DTCP Volume 1
Supplement G
Mapping DTCP to WirelessHD
(Informational Version)

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

Revision 1.0
July 11, 2008

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

Figures

Tables

Volume 1 Supplement G DTCP Mapping to WirelessHD

V1SG.1 Introduction

This supplement maps DTCP onto WirelessHD. All aspects of IEEE 1394 DTCP functionally except those described in Appendix D are preserved and this supplement only details WirelessHD DTCP specific changes or additions.

V1SG.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 When the publications are superseded by an approved revision, the revision shall apply.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
- WirelessHD Specification

V1SG.1.2 Terms and Abbreviations

CTB	Channel Time Block
DTCP-WirelessHD	DTCP volume 1 Supplement G
RTT	Round Trip Time
STID	STation IDentifier
WVAN	Wireless Video Area Network

V1SG.2 Modifications to 4.2.3.2 Extended Format Fields (Optional Components of the Device Certificate)

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

V1SG.3 Modifications to Chapter 5 Restricted Authentication

Restricted authentication is not permitted for DTCP-WirelessHD transports.

V1SG.4 Modifications to Chapter 6 Content Channel Management Protection

V1SG.4.1 Modifications to 6.2.1 Exchange Keys

DTCP-WirelessHD requires only a single exchange key for all defined EMI Modes.

V1SG.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 defined EMI Modes to protect the content.
- Seed for content channel N_C generated by the source device which is sent in plain text to all sink devices.
- Constant value C_a, C_b, C_c which corresponds to EMI Mode.

The Content Key is generated as follows:

K_C = J-AES(K_X, f[Ext || EMI], N_C) Where:

f[Ext || EMI] {

f[Ext || EMI]=C_a when (Ext = 0_2 || EMI = 11_2)= Mode A

f[Ext || EMI]=C_b when (Ext = 0_2 || EMI = 10_2)= Mode B

f[Ext || EMI]=C_c when (Ext = 0_2 || EMI = 01_2)= Mode C

}

EMI Mode	Ext bit Value	EMI bits Value	Description
Mode A	0_2	11_2	Copy-never (CN)
Mode B	0_2	10_2	Copy-one-generation (COG)
Mode C	0_2	01_2	No-more-copies (NMC)
N.A.	0_2	00_2	Copy-free (CF)
Reserved Mode1	1_2	11_2	Reserved
Reserved Mode2	1_2	10_2	Reserved
Reserved Mode3	1_2	01_2	Reserved
Reserved Mode4	1_2	00_2	Reserved

Table1 EMI Mode and EMI description

C_a, C_b, and C_c are universal secret constants assigned by the DTLA. The values for these constants are specified in Volume 2 Chapter 10.

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

V1SG.4.3 Exchange Key Expiration

Both source and sink devices shall expire their Exchange Keys when they are detached from the WVAN. For avoidance of doubt, this means that a source device shall expire its Exchange Keys when it is detached from the WVAN, and a sink device shall expire its Exchange Keys when it is detached from the WVAN.

V1SG.4.4 Detached status of WirelessHD devices

A Station shall regard it is detached when it becomes disassociated status with a Coordinator. A Coordinator shall regard it is detached when it detects all Stations in the WVAN become disassociated status with it.

V1SG.4.5 N_c Update Process

WirelessHD provides isochronous data transfer services. For isochronous data transfer, there is no change to the description in Section 6.3.2 of update procedure and timing for N_c.

V1SG.4.6 Modification to 6.3.3 Odd/Even Bit

The Odd/Even bit transferred over WirelessHD is set to the DTCP specified field in CP header defined in “WirelessHD specification” as follows;

msb			lsb
Ext	EMI		Odd/Even

Figure 1 DTCP specified field Format

V1SG.4.7 Modification to 6.4.2 Encryption Mode Indicator(EMI)

The Ext bit and EMI bits that encode EMI Mode transferred over WirelessHD are set to the DTCP specified field. The locations of the Ext bit and EMI bits are shown by Figure 1 DTCP specified field Format.
The encoding used for the Ext bit and EMI bits is shown by Table1 in V1SG.4.2.

V1SG.4.8 Modifications to 6.6.1 Baseline Cipher

For WirelessHD, the baseline cipher is AES-128 using the Counter mode (CTR). AES-128 is described in FIPS 197 dated November 26, 2001 and the CTR mode is described in NIST SP 800-38A 2001 Edition.

