

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Lignes directrices pour l'interopérabilité des dispositifs domestiques DLNA
(Digital Living Network Alliance) –
Partie 3: Protection des liaisons**

WATERMARK



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2010 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
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.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you 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It also gives information on projects, replaced and withdrawn publications.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 on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

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.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

**Lignes directrices pour l'interopérabilité des dispositifs domestiques DLNA
(Digital Living Network Alliance) –
Partie 3: Protection des liaisons**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XB

ICS 33.100; 35.100.05; 35.110

ISBN 978-2-83220-366-8

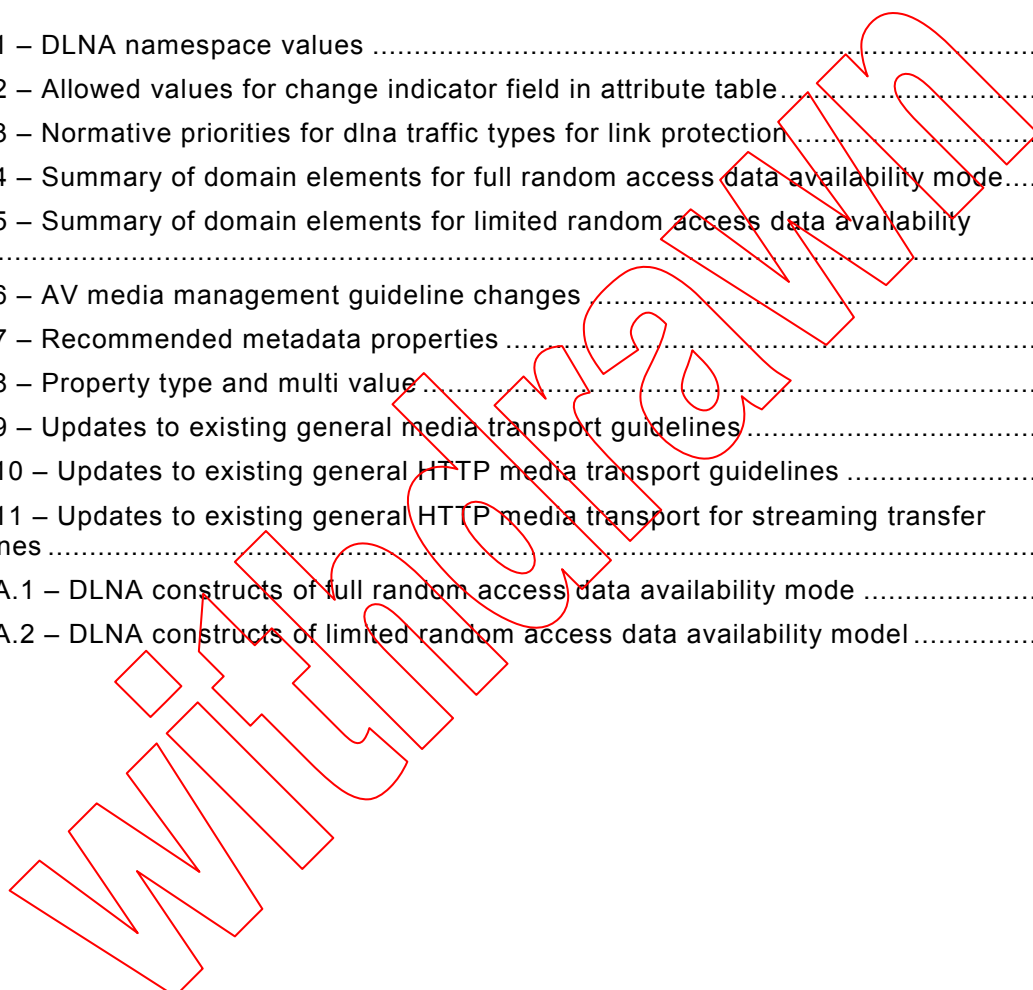
**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	5
1 Scope.....	7
2 Normative reference.....	7
3 Terms, definitions and acronyms.....	8
3.1 Terms and definition.....	8
3.2 Abbreviation terms.....	12
4 DLNA home network architecture.....	13
5 DLNA device model.....	13
6 Guideline terminology and conventions.....	13
6.1 Guideline compliance classifiers.....	13
6.2 Standard of specification usage classifiers.....	13
6.3 Guideline font usage conventions.....	14
6.4 Guideline syntax notation convention.....	14
6.5 Guideline normative and informative text conventions.....	15
6.6 DLNA XML namespaces and schemas.....	15
7 Common link protection guidelines.....	15
7.1 General.....	15
7.2 Conditions for measuring time in message exchanges.....	18
7.3 Networking and connectivity.....	18
7.3.1 General.....	18
7.3.2 New general capability requirements – Bluetooth NC CP – Power saving modes.....	18
7.4 Device discovery and control.....	19
7.5 Media management.....	19
7.5.1 Media management – AV media management.....	19
7.5.2 AV media management guidelines.....	22
7.6 Media transport.....	25
7.6.1 General.....	25
7.6.2 Media transport protocols.....	25
7.6.3 HTTP transport.....	27
7.6.4 HTTP media transport for streaming transfer guidelines.....	34
7.6.5 HTTP media transport for interactive transfer guidelines.....	34
7.6.6 RTP transport.....	35
7.7 Content conversion device virtualization.....	36
7.8 Media interoperability unit (MIU).....	36
7.9 Link protection technology guidelines requirements.....	36
7.9.1 Link protection system – DTCP-IP.....	36
7.9.2 Link protection system – Windows media DRM for network devices.....	37
8 DTCP-IP link protection system guidelines.....	37
8.1 General.....	37
8.2 Networking and connectivity.....	37
8.2.1 Networking and connectivity – General capability requirements.....	37
8.2.2 New DLNAQOS requirements QoS requirement for DTCP-IP traffic.....	38
8.2.3 New device requirements – Common NC CP – Wireless security.....	38
8.3 Device discovery and control.....	38
8.4 Media management.....	38

