MOST

Media **O**riented **S**ystems **T**ransport

Multimedia and Control Networking Technology

MOST Content Protection Scheme HDCP Implementation Rev 1.2 03/2018

MOSTCO CONFIDENTIAL

See page 3 for the terms of disclosure

Legal Notice

COPYRIGHT

LICENSE DISCLAIMER

Nothing on any MOST Cooperation Web Site, or in any MOST Cooperation document, shall be construed as conferring any license under any of the MOST Cooperation or its members or any third party's intellectual property rights, whether by estoppel, implication, or otherwise.

CONTENT AND LIABILITY DISCLAIMER

MOST Cooperation or its members shall not be responsible for any errors or omissions contained at any MOST Cooperation Web Site, or in any MOST Cooperation document, and reserves the right to make changes without notice. Accordingly, all MOST Cooperation and third party information is provided "AS IS". In addition, MOST Cooperation or its members are not responsible for the content of any other Web Site linked to any MOST Cooperation Web Site. Links are provided as Internet navigation tools only.

MOST COOPERATION AND ITS MEMBERS DISCLAIM ALL WARRANTIES WITH REGARD TO THE INFORMATION (INCLUDING ANY SOFTWARE) PROVIDED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

In no event shall MOST Cooperation or its members be liable for any damages whatsoever, and in particular MOST Cooperation or its members shall not be liable for special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue, or loss of use, arising out of or related to any MOST Cooperation Web Site, any MOST Cooperation document, or the information contained in it, whether such damages arise in contract, negligence, tort, under statute, in equity, at law or otherwise.

FEEDBACK INFORMATION

Any information provided to MOST Cooperation in connection with any MOST Cooperation Web Site, or any MOST Cooperation document, shall be provided by the submitter and received by MOST Cooperation on a non-confidential basis. MOST Cooperation shall be free to use such information on an unrestricted basis.

TRADEMARKS

MOST Cooperation and its members prohibit the unauthorized use of any of their trademarks. MOST Cooperation specifically prohibits the use of the MOST Cooperation LOGO unless the use is approved by the Steering Committee of MOST Cooperation.

SUPPORT AND FURTHER INFORMATION

For more information on the MOST technology, please contact:

MOST Cooperation
Administration
Emmy-Noether-Str. 14
76131 Karlsruhe
Germany

Tel: (+49) (0) 721 966 50 00

E-mail: contact@mostcooperation.com
Web: www.mostcooperation.com

This Specification is Confidential Information of the MOST Cooperation. It may only be disclosed to member companies. Member companies wishing to discuss these Specifications with suppliers or other third parties must ensure that a commercially standard form of non-disclosure agreement has been previously executed by the party receiving such Specifications. Use of these Specifications may only be for purposes for which they are intended by the MOST Cooperation. Unauthorized use or disclosure is a violation of law.

Contents

Bibliography

All documents, which are referenced by this MOST document, are listed here along with their versions.

Document		Revision
[1]	MOST Specification	3.0
[2]	MOST Specification for Stream Transmission	3.0.5
[3]	MOST Content Security Specification	1.3
[4]	HDCP Interface Independent Adaptation Specification	2.1
[5]	ISO/IEC 13818-1 Information technology — Generic coding of moving pictures and associated audio information: Part 1 - Systems	
[6]	MOST GeneralFBlock FBlock Template Specification	3.0.7
[7]	HDCP FBlock Specification	1.0.1

Document History

Content Protection Scheme HDCP Implementation Rev. 1.2

Change Ref.	Section	Changes
1V2_001	Bibliography	Updated reference to MOST Specification for Stream Transmission, HDCP FBlock Specification and GeneralFBlock.
1V2_002	2	Removed HDCP_Status from listed HDCP FBlock functions.
1V2_003	3.2	Combined PES private data and HDCP info bytes into PES header.

Content Protection Scheme HDCP Implementation Rev. 1.1

Change Ref.	Section	Changes
1V1_001	3	– Distinction between A/V Streaming and GenericPCM

Content Protection Scheme HDCP Implementation Rev. 1.0

Change Ref.	Section	Changes
1V0_001	All	– Initial Revision

1 Introduction

1.1 Purpose

This document describes the MOST functions and services required to enable High-bandwidth Digital Content Protection System Interface Independent Adaptation [4].

