regular Procedure – With Transmitter'

<Test Case>

The steps described under [Before Starting Authentication] and [Authentication and Key Exchange] (for [Test Case 2 – Previously connected *Receiver ID*]) in '2C-01 Regular Procedure – With Transmitter' are performed.

[Locality Check]

(STEP 2C-03-1)

- ☐ TE transmits LC_Init message
- ☐ TE transmits AKE_Init message

(STEP 2C-03-2)

- ☐ DUT transmits AKE_Send_Cert message
  - ➢ If DUT does not transmit AKE_Send_Cert message, then FAIL (Ref-2C-2)

The steps under [Test Case 2 – Previously connected *Receiver ID*] described in '2C-01 Regular Procedure – With Transmitter' are performed.

- ☐ If DUT successfully completes authentication with the new r_{tx} value provided in the second AKE_Init message, then PASS

2C-04. Irregular Procedure – New Authentication after SKE_Send_Eks

Test Objective

Verify the Receiver DUT restarts authentication when a new AKE_Init and r_{tx} is transmitted right after the reception of SKE_Send_Eks.

Required Test Method

<Connection Setup>

Same as '2C-01 Regular Procedure – With Transmitter'

<Test Case>

The steps described under [Before Starting Authentication] and [Authentication and Key Exchange] (for [Test Case 2 – Previously connected *Receiver ID*]) and [Locality Check] in '2C-01 Regular Procedure – With Transmitter' are performed.

[Session Key Exchange]

(STEP 2C-04-1)

- ☐ TE transmits SKE_Send_Eks and Type message
- ☐ TE transmits AKE_Init message

(STEP 2C-04-2)

- ☐ DUT transmits AKE_Send_Cert message
  - ➢ If DUT does not transmit AKE_Send_Cert message, then FAIL (Ref-2C-2)

The steps under [Test Case 2 – Previously connected *Receiver ID*] described in '2C-01 Regular Procedure – With Transmitter' are performed.

- ☐ If DUT successfully completes authentication with the new r_{tx} value provided in the second AKE_Init message, then PASS

2C-05. Irregular Procedure – New Authentication during Link Synchronization

Test Objective

Verify the Receiver DUT restarts authentication when a new AKE_Init and r_{tx} is transmitted during Link Synchronization.

Required Test Method

<Connection Setup>

Same as '2C-01 Regular Procedure – With Transmitter'

<Test Case>

The steps described under [Before Starting Authentication] and [Authentication and Key Exchange] (for [Test Case 2 – Previously connected *Receiver ID*]) and [Locality Check] in '2C-01 Regular Procedure – With Transmitter' are performed.

[Session Key Exchange]

(STEP 2C-05-1)

- ☐ TE transmits SKE_Send_Eks and Type messages
- ☐ TE enables HDCP Encryption 200ms after transmitting SKE_Send_Eks message
- ☐ TE transmits AKE_Init message

(STEP 2C-05-2)

- ☐ DUT transmits AKE_Send_Cert message
  - ➢ If DUT does not transmit AKE_Send_Cert message, then FAIL (Ref-2C-2)

The steps under [Test Case 2 – Previously connected *Receiver ID*] described in '2C-01 Regular Procedure – With Transmitter' are performed.

- ☐ If DUT successfully completes authentication with the new r_{tx} value provided in the second AKE_Init message, then PASS

3. Repeater Tests

Repeater DUTs are tested for compliance with the DisplayPort HDCP2.3 specification by connecting them to Receivers (TE pseudo-Sink), Repeaters (TE pseudo-Repeater) and Transmitters (TE pseudo-Source).

3A. Downstream Procedure with Receiver

In this test, a DisplayPort Receiver (TE pseudo-Sink) is connected to the downstream HDCP2.3-protected Interface Port of the Repeater DUT. An HDCP2.3 Transmitter (providing HDCP2.3-protected content) is connected to the upstream HDCP2.3-protected Interface Port of the Repeater DUT.

The operation of the DUT under 1, 2 and 4-lane Main Link configuration is tested.

3A-01. Regular Procedure – With previously connected Receiver (With stored k_m)

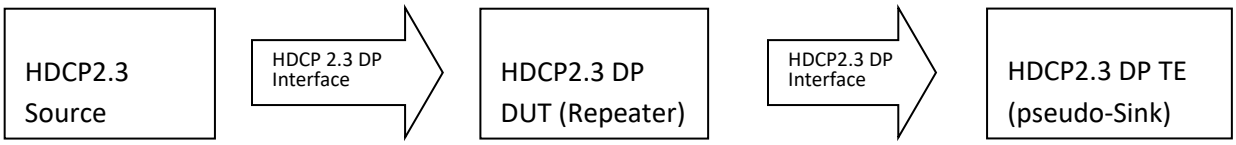
Test Objective

Verify the Repeater's implementation of the HDCP2.3 protocol when an HDCP2.3 Receiver (that was previously connected) is attached.

Required Test Method

<Connection Setup>

- ☐ Connect an HDCP Source device to the upstream HDCP-protected Interface Port of DUT
- ☐ Connect TE (pseudo-Sink) to the downstream HDCP-protected Interface Port of DUT



<Configuration of TE>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

<Test Case>

Same as '1A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

3A-02. Regular Procedure – With newly connected Receiver (Without stored k_m)

Test Objective

Verify the Repeater's implementation of the HDCP2.2 protocol when an HDCP2.2 Receiver (not previously connected) is attached.

Required Test Method

<Connection Setup>

Same as '3A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

<Configuration of TE>

Same as '1A-02 Regular Procedure – With newly connected Receiver (Without stored k_m)'

<Test Case>

Same as '1A-02 Regular Procedure – With newly connected Receiver (Without stored k_m)'

3A-03. Irregular Procedure – Verify Receiver Certificate

Test Objective

Verify the Repeater DUT considers it a failure of authentication when verification of Receiver certificate fails.

Required Test Method

<Connection Setup>

Same as '3A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

<Configuration of TE>

Same as '1A-08 Irregular Procedure – Verify Receiver Certificate'

<Test Case>

Same as '1A-08 Irregular Procedure – Verify Receiver Certificate'

3A-04. Irregular Procedure – Invalid H'

Test Objective

Verify the Repeater DUT considers it a failure of authentication if the Receiver provides a value for H' that does not match H, or does not respond with H' in the allotted time.

Required Test Method

<Connection Setup>

Same as '3A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

<Configuration of TE>

Same as '1A-10 Irregular Procedure – Invalid H''

<Test Case>

Same as '1A-10 Irregular Procedure – Invalid H''

3A-05. Irregular Procedure – Pairing Failure

Test Objective

Verify the Repeater DUT considers it a failure of authentication if the Receiver does not send AKE_Send_Pairing_Info.

Required Test Method

<Connection Setup>

Same as '3A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

<Configuration of TE>

Same as '1A-11 Irregular Procedure – Pairing Failure'

<Test Case>

Same as '1A-11 Irregular Procedure – Pairing Failure'

3A-06. Irregular Procedure – Locality Failure

Test Objective

Verify the Repeater DUT considers it a failure of authentication if the Receiver provides a value for L' that does not match L, or does not responds with L' in the allotted time.

Required Test Method

<Connection Setup>

Same as '3A-01 Regular Procedure – With previously connected receiver (With stored k_m)'

<Configuration of TE>

Same as '1A-12 Regular Procedure – Locality Pre-Compute Support'

<Test Case>

Same as '1A-12 Regular Procedure – Locality Pre-Compute Support'

3B. Downstream Procedure with Repeater

In this test, a DisplayPort Repeater (TE pseudo-Repeater) is connected to the downstream HDCP2.2-protected Interface Port of the Repeater DUT. A DisplayPort HDCP2.2 Transmitter (providing HDCP2.2-protected content) is connected to the upstream HDCP2.2-protected Interface Port of the Repeater DUT.

The operation of the DUT under 1, 2 and 4-lane Main Link configuration is tested.

3B-01. Regular Procedure – With Repeater

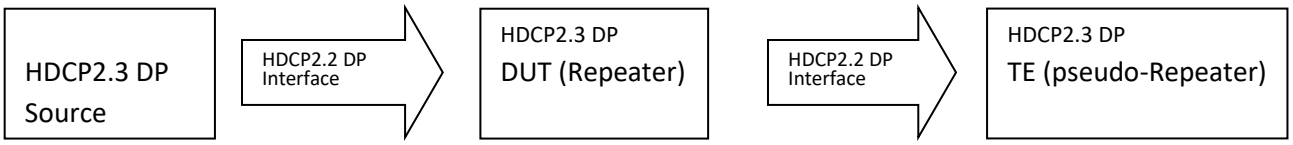
Test Objective

Verify the Repeater DUT's implementation of the HDCP2.3 Protocol when an HDCP2.3 repeater attached under nominal circumstances.

Required Test Method

<Connection Setup>

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



<Configuration of TE>

Same as '1B-01 Regular Procedure – With Repeater' except for the following change

- RepeaterAuth_Send_ReceiverID_List:DEVICE_COUNT = 30
- RepeaterAuth_Send_ReceiverID_List:DEPTH = 3

<Test Case>

Same as '1B-01 Regular Procedure – With Repeater'

3B-02. Irregular Procedure – Timeout of Receiver ID list

Test Objective

Verify the Repeater DUT considers it a failure of authentication if the downstream repeater does not respond with RepeaterAuth_Send_ReceiverID_List prior to expiration of watchdog timer.

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:

- ☐ TE does not respond with RepeaterAuth_Send_ReceiverID_List within the 3 second timeout of the receipt of SKE_Send_Eks

<Test Case>

Same as '1B-02 Irregular Procedure – Timeout of Receiver ID list'

3B-03. Irregular Procedure – Verify V'

Test Objective

Verify the Repeater DUT considers it a failure of authentication if the repeater provides a value for V' that does not match V.

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:

- ☐ TE provides an incorrect value for V'

<Test Case>

Same as '1B-03 Irregular Procedure – Verify V''

3B-04. Irregular Procedure – MAX_DEVS_EXCEEDED

Test Objective

Verify the Repeater DUT considers it a failure of authentication if the repeater sets the MAX_DEVS_EXCEEDED bit in the RepeaterAuth_Send_ReceiverID_List message.

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:

- ☐ TE sets MAX_DEVS_EXCEEDED to 'TRUE' in RepeaterAuth_Send_ReceiverID_List message

<Test Case>

Same as '1B-04 Irregular Procedure – MAX_DEVS_EXCEEDED'

3B-05. Irregular Procedure – MAX_CASCADE_EXCEEDED

Test Objective

Verify the Repeater DUT considers it a failure of authentication if the repeater sets the MAX_CASCADE_EXCEEDED bit in the RepeaterAuth_Send_ReceiverID_List message.

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:

- ☐ TE sets MAX_CASCADE_EXCEEDED to 'TRUE' in RepeaterAuth_Send_ReceiverID_List message

<Test Case>

Same as '1B-06 Irregular Procedure – MAX_CASCADE_EXCEEDED'

3B-06. Irregular Procedure – Rollover of *seq_num_V*

Test Objective

Verify the Repeater DUT initiates re-authentication when a rollover of *seq_num_V* is detected from the downstream repeater.

Required Test Method

<Connection Setup>

Same as '3B-01 Regular Procedure – With Repeater'

<Configuration of TE>

Same as '3B-01 Regular Procedure – With Repeater'

<Test Case>

Same as '1B-09 Irregular Procedure – Rollover of *seq_num_V*'

3B-07. Irregular Procedure – Failure of Content Stream Management

Test Objective

Verify the Repeater DUT re-attempts Content Stream Management following a failure of Content Stream Management.

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:

- ☐ TE provides an incorrect value for M'

<Test Case>

Same as '1B-10 Irregular Procedure – Failure of Content Stream Management'

3C. Upstream Procedure with Transmitter

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

- An HDCP2.3 DisplayPort Transmitter (TE pseudo-Source) is connected to the upstream HDCP2.3-protected Interface Port and an HDCP2.3 DisplayPort Receiver (TE pseudo-Sink) is connected to the downstream HDCP2.3-protected Interface Port of the Repeater DUT.
- An HDCP2.3 DisplayPort Transmitter (TE pseudo-Source) is connected to the upstream HDCP2.3-protected Interface Port and a DisplayPort HDCP2.3 Repeater (TE pseudo-Repeater) is connected to the downstream HDCP2.3-protected Interface Port of the DisplayPort Repeater DUT.