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

V1SG.4.9 Modification to 6.6.3 Content Encryption Formats

DTCP protected content is transferred via sub-packet defined in “WirelessHD specification”. The sub-packet has a CP sub-packet Header which is 16 bits unencrypted field used for carrying Embedded CCI. Encrypted content in sub-packet is an encrypted frame and it can range from 0 to 2^{20} bytes in length.
The format of sub-packet is defined in “WirelessHD specification”.

V1SG.4.10 Embedded CCI

The Embedded CCI (Section 6.4.1 or Section 6.4.5.1) is carried in CP sub-packet Header. The format of CP sub-packet header is defined in “WirelessHD specification”.

V1SG.4.10.1 Embedded CCI for Audio stream

There are four types of Audio stream defined in “WirelessHD specification” and Embedded CCI is defined for each type of Audio stream.
The audio type for Audio component of audiovisual stream is referred as “General Audio”.
Three audio types defined in DTCP specification are also defined. Type 1 audio is referred as “IEC 60958 Identified Audio”, Types 2 audio is referred as “DVD Audio” and Type 3 audio is referred as “Super Audio CD”.

V1SG.5 Modifications to Chapter 8 (AV/C Digital Interface Command Set Extensions)

V1SG.5.1 Modifications to 8.1 Introduction

DTCP-WirelessHD uses AV/C message packet to send/receive DTCP control packets, status command packets, and response packets, which is defined in “WirelessHD AV/C specification”.
Devices shall wait at least one second for a response to a command except SRM subfunction and shall wait at least ten seconds for a response to a command with SRM subfunction before timing out.

V1SG.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 WirelessHD DTCP Control Packet Format. The AKE control command subfields used with WirelessHD have the same values and functions as detailed in Chapter 8.

	msb							lsb
Byte [0]	reserved (zero)				ctype/response			
Byte [1]	category = 0000_2 (AKE)				AKE_ID			
Byte [2]	AKE_ID dependent field							
Byte [3]								
Byte [4]								
Byte [5]								
Byte [6]	AKE_label							
Byte [7]	number(option)				status			
Byte [8]	AKE_Info							
-								
-								
Byte [7+m]								

Figure 2 WirelessHD DTCP Control Packet Format

- ctype/response has the same values as referenced in chapter 8 of DTCP Volume 1 specification and specified by the AV/C Digital Interface Command Set. The possible values for DTCP-WirelessHD are specified in V1SG.5.4.
- The Reserved bits are reserved for future definition and are currently defined to have a value of zero.
- Byte[1]..Byte[7] are identical to Operand[0]..Operand[6] as specified in section 8.3.1.
- The AKE_Info field is identical to the data field specified in section 8.3.1.
- The AKE_label and source STID of each control command should be checked to ensure that it is from the appropriate controller.
- Unless otherwise noted in the description of each subfunction, if a given command frame includes an AKE_Info field, the corresponding response frame does not have an AKE_Info field.
- For WirelessHD DTCP Control packet, fragmentation is not defined.

The data length of WirelessHD DTCP Control Packet is exchanged via a Length field defined in “WirelessHD specification”.

V1SG.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 WirelessHD DTCP Status Packet Format. The AKE status command subfields used with WirelessHD have the same values and functions as detailed in Chapter 8.

	msb							lsb
Byte [0]	reserved (zero)				ctype/response			
Byte [1]	category = 0000_2 (AKE)				AKE_ID = 0000_2			
Byte [2]	AKE_ID dependent field							
Byte [3]								
Byte [4]								
Byte [5]								
Byte [6]	AKE_label=FF_{16}							
Byte [7]	F_{16}				status			

Figure 3 WirelessHD DTCP Status Packet Format

- ctype/response has the same values as referenced in chapter 8 of DTCP Volume 1specification and specified by the AV/C Digital Interface Command Set. The possible values for DTCP-WirelessHD are specified in V1SG.5.4.
- The Reserved bits are reserved for future definition and are currently defined to have a value of zero.
- Byte[1]..Byte[7] are identical to Operand[0]..Operand[6] as specified in Section 8.3.2.

V1SG.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[1]	REJECTED

Table 2 AKE Status Command Status Field

[1] It is recommended that implementers not use the "No information" response.

V1SG.5.4 ctype/response values(informative)

Value	Command type / Response type
0_{16}	CONTROL
1_{16}	STATUS
2_{16}	SPECIFIC INQUIRY
3_{16}	Not used
4_{16}	Not used
5_{16}– 7_{16}	Reserved for future extension
8_{16}	NOT IMPLEMENTED
9_{16}	ACCEPTED
A_{16}	REJECTED
B_{16}	Not used
C_{16}	IMPLEMENTED/STABLE
D_{16}	Not used
E_{16}	Reserved for future extension
F_{16}	Not used

Table 3 ctype/response values(informative)

V1SG.5.5 Modifications to 8.3.3

V1SG.5.5.1 AKE_ID dependent field

DTCP-WirelessHD implementations only require a single exchange key, specifically Bit 4 of exchange_key field will be used for transporting all DTCP Protected content over WirelessHD for all defined EMI.
For DTCP-WirelessHD, 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 optional[2] and not used to handle Bit 4 of Exchange_key field.

