

DTCP Volume 1
Supplement E
Mapping DTCP to IP
(Informational Version)

Hitachi, Ltd.

Intel Corporation

Matsushita Electric Industrial Co., Ltd.

Sony Corporation

Toshiba Corporation

Revision 1.0

November 24, 2003

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.

Copyright © 1997 - 2003 by Hitachi, Ltd., Intel Corporation, Matsushita Electric Industrial Co., Ltd., 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.

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

Table of Contents

DTCP VOLUME 1	1
SUPPLEMENT E	1
MAPPING DTCP TO IP	1
(INFORMATIONAL VERSION)	1
PREFACE	2
Notice	2
Intellectual Property	2
Contact Information	2
VOLUME 1 SUPPLEMENT E DTCP MAPPING TO IP	6
V1SE.1 Introduction	6
V1SE.1.1 Related Documents	6
V1SE.1.2 Terms and Abbreviations	6
V1SE.2 Modifications to 4.2.3.2 Extended Format Fields (Optional Components of the Device Certificate)	7
V1SE.3 Modifications to Chapter 5 Restricted Authentication	7
V1SE.4 Modifications to Chapter 6 Content Channel Management Protection	7
V1SE.4.1 Modifications to 6.2.1 Exchange Keys	7
V1SE.4.2 Modifications to 6.2.2.2 K_C for AES-128	7
V1SE.4.3 Modifications to 6.3.1 Establishing Exchange Keys	8
V1SE.4.4 Modifications to 6.3.2 Establishing Content Keys	8
V1SE.4.5 Modifications to 6.3.3 Odd/Even Bit	8
V1SE.4.6 Modifications to 6.4.1 Embedded CCI	8
V1SE.4.7 Modifications to 6.4.2 Encryption Mode Indicator (EMI)	9
V1SE.4.8 Modifications to 6.4.3 Relationship between Embedded CCI and EMI	9
V1SE.4.9 Modification to 6.4.4.1 Format-cognizant source function	10

V1SE.4.10 Modification to 6.4.4.2 Format-non-cognizant source function	10
V1SE.4.11 Modifications to 6.4.4.3 Format-cognizant recording function	11
V1SE.4.12 Modifications to 6.4.4.4 Format-cognizant sink function	11
V1SE.4.13 Modification to 6.4.4.5 Format-non-cognizant recording function	12
V1SE.4.14 Modifications to 6.4.5.1 Embedded CCI for audio transmission	12
V1SE.4.15 Modifications to 6.4.5.3 Audio-format-cognizant source function	12
V1SE.4.16 Modifications to 6.4.5.5 Audio-format-cognizant recording function	13
V1SE.4.17 Modifications to 6.4.5.6 Audio-format cognizant sink function	13
V1SE.4.18 Modifications to 6.6.1 Baseline Cipher	13
V1SE.4.19 Modifications to 6.6.2.1 AES-128 Cipher	13
V1SE.4.20 Modification to 6.6.3 Content Encryption Formats	14
V1SE.4.21 Modifications to 6.7.1 Move Function	14
V1SE.5 Modifications to Chapter 8 (AV/C Digital Interface Command Set Extensions)	15
V1SE.5.1 Modifications to 8.1 Introduction	15
V1SE.5.2 Modifications to 8.3.1 AKE Control Command	15
V1SE.5.3 Modification to 8.3.2 AKE Status Command	16
V1SE.5.4 Modifications to 8.3.3	17
V1SE.5.5 Modifications to AKE Subfunctions	18
V1SE.5.6 Modifications to 8.4 Bus Reset Behavior	18
V1SE.6 Additional Requirements and Recommendations	18
V1SE.6.1 Authentication Capability Constraint	18
V1SE.6.2 Internet Datagram Header Time To Live (TTL) Constraint	18
V1SE.6.3 802.11 Constraint	18
V1SE.6.4 DTCP-IP Move Protocol	18
V1SE.6.5 Recommended MIME type for DTCP protected content	18
V1SE.6.6 Identification of DTCP Sockets	19

