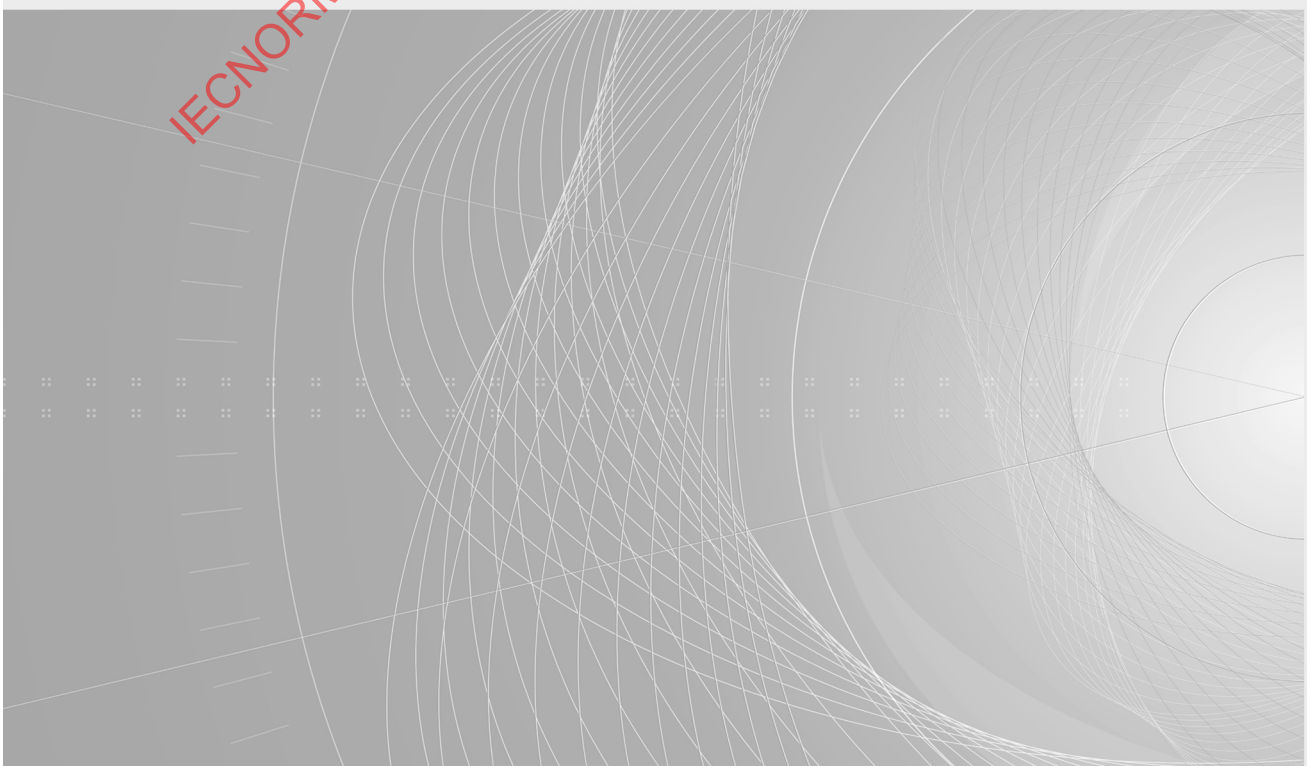
IEC 62481-3

Edition 3.0 2017-07

INTERNATIONAL STANDARD

colour inside

Digital living network alliance (DLNA) home networked device interoperability guidelines –
Part 3: Link protection



IEC 62481-3:2017-07(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC 62481-3

Edition 3.0 2017-07

INTERNATIONAL STANDARD

Digital living network alliance (DLNA) home networked device interoperability guidelines –
Part 3: Link protection

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.160; 35.100.05; 35.110

ISBN 978-2-8322-4541-5

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

DIGITAL LIVING NETWORK ALLIANCE (DLNA) HOME NETWORKED DEVICE INTEROPERABILITY GUIDELINES –

Part 3: Link protection

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62481-3 has been prepared under technical area 8: Multimedia home systems and applications for end-user network, of IEC technical committee 100: Audio, video and multimedia systems and equipment.

This third edition cancels and replaces the second edition published in 2013. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) editorial updates;

b) clarification for some of the guidelines that were ambiguous.

The text of this International Standard is based on the following documents:

CDV	Report on voting
100/2732/CDV	100/2882/RVC

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of IEC 62481 series, published under the general title *Digital Living Network Alliance (DLNA) home networked device interoperability guidelines,* can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Consumers are acquiring, viewing, and managing an increasing amount of digital media (photos, music, and video) on devices in the consumer electronics (CE), mobile, and personal computer (PC) domains. As such, they want to conveniently enjoy the content, regardless of the source, across different devices and locations in the home. The digital home vision integrates the Internet, mobile, and broadcast networks through a seamless, interoperable network, which will provide a unique opportunity for manufacturers and consumers alike. In order to achieve this interoperability, a common set of industry design guidelines is needed that allows vendors to participate in a growing marketplace, leading to more innovation, simplicity, and value for consumers. This document serves that purpose and provides vendors with the information needed to build interoperable networked platforms and devices for the digital home.

DIGITAL LIVING NETWORK ALLIANCE (DLNA) HOME NETWORKED DEVICE INTEROPERABILITY GUIDELINES –

Part 3: Link protection

1 Scope

This part of IEC 62481, the DLNA guidelines, specifies the DLNA Link Protection guidelines, which are an extension of the DLNA guidelines. DLNA Link Protection is defined as the protection of a content stream between two devices on a DLNA network from illegitimate observation or interception using the protocols defined within this part of DLNA guidelines.

Content protection is an important mechanism for ensuring that commercial content is protected from piracy and illegitimate redistribution. Link Protection is a technique that enables distribution of protected commercial content on a home network, thus resulting in greater consumer flexibility while still preserving the rights of copyright holders and content providers.

The guidelines in this part of DLNA guidelines reference existing technologies for Link Protection and provide mechanisms for interoperability between different implementations as well as integration with the DLNA architecture.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62481-1-1:2017, *Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 1-1: Architecture and protocols*

IEC 62481-2:2017, *Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 2: DLNA media formats*

ISO/IEC 13818-1, *Information technology – Generic coding of moving pictures and associated audio information: Systems*

ISO/IEC 29341-3-10, *Information technology – UPnP Device Architecture – Part 3-10: Audio Video Device Control Protocol – Audio Video Transport Service*

ISO/IEC 29341-3-11, *Information technology – UPnP Device Architecture – Part 3-11: Audio Video Device Control Protocol – Connection Manager Service*

IETF RFC 1191, Path MTU Discovery, J. Mogul, DECWRL, S. Deering, Stanford University
http://www.ietf.org/rfc/rfc1191.txt

IETF RFC 2045, Multipurpose Internet Mail Extensions (MIME) Part One

IETF RFC 2327, SDP: Session Description Protocol, M. Handley, V. Jacobson, ISI/LBNL
https://www.ietf.org/rfc/rfc2327.txt

IETF RFC 2616, Hypertext Transfer Protocol – HTTP/1.1, R. Fielding, UC Irvine, J. Gettys, Compaq/W3C, J. Mogul, Compaq, H. Frystyk, W3C/MIT, L. Masinter, Xerox, P. Leach, Microsoft*, T. Berners-Lee
http://www.ietf.org/rfc/rfc2616.txt?number=2616

IETF RFC 3550, RTP: A Transport Protocol for Real-Time Applications, H. Schulzrinne, Columbia University, S. Casner, Packet Design, R. Frederick, Blue Coat Systems Inc., V. Jacobson, Packet Design
http://www.ietf.org/rfc/rfc3550.txt

IETF RFC 3551, RTP Profile for Audio and Video Conferences with Minimal Control, H. Schulzrinne, Columbia University, S. Casner, Packet Design
http://www.ietf.org/rfc/rfc3551.txt

IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, T. Berners-Lee, R. Fielding, L. Masinter, January 2005
http://www.ietf.org/rfc/rfc3986.txt

DTCP Volume 1 (informational version), Digital Transmission Content Protection Specification Volume1
http://www.dtcp.com/specifications.aspx

DTCP Volume 1 Supplement E (informational version), DTCP Volume 1 Supplement E Mapping DTCP to IP
http://www.dtcp.com/specifications.aspx

DTCP Audio Compliance Rules EXHIBIT B-2, Compliance rules for licensed products that receive or transmit commercial audio works
http://www.dtcp.com/agreements.aspx

DTCP Adopter Agreement, DTCP Adopter Agreement, Digital Transmission Protection License Agreement, DTLA Digital Transmission Licensing Administrator
http://www.dtcp.com/

IEEE 802.1Q, IEEE standard for information technology – Telecommunications and information exchange between systems – IEEE standard for local and metropolitan area networks – Common specifications – Virtual Bridged Local Area Networks

IEEE 802.11, IEEE standard for information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks-specific requirements – Part 11: Wireless LAN Medium, Access Control (MAC) and Physical Layer (PHY) specifications

WMDRM-ND, Windows Media DRM for Network Devices, Windows Media Technologies
http://wmlicense.smdisp.net/licenserequest/default.asp

RTP Payload format for WMV and WMA, RTP Payload Format for Windows Media Audio and Video, Microsoft Corporation
http://download.microsoft.com/download/5/5/a/55a7b886-b742-4613-8ea8-d8b8b5c27bbc/RTPPayloadFormat_for_WMAandWMV_v1.doc

3 Terms, definitions, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
AKE
Authentication and Key Exchange
step in a Link Protection System where the receiving device is authenticated and given the correct keys for the content

3.1.2
ASF
Advanced System Format
media format encapsulation for the transmission of content

3.1.3
AV
Audio with Video
media content that contains both moving pictures and sound

3.1.4
AVT
Audio Video Transport
UPnP service that provides network-based control for common transport operations such as play, stop, pause, next, previous, and seek

Note 1 to entry: The AVTransport service specification is a standard UPnP DCP.

3.1.5
Cleartext
unencrypted content

Note 1 to entry: Within this standard, the content stream after decryption by the upstream content protection system and before encryption by the Link Protection System.

3.1.6
Cleartext Byte Domain
specification of a byte position in the Cleartext content stream

Note 1 to entry: For a complete explanation of seek operations on link protected content, see Annex A.

3.1.7
Cleartext Byte Seek Request Header
request that a certain position in the Cleartext byte stream be returned

Note 1 to entry: This term is used to signify any of these different transport layer request headers.

Note 2 to entry: When used in a guideline, Cleartext Byte Seek Request Header implies that the guideline applies to all uses of any of the request headers.

3.1.8
Cleartext Byte Seek Response Header
response that declares the range of bytes returned in the Cleartext byte stream

Note 1 to entry: This term is used to signify any of these different transport layer response headers.

Note 2 to entry: When used in a guideline, this implies that the guideline applies to all uses of any of the request headers.

3.1.9
comply
conform
be in accordance with referenced requirements; where the reference includes both mandatory and optional requirements, only the mandatory elements are considered necessary for compliance

Note 1 to entry: Optional requirements continue to be optional. Any variation from these expectations shall be specifically noted.

Note 2 to entry: "Comply with" can be used interchangeably with "conform to" (includes the variations of complies, complying, compliance, compliant; conforms, conforming, conformance, conformant).

3.1.10
CMS
ConnectionManager:1 Service
UPnP service that provides information about the supported transport protocols and media formats of a UPnP device

Note 1 to entry: The CMS specification is a standard UPnP DCP.

3.1.11
CSRC
Contributing SouRCe
source used for the RTP Media Transport

3.1.12
Decoder Friendly Alignment Position
position in the bitstream defined for decoder friendly alignment

Note 1 to entry: A Decoder Friendly Alignment Position is always the start of a Media Format Alignment Element. Generally, the decoder can begin to process data without any other internal state information about the stream. The decoder can begin processing at that point and create a valid output rendering. This value is defined for the individual media format profiles that have Decoder Friendly Alignment Positions.

3.1.13
DLNA
Digital Living Network Alliance
organization that created this series of documents, the DNLA guidelines

3.1.14
DLNA Link Protection
protection, using DLNA protocol elements as defined in these guidelines, of a content stream between two devices on a DLNA network from illegitimate observation or interception

3.1.15
DLNAQOS_UP
DLNA QoS User Priority
DLNA-defined QoS label used to correlate an underlying IEEE 802.1Q user priority and WMM access category to a DLNA traffic type(s)

3.1.16
DTCP
Digital Transmission Content Protection
Link Protection System

3.1.17
DTCP-IP
Digital Transmission Content Protection over IP networks
DTCP as applied to IP based networks

3.1.18
GOP
Group Of Pictures
defined grouping of information in the MPEG 2 media format

3.1.19
HTTP
Hyper Text Transfer Protocol
protocol for transferring files across the Internet

Note 1 to entry: Requires an HTTP client program on one end, and an HTTP server program on the other end.

3.1.20
Link Protection
protection of a content stream between two devices on a DLNA network from illegitimate observation or interception

3.1.21
Link Protection Alignment Element
unit of content carried within a link-protected content stream

Note 1 to entry: This typically starts with a packet header that is defined by the Link Protection System and contains bytes of the link-protected stream.

3.1.22
Link Protection System
specific collection of technologies with corresponding rules that enable secure content transfer between two endpoints

3.1.23
Media Format Alignment Element
unit of content carried within an unprotected content stream

Note 1 to entry: This typically starts at a Decoder Friendly Alignment Position for the given media format and contains an integral number of units of content as defined by the media format in use. This value is defined within the media format profile specification.

3.1.24
MIME
Multipurpose Internet Mail Extension
standard system for identifying the type of data contained in a file

Note 1 to entry: MIME is an internet protocol that allows sending binary files across the internet as attachments to e-mail messages. This includes graphics, photos, sound, video files, and formatted text documents.

3.1.25
Network Byte Domain
specification of a byte position in the content stream as it is carried on the network transport

Note 1 to entry: For content binaries that use a Link Protection System, this will include encryption and any headers or padding necessary for the Link Protection System.

3.1.26
PCP
Protected Content Packet
packet format for DTCP-IP link protected content as defined in DTCP Volume 1 and DTCP Volume 1 Supplement E

3.1.27
PS
Program Stream
MPEG-2 AV stream format

3.1.28
RTP
Real Time Protocol
media transport that provides end-to-end network transport functions for transmitting real-time data, such as AV

Note 1 to entry: RTP provides services such as payload type identification, sequence numbering, time-stamping, and delivery monitoring.

