MOST

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

Multimedia and Control Networking Technology

MOST Content Protection Scheme DTCP Implementation Rev 3.0.2 03/2013

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
D-76185 Karlsruhe
Germany

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

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

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
[3]	**MOST Content Security Specification**	1.2
[4]	5C Digital Transmission Content Protection Specification Volume 1	1.7
[5]	DTCP Volume 1 supplement B, mapping DTCP to MOST (M6)	1.2
[6]	**MOST GeneralFBlock FBlock Template Specification**	3.0.4
[7]	DTCP Volume 1 supplement H, mapping DTCP to MOST (AES-128)	1.0

Document History

Changes Specification 3.0.1 to Specification 3.0.2

Change Ref.	Section	Changes
3V0.2_001	4	– Replaced non-Ack Method OPTypes with OPTypes with SenderHandle. – Updated function and parameter names.

Changes Specification 3.0 to Specification 3.0.1

Change Ref.	Section	Changes
3V0.1_001	All	– DTCP according Supp. H (DTCP with AES-128) added.

Changes Specification 2.2-00 to Specification 3.0

Change Ref.	Section	Changes
3V0_001	All	– Changed to 3.0 Draft Template
3V0_002	3.1	– Added figures to explain the transport mechanism – Deleted Figure 3-2
3V0_003	-	– Moved document references from Introduction to Bibliography.
3V0_004	Bibliogr.	– Moved bibliography from section 1.2 to separate chapter. – Added GeneralFBlock Rev. 3.0.0 to referenced documents.
3V0_005	1.2	– Added “Transport Stream” to list of terms.
3V0_006	2	– Removed descriptions of functions that are contained in the GeneralFBlock template. Added reference instead.
3V0_007	3.1	– Changed order of sections to better reflect structure.
3V0_008	3.1.4	– New section on synchronous transport.
3V0_009	3.2	– New section on A/V Packetized MOST-DTCP format.
3V0_010	Appendix A	– Added “Appendix A: DTCP Robustness Measures.”

Changes Specification 1.0-00 to Specification 2.2-00

Version	Date	Section	Comment on changes
– 1.0-00	– 2001-12-10	– -	– First version
– 1.1-06	– 2004-02-09	– All	– Major updates
– 1.1-07	– 2004-04-01	– -	– DRAFT removed
– 1.1-08	– 2004-05-28	– 3 – 5	– Updated Function Catalog – Added Chapter 5: Message Sequence Charts
– 1.1-09	– 2004-06-03	– 3, 5	– Updates from WG meeting
– 1.1-10	– 2005-01-12	– 3	– Updates from WG meeting
– 2.0-00	– 2005-02-28	– All – 3, 5	– New template – Updates from WG meeting
– 2.0-01	– 2005-03-14	– 2 – 5 (now 4)	– Chapter 2 in 2.0-00 deleted, by request of WG-DA – Introduction included, by request of WG-DA

Version	Date	Section	Comment on changes
– 2.0-02	– 2005-03-14	– 4	– Collaboration diagram included, by request of WG-DA
– 2.0-03	– 2005-06-20	– All	– Update from WG Telephone Conference
–	– 2006-06-28	– All	– WG work
–	– 2006-09-12	– All	– TeleCon updates
–	– 2006-10-12	– All	– WG work
– 2.1-06	– 2007-01-25	– 4.7,4.8,4.9	– Update MSC Sequences according changes in DTCP_Status, DTCP_Control
– 2.1-07	– 2007-01-30	– All	– WG work
– 2.2	– 2007-03-12	– All	– Reference to MOST Stream Transmission Specification changed to Revision 1.3. – Updated Enumerations. – Renamed parameter Control to Control_5C. – Renamed parameter Status to Status_5C. – Renamed parameter SourceNr. / SinkNr. To SourceSinkNr.

1 Introduction

1.1 Purpose

Today, two ways exist for implementing DTCP mechanisms into MOST systems. These are:

- 5C DTCP specification Volume 1, Supplement B / Supplement H: Mapping DTCP to MOST
- 5C DTCP specification Volume 1, Supplement E: Mapping DTCP to IP

The details of DTCP can be found at www.dtcp.com.

This document describes the MOST functions and services required to enable Digital Transmission Content Protection (DTCP) protocols according to "**Supplement B**" with M6 cipher and "**Supplement H**" with AES-128 cipher only.
For an implementation according to "Supplement E", please refer to the MOST Cooperation document "MOST_ContentProtectionScheme_DTCP-IP_Implementation".

Note: *Every usage of DCTP requires a license agreement with DTLA (Digital Transmission License Administrator). In particular, the implementation of this DTCP specification on the MOST Network requires full compliance with the DTCP license agreement and its procedural appendix, compliance rules, and policy statements.*

1.2 Terms and Abbreviations

BW	BW relates to allocated block width
DTCP	Digital Transmission Content Protection
Sink	The target of a data transfer
Source	The origin of a data transfer
TS	Transport Stream

2 DTCP Functions

The following functions are contained in the *GeneralFBlock Template Specification [6]*.

FktID	Name
0x120	DTCP_StartProcess
0x121	DTCP_Control
0x122	DTCP_Status
0x123	DTCP_CipherStatus
0x124	DTCP_Info
0x125	DTCP_ContentKeyProcess

3 Protected Content

For implementing the DTCP mechanisms, the data to be protected is encrypted, transmitted and decrypted in packetized form. Embedded information has to be transported as part of the encrypted section.

Exchange key Expiration
The Exchange Keys of source devices expire when the sources stop output of protected content. Sources are considered to have stopped output when there are no synchronous connections or asynchronous data transfers for audiovisual or audio content

Detailed definition of a synchronous connection:
- A logical connection between MOST devices
- Is not bound to specific MOST Source Numbers or MOST Sink Numbers
- Is not bound to specific allocated channels
- Is not affected by low-level unlocks or bus-resets

Packetizing of streaming content
For streaming content, two packetizing schemes are available:

- Generic MOST-DTCP Format.
- A/V Packetized MOST-DTCP Format

Embedded Information
Depending on the stream type and origin, specific “Embedded Information” is carried over a dedicated SAD channel or in an area called “Info”. The “MOST Stream Transmission” document specifies the appropriate parameters and information to be used for the different streams available on MOST.

3.1 Generic MOST-DTCP Format

To pack streaming data in DTCP packets two additional Stream-Associated-Data channels (SADs) are used:

- SAD0 transmits the unprotected header information.
  Unused areas between two headers are reserved and must be transmitted as “0x00”.

- SAD1 is defined to transmit the protected “Embedded Information”.
  Unused areas are reserved and must be transmitted as “0x00”.

Note: *The correlation between the header and the packet is shown in the following figure. The packet starts one frame upon after reception of Header [3].*

The gray areas refer to protected content (PC). The white areas are unprotected headers.

Data Frame	Byte [0] SAD0 - Header	Byte [1] SAD1 - Info	Byte [2]		...	Byte[BW-1]
…	Header [0]	Info [M-3]	Data	Data	Data	Data
…	Header [1]	Info [M-2]	Data	Data	Data	Data
…	Header [2]	Info [M-1]	Data	Data	Data	Data
…	Header [3]	Info [M]	Data	Data	Data	Data [N]
A	reserved	Info [0]	Data [0]	Data [1]	Data [..]	Data [BW-3]
A + 1	reserved	Info [1]	Data [BW-2]	Data [BW-1]	Data	Data
A + 2	reserved	Info [2]	Data	Data	Data	Data
A + 3	reserved	Info [3]	Data	Data	Data	Data
A + 4	reserved	…	Data	Data	Data	Data
A + 5	reserved	…	Data	Data	Data	Data
A + 6	Header [0]	Info [M-3]	Data	Data	Data	Data
…	Header [1]	Info [M-2]	Data	Data	Data	Data
…	Header [2]	Info [M-1]	Data	Data	Data	Data
…	Header [3]	Info [M]	Data	Data	Data	Data [N]
B	reserved	Info [0]	Data [0]	Data [1]	Data[..]	Data [BW-3]
B + 1	reserved	Info [1]	Data [BW-2]	Data [BW-1]	Data	Data
B + 2	reserved	Info [2]	Data	Data	Data	Data
…	reserved	Info [3]	Data	Data	Data	Data

Figure 3-1: Streaming Data with Additional SADs (Frame-by-Frame View)

3.1.1 Definition of Header Bytes

This section describes the definition of the DTCP header bytes used in the previous chapter.

Name	Purpose	MSB							LSB
Header [0]	SyncHi 0x3C	0	0	1	1	1	1	0	0
Header [1]	SyncLo 0xB2	1	0	1	1	0	0	1	0
Header [2]	DTCP information	Defined by “Supplement B” or “Supplement H” DTCP specification							
Header [3]	Extension	Reserved, set to “0x00”							

Table 3-1: Definitions of the Header Bytes

The used sync pattern 0x3CB2 is a 4th order PN-series with a length of 15 bits, padded with a zero bit.

