Notice

THIS DOCUMENT IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel Corporation disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted herein. The cryptographic functions described in this specification may be subject to export control by the United States, Japanese, and/or other governments.

Copyright ©2019 Intel Corporation. Third-party brands and names are the property of their respective owners.

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

04 Apr 2011 – Version 1.0. Publication on DCP, LLC website.


09 Apr 2019 – Version 1.3 Changes made to CTS
Table of Contents

INTRODUCTION 6

DEFINITIONS 7

HDCP INTERFACE INDEPENDENT ADAPTATION COMPLIANCE TEST SPECIFICATION 9

1. TRANSMITTER TEST 9

1A. Downstream procedure with Receiver 9
1A-01. Regular Procedure – With previously connected Receiver (With stored $k_m$) 10
1A-02. Regular Procedure – With newly connected Receiver (Without stored $k_m$) 14
1A-03. Regular Procedure – Receiver disconnect after AKE_Init 15
1A-04. Regular Procedure – Receiver disconnect after $k_m$ 16
1A-05. Regular Procedure – Receiver disconnect after locality check 17
1A-06. Regular Procedure – Receiver disconnect after $k_s$ 18
1A-07. Irregular Procedure – Rx certificate not received 19
1A-08. Irregular Procedure – Verify Receiver Certificate 20
1A-09. Irregular Procedure – SRM 21
1A-10. Irregular Procedure – Invalid $H'$ 22
1A-11. Irregular Procedure – Pairing Failure 24
1A-12. Irregular Procedure – Locality Failure 26
1A-13. Regular Procedure – Locality Pre-Compute Support 28
1A-14. Regular Procedure – Authentication with HDCP 2.2 Receiver 29

1B. Downstream procedure with Repeater 30
1B-01. Regular Procedure – With Repeater 31
1B-02. Regular Procedure – Authentication with HDCP 2.0 Repeater 34
1B-03. Regular Procedure – Re-authentication on Receiver Connected Indication 37
1B-04. Irregular Procedure – Timeout of Receiver ID list 38
1B-05. Irregular Procedure – Verify $V'$ 39
1B-06. Irregular Procedure – MAX_DEVS_EXCEEDED 41
1B-07. Irregular Procedure – MAX.CASCADE.EXCEEDED 42
1B-08. Irregular Procedure – Rollover of seq_num_V 43
1B-09. Irregular Procedure – Failure of Content Stream Management 45
1B-10. Regular Procedure – Authentication with HDCP 2.2 Repeater 47

2. RECEIVER TESTS 48
HDCP Interface Independent Adaptation Revision 2.3
Intel Corporation / Digital Content Protection, LLC
Compliance Test Specification
Version 1.2
01 Mar 2019

2C. Upstream procedure with Transmitter

2C-01. Regular Procedure – With transmitter
2C-02. Irregular Procedure – New Authentication after AKE_Init
2C-03. Irregular Procedure – New Authentication during Locality Check
2C-04. Irregular Procedure – New Authentication after SKE_Send_Eks
2C-05. Irregular Procedure – New Authentication during Link Synchronization
2C-06. Irregular Procedure – Invalid L

3. REPEATER TESTS

3A. Downstream Procedure with Receiver

3A-01. Regular Procedure – With previously connected Receiver (With stored $k_m$)
3A-02. Regular Procedure – With newly connected Receiver (Without stored $k_m$)
3A-03. Irregular Procedure – Rx certificate not received
3A-05. Irregular Procedure – Invalid $H’$
3A-06. Irregular Procedure – Pairing Failure
3A-07. Regular Procedure – Locality Pre-Compute Support
3A-08. Regular Procedure – Authentication with HDCP 2.2 Receiver

3B. Downstream Procedure with Repeater

3B-01. Regular Procedure – With Repeater
3B-02. Irregular Procedure – Timeout of Receiver ID list
3B-03. Irregular Procedure – Verify $V’$
3B-04. Irregular Procedure – MAX_DEVS_EXCEEDED
3B-05. Irregular Procedure – MAX.Cascade_EXCEEDED
3B-06. Irregular Procedure – Rollover of seq_num_V
3B-07. Irregular Procedure – Failure of Content Stream Management
3B-08. Regular Procedure – Authentication with HDCP 2.2 Repeater

3C. Upstream Procedure with Transmitter

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

3C-01. Regular Procedure – Transmitter – DUT – Receiver
3C-02. Regular Procedure – Receiver Disconnect Propagation when an Active Receiver is Disconnected Downstream
3C-03. Regular Procedure – Receiver Connected when an Active Receiver is Connected Downstream
3C-04. Irregular Procedure – New Authentication after AKE_Init
3C-05. Irregular Procedure – New Authentication during Locality Check
3C-06. Irregular Procedure – New Authentication after SKE_Send_Eks
3C-07. Irregular Procedure – New Authentication during Link Synchronization
3C-08. Irregular Procedure – Rx Certificate invalid
3C-09. Irregular Procedure – Invalid $H’$

Page 4 of 131
3C-10. Irregular Procedure – Locality Failure 94
3C-11. Irregular Procedure – Invalid L 96

☐ Repeater (DUT) Connected to Transmitter (TE pseudo-Source) and Repeater (TE pseudo-Repeater) 97
3C-12. Regular Procedure – Transmitter – DUT – Repeater (With stored km) 98
3C-13. Regular Procedure – Propagation of HDCP2_0 REPEATER_DOWNSTREAM flag 101
3C-14. Regular Procedure – Propagation of HDCP1_DEVICE_DOWNSTREAM flag 103
3C-15. Regular Procedure – Content Stream Management 104
3C-16. Irregular Procedure – Timeout of Receiver ID list 106
3C-17. Irregular Procedure – Verify V’ 107
3C-18. Irregular Procedure – DEVICE_COUNT 108
3C-19. Irregular Procedure – DEPTH 110
3C-20. Irregular Procedure – MAX_DEVS_EXCEEDED 112
3C-21. Irregular Procedure – MAXCASCADE_EXCEEDED 113

4. REFERENCE 114
Introduction

Purpose and Scope

This document specifies test procedures that will be used to test devices for compliance with the HDCP Specification Interface Independent Adaptation Revision 2.3.

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

Normative References

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 Parameters (PCP)

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

Source Capability

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

Source_LocalityPrecompute Does the DUT support pre-computation of L during the locality check protocol. (Y/N)

Receiver Capability

Receiver_LocalityPrecompute Does the DUT support pre-computation of L’ during the locality check protocol. (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)

Repeater_LocalityPrecomputeTx Does the DUT’s downstream port support pre-computation of L during the locality check protocol. (Y/N)

Repeater_LocalityPrecomputeRx Does the DUT’s upstream port support pre-computation of L’ during the locality check protocol. (Y/N)
HDCP Interface Independent Adaptation Compliance Test Specification

The HDCP Interface Independent Adaptation 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).

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

![Diagram](DUT(Source)→HDCP Interface→TE(pseudo-Sink))

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

<Configuration of TE>

<table>
<thead>
<tr>
<th>Message:</th>
<th>Parameter:</th>
<th>Value:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and Key Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AKE_Send_Cert</td>
<td>REPEATER</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>cert$_{rx}$</td>
<td>Valid</td>
</tr>
<tr>
<td>AKE_Receiver_Info</td>
<td>Version</td>
<td>0x03</td>
</tr>
<tr>
<td></td>
<td>RECEIVER_LOCALITY_PRECOMPUTE_SUPPORT</td>
<td>TRUE (within 100 ms timeout)</td>
</tr>
<tr>
<td>AKE_Send_rrx</td>
<td>$r_{rx}$</td>
<td>Valid (within 100 ms timeout)</td>
</tr>
<tr>
<td>AKE_Send_H_prime</td>
<td>$H'$</td>
<td>Valid (within 200 ms timeout)</td>
</tr>
<tr>
<td>Pairing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AKE_Send_Pairing_Info</td>
<td>$E_{kh_k_m}$</td>
<td>Valid (used only for first time)</td>
</tr>
<tr>
<td>Locality Check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTT_Ready</td>
<td></td>
<td>Valid</td>
</tr>
<tr>
<td>LC_Send_L_prime</td>
<td>$L'$</td>
<td>Valid (within 7 ms timeout)</td>
</tr>
</tbody>
</table>
<Test Case>

[Before Starting Authentication]

(STEP 1A-01-1)

☐ TE transmits Receiver Connected Indication

☐ DUT may begin transmitting low value, unencrypted signal with HDCP Encryption disabled

➤ If DUT begins the Authentication and Key Exchange without sending unencrypted video signal, then WARNING (Ref-1A-1)

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

[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 transmitting Receiver Connected Indication, then FAIL (Ref-1A-2)

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

☐ DUT transmits AKE_Transmitter_Info

➤ If DUT does not transmit AKE_Transmitter_Info within 100 ms of AKE_Init, then FAIL (Ref-1A-2)

If Source_LocalityPrecompute = Y

➤ If TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT bit of TRANSMITTER_CAPABILITY_MASK is not set, then FAIL (Ref-1A-3)

If Source_LocalityPrecompute = N

➤ If TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT bit of TRANSMITTER_CAPABILITY_MASK is set, then FAIL (Ref-1A-3)
STEP 1A-01-3

- TE sends AKE_Send_Cert message
- TE sends AKE_Receiver_Info message within 100 ms of AKE_Transmitter_Info
- DUT sends AKE_Stored_km message
  - If DUT sends AKE_No_Stored_km message, then NOTE (“DUT does not appear to implement persistent pairing for faster authentication”)
  - If DUT does not send AKE_Stored_km message within 100 ms, then FAIL (Ref-1A-2)
- TE sends AKE_Send_rrx message
- TE computes $H'$ and sends AKE_Send_H_prime message within the 200 ms timeout at the transmitter

[Locality Check]

STEP 1A-01-4

- DUT sends LC_Init message
  - If DUT does not send LC_Init message within 100 ms of transmission of AKE_Send_H_prime message, then FAIL (Ref-1A-5)

If Source_LocalityPrecompute = N

  - TE computes $L'$ and sends LC_Send_L_prime message within the 7 ms timeout at the transmitter

If Source_LocalityPrecompute = Y

  - TE computes $L'$ and sends RTT_Ready message
  - DUT transmits RTT_Challenge
    - If DUT does not send RTT_Challenge message within 5 seconds of transmission of RTT_Ready message, then FAIL (Ref-1A-5)
    - If least significant 128-bits of L do not match computed $L'$, then FAIL (Ref-1A-5)
  - TE sends LC_Send_L_prime message within 7 ms timeout
[Session Key Exchange]

(STEP 1A-01-5)

☐ DUT sends SKE_Send_Eks message

➢ If DUT does not send SKE_Send_Eks message within 100 ms of transmission of LC_Send_L_prime message, 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 within 10 seconds of transmission of SKE_Send_Eks message, 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 and does not complete pairing

<Test Case>

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

[Authentication and Key Exchange]

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

(STEP 1A-02-1)

☐ TE sends AKE_Send_Cert message

☐ TE sends AKE_Receiver_Info message within 100 ms of AKE_Transmitter_Info

☐ DUT transmits AKE_No_Stored_km message

- If DUT does not transmit AKE_No_Stored_km message within 100 ms, then FAIL (Ref-1A-2)

