High-bandwidth Digital Content Protection System

Amendment of Interface Independent Adaptation for HDCP Professional

Revision 2.2

07 September, 2016

Digital Content Protection LLC

Notice

Acknowledgement

Biamp Systems and Exterity have contributed to the development of this specification.

Intellectual Property

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

Contact Information

Digital Content Protection LLC
C/O Vital Technical Marketing, Inc.
3855 SW 153rd Drive
Beaverton, OR 97006

Email: info@digital-cp.com

Web: www.digital-cp.com

Revision History

Table of Contents

1. Introduction

1.1 Scope

This specification, referred to as HDCP Professional, Revision 2.2, describes the requirements for the implementation of HDCP in Professional AV systems. This document is an amendment to the "High-bandwidth Digital Content Protection (HDCP) System: Interface Independent Adaptation, Revision 2.2" specification. This specification is designed for the Professional AV industry and enables the support of relaxed topology limits within an HDCP System. The requirements described in this specification only apply to HDCP Professional Repeaters. This specification can be applied over any wired or wireless interface as explained in subsequent chapters.

Implementations must include all elements of the content protection system applicable to HDCP Repeaters that are described herein and in the HDCP IIA specification, Revision 2.2, unless the element is specifically identified as informative or optional. Where the mandatory or optional requirements specified in the HDCP IIA specification and this specification are different, the mandatory or optional requirements specified in this specification take precedence for the implementation of HDCP Professional Repeaters. Adopters must also ensure that implementations satisfy the robustness and compliance rules described in the technology license.

Device discovery and association, and link setup and teardown, is outside the scope of this specification.

1.2 Definitions

This amendment adds the following definition under Section 1.2.

Exempt HDCP Professional Repeaters. HDCP Professional Repeaters that are exempt by DCP LLC from downloading the SRM at least once every quarter, are referred to as Exempt HDCP Professional Repeaters.

HDCP Professional Repeater. An HDCP Repeater that is designed in adherence to HDCP Professional, Revision 2.20, is referred to as an HDCP Professional Repeater.

2. Authentication Protocol

This amendment adds the following requirement under Section 2.5.

2.1 Authentication with Repeaters

The downstream port of an HDCP Professional Repeater must be HDCP2.2-compliant, whereas the upstream port of an HDCP Professional Repeater may be HDCP1.4-compliant or HDCP2.2-compliant.

HDCP Professional Repeaters are not required to enforce topology limits i.e. if the computed DEVICE_COUNT or DEPTH exceeds thirty one or four respectively, such repeaters are not required to treat the condition as an error and are not required to set the MAX_DEVS_EXCEEDED or MAX_CASCADE_EXCEEDED values to 'true' (See the state diagram in Section 2.3). When an HDCP Professional Repeater receives a MAX_DEVS_EXCEEDED or a MAX_CASCADE_EXCEEDED error from a downstream HDCP Repeater, it need not propagate the error to the upstream HDCP Transmitter.

The HDCP Professional Repeater must report itself as an HDCP Receiver that is not an HDCP Repeater to the most upstream HDCP Transmitter (for e.g. by setting the REPEATER bit to 0), if the upstream port of such HDCP Professional Repeater is HDCP1.x-compliant. The HDCP Professional Repeater must report itself as an HDCP Repeater (for e.g. by setting REPEATER ='true' in the AKE_Send_Cert message as defined in the HDCP IIA specification, Revision 2.2), with a DEPTH value equal to 1 and DEVICE_COUNT value equal to 1, to the most upstream HDCP Transmitter, if the upstream port of such HDCP Professional Repeater is HDCP2.2-compliant. It must populate the Receiver ID list with the *Receiver ID* of any one of the HDCP Devices attached to its downstream port and must propagate the DEVICE_COUNT (which is set to 1), DEPTH (which is set to 1), Receiver ID list and other values as part of the RepeaterAuth_Send_ReceiverID_List message to the upstream HDCP Transmitter.

