DTCP Volume 1

Supplement F

DTCP 1394 Additional Localization

(Informational Version)

Hitachi, Ltd.

Intel Corporation

Matsushita Electric Industrial Co., Ltd.

Sony Corporation

Toshiba Corporation

Revision 1.0

June 15, 2007

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

Volume 1 Supplement F DTCP 1394 Additional Localization

V1SF.1 Introduction

This supplement describes DTCP 1394 additional localization. All aspects of IEEE 1394 DTCP functionality are preserved.

V1SF.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 When the publications are superseded by an approved revision, the revision shall apply.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
- Volume 1 Supplement D DTCP Use of IEEE1394 Similar Transports

V1SF.1.2 Terms and Abbreviations

RTT	Round Trip Time

V1SF.2 Purpose and Scope

Source devices that support Full Authentication or Enhanced Restricted Authentication must implement Additional Localization (AL) as specified in this Supplement F[1].

Sink devices must implement AL as specified in this Supplement F, except for sink devices that are manufactured so as to be capable of receiving content only from source device without AL.

A device that has both source and sink functions is not required to implement AL if the device's source function is not required to implement AL even if the device's sink function is required to implement AL.

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 7 milliseconds 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 a required capability. If background RTT testing is supported, the source device will add the sink device’s Device ID to the RTT registry if not registered and set content transmission counter to 40 hours only if the source device measures a RTT value of 7 milliseconds or less during RTT test.

When RESPONSE2 subfunction is received, ID_U shall be used instead of Device ID in above processes.

[1] This rule is applied except as otherwise provided in the Compliance Rules.

V1SF.3 Protected RTT Protocol

V1SF.3.1 Protocol

Protected RTT protocol is described in Figure 1 and is used in RTT-AKE and Background RTT check procedures. 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.

