HDCP for Bluetooth

HDCP overview and its use in Miracast and AVDTP

16-Sep-16

Author: Binu E R

Abstract

High-Bandwidth Digital Content Protection (HDCP) enables secure audio and video distribution over a wide range of digital audiovisual interconnection technologies. This whitepaper provides an overview of HDCP 2.2 and explains how it works over wired technologies like HDMI2.0, HDBaseT, DisplayPort, MHL, USB as well as wireless technologies like Miracast, WirelessHD and WHDI. It further describes how HDCP can be extended for use in applications like Bluetooth for AVDTP.

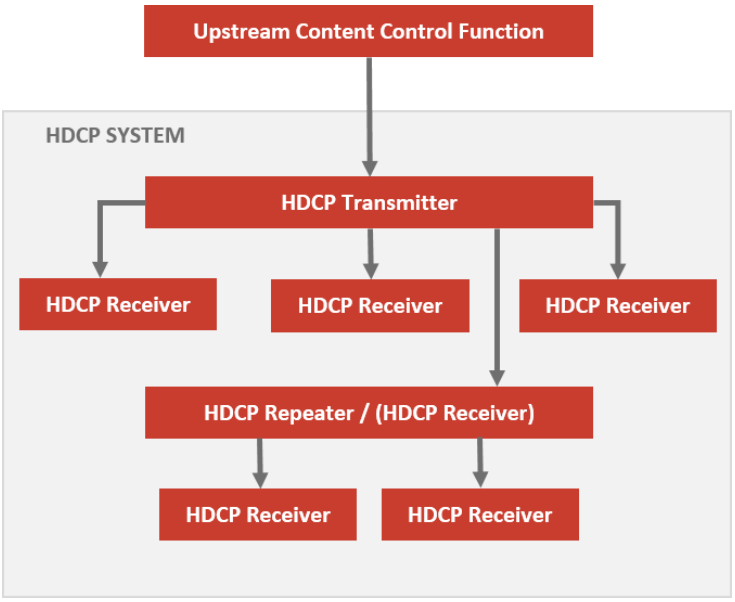

Figure 1 - Overview

Contents

Figures

Tables

Introduction

Bluetooth specifies Audio/Video Distribution Transport Protocol (AVDTP) for audio and/or video distribution connections and streaming of audio or video media over the Bluetooth air interface. It defines the signaling for stream setup (negotiation and establishment) and the mechanism for media transmission for audio and video over Logical Link Control and Adaptation Protocol (L2CAP) layer.