☐ Repeater (DUT) Connected to Transmitter (TE pseudo-Source) and Receiver (TE pseudo-Sink)

In this test, an HDCP2.3 DisplayPort Transmitter (TE pseudo-Source) is connected to the upstream HDCP2.3-protected Interface Port of the DisplayPort Repeater DUT. An HDCP2.3 DisplayPort Receiver (TE pseudo-Sink) is connected to the downstream HDCP2.3-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

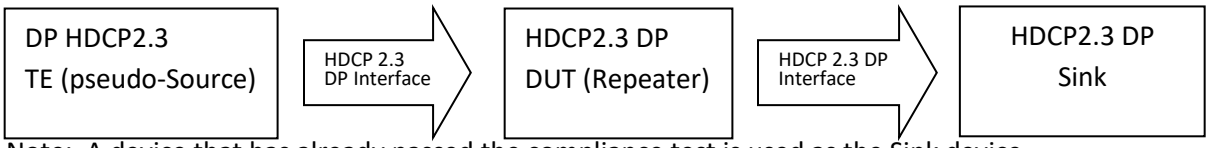
Test Objective

Verify the Repeater DUT's implementation of the HDCP2.2 Protocol when an HDCP2.2 Transmitter is connected to the upstream Repeater port and an HDCP2.2 Receiver is connected to the downstream Repeater port.

Required Test Method

<Connection Setup>

- ☐ Connect TE (pseudo-Source) to the upstream HDCP2.2-protected Interface Port of DUT
- ☐ Connect an HDCP Sink to the downstream HDCP-protected Interface Port of DUT



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

<Test Case>

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

[Authentication and Key Exchange]

(STEP 2C-01-2) described in '2C-01 Regular Procedure – With Transmitter' are performed, with the following changes:

- ☐ TE begins sending unencrypted video signal with HDCP2.2 Encryption disabled
- ☐ TE transmits AKE_Init message
- ☐ DUT transmits AKE_Send_Cert message
  - ➢ If DUT does not transmit AKE_Send_Cert message, then FAIL (Ref-2C-2)
  - ➢ If REPEATER is 'FALSE' in AKE_Send_Cert message, then FAIL (Ref-2C-3)

The remaining steps described in [Authentication and Key Exchange] (both test cases) and the steps described in [Pairing], [Locality Check], and [Session Key Exchange] in '2C-01 Regular Procedure – With Transmitter' are performed.

[Authentication with Repeaters]

(STEP 3C-01-1)

- ☐ DUT transmits RepeaterAuth_Send_ReceiverID_List message
  - ➢ If DUT does not transmit RepeaterAuth_Send_ReceiverID_List message within 3 second timeout of SKE_Send_Eks, then FAIL(Ref-1B-2)
  - ➢ If RepeaterAuth_Send_ReceiverID_List:MAX_DEVS_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)
  - ➢ If RepeaterAuth_Send_ReceiverID_List:MAX_CASCADE_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)
  - ➢ If RepeaterAuth_Send_ReceiverID_List:DEPTH is not one, then FAIL(Ref-3C-2)
  - ➢ If RepeaterAuth_Send_ReceiverID_List:DEVICE_COUNT is not one, then FAIL(Ref-3C-2)
  - ➢ If RepeaterAuth_Send_Receiver_ID_List:HDCP2_0_REPEATER_DOWNSTREAM is 'TRUE', then FAIL (Ref-3C-8)
  - ➢ If RepeaterAuth_Send_Receiver_ID_List:HDCP1_DEVICE_DOWNSTREAM is 'TRUE', then FAIL (Ref-3C-8)
  - ➢ If RepeaterAuth_Send_Receiver_ID_List:*Seq_num_V* is not 0, then FAIL (Ref-3C-7)

(STEP 3C-01-2)

- ☐ TE compares computed value of most significant 128 bits of V to 128 bits of V' received in RepeaterAuth_Send_ReceiverID_list.
  - ➢ If most significant 128 bits of V' do not match the most significant 128 bits of V, then FAIL (Ref-1B-2)
- ☐ TE transmits RepeaterAuth_Send_Ack message with valid least 128 bits of V within two second of receipt of RepeaterAuth_Send_ReceiverID_list

(STEP 3C-01-3)

[Content Stream Management] – Two test cases; both are performed.

[Test Case 1 – Content Stream Management done in serial with propagation of topology information]

- ☐ TE transmits RepeaterAuth_Stream_Manage message within 5seconds after transmitting RepeaterAuth_Send_Ack message with Type set to 0, and 100ms prior to the transmission of the corresponding Content Streams

[Test Case 2 – Content Stream Management done in parallel with propagation of topology information]

☐ TE transmits RepeaterAuth_Stream_Manage message within 5seconds after successful completion exchange of Ks, with Type set to 0

[Both Test Cases]

☐ DUT transmits RepeaterAuth_Stream_Ready message

- If DUT does not transmit RepeaterAuth_Stream_Ready message within 100 ms of transmission of RepeaterAuth_Stream_Manage, then FAIL (Ref-1B-5)
- If the value of M' received in the RepeaterAuth_Stream_Ready message does not match the TE's calculated value of M, then FAIL (Ref-1B-5)

☐ TE Enables HDCP Encryption

(STEP 3C-01-4)

☐ If DUT completes the authentication process successfully, then PASS

3C-02. Regular Procedure – Receiver Disconnect Propagation when an Active Receiver is Disconnected Downstream

Test Objective

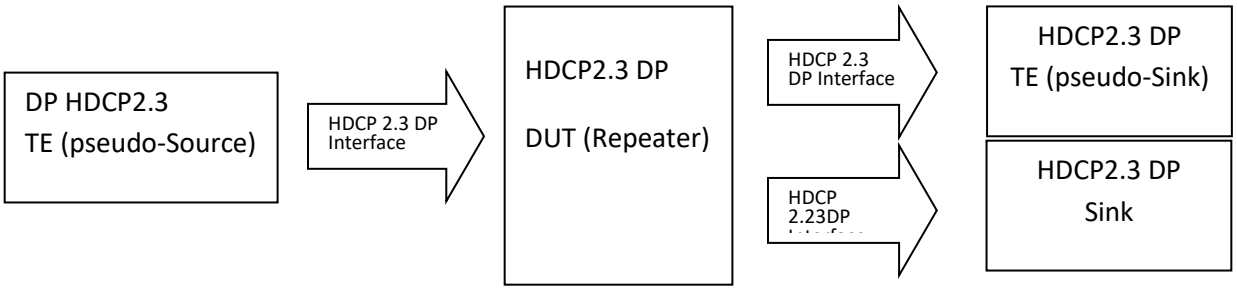
Verify the Repeater DUT sends an updated RepeaterAuth_Send_ReceiverID_List message when an active downstream Receiver is disconnected when HDCP Content is flowing.

Required Test Method

This test is performed if Repeater_MultipleOutputs = Y, otherwise SKIP

<Connection Setup>

- ☐ Connect TE (pseudo-Source) to the upstream HDCP2.3-protected Interface Port of DUT
- ☐ Connect TE (pseudo-Sink) to the one downstream HDCP2.3-protected Interface Port of DUT
- ☐ Connect HDCP2.3 Sink to another downstream HDCP-protected Interface Port of DUT



Note: A device that has already passed the DP HDCP2.2 compliance test is used as the Sink device

<Test Case>

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

The steps described under [Authentication and Key Exchange] in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' are performed.

The remaining steps described in [Authentication and Key Exchange] and the steps described in [Pairing], [Locality Check], and [Session Key Exchange] in '2C-01 Regular Procedure – With Transmitter' are performed.

[Authentication with Repeaters]

(STEP 3C-01-1) described in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' is performed with the following changes:

- ☐ DUT transmits RepeaterAuth_Send_ReceiverID_List message
  - If DUT does not transmit RepeaterAuth_Send_ReceiverID_List message within 3 second timeout of SKE_Send_Eks, then FAIL(Ref-1B-2)
  - If RepeaterAuth_Send_ReceiverID_List:MAX_DEVS_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)
  - If RepeaterAuth_Send_ReceiverID_List:MAX_CASCADE_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)
  - If RepeaterAuth_Send_ReceiverID_List:DEPTH is not one, then FAIL(Ref-3C-2)
  - If RepeaterAuth_Send_ReceiverID_List:DEVICE_COUNT is not two, then FAIL(Ref-3C-2)
  - If RepeaterAuth_Send_ReceiverID_List:HDCP2_0_REPEATER_DOWNSTREAM is 'TRUE', then FAIL.
  - If RepeaterAuth_Send_ReceiverID_List:HDCP1_DEVICE_DOWNSTREAM is 'TRUE', then FAIL.
  - If RepeaterAuth_Send_ReceiverID_List:*seq_num_v* is not 0, then FAIL (Ref-3C-7).

(STEP 3C-01-2) described in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' is performed

[Disconnect of Downstream Sink]

(STEP 3C-02-1)

- ☐ TE (pseudo-Sink) sends Receiver Disconnect Indication
  - If DUT transmits Receiver Disconnect upstream, then FAIL (Ref-3C-3)

(STEP 3C-02-2)

- ☐ DUT transmits RepeaterAuth_Send_ReceiverID_List message
  - If DUT does not transmit RepeaterAuth_Send_ReceiverID_List message within 3 second of TE (pseudo-Sink) disconnect, then FAIL(Ref-1B-2)
  - If RepeaterAuth_Send_ReceiverID_List:MAX_DEVS_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)

- If RepeaterAuth_Send_ReceiverID_List:MAX_CASCADE_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)
- If RepeaterAuth_Send_ReceiverID_List:DEPTH is not one, then FAIL(Ref-3C-2)
- If RepeaterAuth_Send_ReceiverID_List:DEVICE_COUNT is not one, then FAIL(Ref-3C-2)
- If content stream to remaining receiver is interrupted, then WARNING (Ref-3C-7)

☐ If the DUT does not propagate Receiver Disconnect upstream when an active downstream Sink is disconnected, and transmits an updated RepeaterAuth_Send_ReceiverID_List message, then PASS

3C-03. Regular Procedure – Receiver Connected when an Active Receiver is Connected Downstream

Test Objective

Verify the Repeater DUT sends an updated RepeaterAuth_Send_ReceiverID_List message when a new active downstream Receiver is connected and HDCP Content is flowing.

Required Test Method

This test is performed if Repeater_MultipleOutputs = Y, otherwise SKIP

<Connection Setup>

Same as '3C-02 Regular Procedure – Receiver Disconnect Propagation when an Active Receiver is Disconnected Downstream' with one exception:

- TE (pseudo-Sink) is in disconnected state

<Test Case>

The steps described under [Before Starting Authentication] to [Authentication with Repeaters] in '3C-02 Regular Procedure – Receiver Disconnect Propagation when an Active Receiver is Disconnected and Reconnected Downstream' are performed.

[Connect Active Downstream Sink]

(STEP 3C-03-1)

☐ TE (pseudo-Sink) sends Receiver Connect indication to DUT

- If DUT propagates Receiver Connect indication upstream, then FAIL (Ref-3C-3)

(STEP 3C-03-2)

☐ DUT transmits RepeaterAuth_Send_ReceiverID_List message

- If DUT does not transmit RepeaterAuth_Send_ReceiverID_List message within 3 second of TE (pseudo-Sink) connect, then FAIL(Ref-1B-2)
- If RepeaterAuth_Send_ReceiverID_List:MAX_DEVS_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)
- If RepeaterAuth_Send_ReceiverID_List:MAX_CASCADE_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)
- If RepeaterAuth_Send_ReceiverID_List:DEPTH is not one, then FAIL(Ref-3C-2)

- If RepeaterAuth_Send_ReceiverID_List:DEVICE_COUNT is not two, then FAIL(Ref-3C-2)
- If content stream to remaining receiver is interrupted, then WARNING (Ref-3C-3)

☐ If the DUT transmits updated RepeaterAuth_Send_ReceiverID_List message upon connection of a new downstream HDCP Receiver, then PASS

3C-04. Irregular Procedure – New Authentication after AKE_Init

Test Objective

Verify the Repeater DUT restarts authentication when a new AKE_Init and r_{tx} is transmitted right after the transmission of AKE_Init in the unauthenticated state.