The HDCP Professional Repeater is required to manage System Renewability Messages (SRMs) carrying the Receiver ID revocation list. The validity of an SRM is established by verifying the integrity of its signature with the Digital Content Protection LLC public key, which is specified by the Digital Content Protection LLC. The HDCP Professional Repeater must periodically download an HDCP 2 SRM and a corresponding timestamp, *timestamp*, from https://www.digital-cp.com/sites/default/files/resources/HDCP2.SRM and https://www.digital-cp.com/sites/default/files/HDCPPro.timestamp respectively. The downstream port of the HDCP Professional Repeater must verify the integrity of the SRM by checking the signature of the SRM using $kpub_{dcp}$. Failure of this integrity check must constitute an authentication failure and must cause the HDCP Professional Repeater to abort the authentication protocol with all the downstream HDCP Devices that are attached to the HDCP Professional Repeater. The HDCP Professional Repeater must also check to see if the *Receiver ID* of the connected device, or any of the *Receiver ID*s received as part of the Receiver ID list from the attached downstream HDCP Repeater, is found in the revocation list. If any downstream *Receiver ID* is found in the revocation list, authentication must fail and the authentication protocol must be aborted with all the downstream HDCP Devices that are attached to the HDCP Professional Repeater.

DCP LLC publishes the most recent SRM and a corresponding *timestamp*, at https://www.digital-cp.com/sites/default/files/resources/HDCP2.SRM and https://www.digital-cp.com/sites/default/files/HDCPPro.timestamp respectively, once

every quarter on a specific date. The date of timestamp publication is Feb 1st, May 1st, Aug 1st, Nov 1st of every year (GMT). HDCP Professional Repeaters may attempt to download the SRM on the dates specified above, but must be designed to recognize that they may not receive the most recent SRM and timestamp information on those dates. HDCP Professional Repeaters, except Exempt HDCP Professional Repeaters, must download the most recent SRM at least once every quarter i.e. the maximum duration between subsequent SRM downloads must be one quarter. If the SRM download fails, the HDCP Professional Repeater must reattempt the download. If the HDCP Professional Repeater is not able to successfully download the most recent SRM at least once in any given quarter, it must not function as an HDCP Professional Repeater, but may function as an HDCP Repeater that is not an HDCP Professional Repeater.

Exempt HDCP Professional Repeaters may be configured to download SRMs either when notified by DCP LLC or at a DCP-approved periodicity.

The *timestamp* specifies the most recent SRM version published by DCP LLC and is constructed as given below. All values are in big-endian order.

> HDCP2.x SRM Version (16-bits) || Date Time (32-bits) || DCP LLC Signature (3072-bits), where
>
> Date Time = Binary Representation [4-digit Year (16-bits) || Month (8-bits) || Day (8-bits)]

The latest HDCP2.x SRM Version is concatenated with the date when the timestamp was published by DCP LLC and the DCP LLC Signature. The date is represented in Greenwich Mean Time (Zulu time). For e.g. Jan 1, 2012 is represented as 0000011111011100 00000001 00000001. The date will be set by DCP LLC to the date of timestamp publication. The DCP LLC signature is calculated over (HDCP2.x SRM Version || 4-digit Year || Month || Day). RSASSA-PKCS1-v1_5 is the signature scheme used as defined by PKCS #1 V2.1: RSA Cryptography Standard. SHA-256 is the underlying hash function.

The latest timestamp information and the most recent SRM will be stored on the HDCP Professional Repeater during its initial operation. Subsequently, the HDCP Professional Repeater receives the latest SRM and timestamp information by downloading it at least once every quarter from https://www.digital-cp.com/sites/default/files/resources/HDCP2.SRM and https://www.digital-cp.com/sites/default/files/HDCPPro.timestamp respectively. The HDCP Professional Repeater must verify the signature on the received timestamp using $kpub_{dcp}$. If signature verification fails, it must not function as an HDCP Professional Repeater, but may function as an HDCP Repeater that is not an HDCP Professional Repeater.

The date information on the timestamp must reflect the most recent date of publication of the timestamp. The HDCP Professional Repeater calculates the most recent date of publication of the timestamp based on the current date as obtained from its own clock. If the date information on the received timestamp precedes the most recent date of

publication as calculated by the HDCP Professional Repeater, it must reject the timestamp and must not function as an HDCP Professional Repeater. For e.g., if the current date as obtained from the internal clock of the HDCP Professional Repeater is July 08th, 2015, the HDCP Professional Repeater calculates the most recent date of publication of the timestamp to be Feb 1st 2015. If the date information on the received timestamp succeeds the current date and time as obtained from its own clock, the HDCP Professional Repeater must accept the received timestamp as the latest timestamp information from https://www.digital-cp.com/sites/default/files/HDCPPro.timestamp.