3.1.2 Embedded Information (Info Bytes)

SAD1 delivers the encrypted, flexible-length info field, which is carrying the “Embedded Information”. Info[0] indicates the number of info bytes following. Info [1] indicates the media type. The usage and mapping of “Embedded Information” to Info [2]….Info [M] depends on the type and content of the stream and is specified in the document “MOST Stream Transmission”.

Note: *Generally, unused info bytes are reserved and must be transmitted as “0x00”.*

3.1.3 Generic MOST-DTCP Packet Length

A packet always consists of an unprotected header channel (SAD0), the protected info channel (SAD1) and a variable number of protected data channels (Byte[2..BW-1]).

Note: *The protected channels (SAD1 / Byte[2..BW-1]) may be subdivided into several “Encryption frames”.*

Packet Length = (k * EFS * BW) / (BW-1)
Packet Length = n * BW

k, n : Element of N

EFS: Encryption Frame Size as defined in “Supplement B” / “Supplement H” of the 5C DTCP Specification

Based on the formula above, the “MOST Stream Transmission” [2] document defines for each supported stream the Encryption Frame Size.

3.1.4 Synchronous Applications

The Generic MOST-DTCP Format is transmitted transparently over the bus. Typical application cases include PCM audio data.

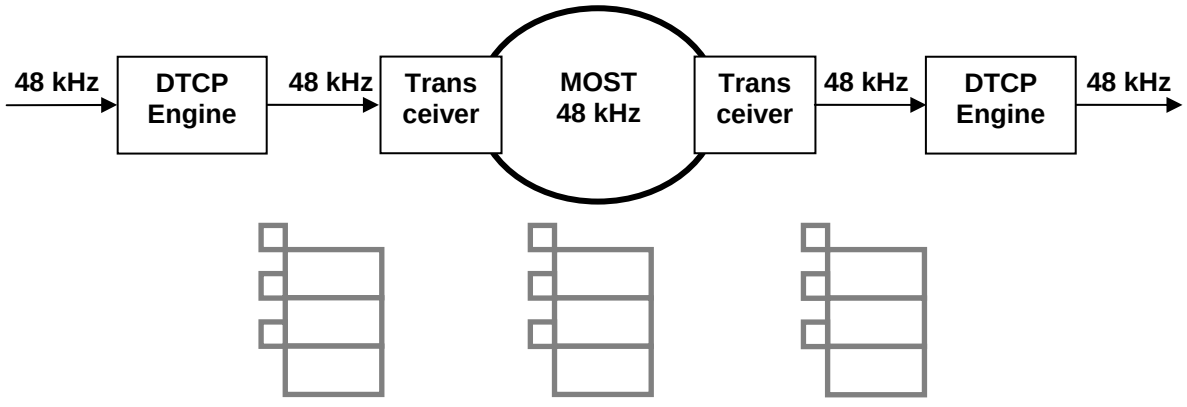


Figure 3-2: Synchronous transport of DTCP encrypted data

3.1.5 DiscreteFrame Applications

The DTCP engine will generate the same Generic MOST-DTCP Format as used for synchronous transmission. In contrast to the synchronous transmission the DiscreteFrame Isochronous Format on MOST is used to transport the data over MOST.

Depending on the used transceiver interface the data may be supplied in frame format (I²S legacy approach) or as packets (MediaLB).

3.1.6 I²S Legacy Approach

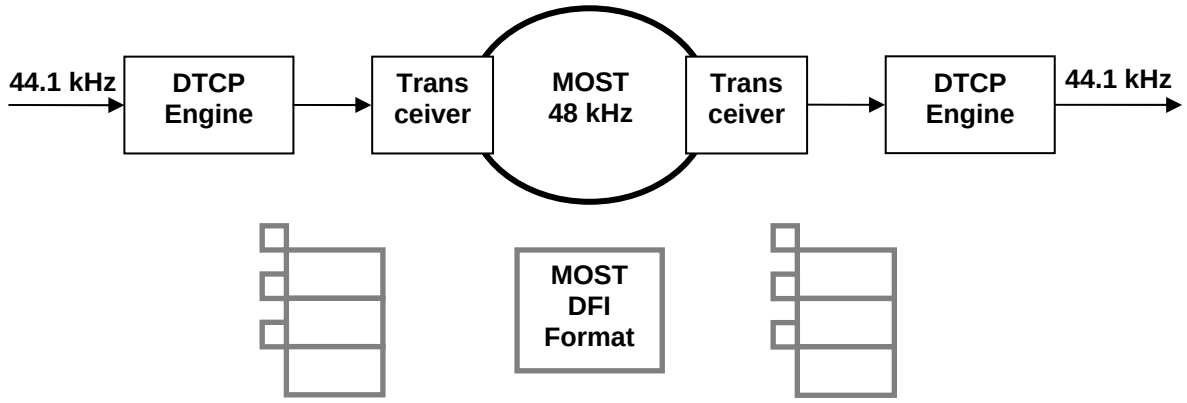


Figure 3-3: DiscreteFrame Isochronous transport of DTCP encrypted data by using I^2S port of transceiver

Content: “Audio of DVD-Audio” (MediaType 0x22)

Resulting MOST BlockWidth: 6 bytes per frame (2 bytes Info & 4 bytes LPCM) with supplement B.

DTCP Encryption Frame Size: 8 bytes
MOST Packet Length: 48 bytes

(Parameters taken from the “MOST Stream Transmission Specification” [2])

Frame	Byte [0]	Byte [1]	Byte [2]	Byte [3]	Byte [4]	Byte [5]
1	0x3C	(0x00)	Data [16]	Data [17]	Data [18]	Data [19]
2	0xB2	(0x00)	Data [20]	Data [21]	Data [22]	Data [23]
3	DTCP	(0x00)	Data [24]	Data [25]	Data [26]	Data [27]
4	0x00	(0x00)	Data [28]	Data [29]	Data [30]	Data [31]
5	(0x00)	0x07	Data [0]	Data [1]	Data [2]	Data [3]
6	(0x00)	0x22	Data [4]	Data [5]	Data [6]	Data [7]
7	(0x00)	CCI	Data [8]	Data [9]	Data [10]	Data [11]
8	(0x00)	ISRC	Data [12]	Data [13]	Data [14]	Data [15]
9	0x3C	ISRC	Data [16]	Data [17]	Data [18]	Data [19]
10	0xB2	(0x00)	Data [20]	Data [21]	Data [22]	Data [23]
11	DTCP	(0x00)	Data [24]	Data [25]	Data [26]	Data [27]
12	0x00	(0x00)	Data [28]	Data [29]	Data [30]	Data [31]
13	(0x00)	0x07	Data [0]	Data [1]	Data [2]	Data [3]
14	(0x00)	0x22	Data [4]	Data [5]	Data [6]	Data [7]
15	(0x00)	CCI	Data [8]	Data [9]	Data [10]	Data [11]
16	(0x00)	ISRC	Data [12]	Data [13]	Data [14]	Data [15]

Figure 3-4: DVD-Audio Stream Protected by MOST-DTCP

3.2 A/V Packetized MOST-DTCP Format

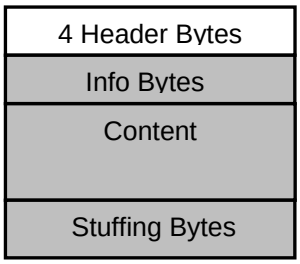


Figure 3-5: A/V Packetized MOST-DTCP Format

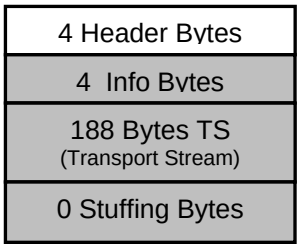


Figure 3-6: Transport Stream Example A/V Packetized MOST-DTCP Format

3.2.1 Definition of Header Bytes

This section describes the definition of the DTCP header bytes used in the previous chapter.

Name	Purpose	MSB							LSB
Header [0]	SyncHi 0x3C	0	0	1	1	1	1	0	0
Header [1]	SyncLo 0xB2	1	0	1	1	0	0	1	0
Header [2]	DTCP information	Defined by “Supplement B” / “Supplement H” of DTCP specification							
Header [3]	Extension	Reserved, set to “0x00”							

Table 3-2: Definitions of the Header Bytes

The used sync pattern 0x3CB2 is a 4th order PN-series with a length of 15 bits, padded with a zero bit.

3.2.2 Embedded Information (Info Bytes)

Info[0] indicates the number of info bytes following. Info [1] indicates the media type. The usage and mapping of “Embedded Information” depends on the type and content of the stream and is specified in the document “MOST Stream Transmission”.