3.1.29
RTSP
Real Time Streaming Protocol
protocol within the RTP protocol suite

3.1.30
RTT
Round Trip Time
time between sending a network packet to a remote host and the time that the response is received

3.1.31
SDP
Session Description Protocol
protocol within the RTP protocol suite

3.1.32
SOAP
Simple Object Access Protocol
XML based messaging protocol used to exchange service requests and responses over a network

3.1.33
Time Domain
specification of a position in the content stream in time units

3.1.34
TS
Transport Stream
MPEG-2 AV stream format

3.1.35
UCDAM
Uniform Client Data Availability Model
model for representing which bytes of a content binary are available on a server for seek operations

Note 1 to entry: See clause 10 of IEC 62481-1-1:2017 for a full definition.

3.1.36
UPnP
architecture for pervasive peer-to-peer network connectivity of devices of all form factors

Note 1 to entry: UPnP is designed to bring easy-to-use, flexible, standards-based connectivity to ad-hoc or unmanaged networks whether in the home, in a small business, public spaces, or attached to the Internet.

Note 2 to entry: UPnP is a distributed, open networking architecture that leverages TCP/IP and Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and public spaces.

3.1.37
URI
Uniform Resource Identifier
W3C's codification of the name and address syntax of present and future objects on the internet

Note 1 to entry: In its most basic form, a URI consists of a scheme name (such as file, http, ftp, news, mailto, gopher) followed by a colon, followed by a path whose nature is determined by the scheme that precedes it. URI is the umbrella term for URNs, URLs, and all other Uniform Resource Identifiers.

3.1.38
VOBU
Video OBject Unit
grouping of information in the MPEG 2 media format

3.1.39
WEP
Wired Equivalency Privacy
wireless privacy standard used in conjunction with IEEE 802.11 networks

3.1.40
WMA
Windows Media Audio
audio compression binary format

3.1.41
WMDRM-ND
Windows Media DRM for Network Devices
Link Protection System

3.1.42
WMV
Windows Media Video
AV compression binary format

3.1.43
WPA
WiFi Protected Access
system to secure a wireless IEEE 802.11 network

3.1.44
WPA2
WiFi Protected Access version 2
system to secure a wireless IEEE 802.11 network

3.2 Abbreviated terms

MPEG-2	Moving Picture Experts Group phase 2

3.3 Conventions

In IEC 62481-1-1:2017 and this document, a number of terms, conditions, mechanisms, sequences, parameters, events, states, or similar terms are printed with the first letter of each word in uppercase and the rest in lowercase (e.g., Move). Any lowercase uses of these words have the normal technical English meaning.

4 DLNA home network architecture

See Clause 4 of IEC 62481-1-1:2017 for detailed descriptions of the DLNA home network architecture.

5 DLNA device model

See Clause 5 of IEC 62481-1-1:2017 for detailed descriptions of the DLNA device model. This document extends the existing DLNA devices and system usages to include link-protected content used for the following:

- 2-box Pull system usage;
- 2-box Push system usage;
- 3-box system usage,

for transfer and rendering of content items. These are the only system usages that are currently in scope for the use of DLNA Link Protection.

6 Guideline terminology and conventions

See Clause 6 of IEC 62481-1-1:2017 for a full description of the DLNA document conventions.

7 Common Link Protection guidelines

7.1 General

See 7.1 of IEC 62481-1-1:2017 for guideline and attribute table layout descriptions.

7.2 Conditions for measuring time in message exchanges

These guidelines define in certain cases time constraints for the exchange of messages between two communicating endpoints. These time constraints have been defined as a means to provide some operational consistency between the two communicating endpoints. However, in best-effort networks, actual time measurements for exchanging messages show wide variations depending on perturbations derived from network conditions, traffic, available bandwidth, and others. Therefore, the following recommendations should be applied when making time measurements.

- The two communicating endpoints should establish communications under Ideal Network Conditions.
- Time measurements at a given layer assume that the underlying layers preserve the communication channel. For example, time measurements at the HTTP layer cannot be valid if the underlying TCP/IP channel breaks during the measurements.
- Unless specified otherwise, time measurements assume that the communicating devices are both in active mode. This means that time measurements should not include transitions from sleep mode to active mode.

7.3 Networking and connectivity

For DTCP-IP specific requirements, see 8.2. For WMDRM-ND specific requirements, see 9.3.

7.4 Device discovery and control

For detailed information, see Clause 9 of IEC 62481-1-1:2017. For DTCP-IP specific guidelines, see 8.4. For WMDRM-ND specific guidelines, see 9.4.

7.5 Media management

7.5.1 General

This subclause covers the guidelines for implementing media management using the UPnP AV architecture with DLNA Link Protection. For detailed subclause information see Clause 10 of

IEC 62481-1-1:2017. For DTCP-IP specific guidelines, see 8.5. For WMDRM-ND specific guidelines, see 9.5.

Many of the guidelines for 7.5 as well as 7.6 have to do with the structures necessary to perform seek operations over the link protected content. IEC 62481-1-1:2017 defines two models of seek operations: the Full Data Seek Availability model and the Limited Data Seek Availability model. These two models continue to operate for content using DLNA Link Protection. However, for this content, we introduce the concept of the Network Byte Domain (the protected content stream as it flows over the network) and the Cleartext Byte Domain (representing positions within the content before encryption by the Link Protection System). This allows the Content Receiver to seek to byte positions in the content as if no Link Protection had been applied. For content binaries using DLNA Link Protection, if the Content Receiver performs a byte seek operation in the Cleartext Byte Domain, it can issue requests for the same byte positions that it would if the content were sent without any Link Protection. The Content Receiver does not need to convert between positions in the Cleartext and positions in the encrypted content. For a detailed explanation of seeking and link protected content, see Annex A.

Table 1 and Table 2 summarize the structures used for each of the domains and seek models. Table 3 contains the media management guidelines for devices using DLNA Link Protection.

Table 1 – Summary of Domain Elements for Full Random Access Data Availability model

Function	Time Domain	Network Byte Domain	Cleartext Byte Domain
Domain and model support	op-param a-val	op-param b-val	flags-param Bit 15: CleartextByteSeek-full
SDP indication of domain support	Range	Domain Not Available	Domain Not Available
File size	res@duration	res@size	res@dlna:cleartextSize
HTTP request header to execute Seek operation	TimeSeekRange.dlna.org	Range	Cleartext Byte Seek Request Header DTCP-IP: Range.dtcp.com WMDRM-ND: Cleartext-Range.dlna.org
HTTP response header for Seek operation	TimeSeekRange.dlna.org	Content-Range	Cleartext Byte Seek Response Header DTCP-IP: Content-Range.dtcp.com WMDRM-ND: Cleartext-Content-Range.dlna.org
RTSP header to execute Seek operation	Range	Domain Not Available	Domain Not Available
HTTP message body size	Not defined	Content-Length	Content-Length HTTP message body size is always specified by the Content-Length response header

Table 2 – Summary of Domain Elements for Limited Random Access Data Availability model

Function	Time Domain	Network Byte Domain	Cleartext Byte Domain
Domain and model support	flags-param Bit 30: lop-npt	flags-param Bit 29: lop-bytes	flags-param Bit 14: lop-cleartextbytes
SDP indication of domain support	Range	Domain Not Available	Domain Not Available
HTTP request header to execute Seek operation	TimeSeekRange.dlna.org	Range	Cleartext Byte Seek Request Header DTCP-IP: Range.dtcp.com WMDRM-ND: Cleartext-Range.dlna.org
HTTP response header for Seek operation	TimeSeekRange.dlna.org	Content-Range	Cleartext Byte Seek Response Header DTCP-IP: Content-Range.dtcp.com WMDRM-ND: Cleartext-Content-Range.dlna.org
RTSP header to execute Seek operation	Range	Domain Not Available	Domain Not Available
HTTP header to request the available range		getAvailableSeekRange.dlna.org	
HTTP response header for available range	availableSeekRange.dlna.org (with npt-range)	availableSeekRange.dlna.org (with byte-range)	availableSeekRange.dlna.org (with mode-flag) Cleartext Byte Seek Response Header DTCP-IP: Content-Range.dtcp.com WMDRM-ND: Cleartext-Content-Range.dlna.org
RTSP header to request the available range	DESCRIBE	Domain Not Available	Domain Not Available
RTSP header for specifying the available range	Available-Range.dlna.org	Domain Not Available	Domain Not Available
s_0 is increasing		flags-param Bit 27: s_0-increasing	
s_N is increasing		flags-param Bit 26: s_N-increasing	

See A.6 for an explanation of the various seek domains for link protected content.

7.5.2 Updates to existing general AV Media Management guidelines

7.5.2.1 Affected guidelines in IEC 62481-1-1:2017

Table 3 – AV Media Management guideline changes

Guideline updated	Location in IEC 62481-1-1:2017
MM flags-param (Flags Parameter)	10.1.3.24.2 (GUN 3WJUU)
MM lop-npt, lop-bytes, and lop-cleartextbytes (Limited Operations Flags): Common	10.1.3.29.1(GUN OTHY2)
MM lop-npt lop-bytes, and lop-cleartextbytes (Limited Operations Flags): HTTP	10.1.3.30 (GUN WJUUP)
MM lop-npt, lop-bytes, and lop-cleartextbytes (Limited Operations Flags): RTP	10.1.3.31 (GUN UX6UW)
MM IFO File	10.1.4.9.1 (GUN VDY7V) 10.1.4.9.2 (GUN 4VF4V) 10.1.4.9.4 (GUN V6GS6) 10.1.4.9.6 (GUN 23HQ6) 10.1.4.9.7 (GUN ZQRDX)

7.5.2.2 MM IFO file

7.5.2.2.1

[GUIDELINE] If an IFO file is provided by the UPnP AV MediaServer or Push Controller for any content binary which corresponds to a media format profile using DLNA Link Protection then the IFO shall not be encrypted or encapsulated by the Link Protection System used for the content binary.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	n/a	VHRUV	

[**COMMENT**] IFO file needs to be made available as Cleartext.

7.5.2.2.2

[GUIDELINE] If an IFO file is provided by the UPnP AV MediaServer or Push Controller for any content binary which corresponds to a media format profile using DLNA Link Protection the byte data and time data in the IFO file shall refer to the byte position and time position within the unprotected content stream.

[**ATTRIBUTES**]

M	A	DMS +PU+	M-DMS	n/a	n/a	KWDR4	

[**COMMENT**] Byte positions are given with respect to the unprotected content stream and not a byte position within the protected content stream.

7.5.3 New general AV Media Management guidelines

7.5.3.1 MM Media Class of link protected content

[GUIDELINE] A content object that represents a link protected form of one of the DLNA media classes shall use the media class value of the unprotected content.

[**ATTRIBUTES**]

M	R	DMS	M-DMS	n/a	IEC 62481-2:2017	WTLQ8	

[**COMMENT**] For example, use object.item.videoItem or a derived class for the upnp:class value of link protected content that, in its unprotected form conforms to the DLNA "AV" media class.

7.5.3.2 MM DIDL-Lite byte metadata properties

[GUIDELINE] For resources that specify a content binary that uses DLNA Link Protection all metadata with byte units shall refer to the Network Byte Domain (i.e. link protected content as it is transmitted between the serving and rendering endpoints), unless specified by the definition of the metadata item, to refer to the Cleartext Byte Domain.

[ATTRIBUTES]

M	A	DMS	M-DMS	n/a	IEC 62481-1-1: 2017	O67G8	

[COMMENT] The length of the protected content stream can be longer due to encryption additional headers for packetization and any necessary padding.

7.5.3.3 MM CP: res@dlna:cleartextSize

7.5.3.3.1

[GUIDELINE] A UPnP AV MediaServer should additionally provide non-empty and non-whitespace values for metadata properties as shown in Table 4 for <res> elements that describe content binaries which use a Link Protection System.

Table 4 – Recommended metadata properties

upnp:class value	Property names
object.item.audioItem	res@dlna:cleartextSize
object.item.imageItem	res@dlna:cleartextSize
object.item.videoItem	res@dlna:cleartextSize

[ATTRIBUTES]

S	A	DMS	M-DMS	n/a	IEC 62481-1-1: 2017	DR47I	

[COMMENT] This guideline helps resolve dependency issues that Rendering Endpoints have, on knowing the size in bytes of the unprotected content stream.

7.5.3.3.2

[GUIDELINE] If flags-param bit 15 equals 1 and sN-increasing flag is false, then the Content Source shall provide content length information in the res@dlna:cleartextSize value of the <res> element.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IEC 62481-1-1: 2017	OFRD2	

7.5.3.3.3

[GUIDELINE] If the UPnP AV MediaServer specifies the res@dlna:cleartextSize value of the content binary it shall be the size in bytes of the unprotected content binary before any Link Protection headers padding or encryption have been added, see Table 5.

Table 5 – Property type and multi value

Property name	Property type	Multiple value
res@dlna:cleartextSize	unsigned long	No

The prefix for res@dlna:cleartextSize shall be "dlna" and the namespace shall be "urn:schemas-dlna-org:metadata-1-0/".

[ATTRIBUTES]

M	A	DMS	M-DMS	n/a	n/a	VWWTL	

7.5.3.4 MM CP: DIDL-Lite protocolInfo value

[GUIDELINE] A UPnP AV MediaServer may contain resources that specify encrypted content binaries if the format profile so specifies.

[ATTRIBUTES]

O	A	DMS	M-DMS	n/a	IEC 62481-1-1: 2017	KJVW4	

[COMMENT] Refer to IEC 62481-1-1:2017, 10.1.3.16.5 (GUN NKQ9V), which prohibits transport layer encryption unless the media format profile explicitly states it is required. This guideline clarifies that some media format profiles might use Link Protection and are hence encrypted. The Link Protection System is specified within the media format profile of the content.

7.5.3.5 MM CP: LP-flag (Link Protection flag)

7.5.3.5.1

[GUIDELINE] If the content binary described by the protocolInfo uses DLNA Link Protection when it is transmitted then the LP-flag shall be true.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	n/a	P8F3M	

[COMMENT] The specifics of the Link Protection System used and parameters for setting up the connection can be found in the MIME type or other protocolInfo parameters.

