Digital Transmission Licensing Administrator

DTCP2 Volume 1 Supplement A
DTCP2-USB
(Informational Version)

Intel Corporation

Maxell, Ltd.

Panasonic Corporation

Sony Corporation

Toshiba Corporation

Verimatrix, Inc., Contributor

Revision 1.0

January 28, 2020

Preface

Notice

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 dtcp-services@dtcp.com.

Printing History:

2020-01-28	**DTCP2 Volume 1 Supplement A DTCP2-USB Revision 1.0 (Informational Version)**

TABLE OF CONTENTS

1 Introduction

This supplement describes the mapping of DTCP2 protocol onto Universal Serial Bus (USB). Latter referred as DTCP2-USB. This mapping to USB preserves all aspects of the DTCP2 protocol specified in [DTCP2], except those ones that are explicitly mentioned in this document. This supplement is intended to be read with the DTCP2 specification [DTCP2].

1.1 Related Documents

[USB2] USB 2.0 Specification
https://www.usb.org/document-library/usb-20-specification

[USBCS] Universal Serial Bus Device Class Definition for Content Security Devices
https://usb.org/sites/default/files/ContentSecurity_v2.0.pdf

[USBCSM2] USB Content Security Method 2 Digital Transmission Content Protection Implementation Specification
https://www.usb.org/sites/default/files/csm2_v1_0.pdf

[DTCP2] Digital Transmission Content Protection 2 (DTCP2) Specification Volume 1

1.2 Additional Terms and Abbreviations

CS	Content Security
CSM	Content Security Method
CSNS	Content Security Notification Service
USB Host	The host computer system where the USB Host Controller is installed. This includes the host hardware platform (CPU, bus, etc.) and the operating system in use. [USB2]
USB Device	A physical entity that can be attached in the Universal Serial Bus to the USB Host and performs a function.
USB Reset	After receiving a reset, USB Device is addressable at the default address, is not configured and is not initially suspended. See 7.1.7.5 Reset Signaling at [USB2]
USB Device Address	A seven-bit value representing the address of a device on the USB. Devices are assigned a unique device address by the USB System Software.
USB Default Address	An address defined by the USB Specification and used by a USB Device when it is first powered or reset. The default address is 00H.
DTCP2-IP	DTCP2 mapping over IP as defined in [DTCP2]

2 Modifications to DTCP2 Specification

This specification does not introduce any changes or additions to the datagram formats or message exchange flows specified in [DTCP2] for DTCP2-IP.

2.1 Modifications to Chapter 4.4 (Protocol Flow)

In DTCP2-USB USB Host always initiates the authentication protocol. When a USB Host acts as a source device, the USB Host initiates the AKE by using the TRIGGER subfunction defined below, and the following protocol flow remains the same.

2.2 Modifications to Chapter 4.6 (Localization)

Devices conforming DTCP2-USB shall not support Remote Access AKE (RA-AKE). Thus, when operating over USB localization is always mandatory.

The Internet protocol time to live (TTL) requirement is not applicable for DTCP2-USB. Hence, this requirement is not applicable for DTCP2-USB.

Wireless LAN Security Requirements are not applicable for DTCP2-USB. Hence, this requirement is not applicable for DTCP2-USB.

2.3 Modifications to Chapter 5 (Key and Content Management)

Since, DTCP2-USB Devices shall not support remote access all references to K_R can be ignored.

DTCP2-USB Devices, both sources and sinks, shall expire all Exchange Keys when they detect themselves being detached from the physical USB interface or when they receive USB Reset from the USB Host. A USB Host shall expire all keys associated with a specific USB Device when it detects that this specific device has been detached from the physical USB interface or if the USB Host sends a USB Reset to this specific USB Device.

In DTCP2-USB, generation and sharing of N_C and ID_s values follows the same principles as defined in DTCP2-IP for RTP and HTTP transfers. When a Multicast Exchange Key is negotiated, source device generates both N_C and ID_s using RNG. When a Session Exchange key is negotiated, source generates only N_C and the sink generates ID_s using RNG. Source and sink share these values using CONTENT_KEY_REQ that is initiated by the sink device after EXCHANGE_KEY.