- If DUT sends AKE_Stored_km message, then FAIL (Ref-1A-2)

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

☐ If DUT sends AKE_No_Stored_km message, then PASS
1A-03. Regular Procedure – Receiver disconnect after AKE_Init

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE>

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

<Test Case>

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

[Authentication and Key Exchange]

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

- TE transmits Receiver Disconnected Indication after AKE_Init message
- TE transmits Receiver Connected Indication (duration of disconnect is interface dependent)

(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-1)
- If DUT re-starts Authentication and Key Exchange on detecting Receiver Connected Indication and performs (STEP 1A-01-2) as described in ‘1A-01 Regular Procedure – With previously connected Receiver (With stored \( k_m \))’, then PASS
1A-04. Regular Procedure – Receiver disconnect after $k_m$

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE>

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

<Test Case>

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

[Authentication and Key Exchange]

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

☐ TE transmits Receiver Disconnected Indication after AKE_Stored_km message

☐ TE transmits Receiver Connected Indication (duration of disconnect is interface dependent)

(STEP 1A-04-1)

☐ DUT restarts Authentication and Key Exchange

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

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

☐ If DUT re-starts Authentication and Key Exchange on detecting Receiver Connected Indication and performs (STEP 1A-01-2) as described in ‘1A-01 Regular Procedure – With previously connected Receiver (With stored $k_m$)’, then PASS
**1A-05. Regular Procedure – Receiver disconnect after locality check**

**Test Objective**

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

**Required Test Method**

<Connection Setup>

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

<Configuration of TE>

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

<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 kₘ)’ are performed.

[Locality Check]

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

- TE transmits Receiver Disconnected Indication after LC_Init message
- TE transmits Receiver Connected Indication (duration of disconnect is interface dependent)

(STEP 1A-05-1)

- DUT restarts Authentication and Key Exchange
  - If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in ‘1A-01 Regular Procedure – With previously connected Receiver (With stored kₘ)’, then FAIL (Ref-1A-7)
  - If DUT enables HDCP Encryption, then FAIL (Ref-1A-1)
- If DUT re-starts Authentication and Key Exchange on detecting Receiver Connected Indication and performs (STEP 1A-01-2) as described in ‘1A-01 Regular Procedure – With previously connected Receiver (With stored kₘ)’, then PASS
1A-06. Regular Procedure – Receiver disconnect after \( k_s \)

**Test Case**

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

**Required Test Method**

<Connection Setup>

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

<Configuration of TE>

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

<Test Case>

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

[Session Key Exchange]

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

- TE transmits Receiver Disconnected Indication after SKE_Send_Eks message
- TE transmits Receiver Connected Indication (duration of disconnect is interface dependent)

(STEP 1A-06-1)

- DUT restarts Authentication and Key Exchange
  - If DUT does not restart Authentication and Key Exchange and complete (STEP 1A-01-2) as described in ‘1A-01 Regular Procedure – With previously connected Receiver (With stored \( k_m \))’, then FAIL (Ref-1A-7)
  - If DUT enables HDCP Encryption, then FAIL (Ref-1A-1)
- If DUT re-starts Authentication and Key Exchange on detecting Receiver Connected Indication and performs (STEP 1A-01-2) as described in ‘1A-01 Regular Procedure – With previously connected Receiver (With stored \( k_m \))’, then PASS
1A-07. 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-07-1)

☐ TE does not respond with AKE_Send_Cert
  
  ➢ If DUT transmits AKE_No_Stored_km, then FAIL (Ref-1A-2)
  
  ➢ If DUT transmits AKE_Stored_km, then FAIL (Ref-1A-2)
  
  ➢ If DUT enables HDCP Encryption, then FAIL (Ref-1A-1)

☐ If DUT aborts authentication, then PASS
1A-08. Irregular Procedure – Verify Receiver Certificate

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE>

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

- TE provides invalid value for cert_rx

<Test Case>

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

[Authentication and Key Exchange]

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

(STEP 1A-08-1)

☐ TE provides invalid cert_rx as part of AKE_Send_Cert

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

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

☐ If DUT aborts authentication, then PASS
1A-09. Irregular Procedure – SRM

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE>

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

<Test Case>

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

[Authentication and Key Exchange]

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

(STEP 1A-09-1)

☐ TE provides revoked Receiver ID as part of AKE_Send_Cert

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

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

☐ If DUT aborts Authentication and Key Exchange within 2 seconds of receipt of revoked Receiver ID, then PASS.

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 rrx as part of AKE_Init.
1A-10. Irregular Procedure – Invalid $H'$

**Test Objective**

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

**Required Test Method**

<Connection Setup>

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

<Configuration of TE>

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

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

<Test Case>

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

[Authentication and Key Exchange]

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

Three test cases; all are performed

[Test Case 1 – Invalid $H'$]

**(STEP 1A-10-1)**

- TE sends AKE_Send_Cert message (with previously paired Receiver ID)
- DUT sends AKE_Stored_km message
  - If DUT does not send AKE_Stored_km message, then NOTE (“DUT does not appear to implement persistent pairing for faster authentication”)
- TE provides invalid $H'$ as part of AKE_Send_H_prime
  - If DUT enables HDCP Encryption, then FAIL (Ref-1A-1)
If DUT transmits LC_Init, then FAIL (Ref-1A-8)

If DUT aborts authentication, then PASS

[Test Case 2 – AKE_Send_H_prime timeout after AKE_Stored_km]

(STEP 1A-10-2)

TE sends AKE_Send_Cert message (with previously paired Receiver ID)

DUT sends AKE_Stored_km message

If DUT does not send AKE_Stored_km message, then NOTE ("DUT does not appear to implement persistent pairing for faster authentication"); TE ends test

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-1)

If DUT transmits LC_Init, then FAIL (Ref-1A-8)

If DUT aborts authentication, then PASS

[Test Case 3 – AKE_Send_H_prime timeout after AKE_No_Stored_km]

(STEP 1A-10-3)

TE sends AKE_Send_Cert message (with unpaired Receiver ID)

DUT sends AKE_No_Stored_km message

If DUT does not send AKE_No_Stored_km message, then FAIL (Ref-1A-2)

TE does not respond with AKE_Send_H_prime within 1 sec

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

If DUT transmits LC_Init, then FAIL (Ref-1A-8)

If DUT aborts authentication, then PASS
1A-11. Irregular Procedure – Pairing Failure

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE>

Same as ‘1A-01 Regular Procedure – With previously connected receiver (With stored km) 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 km)’ are performed.

[Authentication and Key Exchange]

(STEP 1A-01-2) described in ‘1A-01 Regular Procedure – With previously connected Receiver (With stored km),’ is performed.

(STEP 1A-11-1)

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

(STEP 1A-11-2)

- TE sends AKE_Send_rrx message
- TE computes H’ and sends AKE_Send_H_prime message within 1 sec
(STEP 1A-11-3)

☐ TE does not send AKE_Send_Pairing_Info message within 200 ms of the reception of AKE_Send_H_prime

☐ If DUT aborts authentication, then PASS

Note: TE does not complete pairing.
1A-12. Irregular Procedure – Locality Failure

Test Objective

Verify the Source DUT considers it a failure of authentication if the Receiver provides a value for $L'$ that does not match $L$, 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-12-1)

1a - If Source_LocalityPrecompute = N

☐ TE provides invalid $L'$ as part of LC_Send_L_prime message

1b - If Source_LocalityPrecompute = Y

☐ TE transmits RTT_Ready

☐ DUT transmits RTT_Challenge

➢ If DUT does not send RTT_Challenge message within 100 ms, then FAIL (Ref-1A-5)
➢ If least significant 128 bits of L do not match L’, then FAIL (Ref-1A-5)

☐ TE transmits incorrect MSBs of L’ in LC_Send_L_prime message

(STEP 1A-12-2)

☐ DUT reattempts locality check with the transmission of LC_Init

➢ If DUT does not re-attempt locality check with the transmission of LC_Init 1023 additional times (for a total of 1024 trials), then NOTE (“Locality check failed, but DUT did not re-start authentication”) or (“Locality check failed, and DUT aborted authentication after XX attempts.”)

(STEP 1A-12-3)

☐ DUT aborts authentication

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

☐ If DUT aborts authentication after 1024 unsuccessful attempts at Locality Check, then PASS

[Test Case 2 – LC_Send_L_prime message timeout]

(STEP 1A-12-4)

☐ TE does not respond with LC_Send_L_prime or RTT_Ready within 7 ms after transmission of LC_Init

(STEP 1A-12-5)

☐ DUT reattempts locality check with the transmission of LC_Init

➢ If DUT does not re-attempt locality check with the transmission of LC_Init 1023 additional times (for a total of 1024 trials), then NOTE (“Locality check failed, but DUT did not re-start authentication”) or (“Locality check failed, and DUT aborted authentication after XX attempts.”)

(STEP 1A-12-6)

☐ DUT aborts authentication

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

☐ If DUT aborts authentication after 1024 unsuccessful attempts at Locality Check, then PASS
1A-13. Regular Procedure – Locality Pre-Compute Support

Test Objective

Verify the Source DUT properly configures the TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT flag for non HDCP 2.2 devices.

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 sets AKE_Receiver_Info.VERSION = 0x01; indicating HDCP 2.1 receiver

<Test Case>

Note: Only performed when Source_LocalityPrecompute = Y

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-13-1)

- DUT initiates authentication by transmitting AKE_Init

- DUT transmits AKE_Transmitter_Info with
  TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT = 0

  - If DUT does not transmit AKE_Transmitter_Info within 100 ms of AKE_Init, then FAIL (Ref-1A-5)

  - If DUT transmits AKE_Transmitter_Info with
    TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT = 1, then FAIL (Ref-1A-5)

- If DUT restarts Authentication and Key Exchange with
  TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT = 0, then PASS
1A-14. Regular Procedure – Authentication with HDCP 2.2 Receiver

Test Objective

Verify that the Source DUT correctly authenticates with a HDCP 2.2 capable receiver.

Required Test Method

<Connection Setup>

Same as ‘1A-01 Regular Procedure – With previously connected receiver (With stored km)’

<Configuration of TE>

Same as ‘1A-01 Regular Procedure – With previously connected receiver (With stored km)’ except for the following change:

- TE sets AKE_Receiver_Info.VERSION = 0x02; indicating HDCP 2.2 receiver

<Test Case>

The steps described under [Before Starting Authentication] and [Locality Check] in ‘1A-01 Regular Procedure – With previously connected receiver (With stored km)’ are performed.