Required Test Method

<Connection Setup>

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

<Test Case>

Same as '2C-02 Irregular Procedure – New Authentication after AKE_Init' with the following changes:

(STEP 2C-01-2)

- ☐ TE begins sending unencrypted video signal with HDCP Encryption disabled
- ☐ TE transmits AKE_Init message
- ☐ DUT transmits AKE_Send_Cert message
  - ➢ If DUT does not transmit AKE_Send_Cert message, then FAIL (Ref-2C-2)
  - ➢ If AKE_Send_Cert:REPEATER is 'FALSE', then FAIL (Ref-2C-3)

The steps described under [Test Case 1 – Not Previously Connected *Receiver ID*] in '2C-01 Regular Procedure – With Transmitter' are performed

- ☐ If DUT successfully completes authentication with new r_{tx} value provided in the second AKE_Init message, then PASS

3C-05. Irregular Procedure – New Authentication during Locality Check

Test Objective

Verify the Repeater DUT restarts authentication when a new AKE_Init and r_{tx} is transmitted right after the reception of LC_Init.

Required Test Method

<Connection Setup>

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

<Test Case>

Same as '2C-03 Irregular Procedure – New Authentication during Locality Check' with the following changes:

(STEP 2C-01-2)

- ☐ TE begins sending unencrypted video signal with HDCP Encryption disabled
- ☐ TE transmits AKE_Init message
- ☐ DUT transmits AKE_Send_Cert message
  - ➢ If DUT does not transmit AKE_Send_Cert message, then FAIL (Ref-2C-2)
  - ➢ If AKE_Send_Cert:REPEATER is 'FALSE', then FAIL (Ref-2C-3)

The steps described under [Test Case 1 – Not Previously Connected *Receiver ID*] in '2C-01 Regular Procedure – With Transmitter' are performed

- ☐ If DUT successfully completes authentication with new r_{tx} value provided in the second AKE_Init message, then PASS

3C-06. Irregular Procedure – New Authentication after SKE_Send_Eks

Test Objective

Verify the Repeater DUT restarts authentication when a new AKE_Init and r_{tx} is transmitted right after the reception of SKE_Send_Eks.

Required Test Method

<Connection Setup>

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

<Test Case>

Same as '2C-04 Irregular Procedure – New Authentication after SKE_Send_Eks' with the following changes:

(STEP 2C-01-2)

- ☐ TE begins sending unencrypted video signal with HDCP Encryption disabled
- ☐ TE transmits AKE_Init message
- ☐ DUT transmits AKE_Send_Cert message
  - If DUT does not transmit AKE_Send_Cert message, then FAIL (Ref-2C-2)
  - If AKE_Send_Cert:REPEATER is 'FALSE', then FAIL (Ref-2C-3)

The steps described under [Test Case 1 –Not Previously Connected *Receiver ID*] in '2C-01 Regular Procedure – With Transmitter' are performed

- ☐ If DUT successfully completes authentication with new r_{tx} value provided in the second AKE_Init message, then PASS

3C-07. Irregular Procedure – New Authentication during Link Synchronization

Test Objective

Verify the Repeater DUT restarts authentication when a new AKE_Init and rtx is transmitted during Link Synchronization.

Required Test Method

<Connection Setup>

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

<Test Case>

Same as '2C-05 Irregular Procedure – New Authentication during Link Synchronization' with the following changes:

(STEP 2C-01-2)

- ☐ TE begins sending unencrypted video signal with HDCP Encryption disabled
- ☐ TE transmits AKE_Init message
- ☐ DUT transmits AKE_Send_Cert message
  - ➢ If DUT does not transmit AKE_Send_Cert message, then FAIL (Ref-2C-2)
  - ➢ If AKE_Send_Cert:REPEATER is 'FALSE', then FAIL (Ref-2C-3)

The steps described under [Test Case 1 – Previously Connected *Receiver ID*] in '2C-01 Regular Procedure – With Transmitter' are performed

- ☐ If DUT successfully completes authentication with new r_{tx} value provided in the second AKE_Init message, then PASS

3C-08. Irregular Procedure – Rx Certificate invalid

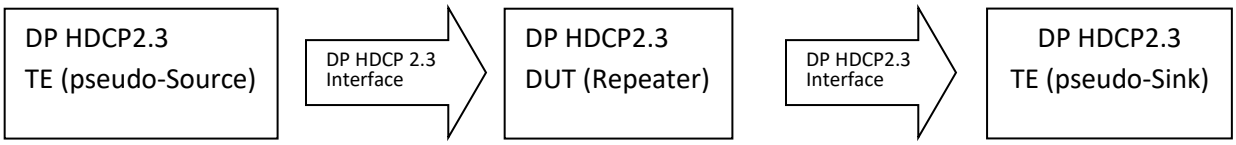
Test Objective

Verify the Repeater DUT considers it a failure of authentication and does not send RepeaterAuth_Send_ReceiverID_List message when the certificate received from the Receiver is invalid.

Required Test Method

<Connection Setup>

- ☐ Connect TE (pseudo-Source) to the upstream HDCP-protected Interface Port of DUT
- ☐ Connect TE (pseudo-Sink) to the downstream HDCP-protected Interface Port of DUT



<Configuration of TE (pseudo-Sink)>

Same as '1A-08 Irregular Procedure – Verify Receiver Certificate'

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' are performed.

[Authentication with Repeaters]

(STEP 3C-08-1)

- ☐ DUT reads invalid certificate of downstream pseudo-Sink
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
  - ➢ If DUT transmits AKE_No_Stored_km or AKE_Stored_km, then FAIL (Ref-1A-8)

(STEP 3C-08-2)

- ☐ TE (pseudo-Source) waits for DUT to transmit RepeaterAuth_Send_ReceiverID_List message for a maximum time of 3 seconds
  - ➢ If DUT transmits RepeaterAuth_Send_ReceiverID_List message, then FAIL (Ref-3C-5)

- ☐ If DUT treats invalid downstream certificate as an authentication failure and does not transmit RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS

3C-09. Irregular Procedure – Invalid H'

Test Objective

Verify the Repeater DUT considers it a failure of authentication and does not send RepeaterAuth_Send_ReceiverID_List message when the Receiver provides a value for H' that does not match H; or does not respond with H' in the allotted time.

Required Test Method

<Connection Setup>

Same as '3C-08 Irregular Procedure – Rx Certificate invalid'

<Configuration of TE (pseudo-Sink)>

Same as '1A-10 Irregular Procedure – Invalid H''

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' are performed.

[Authentication with Repeaters]

Two test cases; both are performed

[Test Case 1 – Invalid H']

(STEP 3C-09-1)

- ☐ DUT reads invalid *H'* of downstream pseudo-Sink
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
  - ➢ If DUT transmits LC_Init, then FAIL (Ref-1A-8)

[Test Case 2 – AKE_Send_H_prime timeout after AKE_Stored_km]

(STEP 3C-09-2)

- ☐ TE (pseudo-Sink) does not provide AKE_Send_H_prime message within 200ms timeout at the DUT
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
  - ➢ If DUT transmits LC_Init, then FAIL (Ref-1A-8)

[Both Test Cases]

(STEP 3C-09-3)

- ☐ TE (pseudo-Source) waits for DUT to transmit RepeaterAuth_Send_ReceiverID_List message for a maximum time of 3 seconds
    - ➢ If DUT transmits RepeaterAuth_Send_ReceiverID_List message, then FAIL (Ref-3C-5)
- ☐ If DUT treats invalid downstream H' or timeout of AKE_Send_H_prime as an authentication failure and does not transmit RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS

3C-10. Irregular Procedure – Locality Failure

Test Objective

Verify the Repeater DUT considers it a failure of authentication and does not send RepeaterAuth_Send_ReceiverID_List message when the Receiver provides a value for L' that does not match L.

Required Test Method

<Connection Setup>

Same as '3C-08 Irregular Procedure – Rx Certificate invalid'

<Configuration of TE (pseudo-Sink)>

Same as '1A-12 Irregular Procedure – Locality Failure'

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' are performed.

[Authentication with Repeaters]

(STEP 3C-10-1)

- ☐ DUT reads invalid *L'* of downstream pseudo-Sink
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
- ☐ DUT reattempts locality check with the transmission of LC_Init 1023 additional times (for a total max of 1024 trials) with new Rn
  - ➢ If Rn is not different in each attempt then FAIL
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)

(STEP 3C-10-2)

- ☐ TE (pseudo-Source) waits for DUT to transmit RepeaterAuth_Send_ReceiverID_List message for a maximum time of 3 seconds
  - ➢ If DUT transmits RepeaterAuth_Send_ReceiverID_List message, then FAIL (Ref-3C-5)
- ☐ If DUT treats invalid downstream L' as an authentication failure and does not transmit RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS

☐ Repeater (DUT) Connected to Transmitter (TE pseudo-Source) and Repeater (TE pseudo-Repeater)

In this test, DP HDCP2.2 Transmitter (TE pseudo-Source) is connected to the upstream HDCP2.2-protected Interface Port of the DP Repeater DUT. An HDCP2.2 DP Repeater (TE pseudo-Repeater) is connected to the downstream HDCP2.2-protected Interface Port of the Repeater (DUT).

3C-11. Regular Procedure – Transmitter – DUT – Repeater (With stored km)

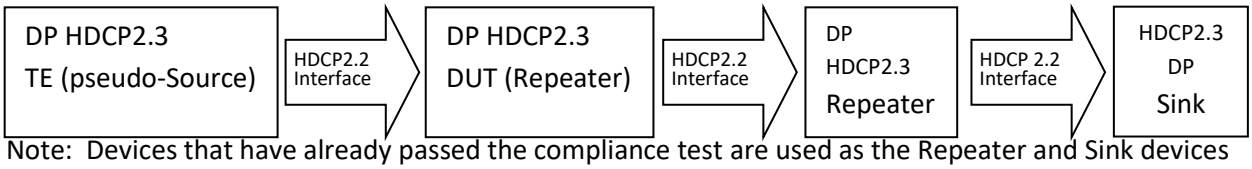
Test Objective

Verify the DP HDCP2.3 Repeater DUT's implementation of the HDCP2.3 Protocol when a DP HDCP2.3 Transmitter is connected to the upstream Repeater port and an HDCP2.3 Repeater is connected to the downstream Repeater port.

Required Test Method

<Connection Setup>

- ☐ Connect TE (pseudo-Source) to the upstream HDCP-protected Interface Port of DUT
- ☐ Connect an HDCP Repeater and HDCP Sink to the downstream HDCP-protected Interface Port of DUT



Note: Devices that have already passed the compliance test are used as the Repeater and Sink devices

Note: Downstream Repeater and Sink need to be HDCP 2.2 compatible devices.

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' are performed, with the following changes:

[Authentication with Repeaters]

(STEP 3C-11-1)

- ☐ DUT transmits RepeaterAuth_Send_ReceiverID_List message
  - ➢ If DUT does not transmit RepeaterAuth_Send_ReceiverID_List message within 3 second timeout of SKE_Send_Eks, then FAIL(Ref-1B-2)
  - ➢ If RepeaterAuth_Send_ReceiverID_List:MAX_DEVS_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)
  - ➢ If RepeaterAuth_Send_ReceiverID_List:MAX_CASCADE_EXCEEDED is 'TRUE', then FAIL(Ref-3C-1)
  - ➢ If RepeaterAuth_Send_ReceiverID_List:DEPTH is not two, then FAIL(Ref-3C-2)

- If RepeaterAuth_Send_ReceiverID_List:DEVICE_COUNT is not two, then FAIL(Ref-3C-2)
- If RepeaterAuth_Send_ReceiverID_List:HDCP2_0_REPEATER_DOWNSTREAM is 'TRUE', then FAIL (Ref-3C-8)
- If RepeaterAuth_Send_ReceiverID_List:HDCP1_DEVICE_DOWNSTREAM is 'TRUE', then FAIL (Ref-3C-8)
- If RepeaterAuth_Send_ReceiverID_List:V' is not valid 128 bits, then FAIL (Ref-1B-4)

The remaining steps including (STEP 3C-01-2) described in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' are performed

☐ If DUT completes the authentication process successfully, then PASS

3C-12. Regular Procedure – Receiver disconnect after AKE_Init

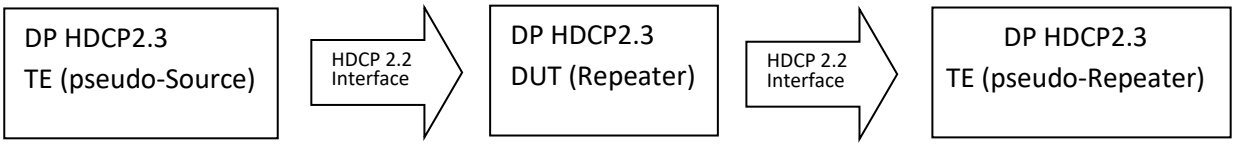
Test Objective

Verify the Repeater DUT propagates Receiver Disconnect and Receiver Connect Indication on Repeater disconnect and connect, respectively.

Required Test Method

<Connection Setup>

- ☐ Connect TE (pseudo-Source) to the upstream HDCP-protected Interface Port of DUT
- ☐ Connect TE (pseudo-Repeater) to the downstream HDCP-protected Interface Port of DUT



<Configuration of TE (pseudo-Repeater)>

Message:	Parameter:	Value:
Authentication and Key Exchange		
AKE_Send_Cert	RxCaps:VERSION	0x02
	RxCaps:RECEIVER_CAPABILITY_MASK	0x00
	RxCaps:REPEATER	TRUE(1)
	RxCaps:HDCP_CAPABLE	TRUE(1)
	r_{rx}	Valid
	$cert_{rx}$	Valid
AKE_Send_H_prime	H’	Valid (within 200ms timeout)
Pairing		
AKE_Send_Pairing_Info	E_{kh}_k_m	Valid (used only for first time)
Locality Check		
LC_Send_L_prime	L’	Valid (within 16ms timeout)
Authentication with Repeater		
RepeaterAuth_Send_ReceiverID_List	RxInfo:MAX_DEVS_EXCEEDED	FALSE
	RxInfo:MAX_CASCADE_EXCEEDED	FALSE
	RxInfo:HDCP2_0_REPEATER_DOWNSTREAM	FALSE
	RxInfo:HDCP1_DEVICE_DOWNSTREAM	FALSE
	RxInfo:DEVICE_COUNT	30
	RxInfo:DEPTH	3

	Receiver ID List	(DEVICE_COUNT * 5) bytes
	V'	16 bytes, Valid (within 3 second timeout)
	seq_num_V	Valid

<Test Case>

The steps described under [Before Starting Authentication] to [Authentication and Key Exchange] in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' are performed.

[Authentication and Key Exchange]

(STEP 3C-12-1)

- ☐ TE (pseudo-Repeater) sends *Receiver Disconnect Indication* after AKE_Init message
- ☐ DUT either
  - (a) sets REAUTH_REQ in RxStatus register and clears REPEATER in RxCaps of AKE_Send_Cert message

    or

  - (b) Send *Receiver Disconnect Indication* to upstream TE (Pseudo-Source)
    - ➢ If DUT does not
      - (a) set REAUTH_REQ in RxStatus and clear REPEATER in RxCaps of AKE_Send_Cert message
        or
      - (b) Send *Receiver Disconnect Indication* to TE(pseudo-Source), then FAIL(Ref-3C-4)

(STEP 3C-12-2)

- ☐ TE (pseudo-Repeater) sends *Receiver Connect Indication*
- ☐ DUT either
  - (a) sets REAUTH_REQ in RxStatus register and REPEATER in RxCaps of AKE_Send_Cert message

    or

  - (b) Send *Receiver Connect Indication* to upstream TE (Pseudo-Source)
    - ➢ If DUT does not
      - (a) set REAUTH_REQ in RxStatus and REPEATER in RxCaps of AKE_Send_Cert message

or

(b) Send *Receiver Connect Indication* to TE(pseudo-Source), then FAIL(Ref-3C-4)

- If DUT sends *Receiver Connect Indication* before TE(pseudo-Repeater) and REPEATER is set in RxCaps of AKE_Send_Cert message, then FAIL(Ref-3C-4)

(STEP 3C-12-3)

- ☐ TE (pseudo-Source) restarts Authentication and Key Exchange with DUT
- ☐ DUT restarts Authentication and Key Exchange with downstream TE(Pseudo-repeater)
  - If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in '1A-01 Regular Procedure- With previously connected Receiver (With stored Km)', then FAIL (Ref-1A-7)
  - If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)
- ☐ If DUT either properly sets and clears REAUTH_REQ in RxStatus register and REPEATER in AKE_Send_Cert message, or propagates the de-asserted and re-asserted HPD on Repeater disconnect and connect respectively, then PASS

3C-13. Regular Procedure – Receiver disconnect after k_m

Test Objective

Verify the Repeater DUT restarts authentication after the Repeater is disconnected and reconnected following the exchange of K_m.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '3C-12 Regular – Receiver disconnect after AKE_Init'

<Test Case>

The steps described under [Before Starting Authentication] to [Authentication and Key Exchange] in '3C-01 Regular Procedure – Transmitter – DUT – Receiver' are performed.

[Authentication and Key Exchange]

(STEP 3C-13-1)

- ☐ TE (pseudo-Repeater) sends *Receiver Disconnect Indication* after AKE_Stored_Km or AKE_No_Stored_Km message
- ☐ DUT either
  - (a) sets REAUTH_REQ in RxStatus register and asserts CP_IRQ interrupt and clears REPEATER in RxCaps of AKE_Send_Cert message

    or

  - (b) Send *Receiver Disconnect Indication* to upstream TE (Pseudo-Source).
    - ➢ If DUT does not
      - (a) set REAUTH_REQ in RxStatus and asserts CP_IRQ interrupt and clear REPEATER in RxCaps of AKE_Send_Cert message
        or
      - (b) Send *Receiver Disconnect Indication* to TE(pseudo-Source), then FAIL(Ref-3C-4)

(STEP 3C-13-2)

- ☐ TE (pseudo-Repeater) sends *Receiver Connect Indication*

☐ DUT either

(a) sets REAUTH_REQ in RxStatus register, asserts CP_IRQ interrupt and REPEATER in RxCaps of AKE_Send_Cert message

or

(b) Send *Receiver Connect Indication* to upstream TE (Pseudo-Source)
- If DUT does not
  (a) set REAUTH_REQ in RxStatus, asserts CP_IRQ interrupt and REPEATER in RxCaps of AKE_Send_Cert message
  or
  (b) Send *Receiver Connect Indication* to TE(pseudo-Source), then FAIL(Ref-3C-4)
- If DUT sends *Receiver Connect Indication* before TE(pseudo-Repeater) and REPEATER is set in RxCaps of AKE_Send_Cert message, then FAIL(Ref-3C-4)

(STEP 3C-13-3)

☐ TE (pseudo-Source) restarts Authentication and Key Exchange with DUT

☐ DUT restarts Authentication and Key Exchange with downstream TE(Pseudo-repeater)

- If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in '1A-01 Regular Procedure- With previously connected Receiver (With stored Km)', then FAIL (Ref-1A-7)

- If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)

☐ If DUT either properly sets and clears REAUTH_REQ in RxStatus register and REPEATER in AKE_Send_Cert message, or propagates the de-asserted and re-asserted HPD on Repeater disconnect and connect respectively, then PASS

3C-14. Regular Procedure – Receiver disconnect after locality check

Test Objective

Verify the Repeater DUT restarts authentication after the Repeater is disconnected and reconnected after locality check is initiated.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Test Case>

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

[Locality Check]

(STEP 3C-14-1)

- ☐ TE (pseudo-Repeater) sends *Receiver Disconnect Indication* after LC_init message.
- ☐ DUT either

  (a) sets REAUTH_REQ in RxStatus register, asserts CP_IRQ interrupt and clears REPEATER in RxCaps of AKE_Send_Cert message

  or

  (b) Send *Receiver Disconnect Indication* to upstream TE (Pseudo-Source).
  - If DUT does not
    (a) set REAUTH_REQ in RxStatus, asserts CP_IRQ interrupt and clear REPEATER in RxCaps of AKE_Send_Cert message
    or
    (b) Send *Receiver Disconnect Indication* to TE(pseudo-Source), then FAIL(Ref-3C-4)

(STEP 3C-14-2)

- ☐ TE (pseudo-Repeater) sends *Receiver Connect Indication*
- ☐ DUT either

(a) sets REAUTH_REQ in RxStatus register, asserts CP_IRQ interrupt and REPEATER in RxCaps of AKE_Send_Cert message

or

(b) Send *Receiver Connect Indication* to upstream TE (Pseudo-Source)
- If DUT does not
  (a) set REAUTH_REQ in RxStatus, asserts CP_IRQ interrupt and REPEATER in RxCaps of AKE_Send_Cert message
  or
  (b) Send *Receiver Connect Indication* to TE(pseudo-Source), then FAIL(Ref-3C-4)
- If DUT sends *Receiver Connect Indication* before TE(pseudo-Repeater) and REPEATER is set in RxCaps of AKE_Send_Cert message, then FAIL(Ref-3C-4)

(STEP 3C-14-3)

☐ TE (pseudo-Source) restarts Authentication and Key Exchange with DUT

☐ DUT restarts Authentication and Key Exchange with downstream TE(Pseudo-repeater)

- If DUT does not restart Authentication and Key Exchange and complete(STEP 1A-01-2) as described in '1A-01 Regular Procedure- With previously connected Receiver (With stored Km)', then FAIL (Ref-1A-7)

- If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)

☐ If DUT either properly sets and clears REAUTH_REQ in RxStatus register and REPEATER in AKE_Send_Cert message, or propagates the de-asserted and re-asserted HPD on Repeater disconnect and connect respectively, then PASS

3C-15. Regular Procedure – Receiver disconnect after K_s

Test Objective

Verify the Repeater DUT restarts authentication after the Repeater is disconnected and reconnected following the exchange of K_s.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Test Case>

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

[Session Key Exchange]

(STEP 3C-15-1)

- ☐ TE (pseudo-Repeater) sends *Receiver Disconnect Indication* after SKE_Send_Eks message.
- ☐ DUT either

  (a) sets REAUTH_REQ in RxStatus register, asserts CP_IRQ interrupt and clears REPEATER in RxCaps of AKE_Send_Cert message

  or

  (b) Send *Receiver Disconnect Indication* to upstream TE(Pseudo-Source).
  - If DUT does not
    (a) set REAUTH_REQ in RxStatus, asserts CP_IRQ interrupt and clear REPEATER in RxCaps of AKE_Send_Cert message
    or
    (b) Send *Receiver Disconnect Indication* to TE(pseudo-Source), then FAIL(Ref-3C-4)

(STEP 3C-15-2)

- ☐ TE (pseudo-Repeater) sends *Receiver Connect Indication*

☐ DUT either

(a) sets REAUTH_REQ in RxStatus register, asserts CP_IRQ interrupt and REPEATER in RxCaps of AKE_Send_Cert message

or

(b) Send *Receiver Connect Indication* to upstream TE (Pseudo-Source).
- If DUT does not
  (a) set REAUTH_REQ in RxStatus, asserts CP_IRQ interrupt and REPEATER in RxCaps of AKE_Send_Cert message
  or
  (b) Send *Receiver Connect Indication* to TE(pseudo-Source), then FAIL(Ref-3C-4)
- If DUT sends *Receiver Connect Indication* before TE(pseudo-Repeater) and REPEATER is set in RxCaps of AKE_Send_Cert message, then FAIL(Ref-3C-4)

(STEP 3C-15-3)

☐ TE (pseudo-Source) restarts Authentication and Key Exchange with DUT.

☐ DUT restarts Authentication and Key Exchange with downstream TE(Pseudo-repeater)

- If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in '1A-01 Regular Procedure- With previously connected Receiver (With stored Km)', then FAIL (Ref-1A-7)

- If DUT enables HDCP Encryption but fails to turn it off before restarting Authentication, then FAIL (Ref-1A-2)

☐ If DUT either properly sets and clears REAUTH_REQ in RxStatus register and REPEATER in AKE_Send_Cert message, or propagates the de-asserted and re-asserted HPD on Repeater disconnect and connect respectively, then PASS

3C-16. Irregular Procedure – Timeout of Receiver ID list

Test Objective

Verify the Repeater DUT considers it a failure of authentication and does not send RepeaterAuth_Send_ReceiverID_List message when the downstream repeater fails to provide RepeaterAuth_Send_ReceiverID_List message prior to expiration of the watchdog timer.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure –Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in '3C-12 Regular Procedure – Transmitter – DUT – Repeater (With stored k_m)' are performed.

[Authentication with Repeaters]

(STEP 3C-16-1)

- ☐ DUT waits maximum of 3 seconds for downstream TE (pseudo-Repeater) to send RepeaterAuth_Send_ReceiverID_List

(STEP 3C-16-2)

- ☐ DUT disables HDCP encryption, if enabled, after the expiration of the three second timer
  - ➢ If DUT disables encryption before the timer expires, then FAIL (Ref-1B-2)
  - ➢ If DUT does not disable encryption after the timer expires, then FAIL (Ref-1B-2)
  - ➢ If DUT sends RepeaterAuth_Send_Ack message, then FAIL (Ref-1B-2)

(STEP 3C-16-3)

- ☐ DUT does not transmit RepeaterAuth_Send_ReceiverID_List to TE (pseudo-Source)
  - ➢ If DUT transmits RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-5)
- ☐ If DUT treats timeout of watchdog timer for RepeaterAuth_Send_ReceiverID_List from downstream TE pseudo-Repeater as an authentication failure and does not transmit RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS

3C-17. Irregular Procedure – Verify V'

Test Objective

Verify the Repeater DUT considers it a failure of authentication and does not send RepeaterAuth_Send_ReceiverID_List message when the downstream repeater provides a value for V' that does not match V.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '1B-03 Irregular Procedure – Verify V''

<Test Case>

Same as '1B-03 Irregular Procedure – Verify V''

[Authentication with Repeaters]

(STEP 3C-17-1)

- ☐ DUT does not transmit RepeaterAuth_Send_ReceiverID_List to TE (pseudo-Source)
  - ➢ If DUT transmits RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-5)
- ☐ If DUT treats the mismatch of V and invalid V' from downstream TE pseudo-Repeater as an authentication failure and does not transmit RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS

3C-18. Irregular Procedure – DEVICE_COUNT

Test Objective

Verify the Repeater DUT asserts MAX_DEVS_EXCEEDED bit in RepeaterAuth_Send_ReceiverID_List message if the computed DEVICE_COUNT exceeds 31.

Required Test Method

<Connection Setup>

Same as '3C-13 Regular Procedure – Propagation of HDCP2_0_REPEATER_DOWNSTREAM flag'

<Configuration of TE (pseudo-Repeater)>

Same as '3C-12 Regular Procedure – Transmitter – DUT – Repeater (With stored km)' except for the following change:

- ☐ TE (pseudo-Repeater) sets DEVICE_COUNT = 31

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in '3C-12 Regular Procedure – Transmitter – DUT – Repeater (With stored k_m)' are performed.

[Authentication with Repeaters]

(STEP 3C-18-1)

- ☐ TE (pseudo-Repeater) sends RepeaterAuth_Send_ReceiverID_List
- ☐ DUT disables HDCP encryption, if enabled, after computing DEVICE_COUNT
  - ➢ If DUT disables encryption before TE (pseudo-Repeater) transmits RepeaterAuth_Send_ReceiverID_List message, then FAIL (Ref-3C-1)
  - ➢ If DUT does not disable encryption after computing DEVICE_COUNT, then FAIL (Ref-3C-1)

(STEP 3C-18-2)

- ☐ DUT sets MAX_DEVS_EXCEEDED flag and transmits RepeaterAuth_Send_ReceiverID_List to TE (pseudo-source)
  - ➢ If DUT does not transmit RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-1)
  - ➢ If MAX_DEVS_EXCEEDED is 'FALSE', then FAIL (Ref-3C-1)

- ☐ If DUT considers it an authentication failure when topology maximums are exceeded and signals MAX_DEVS_EXCEEDED error in RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS

3C-19. Irregular Procedure – DEPTH

Test Objective

Verify the Repeater DUT asserts MAX_CASCADE_EXCEEDED bit in RepeaterAuth_Send_ReceiverID_List message if the computed DEPTH for it exceeds four.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init' except for the following change:

- ☐ TE (pseudo-Repeater) sets DEPTH = 4

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in '3C-12 Regular Procedure – Transmitter – DUT – Repeater (With stored k_m)' are performed.

[Authentication with Repeaters]

(STEP 3C-19-1)

- ☐ TE (pseudo-Repeater) sends RepeaterAuth_Send_ReceiverID_List
- ☐ DUT disables HDCP encryption, if enabled, after computing DEPTH
  - ➢ If DUT disables encryption before TE (pseudo-Repeater) transmits RepeaterAuth_Send_ReceiverID_List message, then FAIL (Ref-3C-1)
  - ➢ If DUT does not disable encryption after computing DEPTH, then FAIL (Ref-3C-1)

(STEP 3C-19-2)

- ☐ DUT sets MAX_CASCADE_EXCEEDED flag and transmits RepeaterAuth_Send_ReceiverID_List to TE (pseudo-source)
  - ➢ If DUT does not transmit RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-1)
  - ➢ If MAX_CASCADE_EXCEEDED is 'FALSE', then FAIL (Ref-3C-1)

- ☐ If DUT considers it an authentication failure when topology maximums are exceeded and signals MAX_CASCADE_EXCEEDED error in RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS

3C-20. Irregular Procedure – MAX_DEVS_EXCEEDED

Test Objective

Verify the Repeater DUT asserts MAX_DEVS_EXCEEDED bit in RepeaterAuth_Send_ReceiverID_List message when it receives a MAX_DEVS_EXCEEDED status from the downstream pseudo-Repeater.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '1B-04 Irregular Procedure – MAX_DEVICES_EXCEEDED'

<Test Case>

Same as '1B-04 Irregular Procedure – MAX_DEVICES_EXCEEDED'

[Authentication with Repeaters]

(STEP 3C-20-1)

- ☐ DUT sets MAX_DEVS_EXCEEDED flag and transmits RepeaterAuth_Send_ReceiverID_List to TE (pseudo-source)
  - ➢ If DUT does not transmit RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-1)
  - ➢ If MAX_DEVS_EXCEEDED is 'FALSE', then FAIL (Ref-3C-1)
- ☐ If DUT treats the reception of MAX_DEVS_EXCEEDED from downstream TE pseudo-Repeater as an authentication failure and signals MAX_DEVS_EXCEEDED error in RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS

3C-21. Irregular Procedure – MAX_CASCADE_EXCEEDED

Test Objective

Verify the Repeater DUT asserts MAX_CASCADE_EXCEEDED bit in RepeaterAuth_Send_ReceiverID_List message when it receives a MAX_CASCADE_EXCEEDED status from the downstream pseudo-Repeater.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '1B-05 Irregular Procedure – MAX_CASCADE_EXCEEDED'

<Test Case>

Same as '1B-05 Irregular Procedure – MAX_CASCADE_EXCEEDED'

[Authentication with Repeaters]

(STEP 3C-21-1)

- ☐ DUT sets MAX_CASCADE_EXCEEDED flag and transmits RepeaterAuth_Send_ReceiverID_List to TE (pseudo-source)
  - If DUT does not transmit RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-1)
  - If MAX_CASCADE_EXCEEDED is 'FALSE', then FAIL (Ref-3C-1)
- ☐ If DUT treats the reception of MAX_CASCADE_EXCEEDED from downstream TE pseudo-Repeater as an authentication failure and signals MAX_CASCADE_EXCEEDED error in RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source) and does not transmit RepeaterAuth_Send_Ack to downstream TE(pseudo-Repeater), then PASS

3C-22. Regular Procedure – Repeater with zero downstream device

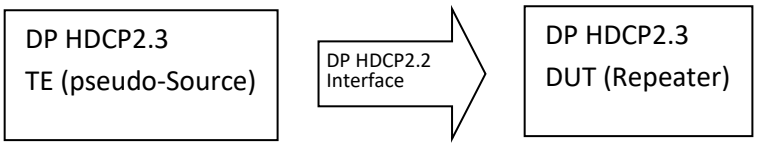
Test Objective

Verify the Repeater DUT having no downstream devices either do the authentication with upstream as a Receive or does not do the authentication.

Required Test Method

<Connection Setup>

- ☐ Connect TE(pseudo-Source) to the upstream HDCP-protected Interface Port of DUT



<Test Case>

DUT (Repeater) should follow either one of two possible cases.

[Test Case 1: No authentication]

(STEP 3C-22-1)

- ☐ DUT Send *Receiver disconnect Indication* to TE(pseudo-Source)
  - ➢ If DUT sends *Receiver Connect Indication*, then FAIL (Ref-3C-6)
- ☐ If DUT keeps *Receiver disconnect Indication* so that TE(pseudo-Source) does not start authentication, than PASS (Ref-3C-6)

[Test Case 2: Authentication as a Receiver]

(STEP 3C-22-2)

- ☐ DUT Send *Receiver Connect Indication* to TE(pseudo-Source)
- ☐ If DUT performs authentication as a Receiver instead of a Repeater(Ref-3C-6)
  - ➢ If DUT follows the steps specified in “2C-01 Regular Procedure – with transmitter”, then PASS Otherwise, FAIL

3C-23. Regular Procedure – Propagation of HDCP2_0_REPEATER_DOWNSTREAM flag

Test Objective

Verify the Repeater DUT propagates the HDCP2_0_REPEATER_DOWNSTREAM flag upstream when provided by the downstream repeater in RepeaterAuth_Send_ReceiverID_list message.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init' except for the following change:

- ☐ TE (pseudo-Repeater) sets HDCP2_0_REPEATER_DOWNSTREAM to '1'

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in '3C-11 Regular Procedure – Transmitter – DUT – Repeater (With stored k_m)' are performed.

[Authentication with Repeaters]

(STEP 3C-23-1)

- ☐ TE (pseudo-Repeater) sends RepeaterAuth_Send_ReceiverID_List

(STEP 3C-23-2)

- ☐ DUT transmits RepeaterAuth_Send_ReceiverID_List to TE (pseudo-Source)
  - ➢ If DUT does not transmit RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-5)
  - ➢ If DUT does not report HDCP2_0_REPEATER_DOWNSTREAM = 1 in RepeaterAuth_Send_ReceiverID_list, then FAIL (Ref-3C-8)
- ☐ If DUT propagates downstream indication of HDCP2_0_REPEATER_DOWNSTREAM status to upstream TE (pseudo-Source) as part of RepeaterAuth_Send_ReceiverID_List, then PASS

3C-24. Regular Procedure – Propagation of HDCP1_DEVICE_DOWNSTREAM flag

Test Objective

Verify the Repeater DUT propagates the HDCP1_DEVICE_DOWNSTREAM flag upstream when provided by the downstream repeater in RepeaterAuth_Send_ReceiverID_list message.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init' except for the following change:

- ☐ TE (pseudo-Repeater) sets HDCP1_DEVICE_DOWNSTREAM to '1'

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in '3C-11 Regular Procedure – Transmitter – DUT – Repeater (With stored k_m)' are performed

[Authentication with Repeaters]

(STEP 3C-24-1)

- ☐ TE (pseudo-Repeater) sends RepeaterAuth_Send_ReceiverID_List

(STEP 3C-24-2)

- ☐ DUT transmits RepeaterAuth_Send_ReceiverID_List to TE (pseudo-Source)
  - ➢ If DUT does not transmit RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-5)
  - ➢ If DUT does not report HDCP1_DEVICE_DOWNSTREAM = 1 in RepeaterAuth_Send_ReceiverID_list, then FAIL (Ref-3C-8)
- ☐ If DUT propagates downstream indication of HDCP1_DEVICE_DOWNSTREAM status to upstream TE (pseudo-Source) as part of RepeaterAuth_Send_ReceiverID_List, then PASS

3C-25. Regular Procedure – Content Stream Management

Test Objective

Verify the Repeater DUT propagates the Content Stream Management function as determined by the upstream source.

Required Test Method

<Connection Setup>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Configuration of TE (pseudo-Repeater)>

Same as '3C-12 Regular Procedure – Receiver disconnect after AKE_Init'

<Test Case>

The steps described under [Before Starting Authentication] to [Authentication with Repeaters] in '3C-12 Regular Procedure – Transmitter – DUT – Repeater (With stored k_m)' are performed.

(STEP 3C-25-1)

- ☐ TE (pseudo-Source) sends RepeaterAuth_Stream_Manage message

(STEP 3C-25-2)

- ☐ DUT transmits RepeaterAuth_Stream_Ready message within 100ms
  - ➢ If DUT does not transmit RepeaterAuth_Stream_Ready message within 100ms, then FAIL (Ref-1B-5)
  - ➢ If M' provided in RepeaterAuth_Stream_Ready message does not match TE's calculation of M, then FAIL (Ref-1B-5)

(STEP 3C-25-3)

- ☐ DUT sends RepeaterAuth_Stream_Manage message to TE (pseudo-Repeater)
  - ➢ If DUT does not transmit RepeaterAuth_Stream_Manage message at least 100ms before transmitting the corresponding Content Stream, then FAIL (Ref-1B-5)

[Three test cases; all are performed]

[Test case 1 – Valid M']

(STEP 3C-25-4)

- ☐ TE responds with RepeaterAuth_Stream_Ready message within 100ms with valid M'
- ☐ DUT transmits stream
  - ➢ If DUT does not transmit stream referenced in RepeaterAuth_Stream_Manage message, then FAIL (Ref-1B-5)
  - ➢ If DUT transmits Content Stream earlier than 100ms after transmission of RepeaterAuth_Stream_Manage message, then FAIL (Ref-1B-5)

[Test case 2 –Invalid M']

(STEP 3C-25-5)

- ☐ TE responds with RepeaterAuth_Stream_Ready message within 100ms with invalid M'
- ☐ DUT does not transmit stream
  - ➢ If DUT transmits stream referenced in RepeaterAuth_Stream_Manage message, then FAIL (Ref-1B-5)
- ☐

4. Reference

Refer to the High-bandwidth Digital Content Protection System – Mapping HDCP to DisplayPort Revision 2.3.

Ref-1A. Downstream procedure with Receiver

Ref-1A-1.

Reference	Requirement
2.8 HDCP Transmitter State Diagram Page 28	Transmitter's decision to begin authentication is dependent on events such as detection of an HDCP Receiver, availability of premium content or other implementation dependent details in the transmitter. In the event of authentication failure, an HDCP Receiver must be prepared to process subsequent authentication attempts. The HDCP Transmitter may cease to attempt authentication for transmitter-specific reasons, which include receiving a Receiver Disconnected Indication or after a certain number of authentication re-attempts by the transmitter. The transmitter must not initiate authentication unless it determines that the receiver is HDCP-capable.

Ref-1A-2.

Reference	Requirement
State H1: Transmit Low-value Content Page 29	**State H1: Transmit Low-value Content.** In this state the transmitter should begin sending an unencrypted signal with HDCP Encryption disabled. The transmitted signal can be a low value content or informative on-screen display. This will ensure that a valid video signal is displayed to the user before and during authentication. **Transition H1: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.
State A5: Authenticated Page 31	**State A5: Authenticated.** At this time, and at no prior time, the HDCP Transmitter has completed the authentication protocol. A periodic Link Synchronization is performed to maintain cipher synchronization between HDCP Transmitter and HDCP Receiver.

Ref-1A-3.

Reference	Requirement
2.2 Authentication and Key Exchange Page 12	Authentication and Key Exchange (AKE) is the first step in the authentication protocol. Figure 2-1 and Figure 2-2 illustrates the AKE. The HDCP Transmitter (*Device A*) can initiate authentication at any time, even before a previous authentication exchange has completed. The HDCP Transmitter initiates a new HDCP Session by sending a new r_{tx} and TxCaps as part of the

	authentication initiation message, AKE_Init. Message formats are defined in Section 4.2. • The transmitter may attempt to read AKE_Send_Cert sooner than 100ms and the receiver may respond with AUX_DEFERs until the message is ready to be read. The transmitter aborts the authentication protocol if (a) the AKE_Send_Cert message is not available for the transmitter to start the read after 100ms or (b) the transmitter has not received the entire AKE_Send_Cert message within 110ms since the initiation of the AKE_Send_Cert message read.
State A1: Exchange K_m Page 30	**State A1: Exchange K_m.** In this state, the HDCP Transmitter initiates authentication by writing AKE_Init message to the HDCP Receiver. It reads AKE_Send_Cert from the receiver within the time period specified in Section 2.2 If the HDCP Transmitter does not have km stored corresponding to the Receiver ID, it generates Ekpub(km) and sends Ekpub(km) as part of the AKE_No_Stored_km message to the receiver after verification of signature on certrx. It performs integrity check on the SRM and checks to see whether the Receiver ID of the connected HDCP Device is in the revocation list. It computes H, receives AKE_Send_H_prime message from the receiver containing H' within the time period specified in section 2.2 and Compares H' against H. If the HDCP Transmitter has km stored corresponding to the Receiver ID, it writes AKE_Stored_km message containing Ekh(km) and m to the receiver, performs integrity check on the SRM, checks to see whether the Receiver ID of the connected HDCP Device is in the revocation list. It computes H, reads AKE_Send_H_prime message from the receiver containing H' within the time period specified in Section 2.2 and compares H' against H. If the HDCP Transmitter does not have a km stored corresponding to the Receiver ID, it implements pairing with the HDCP receiver as explained in Section 2.2.1.

Ref-1A-4.

Reference	Requirement
2.2.1 Pairing Page 15	To speed up the AKE process, pairing must be implemented between the HDCP Transmitter and HDCP Receiver in parallel with AKE. When AKE_No_Stored_km message is received from the transmitter, it is an indication to the receiver that the transmitter does not have k_m stored corresponding to the receiver. In this case, after computing *H'*, the HDCP Receiver ☐ Computes 128-bit k_h = SHA-256($kpriv_{rx}$)[127:0].

	☐ Generates 128-bit $E_{kh}(k_m)$ by encrypting k_m with k_h using AES as illustrated in Figure 2.3. ☐ Asserts PAIRING_AVAILABLE and generates CP_IRQ when AKE_Send_Pairing_Info to the transmitter containing the 128-bit $E_{kh}(k_m)$ is available for the transmitter to read. This message must be available for the transmitter to read within 200ms from the time the transmitter begins reading the AKE_Send_H_Prime message parameters from the HDCP Receiver. The transmitter reads the PAIRING_AVAILABLE status bit in the RxStatus register as soon as it receives the CP_IRQ interrupt. If the PAIRING_AVAILABLE status bit is set, the transmitter reads the AKE_Send_Pairing_Info message. The transmitter may attempt to read AKE_Send_Pairing_Info message sooner than 200ms and the receiver may respond with AUX_DEFERs until the message is ready to be read. Authentication fails and the transmitter aborts the authentication protocol if (a) the AKE_Send_Pairing_Info message is not available for the transmitter to start the read after 200ms or (b) the transmitter has not received the entire AKE_Send_Pairing_Info message withing 5ms since the initiation of the AKE_Send_Pairing_Info message read. On reading AKE_Send_Pairing_Info message, the HDCP Transmitter may persistently store *m* (which is r_{tx} concatenated with $r_{rx}(r_{tx}||r_{rx})$, k_m and $E_{kh}(k_m)$ along with *Receiver ID*. Note: The HDCP Transmitter may store in its non-volatile storage *m*, k_m, and $E_{kh}(k_m)$ along with corresponding *Receiver ID*s of all HDCP Receivers with which pairing was implemented by the HDCP Transmitter.

Ref-1A-5.

Reference	Requirement
2.3 Locality Check Page 16	Locality check is performed after AKE and pairing. The HDCP Transmitter initiates locality check by sending a 64-bit pseudo-random nonce r_n to the downstream receiver. The HDCP Transmitter • Initiates locality check by sending LC_Init message containing a 64-bit pseudo-random nonce r_n to the HDCP Receiver. • Sets its watchdog timer to 16ms. The LC_Send_L_prime message must be received by the transmitter within 16ms from the time the transmitter finishes writing the LC_Init message parameters to the HDCP Receiver i.e. 16ms from the time the last byte of m has been written to the time the last byte of LC_Send_L_prime message has been received. If the LC_Send_L_prime message is not received by the transmitter within 16ms, locality check fails and the transmitter aborts the authentication protocol.

	• Computes L = HMAC-SHA256(r_n, k_d XOR r_{rx}) where HMAC-SHA256 is computed over r_n and the key used for HMAC is k_d XOR r_{rx}, where r_{rx} is XORed with the least-significant 64-bits of k_d. • On receiving LC_Send_L_prime message, compares L and *L'*. Locality check fails if L is not equal to *L'*.
State A2: Locality Check Page 30	**State A2: Locality Check.** In this state, the HDCP Transmitter implements the locality check as explained in Section 2.3 with the HDCP Receiver.

Ref-1A-6.

Reference	Requirement
2.4 Session Key Exchange Page 18	Successful completion of AKE and locality check stages affirms to HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. Session Key Exchange (SKE) is initiated by the HDCP Transmitter after a successful locality check. The HDCP Transmitter sends encrypted Session Key to the HDCP Receiver at least 200 ms before enabling HDCP Encryption and beginning the transmission of HDCP Content. If the attached HDCP Receiver is not an HDCP Repeater, the HDCP Transmitter also writes the Type value corresponding to the Content Stream to be transmitted to the HDCP Receiver at least 200 ms before enabling HDCP Encryption. HDCP Encryption may be enabled 200 ms after the transmission of the encrypted Session Key and Type value to the HDCP Receiver and at no time prior. Type value is written only to HDCP Receivers that are not HDCP Repeaters. Content encrypted with the Session Key ks starts to flow between the HDCP Transmitter and HDCP Receiver. HDCP Encryption must be enabled only after successful completion of AKE, locality check and SKE stages. During SKE, the HDCP Transmitter • Generates a pseudo-random 128-bit session key k_s and 64-bit pseudo-random number r_{iv}. • Performs key derivation as explained in Section 2.7 to generate 128-bit $dkey_2$ where $dkey_2$ is the derived key when ctr=2. • Computes 128-bit $E_{dkey}(k_s) = k_s$ XOR ($dkey_2$ XOR r_{rx}), where r_{rx} is XORed with the least-significant 64-bits of $dkey_2$. • Writes SKE_Send_Eks message containing $E_{dkey}(k_s)$ and r_{iv} to the HDCP Receiver.
State A3: Exchange k_s Page 31	**State A3: Exchange k_s.** The HDCP Transmitter sends encrypted Session Key, $E_{dkey}(k_s)$, and r_{iv} to the HDCP Receiver as part of the SKE_Send_Eks message. It may enable HDCP Encryption 200ms after sending encrypted Session Key. HDCP Encryption must be enabled only after successful completion of AKE, locality check and SKE stages.

Ref-1A-7.

Reference	Requirement
Transition Any State: H0. Page 29	**Transition Any State: H0.** Reset conditions at the HDCP Transmitter or disconnect of the connected HDCP capable receiver cause the HDCP Transmitter to enter the No Receiver Attached state.
Transition H0:H1. Page 29	**Transition H0:H1.** The detection of a sink device (through Receiver Connected Indication) indicates to the transmitter that a sink device is connected and ready to display the received content. When the receiver is no longer active, the transmitter is notified through Receiver Disconnected Indication.

Ref-1A-8.

Reference	Requirement
Transition A1:H1 Page 30	**Transition A1:H1.** This transition occurs on failure of signature verification oncertrx, failure of SRM integrity check, if Receiver ID of the connected HDCP Device is in the revocation list or if there is a mismatch between H and H'. This transition also occurs if AKE_Send_H_prime message is not received within the time period specified in Section 2.2.
Transition A1:A2 Page 30	**Transition A1:A2.** The HDCP Transmitter implements locality check after successful completion of AKE and pairing.

Ref-1A-9.