Note: *Generally, unused Info Bytes are reserved and must be transmitted as “0x00”.*

3.2.3 Stuffing Bytes

The Stuffing Bytes are used to extend the size of the content to the next block boundary of the used cipher. For MOST-DTCP the EFS must be a multiple of 8 bytes with supplement B, and a multiple of 16 bytes with supplement H. A specific value for the Stuffing Bytes is not defined.

3.2.4 A/V Packetized MOST-DTCP Packet Length

EFS = Info + Content + Stuffing

Packet Length = EFS + 4 Header Bytes

EFS: Encryption Frame Size as defined in MOST Specification for Stream Transmission [2].

Based on the formula above, the “MOST Stream Transmission” document defines for each supported stream the Encryption Frame Size.

3.2.5 Example

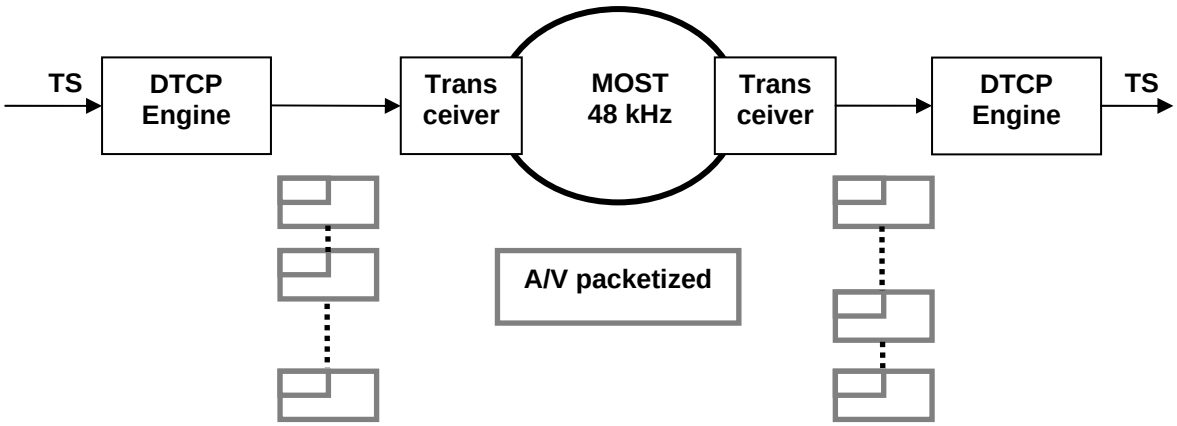


Figure 3-7: Transport of A/V Packetized MOST-DTCP encrypted data

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 DTCP connection establishment (Authentication followed by a Content Key Exchange) is figured out.

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

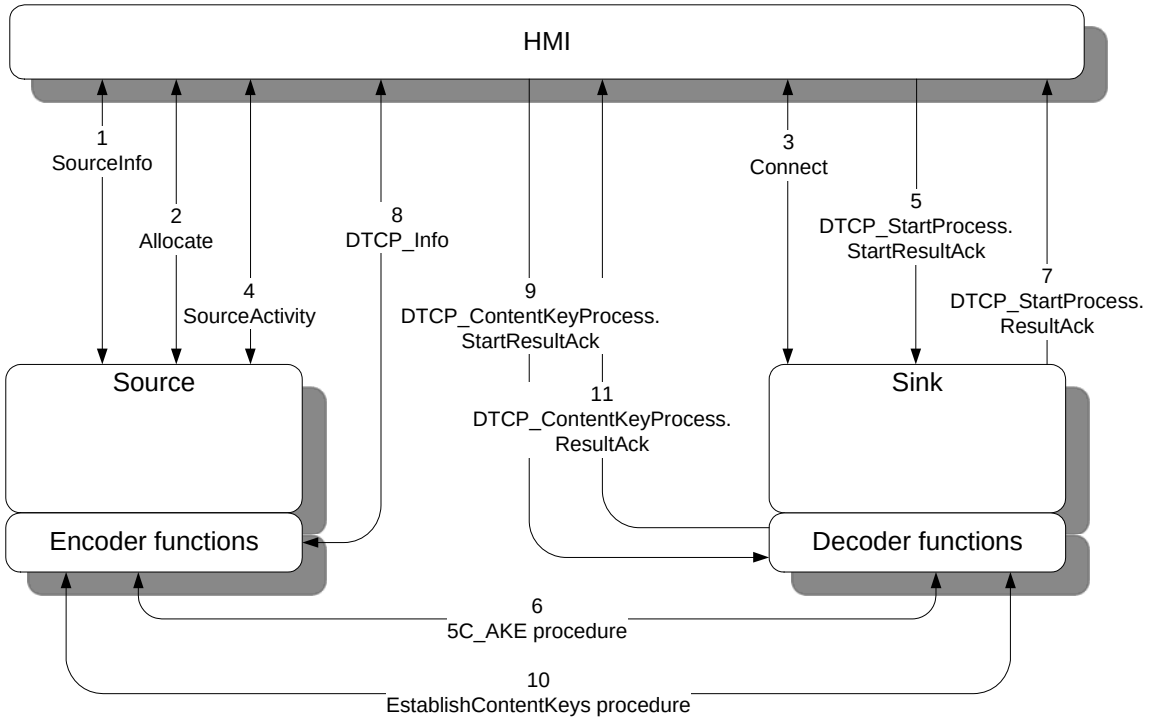


Figure 4-1: Collaboration Diagram 1: DTCP Connection Establishment (Authentication Followed by a Content Key Exchange)

Note: In MOST, during the Establish Content Keys procedure, the DTCP parameter "isochronous_channel_number" of the "Content_Key_Req" AKE subfunction is filled with the MOST parameter SourceNr, which has values in the range of 1...63.

4.2 Speculative Authentication

Use Case:	Speculative DTCP Authentication		
Description:	The Speculative DTCP Authentication takes place during the start of the MOST Network		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:	Speculative DTCP Authentication is only an optional element at this time.		

Table 4-1: MSC 1 Speculative Authentication

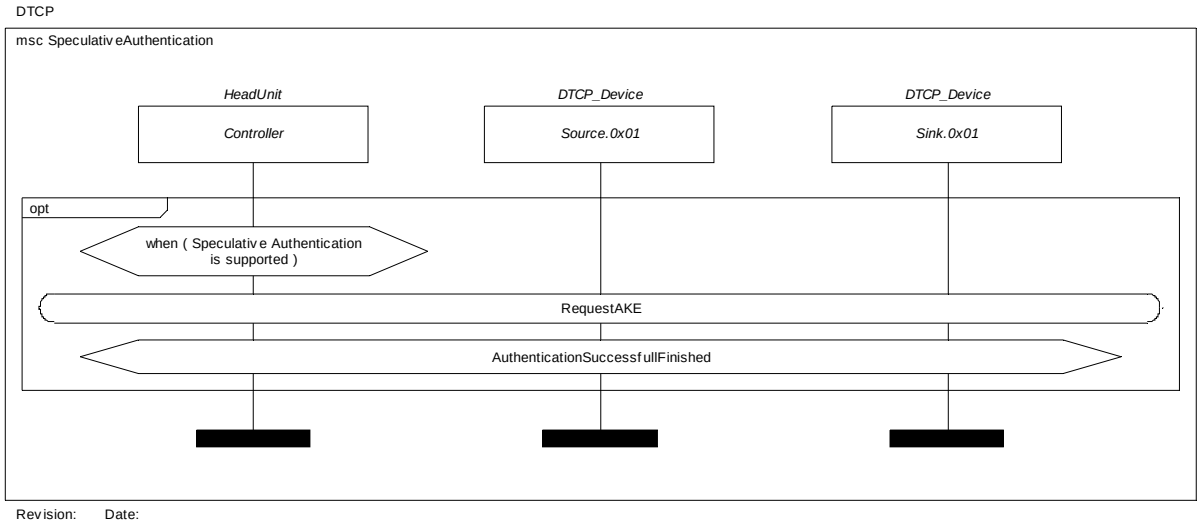


Figure 4-2: MSC 1 Speculative Authentication

4.3 The User Requests a DTCP Audio Connection

Use Case:	The passenger requests a DTCP audio connection		
Description:	The passenger initiates the establishment of a DTCP audio connection. If necessary, the DTCP Authentication Process is executed, before the Content Keys are calculated.		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
	X		
Remarks:			