Note: *Every usage of HDCP requires a license agreement with Digital CP (Digital Content Protection LLC). In particular, the implementation of this HDCP specification on the MOST network requires full compliance with the HDCP license agreement and its procedural appendix, compliance rules, and policy statements. The details of HDCP can be found at www.digital-cp.com.*

1.2 Terms and Abbreviations

BW	BW relates to allocated block width
HDCP	High-bandwidth Digital Content Protection
Sink	The target of a data transfer
Source	The origin of a data transfer
TS	Transport Stream

2 HDCP Functions

The following functions are contained in the *HDCP FBlock Specification [7]*.

FktID	Name
0x0C0	HDCP_ReceiverConnectedIndication
0x0C1	HDCP_ReceiverDisconnectedIndication
0x0C2	HDCP_Control
0x0C4	HDCP_DecipherStatus
0x0C5	HDCP_Assign

Table 2-1: HDCP functions

For MOST, packets use an FBlockID and InstID determined by procedures above the HDCP layer. Also, parameter values spanning more than one byte follow the convention in [1] of sending the most-significant byte first.

An FBlock represents not more than one HDCP transmitter (otherwise addressing with FBlockID and InstID would not be sufficient).
Different MOST sources of the same FBlock will be seen as one HDCP transmitter which uses the same session key; refer to the HDCP Interface Independent Adaptation Specification [4], p. 52.

For RTT the pre-computed option is mandatory.

The following events required by the HDCP Interface Independent Adaptation Specification [4] are mapped to corresponding MOST functions:

HDCP event	MOST function
Receiver Connected Indication	HDCP_ReceiverConnectedIndication
Receiver Disconnected Indication	HDCP_ReceiverDisconnectedIndication
HDCP-capable	This information is provided by SourceInfo / SinkInfo [6]
The Upstream Content Control Function according to [4] is beyond this specification.	

Table 2-2: Mapping HDCP events to MOST functions

3 Protected Content

For implementing the HDCP mechanisms, the data to be protected is encrypted, transmitted and decrypted. Embedded information (e.g., HDCP Info Bytes) has to be transported as part of the encrypted section.

In Figure 3-1, Figure 3-3, and Figure 3-4, the payload is encrypted. In Figure 3-2, it is not encrypted.

3.1 A/V Streaming

Packetizing of streaming content (A/V Packetized)
The streaming content is packetized in a Transport Stream [5].

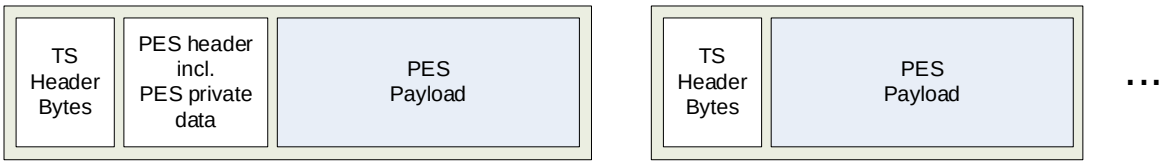

Figure 3-1: Example MOST HDCP

When HDCP encryption is disabled, the PES header HDCP private data block is not included.

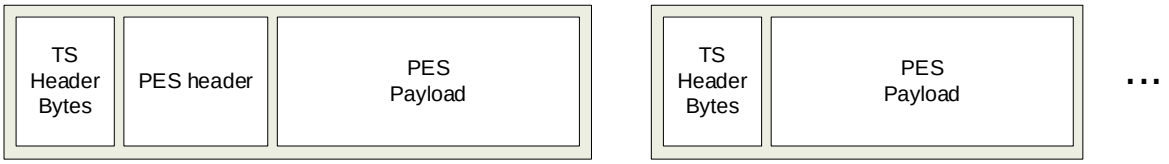

Figure 3-2: Example without HDCP encryption

3.2 GenericPCM

GenericPCM with HDCP (Synchronous Transmission Class)