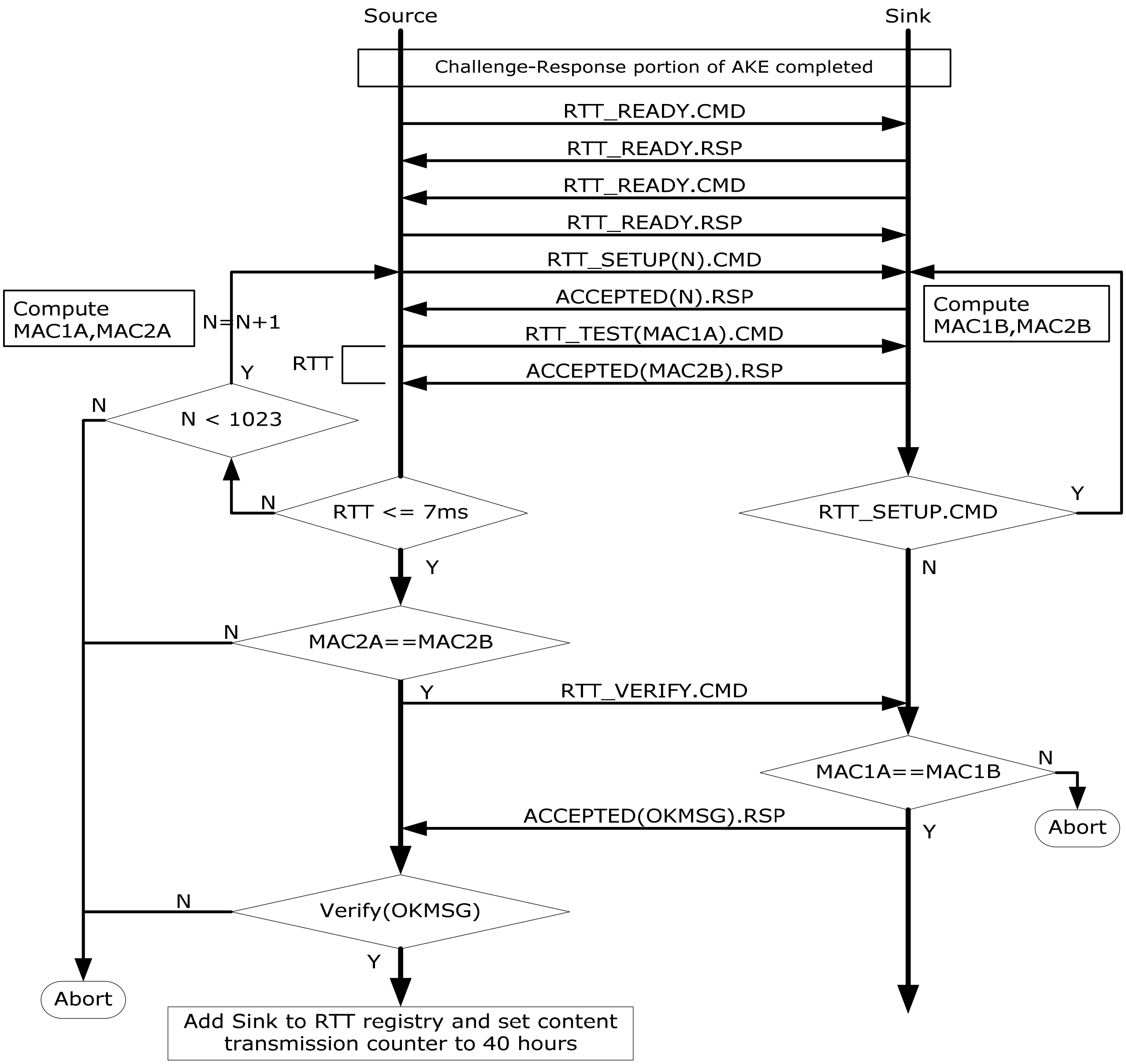

Figure 1 RTT Protocol Diagram

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 7 milliseconds 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 7 milliseconds:

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.

V1SF.3.2 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 7 milliseconds 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.

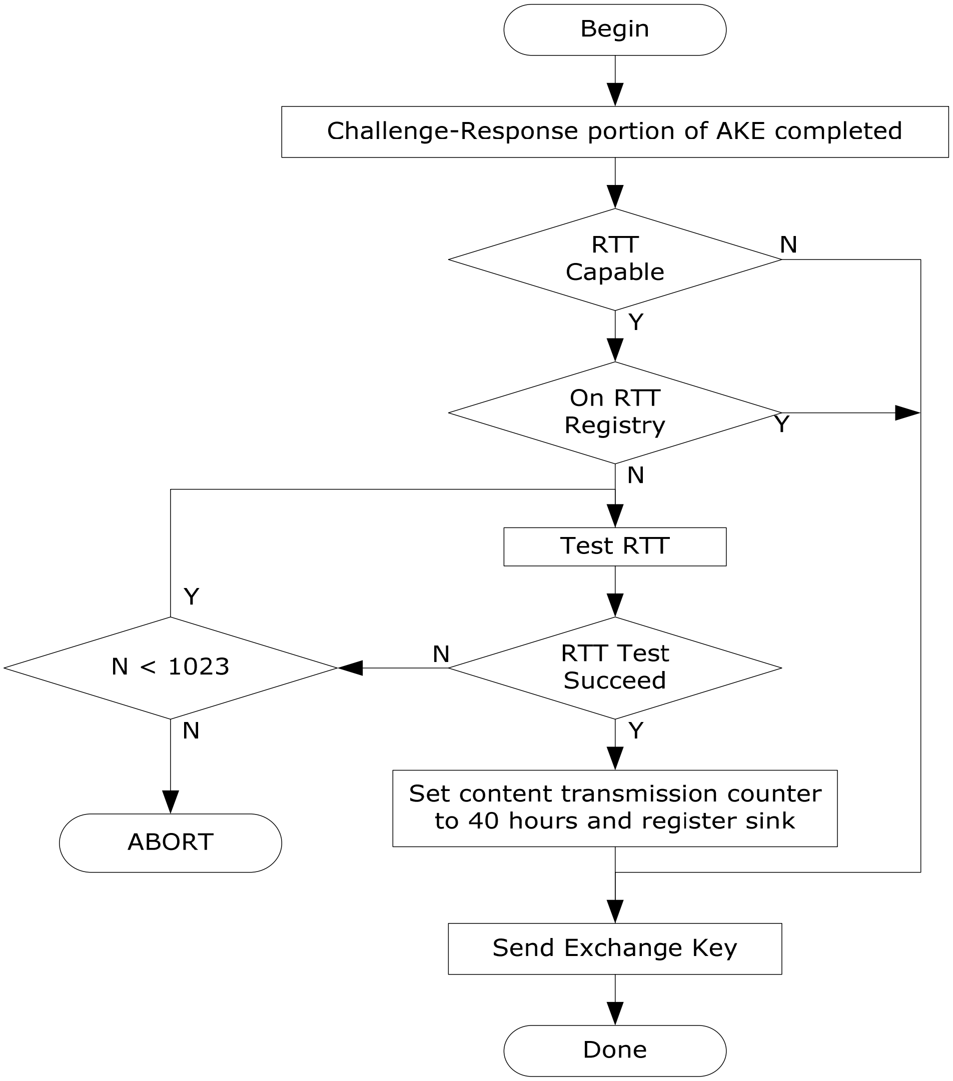
Begin
Challenge-Response portion of AKE completed
RTT Capable
N
Y
On RTT Registry
Y
N
Test RTT
Y
N < 1023
N
RTT Test Succeed
N
Y
Set content transmission counter to 40 hours and register sink
ABORT
Send Exchange Key
Done