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

Table 4 AKE_procedure values

[2] Features of this specification that are labeled as “optional” describe capabilities whose usage has not yet been established by DTLA.
[3] Devices that support extended device certificates use the Extended Full Authentication procedure described in this chapter.
[4] Features of this specification that are labeled as “optional” describe capabilities whose usage has not yet been established by DTLA.

V1SG.5.5.2 Modifications to Authentication selection

	Sink supported authentication procedures	
Source 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 5 Authentication selection

V1SG.5.5.3 Modification to Exchange_key values

DTCP-WirelessHD uses a single exchange key defined in the following table.

Bit	Exchange_key
0 (lsb)	Prohibited
1	Prohibited
2	Prohibited
3	Prohibited
4	Exchange Key for AES-128 CTR mode
5 – 7 (msb)	Reserved for future extension and shall be zero

Table 6 Exchange_key values

V1SG.5.6 Modifications to AKE Subfunctions

Subfunction modified for DTCP-WirelessHD are described in the DTCP specification available under license from the DTLA.

V1SG.5.7 Modifications to 8.4 Bus Reset Behavior

Source device and sink device shall immediately stop authentication procedure between the devices if each device detects either device is detached from the WVAN during authentication procedure.

V1SG.6 Additional Localization via RTT

This section specifies Additional Localization for the WirelessHD.

V1SG.6.1 Purpose and Scope

Source devices and Sink devices must implement Additional Localization (AL) as specified in this section.
Source devices with AL when conducting an AKE with a Sink device with AL, the source devices must perform a RTT test if the sink device's Device ID is not on the source device's RTT registry.
Source devices will add a Sink device's Device ID to the Source device's RTT registry, will set the content transmission counter for the sink device to 40 hours, and will provide an exchange key only if the source device measures a RTT value of 1 millisecond or less during RTT test.
Source devices when transmitting content will update content transmission counters of all RTT registered sink devices and are required to remove the Device ID of a sink device from the RTT registry after counting 40 hours of content transmission.
Background RTT testing is not supported for WirelessHD because the method of measuring RTT in "WirelessHD Specification" is specified only for RTT-AKE case.
When RESPONSE2 subfunction is received, ID_U shall be used instead of Device ID in above processes.

V1SG.6.2 Protected RTT Protocol

V1SG.6.2.1 Protocol

Protected RTT protocol is described in Figure 4 and is used in RTT-AKE procedure. The RTT protocol is executed after the Challenge-Response portion of the AKE is completed. SHA-1 is used to construct following messages that are exchanged during RTT testing protocol to ensure that source and sink which completed Challenge-Response portion of AKE are only ones involved in RTT testing.

- MAC1A = MAC1B = $[\text{SHA-1}(MK+N)]_{msb80}$
- MAC2A = MAC2B = $[\text{SHA-1}(MK+N)]_{lsb80}$
- OKMSG = $[\text{SHA-1}(MK+N+1)]_{msb80}$
  Where MK is 160 bits and equal to SHA-1(Kauth||Kauth), N is 16 bit number that ranges from 0 to 1023, and "+" used in RTT Protocol means mod 2^{160} addition.