The HDCP Professional Repeater must verify that the HDCP2.x SRM Version on the timestamp matches the SRM Version field on the downloaded SRM. If there is a mismatch of Version numbers, the HDCP Repeater must not function as an HDCP Professional Repeater, but may function as an HDCP Repeater that is not an HDCP Professional Repeater.

HDCP Professional Repeaters must implement a secure clock such that the download and verification of the most recent SRM and *timestamp*, as required by the HDCP Professional Specification, are reasonably accurately enforced by the HDCP Professional Repeater.

2.2 HDCP Professional Repeater Downstream State Diagram

The downstream state diagram for the HDCP Professional Repeater is the same as the state diagram described in Section 2.10.2 of the HDCP Interface Independent Adaptation, Revision 2.2 Specification, except for the following changes.

State F1: Exchange k_m. In this state, the downstream side 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 downstream side does not receive AKE_Receiver_Info message within 100ms of the transmission of AKE_Transmitter_Info message, it indicates that the HDCP Receiver is an HDCP 2.0-compliant Device.

If the downstream side does not have k_m stored corresponding to the *Receiver ID*, it generates $E_{kpub(km)}$ and sends $E_{kpub(km)}$ as part of the AKE_No_Stored_km message to the receiver after verification of signature on $cert_{rx}$. It performs integrity check on the SRM and checks to see whether the *Receiver ID* of the connected HDCP Device is in the revocation list. It 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 downstream side has k_m stored corresponding to the *Receiver ID*, it sends AKE_Stored_km message containing $E_{kh(km)}$ and *m* to the receiver, performs integrity check on the SRM, checks to see whether the *Receiver ID* of the connected HDCP

Device is in the revocation list, 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 200ms after sending AKE_Stored_km to the receiver and compares *H'* against H.

If the downstream side 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.

Transition F1:P1. This transition occurs on failure of signature verification on $cert_{rx}$, failure of SRM integrity check, if *Receiver ID* of the connected HDCP Device is in the revocation list or if there is a mismatch between H and *H'*. This transition also occurs if AKE_Send_H_prime message is not received within one second after sending AKE_No_Stored_k_m or within 200ms after sending AKE_Stored_km to the receiver.

State F7: Verify Receiver ID List. If a transition in to this state occurs from State F6, the watchdog timer is cleared. If both MAX_DEVS_EXCEEDED and MAX_CASCADE_EXCEEDED are not 'true', computes *V*. If the connected HDCP Repeater is HDCP 2.0-compliant, compares *V* and *V'*. If the connected HDCP Repeater is not HDCP 2.0-compliant, compares the most significant 128-bits of *V* and *V'*. The *Receiver ID*s from the Receiver ID list are compared against the current revocation list.

Transition F7:P1. 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 ID*s in the Receiver ID list are found in the current revocation list or if the downstream side 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 received from the connected HDCP Repeater also causes this transition.

Transition F7:F5. This transition is made 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.

Transition F7:F8. This transition occurs if the connected HDCP Repeater is not HDCP 2.0-compliant, on successful verification of the most significant 128-bits of *V* and *V'*, none of the reported *Receiver IDs* are in the current revocation list, the downstream side does not detect a roll-over of *seq_num_V* and the downstream topology does not exceed specified maximums.