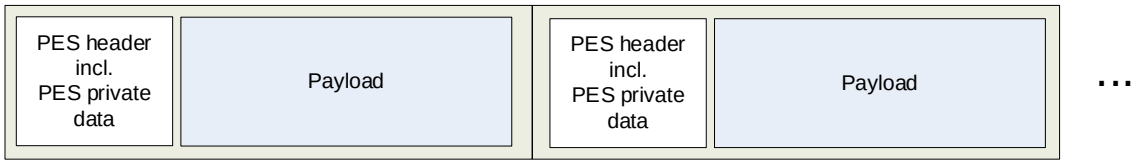

Figure 3-3: Example GenericPCM with HDCP

GenericPCM with HDCP (via PES/TS)
The streaming content is packetized in a Transport Stream [5].

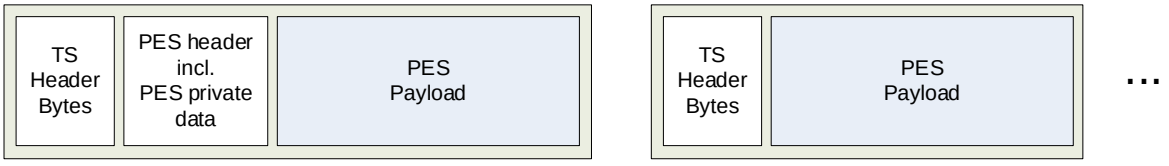

Figure 3-4: Example GenericPCM via PES/TS

4 Message Sequence Charts

The following dynamic specification is an implementation recommendation. There may exist valid reasons in particular circumstances to ignore a particular item, to change its detailed behavior or to add items, etc. However, the full implications (e.g., interoperability) must be understood and carefully weighted before choosing a different course.

4.1 Overview

In the example collaboration diagram, a complete HDCP connection establishment (Authentication followed by a Content Key Exchange) is illustrated.

For reasons of clarity, requests and responses are merged, if possible (without referring to the relevant OPTypes). Otherwise, the communication is outlined by explicitly using the OPTypes.

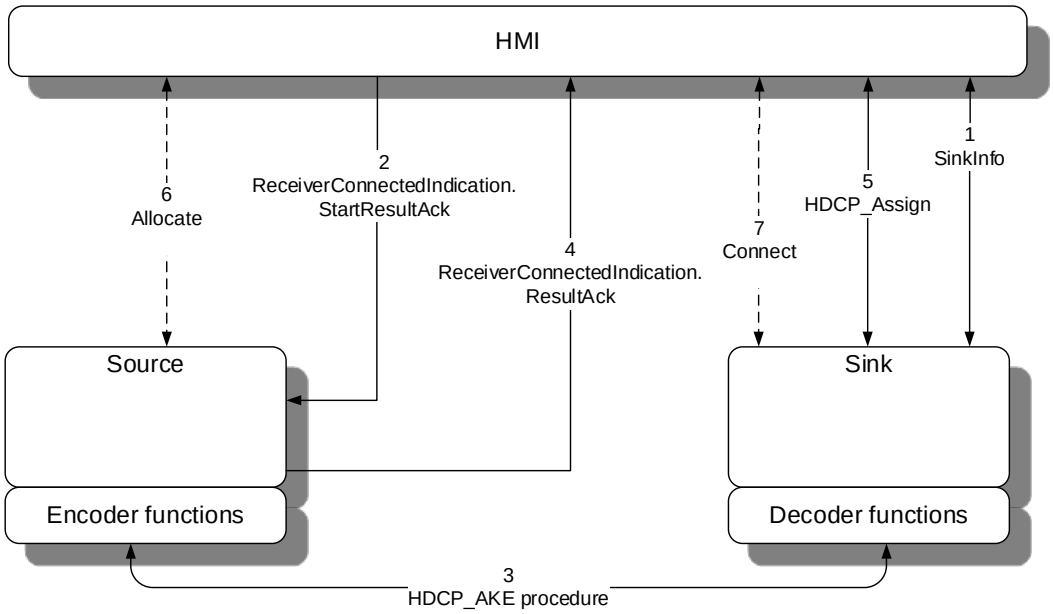

Figure 4-1: Collaboration Diagram 1: HDCP Connection Establishment (Authentication Followed by a Content Key Exchange)