Table 4-2: MSC 2 The User Requests a DTCP Audio Connection

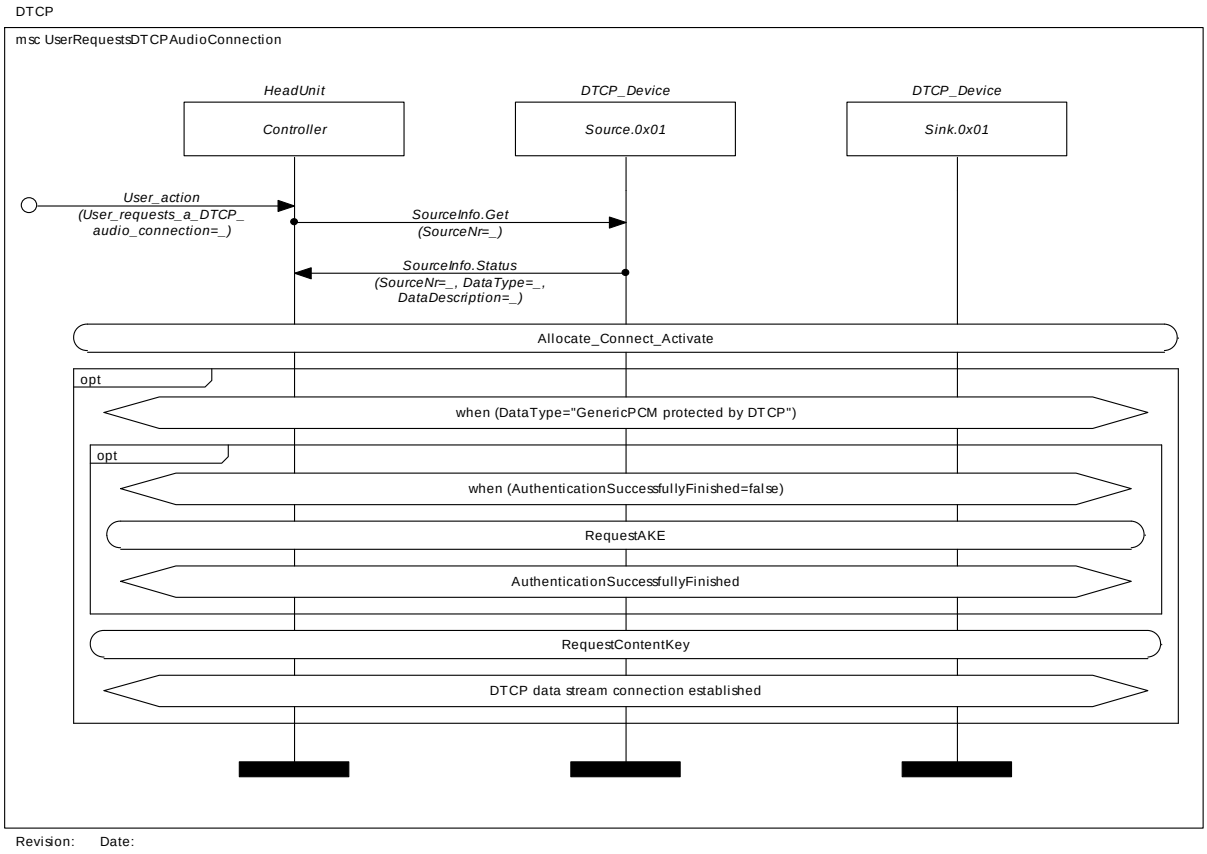


Figure 4-3: MSC 2 The User Requests a DTCP Audio Connection

4.4 Request Exchange Key Calculation

Use Case:	Request for calculating the Exchange Keys		
Description:	The HeadUnit starts the DTCP 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 4-3: MSC 3 Request Exchange Key Calculation

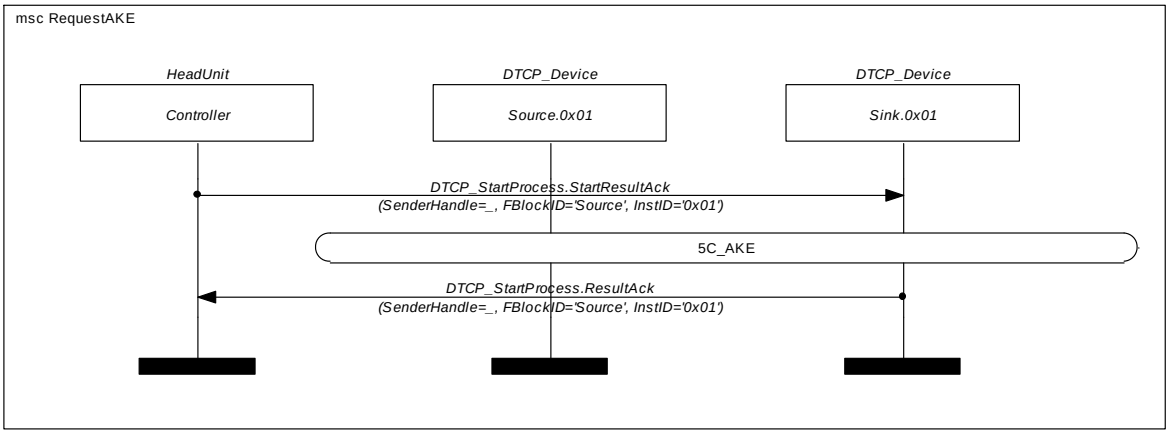


Figure 4-4: MSC 3 Request Exchange Key Calculation

4.5 Request Content Key Calculation

Use Case:	Request for calculating the Content Keys		
Description:	The HeadUnit initiates the calculation of the Content Keys. To do so, it delivers audio stream relevant information of the source device to the sink.		
Prior Condition:	The requested audio connection is to be protected in accordance to the DTCP specification		
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:	The establishing of Content Keys is done on “SourceNr”-level		

Table 4-4: MSC 4 Request for Calculating the Content Keys

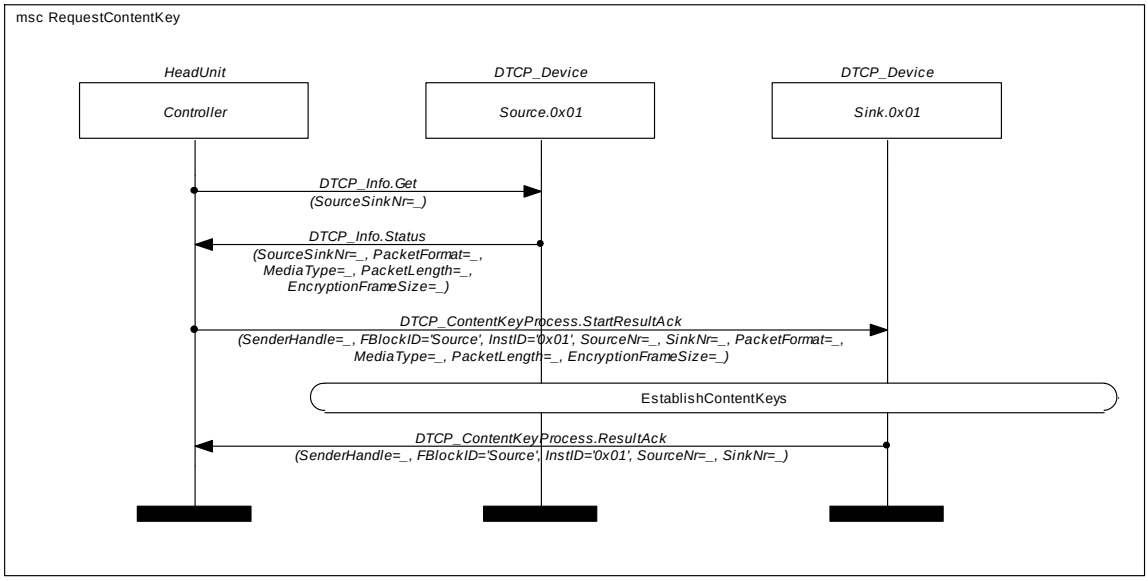


Figure 4-5: MSC 4 Request for Calculating the Content Keys

4.6 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 4-5: MSC 5 Allocate, Connect and Activate

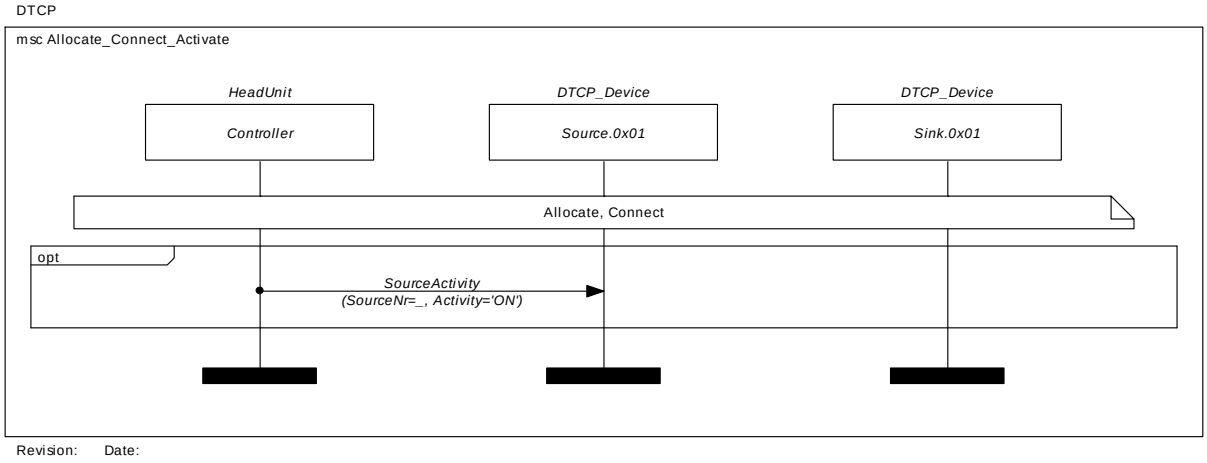


Figure 4-6: MSC 5 Allocate, Connect and Activate

4.7 Calculate Exchange Key (Example)

Use Case:	Calculate the Exchange Keys		
Description:	Calculate the Exchange Keys in accordance to the DTCP Specification Vol.1 (Informational Version)		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:	In this example, all three Exchange Keys are calculated		

Table 4-6: MSC 6 Calculate the Exchange Key

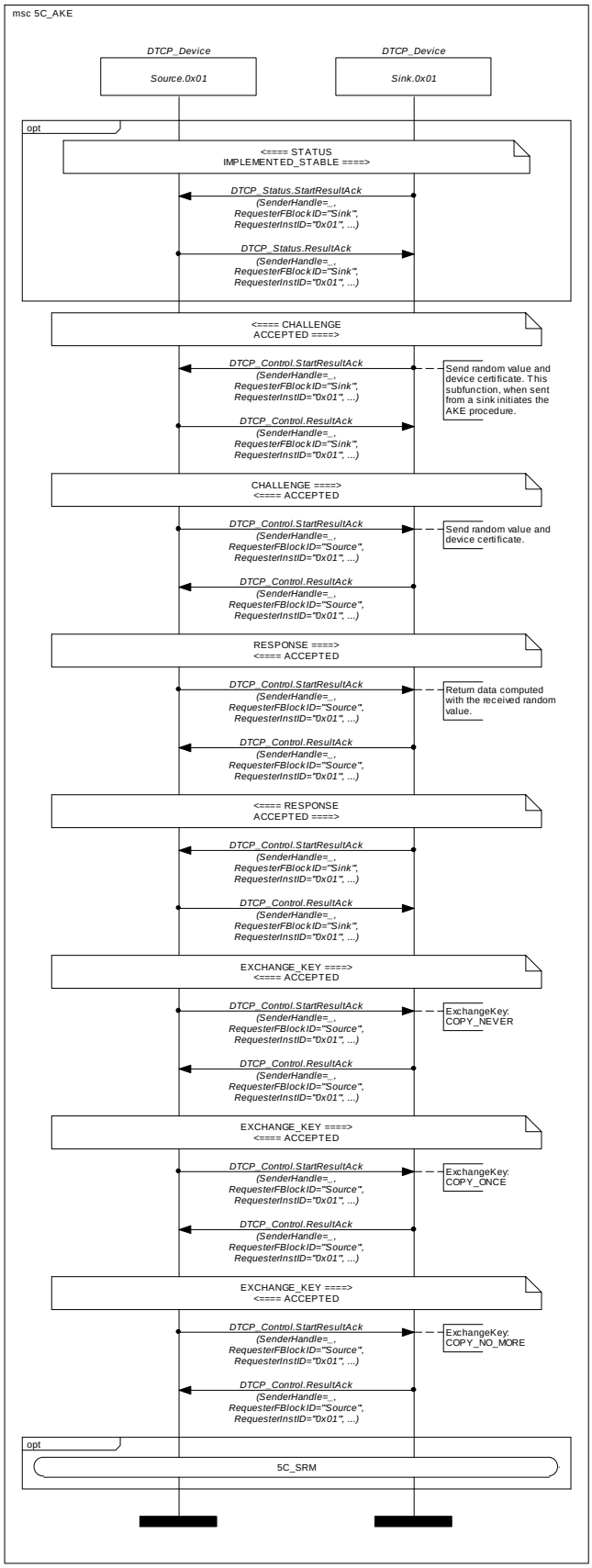


Figure 4-7: MSC 6 Calculate the Exchange Key

4.8 Establish Content Keys

Use Case:	Establish the Content Keys		
Description:	Establish the Content Keys in accordance to the DTCP Specification Vol.1 (Informational Version)		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:			

Table 4-7: MSC 7 Establish the Content Keys

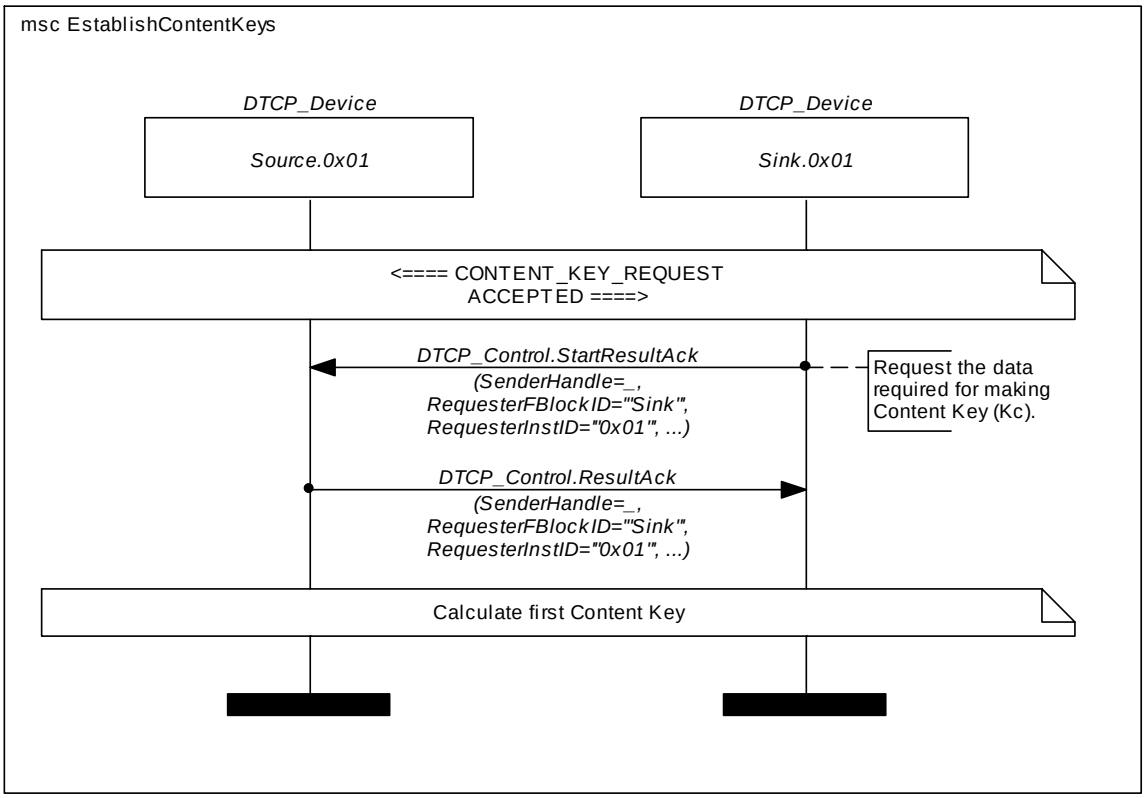


Figure 4-8: MSC 7 Establish the Content Keys

4.9 SRM

Use Case:	SRM update		
Description:	SRM update in accordance to the DTCP Specification Vol.1 (Informational Version)		
Prior Condition:			
Initiator:	Passenger	Internal	Comment
		X	
Remarks:			

Table 4-8: MSC 8 5C_SRM

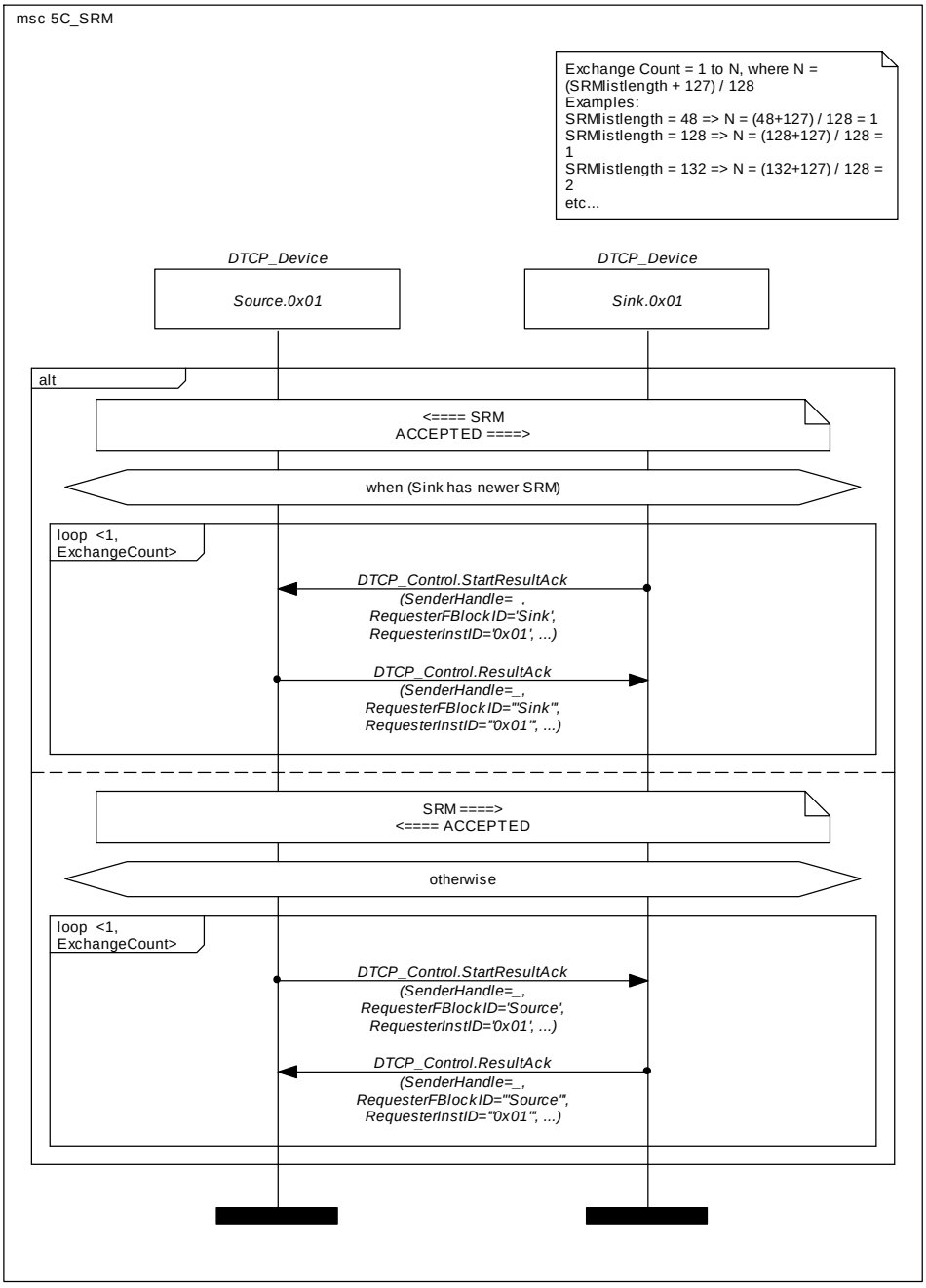


Figure 4-9: MSC 8 5C_SRM

4.10 Error Handling: Software Error of the Source Device

Use Case:	Software error of the source device		
Description:	A software error of the source device occurs.		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:			

Table 4-9: MSC 9 Software Error of the Source Device

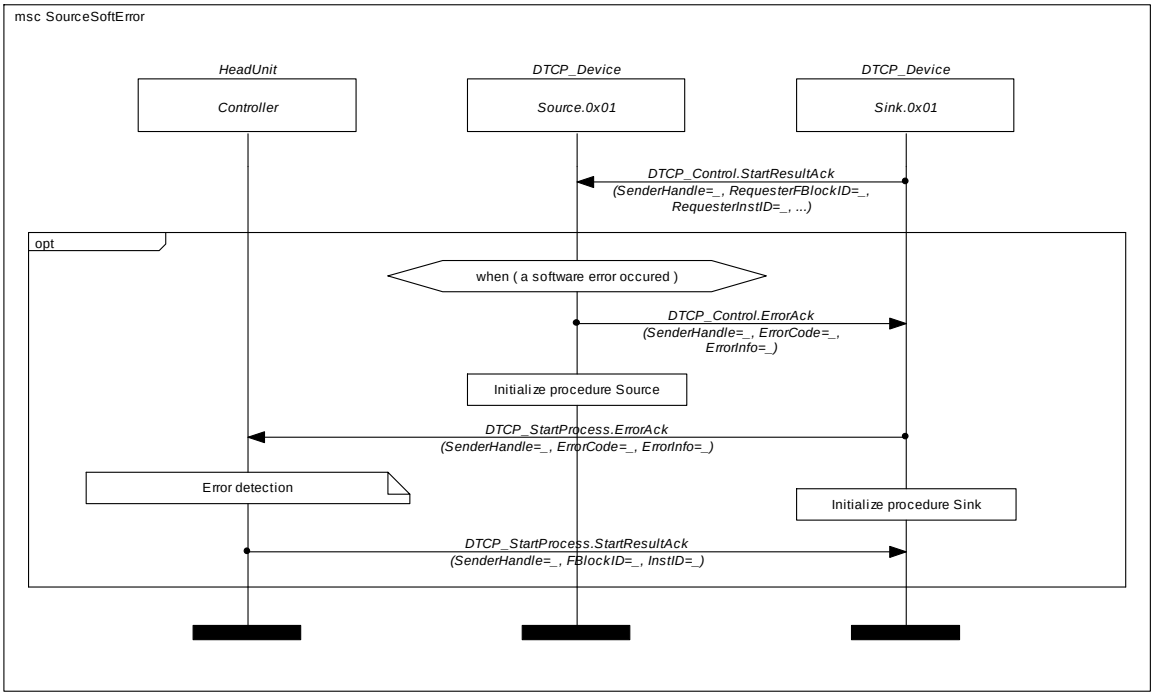


Figure 4-10: MSC 9 Software Error of the Source Device

4.11 Error Handling: Software Error of the Sink Device

Use Case:	Software error of the sink device		
Description:	A software error of the sink device occurs.		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:			

Table 4-10: MSC 10 Software Error of the Sink Device

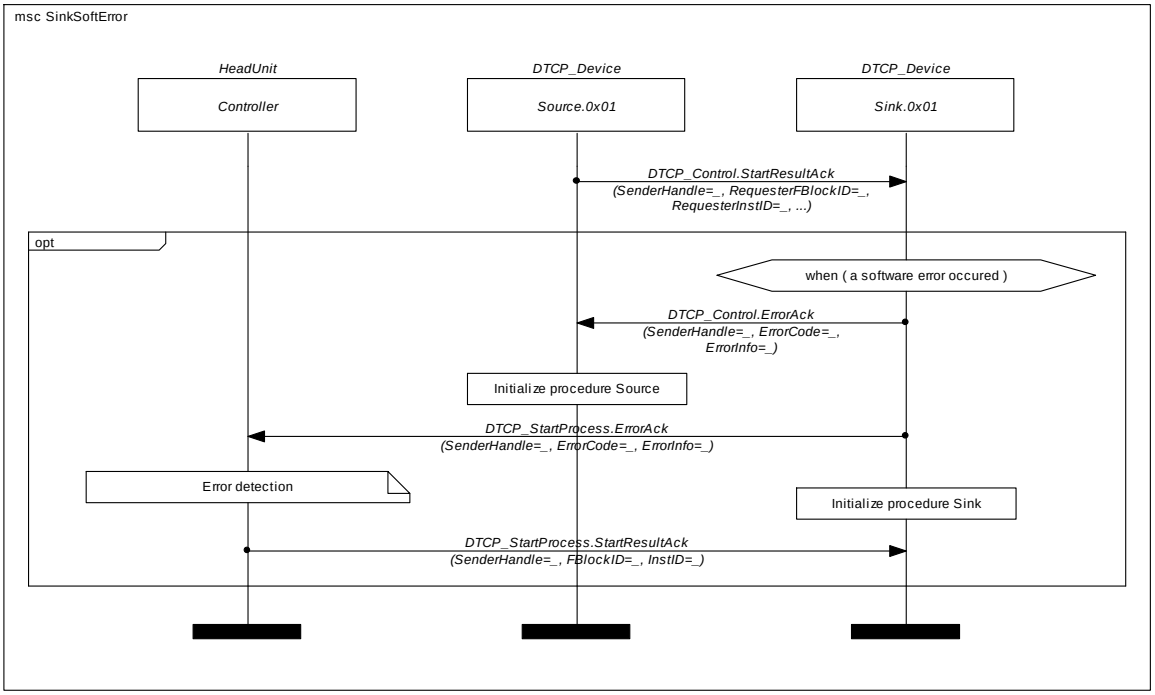


Figure 4-11: MSC 10 Software Error of the Sink Device

4.12 Error Handling: Hardware Error of the Source Device

Use Case:	Hardware error of the source device		
Description:	A hardware error of the source device occurs.		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:			

Table 4-11: MSC 11 Hardware Error of the Source Device

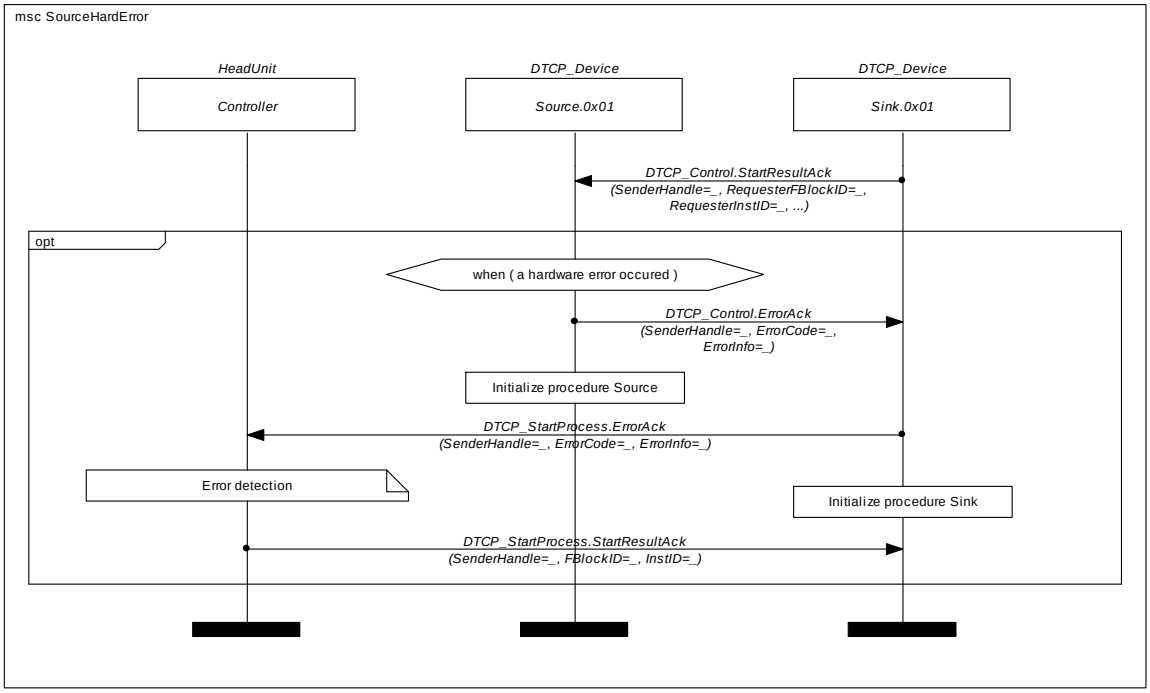


Figure 4-12: MSC 11 Hardware Error of the Source Device

4.13 Error Handling: Hardware Error of the Sink Device

Use Case:	Hardware error of the sink device		
Description:	A hardware error of the sink device occurs.		
Prior Condition:			
Initiator:	**Passenger**	**Internal**	**Comment**
		X	
Remarks:			

Table 4-12: MSC 12 Hardware Error of the Sink Device

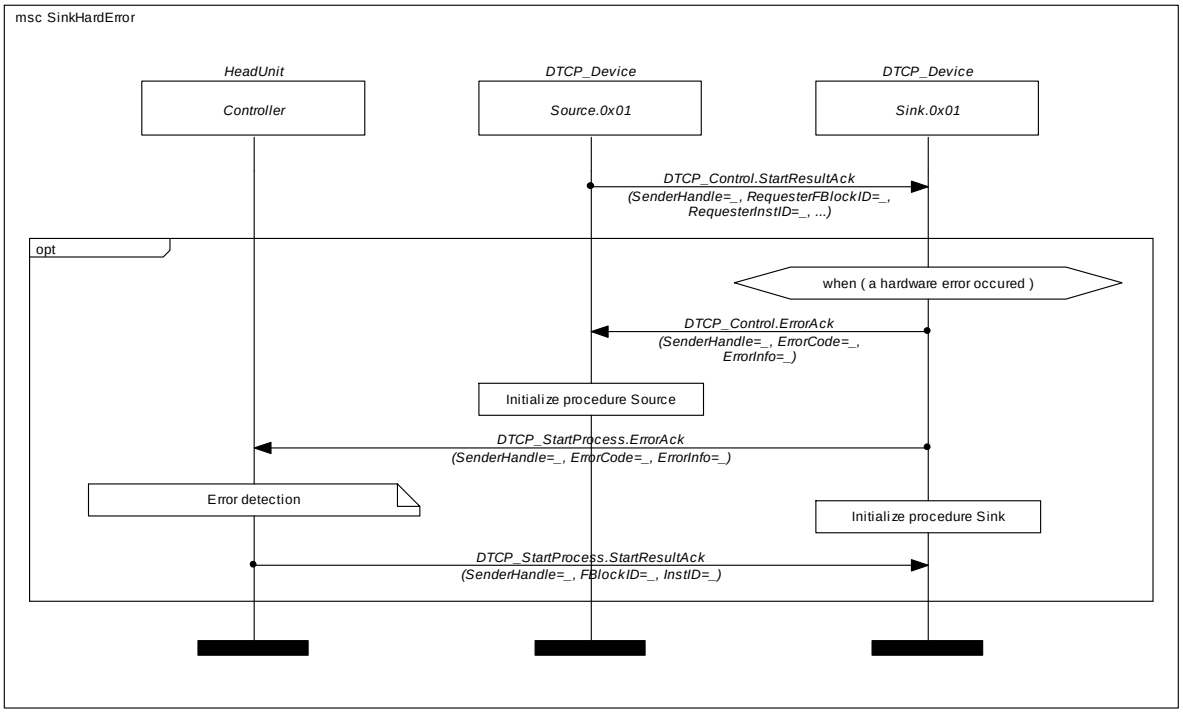


Figure 4-13: MSC 12 Hardware Error of the Sink Device

4.14 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 decoded data.		
Prior Condition:			
Initiator:	Passenger	Internal	Comment
		X	
Remarks:			

Table 4-13: MSC 13 Decode Error of the Sink Device

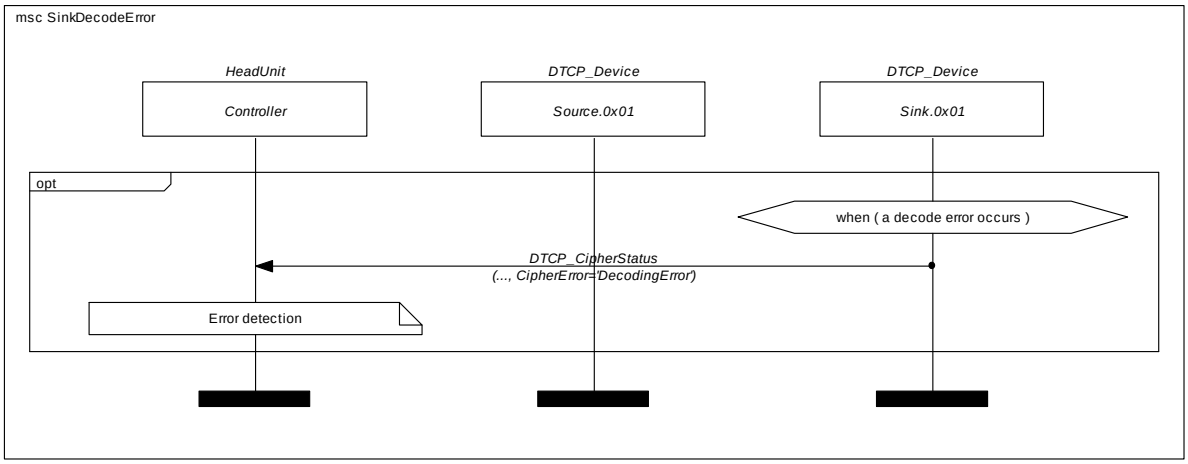


Figure 4-14: MSC 13 Decode Error of the Sink Device

5 Appendix A: Generic MOST-DTCP Format Robustness Measures

This appendix describes the measures used to increase DTCP stream transmission robustness in a disturbed environment regarding Generic MOST-DTCP Format.