7.5.3.5.2

[GUIDELINE] If the content binary described by the protocolInfo does not use DLNA Link Protection when it is transmitted then the LP-flag shall be false.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	n/a	WWTLQ	

7.5.3.6 MM CP: cleartextbyteseek-full

7.5.3.6.1

[GENERAL] Byte based full seek data availability with the Cleartext Byte Seek Request Header

7.5.3.6.2

[GUIDELINE] If a content binary uses a Link Protection System over the HTTP media transport protocol the meaning of the cleartextbyteseek-full flag shall be as follows: True = the content source supports the Cleartext Byte Seek Request Header under the Full Random Access data availability model; False = the content source does not support the Cleartext Byte Seek Request Header under the Full Random Access data availability model. The guidelines of the Full Random Access data availability model for link protected content are defined in 7.6.3.2.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	n/a	TLQ89	

[COMMENT] The Cleartext Byte Seek Request Header can be different depending on the Link Protection System used. For the general header guideline, see 7.6.6.3, for the DTCP-IP Link Protection System, see 8.6.1.2 for the WMDRM-ND Link Protection System, see 9.6.1.7 for the definition of this header. The Cleartext Byte Seek Request Header allows an endpoint to specify a byte range in the Cleartext Byte Domain to be returned by the server.

7.5.3.7 MM CP: lop-cleartextbytes flag

7.5.3.7.1

[GENERAL] Byte based limited seek data availability with Cleartext Byte Seek Request Header.

7.5.3.7.2

[GUIDELINE] If a content binary uses a Link Protection System over the HTTP media transport protocol the meaning of the lop-cleartextbytes flag shall be as follows True = The content source supports the Cleartext Byte Seek Request Header under the Limited Random Access data availability model. False = The content source does not support the Cleartext Byte Seek Request Header under the Full Limited data availability model. The guideline of the Limited Random Access data availability model for link protected content is defined by 7.6.3.3.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	n/a	RKJVW	

[COMMENT] The Cleartext Byte Seek Request Header can be different depending on the Link Protection System used. For the general header guideline, see 7.6.6.3, for the DTCP-IP Link Protection System, see 8.6.1.2, for the WMDRM-ND Link Protection System, see 9.6.1.7 for the

definition of this header. The Cleartext Byte Seek Request Header allows an endpoint to specify a byte range in the Cleartext Byte Domain to be returned by the server.

7.5.4 MediaRenderer device guidelines

7.5.4.1 MM CP: Link Protection state error

[GUIDELINE] The AVT:TransportStatus instance state variable should be set to ERROR_OCCURRED if the AVT:SetAVTransportURI method failed because of a device authentication failure, or because Link Protection restrictions (e.g. RTT) were not met between the content source and the content receiver.

[ATTRIBUTES]

S	A	DMR	n/a	n/a	ISO/IEC 29341-3-10	WDR47	

[COMMENT] UPnP MediaRenderers define new allowed values for the AVT.TransportStatus instance state variable to represent a Link Protection error condition.

7.5.4.2 MM CP: Link Protection human readable error message

7.5.4.2.1

[GUIDELINE] If the media connection to the content receiver (e.g. a UPnP AV MediaRenderer) fails with HTTP or RTSP error 403 (Forbidden) the content receiver should respond to a AVT:SetAVTransportURI AVT:Play AVT:Seek AVT:Previous or AVT:Next request with a UPnP AV error code 722 (Can't determine allowed uses).

[ATTRIBUTES]

S	A	DMR	n/a	n/a	ISO/IEC 29341-3-10	G8YKV	

7.5.4.2.2

[GUIDELINE] If the UPnP AV MediaRenderer knows the specific reason of the failure, it may use a localized human-readable error message in the errorDescriptiontag of the SOAP response indicating failure of device authentication or that Link Protection restrictions (e.g. RTT) were not met.

[ATTRIBUTES]

O	A	DMR	n/a	n/a	ISO/IEC 29341-3-10	JVW4I	

7.6 Media Transport

7.6.1 General

This subclause covers the guidelines for the Media Transport layer. For detailed information see Clause 11 of IEC 62481-1-1:2017. For DTCP-IP-specific guidelines, see 8.6. For WMDRM-ND-specific guidelines, see 9.6.

The following subclauses contain guidelines for the use of Media Transports in DLNA devices. The guidelines are organized into a table that covers those common among all Media Transports

and then subclauses/tables that cover guidelines for specific Media Transport protocols such as HTTP and others. For detailed information, see 11.4 of IEC 62481-1-1:2017.

Many of the guidelines in this subclause define the byte seek operations available on the content. See the 7.5.1 for a summary of the headers and flags used to represent the various byte domains and seek models.

7.6.2 Updates to existing general Media Transport guidelines

Table 6 specifies the updates to existing general Media Transport guidelines.

Table 6 – Updates to existing general Media Transport guidelines

Guideline updated	Location in IEC 62481-1-1:2017
MT normative random access data availability models	11.4.2.14.1 (GUN YPY8R)
MT "Full Random Access Data Availability" model	11.4,2.15.1 (GUN D7KPW) 11.4.2.15.2 (GUN 5VMHZ)
MT "Limited Random Access Data Availability" model	11.4.2.16.1 (GUN 7KPWX) 11.4.2.16.2 (GUN W5HZV) 11.4.2.16.3 (GUN KPWXV) 11.4.2.16.4 (GUN VMHZL)

7.6.3 New general Media Transport guidelines

7.6.3.1 MT CP: link protected content

[GUIDELINE] Any key exchange required to decode a link protected content binary shall follow the requirements of the Link Protection System in use.

[ATTRIBUTES]

M	R	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	n/a	7G8YK	

7.6.3.2 MT CP: Play ready

[GUIDELINE] Initiation of Link Protection specific setup operations should occur while browsing for content or upon invocation of AVT:SetAVTransportURI.

[Attributes]

S	A	DMP DMR	M-DMP	n/a	ISO/IEC 29341-3-11 ISO/IEC 29341-3-10	R6EOV	

[COMMENT] Link Protection setup operations (such as RTT testing and authentication of the endpoint and key exchange) can take considerable time. Wait times can be noticeably reduced by these operations as soon as possible, instead of waiting until the HTTP connection is established.

7.6.3.3 MT CP: metadata and transport headers for Link Protection

[GUIDELINE] For resources that specify a content binary that uses DLNA Link Protection, unless otherwise specified, all transport layer headers with byte units shall refer to the link protected content as it is transmitted between the serving and rendering endpoints (i.e. with encryption, Link Protection headers, and any necessary padding added).

[ATTRIBUTES]

M	C	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	n/a	VW4I6	

7.6.4 HTTP transport

There are many possible transport protocols that can be used for the transfer of content. The baseline mandatory Media Transport protocol for DLNA devices is HTTP. Subclauses 7.6.5 to 7.6.8 contain the guidelines that pertain to the HTTP transport and are sorted into those that are common to all HTTP transfers, guidelines specific to a Streaming Transfer, guidelines specific to an Interactive Transfer, and guidelines specific to a Background Transfer. For detailed information, see IEC 62481-1-1:2017, 11.4.3.

7.6.5 Updates to existing general HTTP Media Transport guidelines

7.6.5.1 Summary

Table 7 lists these updates.

Table 7 – Updates to existing general HTTP Media Transport guidelines

Guideline updated	Location in IEC 62481-1-1:2017
MT HTTP Header: contentFeatures.dlna.org	11.4.3.11.7 (GUN P7NKR)
MT HTTP Common Random Access Data Availability guidelines	11.4.3.18.1 (GUN J4YC9)
MT HTTP Data Range of "Full Random Access Data Availability"	11.4.3.19.2 (GUN 8A57U) 11.4.3.19.4 (GUN 368A5)
MT HTTP: Data Range of "Limited Random Access Data Availability"	11.4.3.20.1 (GUN OUBZ3) 11.4.3.20.2 (GUN KR8WA) 11.4.3.20.4 (GUN 868PW) 11.4.3.20.8 (GUN UBZ33) 11.4.3.20.9 (GUN NTSXZ) 11.4.3.20.11 (GUN 4NTSX) 11.4.3.20.12 (GUN TSXZZ) 11.4.3.20.16 (GUN 8DU64)
MT HTTP Header: RANGE (Server)	11.4.3.22.2 (GUN Z33H5) 11.4.3.22.3 (GUN 8WAAX)
MT HTTP Time-Based Seek (Server)	11.4.3.23.1 (GUN U8UZX)

7.6.5.2 MT HTTP common random access data availability guidelines

[GUIDELINE] If an HTTP Server Endpoint supports the Cleartext Byte Seek Request Header for the specified URI, it shall process any requested range in the random access data range at the same time.

[ATTRIBUTES]

M	C	DMS +PU+	M-DMS	n/a	n/a	8F3M2	

[COMMENT] This is a general requirement that random access requests to be supported on the entire [r_0, r_N] data range over the Cleartext Byte Domain.

7.6.5.3 MT HTTP data range of "Full Random Access Data Availability"

7.6.5.3.1

[GUIDELINE] The byte position of 0 for the Cleartext Byte Seek Request Header field shall refer to the beginning of the content binary.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	n/a	O4R8S	A

7.6.5.3.2

[GUIDELINE] If an HTTP Server Endpoint receives an HTTP GET request for a content binary which uses a Link Protection System and that omits all of the headers used for seek operations (i.e. the RANGE HTTP header, the Cleartext Byte Seek Request Header and the TimeSeekRange.dlna.org HTTP header), then the HTTP Server Endpoint shall infer a requested byte position of 0 (i.e. respond from the beginning of the content binary).

This guideline shall also apply when s_0-increasing is false and none of the above headers are supported by the HTTP server.

[ATTRIBUTES]

M	A	DMS	M-DMS	n/a	IETF RFC 2616	T5GV8	A

7.6.5.3.3

[GUIDELINE] For a content binary that uses a Link Protection System, if an HTTP Server Endpoint supports the Cleartext Byte Seek Request Header with the "Full Random Access Data Availability" model, the HTTP Server Endpoint should specify the byte length of the returned entity (in the Cleartext Byte Domain) via the instance-length included in the appropriate Cleartext Byte Seek Response Header of the Target Response to a HTTP GET/HEAD request with the Cleartext Byte Seek Request Header.

[ATTRIBUTES]

S	C	DMS +PU+	M-DMS	n/a	IETF RFC 2616	W4I6W	

[COMMENT] The Cleartext Byte Seek Request Header can be different depending on the Link Protection System used. For the general requirements of the header see guideline 7.6.10.2, for the DTCP-IP Link Protection System, see guideline 8.6.1.2, for the WMDRM-ND Link Protection System, see guideline 9.6.1.7 for the definition of this header.

Similarly, the Cleartext Byte Seek Response Header can also be different depending on the Link Protection System used. For the DTCP-IP Link Protection System, see guideline 8.6.1.3, for the WMDRM-ND Link Protection System, see guideline 9.6.1.8 for the definition of this header.

7.6.5.3.4

[GUIDELINE] For a content binary that uses a Link Protection System, if an HTTP Client Endpoint wants to get the instance-length of a content binary in the Cleartext Byte Domain, then it should use an HTTP HEAD request with the Cleartext Byte Seek Request Header that specifies 0 for the first-cleartextbyte-pos and omits the last-cleartextbyte-pos.

[ATTRIBUTES]

S	C	DMP DMR	M-DMP	n/a	IETF RFC 2616	47I2C	

[COMMENT] The response will include the Cleartext Byte Seek Response Header. If the instance length is known, then it will be the number of bytes in the UCDAM $[s_0, s_N]$ data range for the Cleartext Byte Domain. Otherwise, the instance-length token will be "*".

The Cleartext Byte Seek Request Header can be different depending on the Link Protection System used. For the general requirements of the header, see guideline 7.6.10.2, for the DTCP-IP Link Protection System, see guideline 8.6.1.2, for the WMDRM-ND Link Protection System, see guideline 9.6.1.7 for the definition of this header.

7.6.5.3.5

[GUIDELINE] For a content binary that uses a Link Protection System, if an HTTP Server Endpoint knows the instance-length of a content binary, then it shall provide the instance-length in the Cleartext Byte Seek Response Header.

This behaviour is required for scenarios where the HTTP Server is serving stored content.

[ATTRIBUTES]

M	A	DMS	M-DMS	n/a	IETF RFC 2616	R47I2	

7.6.5.4 MT HTTP: data range of "Limited Random Access Data Availability"

7.6.5.4.1

[GUIDELINE] If the HTTP request contains a getAvailableSeek.Range.dlna.org HTTP header, an HTTP Server Endpoint shall provide the currently-available cleartextbyte-range using the Cleartext Byte Seek Response Header in the HTTP Target Response when all of the following are true:

- the requested content binary uses a Link Protection System and supports the Cleartext Byte Seek Request;
- the requested content binary operates under the "Limited Random Access Data Availability" model;
- the HTTP request does not include a TimeSeekRange.dlna.org header or a Cleartext Byte Seek Request header.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	F3M2V	C

[COMMENT] Since the syntax of the availableSeekRange.dlna.org header does not accommodate a cleartextbyte-range, the available Cleartext byte range for link protected content is returned using the Cleartext Byte Seek Response Header. Two headers need to be returned in this case: the Cleartext Byte Seek Response Header to indicate the available bytes range within the Cleartext Byte Domain, and the availableSeekRange.dlna.org header to indicate the limited operation mode supported, the available time range, and/or the available network (non-Cleartext) byte domain range. See A.6 for an explanation of the various seek domains for link-protected content.

If either the TimeSeekRange.dlna.org or a Cleartext Byte Seek header is included in the content request for link protected content, the Cleartext Byte Seek Response Header cannot be used to indicate the available Cleartext domain range. For requests of this form, the Cleartext Byte Seek

Response Header will indicate the Cleartext domain of the actual response body, as described in guidelines 7.6.6.3.3 (GUN 5JYDY) and 7.6.5.6 (GUN M2V86).

7.6.5.4.2

[GUIDELINE] If the Cleartext Byte Seek Response Header is provided, the syntax of the availableSeekRange.dlna.org header is modified as follows:

- availableSeekRange-line = "availableSeekRange.dlna.org" *LWS ":" *LWS mode-flag [SP range specifier]

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IEC 62481-1-1: 2017	NQ9NX	N

[COMMENT] This change in syntax for the availableSeekRange-line allows for the mode-flag to be provided without requiring a range specifier. This allows the Cleartext byte range to be provided via the Cleartext Byte Seek Response Header and the Limited Random Access Data Availability mode to be provided via the availableSeekRange.dlna.org header when neither time-seek nor non-Cleartext byte seek are supported on a protected content binary. The components of the availableSeekRange-line are defined in IEC 62481-1-1:2017, 11.4.3.20.8 (GUN UBZ33).

