DTCP Volume 1 Supplement H
Mapping DTCP to MOST AES-128
(Informational Version)

Hitachi, Ltd.
Intel Corporation
Panasonic Corporation
Sony Corporation
Toshiba Corporation

Revision 1.0
March 8, 2012
Preface

Legal 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 provided by
Hitachi, Intel, PANASONIC, Sony, Toshiba (collectively, the “5C”) and/or DTLA. The 5C and DTLA disclaim
all liability, including liability for infringement of any proprietary rights, relating to use of information in
this Specification. No license, express or implied, by estoppel or otherwise, to any intellectual property
rights is granted herein.

Some portions of this document, identified as "Draft" are in an intermediate draft form and are subject to
change without notice. Adopters and other users of this Specification are cautioned that these portions are
preliminary, and that products based on it may not be interoperable with the final version or subsequent
versions thereof.

Copyright © 1997 - 2012 by Hitachi, Ltd., Intel Corporation, Panasonic Corporation, Sony Corporation,
and Toshiba Corporation (collectively, the “5C”). Third-party brands and names are the property of their
respective owners.

Intellectual Property

Implementation of this specification requires a license from the Digital Transmission Licensing
Administrator.

Contact Information

Feedback on this Specification should be addressed to dtla-comment@dtcp.com.

The Digital Transmission Licensing Administrator can be contacted at dtla-manager@dtcp.com.

Table of Contents

V1SH 1 INTRODUCTION ................................................................................................................................................. 4
V1SH 1.1 RELATED DOCUMENTS ................................................................................................................................. 4
V1SH 1.2 TERMS AND ABBREVIATIONS .......................................................................................................................... 4

V1SH 2 MODIFICATIONS TO CHAPTER 6 (CONTENT CHANNEL MANAGEMENT AND PROTECTION) ........................................... 4
V1SH 2.1 EXCHANGE KEY EXPIRATION .............................................................................................................................. 4
V1SH 2.2 Nc UPDATE PROCESS .............................................................................................................................................. 4
V1SH 2.3 PROTECTED CONTENT HEADER .......................................................................................................................... 4
V1SH 2.4 EMBEDDED CCI ....................................................................................................................................................... 5
   V1SH 2.4.1 DTCP_Descriptor MPEG-PS ........................................................................................................................... 5
V1SH 2.5 CONTENT ENCRYPTION FORMATS .................................................................................................................... 5
V1SH 2.6 MODIFICATIONS TO 6.6.1 BASELINE CIPHER ..................................................................................................... 5
V1SH 2.7 MODIFICATIONS TO 6.6.2.1 AES-128 CIPHER ..................................................................................................... 5

V1SH 3 MODIFICATIONS TO CHAPTER 8 (AV/C DIGITAL INTERFACE COMMAND SET EXTENSIONS) .......................................................... 6
V1SH 3.1 CONTROL PACKET FORMAT .............................................................................................................................. 6
V1SH 3.2 STATUS PACKET FORMAT .................................................................................................................................. 7

V1SH 4 MOST DTCP PROTOCOLS ........................................................................................................................................... 7

V1SH 5 MODIFICATIONS TO 4.2.3.2 EXTENDED FORMAT FIELDS (OPTIONAL COMPONENTS OF THE DEVICE CERTIFICATE) .......... 7

Figures

Figure 1 MOST Protected Content Packet ................................................................................................................................. 4
Figure 2 MOST DTCP Control Packet Format ........................................................................................................................... 6
Figure 3 MOST DTCP Status Packet Format ............................................................................................................................. 7
V1SH 1 Introduction
This supplement maps DTCP onto the Media Oriented Systems Transport (MOST). All aspects of IEEE 1394 DTCP functionally are preserved except those described in Appendix D of Volume 1 which does not apply to this mapping and this supplement only details MOST DTCP specific changes or additions.

V1SH 1.1 Related Documents
This specification shall be used in conjunction with the following publications. When the publications are superseded by an approved revision, the revision shall apply.