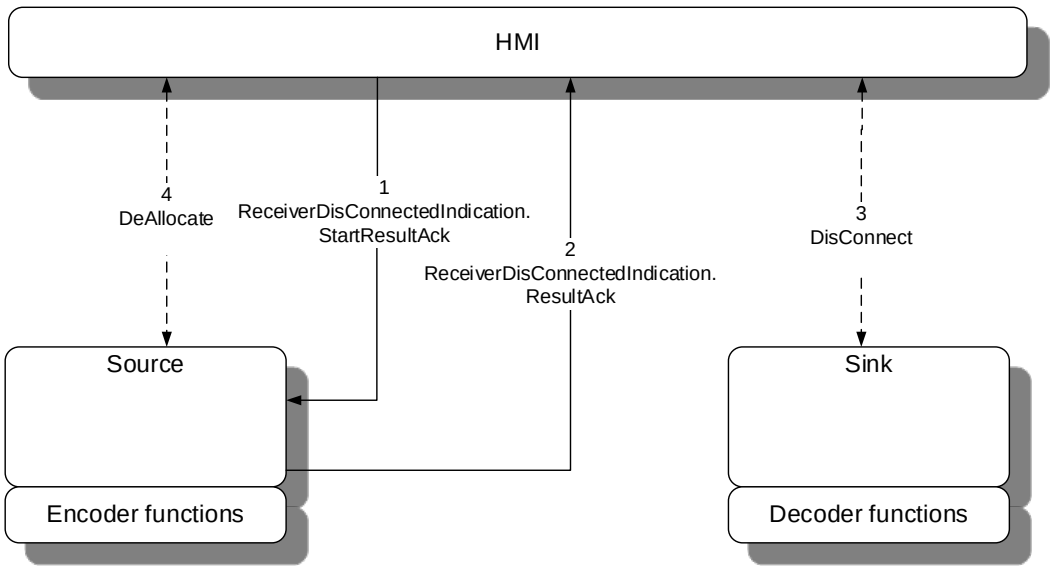

Figure 4-2: Collaboration Diagram 2: HDCP_Disconnection

4.2 The HDCP Receiver is connected

Use Case:	The HDCP receiver is connected		
Description:	The HDCP receiver is connected. If the receiver is HDCP-capable the HDCP Authentication Process is executed.		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
	X		
Remarks:			