7.6.5.5 MT HTTP: data range of "Limited Random Access Data Availability"

[GUIDELINE] For a content binary that uses a Link Protection System, the Cleartext Byte Seek Request Header shall be used as the mechanism for byte-based seek operations on the HTTP transport protocol that are specified in the Cleartext Byte Domain.

The RANGE header shall be used as the mechanism for specifying byte seek operations on the HTTP transport protocol that are specified in the Network Byte Domain. The seek-able data range shall be equivalent to the random access data range of $[r_0, r_N]$.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	IETF RFC 2616	3M2V8

[COMMENT] The Cleartext Byte Seek Request Header can be different depending on the Link Protection System used. For the general requirements of the header, see guideline 7.6.10.2, for the DTCP-IP Link Protection System, see guideline 8.6.1.2, for the WMDRM-ND Link Protection System, and see guideline 9.6.1.7 for the definition of this header.

7.6.5.6 MT HTTP Time-Based Seek (Server)

[GUIDELINE] If an HTTP Server Endpoint supports both time-based-seek operations and byte based operations in the Cleartext Byte Domain on a resource that uses a Link Protection System, then it shall specify a cleartextbyte-range value using the Cleartext Byte Seek Response Header in addition to the npt-range value using the TimeSeekRange.dlna.org header in the HTTP Target Response to the HTTP request with the TimeSeekRange.dlna.org header field unless one of the following exceptions applies.

Exceptions:

If all of the following conditions are true:

- the data access model is the Limited Random Access Data Availability model and the mode-flag (as indicated in availableSeekRange.dlna.org) is "1";
- the HTTP request includes a valid PlaySpeed.dlna.org header;
- the media format profile corresponding to the requested resource requires a modified form of the content binary in a time-seek response (e.g. MP4 container-based media profiles).

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	M2V86	E

[COMMENT] For link-protected content, the instance range is returned using the Cleartext Byte Seek Response Header and not using the TimeSeekRange.dlna.org header. Therefore, both headers are necessary to indicate the byte position within the Cleartext Byte Domain.

The instance-duration and npt-range values of TimeSeekRange.dlna.org is defined in IEC 62481-1-1:2017, 11.4.3.23.2 (GUN S2RRM).

The cleartextbyte-range and instance-length values for the Cleartext Byte Seek Response Header are defined for the DTCP-IP Link Protection System in guideline 8.6.1.3, for the WMDRM-ND Link Protection System in guideline 9.6.1.8.

EXAMPLE 1

TimeSeekRange.dlna.org: npt=335.1-336.1/40445.4

Content-Range.dtcp.com: bytes 1539686400-1540210688/304857907200

EXAMPLE 2

TimeSeekRange.dlna.org: npt=00:05:35.2-00:05:38.1/*

Content-Range.dtcp.com: bytes 1539686400-1540210688/*

7.6.5.7 MT caching directives for HTTP 1.0

[GUIDELINE] An HTTP Server Endpoint that transfers content using DLNA Link Protection as the response to an HTTP/1.0 GET request shall prevent intermediate caching by including among the HTTP response headers the directive

- Pragma: no-cache.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	VLBIV	

7.6.5.8 MT caching directives for HTTP 1.1

[GUIDELINE] An HTTP Server Endpoint that transfers content using DLNA Link Protection as the response to an HTTP/1.1 GET request shall prevent intermediate caching by including among the HTTP response headers the directive

- Pragma: no-cache,
- Cache-control: no-cache.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	JYDYG	

7.6.6 New general HTTP Media Transport guidelines

7.6.6.1 HTTP error codes for unavailable content

[GUIDELINE] If an HTTP Server Endpoint receives a request for a content binary with an HTTP GET or HEAD request and the Server Endpoint cannot make that content available because of a content protection license issue, the HTTP Server Endpoint should respond with an error code of 403 (Forbidden).

[ATTRIBUTES]

S	A	DMS	M-DMS	n/a	IETF RFC 2616	6EOVL	

[COMMENT] By the HTTP specification, the HTTP Server Endpoint can place additional information about the cause of the error in the entity body of the response.

7.6.6.2 MT byte position definitions

[GUIDELINE] For content that uses DLNA Link Protection, unless otherwise stated, all references in IEC 62481-1-1:2017 that refer to byte positions or byte based seek operations (such as the Range, Content-Range, and Content-Length headers, as well as the byte unit values of instance-length and byte-range of the TimeSeekRange.dlna.org header) shall refer to byte positions in the Network Byte Domain (i.e. after encryption and any Link Protection headers and padding have been added).

[ATTRIBUTES]

M	C	DMS +PU+ DMR DMP	M-DMS M-DMP	n/a	IEC 62481-1-1: 2017	LG6NX	

7.6.6.3 MT HTTP header: Cleartext Byte Seek Request Header (server)

7.6.6.3.1

[GUIDELINE] If the HTTP Server Endpoint is transporting content using DLNA Link Protection, the HTTP Server Endpoint should support receiving the Cleartext Byte Seek Request Header as defined in the guidelines below for the HTTP GET and HEAD methods.

[ATTRIBUTES]

S	L	DMS +PU+	M-DMS	n/a	IETF RFC 2616	3PVBR	

7.6.6.3.2

[GUIDELINE] If the HTTP Server Endpoint is transporting content using DLNA Link Protection, and the HTTP Server Endpoint receives the Cleartext Byte Seek Request Header in a HEAD request, then the HTTP server may respond without the Cleartext Byte Seek Response Header.

[ATTRIBUTES]

O	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	EOVLB	

7.6.6.3.3

[Guideline] If the HTTP Server Endpoint is transporting content using DLNA Link Protection, and an HTTP Server Endpoint returns the data range requested with the Cleartext Byte Seek Request Header, it shall specify the Cleartext Byte Seek Response Header in the target response. Furthermore, the HTTP response code shall be: 200 (OK).

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	5JYDY	

[**COMMENT**] The positions specified in this header refer to positions in the Cleartext Byte Domain.

7.6.6.3.4

[GUIDELINE] If the HTTP Server Endpoint is transporting content using DLNA Link Protection, it shall respond with the Cleartext Byte Seek Response Header for a request specified with the Cleartext Byte Seek Request Header in the HTTP GET request.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	X5JYD	

7.6.6.3.5

[GUIDELINE] If the HTTP Server Endpoint is transporting content using DLNA Link Protection and the HTTP Server Endpoint uses the Cleartext Byte Seek Response Header, then the provided values shall be accurate with respect to the requested range over the Cleartext Byte Domain allowing for alignment at boundaries within the content binary. Specifically,

- the first byte position specified in the Cleartext Byte Seek Response Header shall match the first requested byte in the Cleartext Byte Seek Request Header or start at a Decoder Friendly Alignment Position for the given format profile containing the requested byte,
- the last byte position specified in the Cleartext Byte Seek Response Header shall properly match the last byte requested in the Cleartext Byte Seek Request Header or end at the endpoint of a Media Format Alignment Element for the given format profile in use.

The value indicating the instance-length shall indicate the length of the entire original content binary over the Cleartext Byte Domain (i.e. before encryption and any Link Protection packetization) or asterisk (*) if unknown.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	OVLBI	

[COMMENT] The Decoder Friendly Alignment Position is defined for each of the media format profiles specified in 8.8 and 9.8.

The Media Format Alignment Element is defined for each of the media format profiles specified in 8.8 and 9.8.

7.6.6.3.6

[GUIDELINE] If the HTTP Server Endpoint is transporting content using DLNA Link Protection and the HTTP Server Endpoint uses the Cleartext Byte Seek Response Header to return a

specific range of data, the first byte of the HTTP Entity Body shall correspond to the start of a Link Protection Alignment Element for the given Link Protection System in use.

[ATTRIBUTES]

M	C	DMS +PU+	M-DMS	n/a	IETF RFC 2616	6X5JY	

[COMMENT] There has typically been a seek operation where the bytes returned do not correspond to the bytes following the previous packet. In order to allow decryption to correctly operate, the client needs to be able to start decryption at the start of the HTTP Entity body.

7.6.6.3.7

[GUIDELINE] If the range requested with the Cleartext Byte Seek Request Header is not valid for the resource with a URI specified in the HTTP request, then the HTTP Server Endpoint shall respond with the HTTP response code of: 416 (Requested Range Not Satisfiable).

When encountering syntax errors with the Cleartext Byte Seek Request Header, the HTTP server shall use the HTTP response code 400 (Bad Request).

[ATTRIBUTES]

M	C	DMS +PU+	M-DMS	n/a	IETF RFC 2616	VALG6	

[COMMENT] HTTP response code 416 is used when the HTT Server Endpoint supports seeking in the Cleartext Byte Domain for the specified content binary, but is unable to comply with the request because the requested range is not currently available on the server.

7.6.6.3.8

[GUIDELINE] If an HTTP request with a Cleartext Byte Seek Request Header for the URI can never be processed/satisfied by the HTTP Server Endpoint, for example, in the case of real-time transcoding or live content, then the HTTP Server Endpoint shall respond with 406 (Not Acceptable).

[ATTRIBUTES]

M	L	DMS +PU+	M-DMS	n/a	IETF RFC 2616	ALG6N	

[COMMENT] HTTP response code 406 is used when the HTTTP Server Endpoint does not support seeking in the Cleartext Byte Domain for the specified content binary and the request includes the Cleartext Byte Seek Request Header.

Note that using a Cleartext Byte Seek Request Header with a starting position of 0 and requesting the entire range of available content is still using the Cleartext Byte Seek Request Header.

This includes the case where the incorrect Cleartext Byte Seek Request Header is used for the type of the content binary. For the specification of the header for the given link protect system used, see guideline 8.6.1.3 for the DTCP-IP Link Protection System, for the WMDRM-ND Link Protection System, see guideline 9.6.1.8.

7.6.6.3.9

[GUIDELINE] If an HTTP Server Endpoint receives a GET or HEAD request with both the Cleartext Byte Seek Request Header and the RANGE header, then the HTTP Server Endpoint shall respond with 406 (Not Acceptable).

[ATTRIBUTES]

M	L	DMS +PU+	M-DMS	n/a	IETF RFC 2616	V3PVB	

[COMMENT] The client cannot specify this situation, see guideline 7.6.6.4.3.

7.6.6.3.10

[GUIDELINE] If an HTTP Server Endpoint can support HTTP requests with a specified byte range as expressed in the Cleartext Byte Seek Request Header for a particular URI, then the HTTP Server Endpoint should support persistent connections (HTTP/1.1) for that URI.

[ATTRIBUTES]

S	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	4N2GT	

[COMMENT] Content that is requested with the byte range option can often get many requests using the Cleartext Byte Seek Request Header in a short period of time, potentially causing content serving devices to run out of available sockets.

7.6.6.3.11

[GUIDELINE] An HTTP Server Endpoint should support HTTP requests that specify the Cleartext Byte Seek Request Header by implementing behaviour that returns the requested entity-body with the 200 (OK) HTTP header.

[ATTRIBUTES]

S	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	YDYGD	

7.6.6.4 MT HTTP header: Cleartext Byte Seek Request Header (client)

7.6.6.4.1

[GUIDELINE] HTTP Client Endpoints shall not issue an HTTP GET and HEAD requests with the Cleartext Byte Seek Request Header for content items that do not explicitly state support for the Cleartext Byte Seek Request Header via the 4th field cleartextbyteseek-full flag or the lop-cleartextbytes flag of the flags-param, as defined in guideline 7.5.2.2.

[ATTRIBUTES]

M	L	DMP DMR	n/a	n/a	IETF RFC 2616	6NXR7	A

[COMMENT] This prohibition includes HTTP GET and HEAD requests with a range that includes the entire content binary.

7.6.6.4.2

[GUIDELINE] HTTP Client Endpoints shall specify byte positions within the Cleartext Byte Domain (before Link Protection encryption, headers, or padding is added) when using the Cleartext Byte Seek Request Header.

[ATTRIBUTES]

M	L	DMP DMR	n/a	n/a	IETF RFC 2616	G6NXR	A

7.6.6.4.3

[GUIDELINE] HTTP Client Endpoints shall not specify an HTTP GET or HEAD request that includes both the Cleartext Byte Seek Request Header and the HTTP RANGE header.

[ATTRIBUTES]

M	L	DMP DMR	n/a	n/a	IETF RFC 2616	PVBRV	A

[COMMENT] It is unlikely that the request will be satisfiable with specifications for both the byte position in the Network Byte Domain and the Cleartext Byte Domain.

7.6.7 Updates to existing general HTTP Media Transport for Streaming Transfer guidelines

7.6.7.1 Summary

Table 8 lists the updates to existing general HTTP Media Transport for Streaming Transfer guidelines.

Table 8 – Updates to existing general HTTP Media Transport for Streaming Transfer guidelines

Guideline updated	Location in IEC 62481-1-1:2017
MT HTTP Fast Forward Scan Media Operation	11.4.3.45.1 (GUN TY7CW)
MT HTTP Streaming Slow Forward Scan Media Operation	11.4.3.46.1 (GUN L6RNZ)
MT HTTP Streaming Fast Backward Scan Media Operation	11.4.3.47.1 (GUN Y7CWO)
MT HTTP Streaming Slow Backward Scan Media Operation	11.4.3.48.1 (GUN 6RNZ6)
MT HTTP Streaming Scan Media Operations	11.4.3.49.1 (GUN 6TQT3)
MT HTTP Media Operation support within a Profile	11.4.3.52.2 (GUN Z8H8X)
MT Combined RANGE, Time based Seek, and Play Speed HTTP Requests	11.4.3.56.2 (GUN CPWAE)
MT HTTP Header: realTimeInfo.dlna.org	11.4.3.57.6 (GUN R2GYQ)

7.6.7.2 MT HTTP Seek media operation

7.6.7.2.1

[GUIDELINE] A streaming HTTP Client Endpoint should implement the Seek media operation on content using DLNA Link Protection by using the RANGE, Cleartext Byte Seek Request Header, or the TimeSeekRange.dlna.org header, if those headers are supported by the HTTP Server for the content binary.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	n/a	5K83S	A

[COMMENT] The Cleartext Byte Seek Request Header can be different depending on the Link Protection System used. For the general header guidelines, see 7.6.10.2, for the DTCP-IP Link Protection System, see guideline 8.6.1.2, for the WMDRM-ND Link Protection System, see guideline 9.6.1.7 for the definition of this header.