Figures

Figure 1 Protected Content Packet Format	14
Figure 2 DTCP-IP Control Packet Format	15
Figure 3 Status Packet Format	16

Tables

Table 1 Length of Keys and Constants (Content Channel Management)	8
Table 2 EMI Mode and E-EMI Description	9
Table 3 Relationship between E-EMI and Embedded CCI	9
Table 4 Format-Cognizant Source Function CCI handling	10
Table 5 Format-Non-Cognizant Source Function CCI handling	10
Table 6 Format-cognizant recording function CCI handling	11
Table 7 Format-cognizant sink function CCI handling	11
Table 8 Format-non-cognizant recording function CCI handling	12
Table 9 Audio Embedded CCI Values	12
Table 10 Audio-format cognizant source function CCI handling	12
Table 11 Audio-format-cognizant recording function CCI handling	13
Table 12 Audio-format-cognizant sink function CCI handling	13
Table 13 AKE Status Command Status Field	16
Table 14 AKE_procedure values	17
Table 15 Authentication selection	17
Table 16 Exchange_key values	17

Volume 1 Supplement E DTCP Mapping to IP

V1SE.1 Introduction

This supplement describes the mapping of DTCP onto Internet Protocol (IP). All aspects of IEEE 1394 DTCP functionally are preserved and this supplement only details DTCP-IP specific changes or additions.

V1SE.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
- RFC768 User Datagram Protocol
- RFC791 Internet Protocol
- RFC793 Transmission Control Protocol
- RFC2616 Hypertext Transfer Protocol – HTTP/1.1
- RFC1889 RTP: A Transport Protocol for Real-Time Applications

V1SE.1.2 Terms and Abbreviations

DTCP-IP	DTCP volume 1 Supplement E
DTCP Socket	Means the Socket used for AKE commands
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
PCP	Protected Content Packet
RTP	Real-time Transport Protocol
Socket	Means IP-address concatenated with port number [e.g. <host>: <port>]
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

V1SE.2 Modifications to 4.2.3.2 Extended Format Fields (Optional Components of the Device Certificate)

For IP, the optional content channel cipher for AES-128 is not used.

V1SE.3 Modifications to Chapter 5 Restricted Authentication

Restricted authentication is not permitted for DTCP-IP transports.

V1SE.4 Modifications to Chapter 6 Content Channel Management Protection

V1SE.4.1 Modifications to 6.2.1 Exchange Keys

DTCP-IP requires only a single exchange key for all defined E-EMI.

V1SE.4.2 Modifications to 6.2.2.2 K_C for AES-128

The Content Key (K_C) is used as the key for the content encryption engine. K_C is computed from the three values shown below:

- Exchange Key K_X where only a single exchange key is used for all E-EMIs to protect the content.
- A random number N_C generated by the source device using RNG_F which is sent in plain text to all sink devices.
- Constant value C_{A0} , C_{B1} , C_{B0} , C_{C1} , C_{C0} , or C_{D0} which corresponds to an E-EMI value in the packet header.

The Content Key is generated as follows:

$$K_C = J\text{-AES}(K_X, f[\text{E-EMI}], N_C) \quad \text{Where:}$$

$$f[\text{E-EMI}] \{$$

$$f[\text{E-EMI}] = C_{A0} \text{ when E-EMI = Mode A0}$$

$$f[\text{E-EMI}] = C_{B1} \text{ when E-EMI = Mode B1}$$

$$f[\text{E-EMI}] = C_{B0} \text{ when E-EMI = Mode B0}$$

$$f[\text{E-EMI}] = C_{C1} \text{ when E-EMI = Mode C1}$$

$$f[\text{E-EMI}] = C_{C0} \text{ when E-EMI = Mode C0}$$

$$f[\text{E-EMI}] = C_{D0} \text{ when E-EMI = Mode D0}$$

$$\}$$

C_{A0} , C_{B1} , C_{B0} , C_{C1} , C_{C0} , and C_{D0} are universal secret constants assigned by the DTLA. The values for these constants and the definition of the function $J\text{-AES}()$ are specified in DTCP Specification available under license from DTLA.