Table 4-1: The User Requests an HDCP Audio Connection

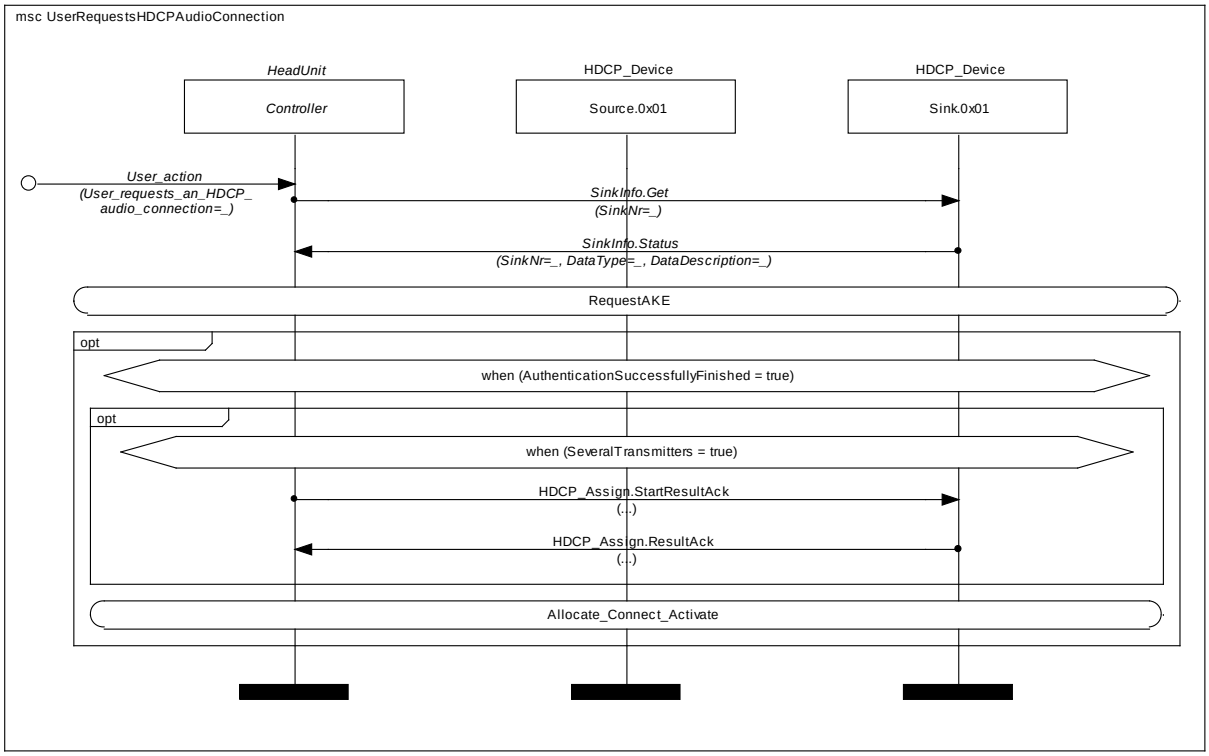

Figure 4-3: The HDCP receiver is connected

4.3 Request Exchange Key Calculation

Use Case:	Request for calculating the Exchange Keys		
Description:	The HeadUnit starts the HDCP Authentication Procedure and therefore initiates the calculation of the Exchange Keys.		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:	The AKE is done on device-level		

Table 4-2: Request Exchange Key Calculation

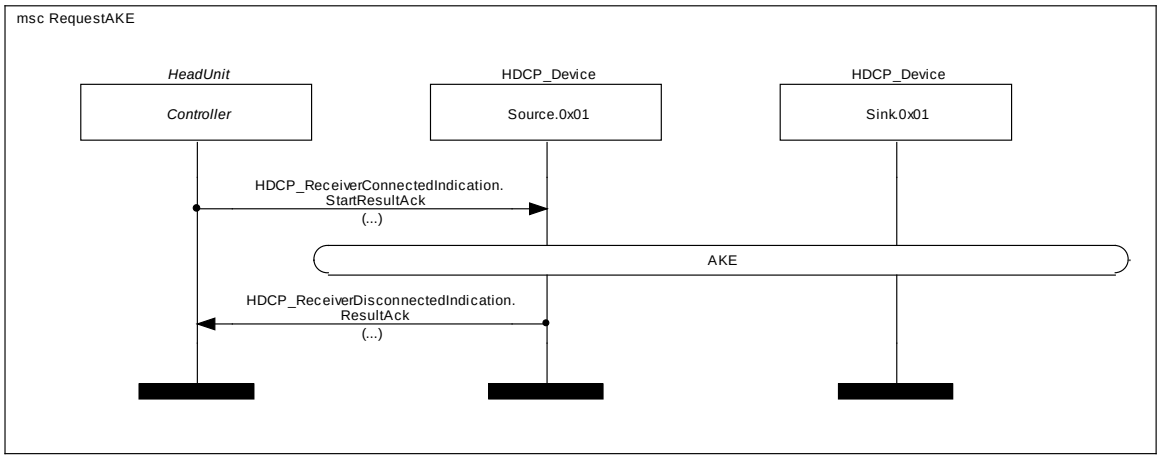

Figure 4-4: Request Exchange Key Calculation

4.4 Allocate, Connect and Activate

Use Case:	Allocate, connect and activate		
Description:	The HeadUnit allocates synchronous timeslots on the MOST network, connects the audio source and sink to it and optionally activates the output of audio data.		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:			