[Session Key Exchange]

(STEP 1A-14-1)

- DUT sends SKE_Send_Eks message
  - If DUT sends HMAC(riv) as part of SKE_Send_Eks, then FAIL ((STEP 1A-01-1)Ref-1A-10)
  - If DUT does not send SKE_Send_Eks message within 100 ms of transmission of LC_Send_L_prime message, then FAIL (Ref-1A-6)

(STEP 1A-14-2)

- 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 within 10 seconds of transmission of SKE_Send_Eks message, then FAIL (Ref-1A-6)
- If DUT successfully completes the authentication process, then PASS
**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

![Diagram showing connection between DUT (Source), HDCP Interface, and TE (pseudo-Repeater)]

<Configuration of TE>

<table>
<thead>
<tr>
<th>Message</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication and Key Exchange</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AKE_Send_Cert</td>
<td>REPEATER</td>
<td>TRUE</td>
</tr>
<tr>
<td></td>
<td>cert_rx</td>
<td>Valid</td>
</tr>
<tr>
<td>AKE_Receiver_Info</td>
<td>Version</td>
<td>0x03</td>
</tr>
<tr>
<td></td>
<td>Receiver_Capability_Mask</td>
<td>0x0001</td>
</tr>
<tr>
<td>AKE_Send_rrx</td>
<td>r_rx</td>
<td>Valid (within 100 ms timeout)</td>
</tr>
<tr>
<td>AKE_Send_H_prime</td>
<td>H'</td>
<td>Valid (within 200 ms timeout)</td>
</tr>
<tr>
<td><strong>Pairing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AKE_Send_Pairing_Info</td>
<td>E_{kh}.k_m</td>
<td>Valid (used only for first time)</td>
</tr>
<tr>
<td><strong>Locality Check</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LC_Send_L_prime</td>
<td>L'</td>
<td>Valid (within 7 ms timeout)</td>
</tr>
<tr>
<td><strong>Authentication with Repeater</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RepeaterAuth_Send_ReceiverID_List</td>
<td>MAX.Devs_EXCEEDED</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>MAX.Cascade.EXCEEDED</td>
<td>FALSE</td>
</tr>
<tr>
<td></td>
<td>DEVICE.COUNT</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>DEPTH</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Receiver ID List</td>
<td>(DEVICE.COUNT * 5) bytes</td>
</tr>
<tr>
<td></td>
<td>V'</td>
<td>Valid (within 3 second timeout)</td>
</tr>
<tr>
<td></td>
<td>seq_num_V</td>
<td>Valid</td>
</tr>
</tbody>
</table>
<Test Case>

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

[Authentication with Repeaters]

(STEP 1B-01-1)

- TE clears MAX_CASCADE_EXCEEDED, MAX_DEVS_EXCEEDED, HDCP2_0_REPEATER_DOWNSTREAM, and HDCP1_DEVICE_DOWNSTREAM flags, sets DEPTH and DEVICE_COUNT to the configured values, initializes $seq_{num}_V$ to 0, generates the ReceiverID_List and computes $V'$; sending the 128 most significant bits to the DUT in the RepeaterAuth_Send_ReceiverID_List message
- 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 second, then FAIL (Ref-1B-1)
  - 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-4)

(STEP 1B-01-2)

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

- DUT Transmits RepeaterAuth_Stream_Manage message
  - If DUT does not transmit RepeaterAuth_Stream_Manage message within 200 ms of TE receiving SKE_Send_Eks, then FAIL (Ref-1B-5)
- TE responds with RepeaterAuth_Stream_Ready message within 100 ms

(STEP 1B-01-3)

- DUT begins transmitting Content Stream within 10 seconds of completion of Content Stream Management and Authentication with Repeater.
If DUT begins transmitting Content Stream before 100 ms after completion of Content Stream Management, then FAIL (Ref-1B-5)

If DUT successfully completes the authentication process, then PASS
1B-02. Regular Procedure – Authentication with HDCP 2.0 Repeater

Test Objective

Verify that the Source DUT correctly authenticates with a HDCP 2.0 capable repeater.

Required Test Method

<Connection Setup>

Same as ‘1B-01 Regular Procedure – With Repeater’

<Configuration of TE>

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

☐ TE does not transmit AKE_Receiver_Info

<Test Case>

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

[Authentication and Key Exchange]

(STEP 1B-02-1)

☐ DUT initiates authentication by transmitting AKE_Init

➢ If DUT does not transmit AKE_Init within 10 seconds of TE transmitting Receiver Connected Indication, then FAIL (Ref-1A-2)

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

☐ DUT transmits AKE_Transmitter_Info

➢ If DUT does not transmit AKE_Transmitter_Info within 100 ms of AKE_Init, then FAIL (Ref-1A-2)

If Source_LocalityPrecompute = Y

➢ If TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT bit of TRANSMITTER_CAPABILITY_MASK is not set, then FAIL (Ref-1A-3)

If Source_LocalityPrecompute = N
➢ If TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT bit of TRANSMITTER_CAPABILITY_MASK is set, then FAIL (Ref-1A-3)

(STEP 1B-02-2)

☐ TE sends AKE_Send_Cert message

☐ TE sends does not send AKE_Receiver_Info message within 100 ms of AKE_Transmitter_Info

☐ DUT sends AKE_Stored_km message

➢ If DUT sends AKE_No_Stored_km message, then NOTE ("DUT does not appear to implement persistent pairing for faster authentication")

➢ If DUT does not send AKE_Stored_km message within 100 ms, then FAIL (Ref-1A-2)

☐ TE sends AKE_Send_rrx message

☐ TE computes $H'$ and sends AKE_Send_H_prime message within the 200 ms timeout at the transmitter

[Locality Check]

(STEP 1B-02-3)

☐ DUT sends LC_Init message

➢ If DUT does not send LC_Init message within 100 ms, then FAIL (Ref-1A-5)

☐ TE computes $L'$ and sends LC_Send_L_prime message within the 7 ms timeout at the transmitter

➢ If DUT sends RTT_Challenge message, then FAIL (Ref-1A-5)

[Session Key Exchange]

(STEP 1B-02-4)

☐ DUT sends SKE_Send_Eks message

➢ If DUT does not send SKE_Send_Eks message within 100 ms, then FAIL (Ref-1A-6)
(STEP 1B-02-5)

☐ 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 within 10 seconds of transmission of SKE_Send_Eks message, then FAIL (Ref-1A-6)

[Authentication with Repeaters]

(STEP 1B-02-6)

☐ TE clears MAX_CASCADE_EXCEEDED, MAX_DEVS_EXCEEDED, sets DEPTH and DEVICE_COUNT to the configured values, generates the ReceiverID_List and computes V’; before sending the RepeaterAuth_Send_ReceiverID_List message

➢ If DUT transmits RepeaterAuth_Send_Ack message, then FAIL (Ref-1B-1)

➢ If DUT transmits RepeaterAuth_Stream_Manage message, then FAIL (Ref-1B-5)

➢ If DUT disables HDCP Encryption, then FAIL (Ref-1B-2)

☐ If DUT successfully completes the authentication process, then PASS
1B-03. Regular Procedure – Re-authentication on Receiver Connected Indication

Test Objective

Verify that the Source DUT initiates re-authentication when a Receiver Connected Indication 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-03-1)

☐ TE transmits Receiver Connected Indication

(STEP 1B-03-2)

☐ 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 Receiver Connected Indication and performs (STEP 1A-01-1) as described in ‘1A-01 Regular Procedure – With previously connected Receiver (With stored $k_m$)’, then PASS
1B-04. 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-04-1)

- 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-04-2)

- 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-3)
  
  - If DUT does not disable encryption, if enabled, after the timer expires, then FAIL (Ref-1B-3)

- If DUT aborts authentication, then PASS
1B-05. 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 km)’ are performed.

Two test cases; both are performed

[Authentication with Repeaters]

[Test Case 1 – Incorrect value for most significant 128-bits of V’]

(STEP 1B-05-1)

☐ TE clears MAX CASCADE EXCEEDED, MAX DEVS EXCEEDED, HDCP2_0 REPEATER DOWNSTREAM, and HDCP1 DEVICE DOWNSTREAM flags, sets DEPTH and DEVICE COUNT to the configured values, initializes seq num V to 0, generates the ReceiverID List and computes V’; sending an incorrect value for the 128 most significant bits to the DUT in the RepeaterAuth_Send_ReceiverID_List message

[Test Case 2 – REAUTH REQ = ‘true’]

(STEP 1B-05-2)

☐ TE clears MAX CASCADE EXCEEDED, MAX DEVS EXCEEDED, HDCP2_0 REPEATER DOWNSTREAM, and HDCP1 DEVICE DOWNSTREAM flags, sets DEPTH and DEVICE COUNT to the configured values, initializes seq num V to 0,
generates the ReceiverID_List and computes V'; sending the 128 most significant bits to the DUT in the 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 1 second, then FAIL (Ref-1B-1)
  ➢ 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-4)

☐ TE transmits Receiver_AuthStatus message with REAUTH_REQ set ‘true’

[All Test Cases]

(STEP 1B-05-3)

☐ DUT disables HDCP encryption, if enabled, after receiving invalid V’ or REAUTH_REQ = ‘true’
  ➢ If DUT does not disable encryption, if enabled, then FAIL (Ref-1B-4) and (Ref-1B-1)

☐ If DUT aborts authentication, then PASS
1B-06. 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-06-1)

☐ TE clears MAX_CASCADE_EXCEEDED, DEPTH, DEVICE_COUNT, HDCP2_0_REPEATER_DOWNSTREAM, and HDCP1_DEVICE_DOWNSTREAM; sets MAX_DEVS_EXCEEDED to ‘TRUE’ and does not generate the ReceiverID_List 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-06-2)

☐ DUT disables HDCP encryption, if enabled, after receiving MAX_DEVS_EXCEEDED error.

➢ If DUT does not disable encryption, if enabled, after receiving MAX_DEVS_EXCEEDED error, then FAIL (Ref-1B-4)

☐ If DUT aborts authentication, then PASS.
1B-07. 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 km)’ are performed.

(STEP 1B-07-1)

☐ TE clears MAX_DEVS_EXCEEDED, DEPTH, DEVICE_COUNT, HDCP2_0_REPEATER_DOWNSTREAM, and HDCP1_DEVICE_DOWNSTREAM; sets MAX_CASCADE_EXCEEDED to ‘TRUE’ and does not generate the ReceiverID_List 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-07-2)

☐ 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-4)

☐ If DUT aborts authentication, then PASS
1B-08. 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 km)’ are performed.