Additional rules for AES-128 Cipher are described in the DTCP Specification available available under license from the DTLA.

V1SE.4.2.1 Modifications to 6.2.2.2.1 AES-128 Related Key and Constant Sizes

Followings are the lengths of the keys and constants described above:

Key or Constant	Size (bits)
Exchange Key (K_X)	96
Scrambled Exchange Key (K_{SX})	96
Constants ($C_{A0}, C_{B1}, C_{B0}, C_{C1}, C_{C0}, C_{D0}$)	96
Content Key for AES-128 Baseline Cipher (K_C)	128
Nonce for Content Channel (N_C)	64

Table 1 Length of Keys and Constants (Content Channel Management)

V1SE.4.3 Modifications to 6.3.1 Establishing Exchange Keys

It is recommended that source devices expire their Exchange Keys when all content transmission has ceased for at least 2 hours.

Devices must expire their Exchange Keys when they detect themselves being disconnected from the medium. For wireless mediums this means when device detects that it is not connected to an access point or it is not directly connected to another device.

Source devices can not change or expire Exchange key(s) during content transmission.

V1SE.4.4 Modifications to 6.3.2 Establishing Content Keys

For RTP transfers, source device generates a 64 bit random number as an initial value for N_C . N_C is updated periodically by incrementing it by $1 \text{ mod } 2^{64}$ while at least on RTP transmission with PCP is in progress regardless of the value of E-EMI. The same value of N_C shall be used for all RTP simultaneous transmissions. The minimum period for update of the N_C is defined as 30 seconds, and the maximum period is defined as 120 seconds.

For HTTP transfers, source devices generate a 64 bit random number as an initial value of N_C for the initial TCP connection. The initial N_C for subsequent TCP connections must be different (another random number may be generated). If a HTTP response has more than 128 MB of content, N_C shall be updated every 128MB. N_C is updated by incrementing it by $1 \text{ mod } 2^{64}$. When plural HTTP responses are transmitted using the same TCP connection, N_C for subsequent HTTP response shall be updated from the latest N_C for the TCP connection.

V1SE.4.5 Modifications to 6.3.3 Odd/Even Bit

The Odd/Even Bit is not used in DTCP-IP as N_C value is sent with each PCP.

V1SE.4.6 Modifications to 6.4.1 Embedded CCI

Embedded CCI is carried as part of the content stream. Many content formats including MPEG have fields allocated for carrying the CCI associated with the stream. The definition and format of CCI is specific to each content format. Information used to recognize the content format should be embedded within the content.

V1SE.4.7 Modifications to 6.4.2 Encryption Mode Indicator (EMI)

E-EMI Mode	E-EMI Value	Description
Mode A0	1100 ₂	Copy-never (CN)
Mode B1	1010 ₂	Copy-one-generation (COG) [Format-cognizant recording only]
Mode B0	1000 ₂	Copy-one-generation [Format-non-cognizant recording permitted]
Mode C1	0110 ₂	Move (Audiovisual)
Mode C0	0100 ₂	No-more-copies (NMC)
Mode D0	0010 ₂	Copy-free with EPN asserted (CF/EPN)
N.A.	0000 ₂	Copy-free (CF)
	---- ₂	All other values reserved

Table 2 EMI Mode and E-EMI Description

V1SE.4.8 Modifications to 6.4.3 Relationship between Embedded CCI and EMI

E-EMI	Embedded CCI					
	CF	CF/EPN	NMC	COG-AV	COG-Audio	CN
Mode A0 (CN)	Allowed	Allowed	Allowed ¹	Allowed	Allowed	Allowed
Mode B1 (Format cognizant only recordable)	Allowed	Allowed	Prohibited	Allowed	Allowed	Prohibited
Mode B0 (Format non-cognizant recordable)	Allowed	Allowed	Prohibited	Allowed	Prohibited	Prohibited
Mode C1 (MOVE)	Prohibited	Prohibited	Allowed	Prohibited	Prohibited	Prohibited
Mode C0 (NMC)	Allowed	Allowed	Allowed	Allowed	Allowed	Prohibited
Mode D0 (CF/EPN)	Allowed	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
N.A.	Allowed	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited

Table 3 Relationship between E-EMI and Embedded CCI

¹ Not typically used.