7.6.7.2.2

[GUIDELINE] For every audio content binary using DLNA Link Protection, if a streaming HTTP Client Endpoint wants to perform a Fast Forward Scan media operation (positive play speed greater than 1×), then it should use one of these methods:

- issuing multiple HTTP GET requests with a specified Cleartext Byte Seek Request Header field, or
- issuing a single HTTP GET request with a specified PlaySpeed.dlna.org header field.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	YUX7M	A

7.6.7.2.3

[GUIDELINE] For every AV content binary using DLNA Link Protection, if a streaming HTTP Client Endpoint performs a Fast Forward Scan media operation (positive play speed greater than 1×), then the HTTP Client Endpoint should support the following method:

- issuing a single HTTP GET request with a specified PlaySpeed.dlna.org header field.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	SW9IL	A

7.6.7.2.4

[GUIDELINE] For every audio content binary using DLNA Link Protection, if a streaming HTTP Client Endpoint wants to perform a Slow Forward Scan media operation (positive play speed less than 1×), then it should use one of these methods:

- issuing multiple HTTP GET requests with a specified Cleartext Byte Seek Request Header field, or
- issuing a single HTTP GET request with a specified PlaySpeed.dlna.org header field.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	RADAX	A

7.6.7.2.5

[GUIDELINE] For every AV content binary using DLNA Link Protection, if a streaming HTTP Client Endpoint performs a Slow Forward Scan media operation (positive play speed less than 1×), then the HTTP Client Endpoint should support the following method:

- issuing a single HTTP GET request with a specified PlaySpeed.dlna.org header field.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	2U6TN	A

7.6.7.2.6

[GUIDELINE] For every audio content binary using DLNA Link Protection, if a streaming HTTP Client Endpoint wants to perform a Fast Backward Scan operation (negative play speed less than −1×), then it should use one of these methods:

- issuing multiple HTTP GET requests with a specified Cleartext Byte Seek Request Header field,
- issuing multiple HTTP GET requests with a specified TimeSeekRange.dlna.org header field,
- issuing a single HTTP GET request with a specified PlaySpeed.dlna.org header field.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	2WZ7Q	A

7.6.7.2.7

[GUIDELINE] For every AV content binary using DLNA Link Protection, if a streaming HTTP Client Endpoint performs a Fast Backward Scan media operation (negative play speed less than −1×), then the HTTP Client Endpoint should support the following method:

- issuing a single HTTP GET request with a specified PlaySpeed.dlna.org header field.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	YFQO6	A

7.6.7.2.8

[GUIDELINE] For every audio content binary using DLNA Link Protection, if a streaming HTTP Client Endpoint wants to perform a Slow Backward Scan media operation (negative play speed greater than or equal to −1×), then it should use one of these methods:

- issuing multiple HTTP GET requests with a specified Cleartext Byte Seek Request Header field, or
- issuing a single HTTP GET request with a specified PlaySpeed.dlna.org header field.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	29BM2	A

7.6.7.2.9

[GUIDELINE] For every AV content binary using DLNA Link Protection, if a streaming HTTP Client Endpoint wants to perform a Slow Backward Scan media operation (negative play speed less than zero and greater than or equal to −1×), then the HTTP Client Endpoint should support the following method:

- issuing a single HTTP GET request with a specified PlaySpeed.dlna.org header field.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	FFN2S	A

7.6.7.2.10

[GUIDELINE] If a streaming HTTP Client Endpoint wants to stop a normal playback stream in order to start a scan operation playback using the Cleartext Byte Seek Request Header under conditions where guideline 11.4.3.5.6 (GUN Y8RWS) in IEC 62481-1-1:2017 applies, then it should close the original HTTP connection before issuing a GET request with the Cleartext Byte Seek Request Header to perform scan operations (a.k.a. trick modes). After closing the original connection, the streaming HTTP Client Endpoint should open a new HTTP connection for the scan operation. Note that the new HTTP connection may be a persistent connection, which allows the client to issue multiple GET requests on a single HTTP connection.

[ATTRIBUTES]

S	A	DMP DMR +DN+ +DNSYNC+	M-DMP	n/a	IETF RFC 2616	QFAIG	A

[**COMMENT**] Transitions from scan operations to normal playback may be achieved by making open ended (i.e. last-byte-pos value in Range header is absent) GET requests with the Cleartext Byte Seek Request Header.

7.6.7.2.11

[GUIDELINE] If an HTTP Server Endpoint supports byte Cleartext Byte Seek and/or TimeSeekRange.dlna.org capabilities on the content for a particular DLNA media format profile, it should support this on all content with this media format profile.

[ATTRIBUTES]

S	A	DMS +PU+	M-DMS	n/a	n/a	RDH6E	

[COMMENT] In some cases, such as transcoded or live content, it may be difficult to support byte Cleartext Byte Seek and/or TimeSeekRange.dlna.org.

7.6.7.2.12

[GUIDELINE] If a streaming HTTP Server Endpoint receives an HTTP GET request with the Cleartext Byte Seek Request and (TimeSeekRange.dlna.org or PlaySpeed.dlna.org) header fields, then the Cleartext Byte Seek Request Header field takes the highest precedence and the server shall ignore the other time seek and play speed fields.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	ISOLO	

[COMMENT] This guideline covers what a streaming HTTP Server endpoint needs to do if it receives an HTTP request with Cleartext Byte Seek and other DLNA fields for play speed or time based seek. This guideline also infers how a streaming HTTP Client endpoint can expect an HTTP Server Endpoint to behave.

7.6.7.2.13

[GUIDELINE] If an HTTP Server Endpoint receives an HTTP GET or HEAD request with a Cleartext Byte Seek and realTimeInfo.dlna.org header, then an HTTP Server Endpoint shall never reply with a finite max-lag-time parameter value.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	LHLTF	

[COMMENT] This guideline obliges an HTTP Server Endpoint to not change the content data bytes in a reply to a request with a Cleartext Byte Seek Request Header.

7.6.7.2.14

[GUIDELINE] If a streaming HTTP Client Endpoint performs a Pause media operation on a DLNA Link Protected binary, then the HTTP Client Endpoint shall support all of the following Pause media operation methods:

- Disconnecting and Seeking: Disconnecting the HTTP connection and Cleartext byte-based seek transport layer features as the mechanism for Pause-Release;
- Disconnecting and Seeking: Disconnecting the HTTP connection and using time-based seek transport layer features as the mechanism for Pause-Release.

[ATTRIBUTES]

M	L	DMP DMR	M-DMP	n/a	IETF RFC 2616	LQWYS	A

7.6.8 MT RANGE behaviour for Interactive Transferred Content

[GUIDELINE] For a content binary that uses a Link Protection System, the Cleartext Byte Seek Request Header may be used for Interactive Transfers when the "Full Random Access Data Availability" model or the "Limited Random Access Data Availability" model with mode-flag=1 applies to the HTTP Server Endpoint serving the content binary.

[ATTRIBUTES]

O	C	DMS DMR DMP +PU+	M-DMS M-DMP	n/a	n/a	VBRVS	A

7.6.9 RTP transport

Subclauses 7.6.10 to 7.6.11 cover the guidelines for the RTP transport protocol for content transmitted using DLNA Link Protection. For detailed information, see IEC 62481-1-1:2017, 11.4.4, Media Transport: RTP Transport.

7.6.10 Update existing general RTP Transport guidelines

7.6.10.1 MT RTP Packet size

[GUIDELINE] A Serving Endpoint should limit the size of the RTP carrying content using DLNA Link Protection so that the size of the encrypted packet, including protocol headers, Link Protection headers, and any necessary padding will not exceed the Maximum Transmission Unit (MTU) used in the home network.

[ATTRIBUTES]

S	A	DMS +PU+	M-DMS	n/a	IETF RFC 1191	2GTDF	

[COMMENT] Link Protection encapsulation can add headers and padding and will increase payload size.

7.6.10.2 MT RTP Play Media operation

[GUIDELINE] If an RTSP Server Endpoint receives a request for a content binary with an RTSP PLAY or SETUP request and the Server Endpoint cannot make that content available because of a content protection license issue, the RTSP Server Endpoint should respond with an error code of 403 (Forbidden).

[ATTRIBUTES]

S	A	DMS +PU+	M-DMS	n/a	IETF RFC 1191	BRVS3	

7.6.11 New general RTP Transport guidelines: MT: RTP support for link protected content

[GUIDELINE] Serving Endpoints and Receiving Endpoints that implement a Link Protection System and that support the RTP Media Transport for non-link-protected content should implement the Link Protection System for the RTP Media Transport.

[ATTRIBUTES]

S	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	WMDRM-ND	N2GTD	A

[COMMENT] Content Receivers and Content Sources that implement a Link Protection System and also support the optional RTP Media Transport are recommended to extend their support for the Link Protection System to include the RTP Media Transport.

7.7 Content conversion device virtualization

The guidelines contained in IEC 62481-1-1:2017, Clause 12 hold identically for devices exchanging content using DLNA Link Protection. Correspondingly, there are no additional DTCP-IP or WMDRM-ND specific guidelines in Clauses 8 or 9 for content conversion and device virtualization.

7.8 Link Protection technology guidelines

7.8.1 Link Protection System: DTCP-IP

7.8.1.1

[GUIDELINE] If a device supports DLNA Link Protection it shall support DTCP-IP as defined in these guidelines.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E DTCP Adopter Agreement DTCP Audio Compliance Rules EXHIBIT B-2	BSTW5	A

7.8.1.2

[GUIDELINE] If a UPnP AV Media Server supports DLNA Link Protection it shall be capable of exposing and transferring at least one of the DLNA media format profiles with DTCP-IP Link Protection.

[ATTRIBUTES]

M	A	DMS	M-DMS	n/a	n/a	K83SN	

7.8.1.3

[GUIDELINE] If a UPnP AV Media Renderer Control Point supports DLNA Link Protection it shall be capable of transferring at least one of the DLNA media format profiles with DTCP-IP Link Protection.

[ATTRIBUTES]

M	A	+PU+	n/a	n/a	n/a	STW5C	A

7.8.1.4

[GUIDELINE] If a UPnP AV MediaServer supports DLNA Link Protection the content objects that it exposes for which DTCP-IP is permitted as an output shall have a <res> element with a profile ID using the DTCP_ prefix.

[ATTRIBUTES]

M	A	DMS	M-DMS	n/a	n/a	83SNB	

[COMMENT] The phrase "permitted as an output" refers to usage that is in compliance with policy requirements that the endpoint is subject to and that are defined by the entity governing the usage of the content. This excludes product design decisions or product manufacturer's policy. While a definition of these policies is outside the scope of the DLNA Link Protection guidelines the behaviour expressed by this guideline will result in improved interoperability.

7.8.1.5

[GUIDELINE] If a Push Controller supports DLNA Link Protection the content that it streams for which DTCP-IP is permitted as an output shall be available with DTCP-IP Link Protection.

[ATTRIBUTES]

M	A	+PU+	n/a	n/a	n/a	TW5CS	

7.8.1.6

[GUIDELINE] If a device supports the DTCP-IP Link Protection System, it shall support all guidelines in IEC 62481-1-1:2017, modified by the guidelines stated in Clause 7 of this document and 8.3, 8.5, and 8.6.1, and if the RTP media transport format is supported as given in 8.6.2.2 to 8.6.2.4.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	IEC 62481-1-1: 2017	GTDFW	A

7.8.2 Link Protection System: Windows Media DRM for network Devices

7.8.2.1

[GUIDELINE] If a device supports DLNA Link Protection it may support WMDRM-ND as defined in these guidelines.

[ATTRIBUTES]

O	A	DMS DMP DMR	M-DMS M-DMP	n/a	WMDRM-ND RTP Payload format for WMV and WMA	3SNB9	A

7.8.2.2

[GUIDELINE] If a UPnP AV MediaServer supports DLNA Link Protection the content objects that it exposes for which WMDRM-ND is permitted as an output may have a <res> element with a profile ID using the WMDRM_ prefix.

[ATTRIBUTES]

O	A	DMS	M-DMS	n/a	n/a	W5CS8	A

[COMMENT] The phrase "permitted as an output" refers to usage that is in compliance with policy requirements that the endpoint is subject to and that are defined by the entity governing the usage of the content. This excludes product design decisions or product manufacturer's policy. While definition of these policies is outside the scope of the DLNA Link Protection guidelines the optional behaviour expressed by this guideline will result in improved interoperability. Content objects that are only permitted to be output over WMDRM-ND can be optionally exposed on the network with WMDRM-ND protection. Content objects that are permitted to be output over both DTCP-IP and WMDRM-ND can be optionally exposed on the network with WMDRM-ND protection, in addition to being exposed with the required DTCP-IP protection.

7.8.2.3

[GUIDELINE] If a Push Controller supports DLNA Link Protection the content that it streams, for which WMDRM-ND is permitted as an output, may be available with WMDRM-ND Link Protection.

[ATTRIBUTES]

O	A	+PU+	n/a	n/a	n/a	5CS88	

7.8.2.4

[GUIDELINE] If a device supports the WMDRM-ND Link Protection System it shall support all guidelines in IEC 62481-1-1:2017, modified by the guidelines stated in Clause 7 of this document and 9.2, 9.3, 9.4, and 9.6.1, and if the RTP media transport (9.6.2) is supported.

[ATTRIBUTES]

M	A	DMS DMP DMR	M-DMS M-DMP	n/a	IEC 62481-1-1: 2017	SNB9F	A

8 DTCP-IP Link Protection System guidelines

8.1 General

This clause contains the guidelines that are specific to the DTCP-IP Link Protection System.

See Clause 7 for general guidelines for devices that implement DTCP-IP.

8.2 CP DTCP-IP general guidelines

[GUIDELINE] A device that implements DTCP-IP shall comply with all requirements in the DTCP-IP specifications at the time the product is offered to the market.

[ATTRIBUTES]

M	R	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E DTCP Audio Compliance Rules EXHIBIT B-2 DTCP Adopter Agreement	5GV8W	A

[COMMENT] Reference DTCP Adopter Agreement defines a grace period that allows vendors to ship products which are conformant with previous specifications.

8.3 Networking and connectivity

8.3.1 General

This subclause contains the guidelines that are specific to DTCP-IP use of the networking capabilities described in Clause 8 of IEC 62481-1-1:2017.