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

(STEP 1B-08-1)

- TE sets seq_num_V to 0xFFFFFFFFh
- TE simulates disconnect of an active downstream device by decrementing DEVICE_COUNT and adjusting the ReceiverID_List and transmits RepeaterAuth_Send_ReceiverID_List message
- DUT transmits 128 least significant bits to TE in the RepeaterAuth_Send_Ack message
  - If DUT does not transmit RepeaterAuth_Send_Ack message within one second, then FAIL (Ref-1B-1)
  - If 128 least significant bits transmitted by DUT do not match the 128 least significant bits computed by the TE, then FAIL (Ref-1B-4)

(STEP 1B-08-2)

- TE sets seq_num_V to 0x0000000h (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 ReceiverID_List and transmits RepeaterAuth_Send_ReceiverID_List message

(STEP 1B-08-3)

- 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 km)’, then FAIL (Ref-1B-4)

- 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 km)’, then PASS
1B-09. 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-09-1)

- DUT transmits RepeaterAuth_Stream_Manage message
  
  ➢ If DUT does not transmit RepeaterAuth_Stream_Manage message within 200 ms of TE receiving SKE_Send_Eks, then FAIL (Ref-1B-5)

- TE responds with RepeaterAuth_Stream_Ready message within 100 ms with incorrect value for $M'$

(STEP 1B-09-2)

- DUT transmits RepeaterAuth_Stream_Manage message with incremented $seq\_num\_M$
If DUT transmits content stream without resending
RepeaterAuth_Stream_Manage message, then FAIL (Ref-1B-5)

If DUT transmits RepeaterAuth_Stream_Manage message with same
seq_num_M, then FAIL (Ref-1B-5)

If DUT does not transmit new RepeaterAuth_Stream_Manage message, then
WARNING (Ref-1B-5)

☐ If DUT transmits new RepeaterAuth_Stream_Manage message after failure of M’
comparison, then PASS

[Test Case 2 – Timeout of RepeaterAuth_Stream_Ready message]

(STEP 1B-09-3)

☐ DUT transmits RepeaterAuth_Stream_Manage message

☐ If DUT does not transmit RepeaterAuth_Stream_Manage message within 200
ms of TE receiving SKE_Send_Eks, then FAIL (Ref-1B-5)

☐ TE does not respond with RepeaterAuth_Stream_Ready message within 100 ms

(STEP 1B-09-4)

☐ DUT transmits RepeaterAuth_Stream_Manage message with incremented seq_num_M

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

☐ If DUT transmits RepeaterAuth_Stream_Manage message with same
seq_num_M, then FAIL (Ref-1B-5)

☐ If DUT does not transmit new RepeaterAuth_Stream_Manage message, then
WARNING (Ref-1B-5)

☐ If DUT transmits new RepeaterAuth_Stream_Manage message after timeout of 100 ms
timer, then PASS
1B-10. Regular Procedure – Authentication with HDCP 2.2 Repeater

Test Objective

Verify the Source DUT correctly authenticates with an HDCP 2.2 capable repeater.

Required Test Method

<Connection Setup>

Same as ‘1B-01 Regular Procedure – With Repeater’

<Configuration of TE>

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

- TE sets AKE_Receiver_Info.VERSION = 0x02; indicating HDCP 2.2 receiver

<Test Case>

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

[Session Key Exchange]

(STEP 1B-10-1)

- DUT sends SKE_Send_Eks message
  
  ➢ If DUT sends HMAC(r_v) as part of SKE_Send_Eks, then FAIL ((STEP 1A-01-1)Ref-1A-10)
  ➢ If DUT does not send SKE_Send_Eks message within 100 ms of transmission of LC_Send_L_prime message, then FAIL (Ref-1A-6)

(STEP 1B-10-2)

- 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 within 10 seconds of transmission of SKE_Send_Eks message, then FAIL (Ref-1A-6)

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

- If DUT successfully completes the authentication process, then PASS
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

![Diagram of TE (pseudo-Source) connected to DUT (Sink) via HDCP Interface]

<Test Case>

[Before Starting Authentication]

(STEP 2C-01-1)

☐ TE detects Receiver Connected Indication

➢ If DUT does not send Receiver Connected Indication 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

☐ TE transmits AKE_Transmitter_Info message with
   TRANSMITTER_LOCALITY_PRECOMPUTED = 1

☐ DUT transmits AKE_Send_Cert message

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

➢ If AKE_Send_Cert:REPEATER is ‘TRUE’, then FAIL (Ref-2C-3)

➢ If DUT transmits AKE_Send_rrx message, then FAIL (Ref-2C-4)
DUT transmits AKE_Receiver_Info message

- If DUT does not transmit AKE_Receiver_Info message within 100 ms of AKE_Transmitter_Info, then FAIL (Ref-2C-4)
- If AKE_Receiver_Info:VERSION is not 0x03h, then FAIL (Ref-2C-5)
- If Receiver_LocalityPrecompute = Y and AKE_Receiver_Info:RECEIVER_LOCALITY_PRECOMPUTE_SUPPORT = ‘false’, then FAIL (Ref-2C-5)
- If Receiver_LocalityPrecompute = N and AKE_Recevier_Info:RECEIVER_LOCALITY_PRECOMPUTE_SUPPRT = ‘true’, then FAIL (Ref-2C-5)

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
- DUT transmits AKE_Send_rrx message
  - If DUT does not transmit AKE_Send_rrx message within 100 ms, then FAIL (Ref-2C-2)

(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
- **☐** DUT transmits AKE_Send_rrx message
  - If DUT does not transmit AKE_Send_rrx message within 100 ms, then FAIL (Ref-2C-2)

**(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-3)

[Both test cases]

[Locality Check]

**(STEP 2C-01-8)**

- TE transmits LC_Init message
  - If Receiver_LocalityPrecompute = Y
    - DUT transmits RTT_Ready message
      - If DUT does not transmit RTT_Ready within 100 ms of LC_Init, then FAIL (Ref-2C-6)
  - TE transmits RTT_Challenge message including correct value of least significant 128 bits of $L$
    - DUT sends LC_Send_L_prime message
      - If DUT does not transmit LC_Send_L_prime message within 7 ms of transmission of:
LC_Init message for Receiver_LocalityPrecompute = N, then FAIL (Ref-2C-6)

RTT_Challenge message for Receiver_LocalityPrecompute = Y, then FAIL (Ref-2C-6)

If Receiver_LocalityPrecompute = N
  ➢ If L' does not match L, then FAIL (Ref-2C-6)

If Receiver_LocalityPrecompute = Y
  ➢ If most significant 128-bits of L' do not match most significant 128-bits of L, then FAIL (Ref-2C-6)

[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:REPEATER is ‘TRUE’, then FAIL (Ref-2C-3)

> If DUT transmits AKE_Receiver_Info message, then FAIL (Ref-2C-4)

> If DUT transmits AKE_Send_rrx message, then FAIL (Ref-2C-4)

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 \( r_\text{tx} \) is transmitted right after the reception of LC_Init

Required Test Method

<Connection Setup>

Same as ‘2C-01 Regular Procedure – With Transmitter’

<Test Case>

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

[Locality Check]

(STEP 2C-03-1)

☐ TE transmits LC_Init message

☐ TE transmits AKE_Init message

(STEP 2C-03-2)

☐ DUT transmits AKE_Send_Cert message

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

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

☐ If DUT successfully completes authentication with the new \( r_\text{tx} \) 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
2C-06. Irregular Procedure – Invalid L

Test Objective

Verify the Receiver DUT does not transmit LC_Send_L_prime message when an incorrect L value is received in the RTT_Challenge message.

Required Test Method

<Connection Setup>

Same as ‘2C-01 Regular Procedure – With Transmitter’

<Test Case>

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

[Locality Check]

(STEP 2C-06-1)

□ TE transmits LC_Init message
  ➢ DUT transmits RTT_Ready message
    • If DUT does not transmit RTT_Ready message within 100ms of LC_Init, then FAIL (Ref-2C-6)

(STEP 2C-06-2)

□ TE transmits RTT_Challenge message including incorrect value of least significant 128-bits of L
  ➢ If DUT transmits LC_Send_L_prime message, then FAIL (Ref-2C-6)

□ TE’s locality check fails after 7ms watchdog timer expires. TE retries an additional 1023 times with incorrect RTT_Ready message.
  ➢ If DUT does not respond to TE transmission of incorrect RTT_Challenge message for a total of 1024 tries, 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).

### 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

![Diagram of connection setup]

<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-07 Irregular Procedure – Rx certificate not received’

Test Case

Same as ‘1A-07 Irregular Procedure – Rx certificate not received’

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE>

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

<Test Case>

Same as ‘1A-08 Irregular Procedure – Verify Receiver Certificate’
3A-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 km)’

<Configuration of TE>
Same as ‘1A-10 Irregular Procedure – Invalid H’’

<Test Case>
Same as ‘1A-10 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-11 Irregular Procedure – Pairing Failure’

<Test Case>

Same as ‘1A-11 Irregular Procedure – Pairing Failure’
3A-07. Regular Procedure – Locality Pre-Compute Support

Test Objective

Verify the Repeater DUT properly configures the TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT flag for non HDCP 2.2 devices.

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 Regular Procedure – Locality Pre-Compute Support’

<Test Case>

Same as ‘1A-13 Regular Procedure – Locality Pre-Compute Support’
3A-08. Regular Procedure – Authentication with HDCP 2.2 Receiver

Test Objective

Verify the Repeater DUT properly authenticates with HDCP 2.2 capable Receiver.

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-14 Regular Procedure – Authentication with HDCP 2.2 Receiver’

<Test Case>

Same as ‘1A-14 Regular Procedure – Authentication with HDCP 2.2 Receiver’
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-04 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-05 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-06 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-07 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-08 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 ‘1B-09 Irregular Procedure – Failure of Content Stream Management’

<Test Case>
Same as ‘1B-09 Irregular Procedure – Failure of Content Stream Management’
3B-08.  Regular Procedure – Authentication with HDCP 2.2 Repeater

Test Objective

Verify the Repeater DUT properly authenticates with HDCP 2.2 capable repeater.

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-14 Regular Procedure – Authentication with HDCP 2.2 Repeater’

<Test Case>

Same as ‘1A-14 Regular Procedure – Authentication with HDCP 2.2 Repeater’
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

☐ TE transmits AKE_Transmitter_Info message with

\[\text{TRANSMITTER_LOCALITY_PRECOMPUTE} = 1\]

☐ 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)
- If DUT transmits AKE_Send_rrx message, then FAIL (Ref-2C-4)
DUT transmits AKE_Receiver_Info message

- If DUT does not transmit AKE_Receiver_Info message within 100 ms of AKE_Transmitter_Info, then FAIL (Ref-2C-4)
- If AKE_Receiver_Info:VERSION is not 0x03h, then FAIL (Ref-2C-5)
- If Receiver_LocalityPrecompute = Y and AKE_Receiver_Info:RECEIVER_LOCALITY_PRECOMPUTE_SUPPORT = ‘false’, then FAIL (Ref-2C-5)
- If Receiver_LocalityPrecompute = N and AKE_Recevier_Info:RECEIVER_LOCALITY_PRECOMPUTE_SUPPRT = ‘true’, then FAIL (Ref-2C-5)

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-3)
- If RepeaterAuth_Send_ReceiverID_List:MAX_DEVS_EXCEEDED is ‘TRUE’, then FAIL(Ref-3C-1)
- If RepeaterAuth_Send_ReceiverID_List:MAX_CASCADE_EXCEEDED is ‘TRUE’, then FAIL(Ref-3C-1)
- If RepeaterAuth_Send_ReceiverID_List:DEPTH is not one, then FAIL(Ref-3C-2)
- If RepeaterAuth_Send_ReceiverID_List:DEVICE_COUNT is not one, then FAIL(Ref-3C-2)
- If RepeaterAuth_Send_Receiver_ID_List:HDCP2_0_REPEATER_DOWNSTREAM is one, then FAIL (Ref-3C-6)
- If RepeaterAuth_Send_Receiver_ID_List:HDCP1DEVICE_DOWNSTREAM is one, then FAIL (Ref-3C-6)
If RepeaterAuth_Send_Receiver_ID_List:V’ is not 128 bits, then FAIL (Ref-1B-4)