- Digital Transmission Content Protection Specification Volume 1 and Volume 2
- MOST Content Security Specification
- MOST Content Protection Scheme – DTCP Implementation
- MOST Specification (Media Oriented Systems Transport Specification)

V1SH 1.2 Terms and Abbreviations
MOST Media Oriented Systems Transport

V1SH 2 Modifications to Chapter 6 (Content Channel Management and Protection)

V1SH 2.1 Exchange Key Expiration
Source devices expire their Exchange Keys when they stop output of protected content\(^1\).

V1SH 2.2 \(N_C\) Update Process
MOST provides Synchronous and Asynchronous data transfer services. For Synchronous data transfer, there is no change to the description in Section 6.3.2 of update procedure and timing for \(N_C\).

For Asynchronous data transfer, the \(N_C\) shall be updated after transmitting no greater than 4 Mbytes.

V1SH 2.3 Protected Content Header
Protected content transferred over MOST has a four byte header. This header is used to carry the bits described in Sections 6.3.3 “Odd/Even Bit” and 6.4.2 “Encryption Mode Indicator (EMI)”.

The Reserved bits are reserved for future definition and are currently defined to have a value of zero.

The Sync Bytes (Sync-High and Sync-Low) are defined in “MOST Content Protection Scheme – DTCP Implementation”.

<table>
<thead>
<tr>
<th>msb</th>
<th>Sync-High</th>
<th></th>
<th>lsb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header [0]</td>
<td>Sync-High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Header [1]</td>
<td>Sync-Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Header [2]</td>
<td>reserved (zero)</td>
<td>EMI</td>
<td>Odd/Even</td>
</tr>
<tr>
<td>Header [3]</td>
<td>reserved (zero)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC[0]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC[N]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

![Figure 1 MOST Protected Content Packet](image)

\(^1\) Sources are considered to have stopped output when there are no Synchronous connections or Asynchronous data transfers for audiovisual or audio content.
**V1SH 2.4 Embedded CCI**
The Embedded CCI (Section 6.4.1 or Section 6.4.5.1) is carried as part of the content stream. The Embedded CCI transmission format for MOST bus is defined in “MOST Content Protection Scheme – DTCP Implementation”.

**V1SH 2.4.1 DTCP_Descriptor MPEG-PS**
The DTCP_descriptor delivers Embedded CCI over the DTCP system when an MPEG-Program Stream (MPEG-PS) is transmitted. The DTCP_descriptor described in Appendix.B is used for DTCP_descriptor for MPEG-PS.

**V1SH 2.5 Content Encryption Formats**
Protected content sent over MOST is encapsulated in the Protected Content Packet (See Figure 1).

For AES-128, the encryption frame size of all forms of content shall be in the inclusive range 16 to 4096 bytes and be a multiple of 4 bytes in length.

The encryption frame size is defined in “MOST Content Protection Scheme – DTCP Implementation”

**V1SH 2.6 Modifications to 6.6.1 Baseline Cipher**
The baseline cipher is AES-128 using the Cipher Block Chaining (CBC). AES-128 is described in FIPS 197 dated November 26, 2001 and the CBC mode is described in NIST SP 800-38A 2001 Edition.

**V1SH 2.7 Modifications to 6.6.2.1 AES-128 Cipher**
For AES-128, Cipher Block Chaining (CBC) is used. AES-128 is described in FIPS 197 dated November 26, 2001 and the CBC mode is described in NIST SP800-38A 2001 Edition.
**V1SH 3 Modifications to Chapter 8 (AV/C Digital Interface Command Set Extensions)**

**V1SH 3.1 Control Packet Format**
This section maps the AKE control command specified in Section 8.3.1 to the MOST DTCP Control Packet Format. The AKE control command sub fields used with MOST have the same values and functions as detailed in Chapter 8.

<table>
<thead>
<tr>
<th>Msb</th>
<th>lsb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Byte [0] reserved (zero)</td>
<td>ctype/response</td>
</tr>
<tr>
<td>Byte [1] category = 0000₂ (AKE)</td>
<td>AKE_ID</td>
</tr>
<tr>
<td>Byte [2]</td>
<td>AKE_ID dependent field</td>
</tr>
<tr>
<td>Byte [3]</td>
<td></td>
</tr>
<tr>
<td>Byte [4]</td>
<td></td>
</tr>
<tr>
<td>Byte [5]</td>
<td>number (option)</td>
</tr>
<tr>
<td>Byte [6]</td>
<td>blocks_remaining</td>
</tr>
<tr>
<td>Byte [7]</td>
<td>data</td>
</tr>
<tr>
<td>Byte [7+m]</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 2 MOST DTCP Control Packet Format*

c-type/response has the same values as referenced in chapter 8 of DTCP specification and specified by the AV/C Digital Interface Command Set.