Table 4-3: Allocate, Connect, and Activate

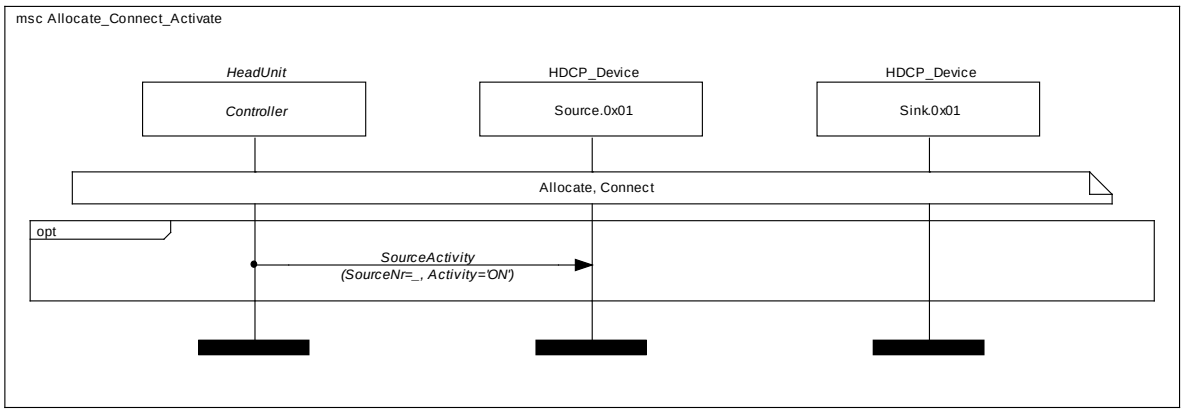

Figure 4-5: Allocate, Connect, and Activate

4.5 Calculate Exchange Key

Perform the exchange key calculation according to HDCP Specification [4].

4.6 SRM

Perform the SRM update according to HDCP Specification [4].

4.7 Error Handling: Decode Error of the Sink Device

Use Case:	Decode error of the sink device		
Description:	A decode error of the sink device occurs, while the sink receives encoded data.		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:			

Table 4-4: Decode Error of the Sink Device

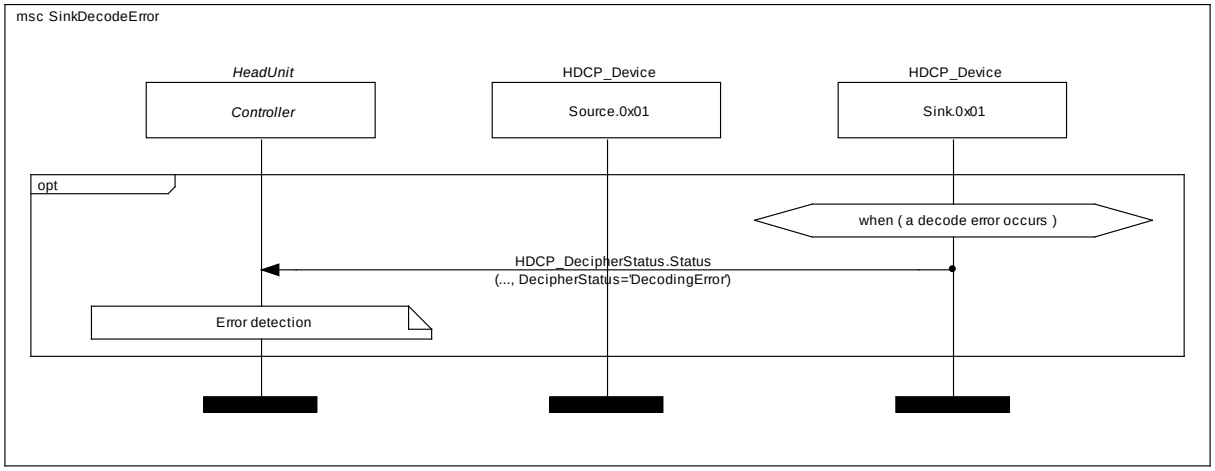

Figure 4-6: Decode Error of the Sink Device

5 Appendix A: List of Figures

6 Appendix B: List of Tables

Notes: