DTCP Volume1 Supplement A Mapping DTCP to USB (Informational Version)

Hitachi, Ltd.
Intel Corporation
Matsushita Electric Industrial Co., Ltd.
Sony Corporation
Toshiba Corporation

Revision 1.3
February 28, 2005

Preface

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. Hitachi, Intel, MEI, Sony, and Toshiba (collectively, the “5C”) 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 these portions are preliminary, and that products based on it may not be interoperable with the final version or subsequent versions thereof.

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.

The URL for the Digital Transmission Licensing Administrator web site is: http://www.dtcp.com.

Table of Contents

PREFACE **2**

Notice **2**

Intellectual Property **2**

Contact Information **2**

VOLUME 1 SUPPLEMENT A DTCP MAPPING TO USB **4**

V1SA.1 Introduction **4**

V1SA.1.1 Related Documents 4

V1SA.1.2 Terms and Abbreviations 4

V1SA.2 Modifications to Chapter 6 (Content Channel Management and Protection) **5**

V1SA.2.1 Exchange Key Expiration 5

V1SA.2.2 N_C Update Process 5

V1SA.2.3 Protected Content Header 5

V1SA.2.4 Embedded CCI 5

V1SA.2.5 Content Encryption Formats 6

V1SA.3 Modifications to Chapter 8 (AV/C Digital Interface Command Set Extensions) **7**

V1SA.3.1 Control Packet Format 7

V1SA.3.2 Status Packet Format 8

V1SA.4 USB DTCP Protocols **9**

Figures

Figure 1 Protected Content Header 5

Figure 2 USB DTCP Control Packet Format 7

Figure 3 Status Packet Format 8

Volume 1 Supplement A DTCP Mapping to USB

V1SA.1 Introduction

This supplement describes the mapping of DTCP onto the Universal Serial Bus (USB). 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 DTCP-USB specific changes or additions.

V1SA.1.1 Related Documents

This specification shall be used in conjunction with the following publications. When the publications are superceded by an approved revision, the revision shall apply.

- Digital Transmission Content Protection Specification Volume 1 and Volume 2
- Universal Serial Bus Device Class Definition For Content Security Devices
- USB Content Security Method 2 Digital Transmission Content Protection Implementation Specification (CSM-2 Specification)
- Universal Serial Bus Revision 2.0 Specification

V1SA.1.2 Terms and Abbreviations

CSM	Content Security Method
CSM-2	USB Content Security Method 2 Digital Transmission Content Protection Implementation Specification (CSM-2 Specification)
CSNS	Content Security Notification Service, Refer to Section 2.2 of USB CSM-2 Specification
SRM	System Renewability Message
USB	Universal Serial Bus

V1SA.2 Modifications to Chapter 6 (Content Channel Management and Protection)

V1SA.2.1 Exchange Key Expiration

Source devices expire their Exchange Keys:

- When they stop output of protected content[1].
- When removed or detached from the USB bus.

V1SA.2.2 N_C Update Process

USB provides Isochronous and Bulk data transfer services. For Isochronous transfers, there is no change to the description in section 6.3.2 of the update procedure and timing for N_C.

For USB Control and Bulk, transfers the N_c shall be updated after transmitting 4 Mbytes.

V1SA.2.3 Protected Content Header

Protected content transferred over USB has a two-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)”.

	msb							lsb
Header[0]	EMI		Reserved (Zero)					
Header[1]	Reserved (Zero)							Odd/ Even
PC[0]	Protected Content							
-								
-								
-								
PC[N]								

Figure 1 Protected Content Header

V1SA.2.4 Embedded CCI

The Embedded CCI (Section 6.4) transmission format for the USB bus can be defined in a proprietary manner, in which case, devices handling such content must be format cognizant.

[1] Sources are considered to have stopped output when there are no isochronous or bulk data endpoints for audiovisual content or audio content.

V1SA.2.5 Content Encryption Formats

Protected content sent over USB is encapsulated in an protected content packet (See **Error! Reference source not found.**).

For M6 the encryption frame size for all forms of content shall be in the inclusive range of 8 to 4 MB and be a multiple of 8 bits in length.

For AES the encrypted frame size for all forms of content shall be in the inclusive range of 16 to 4 MB and be a multiple of 8 bits in length.

V1SA.3 Modifications to Chapter 8 (AV/C Digital Interface Command Set Extensions)

V1SA.3.1 Control Packet Format

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

	msb							lsb
Control[0]	C/R bit	reserved (zero)			ctype/response			
Control[1]	category – 0000_2 (AKE)				AKE_ID			
Control[2]	subfunction							
Control[3]	AKE_Procedure							
Control[4]	exchange_Key							
Control[5]	subfunction_dependent							
Control[6]	AKE_Label							
Control[7]	number				status			
Control[8]	Byte Length N of AKE_Info Field							
Control[9]								
AKE_Info[1]	AKE_Info							
-								
-								
AKE_Info[N]								

Figure 2 USB DTCP Control Packet Format

- Control bytes 0, 8, and 9 are used to map DTCP to USB.
- C/R denotes: Command/Response with the values of 1/0 respectively.
- Ctype has the same values as referenced in chapter 8 of DTCP specification and specified by the AV/C Digital Interface Command Set.
- Control bytes 1..7 are identical to operand bytes 0..6 as specified in section 8.3.1.
- The AKE_Info field is identical to the data field specified in section 8.3.1.

V1SA.3.2 Status Packet Format

This section maps the AKE status command specified in Section 8.3.2 to the USB DTCP Status Packet Format. The AKE status command sub fields used with USB have the same values and functions as detailed in Chapter 8.

	msb							lsb
Control[0]	C/R bit	reserved (Zero)			ctype/response			
Control[1]	Category = 0000_2 (AKE)				AKE_ID = 0000_2			
Control[2]	subfunction							
Control[3]	AKE_procedure							
Control[4]	exchange_key							
Control[5]	subfunction_dependent							
Control[6]	AKE_Label = FF_{16}							
Control[7]	Number = F_{16}				Status			

Figure 3 Status Packet Format

- Control byte 0 is used to map DTCP to USB.
- C/R denotes: Command/Response with the values of 1/0 respectively.
- Ctype has the same values as referenced in Chapter 8 of DTCP specification and specified by the AV/C Digital Interface Command Set.
- Control bytes 1..7 are identical to operand bytes 0..6 as specified in Section 8.3.2.
- 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 needed, as it is supported by low-level USB protocols.

V1SA.4 USB DTCP Protocols

This section describes the exchange of DTCP AKE commands, responses, and status frames via CSM-2 USB requests over a USB device's default control endpoint.

It is important to review the following references in order to understand USB CS protocols.

- Universal Serial Bus Device Class Definition For Content Security Devices
- USB Content Security Method 2 Digital Transmission Content Protection Implementation Specification (CSM-2 Specification).
- Chapters 5, 8, and 9 of the Universal Serial Bus Specification Version 1.1

The USB DTCP Implementation has similar device states as described in the DTCP Volume 1 specification.

Authentication may take place as a part of USB enumeration (speculative authentication), after USB enumeration, or upon demand as needed.

The Content Security Notification Service (**CSNS**) enables a USB device to asynchronously send AKE commands and responses via the CSM-2 requests. The **CSNS** is described in section 2.2 of the USB CSM-2 Specification. **CSNS** is used by an attached USB Device to cause the Host to issue a request that will permit the USB Device to send AKE commands and responses to the Host.

CSMs are activated only upon the receipt of a ***Set_Channel_Settings*** CS Request that specifies and correlates a CSM to a logical channel. If CSM-2 is selected, the host will begin a Host initiated DTCP authentication procedure.

CSNS permits USB DTCP compliant devices to initiate DTCP protocols by prompting the Host to send the needed CS or CSM-2 request.

For example, a USB Device will issue the CS ***Change_Channel_Setting*** notification to activate and correlate a CSM to a logical channel.

The Host upon receipt will issue a ***Set_Channel_Settings*** request in response to the ***Change_Channel_Setting*** notification. It is only upon receipt of a ***Set_Channel_Setting*** request that the CSM is activated and assigned to a logical channel.

If CSM-2 is indicated, then the Host will start a Device initiated DTCP Authentication exchange.