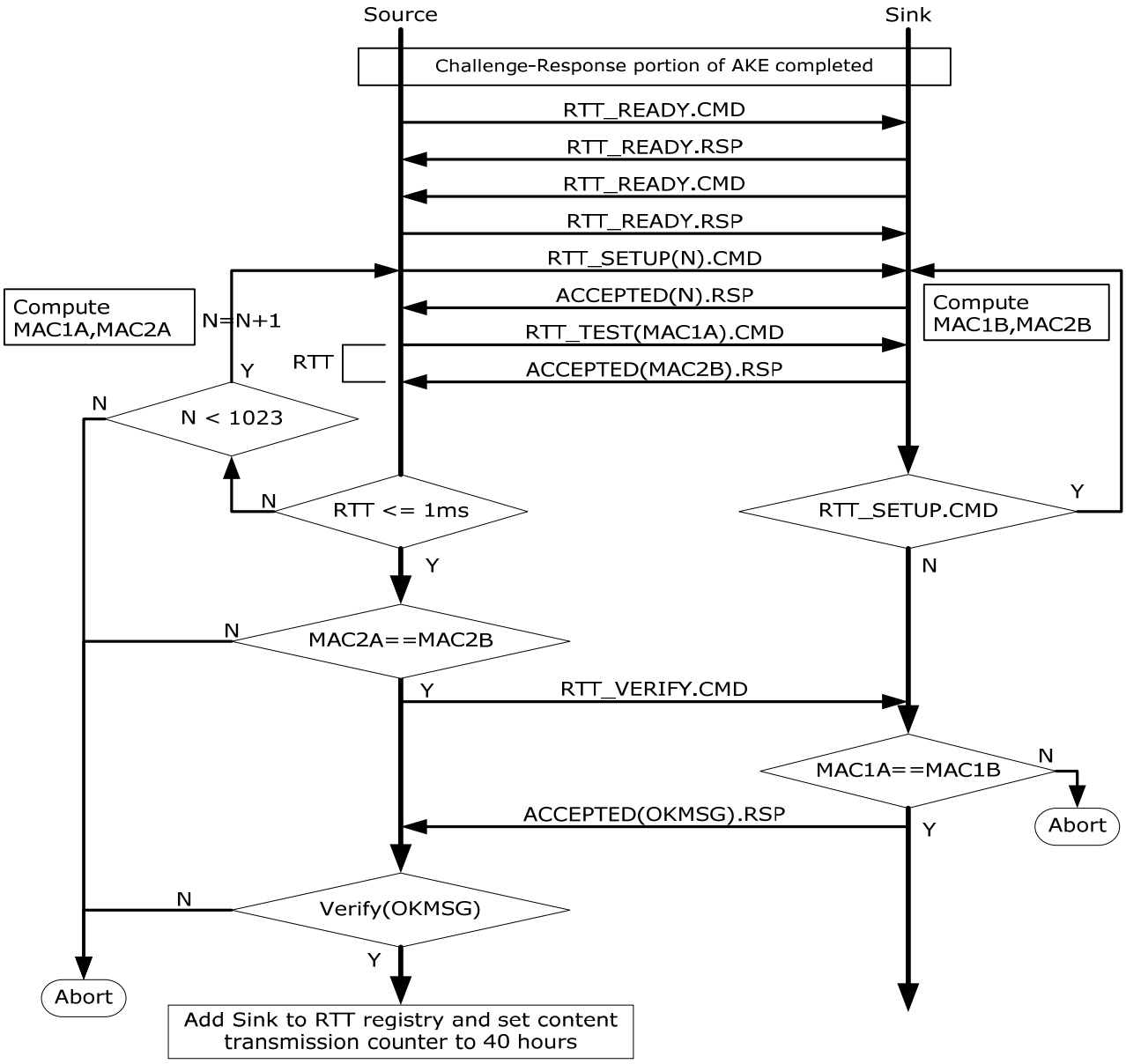

Figure 4 RTT Protocol Diagram

The RTT_READY command is used to indicate that authentication computation is complete and that source and sink devices are ready to execute the RTT test procedure.
The RTT procedure begins by first establishing value of N using the RTT_SETUP command. N is initially set to zero and can range from 0 to 1023 as maximum permitted RTT trials per AKE is 1024. After preparation of MAC values corresponding to N, source device will then measure RTT which is the time interval starting after source transmits RTT_TEST command and terminates upon reception of RTT_TEST accepted response.
If the RTT is greater than 1 millisecond and the value of N is less than 1023 the source will repeat RTT procedure by incrementing N by 1 and reissue RTT_SETUP and RTT_TEST commands.
If the measured RTT is less than or equal to 1 millisecond:

The source device compares most recently computed MAC2A to most recently received MAC2B and if not equal the source device aborts RTT procedure else if equal it sends RTT_VERIFY command to sink device.

The sink device will after receipt of RTT_VERIFY command compare the most recently received MAC1A and most recently computed MAC1B and if not equal aborts RTT procedure else if equal it will send OKMSG in RTT_VERIFY accepted response.

The source device will verify OKMSG and if it is not correct the source device aborts RTT procedure else it will add sink device's Device ID to RTT registry and set content transmission counter to 40 hours. When RESPONSE2 subfunction is received, ID_U shall be used instead of Device ID in above process.

If RTT procedure is aborted the source shall not provide an exchange key.

V1SG.6.2.2 RTT-AKE

The RTT-AKE procedure starts exactly the same as normal AKE but a source device that has DTCP certificate with AL flag set to one must check AL flag value of a sink device and if the AL flag value is also set to one then:

The sink device after completing Challenge-Response portion of AKE will wait and the sink device will abort if it receives any other command than the RTT_READY command, EXCHANGE_KEY command, or AKE_CANCEL command.