The Reserved bits are reserved for future definition and are currently defined to have a value of zero.


MOST DTCP fragmentation rule is defined as follows: The data fields of MOST DTCP Control Packets are limited to a maximum length of 128 bytes. When a given AKE Info is larger than 128 bytes, the *blocks_remaining* field is used to fragment it. When this fragmentation is required, the AKE Info is divided into N blocks that are sent sequentially via the data fields. The size of the data field in the first N-1 fragments shall be 128 bytes.

The *blocks_remaining* field is identical to the data field specified in section 8.3.1 except for the fragmentation rule.

The data field is identical to the data field specified in section 8.3.1 except for the fragmentation rule.

The unique tag supported by exchanging values via the AKE_label field and described in section 8.3.1 is not used because the unique tag supported by exchanging value via a pair of FBlockID and InstID on MOST is equivalent to AKE_Label.

The data length supported by exchanging values via the data_length field is not used because the data length of MOST DTCP Control Packet is exchanged via a Length field defined in “MOST specification”.

2012-03-08 (Informational Version) Page 6 of 7
V1SH 3.2 Status Packet Format
This section maps the AKE status command specified in Section 8.3.2 to the MOST DTCP Status Packet Format. The AKE status command sub fields used with MOST have the same values and functions as detailed in Chapter 8.

| Byte [0] | reserved (zero) | ctype/response |
| Byte [1] | category = 0000₂ (AKE) | AKE_ID = 0000₂ |
| Byte [2] | | AKE_ID dependent field |
| Byte [3] | | |
| Byte [4] | | |
| Byte [5] | | |
| Byte [6] | \(F_{16}\) | status |

Figure 3 MOST DTCP Status Packet Format

cType/response has the same values as referenced in chapter 8 of DTCP specification and specified by the AV/C Digital Interface Command Set.

The Reserved bits are reserved for future definition and are currently defined to have a value of zero.

Byte[1]..Byte[5] are identical to Operand[0]..Operand[4] as specified in Section 8.3.2.


The fixed value of Operand[5] as specified in Section 8.3.2 is not used.

The maximum data field query supported by exchanging values via the data_length field and described in the last paragraph of section 8.3.2 is not used because the device supporting MOST DTCP can accept the maximum size of MOST DTCP Control Packet.

V1SH 4 MOST DTCP Protocols
This section describes the exchange of DTCP AKE commands, responses, and status frames by MOST DTCP Function.

It is important to review the following references in order to understand MOST Security protocols.

MOST Content Security Specification
MOST Content Protection Scheme (CPS) - DTCP Implementation
Chapters 2 and Section 3.1, 3.4 and 3.7 of the MOST Specification Rev2.0

The MOST DTCP Implementation has similar device states as described in the DTCP Volume1 specification.

The HMI manages the synchronous connection via MOST. Authentication may take place after synchronous connection is established, or upon demand as needed.

The Function Block supporting CPS enables a MOST device to asynchronously send AKE command and response via MOST NetService. The Functions used by the Function Block supporting CPS are described in Chapter 3 of the "MOST Content Security Scheme – DTCP Implementation". The Function Blocks supporting CPS are used by Source and Sink devices.

The HMI and the Function Blocks supporting CPS exchange the SourceInfo and SinkInfo. If HMI received SourceInfo that denotes DTCP, the HMI activate DTCP scheme. The HMI sends Sink.DTCP_StartProcess.StartResult() or Sink.ConnectTo.StartResult() to Sink device. Then the Sink device starts DTCP Authentication exchange, after receiving protected content via synchronous connection. After the authentication is completed, the Sink device notifies it to HMI by sending HMI.DTCP_StartProcess.Result() or HMI.ConnectTo.Result().

V1SH 5 Modifications to 4.2.3.2 Extended Format Fields (Optional Components of the Device Certificate)
The optional content channel cipher for AES-128 is not used since the baseline cipher is AES-128.