If more than 512 MB of content is transferred over a USB endpoint, source devices shall update N_C by incrementing the value by 1 mod 2^{64} every 512 MB or at the end of each PCP in which 512 MB boundary is included.

2.4 Modifications to Chapter 6 (Standard Functionality)

DTCP2-USB Devices, both sources and sinks, shall expire K_{XM} when they detect themselves being detached from the physical USB interface or when they receive USB Reset from the USB Host. A USB Host shall expire all keys associated with a specific USB Device when it detects that this specific device has been detached from the physical USB interface or if the USB Host sends a USB Reset to this specific USB Device.

Remote Access AKE (RA-AKE) shall not be supported over USB. A sink device shall not try to do RA-AKE over USB interface. If a source device receives an RA-AKE request over USB it shall response with NOT_IMPLEMENTED.

2.5 Modifications to Chapter 7 (AKE Command Set)

Because Remote Access shall not be supported in DTCP2-USB, all reference to remote access key K_R shall be ignored. Also, RA_REGISTER and RA_MANAGEMENT subfunctions shall be ignored.

A DTCP2-USB implementation shall always return NOT_IMPLEMENTED if it receives a valid DTCP2 request that is prohibited or not supported in DTCP2-USB.

If a DTCP2-USB Device is detached from the physical USB, or is sent a USB Reset during authentication, both source and sink shall immediately abort such authentication.

DTCP2-USB Hosts or devices shall not support remote sink registration or RA-AKE.

2.5.1 TRIGGER subfunction ($F1_{16}$) [Source → Sink]

This subfunction is used by DTCP2 USB Hosts to prompt a DTCP2 USB Device to issue a CHALLENGE or a MV_INITIATE subfunction as a sink device. This subfunction supports maintaining the same protocol flow in DTCP2 USB specification. This subfunction shall not be used when a DTCP2 USB Host acts as a sink device.

The value of AKE_procedure field is zero for this subfunction.

The exchange key field in Control[4] indicates which AKE should be initiated by the DTCP2 USB Device.

The subfunction_dependent field is reserved for future extension and shall be zero.

Both command and response packets of TRIGGER subfunction has no AKE_info field.

3 General Restrictions for DTCP2-USB

If a DTCP2 USB Host source function transmits the same DTCP2 encrypted content to multiple DTCP2 sink functions, each having different USB Device Addresses for the purpose of streaming, a Multicast Exchange Key may be used. Otherwise, a Session Exchange Key shall be used.

If a device has plural DTCP2 sink functions and receives encrypted content concurrently, such sink functions shall run AKE processing through different USB addresses.

No DTCP2 traffic shall ever be sent to the USB Default Address 00H.

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. When implementing DTCP2-USB, it is recommended that the implementation follows [USBCS] and [USBCSM2] with modifications stated below.

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 [USBCS]
- Universal Serial Bus Content Security Method 2 USB Digital Transmission Content Protection Implementation Specification [USBCSM2].
- Chapters 5, 8, and 9 of the Universal Serial Bus Specification Version 2.0 [USB2]

The DTCP2-USB Implementation has similar device states as described in [DTCP2]

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 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 USB 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 USB Host will begin a USB Host initiated DTCP authentication procedure.

CSNS permits USB DTCP compliant devices to initiate DTCP protocols by prompting the USB 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 USB 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.

The implementer of this specification should follow specifications [USBCS] and [USBCSM2], with following modifications to [USBCSM2]:

- bcdVersion defined in 2.3.4 Content Security Method Descriptor would be 0x0200 and
- bString value defined in 2 USB DTCP PROTOCOLS.3.4.1 CSM-2 String Descriptor would be Digital Transmission Content Protection Version 2.00
- Sections 3 DTCP AKE Packet Formats and 4 CSM-2 Protected Content Header are ignored and datagram formats defined in DTCP2-IP are used instead.