HDCP Revision 2.2 on MHL

Compliance Test Specification

Revision 1.0

10 May 2014

Notice

Acknowledgement

Silicon Image Inc. contributed to the development of this specification.

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

Table of Contents

Introduction

Purpose and Scope

This document specifies test procedures that will be used to test devices for compliance with the HDCP on MHL Specification Revision 2.2.

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

Normative References

Digital Content Protection, LLC, “High-bandwidth Digital Content Protection System – Mapping HDCP to MHL”, Revision 2.2, September 11, 2013

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

Glossary of Terms

WARNING	DUT's operation did not meet expectations, but because this test only tests for compliance with recommendations, it cannot be treated as a failure.
PASS	No error(s) were detected in the DUT's operation, although the DUT may have WARNING item(s).
FAIL	Error(s) were detected in the DUT's operation.

Product Capability Parameter (PCP)

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

Source Capability

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

HDCP Mobile High-Definition Link (MHL) Compliance Test Specification

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

1. Transmitter Test

Transmitter's (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).
>
> Note: For all authentication failures (except a failure of SRM integrity or *Receiver ID* in revocation list), the Tx must re-attempt authentication at least once (Ref-1A-1).

1A. Downstream procedure with Receiver

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

1A-01. Regular Procedure – With previously connected Receiver (With stored k_m)

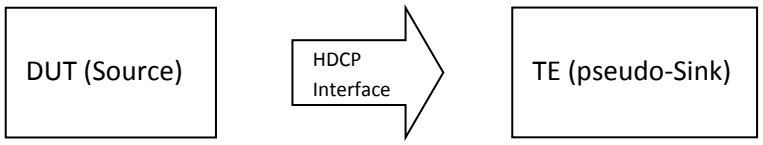
Test Objective

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
	RxCaps:VERSION	0x02
	r_{rx}	Valid
	$cert_{rx}$	Valid
AKE_Send_H_prime	H'	Valid (within 200 ms 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 20 ms timeout)

<Test Case>

[Before Starting Authentication]

(STEP 1A-01-1)

☐ TE asserts HPD

- ☐ DUT should read HDCP2Version register
  - ➢ If DUT does not read HDCP2Version register, then WARNING (Ref-1A-1)
- ☐ DUT may begin transmitting 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 transmit AKE_Init within 10 seconds of TE asserting HPD, then FAIL (Ref-1A-3)
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)

(STEP 1A-01-3)

- ☐ TE sends AKE_Send_Cert message

  NOTE: TE (Sink) sends message to Source by setting the message size in RxStatus (0x70) of HDCP port. Source polls the RxStatus and if message size is not 0, it reads out the message from Read_Message (0x80) of HDCP port
- ☐ DUT sends AKE_Stored_km 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 within 1 sec
    - TE generates $E_{kh}(k_m)$ and sends AKE_Send_Pairing_Info message within 200 ms
  - ➢ If DUT sends AKE_Stored_km message
    - TE computes *H’* and sends AKE_Send_H_prime message within 200 ms 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 5 seconds, then FAIL (Ref-1A-5)
- ☐ TE computes L' and sends LC_Send_L_prime message within the 20 ms timeout at 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, then FAIL (Ref-1A-6)

(STEP 1A-01-6)

- ☐ DUT enables HDCP encryption 200 ms after transmission of SKE_Send_Eks message
  - If DUT enables HDCP encryption in less than 200 ms, then FAIL (Ref-1A-6)
  - If DUT does not enable HDCP encryption between 200 and 10 s, then FAIL (Ref-1A-6)
- ☐ If DUT successfully completes the authentication process, then PASS.

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

<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 de-asserts HPD after AKE_Init message
- ☐ TE asserts HPD

(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 asserted HPD 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 Meth$_o$d

<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 de-asserts HPD after AKE_Stored_km or AKE_No_Stored_km message
- ☐ TE asserts HPD

(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 asserted HPD 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.

$R_e$quired 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 de-asserts HPD after LC_Init message
- ☐ TE asserts HPD

(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 asserted HPD 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 de-asserts HPD after SKE_Send_Eks message
- ☐ TE asserts HPD

(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 enables HDCP Encryption, then FAIL (Ref-1A-2)
- ☐ If DUT re-starts Authentication and Key Exchange on detecting asserted HPD 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 k_s

Test Case

Verify the Source DUT restarts authentication after the receiver sends REAUTH_REQ 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 sends REAUTH_REQ by setting REAUTH_REQ bit of RxStatus after SKE_Send_Eks message

(STEP 1A-07-1)

- ☐ 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 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 – Rx certificate not received

Test Objective

Verify the Source DUT considers it a failure of authentication when the certificate is not received from the Rx during AKE.