8.3.2 New DLNAQOS guidelines: QoS requirement for DTCP-IP traffic

[GUIDELINE] If DLNA QoS as defined in Clause 8 of IEC 62481-1-1:2017 is implemented, all DTCP-IP commands and responses generated by Content Sources and Content Receivers shall be tagged as DLNAQOS_3, or a lower DLNAQOS_UP value, in accordance with Table 7 of IEC 62481-1-1:2017.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	IEC 62481-1-1: 2017	TDFW2	A

[COMMENT] DTCP-IP has an RTT test that puts stringent requirements on the network timing. In order to ensure that these packets get the best available network service, set the DLNAQOS level appropriately. Also assign DTCP-IP messages a priority higher than A/V stream itself.

8.3.3 New common device guidelines: NC CP: wireless security

[GUIDELINE] Devices which use the DTCP-IP Link Protection System with integrated IEEE 802.11 shall ensure that WEP or an equivalent protection mechanism (e.g. WPA or WPA2) is engaged prior to exchanging DTCP AKE commands and protected content via that network interface.

[ATTRIBUTES]

M	R	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1 Supplement E DTCP Adopter Agreement	LQ89T	

[COMMENT] This is a requirement of the DTCP specification.

8.4 Device discovery and control

There are no DTCP-IP specific changes to the guidelines in Clause 9 of IEC 62481-1-1:2017.

8.5 Media Management

8.5.1 General

This subclause covers the guidelines for implementing media management using the UPnP AV architecture that are specific to the DTCP-IP Link Protection System. For detailed information see Clause 11 of IEC 62481-1-1:2017.

8.5.2 MM CP: DTCP-IP URI

[GUIDELINE] A DLNA device shall not rely on the existence of URI parameters to establish the DTCP-IP AKE connection.

[ATTRIBUTES]

M	L	DMP, DMR	n/a	n/a	DTCP Volume 1 Supplement E	8YKV4	

[COMMENT] The DTCP specification allows the DTCP-IP AKE parameters for the host and port to be placed in either the MIME type or within the URI of the content. This specification requires that servers publish the host and port within the MIME type and that rendering devices not rely on that information being within the URI also.

8.5.3 MM CP: mandatory media operations

8.5.3.1

[GUIDELINE] A Rendering Endpoint implementing audio or AV media classes shall implement the same media operations as stated in Guideline 10.1.6.31.1 (GUN: S4HXE) in IEC 62481-1-1:2017 with the following modifications:

- Pause-Release (7.6.7.2.14);
- seek (Guideline 8.6.1.4.1).

[ATTRIBUTES]

M	A	DMP, DMR	M-DMP	n/a	IEC 62481-1-1: 2017 IETF RFC 2616	SHCIH	A

8.5.3.2

[GUIDELINE] A Rendering Endpoint implementing AV media classes shall implement the following media operations:

- Fast Forward Scan (Guideline 8.6.1.4.3);
- Slow Forward Scan (Guideline 8.6.1.4.4);
- Fast Backward Scan (Guideline 8.6.1.4.5);
- Slow Backward Scan (Guideline 8.6.1.4.6).

[ATTRIBUTES]

M	A	DMP, DMR	M-DMP	n/a	IETF RFC 2616	WUYBX	A

[COMMENT] An operation might not always invoke the corresponding media operation due to buffering on the Rendering Endpoint.

8.6 Media Transport

8.6.1 HTTP transport

8.6.1.1 General

This subclause covers the guidelines for implementing Media Transport using the UPnP AV architecture that are specific to the DTCP-IP Link Protection System. For detailed information, see Clause 10 of IEC 62481-1-1:2017.

8.6.1.2 MT HTTP Cleartext Byte Seek Request Header for DTCP-IP

8.6.1.2.1

[GUIDELINE] The HTTP Server and Client endpoints shall use the Range.dtcp.com header as the Cleartext Byte Seek Request Header for content that uses the DTCP-IP Link Protection System transmitted using the HTTP Media Transport protocol.

[ATTRIBUTES]

M	R	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1 Supplement E IETF RFC 2616	4I6WA	A

8.6.1.2.2

[GUIDELINE] The notation of the Range.dtcp.com header field for HTTP Media Transport of content that uses the DTCP-IP Link Protection System shall be as stated below.

[ATTRIBUTES]

M	L	DMP DMR	M-DMP	n/a	DTCP Volume 1 Supplement E IETF RFC 2616	7I2CK	A

- Range.dtcp.com = "Range.dtcp.com" ":" range-specifier
- range-specifier = byte-range-specifier
- byte-range-specifier = bytes-unit "=" byte-range-set
- bytes-unit = "bytes"
- byte-range-set = byte-range-spec
- byte-range-spec = first-cleartextbyte-pos "-" [last-cleartextbyte-pos]
- first-cleartextbyte-pos = 1*DIGIT
- last-cleartextbyte-pos = 1*DIGIT

first-cleartextbyte-pos and last-cleartextbyte-pos apply to the original content binary immediately before DTCP processing, i.e. before encryption and PCP packetization.

Note that the literal "bytes" is case sensitive.

EXAMPLE 1

Range.dtcp.com: bytes=1 539 686 400 –

EXAMPLE 2

Range.dtcp.com: bytes=1 539 686 400 – 1 540 210 688

8.6.1.3 MT HTTP Cleartext Byte Seek Response Header for DTCP-IP

8.6.1.3.1

[GUIDELINE] The HTTP Server and Client endpoints shall use the Content-Range.dtcp.com header as the Cleartext Byte Seek Response Header for content that uses the DTCP-IP Link Protection System transmitted using the HTTP Media Transport protocol.

[ATTRIBUTES]

M	L	DMS DMR DMP +PU+	M-DMS M-DMP	n/a	DTCP Volume 1 Supplement E IETF RFC 2616	2V86H	

8.6.1.3.2

[GUIDELINE] The notation of the Content Range.dtcp.com header field for HTTP Media Transport of content that uses the DTCP-IP Link Protection System shall be as stated below.

- Content-Range.dtcp.com = "Content-Range.dtcp.com" ":" content-range-spec
- content-range-spec = byte-content-range-spec
- byte-content-range-spec = bytes unit SP byte-range-resp-spec "/" (instance-length | "*")
- bytes-unit = "bytes"

- byte-range-resp-spec = first-cleartextbyte-pos "-" last-cleartextbyte-pos
- first-cleartextbyte-pos = 1*DIGIT
- last-cleartextbyte-pos = 1*DIGIT
- instance-length = 1*DIGIT

first-cleartextbyte-pos, last-cleartextbyte-pos and instance-length apply to the content binary over the *Cleartext Byte Domain*, immediately before DTCP processing, i.e. before encryption and PCP packetization.

Note that the literal "bytes" is case sensitive.

Example of Content Range.dtcp.com header.

Content Range.dtcp.com: bytes 1539686400-1540210688/9238118400

[ATTRIBUTES]

M	F	DMS +PU+	M-DMS	n/a	DTCP Volume 1 Supplement E IETF RFC 2616	LBIVE	

8.6.1.4 MT HTTP trickmodes

8.6.1.4.1

[GUIDELINE] For every content binary using the DTCP-IP Link Protection System, if a streaming HTTP Client Endpoint performs a Seek media operation, then the HTTP Client Endpoint shall support all of the following Seek media operation methods:

- Range.dtcp.com header field;
- TimeSeekRange.dlna.org header field.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	n/a	RMK89	A

[COMMENT] Refer to IEC 62481-1-1:2017, 11.4.3.44 (GUNs 9I4UN and PHT47).

8.6.1.4.2

[GUIDELINE] For every AV content binary using the DTCP-IP Link Protection System that supports "Limited Random Access Data Availability" Mode 1 or "Full Random Access Data Availability" model (see 11.4.2.16 of IEC 62481-1-1:2017 for details on mode), an HTTP Server Endpoint shall indicate support in the fourth field of the ProtocolInfo for at least one of

- time-based seek,
- Cleartext Byte Seek.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	IETF RFC 2616	XQWLF	E

[COMMENT] A content binary that is restricted to "Limited Random Access Data Availability" Mode 0 is considered live content and can have limited ability to support scan modes (see IEC 62481-1-1:2017, 11.4.2.16.2 GUN W5HZV).

8.6.1.4.3

[GUIDELINE] For every AV content binary using the DTCP-IP Link Protection System, if a streaming HTTP Client Endpoint performs a Fast Forward Scan media operation (positive play speed greater than 1×), then the HTTP Client Endpoint shall support all of the following methods:

- Issuing multiple HTTP GET requests with a specified Range.dtcp.com header field;
- Issuing multiple HTTP GET requests with a specified TimeSeekRange.dlna.org header field.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	A84FZ	A

8.6.1.4.4

[GUIDELINE] For every AV content binary using the DTCP-IP Link Protection System, if a streaming HTTP Client Endpoint performs a Slow Forward Scan media operation (positive play speed less than 1×), then the HTTP Client Endpoint shall support all of the following methods:

- issuing multiple HTTP GET requests with a specified Range.dtcp.com header field;
- issuing a single HTTP GET request and subsequently using Connection Stalling Method (see guideline IEC 62481-1-1:2017, 11.4.3.43) to accommodate slower decode and display of the streamed content.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	49EQY	

8.6.1.4.5

[GUIDELINE] For every AV content binary using the DTCP-IP Link Protection System, if a streaming HTTP Client Endpoint performs a Fast Backward Scan media operation (negative play speed less than −1×), then the HTTP Client Endpoint shall support all of the following methods:

- issuing multiple HTTP GET requests with a specified Range.dtcp.com header field;
- issuing multiple HTTP GET requests with a specified TimeSeekRange.dlna.org header field.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	MRPVA	A

8.6.1.4.6

[GUIDELINE] For every AV content binary using the DTCP-IP Link Protection System, if a streaming HTTP Client Endpoint wants to perform a Slow Backward Scan media operation (negative play speed less than zero and greater than or equal to −1×), then the HTTP Client Endpoint shall support the following method:

- issuing multiple HTTP GET requests with a specified Range.dtcp.com header field.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	IETF RFC 2616	WDJFZ	A

8.6.2 RTP transport

8.6.2.1 General

This subclause covers the guidelines for the RTP transport protocol for DLNA devices using the DTCP-IP Link Protection System.

8.6.2.2 MT RTP CP:

[GUIDELINE] For A/V Profile ID values in 8.7 for which the following holds:

- the media format profile defines link protected content;
- the Link Protection System used is DTCP-IP.

The RTP encapsulation of this media format profile shall not use a static payload type, see 8.6.2.4.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E IETF RFC 3550 IETF RFC 3551	DYGDM

8.6.2.3 MT DTCP-IP encapsulated media format profiles

8.6.2.3.1

[GUIDELINE] For a content binary that uses the DTCP-IP Link Protection System, the Cleartext content binary shall first be encapsulated into an RTP payload and an RTP header shall be generated adhering to Guidelines 11.4.4.59 to 11.4.4.127 of IEC 62481-1-1:2017, according to the corresponding format profile of the un-encrypted content.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E IETF RFC 3550 IETF RFC 3551	NXR7U

8.6.2.3.2

[GUIDELINE] After the RTP encapsulation of the Cleartext content as per 8.6.1.2.1, the RTP payload thus generated shall be encrypted into a single DTCP PCP as defined in DTCP Volume 1 Supplement E.

The RTP payload includes the encapsulated media portion but not the RTP header, the CSRC list, the extended RTP header, or any RTP padding applied.

[ATTRIBUTES]

M	C	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E IETF RFC 3550 IETF RFC 3551	RVS3E

8.6.2.3.3

[GUIDELINE] All other RTP header information for the DTCP-IP encapsulated payload shall match the corresponding value of the RTP header of the encapsulation of the Cleartext content stream of Guideline 8.6.1.2.1.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	IETF RFC 3550 IETF RFC 3551	DFW2J	

[COMMENT] Any timing information carried in the RTP header of a DTCP-IP encapsulated packet shall match the information available for the un-encrypted RTP payload within.

8.6.2.4 MT RTP CP

[GUIDELINE] If the Link Protection System is DTCP-IP, the SDP media field shall be "application" and a dynamic payload type shall be used.

The rtpmap attribute field shall have "x-dtcp1" as encoding name.

The fmtp attribute field shall have "CONTENTFORMAT=<MIME-Type> DTCP1HOST=<address> DTCP1PORT=<port>" as the format specific parameter.

In this case, <MIME-Type> represents the MIME-type of the RTP encapsulation before Link Protection is applied.

<address> represents the IP address of the AKE host.

<port> represents the port on which the AKE host is listening for authentication and key exchange messages.

The AKE <address> and <port> parameters for all streams defined in the SDP shall be equal.

[ATTRIBUTES]

M	A	DMS DMP DMR	M-DMS M-DMP	n/a	IETF RFC 3550 IETF RFC 3551	NB9FS	

[COMMENT] Refer to IETF RFC 2327

EXAMPLE

m=application 0 RTP/AVP 96

a=rtpmap:96 x-dtcp1/90000

a=fmtp:96 CONTENTFORMAT= video/mp2t DTCP1HOST=192.168.1.1 DTCP1PORT=37654

If the video stream and audio stream are separated, describe 2 kinds of dynamic payload types as follows.

m=application 0 RTP/AVP 96

a=rtpmap:96 x-dtcp1/90000

a=fmtp:96 CONTENTFORMAT=video/mpv DTCP1HOST=192.168.1.1 DTCP1PORT=37654

m=application 0 RTP/AVP 97

a=rtpmap:97 x-dtcp1/90000

a=fmtp:97 CONTENTFORMAT=audio/mpa DTCP1HOST=192.168.1.1 DTCP1PORT=37654

8.7 Content conversion device virtualization

There are no guidelines specific to DTCP-IP for content conversion and device virtualization.

8.8 Volume 2: DTCP-IP profiling guidelines

8.8.1 General

This subclause contains additions to IEC 62481-2:2017, defining the DTCP-IP media format profiles. This subclause also contains guidelines that are specific to the DTCP-IP Link Protection System. The guidelines only apply to DLNA devices that implement the DTCP-IP Link Protection System.

8.8.2 CP DTCP-IP: profile

8.8.2.1

[GENERAL] Profile: **DTCP_***

8.8.2.2

[GUIDELINE] Main characteristics of profiles that are encapsulated using the DTCP-IP Link Protection System are defined in DTCP Volume 1 and DTCP Volume 1 Supplement E.

[ATTRIBUTES]

M	R	HND	MHD	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E	CS88V	

8.8.2.3

[GUIDELINE] The Profile ID of DTCP-IP protected content shall comply with the following syntax:

ProfileID_Protected = "DTCP_" Original_ProfileID

Original_ProfileID = the Profile ID specified in IEC 62481-2:2017 that would be used for the Cleartext version of the same content.