V1SE.4.9 Modification to 6.4.4.1 Format-cognizant source function

Embedded CCI of programs					E-EMI
CF	CF/EPN	NMC	COG-AV	CN	
Don't care	Don't care	*2	Don't care	Present	Mode A0
Don't care	Don't care	Cannot be present	Don't care	Cannot be present	Mode B1
Don't care	Don't care	Cannot be present	Present	Cannot be present	Mode B0
Don't care	Don't care	Present	Cannot be present	Cannot be present	Mode C0
Don't care	Present	Cannot be present ³	Cannot be present	Cannot be present	Mode D0
Present	Cannot be present	Cannot be present	Cannot be present	Cannot be present	N.A.
Other combinations					Transmission Prohibited

Table 4 Format-Cognizant Source Function CCI handling

V1SE.4.10 Modification to 6.4.4.2 Format-non-cognizant source function

E-EMI or recorded CCI ⁴ of source content	E-EMI used for transmission
Copy Never	Mode A0
COG: Format cognizant only recordable	Mode B1
COG: Format non-cognizant recordable	Mode B0
No-more-copies	Mode C0
EPN asserted Copy Free	Mode D0
Copy-Free	N.A.

Table 5 Format-Non-Cognizant Source Function CCI handling

² Don't care, but not typically used.

³ This combination is allowed for format-non-cognizant source function, but is not permitted for format-cognizant source function.

⁴ Recorded CCI is copy control information that is not embedded in the content program and does not require knowledge of the content format to extract.

V1SE.4.11 Modifications to 6.4.4.3 Format-cognizant recording function

E-EMI	Embedded CCI for each program				
	CF	CF/EPN	NMC	COG-AV	CN
Mode A0	Recordable	Recordable	Do not record	*5	Do not record
Mode B1	Recordable	Recordable	Discard entire content stream ⁶	*5	Discard entire content stream ⁶
Mode B0	Recordable	Recordable	Discard entire content stream ⁶	*5	Discard entire content stream ⁶
Mode C0	Recordable	Recordable	Do not record	Do not record	Discard entire content stream ⁶
Mode D0	Recordable	Recordable	Discard entire content stream ⁶	Discard entire content stream ⁶	Discard entire content stream ⁶

Table 6 Format-cognizant recording function CCI handling

V1SE.4.12 Modifications to 6.4.4.4 Format-cognizant sink function

E-EMI	Embedded CCI for each program				
	CF	CF/EPN	NMC	COG-AV	CN
Mode A0	Available for processing	Available for processing	Available for processing ¹	Available for processing	Available for processing
Mode B1	Available for processing	Available for processing	Discard entire content stream ⁷	Available for processing	Discard entire content stream ⁷
Mode B0	Available for processing	Available for processing	Discard entire content stream ⁷	Available for processing	Discard entire content stream ⁷
Mode C0	Available for processing	Available for processing	Available for processing	Available for processing ⁸	Discard entire content stream ⁷
Mode D0	Available for processing	Available for processing	Discard entire content stream ⁷	Discard entire content stream ⁷	Discard entire content stream ⁷

Table 7 Format-cognizant sink function CCI handling

⁵ If the recording function supports recording a CCI value of No-more-copies then the CCI value of No-more-copies shall be recorded with the program. Otherwise the CCI of Copy-never shall be recorded with the program.

⁶ If the function detects this CCI combination among the programs it is recording, the entire content stream is discarded.

⁷ If the function detects this CCI combination among the programs, the entire content stream is discarded.

⁸ If the device has a rule for handling No-more-copies, this program shall be handled according to the rule. Otherwise the program shall be handled as Copy Never.