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-08-1)

- ☐ TE does not respond with AKE_Send_Cert
  - ➢ If DUT transmits AKE_No_Stored_km, then FAIL (Ref-1A-3)
  - ➢ If DUT transmits AKE_Stored_km, then FAIL (Ref-1A-3)
  - ➢ 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 re-start authentication by performing (STEP 1A-01-2) within 2 seconds of AKE_Init, then FAIL (Ref-1A-1)

1A-09. 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-09-1)

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

- 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)

☐ 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 re-start authentication by performing (STEP 1A-01-2) within 2 seconds of receipt of invalid $cert^{rx}$, then FAIL (Ref-1A-1)

1A-10. 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-10-1)

- ☐ TE provides revoked *Receiver ID* as part of AKE_Send_Cert
- ☐ If DUT aborts Authentication and Key Exchange and stops HDCP 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-11. 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-11-1)

- ☐ 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 re-start authentication by performing (STEP 1A-01-2) within 2 seconds of receipt of invalid *H'*, then FAIL (Ref-1A-1)

[Test Case 2 – AKE_Send_H_prime timeout after AKE_Stored_km]

(STEP 1A-11-2)

☐ TE sends AKE_Send_Cert message (with previously paired *Receiver ID*)

☐ DUT sends AKE_Stored_km message

- If DUT sends 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 or AKE_No_Stored_km message, then FAIL (Ref-1A-4)

☐ TE does not respond with AKE_Send_H_prime within the 200 ms 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 re-start authentication by performing (STEP 1A-01-2) after expiration of the 200 ms timeout, then FAIL (Ref-1A-1)

[Test Case 3 – AKE_Send_H_prime timeout after AKE_No_Stored_km]

(STEP 1A-11-3)

☐ 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 AKE_Send_H_prime within 1 sec

- 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 re-start authentication by performing (STEP 1A-01-2) after expiration of the 1 second timeout, then FAIL (Ref-1A-1)

1A-12. 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-12-1)

- ☐ 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-12-2)

- ☐ TE computes *H'* and sends AKE_Send_H_prime message within 1 sec

(STEP 1A-12-3)

- ☐ TE does not send AKE_Send_Pairing_Info message within 200 ms 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 re-start authentication by performing (STEP 1A-01-2) after expiration of the 200 ms timeout, then FAIL (Ref-1A-1)

Note: TE does not complete pairing.

1A-13. 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, or does not respond with L' 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)

<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.

Two test cases; both are performed.

[Test Case 1 – Invalid L']

(STEP 1A-13-1)

- ☐ TE provides invalid *L'* as part of LC_Send_L_prime message

(STEP 1A-13-2)

- ☐ DUT reattempts locality check with transmission of new LC_Init message
  - ➢ If DUT does not reattempt Locality Check up to 1023 additional times (for a total of 1024 attempts), then NOTE ("DUT reattempted Locality Check XX times.")

(STEP 1A-13-3)

- ☐ DUT restarts Authentication and Key Exchange after 1 or more failures of Locality Check
  - ➢ 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 re-start authentication by performing (STEP 1A-01-2) within 2 seconds of receipt of invalid *L'*, then FAIL (Ref-1A-1)

[Test Case 2 – LC_Send_L_prime message timeout]

(STEP 1A-13-4)

- ☐ TE does not respond with LC_Send_L_prime within 20 ms after transmission of LC_Init

(STEP 1A-13-5)

- ☐ DUT reattempts locality check with transmission of new LC_Init message
    - ➢ If DUT does not reattempt Locality Check up to 1023 additional times (for a total of 1024 attempts), then NOTE ("DUT reattempted Locality Check XX times.")

(STEP 1A-13-6)

- ☐ 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 re-start authentication by performing (STEP 1A-01-2) within 2 seconds after time out, 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

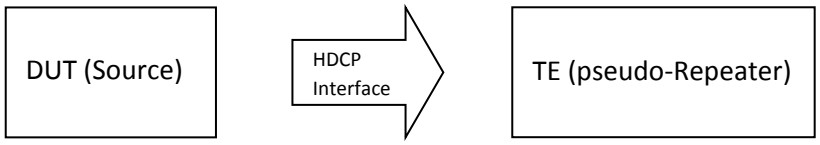
Test Objective

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
	RxCaps:VERSION	0x02
	r_{rx}	Valid
	$cert_{rx}$	Valid
AKE_Send_H_prime	H’	Valid (within 200 ms 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 20 ms 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
	seq_num_V	Valid
	V'	16 bytes, Valid (within 3 second timeout)

<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 value, initializes *seq_num_V* to 0, generates the ReceiverID_List and computes V' in the RepeaterAuth_Send_ReceiverID_List message
- ☐ TE transmits RepeaterAuth_Send_ReceiverID_List message 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 1 s, 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 100 ms before transmitting a given 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 5 sec, then FAIL (Ref-1B-5)
- ☐ TE responds with RepeaterAuth_Stream_Ready message within 100 ms

(STEP 1B-01-3)

- ☐ DUT begins transmitting of a given stream within 10 seconds of completion of Content Stream Management and Authentication with Repeater.
  - ➢ If DUT begins transmitting of a given stream before 100 ms after completion of Content Stream Management, then FAIL (Ref-1B-5)
  - ➢ If DUT does not enable HDCP Encryption, then FAIL (Ref-1A-2)
- ☐ If DUT successfully completes the authentication process, then PASS

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

Test Objective

Verify 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 RepeaterAuth_Send_ReceiverID_List within the 3 second timeout of the receipt of SKE_Send_Eks

<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-02-1)

- ☐ TE does not transmit RepeaterAuth_Send_ReceiverID_List within the 3 second timeout of reception of SKE_Send_Eks.
- ☐ DUT waits three seconds for the reception of RepeaterAuth_Send_ReceiverID_List