8.4.1	Media management – AV media management	38
8.4.2	MM CP – DTCP-IP URI.....	38
8.5	Media transport	39
8.5.1	HTTP transport.....	39
8.5.2	RTP transport.....	40
8.6	Content conversion device virtualization.....	42
8.7	Media interoperability unit (MIU).....	42
8.8	Media format – DTCP-IP profiling guidelines	42
8.8.1	General	42
8.8.2	CP DTCP-IP – Profile	42
8.8.3	CP DTCP-IP – Profile MIME type definition.....	43
8.8.4	CP DTCP-IP – Profile protected and unprotected content portions.....	44
8.8.5	CP DTCP-IP – Profile HTTP encapsulation.....	45
8.8.6	DTCP-IP profile encapsulation.....	45
8.9	General requirements.....	47
8.9.1	General	47
8.9.2	CP DTCP-IP – Requirements.....	47
9	WMDRM-ND link protection system guidelines	47
9.1	General.....	47
9.2	General requirements.....	48
9.2.1	General	48
9.2.2	CP WMDRM-ND – Requirements.....	48
9.2.3	CP WMDRM-ND – Support for HTTP.....	48
9.2.4	CP WMDRM-ND – Support for RTP.....	48
9.2.5	CP WMDRM-ND – Registration and revalidation procedures	49
9.2.6	CP WMDRM-ND – Discovery of content receivers	49
9.3	Networking and connectivity.....	50
9.3.1	Networking and connectivity – General capability requirements	50
9.3.2	CP WMDRM-ND – QoS requirements	50
9.4	Device discovery and control.....	50
9.4.1	General	50
9.4.2	CP WMDRM-ND – Additional rules for DMRs.....	50
9.5	Media management.....	50
9.6	Media transport.....	51
9.6.1	HTTP transport.....	51
9.6.2	RTP transport.....	54
9.7	Content conversion device virtualization.....	56
9.8	Media interoperability unit (MIU).....	56
9.9	Media format – WMDRM-ND profiling guidelines	56
9.9.1	General	56
9.9.2	CP WMDRM-ND – Identification of content transferred using WMDRM-ND.....	56
9.9.3	CP WMDRM-ND – Media format requirements.....	57
9.9.4	CP WMDRM-ND – MIME type.....	57
9.9.5	CP WMDRM-ND – Decoder friendly alignment position.....	57
9.9.6	CP WMDRM-ND – Media format alignment element.....	57
Annex A (informative)	An introduction to DLNA seek operations	58
Bibliography.....		67