Figure 2 AKE-RTT Informative Flow Diagrams

V1SF.3.3 Background RTT Check

The Background RTT check procedure permits either the source or sink device to initiate an RTT background check which is only used to add sink device to source device's RTT registry if not on RTT registry or if already on the source device's RTT registry set the count transmission counter to 40 hours. In case of Background RTT check source devices shall not transmit an exchange key.

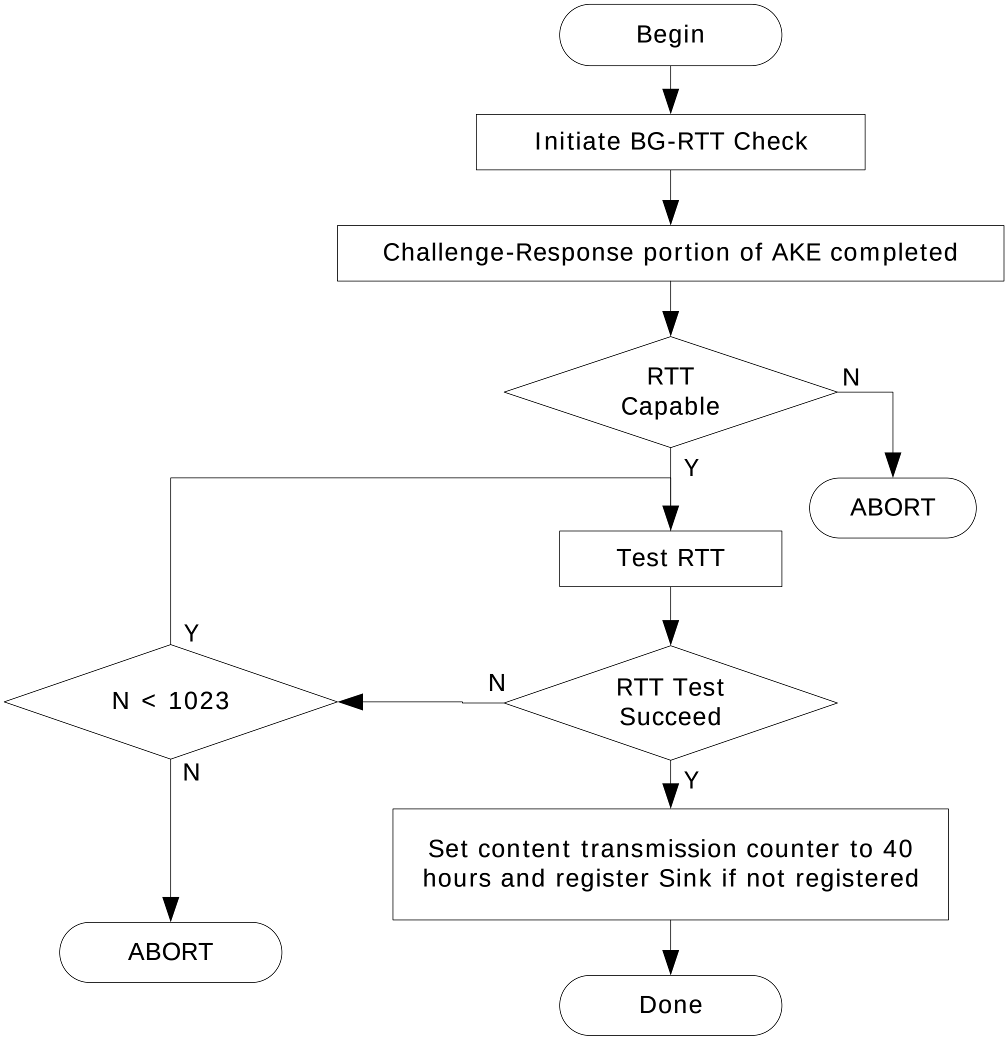
Begin
Initiate BG-RTT Check
Challenge-Response portion of AKE completed
RTT Capable
N
ABORT
Y
Test RTT
Y
N < 1023
N
RTT Test Succeed
N
Y
Set content transmission counter to 40 hours and register Sink if not registered
ABORT
Done

Figure 3 Background RTT Check Informative Flow Diagram

V1SF.4 Additional Commands and Sequences

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