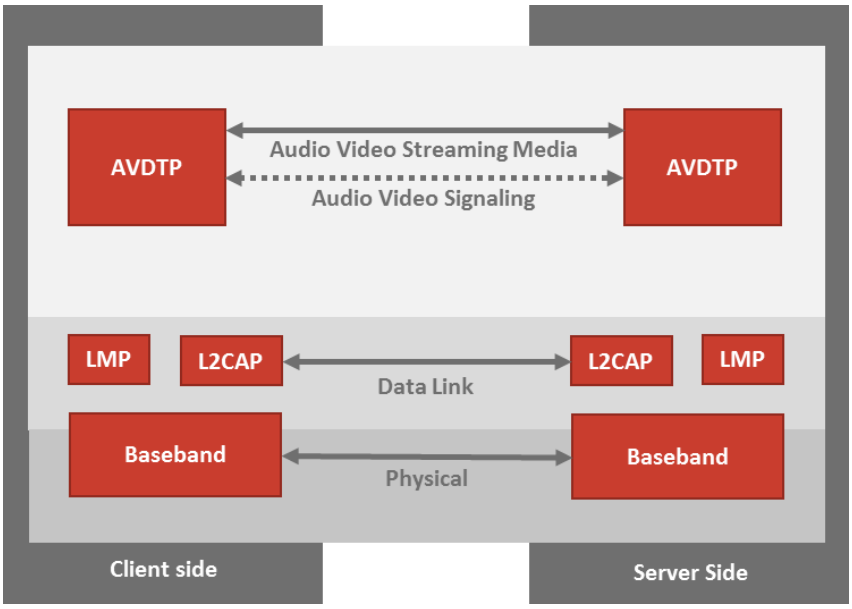

Figure 2 – AVDTP Overview

Digitization of audiovisual content and its transmission (like in the case of AVDTP) results in dramatic improvement in reproduction quality across the transmission and display pipelines. Along with this zero loss reproduction mechanism, unauthorized storage and reproduction of copyrighted content becomes an even bigger challenge. One of the more recent and most common audiovisual interconnect currently is HDMI (1.0 version) and it employs a content protection mechanism known as High-bandwidth Digital Content Protection (HDCP) version 1.x. HDCP defines a mechanism for authentication of the receiver by the transmitter and encryption of the flow of data between the two.

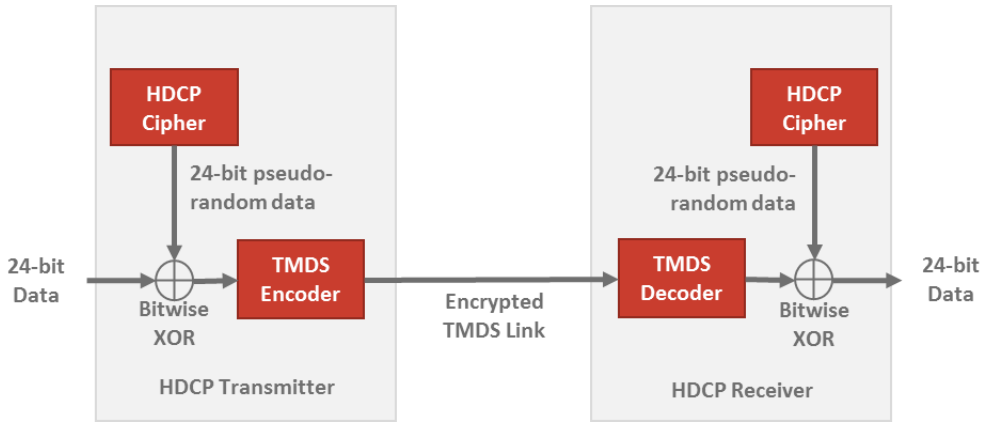

Figure 3 – HDCP Overview

HDCP 2.x, the successor to HDCP 1.x, is now widely used even beyond HDMI in various wired and wireless audiovisual interconnects. In general, raw uncompressed video requires a wired medium and wireless medium uses compressed video due to the comparatively limited bandwidth availability.

The following list includes popular wired interconnects that use HDCP 2.2:

- HDMI 2.0
- DVI
- HDBaseT
- DisplayPort
- MHL
- USB
- DiiVA
- DLI

The following list includes popular wireless interconnects that use HDCP 2.2:

- Wi-Fi Display (Miracast)
- WHDI
- WirelessHD

HDCP

HDCP system consists of a transmitter connected with one or more downstream receivers. As part of content protection, the transmitter takes care of the following:

- Authenticating the receiver
- Encryption of audiovisual content

HDCP uses a low speed bidirectional control/status path used for authentication and a unidirectional high speed path for audiovisual data.

Authentication

HDCP authentication involves Authentication Key Exchange, Locality Check, Session Key Exchange and authentication with repeaters. In the authentication key exchange stage, the transmitter verifies the receiver's public key certificate. The transmitter also performs a locality check to ensure reasonable proximity of the receiver through an echo message to assess if the round trip delay is under 7ms. Pairing the receiver and transmitter for subsequent authentications helps to speed up the Authentication Key Exchange.