Figure 1 – Guideline layout and definitions	16
Figure 2 – Visual map of possible values for the attribute tables	17
Figure A.1 – UCDAM definitions for seek operations	59
Figure A.2 – Full random access data availability model	60
Figure A.3 – Limited random access data availability model mode 0	62
Figure A.4 – Limited random access data availability mode 1	63
Figure A.5 – Content flow unprotected content	65
Figure A.6 – Content flow link protected content	65
Table 1 – DLNA namespace values	15
Table 2 – Allowed values for change indicator field in attribute table	17
Table 3 – Normative priorities for dlina traffic types for link protection	18
Table 4 – Summary of domain elements for full random access data availability mode	20
Table 5 – Summary of domain elements for limited random access data availability model	21
Table 6 – AV media management guideline changes	22
Table 7 – Recommended metadata properties	23
Table 8 – Property type and multi value	23
Table 9 – Updates to existing general media transport guidelines	26
Table 10 – Updates to existing general HTTP media transport guidelines	27
Table 11 – Updates to existing general HTTP media transport for streaming transfer guidelines	34
Table A.1 – DLNA constructs of full random access data availability mode	61
Table A.2 – DLNA constructs of limited random access data availability model	64



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 by technical area 9: Audio, video and multimedia applications for end-user network, of IEC technical committee 100: Audio, video and multimedia systems and equipment.

This bilingual version (2012-11) corresponds to the monolingual English version, published in 2010-11.

The text of this standard is based on the following documents:

CDV	Report on voting
100/1617/CDV	100/1739/RVC

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

The French version of this standard has not been voted upon.

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

A list of all parts of the 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 publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

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

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.

Withdrawn

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

Part 3: Link protection

1 Scope

This part of IEC 62481 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 standard.

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 standard reference existing technologies for link protection and provide mechanisms for interoperability between different implementations as well as integration with the DLNA architecture.

This standard is organized to align with the overall structure of IEC 62481-1 and IEC 62481-2.

2 Normative reference

The following referenced documents are indispensable for the application 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 62481-1:2007, *Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 1: Architecture and protocols*

IEC 62481-2:2007, *Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 2: DLNA media formats*

ISO/IEC 13818-1:2007, *Information technology – Generic coding of moving pictures and associated audio information: Systems*

ISO/IEC 13818-2:2007, *Information technology – Generic coding of moving pictures and associated audio information: Video*

ISO/IEC 14496-2:2004 *Information technology – Coding of audio-visual objects – Part 2: Visual*

Amendment 1 (2004), *Error resilient simple scalable profile*

ISO/IEC 29341-3-10:2008, *Information technology – UPnP device architecture – Part 3-10: Audio video device control protocol – Audio video transport service*

ISO/IEC 29341-3-11:2008, *Information technology – UPnP device architecture – Part 3-11: Audio video device control protocol – Connection manager service*

ISO/IEC 29341-3-12:2008, *Information technology – UPnP device architecture – Part 3-12: Audio video device control protocol – Content directory service*

DTCP Volume 1 (informational version), *Digital transmission content protection specification*
Volume 1, Revision 1.4: February 28, 2005
http://www.dtcp.com/data/info/20050228_dtcp_vol_1_1p4.pdf

DTCP Volume 1 Supplement E (informational version)
Mapping DTCP to IP, Revision 1.1: February 28, 2005
http://www.dtcp.com/data/info/20050228_dtcp_VISE_1p1.pdf

DTCP Audio Compliance Rules EXHIBIT B-2:
Compliance rules for licensed products that receive or transmit commercial audio works,
June 2002
http://www.dtcp.com/data/Compliance_Rules_Audio_020610.pdf

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*

3 Terms, definitions and acronyms

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

3.1 Terms and definition

3.1.1

authentication and key exchange

AKE

step in a link protection system where the receiving device is authenticated and given the correct keys for the content

3.1.2

advanced system format

ASF

media format encapsulation for the transmission of content

3.1.3

audio with video

AV

any media content that contains both moving picture and sound

3.1.4

AV transport

AVT

UPnP service that provides network-based control for common transport operations such as play, stop, pause, next, previous, and seek, a standard UPnP DCP

3.1.5

cleartext

unencrypted 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 for a complete explanation of seek operations on link protected content, see Annex A

3.1.7**cleartext byte seek request header**

used to signify any of those transport layer request headers; implies that the guideline applies to all uses of any of the request headers

3.1.8**cleartext byte seek response header**

used to signify any of those transport layer response headers; implies that the guideline applies to all uses of any of the request headers