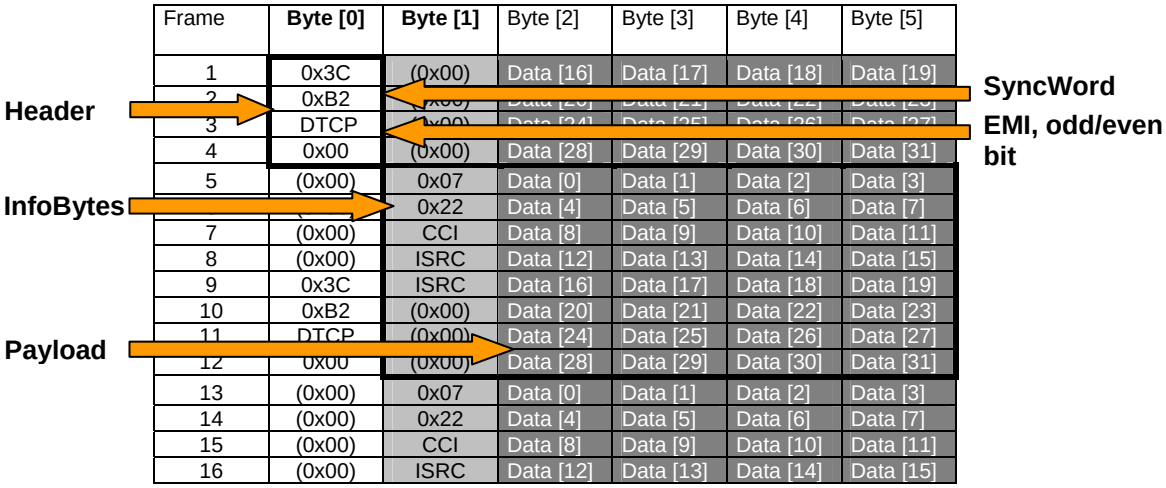
5.1 Description

Problems with DTCP stream transmission can arise from

- Errors in the DTCP packet structure
- Errors in the DTCP packet header
- Errors in the DTCP packet InfoBytes
- Errors in the DTCP packet payload

This appendix offers ways to remedy the effects of those errors. In particular, the DTCP Robustness measures aims at reducing or entirely eliminating fatal odd/even errors and helps to detect simple bit errors in the data area.

In the diagram below, the arrows indicate which areas are covered by the measures detailed here.



Frame	**Byte [0]**	**Byte [1]**	Byte [2]	Byte [3]	Byte [4]	Byte [5]
1	0x3C	(0x00)	Data [16]	Data [17]	Data [18]	Data [19]
2	0xB2					
3	DTCP					
4	0x00	(0x00)	Data [28]	Data [29]	Data [30]	Data [31]
5	(0x00)	0x07	Data [0]	Data [1]	Data [2]	Data [3]
6		0x22	Data [4]	Data [5]	Data [6]	Data [7]
7	(0x00)	CCI	Data [8]	Data [9]	Data [10]	Data [11]
8	(0x00)	ISRC	Data [12]	Data [13]	Data [14]	Data [15]
9	0x3C	ISRC	Data [16]	Data [17]	Data [18]	Data [19]
10	0xB2	(0x00)	Data [20]	Data [21]	Data [22]	Data [23]
11	DTCP	(0x00)	Data [24]	Data [25]	Data [26]	Data [27]
12	0x00	(0x00)	Data [28]	Data [29]	Data [30]	Data [31]
13	(0x00)	0x07	Data [0]	Data [1]	Data [2]	Data [3]
14	(0x00)	0x22	Data [4]	Data [5]	Data [6]	Data [7]
15	(0x00)	CCI	Data [8]	Data [9]	Data [10]	Data [11]
16	(0x00)	ISRC	Data [12]	Data [13]	Data [14]	Data [15]

Figure 5-1: Robustness measures in DVD-Audio Stream Protected by MOST-DTCP

5.2 Measures

The diagram on page 33 presents the details of the preventive measures and the reaction on certain DTCP errors. The diagram gives evidence of the different error causes. It is not intended to describe error detection.

Packet structure errors
Packet structure errors usually manifest themselves as SyncWord corruption. Bit errors within the non encrypted area occur and no DTCP Block will be recognized.
The measure taken is to mute the data output.

Packet header errors - odd/even bit change
When packet header errors occur, the decipher engine may use the wrong (next) content key, which will, for example, lead to disturbed audio.
The measure taken is to not change the content key if the odd/even bit change time is shorter than 30 seconds.

Note: *Before every content key increment, the current content key is stored.*

Packet header errors - EMI errors
When Encryption Mode Indicator (EMI) errors occur, the decipher engine might be using the wrong content key.
The solution is to mute the data output.

Note: *If the EMI is corrupted, the associated frame will be damaged; however, the following frames will be valid again.*

Packet InfoBytes errors
This group of errors is characterized by inconsistent InfoBytes after decryption where the InfoBytes remain defective for several DTCP packets.
The measure taken is to mute the data output and retrieve the current *nonce* from the DTCP source. This is done through the use of DTCP_Control.StartResult (see the EstablishContentKeys MSC in the DTCP Content Protection Scheme Specification.)
If the InfoBytes still remain defective, a new AKE is triggered.

Packet payload errors
The severity of content corruption differs depending on the type of content. For example, in streaming PCM data, bit errors that occur at low rates are often hardly audible. On the other hand, when streaming compressed data, a bit error might lead to the corruption of the complete packet.
The solution is to mute the output if the data decoder recognizes errors in compressed data. Optionally, a detected error in an audio sample can be corrected by interpolation instead of muting.

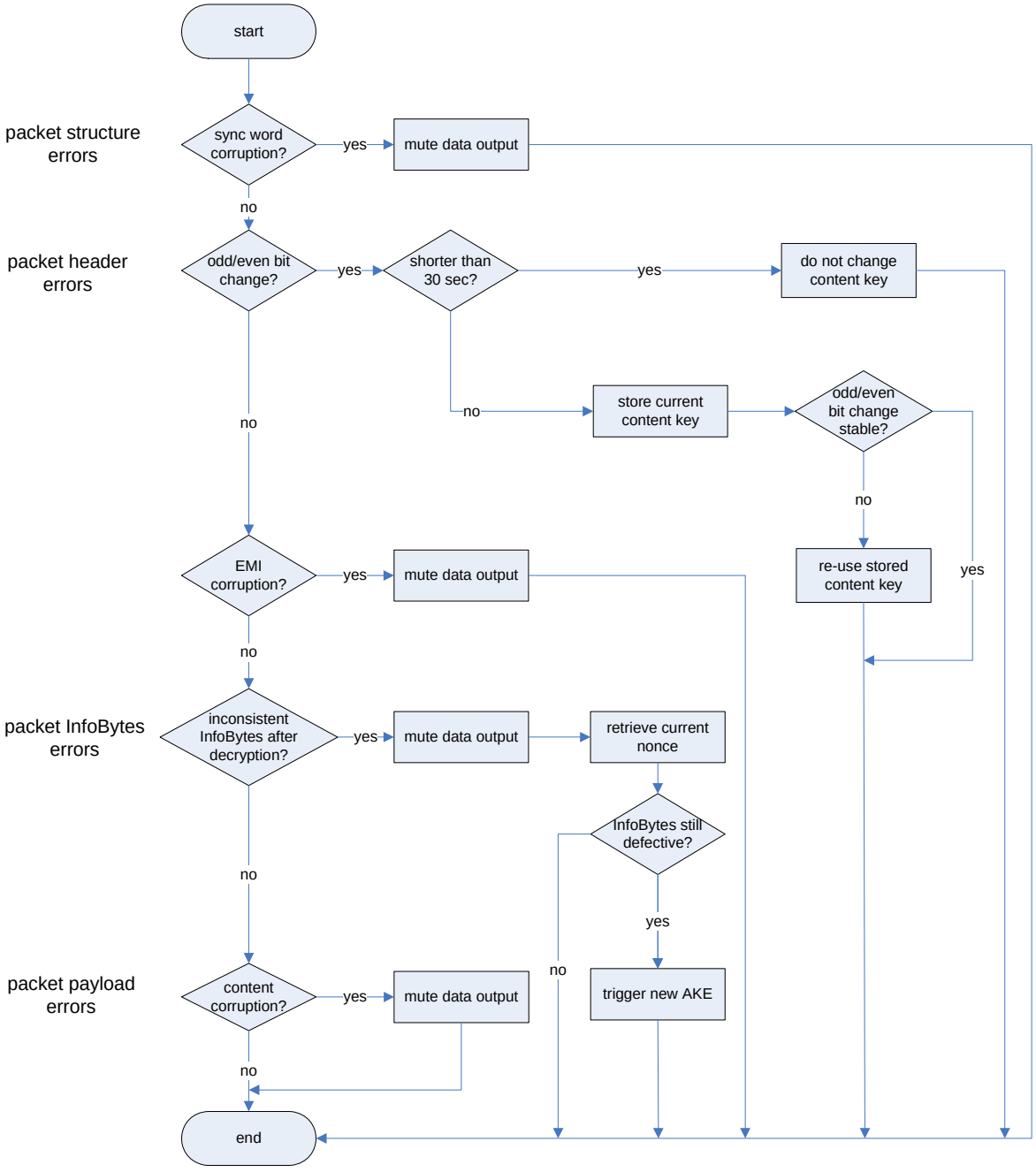


Figure 5-2: DTCP robustness flowchart

6 Appendix B: List of Figures

7 Appendix C: List of Tables