(STEP 1B-02-2)

- ☐ DUT disables HDCP encryption, if enabled, after the expiration of the three 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 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 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 the Source 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 '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 computes invalid *V'* in the RepeaterAuth_Send_ReceiverID_List message
- ☐ TE transmits RepeaterAuth_Send_ReceiverID_List message within the 3 second timeout of the receipt of SKE_Send_Eks

(STEP 1B-03-2)

- ☐ DUT disables HDCP encryption after receiving invalid *V'*
  - ➢ If DUT does not disable encryption after comparing the invalid *V'*, 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 k_m)', then PASS

- If DUT does not attempt to re-start authentication by performing (STEP 1A-01-2) within 2 seconds of receipt of invalid *V'*, then FAIL (Ref-1A-1)

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 transmits RepeaterAuth_Send_ReceiverID_List message 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 k_m)', then PASS

- If DUT does not attempt to re-start authentication by performing (STEP 1A-01-2) within 2 seconds of 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 transmits RepeaterAuth_Send_ReceiverID_List message 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 k_m)', then PASS

- If DUT does not attempt to re-start authentication by performing (STEP 1A-01-2) within 2 seconds of 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 provides a non-zero value for seq_num_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-06-1)

- ☐ 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, generates the ReceiverID_List, set *seq_num_V* to a non-zero value and computes *V'* in the RepeaterAuth_Send_ReceiverID_List message
- ☐ TE transmits RepeaterAuth_Send_ReceiverID_List message within the 3 second timeout of the receipt of SKE_Send_Eks

(STEP 1B-06-2)

- ☐ DUT disables HDCP encryption after receiving a non-zero seq_num_V
  - ➢ If DUT does not disable encryption 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 k_m)', then PASS

- If DUT does not attempt to re-start authentication by performing (STEP 1A-01-2) within 2 seconds of receipt of invalid *V'*, then FAIL (Ref-1A-1)

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

Test Objective

Verify that 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

(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 k_m)', then FAIL (Ref-1A-7)
- ☐ If DUT re-starts Authentication and Key Exchange on detecting asserted HPD and performs (STEP 1A-01-1) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', 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 transmits REAUTH_REQ by setting REAUTH_REQ bit in the RxStatus register

(STEP 1B-08-2)

- ☐ 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 k_m)', then FAIL (Ref-1A-7)
- ☐ If DUT re-starts Authentication and Key Exchange on detecting REAUTH_REQ and performs (STEP 1A-01-1) as described in '1A-01 Regular Procedure – With previously connected Receiver (With stored k_m)', then PASS

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 RecevierID_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-07-1) by incrementing DEVICE_COUNT and adjusting the RecevierID_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-1A-1)
- ☐ 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-1A-1)
- 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-1A-1)

☐ If DUT transmits new 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 sec, then FAIL (Ref-1A-1)

☐ TE does not respond with RepeaterAuth_Stream_Ready message within 100 ms

(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-1A-1)

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

2. Receiver Tests

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

2C. Upstream procedure with Transmitter

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

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

2C-01. Regular Procedure – With transmitter

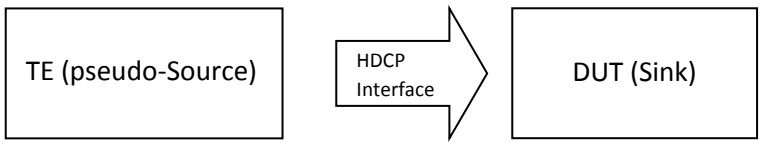
Test Objective

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 asserted HPD
  - ➢ If DUT does not assert 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 transmit AKE_Send_Cert message, 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 transmits AKE_Send_H_prime message
  - ➢ If DUT does not transmit AKE_Send_H_prime within one second timeout, then FAIL (Ref-2C-2)
  - ➢ If *H'* is not equal to *H*, then FAIL (Ref-2C-2)

[Pairing]

(STEP 2C-01-5)

- ☐ DUT transmits AKE_Send_Pairing_Info message
  - ➢ If DUT does not transmit AKE_Send_Pairing_Info message within 200 ms 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 transmits AKE_Send_H_prime message
  - ➢ If DUT does not transmit AKE_Send_H_prime within 200 ms timeout, 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)

[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 transmit LC_Send_L_prime message within 20 ms 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 message
- ☐ TE enables HDCP Encryption 200 ms after transmitting SKE_Send_Eks 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-01-2) 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:RxCaps: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 1 – Not 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 1 – Not 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 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 message
- ☐ TE enables HDCP Encryption 200 ms 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 specification by connecting them to Receivers (TE pseudo-Sink), Repeaters (TE pseudo-Repeater) and Transmitters (TE pseudo-Source).

Note: For all authentication failures Tx must re-attempt authentication at least once (Ref-1A-1).

3A. Downstream Procedure with Receiver

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

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

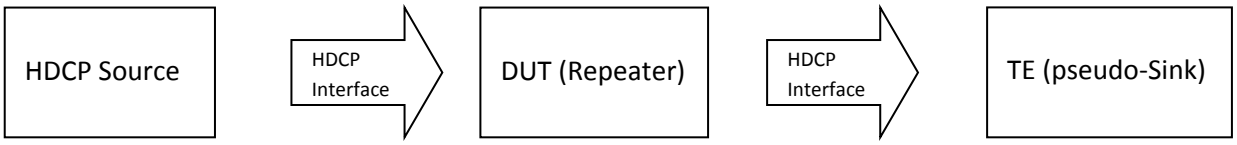
Test Objective

Verify the Repeater's implementation of the HDCP protocol when an HDCP 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 HDCP protocol when an HDCP 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 – Rx certificate not received

Test Objective

Verify the Repeater DUT considers it a failure of authentication when the certificate is not received from the Rx during AKE.

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 – Rx certificate not received'

<Test Case>

Same as '1A-08 Irregular Procedure – Rx certificate not received'

3A-04. 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-09 Irregular Procedure – Verify Receiver Certificate'

<Test Case>

Same as '1A-09 Irregular Procedure – Verify Receiver Certificate'

3A-05. 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-11 Irregular Procedure – Invalid H''

<Test Case>

Same as '1A-11 Irregular Procedure – Invalid H''

3A-06. 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-12 Irregular Procedure – Pairing Failure'

<Test Case>

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

3A-07. 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 respond 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-13 Irregular Procedure – Locality Failure'

<Test Case>

Same as '1A-13 Irregular Procedure – Locality Failure'

3B. Downstream Procedure with Repeater

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

3B-01. Regular Procedure – With Repeater

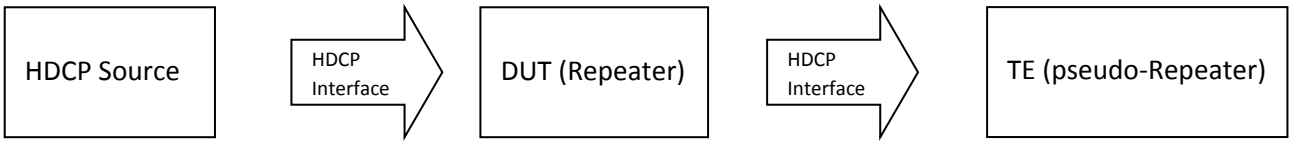
Test Objective

Verify the Repeater DUT works with a 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-05 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 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 Repeater DUT is tested under the following two connection setups:

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

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

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

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

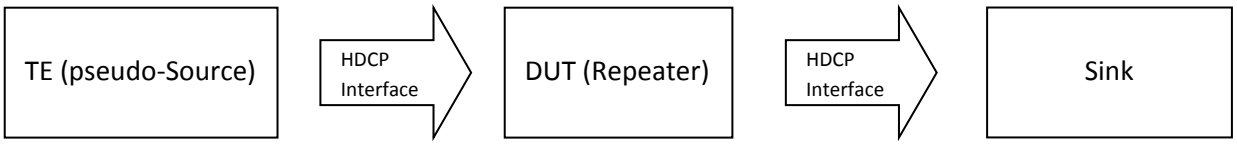
Test Objective

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

Required Test Method

<Connection Setup>

- ☐ Connect TE (pseudo-Source) to the upstream HDCP-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 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 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_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)

- ☐ 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-3)
- ☐ TE transmits RepeaterAuth_Send_Ack message with valid least 128 bits of V within one second of receipt of RepeaterAuth_Send_ReceiverID_list

(STEP 3C-01-3)

[Content Stream Managemet] – 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 5 sec after transmitting RepeaterAuth_Send_Ack message with Type set to 0

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

☐ TE transmits RepeaterAuth_Stream_Manage message within 200 ms after successful completion of Locality Check 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 – ReceiverID_List Propagation when an Active Receiver is Disconnected Downstream

Test Objective

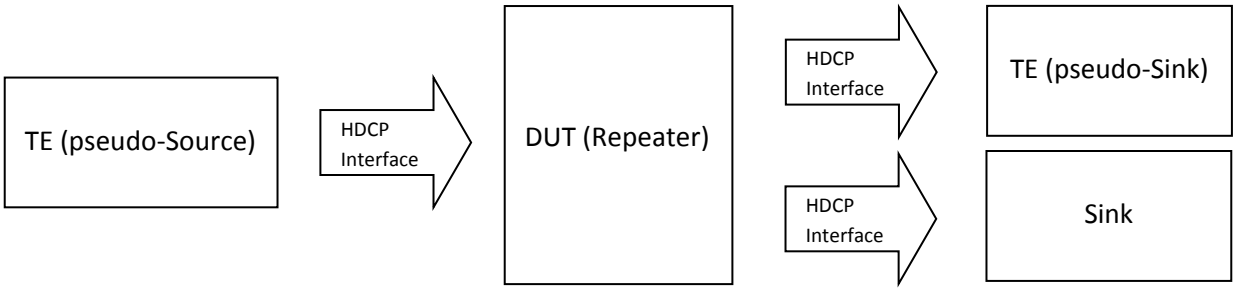
Verify the Repeater DUT sends updated ReceiverID_List messagewhen an active downstream Receiver is disconnected when HDCP Content is flowing.

Required Test Method

This test is performed if Repeater_MultipleOutputs = Y, otherwise SKIP

<Connection Setup>

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

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) de-asserts HPD
  - If DUT de-asserts HPD to 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-3)

☐ If the DUT does not propagate de-asserted HPD to 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 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 ReceiverID_List 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 ReceiverID_List Propagation when an Active Receiver is Disconnected and Reconnected Downstream' are performed

[Connect Active Downstream Sink]

(STEP 3C-03-1)

☐ TE (pseudo-Sink) asserts HPD to DUT

- If the DUT propagates HPD to 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 – 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-08. Irregular Procedure – Rx Certificate invalid

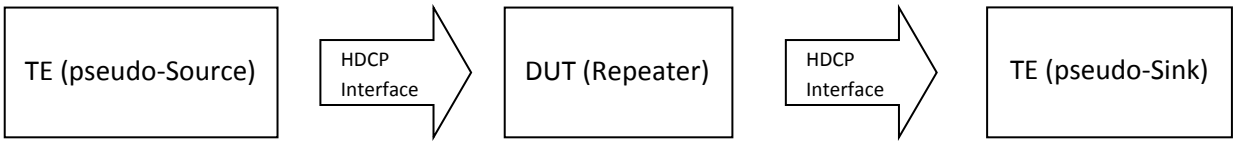
Test Objective

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-09 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 transmit 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-11 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 200 ms 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; or does not respond with L' 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-13 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]

Two test cases; both are performed

[Test Case 1 – Invalid L']

(STEP 3C-10-1)

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

[Test Case 2 – LC_Send_L_prime message timeout]

(STEP 3C-10-2)

- ☐ TE (pseudo-Sink) does not provide LC_Send_L_prime message within 20 ms timeout at the DUT
  - ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-2)

[Both Test Cases]

(STEP 3C-10-3)

- ☐ 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 L' or timeout of LC_Send_L_prime 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, an HDCP Transmitter (TE pseudo-Source) is connected to the upstream HDCP-protected Interface Port of the Repeater DUT. An HDCP Repeater (TE pseudo-Repeater) is connected to the downstream HDCP-protected Interface Port of the Repeater (DUT).

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

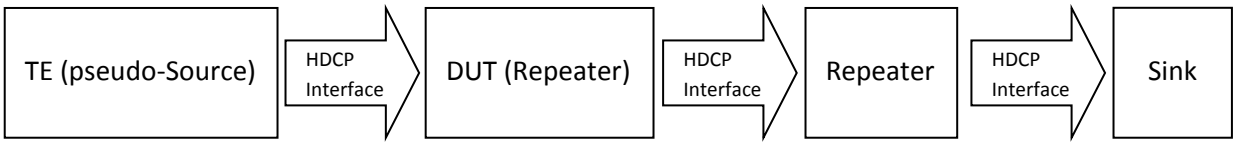
Test Objective

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

Required Test Method

<Connection Setup>

- ☐ Connect TE (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

<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-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 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
- If RepeaterAuth_Send_ReceiverID_List:HDCP1_DEVICE_DOWNSTREAM is 'TRUE', then FAIL

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

☐ If DUT completes the authentication process successfully, then PASS

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

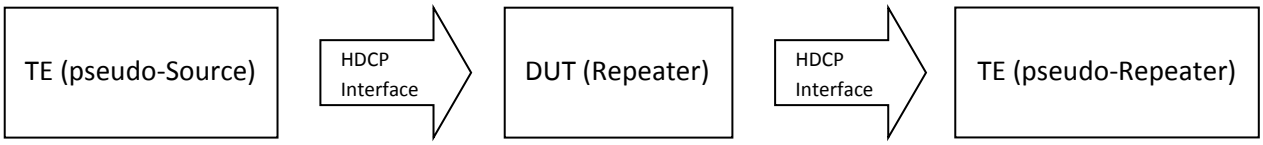
Test Objective

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)>

Authentication and Key Exchange		
AKE_Send_Cert	RxCaps:REPEATER	TRUE
	RxCaps:VERSION	0x02
	r_{rx}	Valid
	$cert_{rx}$	Valid
AKE_Send_H_prime	H’	Valid (within 200 ms 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 20 ms 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
	seq_num_V	0x000000
	V'	16 bytes, Valid (within 3 second timeout)

<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) de-asserts HPD 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) de-asserts HPD 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) de-assert HPD to TE (pseudo-Source), then FAIL (Ref-3C-4)

(STEP 3C-12-2)

- ☐ TE (pseudo-Repeater) asserts HPD
- ☐ DUT either
  - (a) sets REAUTH_REQ in RxStatus and REPEATER in RxCaps of AKE_Send_Cert message

  or

(b) re-asserts HPD 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) re-assert HPD to TE (pseudo-Source), then FAIL (Ref-3C-4)

- If DUT asserts HPD 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 k_m)', 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 Procedure – 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) de-asserts HPD after AKE_Stored_km or AKE_No_Stored_km message
- ☐ DUT either

  (a) sets REAUTH_REQ in RxStatus register and clears REPEATER in RxCaps of AKE_Send_Cert message

  or

  (b) de-asserts HPD 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) de-assert HPD to TE (pseudo-Source), then FAIL (Ref-3C-4)

(STEP 3C-13-2)

- ☐ TE (pseudo-Repeater) asserts HPD
- ☐ DUT either

  (a) sets REAUTH_REQ in RxStatus and REPEATER in RxCaps of AKE_Send_Cert message

  or

  (b) re-asserts HPD 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) re-assert HPD to TE (pseudo-Source), then FAIL (Ref-3C-4)

  - If DUT asserts HPD 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 k_m)', 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) de-asserts HPD after LC_Init message
- ☐ DUT either
  - (a) sets REAUTH_REQ in RxStatus register and clears REPEATER in RxCaps of AKE_Send_Cert message

  or

  - (b) de-asserts HPD 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) de-assert HPD to TE (pseudo-Source), then FAIL (Ref-3C-4)

(STEP 3C-14-2)

- ☐ TE (pseudo-Repeater) asserts HPD
- ☐ DUT either

  (a) sets REAUTH_REQ in RxStatus and REPEATER in RxCaps of AKE_Send_Cert message

  or

  (b) re-asserts HPD 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) re-assert HPD to TE (pseudo-Source), then FAIL (Ref-3C-4)

  - If DUT asserts HPD 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 k_m)', 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) de-asserts HPD after SKE_Send_Eks message
- ☐ DUT either

  (a) sets REAUTH_REQ in RxStatus register and clears REPEATER in RxCaps of AKE_Send_Cert message

  or

  (b) de-asserts HPD 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) de-assert HPD to TE (pseudo-Source), then FAIL (Ref-3C-4)

(STEP 3C-15-2)

- ☐ TE (pseudo-Repeater) asserts HPD
- ☐ DUT either

  (a) sets REAUTH_REQ in RxStatus and REPEATER in RxCaps of AKE_Send_Cert message

  or

  (b) re-asserts HPD 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) re-assert HPD to TE (pseudo-Source), then FAIL (Ref-3C-4)

  - If DUT asserts HPD 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 k_m)', 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-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) and does not transmit RepeaterAuth_Send_Ack to downstream TE (pseudo-Repeater), 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) and does not transmit RepeaterAuth_Send_Ack to downstream TE (pseudo-Repeater), 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-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 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) and does not transmit RepeaterAuth_Send_Ack to downstream TE (pseudo-Repeater), 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

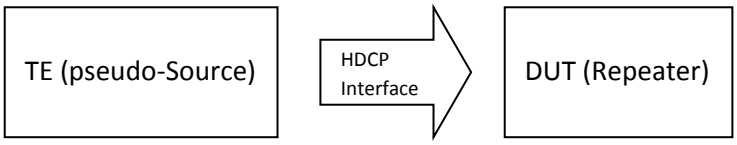
Test Objective

Verify the Repeater DUT having no downstream devices either do the authentication with upstream as a Receiver 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 de-asserts HPD to TE (pseudo-Source)
  - ➢ If DUT asserts HPD to TE, then FAIL (Ref-3C-6)
- ☐ If DUT keeps de-asserting HPD so that TE (pseudo-Source) does not start authentication, then PASS (Ref-3C-6)

[Test Case 2: Authentication as a Receiver]

(STEP 3C-22-2)

- ☐ DUT asserts HPD to TE (pseudo-Source)
- ☐ 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 HDCP_2_0_REPEATER_DOWNSTREAM flag

Test Objective

Verify the Repeater DUT propagates the HDCP_2_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 km)' 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 km)' 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 [Session Key Exchange] in '3C-11 Regular Procedure – Transmitter – DUT – Repeater (With stored km)' 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 100 ms, 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 100 ms 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 100 ms 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 100 ms 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 100 ms with invalid M'
- ☐ DUT does not transmit stream
  - ➢ If DUT transmits stream referenced in RepeaterAuth_Stream_Manage message, then FAIL (Ref-1B-5)

[Test case 3 –Timeout of RepeaterAuth_Stream_Ready message]

(STEP 3C-25-6)

- ☐ TE does not respond with RepeaterAuth_Stream_Ready message within 100 ms
- ☐ DUT does not transmit stream
  - ➢ If DUT transmits stream referenced in RepeaterAuth_Stream_Manage message, then FAIL (Ref-1B-5)
- ☐ If DUT properly responds to confirmation or failure of RepeaterAuth_Stream_Ready message, then PASS

4. Reference

Refer to the High-bandwidth Digital Content Protection System on MHL Specification, Revision 2.2.

Ref-1A. Downstream procedure with Receiver

Ref-1A-1

Reference	Requirement
2.8 HDCP Transmitter State Diagram Page 25	Transmitter's decision to begin authentication is dependent on events such as HPD (Hot Plug Detect) of an attached HDCP Receiver, completion of certain phases of the operating system, a software request, and mode settings. When an HDCP Receiver acknowledges a read of the HDCP2Version register, it must be ready to authenticate, and, in the event of authentication failure, must be prepared to process subsequent authentication attempts. The HDCP Transmitter should not attempt to authenticate until it has successfully obtained an acknowledged read of the HDCP2Version register. Should the HDCP2Version register read or the authentication fail, the HDCP Transmitter must retry periodically, with a period of no more than 2 seconds (preferably much more often). It may cease to attempt authentication only if the HDCP Receiver is clearly disconnected, as with HPD = "Low".

Ref-1A-2

Reference	Requirement
State H1: Transmit Low-value Content Page 26	**State H1: Transmit Low-value Content.** In this state, the transmitter reads the HDCP2Version register. The transmitter determines that the receiver is HDCP 2 capable by reading bit[2] in the receiver's HDCP2Version register. If this bit is set to 1, it indicates that the receiver is HDCP 2 capable. 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.
State A5: Authenticated Page 28	**State A5: Authenticated.** At this time, and at no time prior, the HDCP Transmitter has completed the authentication protocol. In the authenticated state the HDCP Transmitter must poll the *RxStatus* register no less frequently than once every second.

Ref-1A-3

Reference	Requirement

State A1: Exchange K_m Page 27	**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 100ms after writing the AKE_Init message If the HDCP Transmitter does not have k_m stored corresponding to the *Receiver ID*, it generates $E_{kpub}(km)$ and sends $E_{kpub}(km)$ as part of the AKE_No_Stored_km message to the receiver after verification of signature on $cert_{rx}$. 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, reads AKE_Send_H_prime message from the receiver containing *H'* within one second after writing AKE_No_Stored_km to the receiver and compares *H'* against H. If the HDCP Transmitter has k_m stored corresponding to the *Receiver ID*, it writes AKE_Stored_km message containing $E_{kh}(km)$ 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 200 ms after sending AKE_Stored_km to the receiver and compares *H'* against H. If the HDCP Transmitter does not have a k_m 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. ☐ Makes the AKE_Send_Pairing_Info message containing the 128-bit $E_{kh}(k_m)$ 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

	If AKE_Send_Pairing _Info is not available for transmitter to read within 200 ms of the reception of AKE_Send_H_prime, authentication fails and the authentication protocol is aborted. 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 20 ms. The LC_Send_L_prime message must be received by the transmitter within 20ms from the time the transmitter finishes writing the LC_Init message parameters to the HDCP Receiver. Locality check fails if the watchdog timer expires before the last byte of the LC_Send_L_prime message is received by the transmitter. The transmitter then 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 reading LC_Send_L_prime message from the receiver, compares L and *L'*. Locality check fails if L is not equal to *L'*.
State A2: Locality Check Page 27	**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 17	Successful completion of AKE and locality check states 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 200ms before enabling HDCP encryption and beginning the transmission of HDCP content. HDCP encryption may be enabled 200ms after the transmission of the encrypted Session key to the HDCP Receiver and at no time prior. Content encrypted with the session key k_s 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 28	**State A3: Exchange k_s.** The HDCP Transmitter writes 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 200 ms 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 26	**Transition Any State: H0.** Reset conditions at the HDCP Transmitter or loss of HPD cause the HDCP Transmitter to enter the No Receiver Attached State.
Transition H0:H1. Page 26	**Transition H0:H1.** The detection of a sink device (through HPD) indicates to the transmitter that a sink device is connected and ready to display the received content.

Ref-1A-8

Reference	Requirement
Transition A1:A0 Page 27	**Transition A1:A0.** This transition occurs on failure of signature verification on $cert_{rx}$, 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 one

	second after writing AKE_No_Stored_km or within 200 ms after sending AKE_Stored_km to the receiver.
Transition A1:A2 Page 27	**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: A0 Page 27	**Transition A2:A0.** This transition occurs on one or more consecutive locality check failures. Locality check fails when the last byte of the LC_Send_L_prime message is not received by the transmitter within 20 ms and the watchdog timer at the HDCP Transmitter expires or on a mismatch between L and *L'*.

Ref-1B. Downstream procedure with Repeater

Ref-1B-1.

Reference	Requirement
Transition A7:A8. Page 28	**Transition A7:A8.** This transition occurs on successful verification of the most significant 128-bits of *V* and *V'*, none of the reported *Receiver ID*s 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.
Transition A8:A5 Page 29	**Transition A8:A5.** This transition occurs after the RepeaterAuth_Send_Ack message has been written to the repeater and the transmitter has already transmitted Content Stream Management information to the attached HDCP Repeater.

Ref-1B-2.

Reference	Requirement
Section 2.5 Authentication with Repeaters	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

Page 19-20	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, 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 ID*s 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:A0 Page 28	**Transition A6:A0**. The watchdog timer expires before the READY (for RepeaterAuth_Send_ReceiverID_List) has been asserted by the repeater.

Ref-1B-3.

Reference	Requirement
Section 2.5 Authentication with Repeaters Page 21	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. 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 since the HDCP Repeater will not include these fields in the RepeaterAuth_Send_ReceiverID_List message. Authentication fails if the topology maximums are exceeded. HDCP Encryption is disabled and the authentication protocol is aborted.
Transition A7:A0 Page 28	**Transition A7:A0.** 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 ID*s 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 19-20	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, 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 ID*s 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 28	**Transition A7:A8**. This transition occurs on successful verification of the most significant 128-bits of *V* and *V'*, none of the reported *Receiver ID*s 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 23	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. A Type value is 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 and HDCP 2.0-compliant Repeaters.

	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 100ms before the transmission of the corresponding Content Stream 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. 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(k_d).
Section 2.5.2 Downstream Propagation of Content Stream Management Information Page 24	The RepeaterAuth_Stream_Ready message must be available for the transmitter to read within 100ms 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 Stream identified in the corresponding RepeaterAuth_Stream_Manage message. If the RepeaterAuth_Stream_Ready message is not available for the transmitter to read within 100 ms or if M is not equal to M', the HDCP Transmitter must not transmit the Content Stream identified in the corresponding RepeaterAuth_Stream_Manage message. An HDCP Repeater connected to an HDCP 1.x-compliant Transmitter will not receive the RepeaterAuth_Stream_Manage message from the transmitter. In this case, the HDCP Repeater must assign a Type value of 0x00 to all Content Streams received from the HDCP Transmitter. The HDCP Repeater must in turn propagate the received Content Stream management information using the RepeaterAuth_Stream_Manage message further downstream.