Reference	Requirement
2.3 Locality Check Page 17	In the case of a locality check failure due to expiration of the watchdog timer or due to mismatch of L and L' at the HDCP Transmitter, locality check may be reattempted by the HDCP Transmitter for a maximum of 1023 additional attempts (for a maximum allowed 1024 total trials) with the transmission of an LC_Init message containing a new r_n. Failure of locality check on the first attempt and subsequent zero or more reattempts results in an authentication failure and the authentication protocol is aborted.
Transition A2: H1 Page 30	**Transition A2:H1**. This transition occurs on one or more consecutive locality check failures. Locality check fails when the watchdog timer at the HDCP Transmitter expires or on a mismatch between L and L'.

Ref-1A-10.

Reference	Requirement
3.4 Encryption Status Signaling in SST Mode Page 61	When encryption is currently enabled, BS and SR control symbols are replaced by CPBS and CPSR control symbols respectively. In the SST mode, detection of SR indicates that encryption is disabled and detection of CPSR indicates that encryption is enabled. Following the transmission or detection of CPSR, the HDCP Cipher is clocked as explained in Section 3.1 and the resulting key stream bits are used to

	encrypt the data symbols following the CPSR as explained in Section 3.2. The HDCP Cipher is not clocked when HDCP Encryption is disabled.
3.1 Data Encryption Page 54	When HDCP Encryption is applied to a timeslot in the MST mode or when HDCP Encryption is enabled in the SST mode, all data symbols (including video data, secondary data and dummy symbols) must be encrypted and K-codes must not be encrypted. Section 3.3 and 3.4 explains in detail the encryption signaling protocol that is used to enable/disable HDCP Encryption.

Ref-1A-11.

Reference	Requirement
2.6.2 Link Integrity Check in SST Mode Page 26	To Perform link integrity check in SST mode, Bit 5 of VB-ID is used to transmit a known 16-bit pattern, 0x531F, from the transmitter to the receiver one bit at a time. This pattern is referred to as LINK_VERIFICATION_PATTERN. The VB-ID is transmitted on all lanes after every BS/SR/CPBS/CPSR symbol, as described in Display-port specification. 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.
	On Detecting an unrecoverable loss of cipher synchronization the HDCP Receiver must assert the LINK_INTEGRITY_FAILURE bit in the RXStatus register and generate a CP_IRQ interrupt. On receiving a CP_IRQ interrupt, the HDCP Transmitter is required to read the RxSstatus 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 AKE_Init message.

Ref-1B. Downstream procedure with Repeater

Ref-1B-1.

Reference	Requirement
Transition A7:A8 Page 31	**Transition A7:A8.** This transition occurs on successful verification of the most significant 128-bits of *V* and *V',* none of the reported *Receiver IDs* are in the current revocation list, the HDCP Transmitter does not detect a roll-over of *seq_num_V* and the downstream topology does not exceed specified maximum.

Transition A8:A9 page 31	**Transition A8:A9.** This transition occurs after the RepeaterAuth_Send_Ack message has been written to the repeater.

Ref-1B-2.

Reference	Requirement
Section 2.5 Authentication with Repeaters Page 21	After transmitting the SKE_Send_Eks message, the HDCP Transmitter, having determined that REPEATER received earlier in the protocol is set, sets a three second watchdog timer. If the asserted READY status is not received by the HDCP Transmitter within a maximum-permitted time of three seconds after transmitting SKE_Send_Eks message, authentication of the HDCP Repeater fails. With this failure, the HDCP Transmitter disables HDCP Encryption and aborts the authentication protocol with the HDCP Repeater. The HDCP Repeater makes available the most significant 128-bits of *V'* for the transmitter to read as part of the RepeaterAuth_Send_ReceiverID_List message. Whenever the HDCP Transmitter reads the RepeaterAuth_Send_ReceiverID_List message, it verifies the integrity of the Receiver ID list by computing *V* and comparing the most significant 128-bits of *V* and *V'*. If the values do not match, authentication fails, the authentication Protocol is aborted and HDCP Encryption is disabled. On successful verification of Receiver ID list and topology information, i.e. if the values match, none of the reported *Receiver IDs* are in the current revocation list (in the case of the most upstream HDCP Transmitter), the HDCP Transmitter does not detect a roll-over of *seq_num_V,* the downstream topology does not exceed specified maximums (explained below), the HDCP Transmitter (including downstream port of HDCP Repeater) writes the least significant 128-bits of *V* to the HDCP Repeater as part of the RepeaterAuth_Send_Ack message. Every RepeaterAuth_Send_ReceiverID_List message from the repeater to the transmitter must be followed by a RepeaterAuth_Send_Ack message from the transmitter to repeater on successful verification of Receiver ID list and topology information by the transmitter.
Transition A6:H1 page 31	Transition A6:H1 The watchdog timer expires before the READY has been asserted by the repeater.

Ref-1B-3.

Reference	Requirement
Section 2.5 Authentication with Repeaters Page 22	HDCP Repeaters must be capable of supporting DEVICE_COUNT values of up to 31 and DEPTH values of up to 4. If the computed DEVICE_COUNT for an HDCP Repeater exceeds 31, the error is referred to as MAX_DEVS_EXCEEDED error. The repeater sets MAX_DEVS_EXCEEDED bit to one in the RepeaterAuth_Send_ReceiverID_List message. If the computed DEPTH for an HDCP Repeater exceeds four, the error is referred to as MAX_CASCADE_EXCEEDED error. The repeater sets MAX_CASCADE_EXCEEDED bit to one in the RepeaterAuth_Send_ReceiverID_List message. When an HDCP Repeater receives a MAX_DEVS_EXCEEDED or a MAX_CASCADE_EXCEEDED error from a downstream HDCP Repeater, it must propagate the error to the Upstream HDCP Transmitter and assert the READY bit and assert the CP_IRQ interrupt. If a transmitter receives these errors, it must not read the most significant 128-bits of *V',* Receiver ID list and *seq_num_V* from the HDCP Repeater. Authentication fails if the Topology maximums are exceeded. HDCP Encryption is disabled and the Authentication protocol is aborted.
Transition A7:H1 Page 29	**Transition A7:H1**. This transition is made if a mismatch occurs between the most significant 128-bits of *V* and *V'*. This transition is also made if any of the *Receiver IDs* in the Receiver ID list are found in the current revocation list or if the HDCP Transmitter detects a roll-over of *seq_num_V.* A MAX_CASCADE_EXCEEDED or MAX_DEVS_EXCEEDED error also causes this transition.

Ref-1B-4.

Reference	Requirement
Section 2.5 Authentication with Repeaters Page 21	After transmitting the SKE_Send_Eks message, the HDCP Transmitter, having determined that REPEATER received earlier in the protocol is set, sets a three second watchdog timer and polls the HDCP Repeater's READY status bit and if it's set, along with a non-zero Message_Size, reads the RepeaterAuth_Send_ReceiverID_List message. If the asserted READY status is not received by the HDCP Transmitter within a maximum-permitted time of three seconds after transmitting SKE_Send_Eks message, authentication of the HDCP Repeater fails. With this failure, the HDCP Transmitter disables HDCP Encryption and aborts the authentication protocol with the HDCP Repeater. When READY is set and the CP_IRQ interrupt asserted, the HDCP Transmitter reads the RepeaterAuth_Send_ReceiverID_List message. The HDCP Repeater

	makes available the most significant 128-bits of *V'* for the transmitter to read as part of the RepeaterAuth_Send_ReceiverID_List message. Whenever the HDCP Transmitter reads the RepeaterAuth_Send_ReceiverID_List message, it verifies the integrity of the Receiver ID list by computing *V* and comparing the most significant 128-bits of *V* and *V'*. If the values do not match, authentication fails, the authentication protocol is aborted and HDCP Encryption is disabled. On successful verification of Receiver ID list and topology information, i.e. if the values match, none of the reported *Receiver IDs* are in the current revocation list (in the case of the most upstream HDCP Transmitter), the HDCP Transmitter does not detect a roll-over of *seq_num_V,* the downstream topology does not exceed specified maximums (explained below), the HDCP Transmitter (including downstream port of HDCP Repeater) writes the least significant 128-bits of *V* to the HDCP Repeater as part of the RepeaterAuth_Send_Ack message. Every RepeaterAuth_Send_ReceiverID_List message from the repeater to the transmitter must be followed by a RepeaterAuth_Send_Ack message from the transmitter to repeater on successful verification of Receiver ID list and topology information by the transmitter.
Transition A7:A8 Page 31	**Transition A7:A8**. This transition occurs on successful verification of the most significant 128-bits of V and V', none of the reported Receiver IDs are in the current revocation list, the HDCP Transmitter does not detect a roll-over of seq_num_V and the downstream topology does not exceed specified maximums.

Ref-1B-5.

Reference	Requirement
Section 2.5.2 Downstream Propagation of Content Stream Management Information Page 24	The HDCP Transmitter propagates Content Stream management information, which includes Type value assigned to the Content Stream, using the RepeaterAuth_Stream_Manage message to the attached HDCP Repeater. The HDCP Transmitter executes this step after successful completion of Session Key Exchange and before beginning the transmission of a Content Stream after HDCP Encryption to the HDCP Repeater. The RepeaterAuth_Stream_Manage message from an HDCP Transmitter to the attached HDCP Repeater identifies any restriction, as specified by the Upstream Content Control Function, on the transmission of the Content Stream to specific devices. Type values are assigned to the Content Stream by the most upstream HDCP Transmitter based on instructions received from the Upstream Content

	Control Function. The exact mechanism used by the Upstream Content Control Function to instruct the HDCP Transmitter is outside the scope of this specification. Type 0 Content Stream (see Section 4.2.12) may be transmitted by the HDCP Repeater to all HDCP Devices. Type 1 Content Stream (see Section 4.2.12) must not be transmitted by the HDCP Repeater through its HDCP-protected Interface Ports connected to HDCP 1.x-compliant Devices, HDCP 2.0-compliantdevices, and HDCP 2.1-compliant Devices. The HDCP Transmitter must write the RepeaterAuth_Stream_Manage message specifying Type value assigned to the Content Stream, to the attached HDCP Repeater at least 110ms before the transmission of the corresponding Content Streams after HDCP Encryption. The HDCP Transmitter must only send the RepeaterAuth_Stream_Manage message corresponding to the encrypted Content Stream it will transmit to the HDCP Repeater. The HDCP Transmitter initializes *seq_num_M* to 0 at the beginning of the HDCP Session i.e. after AKE_Init is sent. It is incremented by one after the transmission of every RepeaterAuth_Stream_Manage message. On receiving the RepeaterAuth_Stream_Manage message, the HDCP Repeater computes *M'* as given below. HMAC-SHA256 is computed over the concatenation of *StreamID_Type* (see Section 4.2.12) and *seq_num_M* values received as part of the RepeaterAuth_Stream_Manage message. All values are in big-endian order. The key used for HMAC is SHA256(kd). seq_num_M must never be reused during an HDCP Session for the computation of M' (or M). If seq_num_M rolls over, the HDCP Transmitter must disable HDCP Encryption if encryption is enabled, restart authentication by the transmission of a new AKE_Init message.
Section 2.5.2 Downstream Propagation of Content Stream Management Information Page 25	The RepeaterAuth_Stream_Ready message must be available for the transmitter to start the read within 100 ms from the time the transmitter finishes writing the RepeaterAuth_Stream_Manage message parameters to the HDCP Receiver. Every RepeaterAuth_Stream_Manage message from the transmitter to the repeater must be followed by a RepeaterAuth_Stream_Ready message from the repeater to the transmitter. When the RepeaterAuth_Stream_Ready message is read, the HDCP Transmitter verifies the integrity of the message by computing M and comparing this value to M'. If M is equal to M', the HDCP Transmitter may transmit the Content Streams identified in the corresponding RepeaterAuth_Stream_Manage message. The transmitter may attempt to read RepeaterAuth_Stream_Ready message sooner than 100ms and the receiver may respond with AUX_DEFERs until the message is ready to be read. The HDCP Transmitter must not transmit the Content Streams identified in the corresponding RepeaterAuth_Stream_Manage message if

	(a) the RepeaterAuth_Stream_Ready message is not available for the transmitter to start the read after 100ms or (b) the transmitter has not received the entire RepeaterAuth_Stream_Ready message within 7ms since the initiation of the RepeaterAuth_Stream_Ready message read or (c) if M is not equal to M'. Type value is assigned to each Content Stream through the successful transmission/reception of a single RepeaterAuth_Stream_Manage message. The Content Stream shall be associated with such Type value throughout the HDCP Session.

Ref-2. Receiver

Ref-2C. Upstream procedure with Transmitter

Ref-2C-1.

Reference	Requirement
Transition Any State:H0 Page 29	**Transition Any State:H0.** Reset conditions at the HDCP Transmitter or disconnect of the connected HDCP capable receiver cause the HDCP Transmitter to enter the No Receiver Attached state.
Transition H0:H1 Page 29	**Transition H0:H1.** The detection of a sink device (through Receiver Connected Indication) indicates to the transmitter that a sink device is connected and ready to display the received content. When the receiver is no longer active, the transmitter is notified through Receiver Disconnected Indication.

Ref-2C-2.

Reference	Requirement
State B1:Compute k_m Page 33	**State B1: Compute k_m.** In this state, the HDCP Receiver makes the AKE_Send_Cert message available for reading by the transmitter in response to AKE_Init. If AKE_No_Stored_km is received, the receiver decrypts km with kprivrx, calculates H'. It makes AKE_Send_H_prime message available for reading immediately after computation of H' to ensure that the message is received by the transmitter within the time period specified in Section 2.2. If AKE_Stored_kmis received, the HDCP Receiver decrypts Ekh(km) to derive km and calculates H'. It makes AKE_Send_H_prime message available for reading immediately after computation of H' to ensure that the message is received by the transmitter within the time period specified in Section 2.2. If AKE_No_Stored_km is received, this is an indication to the HDCP Receiver that the HDCP Transmitter does not contain a km stored corresponding to its Receiver ID. It implements pairing with the HDCP Transmitter as explained in Section 2.2.1
Transition H0:H1 Page 29	**Transition H0:H1.** The detection of a sink device (through Receiver Connected Indication) indicates to the transmitter that a sink device is connected and ready to display the received content. When the receiver is no longer active, the transmitter is notified through Receiver Disconnected Indication.

Ref-2C-3.

Reference	Requirement
Section 2.2 Authentication and Key Exchange Page 13	Reads AKE_Send_Cert from the receiver containing *certrx*, a 64-bit pseudo-random value (r*rx*) and *RxCaps.* REPEATER bit in *RxCaps* indicates whether the connected receiver is an HDCP Repeater. If REPEATER is set to one, it indicates the receiver is an HDCP Repeater. If REPEATER is zero, the receiver is not an HDCP Repeater.

Section 4.2.2 AKE_Send_Cert (Read) Page 52 and 64	The HDCP Receiver sets REPEATER to 'true' if it is an HDCP Repeater and 'false' if it is an HDCP Receiver that is not an HDCP Repeater. When REPEATER = 'true', the HDCP Receiver supports downstream connections as permitted by the Digital Content Protection LLC license. This bit does not change while the HDCP receiver is active.

Ref-2C-4.

Reference	Requirement
State A2: Locality Check Page 30	**State A2: Locality Check.** In this state, the HDCP Transmitter implements the locality check as explained in Section 2.3 with the HDCP Receiver.
Transition A2:H1 Page 30	**Transition A2:H1.** This transition occurs on one or more consecutive locality check failures. Locality check fails when the watchdog timer at the HDCP Transmitter expires or on a mismatch between L and L'.

Ref-3. Repeater

Ref-3C Upstream procedure with Transmitter

Ref-3C-1.

Reference	Requirement
Section 2.5 Authenticating with Repeaters Page 22	HDCP Repeaters must be capable of supporting DEVICE_COUNT values of up to 31 and DEPTH values of up to 4. If the computed DEVICE_COUNT for an HDCP Repeater exceeds 31, the error is referred to as MAX_DEVS_EXCEEDED error. The repeater sets MAX_DEVS_EXCEEDED bit to one in the RepeaterAuth_Send_ReceiverID_List message. If the computed DEPTH for an HDCP Repeater exceeds four, the error is referred to as MAX_CASCADE_EXCEEDED error. The repeater sets MAX_CASCADE_EXCEEDED bit to one in the RepeaterAuth_Send_ReceiverID_List message. When an HDCP Repeater receives a MAX_DEVS_EXCEEDED or a MAX_CASCADE_EXCEEDED error from a downstream HDCP Repeater, it must propagate the error to the upstream HDCP Transmitter, assert the READY bit and assert the CP_IRQ interrupt. If a transmitter receives these errors, it must not read the most significant 128-bits of V', Receiver ID list and seq_num_V from the HDCP Repeater.

Ref-3C-2.

Reference	Requirement
Section 2.5 Authenticating with Repeaters Page 21	The HDCP Repeater propagates topology information upward through the connection tree to the HDCP Transmitter. 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 connected downstream HDCP Receiver and HDCP Repeaters. The value is calculated as the sum of the number of directly connected downstream HDCP Receiver and HDCP Repeaters plus the sum of the DEVICE_COUNT received from all connected 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 connected HDCP Repeater).

Ref-3C-3.

Reference	Requirement
Section 2.5.1 Topology Information Propagation Due to Topology Changes	When an HDCP Receiver (including HDCP Repeater) is newly connected to the HDCP Repeater or when a connected, active HDCP Receiver with which the HDCP Repeater has successfully completed the authentication protocol is

Page 21	disconnected from the HDCP Repeater, the HDCP Repeater asserts the READY status bit and the CP_IRQ interrupt and must make the RepeaterAuth_Send_ReceiverID_List message available for the upstream HDCP Transmitter to read. The RepeaterAuth_Send_ReceiverID_List message must include the Receiver IDs of all connected and active downstream HDCP Receivers with which the HDCP Repeater has successfully completed the authentication protocol. This enables upstream propagation of the most recent topology information after changes to the topology without interrupting the transmission of HDCP Content.
Section 2.5.1 Upstream Propagation of Topology Information Page 19	This stage is implemented after successful completion of Session Key Exchange. This stage is used to assemble the latest topology information at the beginning of the HDCP Session immediately following an SKE or on subsequent changes to the topology due to connect or disconnect of an HDCP Receiver or HDCP Repeater

Ref-3C-4.

Reference	Requirement
Section 2.10 HDCP Repeater State Diagrams Page 34	When the upstream HDCP-protected interface port of the HDCP Repeater is in an unauthenticated state, it signals the detection of an active downstream HDCP Receiver to the upstream HDCP Transmitter in one of the following ways. The HDCP Repeater must generate the CONNECTION_STATUS_NOTIFY message to indicate plug of an active HDCP Receiver when the most upstream HDCP transmitter is capable of operating in the MST mode. It must pulse IRQ_HPD when the most upstream HDCP Transmitter is capable of operating only in the SST mode(SST-capable only) and has enabled IRQ_HPD are collectively referred to as Receiver connected Indication in this specification. Hot Unplug is referred to as Receiver Disconnected Indication in this specification. Whenever authentication is initiated by the upstream HDCP Transmitter by sending AKE_Init, the HDCP Repeater immediately initiates authentication on all its downstream HDCP-protected interface ports if its downstream ports are in an unauthenticated state. The HDCP Repeater may cache the latest Receiver ID list and topology information received from its downstream ports. Whenever authentication is attempted by the upstream transmitter by sending AKE_Init, the HDCP Repeater may propagate the cached Receiver ID list upstream without initiating a re-authentication on all its downstream ports.
State C0: Unauthenticated. Page 41	**State C0: Unauthenticated.** The device is idle, awaiting the reception of AKE_Init from the HDCP Transmitter to trigger the authentication protocol. If a transition in to this state occurred from State C5, when State C5 is implemented in parallel with State C8, or from State C6, the HDCP Repeater

	must set the REAUTH_REQ status bit in the RxStatus register and assert CP_IRQ interrupt.
Section 2.10 HDCP Repeater State diagrams Page 35	If an HDCP Repeater has no active downstream HDCP Devices, it must authenticate as an HDCP Receiver with REPEATER bit set to zero if it wishes to receive HDCP Content, but must not pass HDCP Content to downstream devices. When the upstream HDCP-protected Interface Port of the HDCP Repeater transition in to an unauthenticated state from an authenticated state(See Transition C5:C0 and Transition C6:C0 in Section 2.10.3), the HDCP Repeater must set the REAUTH_REQ status bit in the RxStatus register and assert CP_IRQ interrupt. If the upstream HDCP Transmitter receives a CP_IRQ interrupt with REAUTH_REQ status bit set, it may initiate re-authentication with the HDCP Repeater with the transmission of a new AKE_Init message.

Ref-3C-5.

Reference	Requirement
Section 2.5.1 Upstream Propagation of Topology Information Page 19	HDCP Repeaters assemble the list of all connected downstream HDCP Receivers as the downstream HDCP-protected Interface Ports of the HDCP Repeater successfully complete the authentication protocol with connected HDCP Receivers. The list is represented by a contiguous set of bytes, with each *Receiver ID* occupying five bytes stored in big-endian order. The total length of the Receiver ID list is five bytes times the total number of connected and active downstream HDCP Devices, including downstream HDCP Repeaters, with which the HDCP Repeater has successfully completed the authentication protocol. This total number is represented in the RepeaterAuth_Send_ReceiverID_List message by the DEVICE_COUNT value. An HDCP-protected Interface Port with no active device connected adds nothing to the list. Also, the *Receiver ID* of the HDCP Repeater itself at any level is not included in its own Receiver ID list. An HDCP-protected Interface Port connected to an HDCP Receiver that is not an HDCP Repeater adds the *Receiver ID* of the connected HDCP Receiver to the list. HDCP-protected Interface Ports that have an HDCP Repeater connected add the Receiver ID list received from the connected downstream HDCP Repeater plus the *Receiver ID* of the connected HDCP Repeater itself.
Transition F1:P1 Page 38	**Transition F1:P1.** This transition occurs on failure of signature verification on $cert_{rx}$ or if there is a mismatch between H and *H'.* This transition also occurs if AKE_Send_H_prime message is not received within the time period specified in Section 2.2.
Transition F2:P1 Page 38	**Transition F2:P1.** This transition occurs on one or more consecutive locality check failures. Locality check fails when the watchdog timer at the downstream side expires or on a mismatch between L and L'.
Transition F6:P1 Page 39	**Transition F6:P1.** The watchdog timer expires before READY has been asserted by the repeater.

Transition F7:P1 Page 39	**Transition F7:P1.** This transition is made if a mismatch occurs between the most significant 128-bits of V and V'. This transition is also made if the downstream side detects a roll-over of seq_num_V. A MAX_CASCADE_EXCEEDED or MAX_DEVS_EXCEEDED error also causes this transition.

Ref-3C-6.

Reference	Requirement
Section 2.10 HDCP Repeater State Diagrams Page 35	If an HDCP Repeater has no active downstream HDCP Devices, it must authenticate as an HDCP Receiver with REPEATER bit set to zero if it wishes to receive HDCP Content, but must not pass HDCP Content to downstream devices

Ref-3C-7.

Reference	Requirement
Section 2.5.1 Upstream Propagation of Topology Information Page 20	The HDCP Repeater initializes seq_num_V to 0 at the beginning of the HDCP Session i.e. after AKE_Init is received. It is incremented by one after the transmission of every RepeaterAuth_Send_ReceiverID_List message. seq_num_V must never be reused during an HDCP Session for the computation of V (or V'). If seq_num_V rolls over, the HDCP Transmitter must detect the roll-over in the RepeaterAuth_Send_ReceiverID_List read from the HDCP Repeater and the transmitter must disable HDCP Encryption if encryption is enabled, restart authentication by the transmission of a new AKE_Init message.

Ref-3C-8.

Reference	Requirement
State C5: Assemble Receiver ID List Page 42	If any downstream port connected to an HDCP Repeater detects the HDCP2_0_REPEATER_DOWNSTREAM or HDCP1_DEVICE_DOWNSTREAM bits read from the repeater to be set to one, the upstream side sets the corresponding bits to one in the RxInfo field which is read by the upstream HDCP Transmitter as part of the RepeaterAuth_Send_ReceiverID_List message