2.3 HDCP Professional Repeater Upstream State Diagram

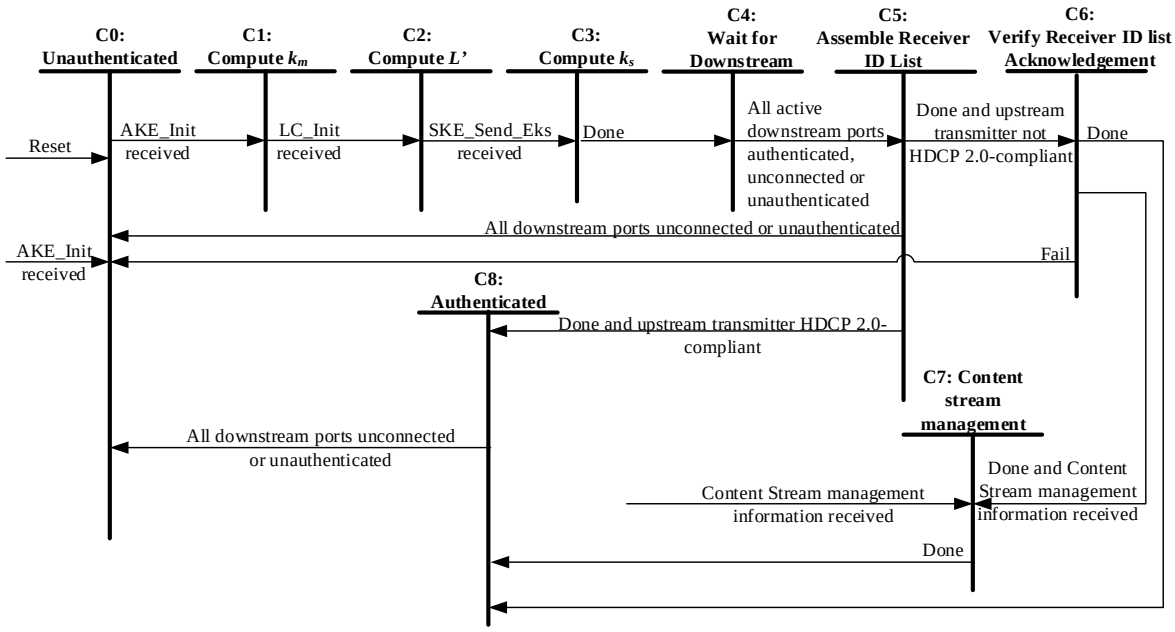

Figure 2.17. HDCP Repeater Upstream Authentication Protocol State Diagram

The HDCP Professional Repeater upstream state diagram, illustrated in Figure 2.17, makes reference to states of the HDCP Professional Repeater downstream state diagram. The upstream state diagram for the HDCP Professional Repeater is the same as the state diagram described in Section 2.10.3 of the HDCP Interface Independent Adaptation, Revision 2.2 Specification, except for the following changes.

State C5: Assemble Receiver ID List. The upstream side populates the Receiver ID list with the *Receiver ID* of any HDCP Receiver attached to its downstream port, where the downstream port arrives in State F5, and must propagate the DEVICE_COUNT (which is set to 1), DEPTH (which is set to 1), Receiver ID list and other values as part of the RepeaterAuth_Send_ReceiverID_List message to the upstream HDCP Transmitter.

The upstream side then computes *V'* and sends RepeaterAuth_Send_ReceiverID_List message to the upstream HDCP Transmitter. When the upstream side receives a MAX_DEVS_EXCEEDED or MAX_CASCADE_EXCEEDED error from a downstream HDCP Repeater, it need not propagate the error to the upstream HDCP Transmitter.

If the computed DEVICE_COUNT or DEPTH at the upstream side exceeds thirty one or four respectively, the upstream port does not treat the condition as an error and does not set the MAX_DEVS_EXCEEDED or MAX_CASCADE_EXCEEDED values to 'true' in the RepeaterAuth_Send_ReceiverID_List message.

If any downstream port connected to an HDCP Repeater receives HDCP2_0_REPEATER_DOWNSTREAM = 'true' or HDCP1_DEVICE_DOWNSTREAM = 'true', the upstream side sets the corresponding values to 'true' in the RepeaterAuth_Send_ReceiverID_List message to the upstream HDCP Transmitter.

Transition C5:C0. This transition occurs if all downstream HDCP-protected Interface Ports have reached the state of unconnected or unauthenticated.

Transition C5:C6. RepeaterAuth_Send_ReceiverID_List message has been sent to the upstream HDCP Transmitter and upstream transmitter is not HDCP 2.0-compliant.

Transition C5:C8. RepeaterAuth_Send_ReceiverID_List message has been sent to the upstream HDCP Transmitter upstream transmitter is HDCP 2.0-compliant.

Delete **Transition C8:C5.**

Transition C8:C0. This transition occurs if all downstream HDCP-protected Interface Ports have reached the state of unconnected or unauthenticated.

Note: Since Link Synchronization may be implemented in parallel with the upstream propagation of topology information (State C4, State C5 and State C6) and Content Stream management (State C7), the link synchronization process (i.e. State C8) may be implemented asynchronously from the rest of the state diagram. The transition into State C8 may occur from any state for which encryption is currently enabled. Also, the transition from state C8 may return to the appropriate state to allow for undisrupted operation.

The upstream side must be prepared to implement the link synchronization process in parallel with the upstream propagation of topology information and Content Stream management if these stages are implemented in parallel by the upstream transmitter.