V1SE.4.13 Modification to 6.4.4.5 Format-non-cognizant recording function

E-EMI of the received stream	Recorded CCI⁹ to be written onto user recordable media
Mode A0	Stream cannot be recorded
Mode B1	Stream cannot be recorded
Mode B0	No-more-copies
Mode C0	Stream cannot be recorded
Mode D0	EPN asserted Copy Free

Table 8 Format-non-cognizant recording function CCI handling

V1SE.4.14 Modifications to 6.4.5.1 Embedded CCI for audio transmission

Value and Abbreviation	Meaning
11	Not defined
10 (COG-audio)	Copy-permitted-per-type
01 (NMC)	No-more-copies
00 (CF)	Copy-free

Table 9 Audio Embedded CCI Values

V1SE.4.15 Modifications to 6.4.5.3 Audio-format-cognizant source function

Embedded CCI of programs			E-EMI
CF	NMC	COG-audio	
Type specific ¹⁰			Mode A0
Don't care	Cannot be present	Don't care	Mode B1
Don't care	Present	Don't care	Mode C0
Present	Cannot be present	Cannot be present	N.A.

Table 10 Audio-format cognizant source function CCI handling

⁹ Recorded CCI is copy control information that is not embedded in the content program and does not require knowledge of the content format to extract.

¹⁰ Usage is specified for each Audio type in Appendix A.

V1SE.4.16 Modifications to 6.4.5.5 Audio-format-cognizant recording function

E-EMI	Embedded CCI of Program		
	CF	NMC	COG-audio
Mode A0	Recordable	Do not record	Recordable ¹¹
Mode B1	Recordable	Discard entire content stream ¹²	Recordable ¹¹
Mode C0	Recordable	Do not record	Recordable ¹¹

Table 11 Audio-format-cognizant recording function CCI handling

V1SE.4.17 Modifications to 6.4.5.6 Audio-format cognizant sink function

E-EMI	Embedded CCI of program		
	CF	NMC	COG-audio
Mode A0	Available for processing	Available for processing	Available for processing
Mode B1	Available for processing	Discard entire content stream ¹²	Available for processing
Mode C0	Available for processing	Available for processing	Available for processing

Table 12 Audio-format-cognizant sink function CCI handling

V1SE.4.18 Modifications to 6.6.1 Baseline Cipher

For IP, 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.

V1SE.4.19 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. Additional rules for AES-128 Cipher are described in the DTCP Specification Available under license from DTLA.

¹¹ The CCI value of No-more-copies shall be recorded with the program. Additional rules for recording are specified by each audio application in Appendix A.

¹² If the function detects this CCI combination among the programs it is recording the entire content stream is discarded.

V1SE.4.20 Modification to 6.6.3 Content Encryption Formats

DTCP encrypted content is sent via Protected Content Packets (PCP) where the format of the PCP is described in the following figure.

	msb						lsb
Header[0]	reserved (zero)		C_A	E-EMI			
Header[1]	exchange_key_label						
Header[2]	N _c (64 bits)						
Header[3]							
Header[4]							
Header[5]							
Header[6]							
Header[7]							
Header[8]							
Header[9]							
Header[10]	Byte length of content denoted as CL (32 bits)						
Header[11]							
Header[12]							
Header[13]							
EC[0]	Content affixed with 0 to 15 bytes of padding						
EC[1]							
EC[2]							
-							
-							
-							
EC[N-1]							

Figure 1 Protected Content Packet Format

Header [0]: C_A means cipher_algorithm where a value of 0₂ denotes AES-128 and the value 1₂ denotes optional cipher. E-EMI is as defined in section V1SE.4.7

Header [1]: Contains exchange_key_label which is described in the DTCP Specification available under license from DTLA.

Header [2..9]: Contains N_c as described in section V1SE.4.2.1.

Header [10..13]: Denotes byte length of content and does not include any padding bytes, where CL is less than or equal to 128 MB.

EC [0..N-1]: Represents encrypted frame and is a multiple of 16 Bytes in length where N = (Int((CL-1)/16)+1)*16 where padding length is equal to N-CL and Int(X) means maximum integer less than or equal to X. The value of each padding Byte is 00₁₆.