3.1.9**connection manager service****CMS**

UPnP service that provides information about the supported transport protocols and media formats of a UPnP device, a standard UPnP DCP

3.1.10**contributing source****CSRC**

source used for the RTP media transport

3.1.11**decoder friendly alignment position**

position in the bitstream defined for decoder friendly alignment; always the start of a media format alignment element that can begin to process data without any other internal state information about the stream so that the decoder can begin processing at that point and create a valid output rendering

3.1.12**digital living network alliance****DLNA**

organization that originally developed this standard

3.1.13**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

3.1.14**DLNA QoS user priority****DLNAQOS_UP**

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

3.1.15**digital transmission content protection****DTCP**

one of the link protection system

3.1.16**digital transmission content protection over IP networks****DTCP-IP**

DTCP as applied IP based network

3.1.17

group of pictures

GOP

defined grouping of information in the MPEG 2 media format

3.1.18

hyper text transfer protocol

HTTP

protocol for transferring files across the Internet

NOTE Requires an HTTP client program on one end, and an HTTP server program on the other end.

3.1.19

link protection alignment element

unit of content carried within a link protected content stream starts with a packet header that is defined by the link protection system and contains bytes of the link protected stream

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 system

specific collection of technologies with corresponding rules that enable secure content transfer between two endpoints

3.1.22

media format alignment element

unit of content carried within an unprotected content stream, 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

3.1.23

multipurpose internet mail extension

MIME

standard system for identifying the type of data contained in a file

NOTE 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.

3.1.24

network byte domain

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

NOTE For content binaries that use a link protection system, this will include encryption and any necessary headers or padding required by the link protection system.

3.1.25

network connectivity – power saving

NC-PS

power saving modes of operations, as defined in IEC 62481-1

3.1.26

protected content packet

PCP

packet format for DTCP-IP link protected content, as defined in DTCP Volume 1 and DTCP Volume 1 Supplement E

3.1.27**program stream****PS**

content binary stream usually in reference to an MPEG-2 AV stream format

3.1.28**real time protocol****RTP**

media transport that provides end-to-end network transport functions for transmitting real-time data, such as AV

NOTE It provides services such as payload type identification, sequence numbering, time-stamping, and delivery monitoring.

3.1.29**real time streaming protocol****RTSP**

protocol within the RTP protocol suite

3.1.30**round trip time****RTT**

time between sending a network packet to a remote host and the time that the response is received

3.1.31**session description protocol****SDP**

protocol within the RTP protocol suite

3.1.32**simple object access protocol****SOAP**

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**transport stream****TS**

content binary stream usually in reference to an MPEG-2 AV stream format

3.1.35**uniform client data availability model****UCDAM**

model for representing which bytes of a content binary are available on a server for seek operations

NOTE See 7.5 of IEC 62481-1 for a full definition.

3.1.36**UPnP**

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

NOTE 1 See ISO/IEC 29341-1 for architecture description.

NOTE 2 It 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. It 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

uniform resource identifier

URI

W3C's codification of the name and address syntax of present and future objects on the Internet

NOTE 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

video object unit

VOBU

defined grouping of information in the MPEG 2 media format

3.1.39

wired equivalency privacy

WEP

wireless privacy standard used in conjunction with IEEE 802.11 networks

3.1.40

Windows media audio

WMA

audio compression binary format

3.1.41

Windows media DRM for network device

WMDRM-ND

one of the link protection system

3.1.42

Windows media video

WMV

AV compression binary format

3.1.43

WiFi protected access

WPA

system to secure a wireless IEEE 802.11 network

3.1.44

WiFi protected access version 2

WPA2

system to secure a wireless IEEE 802.11 network version 2

3.2 Abbreviation terms

BNF	Backus Naur Form
LWS	Linear WhiteSpace
MPEG-2	Moving Picture Experts Group phase 2
MIU	Media Interoperability Unit
MTU	Maximum Transmission Unit

UCDAM	Uniform Content Data Availability Model
UPnP	Universal Plug and Play
W3C	World Wide Web Consortium

4 DLNA home network architecture

Refer to IEC 62481-1, Clause 4 for detailed descriptions of the DLNA home networking architecture.