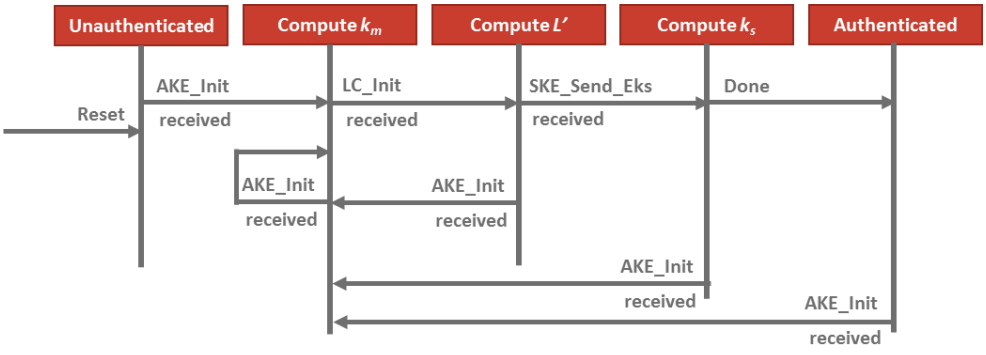

Figure 4 – HDCP Authentication

The transmitter checks if the receiver ID is part of the revocation list and if it is, the authentication fails. The transmitter also periodically receives the revocation list as part of the system renewability messages.

Encryption

HDCP encryption involves bitwise exclusive or (XOR) of audiovisual data (in interface specific format) with a pseudo-random data stream (Cipher Word) generated by the HDCP Cipher. The size of the Cipher Word is interface specific and varies from 24bit to 128bit.

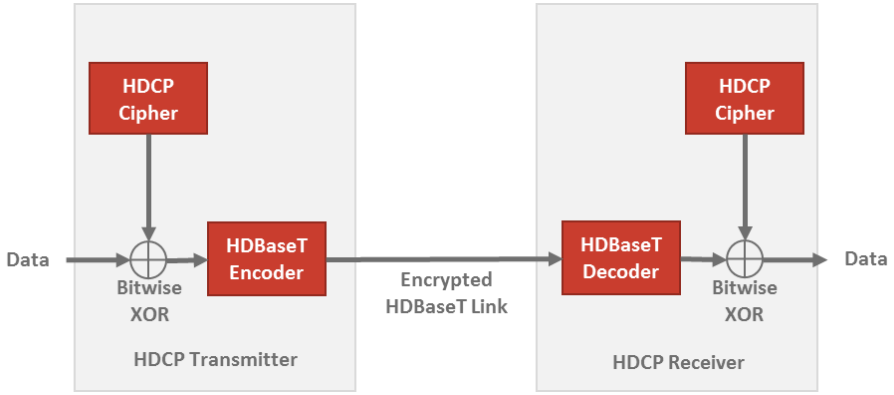

Figure 5 – HDCP Encryption

HDCP in Miracast

Wi-Fi Display (Miracast) defines an interoperable mechanism to discover, pair, connect and render multimedia content sourced wirelessly from a remote source at a sink device. It uses Wi-Fi P2P (Wi-Fi Direct) or Tunneled Direct Link Setup (TDLS) for device discovery and pairing. RTSP is used for capability negotiation and session establishment. The multimedia content streaming over RTP uses MPEG Transport Stream. The video codec used is H.264 and audio codec can be either AAC, AC-3 or LPCM. The complete stack for media streaming is shown in the figure below.