For RTP transfers, each RTP payload is encapsulated by a single PCP.

For HTTP transfers, responses may contain 1 or more PCPs.

V1SE.4.21 Modifications to 6.7.1 Move Function

This supplement defines a Move function in addition to the one described in section 6.7.1 where content with Embedded CCI of No-more-copies content may not be remarked as Copy-one-generation but instead be transmitted as No-more-copies using Mode C1 of E-EMI for IP transport of DTCP protected content and Recording functions may record the received content without remarking embedded CCI. For clarity, the move function shall be used between a single source and a single sink function.

V1SE.5 Modifications to Chapter 8 (AV/C Digital Interface Command Set Extensions)

V1SE.5.1 Modifications to 8.1 Introduction

DTCP-IP uses TCP port to send/receive DTCP control packets, status command packets, and response packets. DTCP Socket identification of source device is described in section V1SE.6.6.

V1SE.5.2 Modifications to 8.3.1 AKE Control Command

This section maps the AKE control command specified in Section 8.3.1 to the DTCP-IP Control Packet Format. Except as otherwise noted, the AKE control command sub fields used with IP have the same values and functions as detailed in Chapter 8.

	msb							lsb
Type[0]	0	0	0	0	0	0	0	1
Length[0]	(msb) Byte Length of Control and AKE_Info Fields (N+8)							
Length[1]	(lsb)							
Control[0]	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							
Control[7]	number(option)				status			
AKE_Info[0..N-1]	AKE_Info							

Figure 2 DTCP-IP Control Packet Format

- Type, Length, and Control byte 0 are used to map DTCP to IP. Where the type field identifies version 1 AKE control packet.
- Ctype/response has the same values as referenced in chapter 8 of DTCP specification and specified by the AV/C Digital Interface Command.
- Control bytes 1..7 are identical to operand bytes 0..6 as specified in section 8.3.1, except for four most significant bits of Control byte 7 which is not used in IP.
- The AKE_Info field is identical to the data field specified in section 8.3.1.
- The AKE_label and source Socket of each control command should be checked to ensure that it is from the appropriate controller.

V1SE.5.3 Modification to 8.3.2 AKE Status Command

This section maps the AKE status command specified in Section 8.3.2 to the DTCP-IP Status Packet Format. Except as otherwise noted, the AKE status command sub fields used with IP have the same values and functions as detailed in Chapter 8.

	msb							lsb
Type[0]	0	0	0	0	0	0	0	1
Length[0]	(msb) Byte length of Control							
Length[1]								(lsb)
Control[0]	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

- Type, Length, and Control byte 0 are used to map DTCP to IP. Where the type field identifies version 1 AKE control packet.
- 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.

V1SE.5.3.1 Modifications to AKE status command status field

Value	Status	Response code
0000 ₂	No error	STABLE
0001 ₂	Support for no more authentication procedures is currently available	STABLE
0111 ₂	Any other error	STABLE
1111 ₂	No information ¹³	REJECTED

Table 13 AKE Status Command Status Field

¹³ It is recommended that implementers not use the “No information” response.

V1SE.5.4 Modifications to 8.3.3

V1SE.5.4.1 AKE_ID dependent field

DTCP-IP implementations only require a single exchange key, specifically Bit 3 of exchange_key field will be used for transporting all DTCP Protected content over IP for all defined E-EMI.

For DTCP-IP both Source and Sink shall support only Full Authentication.

Therefore Restricted Authentication procedure (rest_auth) and Enhanced Restricted Authentication procedure (en_rest_auth) are prohibited. Extended Full Authentication procedure (ex_full_auth) is optional¹⁴ and not used to handle Bit 3 of Exchange_key field.