5 DLNA device model

Refer to IEC 62481-1, Clause 5 for detailed descriptions of the DLNA home networking architecture. This standard 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 the 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

6.1 Guideline compliance classifiers

Reference [9]¹ provides a description of terminology conventions used in all IETF RFC documents. The terminology and conventions used by the DLNA home networked device interoperability guidelines are adapted from this reference. The details of each guideline will carry a compliance classifier from the following set.

[M]ust, Required, Shall: This is the minimum set of requirements that will ensure interoperability and/or robust operation between devices. All devices are expected to comply with these requirements when expressed in unconditional form. A conditional requirement expressed in the form, "If X, then Y shall be implemented", means that the requirement "Y" shall be met when the conditional aspect "X" applies to a given implementation.

[S]hould, Recommended: Recommended items are optional items that are strongly recommended for inclusion in products. The difference between "recommended" items and "optional" items, see below, is one of priority. When considering features for inclusion in a product, recommended items should be included first.

[O]ptional, May: Optional items are suggestions for features that will enhance the user experience or are offered as a less preferred choice relative to another recommended feature. If optional features are included, they shall comply with the requirement to ensure interoperability with other implementations.

6.2 Standard of specification usage classifiers

When specifying guideline details, it is often useful to reiterate or clarify certain aspects of a standard or specification that are often violated or misunderstood. Furthermore, there may be guideline requirements that intentionally contradict or restrict implementation of certain

¹ Figures in square brackets refer to the Bibliography.

aspects of a standard or specification in order to ensure interoperability between DLNA devices. The following classifiers are used in the DLNA home networked device interoperability guidelines to indicate the relationship of a specific guideline requirement to a source standard or specification:

[A]dding: A guideline requirement that adds to or supplements a standard or specification to enhance interoperability. A guideline requirement that does not reference a standard or specification also uses this classifier.

[C]larifying: A guideline requirement that addresses vague or ambiguous aspects of a standard or specification.

[F]ixing: A guideline requirement that intentionally supersedes and fixes aspects of a standard or specification that is incorrect and would otherwise provide a poor user experience or prevent device interoperability.

[L]imiting: A guideline requirement that narrows or specifies an exact behavior in areas where a standard or specification provides for greater degrees of latitude in implementation.

[R]epeating: A guideline requirement that repeats what is already in a standard or specification because of observed and repeated problems with implementations. Whenever a guideline requirement with this usage classifier seems to be in conflict with the actual standard, the standard prevails over the guideline requirement.

6.3 Guideline font usage conventions

The following font usage conventions are used within the DLNA home networked device interoperability guidelines to provide additional clarity.

- Hyperlinks to reference citations are indicated as [number]. For example [1], [20], ...
- HTTP headers and methods are always in bold font, such as CACHE-CONTROL.
- UPnP action names are indicated as: [Service acronym]:[action name], such as CDS: Browse.
- Special terms may be *italicized*. Sometimes a guideline requirement will define a term for use within that guideline and the term will be *italicized*.

6.4 Guideline syntax notation convention

The following are syntax (BNF) notation conventions used within the DLNA home networked device interoperability guidelines to provide readability.

- Linear whitespace (LWS) characters, such as carriage returns, spaces, tabs, or line feeds, are not implied anywhere in any of the syntax (BNF) definitions used within the interoperability guidelines.
- The use of LWS characters is restricted within the DLNA interoperability guideline unless explicitly specified in any of the syntax definitions with reference to UPnP HTTP communications.
- By default, text tokens and values have a case-sensitive treatment unless explicitly noted in the guidelines. This convention also applies to BNF definitions, XML tag names, XML tag values, capability IDs, and HTTP header values for HTTP headers used by the DLNA guidelines. One of the exceptions to this rule applies to the names of HTTP headers. HTTP header names have a case-insensitive treatment. For example TimeSeekRange.dlna.org is the same as timeseekrange.dlna.org. (See IEC 62481-1, 7.5.5.2.6). Other exceptions are described in each guideline which define BNF syntax.

6.5 Guideline normative and informative text conventions

All text that appears in the DLNA interoperability guidelines is to be considered normative unless explicitly stated otherwise, such as informative references and informative appendices. Normative text includes introductory text before guideline requirement tables, but testable requirements are only contained within guideline requirement table entries.