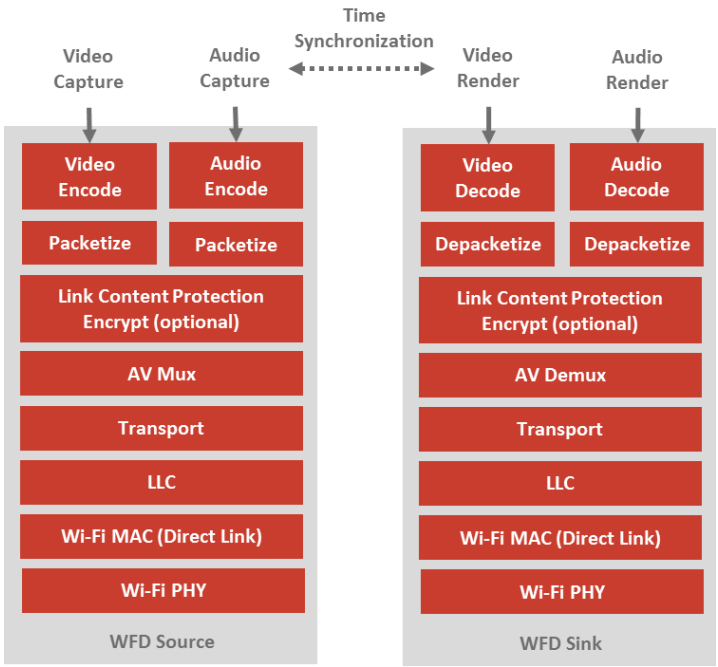

Figure 6 – Miracast/WiFi Display Stack

HDCP based content protection is used to encrypt the PES data of MPEG-TS during transmission. The application layer performs the content protection in an interface independent manner without using

Wi-Fi interface specific mechanisms. HDCP authentication uses a bi-directional TCP connection between the source and sync devices. This TCP connection is kept alive for the complete duration of the connection to facilitate session key renewal. If this connection closes, the associated RTP data stream also stops and the Miracast connection is shut down.

HDCP Encryption is performed only for the PES payload data and the PES headers are not encrypted. Encryption involves performing an XOR operation of the key stream from AES-CTR with the 128 bits of PES payload to produce 128 bits of encrypted output for transmission.

Mapping HDCP for Bluetooth AVDTP

AVDTP defines signaling procedures for announcing Content Protection capabilities during the stream configuration procedure. An earlier version of the standard defines two values for the content protection type – 0 for DTCP and 1 for SCMS-T. But the DTCP mapping is now deemed obsolete and SCMS is out dated. As a result, recent revisions of the specification do not suggest any specific content protection mechanisms and leave it open to the implementer. Hence, implementers need to specifically map HDCP2.2 for content protection in AVDTP.

The HDCP authentication can be performed as part of the Content Security Control procedure. The below table describes the standard Service Capabilities field for single content protection mechanism (e.g. HDCP alone).

7	6	5	4	3	2	1	0	Octet
Service Category = Content Protection								0
LOSC = (n-1 bytes)								1
CP_TYPE_LSB = CP_TYPE_A_LSB								2
CP_TYPE_MSB = CP_TYPE_A_MSB								3
CP_Type Specific Values								n

Table 1 - Service Capabilities Field

The Service Category field is used to indicate the Content Protection message. For HDCP case, CP_TYPE_A_LSB can be set to 0xFF and CP_TYPE_A_MSB to 0xF. The CP_Type Specific Values are mapped to contain the data structures required for AKE/SKE exchange.

Figure The overall Content Security Control procedure flow between the Upper Layer (UL) applications on both ends through AVDTP is shown in figure below. This procedure needs to be performed for Authentication Key Exchange, Locality Check as well as Session Key Exchange.

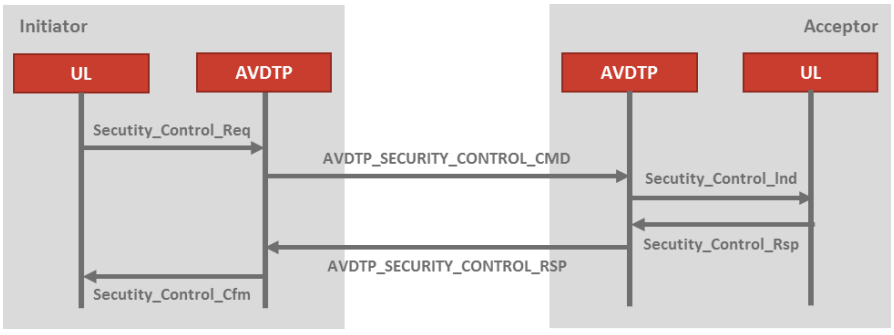

Figure 7 – Content Security Control Procedure through AVDTP

The Reporting Service of Transport procedures can be alternatively used for Session Key renewal and keep alive indication. The private extensions (PRIV) item of Source Description packet (SDES) is used for this purpose.