Ref-2. Receiver

Ref-2C. Upstream procedure with Transmitter

Ref-2C-1.

Reference	Requirement
Transition Any State:H0 Page 26	**Transition Any State:H0.** Reset conditions at the HDCP Transmitter or loss of HPD cause the HDCP Transmitter to enter the No Receiver Attached state.
Transition H0:H1 Page 26	**Transition H0:H1.** The detection of a sink device (through HPD) indicates to the transmitter that a sink device is connected and ready to display the received content.

Ref-2C-2.

Reference	Requirement
State B1:Compute k_m Page 30	**State B1: Compute k_m.** In this state, the HDCP Receiver makes AKE_Send_Cert message available for reading by the transmitter in response to AKE_Init. If AKE_No_Stored_km is received, it decrypts k_m with $kpriv_{rx}$, calculates *H'*. It sends AKE_Send_H_prime message immediately after computation of *H'* to ensure that the message is received by the transmitter within the specified one second timeout at the transmitter. If AKE_Stored_km is received, the HDCP Receiver decrypts $E_{kh}(k_m)$ to derive k_m 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 specified 200 ms timeout at the transmitter. If AKE_No_Stored_km is received, this is an indication to the HDCP Receiver that the HDCP Transmitter does not contain a k_m stored corresponding to its *Receiver ID*. It implements pairing with the HDCP Transmitter as explained in Section 2.2.1.
Transition H0:H1 Page 26	**Transition H0:H1.** The detection of a sink device (through HPD) indicates to the transmitter that a sink device is connected and ready to display the received content.

Ref-2C-3.

Reference	Requirement
Section 2.2 Authentication and Key Exchange Page 13	Reads AKE_Send_Cert from the receiver containing $cert_{rx}$, 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 59	When REPEATER is set to one, this HDCP Receiver supports downstream connections as permitted by the Digital Content Protection LLC license. This bit does not change while the HDCP Receiver is active.

Ref-2C-4.

Reference	Requirement
State A2: Locality Check Page 27	**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:A0 Page 27	**Transition A2:A0.** This transition occurs on one or more consecutive locality check failures. Locality check fails when the last byte of the LC_Send_L_prime message is not received by the transmitter within 20 ms and the watchdog timer at the HDCP Transmitter expires or on a mismatch between L and L'.

Ref-3 Repeaters

Ref-3C Upstream Procedure with Transmitter

Ref-3C-1

Reference	Requirement
Section 2.5 Authentication with Repeaters Page 21	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. 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 since the HDCP Repeater will not include these fields in the RepeaterAuth_Send_ReceiverID_List message.

Ref-3C-2

Reference	Requirement
Section 2.5 Authentication with Repeaters Page 20	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 2.5.1.1	When an HDCP Receiver (including HDCP Repeater) is newly connected to the

Topology Information Propagation Due to Topology Changes Page 22	HDCP Repeater and the HDCP Repeater has already completed the authentication protocol with the upstream HDCP Transmitter, the HDCP Repeater must make the RepeaterAuth_Send_ReceiverID_List message available for the upstream HDCP Transmitter to read, assert the READY status bit and set the Message_Size register to the size of the RepeaterAuth_Send_ReceiverID_List message. 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. An HDCP Repeater, which receives the RepeaterAuth_Send_ReceiverID_List message from a downstream HDCP Repeater, must propagate the message further upstream. 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 18	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 31	The HDCP Repeater signals the first detection of an active downstream HDCP Receiver to the upstream HDCP Transmitter by signaling for Hot Plug Detect (HPD) to the upstream HDCP Transmitter. Once in the authenticated state with one or more downstream HDCP Receivers, subsequent detection by the HDCP Repeater of additional newly active downstream HDCP Receivers is handled as specified in Section 2.5.1.1. 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.
State C0: Unauthenticated. Page 38	**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 upstream side must

	set the REAUTH_REQ status bit in the *RxStatus* register.
Section 2.10 HDCP Repeater State Diagrams Page 32	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 transitions 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. When the upstream HDCP Transmitter detects the REATUH_REQ status bit set by polling, 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 18	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 downstream HDCP Repeater itself.
Transition F1:F0 Page 35	**Transition F1:F0.** 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 one second after sending AKE_No_Stored_km or within 200 ms after sending AKE_Stored_km to the

	receiver.
Transition F2:F0 Page 35	**Transition F2:F0.** This transition occurs on one or more consecutive locality check failures. Locality check fails when the last byte of the LC_Send_L_prime message is not received by the transmitter within 20 ms and the watchdog timer at the downstream side expires or on a mismatch between L and *L'*.
Transition F6:F0 Page 36	**Transition F6:F0.** The watchdog timer expires before READY has been asserted by the repeater.
Transition F7:F0 Page 36	**Transition F7:F0.** 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 32	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 19	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 39	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