EXAMPLE If a content binary that complies with the MPEG_PS_NTSC Profile ID is transferred with DTCP-IP Link Protection, then the Profile ID of the protected content shall be DTCP_MPEG_PS_NTSC.

[ATTRIBUTES]

M	A	HND	MHD	n/a	IEC 62481-2:2017	S88V5	

8.8.2.4

[GUIDELINE] The media carried within the DTCP-IP media format profile, after de-capsulation of DTCP-IP shall be conformant to the original profile ID as specified in the Original_ProfileID portion of the format Profile ID.

[ATTRIBUTES]

M	A	HND	MHD	n/a	IEC 62481-2:2017	B9FS8	

8.8.2.5

[GUIDELINE] A content binary using a DTCP_ Profile ID shall only be transferred using the DTCP-IP Link Protection System.

[ATTRIBUTES]

M	A	HND	MHD	n/a	n/a	FW2J3	

8.8.3 CP DTCP-IP: profile MIME type definition

8.8.3.1

[PROFILES]

DTCP_*

8.8.3.2

[GUIDELINE] When used to describe a content binary, the MIME type used for profiles based on the DTCP-IP Link Protection System shall be as follows:

application/x-dtcp1;DTCP1HOST=<host>;DTCP1PORT=<port>;CONTENTFORMAT=<MIME-type>

<MIME-type> is the MIME-type of the original content before DTCP-IP packetization enclosed in quotation marks.

Where <host> and <port> are the host and port where the serving endpoint is listening for any required AKE exchange.

[ATTRIBUTES]

M	C	DMS +PU+	M-DMS	n/a	IETF RFC 2045 DTCP Volume 1 DTCP Volume 1 Supplement E	VS3EY	

[COMMENT] An example would be in protocolInfo values that are used in <res> elements. Note that the CONTENTFORMAT attribute carries the original MIME type enclosed in quotation marks in adherence to IETF RFC 2045.

8.8.3.3

[GUIDELINE] The <host> value in the MIME type specified by guideline 8.8.3.2 shall be an absolute IP address consistent with the address used for UPnP Communications, formatted according to IETF RFC 3986.

[ATTRIBUTES]

M	R	DMS +PU+	M-DMS	n/a	IETF RFC 3986	XR7U7	C

8.8.3.4

[GUIDELINE] When used to describe a capability of a device, the MIME type used for profiles based on the DTCP-IP Link Protection System shall be as follows:

application/x-dtcp1;CONTENTFORMAT=<MIME-type>

<MIME-type> is the MIME-type, as listed in WMDRM-ND, for the content format profile before DTCP encryption enclosed in quotation marks.

[ATTRIBUTES]

M	C	DMS DMR	M-DMS	n/a	IETF RFC 2045 DTCP Volume 1 DTCP Volume 1 Supplement E	YGDM2	

[COMMENT] Example would be in protocolInfo values that are used in the response to the CMS:GetProtocolInfo action. Note that the CONTENTFORMAT attribute carries the original MIME type enclosed in quotation marks in adherence to IETF RFC 2045

8.8.4 CP DTCP-IP: profile protected and unprotected content portions

8.8.4.1

[PROFILES]

DTCP_*

8.8.4.2

[GUIDELINE] If a content binary contains both a protected portion and a non-protected portion, then the entire content shall be transferred by the Serving Endpoint using a DTCP-IP profile.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	n/a	W2J34	

[COMMENT] In this case, the non-protected portion is transferred with the E-EMI field of the PCP header equal to 0000, without encryption.

8.8.4.3

[GUIDELINE] If a content binary is known to never contain any protected content portions, then the Serving Endpoint should not use the DTCP-IP format profile to describe the content.

[ATTRIBUTES]

S	C	DMS +PU+	M-DMS	n/a	n/a	9FS8V	

[COMMENT] For instance, in case of a server that is capturing a stream that it knows will never have a protected portion, it is preferable to send this content as unprotected content and not use the DTCP-IP Link Protection System.

8.8.4.4

[GUIDELINE] A Rendering Endpoint shall continue to render the input stream correctly in the presence of dynamic changes of E-EMI values during the transfer of the content stream.

[ATTRIBUTES]

M	C	DMP DMR	M-DMP	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E	88V5U	

8.8.4.5

[GUIDELINE] If a Serving Endpoint cannot determine if the content item will ever contain a protected content portion, then the entire content shall be transferred using the Protected Content Packet (PCP) format.

[ATTRIBUTES]

M	C	DMS +PU+	M-DMS	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E	S3EYA	

[COMMENT] In this case, the non-protected portion is transferred with the E-EMI field of the PCP header equal to 0000, without encryption.

8.8.5 CP DTCP-IP: profile HTTP encapsulation

8.8.5.1

[PROFILES]

DTCP_*

8.8.5.2

[GUIDELINE] The first byte of an HTTP response carrying DTCP-IP link protected media content in its entity body shall be aligned to the first byte of a DTCP-IP PCP header.

For DTCP encapsulated content, the Link Protection Alignment Element is a PCP packet consisting of a properly formed PCP header, payload, and any necessary padding.

[ATTRIBUTES]

M	L	DMS +PU+	M-DMR	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E	R7U7Q	

8.8.6 DTCP-IP profile encapsulation

8.8.6.1 DTCP-IP encapsulated content: Alignment Element for PS

8.8.6.1.1

[GENERAL] Mandatory Alignment Element for Cleartext bitstreams using MPEG-2 Program Streams (PS) system.

8.8.6.1.2

[GUIDELINE] The Media Format Alignment Element for Cleartext bitstreams using MPEG-2 Program Stream (PS) to these profiles shall be the MPEG-2 pack.

[ATTRIBUTES]

M	A	n/a	n/a	n/a	ISO/IEC 13818-1	GDM2L	

[COMMENT] This entry clarifies the transport alignment of MPEG-2 Programme Streams encapsulated within the DTCP-IP Link Protection System.

Examples of DLNA Media Format Profiles to which this guideline applies are DTCP_MPEG_PS_NTSC, DTCP_MPEG_PS_PAL, DTCP_MPEG_PS_NTSC_XAC3, DTCP_AVC_PS_HD_DTS, etc.

8.8.6.2 DTCP-IP encapsulated content: Decoder Friendly Alignment Position for PS

8.8.6.2.1

[GENERAL] Mandatory Decoder Friendly Alignment Position for Cleartext bitstreams using a MPEG-2 Program Stream (PS) system.

8.8.6.2.2

[GUIDELINE] The Decoder Friendly Alignment Position for bitstreams using MPEG-2 Program Stream (PS) to these profiles shall be the VOBU boundary.

[ATTRIBUTES]

M	A	n/a	n/a	n/a	ISO/IEC 13818-1	BIVE3	

[COMMENT] This entry clarifies the transport alignment of MPEG-2 Program Streams encapsulated within the DTCP-IP Link Protection System when a Range.dtcp.com is performed.

Note that this is different from the corresponding unprotected content streams where the decoder friendly alignment position is defined as the GOP boundary.

Examples of DLNA Media Format Profiles to which this guideline applies are DTCP_MPEG_PS_NTSC, DTCP_MPEG_PS_PAL, DTCP_MPEG_PS_NTSC_XAC3, DTCP_AVC_PS_HD_DTS, etc.

8.8.6.3 DTCP-IP encapsulated content: Size of each PCP for PS

8.8.6.3.1

[GENERAL] Mandatory Decoder Friendly Alignment Position for Cleartext.

8.8.6.3.2

[GUIDELINE] For content using MPEG-2 Program Stream (PS) transferred with the HTTP transport protocol, the size of each PCP shall be one VOBU except in the following cases:

- when transferring a specific range of content requested with the Range.dtcp.com or TimeSeekRange.dlna.org header;
- when transferring the last VOBU in a content stream;
- when transferring content that includes a splitted VOBU that is caused by an Nc update in the middle of the VOBU as defined in DTCP Volume 1 or DTCP Volume 1 Supplement E.

[ATTRIBUTES]

M	L	DMS +PU+	M-DMS	n/a	DTCP Volume 1 DTCP Volume 1 Supplement E	IVE36	

[COMMENT] Examples of DLNA Media Format Profiles to which this guideline applies are DTCP_MPEG_PS_NTSC, DTCP_MPEG_PS_PAL, DTCP_MPEG_PS_NTSC_XAC3, DTCP_AVC_PS_HD_DTS, etc.

8.8.6.4 DTCP-IP encapsulated content: Alignment Element for TS

8.8.6.4.1

[GENERAL] Mandatory Alignment Element for Cleartext bitstreams using MPEG-2 Transport Stream (TS) system.

8.8.6.4.2

[GUIDELINE] The Media Format Alignment Element for Cleartext bitstreams using DLNA Transport Packets shall be the DLNA Transport Packet.

[ATTRIBUTES]

M	A	n/a	n/a	n/a	IEC 62481-2:2017 ISO/IEC 13818-1	V86HW	

[COMMENT] This entry clarifies the transport alignment of MPEG-2 Transport Streams encapsulated within the DTCP-IP Link Protection System.

Examples of DLNA Media Format Profiles to which this guideline applies are DTCP_MPEG_TS_SD_NA, DTCP_MPEG_TS_SD_EU_T, DTCP_MPEG_TS_JP_T, DTCP_AVC_TS_HD_60_AC3_T, etc.

8.8.6.5 DTCP-IP encapsulated content: Decoder Friendly Alignment Position for TS

8.8.6.5.1

[GENERAL] Mandatory Decoder Friendly Alignment Position for Cleartext bitstreams using MPEG-2 Transport Stream (TS) system.

8.8.6.5.2

[GUIDELINE] The Decoder Friendly Alignment Position for Cleartext bitstreams using DLNA Transport Packets shall be the DLNA Transport Packet boundary.

[ATTRIBUTES]

M	A	n/a	n/a	n/a	IEC 62481-2:2017 ISO/IEC 13818-1	2CKL6	

[COMMENT] Examples of DLNA Media Format Profiles to which this guideline applies are DTCP_MPEG_TS_SD_NA, DTCP_MPEG_TS_SD_EU_T, DTCP_MPEG_TS_JP_T, DTCP_AVC_TS_HD_60_AC3_T, etc.

9 WMDRM-ND Link Protection System guidelines

9.1 Overview

This clause contains guidelines that are specific to the WMDRM-ND Link Protection System. The guidelines only apply to DLNA devices that implement the WMDRM-ND Link Protection System. These guidelines are based on WMDRM-ND in WMDRM-ND.

9.2 General guidelines

9.2.1 CP WMDRM-ND: guidelines

9.2.1.1

[GUIDELINE] Content Receivers that implement WMDRM-ND shall comply with all requirements in the WMDRM-ND specification WMDRM-ND at the time the product is offered to the market.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	WMDRM-ND	I2CKL	A

[COMMENT] The subclause entitled "Common Cryptographic Elements for Receivers" in WMDRM-ND lists requirements on the use of encryption algorithms and on output formats, which need to be satisfied by all Rendering Endpoints that use WMDRM-ND. The subclause entitled "Protocol Requirements for Receivers" in WMDRM-ND lists protocol requirements.

9.2.1.2

[GUIDELINE] Content Sources that implement WMDRM-ND shall comply with all requirements in the WMDRM-ND specification WMDRM-ND at the time the product is offered to the market.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	WMDRM-ND	6WAWI	

[COMMENT] The subclause entitled "Common Cryptographic Elements for Transmitters" in WMDRM-ND lists requirements on the use of encryption algorithms, random number generation and on clock accuracy, which need to be satisfied by all Serving Endpoints that use WMDRM-ND. The subclause entitled "Protocol Requirements for Transmitters" in WMDRM-ND lists protocol requirements.

9.2.2 CP WMDRM-ND: support for HTTP

9.2.2.1

[GUIDELINE] Content Receivers that implement WMDRM-ND shall support the guidelines for the use of WMDRM-ND with the HTTP Media Transport defined in 9.6.1.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	WMDRM-ND	I6WAW	A

9.2.2.2

[GUIDELINE] Content Sources that implement WMDRM-ND shall support the guidelines for the use of WMDRM-ND with the HTTP Media Transport defined in 9.6.1.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	WMDRM-ND	86HW6	

9.2.3 CP WMDRM-ND: support for RTP

9.2.3.1

[GUIDELINE] Content Receivers that implement WMDRM-ND and that support the RTP Media Transport for non-link-protected content should implement WMDRM-ND for the RTP Media Transport.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	WMDRM-ND	YKV4V	A

[COMMENT] Content Receivers and Content Sources that implement WMDRM-ND, and also support the optional RTP Media Transport, are recommended to extend their support for WMDRM-ND to include the RTP Media Transport.

The guidelines on how WMDRM-ND is used with RTSP and RTP are stated in 9.6.2.

9.2.3.2

[GUIDELINE] Content Receivers that implement WMDRM-ND for the RTP Media Transport shall adhere to the guidelines defined in.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	WMDRM-ND	89TV8	A

9.2.3.3

[GUIDELINE] Content Sources that implement WMDRM-ND and that support the RTP Media Transport for non-link-protected content should implement WMDRM-ND for the RTP Media Transport.

[ATTRIBUTES]

S	A	DMS +PU+	M-DMS	n/a	WMDRM-ND	KV4VE	

9.2.3.4

[GUIDELINE] Content Sources that implement WMDRM-ND for the RTP Media Transport shall adhere to the guidelines defined in 9.6.2.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	WMDRM-ND	Q89TV	

9.2.4 CP WMDRM-ND: Registration and Revalidation procedures

9.2.4.1

[GUIDELINE] Content Receivers that implement WMDRM-ND shall implement the mapping of the WMDRM-ND Registration and Revalidation procedures to UPnP, as defined in the section entitled "Registration Using UPnP" in WMDRM-ND.

[ATTRIBUTES]

M	R	DMP DMR	M-DMP	n/a	WMDRM-ND	9TV86	A

[COMMENT] The WMDRM-ND Registration procedure allows the Content Source to uniquely identify the Content Receiver. It also allows the Content Source to discover Content Receivers that do not otherwise announce their presence on the network (e.g., by sending ssdp:alive messages.)

Content Receivers invoke the RegisterDevice action of the X-MS_MediaReceiverRegistrar:1 service (defined in WMDRM-ND) on the Content Source as part of the WMDRM-ND Registration procedure.

This guideline also applies to the DMR Device Class.