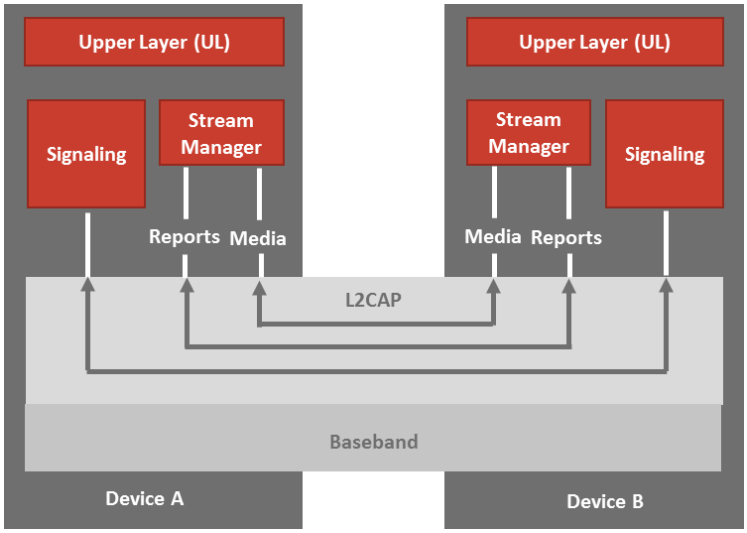

Figure 8 – Stream Management

The Upper Layer (UL) application generates the 128 bit HDCP Cipher used to encrypt the media packets. The peer end UL application performs the decryption.

Availability at Ittiam

Ittiam provides a comprehensive HDCP software stack optimized for various platforms. It is open source free and can be licensed independently for encryption and decryption. As a reference, performance numbers for an ARM Cortex A15 based platform is listed in Table 1.

Operation	Performance
Encryption	58MCPS for 6Mbps stream
Decryption	78MCPS for 6Mbps stream

Table 2 – Cortex-A15 HDCP Performance

In addition to HDCP stack, Ittiam also provides the complete Miracast Sink Solution as well as highly optimized Video (H264) and Audio (AAC/AC3) codecs for Miracast and Bluetooth AVDTP use cases.

Conclusion

HDCP 2.2 is a truly versatile content protection mechanism that can be used in an interface independent manner at the application layer (as seen with Wi-Fi Display use case) or can be 'built into' the interface itself (as seen in HDBaseT use case). It can also be mapped to additional use cases like AVDTP streaming in Bluetooth as illustrated here in this paper. Unlike HDCP1.x, HDCP2.x is best implemented in software and Ittiam has the optimal solution for the same.

References

1. Audio/Video Distribution Transport Protocol Specification Rev. 1.3
2. HDCP Specification Rev. 2.2 Interface Independent Adaptation
3. Wi-Fi Display Specification Rev. 1.1

4. HDCP 2.2 on HDMI Specification
5. DTCP Volume 1 Supplement C Mapping DTCP to Bluetooth
6. RFC 1889 – RTP: A Transport Protocol for Real-Time Applications

Disclaimer

This white paper is for informational purposes only. Ittiam makes no warranties, express, implied or statutory, as to the information in this document. The information contained in this document represents the current view of Ittiam Systems on the issues discussed as of the date of publication. It should not be interpreted to be a commitment on the part of Ittiam, and Ittiam cannot guarantee the accuracy of any information presented after the date of publication.