Bit	AKE_procedure
0 (lsb)	Prohibited
1	Prohibited
2	Full Authentication procedure (full_auth)
3	Extended Full Authentication procedure ¹⁵ (ex_full_auth, optional) ¹⁶
4 - 7 (msb)	Reserved for future extension and shall be zero

Table 14 AKE_procedure values

V1SE.5.4.2 Modifications to Authentication selection

Source supported authentication Procedures	Sink supported authentication procedures	
	Full_auth	Full_auth and Ex_full_auth
Full_auth	Full Authentication	Full Authentication
Full_auth and Ex_full_auth	Full Authentication	Extended Full Authentication

Table 15 Authentication selection

V1SE.5.4.3 Modification to Exchange_key values

DTCP-IP uses a single exchange key.

Bit	Exchange_key
0 (lsb)	Prohibited
1	Prohibited
2	Prohibited
3	Exchange key for AES-128
4 – 7 (msb)	Reserved for future extension and shall be zero

Table 16 Exchange_key values

¹⁴ Features of this specification that are labeled as “optional” describe capabilities whose usage has not yet been established by DTLA.

¹⁵ Devices that support extended device certificates use the Extended Full Authentication procedure described in this chapter.

¹⁶ Features of this specification that are labeled as “optional” describe capabilities whose usage has not yet been established by the 5C.

V1SE.5.5 Modifications to AKE Subfunctions

Subfunctions modified for DTCP-IP are described in the DTCP Specification available under license from the DTLA.

V1SE.5.6 Modifications to 8.4 Bus Reset Behavior

This section does not apply to DTCP-IP.

V1SE.6 Additional Requirements and Recommendations

V1SE.6.1 Authentication Capability Constraint

For DTCP-IP both source and sink devices shall only use Full Authentication.

V1SE.6.2 Internet Datagram Header Time To Live (TTL) Constraint

TTL is described in RFC791 and the following requirements only apply to IP datagrams that transport DTCP AKE commands. Transmitting devices shall set TTL value of such transmitted IP datagrams to a value no greater than 3 and correspondingly receiving devices shall discard such received IP datagrams which have a TTL value greater than 3.

V1SE.6.3 802.11 Constraint

DTCP devices with integrated 802.11 must ensure that WEP is engaged prior to exchanging DTCP AKE commands and protected content via such a network interface. Please note that this requirement to use WEP may be amended to require use of successor technologies as designated by DTLA.

V1SE.6.4 DTCP-IP Move Protocol

Transaction-based is to be defined.

V1SE.6.5 Recommended MIME type for DTCP protected content

DTCP application media type is as follows:

`application/x-dtcp1; CONTENTFORMAT=<mimetype>`

Where **CONTENTFORMAT**, is the standard content media type that is protected by DTCP.

In addition, information identifying DTCP Socket may be included as follows:

`application/x-dtcp1; DTCP1HOST=<host>; DTCP1PORT=<port>;
CONTENTFORMAT=<mimetype>`

Refer to V1SE.6.6.1 for description of **DTCP1HOST** and **DTCP1PORT**.

Content type of HTTP response is set to DTCP application media type.

V1SE.6.6 Identification of DTCP Sockets

DTCP uses a TCP port to support various command and control protocols (i.e. AKE, Exchange Keys, SRM,...) and either TCP or UDP for content transport. This section details recommend practices for identifying DTCP Sockets.

V1SE.6.6.1 URI Recommended Format

This following information is inserted into the query string portion of URI and is used to communicate the source's content and DTCP Socket to the sink. The source obtains the sink's DTCP Socket when the sink establishes a TCP connection to the source.

```
<service>://<host>:<port>/<path>/<FileName>.<FileExtention>?CONTENTPROTECTIONTYPE=DTCP1&DTCP1HOST=<host>&DTCP1PORT=<port>
```

Where:

CONTENTPROTECTIONTYPE, is set to "DTCP1" where 1 represents a DTCP-IP version number that can be incremented in future as the needed.

DTCP1HOST specifies the IP address and **DTCP1PORT** specifies the port number of the DTCP Socket of the source device.

V1SE.6.6.2 HTTP response

Content type of HTTP response is set to DTCP application media type as follows:

```
Content-Type: application/x-dtcp1 ; DTCP1HOST=<host> ; DTCP1PORT=<port> ;  
CONTENTFORMAT=<mimetype>
```