9.2.4.2

[GUIDELINE] Content Sources that implement WMDRM-ND shall implement the mapping of the WMDRM-ND Registration and Revalidation procedures to UPnP, as defined in the section entitled "Registration Using UPnP" in WMDRM-ND.

[ATTRIBUTES]

M	R	DMS +PU+	M-DMS	n/a	WMDRM-ND	4VEJX	

[COMMENT] The WMDRM-ND Registration procedure is to be completed successfully before a Content Source is allowed to deliver content (using any Media Transport) to a Content Receiver.

9.2.4.3

[GUIDELINE] A Content Source that implements WMDRM-ND shall expose the X-MS_MediaReceiverRegistrar:1 service as one of the services offered by the device.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	WMDRM-ND	TV86M	

[COMMENT] The mapping of the WMDRM-ND Registration and Revalidation procedures to UPnP requires implementing the X-MS_MediaReceiverRegistrar:1 service. This service is implemented on the UPnP Content Source device and invoked by the Content Receiver. A Push Controller needs to implement a UPnP device in order to expose the service if it is combined with a DLNA device class that does not require a UPnP device.

9.2.4.4

[GUIDELINE] A Content Receiver that implements WMDRM-ND shall implement an X-MS_MediaReceiverRegistrar:1 service control point.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	WMDRM-ND	V4VEJ	A

9.2.5 CP WMDRM-ND: discovery of Content Receivers

[GUIDELINE] Content Sources that implement WMDRM-ND shall perform the WMDRM-ND Authorization procedure defined in the "Authorization" section of WMDRM-ND before starting the transfer of a content binary to a Content Receiver, and shall not transfer content binaries to a Content Receiver which has not been authorized.

[ATTRIBUTES]

M	R	DMS +PU+	M-DMS	n/a	WMDRM-ND	WAWIF	

[COMMENT] Content Sources can discover Content Receivers by listening for ssdp:alive messages or through the optional mapping of the WMDRM-ND Authorization procedure to UPnP. DMRs are required to send ssdp:alive messages, and can be discovered that way. If a Content Receiver chooses to invoke the *IsAuthorized* UPnP action (part of the mapping of the WMDRM-ND Authorization procedure to UPnP), then this also allows the Content Source to discover the Receiver. Content Receivers that do not send ssdp:alive messages (such as DMPs) might not be discovered until they perform the WMDRM-ND Registration procedure.

9.3 Networking and connectivity

9.3.1 General

Subclause 9.3 contains the guidelines that are specific to WMDRM-ND use of the networking capabilities described in Clause 8 of IEC 62481-1-1:2017.

9.3.2 CP WMDRM-ND: QoS guidelines

[GUIDELINE] If DLNA QoS as defined in Clause 8 of IEC 62481-1-1:2017 is implemented, all WMDRM-ND Proximity Detection messages shall be tagged as DLNAQOS_3, or a lower DLNAQOS_UP value, in accordance with Table 7 of IEC 62481-1-1:2017.

[ATTRIBUTES]

M	A	MHS	HND	n/a	IEC 62481-1-1: 2017	AWIFT	

[COMMENT] Proximity Detection messages are used to measure the round trip time between the Content Source and the Content Receiver. Allowing DLNAQOS_3 for such messages reduces the likelihood that other network traffic will skew the round trip time measurement.

9.4 Device discovery and control

9.4.1 General

This subclause covers the guidelines for implementing device discovery and control using the UPnP device architecture that are specific to the WMDRM-ND Link Protection System. For detailed information, see Clause 9 of IEC 62481-1-1:2017.

9.4.2 CP WMDRM-ND: additional rules for DMRs

[GUIDELINE] If WMDRM-ND is supported by a DMR, then its implementation of the control point for the X-MS_MediaReceiverRegistrar:1 service shall comply with all guidelines in Clause 9 of IEC 62481-1-1:2017 for the DMP device class.

[ATTRIBUTES]

M	A	DMR	n/a	n/a	IEC 62481-1-1: 2017	CKL6L	

[COMMENT] DMRs are required to invoke the RegisterDevice action of the X-MS_MediaReceiverRegistrar:1 service (defined in Appendix 1 of WMDRM-ND) on the Content Source as part of the WMDRM-ND Registration procedure.

This means that the DMR is a UPnP control point for the X-MS_MediaReceiverRegistrar:1 service. Clause 9 of IEC 62481-1-1:2017 specifies rules for UPnP control points. These guidelines also apply to the implementation of the X-MS_MediaReceiverRegistrar:1 control point.

9.5 Media management

There are no WMDRM-ND specific changes to the guidelines in Clause 10 of IEC 62481-1-1:2017.

9.6 Media Transport

9.6.1 HTTP transport

9.6.1.1 General

This subclause covers the guidelines for implementing media transport using the UPnP AV architecture that are specific to the WMDRM-ND Link Protection System. The guidelines in this subclause apply only to DLNA devices that implement WMDRM-ND.

9.6.1.2 CP WMDRM-ND: HTTP support

9.6.1.2.1

[GUIDELINE] When using the WMDRM-ND Link Protection System, HTTP Client Endpoints shall implement the mapping of WMDRM-ND to HTTP as specified in the "HTTP Mappings" subclause of WMDRM-ND.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	WMDRM-ND	KL6LR	A

[COMMENT] HTTP Client Endpoints and HTTP Server Endpoints that implement WMDRM-ND and use the HTTP Media Transport have to follow the rules for how WMDRM-ND is used with HTTP. Those rules are defined in the subclause called "HTTP Mappings" in the WMDRM-ND specification WMDRM-ND.

9.6.1.2.2

[GUIDELINE] When using the WMDRM-ND Link Protection System, HTTP Server Endpoints shall implement the mapping of WMDRM-ND to HTTP as specified in the "HTTP Mappings" subclause of WMDRM-ND.

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a		6HW6W	

9.6.1.3 CP WMDRM-ND: Media Format Profiles that use ASF when using HTTP

[GUIDELINE] When using the WMDRM-ND Link Protection System with the HTTP media transport, a DLNA Endpoint transferring a content binary that uses ASF encapsulation shall follow the rules listed below.

- The rules in the "Data Transfer" subclause of WMDRM-ND.
- The rules in the subclause entitled "Rules Common to All Content" in the "Data Transfer Using HTTP" subclause of WMDRM-ND.
- The rules in the subclause entitled "Windows Media-based Content" in the "Data Transfer Using HTTP" subclause of WMDRM-ND.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	IEC 62481-2:2017 WMDRM-ND	E369K	A

[COMMENT] Content encapsulated in ASF uses ASF Sample Encryption (defined in WMDRM-ND). It involves adding the Advanced Encryption Object in the ASF file header, and including a Sample ID ASF packet extension in each encrypted ASF packet.

Media Format Profiles that use ASF encapsulation are defined in IEC 62481-2:2017.

Examples of such profiles include the WMA profiles in 8.7 of IEC 62481-2:2017 and the WMV9 profiles in 9.7 of IEC 62481-2:2017, and all profiles whose name starts with MPEG4_PS_ASF_.

9.6.1.4 CP WMDRM-ND: MPEG-2 Transport Stream content when using HTTP

[GUIDELINE] When using the WMDRM-ND Link Protection System with the HTTP Media Transport, a DLNA Endpoint transferring a content binary that uses MPEG-2 Transport Stream shall follow the rules listed below.

- The rules in the "Data Transfer" subclause of WMDRM-ND.
- The rules in the subclause entitled "Rules Common to All Content" in the "Data Transfer Using HTTP" subclause of WMDRM-ND.
- The rules in the subclause entitled "MPEG-2 Transport Stream Content" in the "Data Transfer Using HTTP" subclause of WMDRM-ND.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	IEC 62481-2:2017 WMDRM-ND	HW6WF	A

[COMMENT] For content that uses MPEG-2 Transport Stream encapsulation, additional MPEG-2 Transport Packets, called TAG packets, are inserted in front of each protected PES packet in the Transport Stream.

Media Format Profiles that use MPEG-2 Transport Stream encapsulation are defined in IEC 62481-2:2017.

For example, all profiles with names starting with MPEG_TS_, MPEG4_PS_TS_ and AVC_TS_ use MPEG-2 Transport Stream.

9.6.1.5 CP WMDRM-ND: Link Encryption Mode when using HTTP

[GUIDELINE] When using the WMDRM-ND Link Protection System with the HTTP Media Transport, a DLNA Endpoint transferring a content binary that does not use ASF or MPEG-2 Transport Stream encapsulation shall follow the rules listed below.

- The rules in the "Data Transfer" subclause of WMDRM-ND.
- The rules in the subclause entitled "Rules Common to All Content" in the "Data Transfer Using HTTP" subclause of WMDRM-ND.
- The rules in the subclause entitled "Other Content Types" in the "Data Transfer Using HTTP" subclause of WMDRM-ND.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	IEC 62481-2:2017 WMDRM-ND	VE369	A

[COMMENT] In this case, the WMDRM-ND Link Encryption Mode is used. It is defined in the "Link Encryption Mode" subclause of WMDRM-ND. The Content Source partitions the content binary into an arbitrary number of data segments. Each data segment is encrypted independently and transmitted together with a Data Segment Descriptor (defined in WMDRM-ND.)

9.6.1.6 CP WMDRM-ND: Link Protection Alignment Element when using HTTP

[Guideline] When using the WMDRM-ND Link Protection System with the HTTP Media Transport, a Link Protection Alignment Element is defined as follows.

- For ASF Sample Encryption: An ASF packet or the ASF file header.
- For content that use MPEG-2 Transport Stream: A MPEG-2 TS packet.
- For content that use the WMDRM-ND Link Encryption Mode: The framing header defined in the "HTTP Framing Headers" subclause of WMDRM-ND] followed by the number of bytes indicated in the framing header.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	IEC 62481-2:2017 WMDRM-ND	DM2LQ	A

[COMMENT] IEC 62481-2:2017 defines which media format profiles use MPEG-2 Transport Stream.

9.6.1.7 CP WMDRM-ND: Cleartext Byte Seek Request Header

9.6.1.7.1

[Guideline] When using the WMDRM-ND Link Protection System, HTTP Client and Server endpoints shall use the Cleartext-Range.dlna.org header as the Cleartext Byte Seek Request Header.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	N/A	M2LQ7	A

9.6.1.7.2

[GUIDELINE] The notation of the Cleartext-Range.dlna.org header field for HTTP Media Transport of WMDRM-ND link protected content shall be as stated below:

- Cleartext-Range.dlna.org = "Cleartext-Range.dlna.org" ":" range-specifier
- range-specifier = byte-range-specifier
- byte-range-specifier = bytes-unit "=" byte-range-set
- bytes-unit = "bytes"
- byte-range-set = byte-range-spec
- byte-range-spec = first-cleartextbyte-pos "-" [last cleartextbyte pos]
- first-cleartextbyte-pos = 1*DIGIT
- last-cleartextbyte-pos = 1*DIGIT

first-cleartextbyte-pos and last-cleartextbyte-pos apply to the Cleartext Byte Domain, the content binary immediately before WMDRM-ND processing, i.e. before encryption.

Note that the literal "bytes" is case sensitive.

EXAMPLE 1

Cleartext-Range.dlna.org: bytes=1 539 686 400 –

EXAMPLE 2

Cleartext-Range.dlna.org: bytes=1 539 686 400 – 1 540 210 688

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	n/a	7U7QO	A

9.6.1.8 CP WMDRM-ND: Cleartext Byte Seek Response Header

9.6.1.8.1

[GUIDELINE] When using the WMDRM-ND Link Protection System, HTTP Client and Server endpoints shall use the Cleartext-Content-Range.dlna.org header as the Cleartext Byte Seek Response Header.

[ATTRIBUTES]

M	A	DMS DMP DMR +PU+	M-DMP M-DMS	n/a	n/a	3EYAO	A

9.6.1.8.2

[GUIDELINE] The notation of the Cleartext-Content-Range.dlna.org header field for DLNA media transport is as stated below:

- Cleartext-Content-Range.dlna.org = "Cleartext-Content-Range.dlna.org" ":" content-range-spec
- content-range-spec = byte-content-range-spec
- byte-content-range-spec = bytes-unit SP byte-range-resp-spec "/" (instance-length | "*")
- bytes-unit = "bytes"
- byte-range-resp-spec = first-cleartextbyte-pos "-" last-cleartextbyte-pos

- first-cleartextbyte-pos = 1*DIGIT
- last-cleartextbyte-pos = 1*DIGIT
- instance-length = 1*DIGIT

first-cleartextbyte-pos, last-cleartextbyte-pos and instance-length apply to the Cleartext Byte Domain, the content binary immediately before WMDRM-ND processing, i.e. before encryption.

Note that the literal "bytes" is case sensitive.

Example:

Cleartext-Content-Range.dlna.org: bytes 1539686400-1540210688/9238118400M

[ATTRIBUTES]

M	A	DMS +PU+	M-DMS	n/a	n/a	2J344	

[COMMENT] The positions specified in this header refer to positions in the *Cleartext Byte Domain*.

9.6.1.9 CP WMDRM-ND: HTTP Trickmodes

9.6.1.9.1

[GUIDELINE] For every content binary using the WMDRM-ND Link Protection System, if a streaming HTTP Client Endpoint performs a Seek media operation, then the HTTP Client Endpoint shall support a Seek media operation using the TimeSeekRange.dlna.org header field.

[ATTRIBUTES]

M	A	DMP DMR	M-DMP	n/a	n/a	WGDS3	E

[COMMENT] Refer to IEC 62481-1-1:2017, 11.4.3.44 (GUNs 9I4UN and PHT47).

9.6.1.9.2

[GUIDELINE] For every content binary using the WMDRM-ND Link Protection System, if a streaming HTTP Client Endpoint performs a Seek media operation, then the HTTP Client Endpoint should support the following Seek media operation methods:

- the RANGE,header field;
- Cleartext-Range.dlna.org header field.

[ATTRIBUTES]

S	A	DMP DMR	M-DMP	n/a	n/a	TX5AK	A

[COMMENT] Refer to IEC 62481-1-1:2017, 11.4.3.44 (GUNs 9I4UN and PHT47).

9.6.1.9.3

[GUIDELINE] For every AV content binary using the WMDRM-ND Link Protection System that supports "Limited Random Access Data Availability" Mode 1 or "Full Random Access Data Availability" Model (see IEC 62481-1-1:2017, 11.4.2.16 for details on mode), an HTTP Server Endpoint shall indicate support in the fourth field of the ProtocolInfo for time-based seek.