(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-4)

(STEP 3C-01-3)

- TE transmits RepeaterAuth_Send_Ack message with valid least 128 bits of V within one second of receipt of RepeaterAuth_Send_ReceiverID_list
  - If DUT sends Receiver_AuthStatus message with REAUTH_REQ = ‘TRUE’, then FAIL (Ref-1B-1)

(STEP 3C-01-4)

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

[Test Case 1 – Content Stream Management done in serial with propagation of topology information]
- TE transmits RepeaterAuth_Stream_Manage message within 200 ms 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-01-5)

☐ If DUT completes the authentication process successfully, then PASS
3C-02.  Regular Procedure – Receiver Disconnect Propagation when an Active Receiver is Disconnected Downstream

**Test Objective**

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

**Required Test Method**

This test is performed if Repeater_MultipleOutputs = Y, otherwise SKIP

<Connection Setup>

- Connect TE (pseudo-Source) to the upstream 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

![Diagram of connection setup]

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-3)
  - 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)

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

[Disconnect of Downstream Sink]

(STEP 3C-02-1)

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

(STEP 3C-02-2)

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

➢ If content stream to remaining receiver is interrupted, then WARNING (Ref-3C-7)

☐ If the DUT does not propagate Receiver Disconnect upstream when an active downstream Sink is disconnected, and transmits an updated RepeaterAuth_Send_ReceiverID_List message, then PASS
**3C-03. Regular Procedure – Receiver Connected when an Active Receiver is Connected Downstream**

**Test Objective**

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

**Required Test Method**

This test is performed if Repeater_MultipleOutputs = Y, otherwise SKIP

<Connection Setup>

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

- TE (pseudo-Sink) is in disconnected state

<Test Case>

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

[Connect Active Downstream Sink]

**(STEP 3C-03-1)**

- TE (pseudo-Sink) sends Receiver Connect indication to DUT
  - If DUT propagates Receiver Connect indication upstream, then FAIL (Ref-3C-7)

**(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-3)
  - 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-7)

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)
  - If DUT transmits AKE_Send_rrx message, then FAIL (Ref-2C-4)

The steps described under [Test Case 2 – 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)

➤ If DUT transmits AKE_Send_rrx message, then FAIL (Ref-2C-4)

The steps described under [Test Case 2 – 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)
  - If DUT transmits AKE_Send_rrx message, then FAIL (Ref-2C-4)

The steps described under [Test Case 2 – 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)
  - If DUT transmits AKE_Send_rrx message, then FAIL (Ref-2C-4)

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

- If DUT successfully completes authentication with new rtx value provided in the second AKE_Init message, then PASS
3C-08. Irregular Procedure – Rx Certificate invalid

Test Objective

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

Required Test Method

<Connection Setup>

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

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

<Configuration of TE (pseudo-Sink)>

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

<Test Case>

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

[Authentication with Repeaters]

(STEP 3C-08-1)

☐ DUT reads invalid certificate of downstream pseudo-Sink

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

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

(STEP 3C-08-2)

☐ TE (pseudo-Source) waits for DUT to transmit RepeaterAuth_Send_ReceiverID_List message for a maximum time of 3 seconds

➤ If DUT transmits RepeaterAuth_Send_ReceiverID_List message, then FAIL (Ref-3C-5)
If DUT treats invalid downstream certificate as an authentication failure and does not transmit RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS.
3C-09. Irregular Procedure – Invalid H’

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE (pseudo-Sink)>

Same as ‘1A-10 Irregular Procedure – Invalid H’

<Test Case>

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

[Authentication with Repeaters]

Two test cases; both are performed

[Test Case 1 – Invalid H’]

(STEP 3C-09-1)

☐ DUT reads invalid H’ of downstream pseudo-Sink

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

➢ 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-1)

➢ 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-12 Irregular Procedure – Locality Failure’

<Test Case>

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

[Authentication with Repeaters]

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-1)

[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 7 ms timeout at the DUT

☐ DUT may reattempt locality check with the transmission of LC_Init

➢ If DUT reattempts locality check for more than 1024 total attempts, then FAIL (Ref-1A-9)
If DUT enables HDCP Encryption, then FAIL (Ref-1A-1)

[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
3C-11. Irregular Procedure – Invalid L

Test Objective

Verify the Repeater DUT does not transmit LC_Send_L_prime message when an incorrect L value is received in the RTT_Challenge message.

Required Test Method

<Connection Setup>

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

<Configuration of TE (pseudo_Sink)>

Same as ’2C-06 Irregular Procedure – Invalid L’

<Test Case>

Same as ’2C-06 Irregular Procedure – Invalid L’
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-12. 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 may be used as the Repeater and Sink devices as well as TE acting as a pseudo repeater.

Note: Downstream Repeater and Sink need to be HDCP 2.3 compatible devices.

<Configuration of TE (pseudo-Repeater)>

<table>
<thead>
<tr>
<th>Message:</th>
<th>Parameter:</th>
<th>Value:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and Key Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AKE_Send_Cert</td>
<td>REPEATER</td>
<td>TRUE</td>
</tr>
<tr>
<td>AKE_Rx,</td>
<td>cert</td>
<td>Valid</td>
</tr>
<tr>
<td>AKE_Receiver_Info</td>
<td>Version</td>
<td>0x03</td>
</tr>
<tr>
<td>AKE_Rx,</td>
<td>ReceiverCapability</td>
<td>0x0001</td>
</tr>
<tr>
<td>AKE_Send_rrx</td>
<td>r_rx</td>
<td>Valid (within 100 ms timeout)</td>
</tr>
<tr>
<td>AKE_Send_H_prime</td>
<td>H’</td>
<td>Valid (within 200 ms timeout)</td>
</tr>
<tr>
<td>Pairing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AKE_Send_Pairing_Info</td>
<td>E_{kh, km}</td>
<td>Valid (used only for first time)</td>
</tr>
<tr>
<td>Locality Check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LC_Send_L_prime</td>
<td>L’</td>
<td>Valid (within 7 ms timeout)</td>
</tr>
<tr>
<td>Authentication with Repeater</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RepeaterAuth_Send_ReceiverID_List</td>
<td>MAX_DEVS_EXCEEDED</td>
<td>FALSE</td>
</tr>
<tr>
<td>MAX_CASCADE_EXCEEDED</td>
<td>FALSE</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>DEVICE_COUNT</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>DEPTH</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Receiver ID List</td>
<td>(DEVICE_COUNT * 5) bytes</td>
<td></td>
</tr>
<tr>
<td>V'</td>
<td>Valid (within 3 second timeout)</td>
<td></td>
</tr>
<tr>
<td>seq_num_V</td>
<td>Valid</td>
<td></td>
</tr>
<tr>
<td>HDCP2_0_REPEATER_DOWNSTREAM</td>
<td>FALSE</td>
<td></td>
</tr>
<tr>
<td>HDCP1_DEVICE_DOWNSTREAM</td>
<td>FALSE</td>
<td></td>
</tr>
</tbody>
</table>

<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-3)
  - 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 one, then FAIL (Ref-3C-6)
  - If RepeaterAuth_Send_ReceiverID_List:HDCP1DEVICE_DOWNSTREAM is one, then FAIL (Ref-3C-6)
  - If RepeaterAuth_Send_ReceiverID_List:V’ is not 128 bits, then FAIL (Ref-1B-4)
The remaining steps including (3C-01-2) described in ‘3C-01 Regular Procedure – Transmitter – DUT – Receiver’ are performed

☐ If DUT completes the authentication process successfully, then PASS
3C-13. Regular Procedure – Propagation of HDCP2_0_REPEATER_DOWNSTREAM flag

Test Objective

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

Required Test Method

<Connection Setup>

- 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

![Connection Diagram]

TE (pseudo-Source) → HDPC Interface → DUT (Repeater) → HDPC Interface → TE (pseudo-Repeater)

<Configuration of TE (pseudo-Repeater)>

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

- TE (pseudo-Repeater) sets HDCP2_0_REPEATER_DOWNSTREAM to ‘1’

<Test Case>

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

[Authentication with Repeaters]

(STEP 3C-13-1)

- TE (pseudo-Repeater) sends RepeaterAuth_Send_ReceiverID_List

(STEP 3C-13-2)

- 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-14. Regular Procedure – Propagation of HDCP1DEVICE_DOWNSTREAM flag

Test Objective

Verify the Repeater DUT propagates the HDCP1DEVICE_DOWNSTREAM flag upstream when provided by the downstream repeater in RepeaterAuth_Send_ReceiverID_list message.

Required Test Method

<Connection Setup>

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

<Configuration of TE (pseudo-Repeater)>

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

- TE (pseudo-Repeater) sets HDCP1DEVICE_DOWNSTREAM to ‘1’

<Test Case>

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

[Authentication with Repeaters]

(STEP 3C-14-1)

- TE (pseudo-Repeater) sends RepeaterAuth_Send_ReceiverID_List

(STEP 3C-14-2)

- 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 HDCP1DEVICE_DOWNSTREAM = 1 in RepeaterAuth_Send_ReceiverID_list, then FAIL (Ref-3C-8)

- If DUT propagates downstream indication of HDCP1DEVICE_DOWNSTREAM status to upstream TE (pseudo-Source) as part of RepeaterAuth_Send_ReceiverID_List, then PASS
**3C-15. 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-13 Regular Procedure – Propagation of HDCP2_0_REPEATER_DOWNSTREAM flag’

<Configuration of TE (pseudo-Repeater)>

Same as ‘3C-12 Regular Procedure – Transmitter – DUT – Repeater (With stored km)’

<Test Case>

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

**(STEP 3C-15-1)**

- TE (pseudo-Source) sends RepeaterAuth_Stream_Manage message

**(STEP 3C-15-2)**

- DUT transmits RepeaterAuth_Stream_Ready message within 100ms
  - If DUT does not transmit RepeaterAuth_Stream_Ready message within 100 ms, then FAIL (Ref-3C-5)
  - If $M'$ provided in RepeaterAuth_Stream_Ready message does not match TE’s calculation of M, then FAIL (Ref-1B-5)

**(STEP 3C-15-3)**

- 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-15-4)

☐ 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-15-5)

☐ 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-15-6)

☐ 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
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-13 Regular Procedure – Propagation of HDCP2_0_REPEATER_DOWNSTREAM flag’

<Configuration of TE (pseudo-Repeater)>

Same as ‘3C-12 Regular Procedure – Transmitter – DUT – Repeater (With stored km)’

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in ‘3C-12 Regular Procedure – Transmitter – DUT – Repeater (With stored km)’ 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-3)

➤ If DUT does not disable encryption after the timer expires, then FAIL (Ref-1B-3)

(STEP 3C-16-3)

☐ DUT does not transmit RepeaterAuth_Send_ReceiverID_List to TE (pseudo-Source)

➤ If DUT transmits RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-5)

☐ If DUT treats timeout of watchdog timer for RepeaterAuth_Send_ReceiverID_List from downstream TE pseudo-Repeater as an authentication failure and does not transmit RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS
3C-17. Irregular Procedure – Verify V’

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE (pseudo-Repeater)>

Same as ‘1B-05 Irregular Procedure – Verify V’’

<Test Case>

Same as ‘1B-05 Irregular Procedure – Verify V’’

[Authentication with Repeaters]

(STEP 3C-17-1)

☐ DUT does not transmit RepeaterAuth_Send_ReceiverID_List to TE (pseudo-Source)

➤ If DUT transmits RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-5)

☐ If DUT treats the mismatch of V and invalid V’ from downstream TE pseudo-Repeater as an authentication failure and does not transmit RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS
3C-18. Irregular Procedure – DEVICE_COUNT

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE (pseudo-Repeater)>

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

☐ TE (pseudo-Repeater) sets DEVICE_COUNT = 31

<Test Case>

The steps described under [Before Starting Authentication] to [Session Key Exchange] in ‘3C-12 Regular Procedure – Transmitter – DUT – Repeater (With stored km)’ 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-13 Regular Procedure – Propagation of HDCP2_0_REPEATER_DOWNSTREAM flag’

<Configuration of TE (pseudo-Repeater)>

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

☐ TE (pseudo-Repeater) sets 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 km)’ 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-13 Regular Procedure – Propagation of HDCP2.0_REPEATER_DOWNSTREAM flag’

<Configuration of TE (pseudo-Repeater)>

Same as ‘1B-06 Irregular Procedure – MAX_DEVICES_EXCEEDED’

<Test Case>

Same as ‘1B-06 Irregular Procedure – MAX_DEVICES_EXCEEDED’

[Authentication with Repeaters]

(STEP 3C-20-1)

☐ DUT sets MAX_DEVS_EXCEEDED flag and transmits RepeaterAuth_Send_ReceiverID_List to TE (pseudo-source)

➤ If DUT does not transmit RepeaterAuth_Send_ReceiverID_List, then FAIL (Ref-3C-1)

➤ If MAX_DEVS_EXCEEDED is ‘FALSE’, then FAIL (Ref-3C-1)

☐ If DUT treats the reception of MAX_DEVS_EXCEEDED from downstream TE pseudo-Repeater as an authentication failure and signals MAX_DEVS_EXCEEDED error in RepeaterAuth_Send_ReceiverID_List to the upstream TE (pseudo-Source), then PASS
3C-21. Irregular Procedure – MAX_CASCADE_EXCEEDED

Test Objective

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

Required Test Method

<Connection Setup>

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

<Configuration of TE (pseudo-Repeater)>

Same as ‘1B-07 Irregular Procedure – MAX_CASCADE_EXCEEDED’

<Test Case>

Same as ‘1B-07 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), then PASS
4. Reference

Refer to the High-bandwidth Digital Content Protection System – Interface Independent Adaptation, Revision 2.2.

Ref-1A. Downstream procedure with Receiver

Ref-1A-1

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>State H1: Transmit Low-value Content Page 32</td>
<td>In this state the transmitter may begin sending an unencrypted signal with HDCP Encryption disabled. The transmitted signal can be a low value content or informative on-screen display. If low-value content is transmitted, this will ensure that a valid video signal is displayed to the user before and during authentication. At any time a Receiver Connected Indication received from the connected HDCP 2.0-compliant HDCP Repeater causes the transmitter to transition to this state.</td>
</tr>
<tr>
<td>State A5: Authenticated Page 34</td>
<td><strong>State A5: Authenticated.</strong> At this time, and at no prior time, the HDCP Transmitter has completed the authentication protocol. A periodic Link Synchronization is performed to maintain cipher synchronization between HDCP Transmitter and HDCP Receiver.</td>
</tr>
</tbody>
</table>

Ref-1A-2

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| 2.2 Authentication and Key Exchange Page 12 | Authentication and Key Exchange (AKE) is the first step in the authentication protocol. Figure 2.1 and Figure 2.2 illustrates the AKE. The HDCP Transmitter *(Device A)* can initiate authentication at any time, even before a previous authentication exchange has completed. The HDCP Transmitter initiates a new HDCP Session by sending a new \(r_{tx}\) as part of the authentication initiation message, AKE_Init. Message formats are defined in Section 4.3. The HDCP Transmitter

- Initiates authentication by sending an initiation message, AKE_Init, containing a 64-bit pseudo-random value \(r_{tx}\)
- Sends AKE_Transmitter_Info message to the HDCP Receiver before sending either AKE_No_Stored_km or AKE_Stored_km message to the receiver.

Note: The HDCP Transmitter may use mechanisms outside the scope of the HDCP Specification to determine whether the HDCP Receiver is an HDCP 2.0-compliant Device. If the HDCP Transmitter
determines, using mechanisms outside the scope of the HDCP Specification, that the HDCP Receiver is an HDCP 2.0-compliant Device, it need not send the AKE_Transmitter_Info message to the HDCP Receiver.

State A1: Exchange $K_m$
Page 33

State A1: Exchange $K_m$. In this state, the HDCP Transmitter initiates authentication by sending AKE_Init message containing $r_{tx}$ to the HDCP Receiver and sends AKE_Transmitter_Info message to the HDCP Receiver. It receives AKE_Send_Cert from the receiver containing REPEATER and $cert_{rx}$ and AKE_Receiver_info message (if the HDCP Receiver is not HDCP 2.0-compliant). If the HDCP Transmitter does not receive AKE_Receiver_Info message within 100 ms of the transmission of AKE_Transmitter_Info message, it indicates that the HDCP Receiver is an HDCP 2.0-compliant Device.

If the HDCP Transmitter does not have $k_m$ stored corresponding to the Receiver ID, it generates $E_{k_{pub}}(km)$ and sends $E_{k_{pub}}(km)$ 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 receives AKE_Send_rrx message containing $r_{rx}$ from the receiver. It computes $H$, receives AKE_Send_H_prime message from the receiver containing $H'$ within one second after sending 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 sends AKE_Stored_km message containing $E_{k_{h}}(km)$ 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 and receives $r_{rx}$ as part of AKE_Send_rrx message from the receiver. It computes $H$, receives 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-3

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 4.24.</td>
<td>Description:</td>
</tr>
<tr>
<td>TRANSMITTER_</td>
<td>Bits 15:2:Reserved zeros.</td>
</tr>
</tbody>
</table>
### CAPABILITY_MASK Parameter

| Page 67 | Bit 1: TRANSMITTER_CONTENT_CATEGORY_SUPPORT. This bit must be set to 1 by the HDCP Transmitter. | Bit 0: TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT. When this bit is set to one, it indicates that the HDCP Transmitter supports pre-computation of L during the locality check protocol. |

---

#### Ref-1A-4

<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
</tr>
<tr>
<td>- Computes 128-bit $k_h = \text{SHA-256}(k_{priv,rx})[127:0]$.</td>
</tr>
<tr>
<td>- Generates 128-bit $E_{kh}(k_m)$ by encrypting $k_m$ with $k_h$ using AES as illustrated in Figure 2.3.</td>
</tr>
<tr>
<td>- Sends AKE_Send_Pairing_Info to the transmitter containing the 128-bit $E_{kh}(k_m)$.</td>
</tr>
</tbody>
</table>

On receiving AKE_Send_Pairing_Info message, the HDCP Transmitter may persistently store $m$ (which is $r_{tx}$ concatenated with $r_{rx} | r_{tx}$), $k_m$ and $E_{kh}(k_m)$ along with Receiver ID.

If AKE_Send_Pairing_Info is not received by the HDCP Transmitter within 200 ms of the reception of AKE_Send_H_prime, authentication fails and the authentication protocol is aborted.

Note: The HDCP Transmitter may store in its non-volatile storage $m$, $k_m$, and $E_{kh}(k_m)$ along with corresponding Receiver IDs of all HDCP Receivers with which pairing was implemented by the HDCP Transmitter.

---

#### Ref-1A-5

<table>
<thead>
<tr>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>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. If AKE_Receiver_Info.VERSION = 0x01 and the HDCP Transmitter set its TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT bit to one in the AKE_Transmitter_Info message transmitted to the HDCP Receiver, the HDCP</td>
</tr>
</tbody>
</table>

---

Page 116 of 131
Transmitter must initiate re-authentication with the HDPC Receiver with the `TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT` bit set to zero. If the HDPC Receiver is HDPC 2.0-compliant or if the `RECEIVER_LOCALITY_PRECOMPUTE_SUPPORT` bit received as part of the `AKE_Receiver_Info` message is set to zero or the transmitter has set the `TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT` bit to zero in its `AKE_Transmitter_Info` message, the HDPC Transmitter

- Initiates locality check by sending `LC_Init` message containing a 64-bit pseudo-random nonce $r_n$ to the HDPC Receiver.
- Sets its watchdog timer to 7 ms. Locality check fails if the watchdog timer expires before `LC_Send_L_prime` message is received.
- Computes $L = \text{HMAC-SHA256}(r_n, k_d \ XOR \ r_x)$ where HMAC-SHA256 is computed over $r_n$ and the key used for HMAC is $k_d \ XOR \ r_x$, where $r_x$ is XORed with the least-significant 64-bits of $k_d$.
- On receiving `LC_Send_L_prime` message, compares $L$ and $L'$. Locality check fails if $L$ is not equal to $L'$.

If the `RECEIVER_LOCALITY_PRECOMPUTE_SUPPORT` bit received as part of the `AKE_Receiver_Info` message is set to one and the transmitter has set the `TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT` bit to one in its `AKE_Transmitter_Info` message, the HDPC Transmitter

- Initiates locality check by sending `LC_Init` message containing a 64-bit pseudo-random nonce $r_n$ to the HDPC Receiver.
- Computes 256-bit $L = \text{HMAC-SHA256}(r_n \ || \ r_n, k_d \ XOR \ r_x)$ where HMAC-SHA256 is computed over $r_n \ || \ r_n$ and the key used for HMAC is $k_d \ XOR \ r_x$, where $r_x$ is XORed with the least-significant 64-bits of $k_d$. All values are in big-endian order.
- On receiving the `RTT_Ready` message from the receiver, the transmitter sends an `RTT_Challenge` message containing the least significant 128-bits of $L$.
- Sets its watchdog timer to 7 ms. Locality check fails if the watchdog timer expires before `LC_Send_L_prime` message is received.
- On receiving `LC_Send_L_prime` message, the HDPC Transmitter compares the received value with the most significant 128-bits of $L$ and locality check fails if there is a mismatch.

An HDPC Repeater initiates locality check on all its downstream HDPC-protected interface ports by sending unique $r_n$ values to the connected HDPC Devices.
**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

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| 2.4 Session Key Exchange Page 21 | Successful completion of AKE and locality check stages affirms to HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. Session Key Exchange (SKE) is initiated by the HDCP Transmitter after a successful locality check. The HDCP Transmitter sends encrypted Session Key to the HDCP Receiver at least 200 ms before enabling HDCP Encryption and beginning the transmission of HDCP Content. HDCP Encryption may be enabled 200 ms 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 $r_{iv}$.
  - Computes a 256-bit HMAC of $r_{iv} = \text{HMAC-SHA256}(r_{iv}, k_d)$ where HMAC-SHA256 is computed over $r_{iv}$ and the key used for HMAC is $k_d$, if the HDCP Receiver is compliant with HDCP2.3 or higher (i.e. AKE_Receiver_Info. Version = 0x03 or higher)
  - 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 $E_{dkey}(k_s) = k_s \text{ XOR } (dkey_2 \text{ XOR } r_{rx})$, where $r_{rx}$ is XORed with the least-significant 64-bits of $dkey_2$.
  - Sends SKE_Send_Eks message containing $E_{dkey}(k_s)$, $r_{iv}$ and HMAC of $r_{iv}$ to the HDCP Receiver. |

**State A3: Exchange $k_s$.** The HDCP Transmitter sends encrypted Session Key, $E_{dkey}(k_s)$, and $r_{iv}$ to the HDCP Receiver as part of the SKE_Send_Eks message. It may enable HDCP Encryption 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

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
</table>
### Transition Any State: H0.

**Page 32**

**Transition Any State: H0.** Reset conditions at the HDCP Transmitter or disconnect of the connected HDCP capable receiver cause the HDCP Transmitter to enter the No Receiver Attached state.

### Transition H0:H1.

**Page 32**

**Transition H0:H1.** The detection of a sink device (through Receiver Connected Indication) indicates to the transmitter that a sink device is connected and ready to display the received content. When the receiver is no longer active, the transmitter is notified through Receiver Disconnected Indication.

---

**Ref-1A-8**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transition A1:H1</td>
<td>This transition occurs on failure of signature verification on certRx, 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 sending AKE_No_Stored_km or within 200 ms after sending AKE_Stored_km to the receiver.</td>
</tr>
<tr>
<td>Transition A1:A2</td>
<td>The HDCP Transmitter implements locality check after successful completion of AKE and pairing.</td>
</tr>
</tbody>
</table>

---

**Ref-1A-9**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3 Locality Check</td>
<td>In the case of a locality check failure due to expiration of the watchdog timer or due to mismatch of L and L' (or the most significant 128-bits 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 rnr. 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.</td>
</tr>
<tr>
<td>Transition A2: H1</td>
<td>This transition occurs on one or more consecutive locality check failures. Locality check fails when L' (or the most significant 128-bits of L') is not received within 7 ms and the watchdog timer at the HDCP Transmitter expires or on a mismatch between L and L' (or the most significant 128-bits of L').</td>
</tr>
</tbody>
</table>

---

**Ref-1A-10**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
</table>
4.3.10 SKE_Send_EkS (Transmitter to Receiver) Page 63

The HDCP Transmitter constructs the SKE_Send_Eks message as given in Table 4.12 if the HDCP Receiver is compliant with HDCP 2.3 or higher, else the HDCP Transmitter constructs the message as given in Table 4.13.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>No. of Bytes</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKE_Send_Eks{</td>
<td>1</td>
<td>uint</td>
</tr>
<tr>
<td>msg_id</td>
<td>16</td>
<td>uint</td>
</tr>
<tr>
<td>EdTosK[127.0]</td>
<td>8</td>
<td>uint</td>
</tr>
<tr>
<td>rT[63.0]</td>
<td>32</td>
<td>uint</td>
</tr>
</tbody>
</table>

Table 4.12 SKE_Send_Eks Payload

<table>
<thead>
<tr>
<th>Syntax</th>
<th>No. of Bytes</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKE_Send_Eks{</td>
<td>1</td>
<td>uint</td>
</tr>
<tr>
<td>msg_id</td>
<td>16</td>
<td>uint</td>
</tr>
<tr>
<td>EdTosK[127.0]</td>
<td>8</td>
<td>uint</td>
</tr>
<tr>
<td>rT[63.0]</td>
<td>8</td>
<td>uint</td>
</tr>
</tbody>
</table>

Table 4.13 SKE_Send_Eks Payload
Ref-1B. Downstream procedure with Repeater

Ref-1B-1.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1 Upstream Propagation of Topology Information</td>
<td>On successful verification of Receiver ID list and topology information, i.e. if the values match, none of the reported Receiver IDs are in the current revocation list (in the case of the most upstream HDCP Transmitter), the HDCP Transmitter does not detect a roll-over of seq_num_V, the downstream topology does not exceed specified maximums (explained below) and the HDCP Repeater is not HDCP 2.0-compliant, the HDCP Transmitter (including downstream port of HDCP Repeater) sends 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 the repeater on successful verification of Receiver ID list and topology information by the transmitter. The RepeaterAuth_Send_Ack message must be received by the HDCP Repeater within one second from the transmission of the RepeaterAuth_Send_ReceiverID_List message to the HDCP Transmitter if the HDCP Transmitter is not HDCP 2.0-compliant and the downstream topology does not exceed specified maximums. A match between the least significant 128-bits of V and V' indicates successful upstream transmission of topology information. If a mismatch occurs or the RepeaterAuth_Send_Ack message is not received by the repeater within one second, the HDCP Repeater must send the Receiver_AuthStatus message with the REAUTH_REQ set to ‘true’ and must transition in to an unauthenticated state (See Section 2.10.3).</td>
</tr>
</tbody>
</table>

Ref-1B-2.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transition A7:A5. Page 34</td>
<td><strong>Transition A7:A5.</strong> This transition occurs if the connected HDCP Repeater is HDCP 2.0-compliant, on successful verification of V and V', none of the reported Receiver IDs are in the current revocation list, and the downstream topology does not exceed specified maximums.</td>
</tr>
</tbody>
</table>

Ref-1B-3.
Section 2.5.1  
Upstream Propagation of Topology Information  
Page 24  

After transmitting the SKE_Send_Eks message, the HDCP transmitter, having determined that REPEATER received earlier in the protocol is ‘true’, sets a three-second watchdog timer. If the RepeaterAuth_Send_ReceiverID_List message 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.

| Transition A6:H1  
Page 34  |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transition A6:H1.</strong> The watchdog timer expires before the RepeaterAuth_Send_ReceiverID_List is received.</td>
</tr>
</tbody>
</table>

Ref-1B-4.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Section 2.5.1  
Upstream Propagation of Topology Information  
Page 24  | Whenever the RepeaterAuth_Send_ReceiverID_List message is received, the HDCP Transmitter verifies the integrity of the Receiver ID list by computing V and comparing either V and V' (if the connected HDCP Repeater is HDCP 2.0-compliant) or the most significant 128-bits of V and V' (if the connected HDCP Repeater is not HDCP 2.0-compliant). If the values do not match, authentication fails, the authentication protocol is aborted and HDCP Encryption is disabled. |

| Transition A7:H1  
Page 34  |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transition A7:H1.</strong> This transition is made if a mismatch occurs between V and V' (if the connected HDCP Repeater is HDCP 2.0-compliant) or the most significant 128-bits of V and V' (if the connected HDCP Repeater is not HDCP 2.0-compliant). This transition is also made if any of the Receiver IDs in the Receiver ID list are found in the current revocation list or if the HDCP Transmitter detects a roll-over of seq_num_V (if the repeater is not HDCP 2.0-compliant). A MAX_CASCADE_EXCEEDED or MAX_DEVS_EXCEEDED error also causes this transition.</td>
</tr>
</tbody>
</table>

Ref-1B-5.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Section 2.5.2  
Downstream Propagation of Content Stream Management Information  
Page 28  | The HDCP Transmitter must send the RepeaterAuth_Stream_Manage message specifying Type values assigned to the Content Streams, to the attached HDCP Repeater at least 100ms before the transmission of the corresponding Content Streams after HDCP Encryption. The HDCP Transmitter must only send the RepeaterAuth_Stream_Manage message corresponding to encrypted Content Streams it will transmit to the HDCP Repeater. The HDCP Transmitter initializes seq_num_M to 0 at the |
<table>
<thead>
<tr>
<th>State A9: Content Stream Management Page 35</th>
<th>beginning of the HDCP Session i.e. after ( r_{tx} ) is sent. It is incremented by one after the transmission of every RepeaterAuth_Stream_Manage message.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State A9: Content Stream Management</strong></td>
<td>This stage is implemented if Content Stream is to be transmitted and the connected HDCP Repeater is not HDCP 2.0-compliant. The HDCP Transmitter sends the RepeaterAuth_Stream_Manage message specifying Type values assigned to Content Streams, to the attached HDCP Repeater at least 100ms before the transmission of the corresponding Content Streams after HDCP Encryption. It must receive the RepeaterAuth_Stream_Ready message from the HDCP Repeater within 100ms after the transmission of RepeaterAuth_Stream_Manage message and verifies ( M' ). This step fails if the RepeaterAuth_Stream_Ready message is not received within 100ms of if ( M ) is not equal to ( M' ).</td>
</tr>
</tbody>
</table>
## Ref-2. Receiver

### Ref-2C. Upstream procedure with Transmitter

### Ref-2C-1.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transition Any State:H0 Page 32</td>
<td><strong>Transition Any State:H0.</strong> Reset conditions at the HDCP Transmitter or disconnect of the connected HDCP capable receiver cause the HDCP Transmitter to enter the No Receiver Attached state.</td>
</tr>
<tr>
<td>Transition H0:H1 Page 32</td>
<td><strong>Transition H0:H1.</strong> The detection of a sink device (through Receiver Connected Indication) indicates to the transmitter that a sink device is connected and ready to display the received content. When the receiver is no longer active, the transmitter is notified through Receiver Disconnected Indication.</td>
</tr>
</tbody>
</table>

### Ref-2C-2.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>State B1:Compute $k_m$ Page 36</td>
<td><strong>State B1: Compute $k_m$.</strong> In this state, the HDCP Receiver sends AKE_Send_Cert message in response to AKE_Init, sends AKE_Receiver_Info message to the transmitter if AKE_Transmitter_Info message is received from the transmitter, generates and sends $r_x$ as part of AKE_Send_rrx message. If AKE_No_Stored_km is received, it decrypts $k_m$ with $k_{priv_{rx}}$, 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 the HDCP Receiver does not receive AKE_Transmitter_Info message before the reception of AKE_No_Stored_km or AKE_Stored_km message, it indicates that the HDCP Transmitter is an HDCP 2.0-compliant device. If AKE_Stored_km is received, the HDCP Receiver decrypts $E_{wx}(k_m)$ to derive $k_m$ and 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 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.</td>
</tr>
<tr>
<td>Transition H0:H1 Page 32</td>
<td><strong>Transition H0:H1.</strong> The detection of a sink device (through Receiver Connected Indication) indicates to the transmitter that a sink device is connected and ready to display the received content. When the receiver is no longer active, the transmitter is notified through Receiver Disconnected Indication.</td>
</tr>
</tbody>
</table>
no longer active, the transmitter is notified through Receiver Disconnected Indication.

**Ref-2C-3.**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 2.5 Authentication with Repeaters Page 22</td>
<td>The HDCP Transmitter executes authentication with repeaters after Session Key exchange and only when REPEATER is ‘true’, indicating that the connected HDCP Receiver is an HDCP Repeater. Authentication with repeaters stage is used for the upstream propagation of topology information and the downstream propagation of Content Stream management information as explained in Section 2.5.1 and Section 2.5.2 respectively. Authentication with repeaters may be implemented by the HDCP Transmitter in parallel with the flow of encrypted content and Link Synchronization. The Link Synchronization process is explained in Section 2.6.</td>
</tr>
<tr>
<td>Section 4.3.2 AKE_Send_Cert (Receiver to Transmitter) Page 60</td>
<td>The HDCP Receiver sets REPEATER to ‘true’ if it is an HDCP Repeater and ‘false’ if it is an HDCP Receiver that is not an HDCP Repeater. When REPEATER = ‘true’, the HDCP Receiver supports downstream connections as permitted by the Digital Content Protection LLC license.</td>
</tr>
</tbody>
</table>

**Ref-2C-4.**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Section 2.2 Authentication and Key Exchange Page 16 | The HDCP Receiver
- Sends AKE_Send_Cert message in response to AKE_Init
- If AKE_Transmitter_Info message is received, sends AKE_Receiver_Info message to the transmitter after sending the AKE_Send_Cert message to the transmitter.
- Generates and sends 64-bit $r_x$ as part of the AKE_Send_rrx message immediately after receiving either AKE_No_Stored_km or AKE_Stored_km message from the transmitter. |
| Section 2.2 Authentication and Key Exchange Page 13 | The HDCP Transmitter
- Receives AKE_Receiver_Info message from the receiver if the receiver is not an HDCP 2.0-compliant Device. If AKE_Receiver_Info message is not received within 100 ms from the transmission of the AKE_Transmitter_Info message, it indicates to the HDCP Transmitter that the attached HDCP Receiver is an HDCP 2.0-compliant Device. |
Ref-2C-5.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 4.3.19 AKE_Receiver_Info (Receiver to Transmitter) Page 67</td>
<td>LENGTH parameter is the size of the AKE_Receiver_info message in bytes. An HDCP 2.3-compliant Receiver will set the LENGTH parameter equal to six bytes i.e. the combined size of the msg_id, LENGTH, VERSION and RECEIVER_CAPABILITY_MASK parameters. An HDCP 2.3-compliant transmitter that receives an AKE_Receiver_Info message with the LENGTH parameter greater than six bytes must read the msg_id, LENGTH, VERSION and RECEIVER_CAPABILITY_MASK parameters and must ignore the remaining parameters. The HDCP Receiver must set VERSION to 0x03.</td>
</tr>
</tbody>
</table>

Table 4.26 RECEIVER_CAPABILITY_MASK Parameter

| Bits 15:1:Reserved zeros.                                                | Bit 0: RECEIVER_LOCALITY_PRECOMPUTE_SUPPORT. When this bit is set to one, it indicates that the HDCP Receiver supports pre-computation of $L'$ during the locality check protocol. |

Ref-2C-6.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Section 2.3 Locality Check Page 20                                        | If the HDCP Transmitter is HDCP 2.0-compliant or if the TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT bit received as part of the AKE_Transmitter_Info message is set to zero or if the receiver has set the RECEIVER_LOCALITY_PRECOMPUTE_SUPPORT bit to zero in its AKE_Receiver_Info message, the HDCP Receiver
  - Computes a 256-bit value $L' = \text{HMAC-SHA256}(r_n, k_d \text{ XOR } r_{rx})$
  - Sends LC_Send_L_prime message containing 256-bit $L'$
If the TRANSMITTER_LOCALITY_PRECOMPUTE_SUPPORT bit received as part of the AKE_Transmitter_Info message is set to one and the receiver has set the RECEIVER_LOCALITY_PRECOMPUTE_SUPPORT bit to one in its AKE_Receiver_Info message, the HDCP Receiver
  - Computes 256-bit $L' = \text{HMAC-SHA256}(r_n, k_d \text{ XOR } r_{rx})$ if AKE_Transmitter_Info.VERSION = 0x01
  - Computes 256-bit $L' = \text{HMAC-SHA256}(r_n | r_n, k_d \text{ XOR } r_{rx})$ if AKE_Transmitter_Info.VERSION is not equal to 0x01
  - Sends RTT_Ready message to the transmitter when $L'$ calculation is complete and the receiver is ready for the RTT Challenge
  - On receiving the RTT_Challenge message from the transmitter, if the value received in the RTT_Challenge message matches the least
<table>
<thead>
<tr>
<th>State A2: Locality Check</th>
<th>State A2: Locality Check. In this state, the HDCP Transmitter implements the locality check as explained in Section 2.3 with the HDCP Receiver.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transition A2:H1</td>
<td>Transition A2:H1. This transition occurs on one or more consecutive locality check failures. Locality check fails when $L'$ (or the most significant 128-bits of $L'$) is not received within 7 ms and the watchdog timer at the HDCP Transmitter expires or on a mismatch between $L$ and $L'$ (or the most significant 128-bits of $L'$).</td>
</tr>
</tbody>
</table>

significant 128 bits of $L'$, the receiver sends an LC_SEND_L_prime message containing the most significant 128-bits of $L'$. |
Ref-3C Upstream Procedure with Transmitter

Ref-3C-1

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 2.5.1 Upstream Propagation of Topology Information Page 26</td>
<td>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 = ‘true’ 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 = ‘true’ 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 must not transmit V’ (or the most significant 128-bits of V’), DEPTH, DEVICE_COUNT, Receiver ID list and if applicable, HDCP2_0_REPEATER_DOWNSTREAM and HDCP1_DEVICE_DOWNSTREAM.</td>
</tr>
</tbody>
</table>

Ref-3C-2

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 2.5.1 Upstream Propagation of Topology Information Page 25</td>
<td>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).</td>
</tr>
</tbody>
</table>

Ref-3C-3
### Transition C8:C5

**Page 47**

**Transition C8:C5.** This transition occurs only if the upstream HDCP Transmitter is not HDCP 2.0-compliant and on detection of any changes to the topology.

This transition occurs when a downstream port that was previously in the unauthenticated (State P1) or unconnected (State P0) state transitions to the authenticated (State F5) state. For example, the transition may occur when a new HDCP Receiver is connected to a downstream port, that previously had no receiver connected, and the downstream port completes the authentication protocol with the HDCP Receiver. This transition also occurs when a downstream port that was previously in an authenticated state transitions in to an unauthenticated or unconnected state. For example, the transition may occur when an active, authenticated HDCP Receiver attached to the downstream port is disconnected. Reception of a RepeaterAuth_Send_ReceiverID_List message on a downstream port from the connected HDCP Repeater also causes this transition.

---

### Ref-3C-4

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 2.10 HDCP Repeater State Diagrams Page 37</td>
<td>When the upstream HDCP-protected interface port of the HDCP Repeater is in an unauthenticated state, it signals the detection of an active downstream HDCP Receiver to the upstream HDCP Transmitter by propagating the Receiver Connected Indication to the upstream HDCP Transmitter. Whenever authentication is initiated by the upstream HDCP Transmitter by sending AKE_Init, the HDCP Repeater immediately initiates authentication on all its downstream HDCP-protected interface ports if its downstream ports are in an unauthenticated state. The HDCP Repeater may cache the latest Receiver ID list and topology information received from its downstream ports. Whenever authentication is attempted by the upstream transmitter by sending an ( r_u ) value, the HDCP Repeater may propagate the cached Receiver ID list upstream without initiating a re-authentication on all its downstream ports.</td>
</tr>
</tbody>
</table>

---

### Ref-3C-5

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 2.5 Authentication with Repeaters</td>
<td>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</td>
</tr>
</tbody>
</table>
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 Repeater, with which the HDCP Repeater has successfully completed the authentication protocol. This total number is represented in the RepeaterAuth_Send_ReceiverID_List message by the DEVICE_COUNT value. An HDCP-protected Interface Port with no active device connected adds nothing to the list. Also, the Receiver ID of the HDCP Repeater itself at any level is not included in its own Receiver ID list. An HDCP-protected Interface Port connected to an HDCP Receiver that is not an HDCP Repeater adds the Receiver ID of the connected HDCP Receiver to the list. HDCP-protected Interface Ports that have an HDCP Repeater connected add the Receiver ID list received from the connected downstream HDCP Repeater plus the Receiver ID of the connected HDCP Repeater itself.

**Transition F1:P1**

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:P1**

This transition occurs on one or more consecutive locality check failures. Locality check fails when L' (or the most significant 128-bits of L') is not received within 7 ms and the watchdog timer at the downstream side expires or on a mismatch between L and L' (or the most significant 128-bits of L').

**Ref-3C-6**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.11 RepeaterAuth_Send_ReceiverID_List (Receiver to Transmitter) Page 64</td>
<td>The HDCP Repeater sets HDCP2_LEGACY_DEVICE_DOWNSTREAM = 'true' if an HDCP 2.0-compliant Device or HDCP 2.1-compliant Device is attached to any one of its downstream ports, else it sets HDCP2_0_REPEATER_DOWNSTREAM = 'false'. The HDCP Repeater sets HDCP1DEVICE_DOWNSTREAM = 'true' if an HDCP 1.x-compliant Device i.e. an HDCP 1.x-compliant Receiver or an HDCP 1.x-compliant Repeater is attached to any one of its downstream ports, else it sets HDCP1DEVICE_DOWNSTREAM = 'false'.</td>
</tr>
</tbody>
</table>

**Ref-3C-7**

Page 130 of 131
When an HDCP Receiver (including HDCP Repeater) is connected to the HDCP Repeater or when a connected, active HDCP Receiver with which the HDCP Repeater has successfully completed the authentication protocol is disconnected from the HDCP Repeater and the upstream HDCP Transmitter is not HDCP 2.0-compliant, the HDCP Repeater must send the RepeaterAuth_Send_ReceiverID_List message to the upstream HDCP Transmitter which must include the Receiver IDs of all connected and active downstream HDCP Receivers with which the HDCP Repeater has successfully completed the authentication protocol. This enables upstream propagation of the most recent topology information after changes to the topology without interrupting the transmission of HDCP Content.

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1 Upstream Propagation of Topology Information Page 25</td>
<td>When an HDCP Receiver (including HDCP Repeater) is connected to the HDCP Repeater or when a connected, active HDCP Receiver with which the HDCP Repeater has successfully completed the authentication protocol is disconnected from the HDCP Repeater and the upstream HDCP Transmitter is not HDCP 2.0-compliant, the HDCP Repeater must send the RepeaterAuth_Send_ReceiverID_List message to the upstream HDCP Transmitter which must include the Receiver IDs of all connected and active downstream HDCP Receivers with which the HDCP Repeater has successfully completed the authentication protocol. This enables upstream propagation of the most recent topology information after changes to the topology without interrupting the transmission of HDCP Content.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reference</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.1 Upstream Propagation of Topology Information Page 24</td>
<td>When an HDCP Repeater receives HDCP2_LEGACY_DEVICE_DOWNSTREAM = ‘true’ or HDCP1DEVICE_DOWNSTREAM = ‘true’ from a downstream HDCP Repeater, it must propagate this information to the upstream HDCP Transmitter by setting the corresponding values to ‘true’ in the RepeaterAuth_Send_ReceiverID_List message.</td>
</tr>
</tbody>
</table>