The source device then examines the RTT registry and if the sink device's Device ID is on its RTT registry, the source device proceeds to exchange key portion of AKE otherwise the source device initiates a RTT test procedure and if during test it obtains a RTT measurement of 1 millisecond or less it will add the sink device's Device ID to its RTT registry, set content transmission counter to 40 hours, and then proceed to exchange key portion of AKE. When RESPONSE2 subfunction is received, ID_U shall be used instead of Device ID in above process.

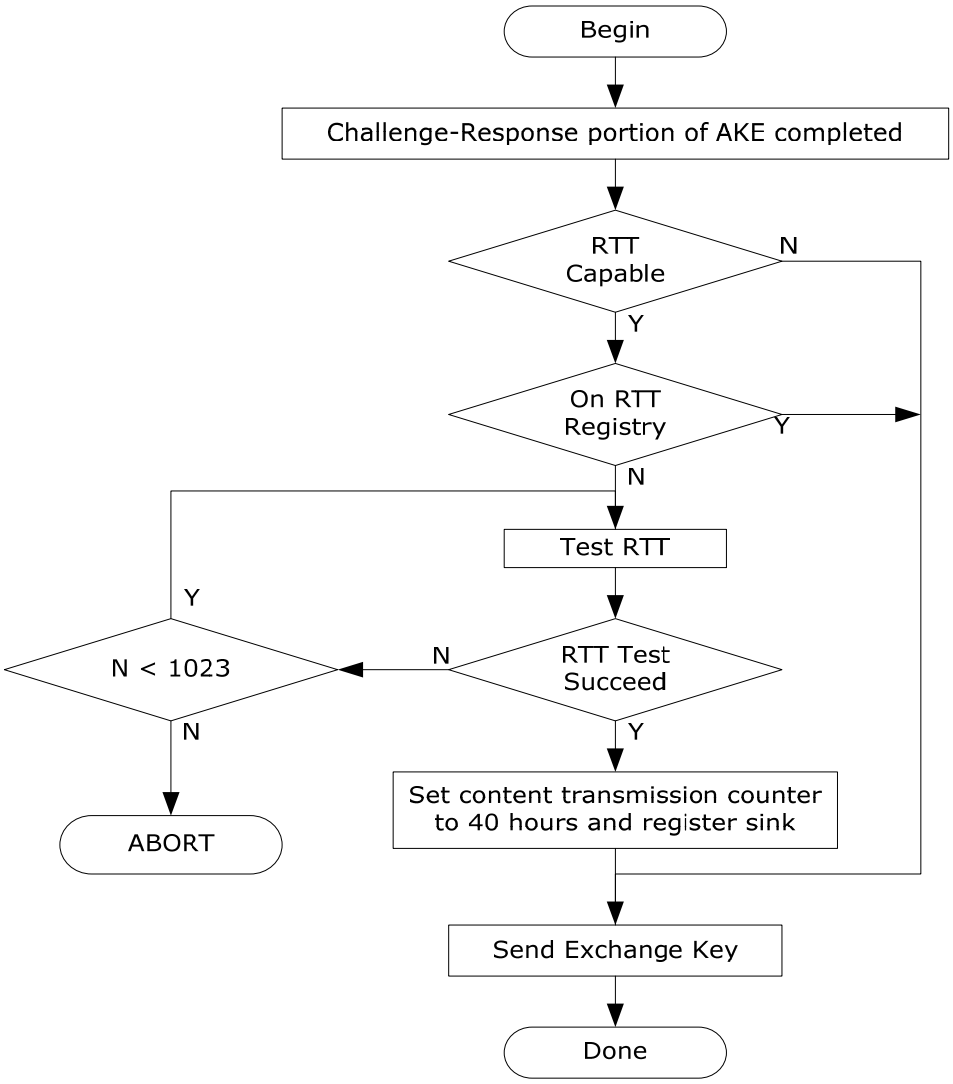

Figure 5 RTT-AKE Informative Flow Diagrams

V1SG.7 Additional Commands and Sequences

Commands for Additional Localization are described in the DTCP specification available under license from the DTLA.

V1SG.8 WirelessHD DTCP Protocols

This section describes the exchange of DTCP AKE commands, responses, and status frames by WirelessHD DTCP Function.

WirelessHD support for RTT is defined in Round Trip Time Verification section of the WirelessHD specification.

Additional rules for WirelessHD DTCP Protocols are described in the DTCP Specification available under license from the DTLA.