6.6 DLNA XML namespaces and schemas

The DLNA interoperability guidelines make numerous references to XML elements and attributes that are defined for DLNA device classes and device capabilities. However, these namespaces are intentionally not defined through a formal DLNA XML schema. This allows the DLNA interoperability guidelines to define new XML elements and attributes in the future, without having to define a new namespace or schema definition. DLNA devices classes and device capabilities are expected to exhibit tolerant behavior when encountering XML elements or attributes that are defined in the future, as required by existing IEC 62481-1, 7.3.24 and 7.4.1.3.1. Table 1 lists the namespace values that are used by DLNA guidelines and the context for their usage.

Table 1 – DLNA namespace values

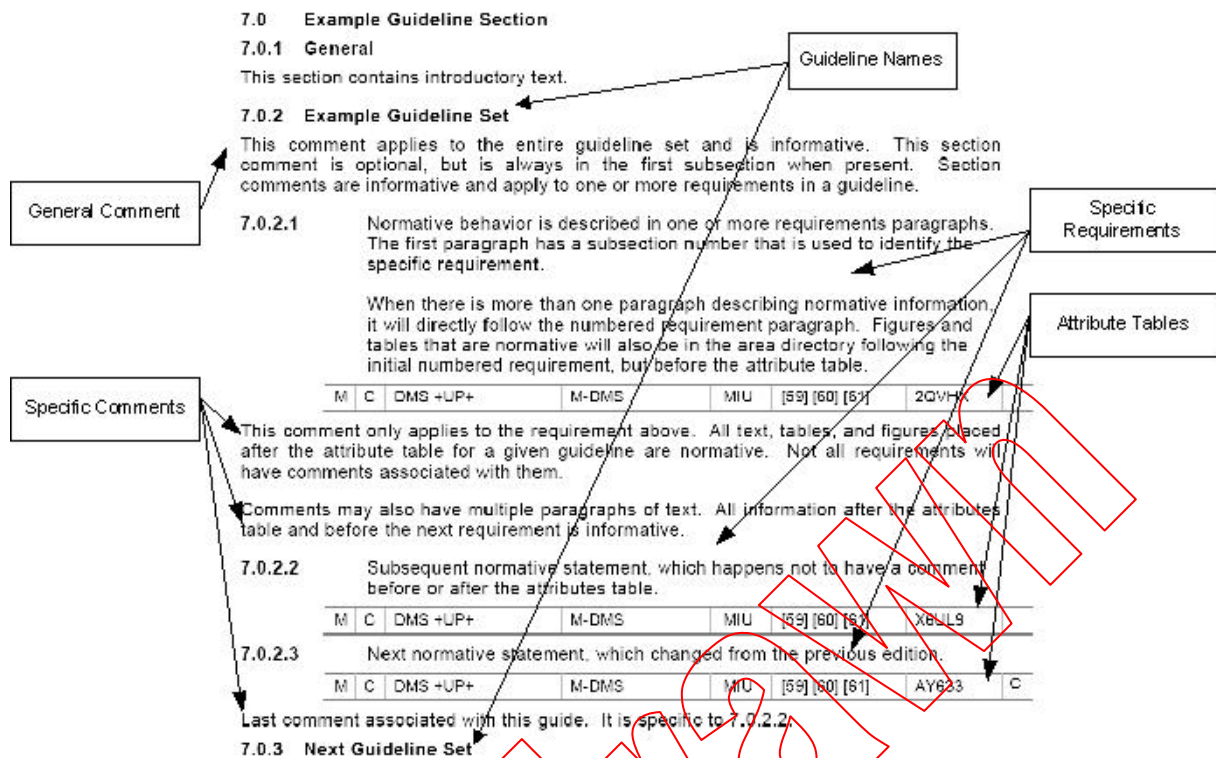
Namespace value	Usage context
urn:schemas-dlna-org:device-1-0	Used for XML elements and attributes defined by DLNA interoperability guidelines for use in UPnP device description files.
urn:schemas-dlna-org:metadata-1-0/	Used for XML elements and attributes defined by DLNA interoperability guidelines for use in DIDL-Lite documents and fragments.

7 Common link protection guidelines

7.1 General

This subclause contains the guidelines that are independent of the underlying link protection system. Subclauses 7.3 through 7.8 relate to the corresponding Subclauses 7.2 to 7.7 in IEC 62481-1. Subclause 7.9 contains information not related to that part and should be read first to provide context for 7.3 through 7.8.

These guidelines are in a clause/subclause format as shown in Figure 1.



IEC 2344/10

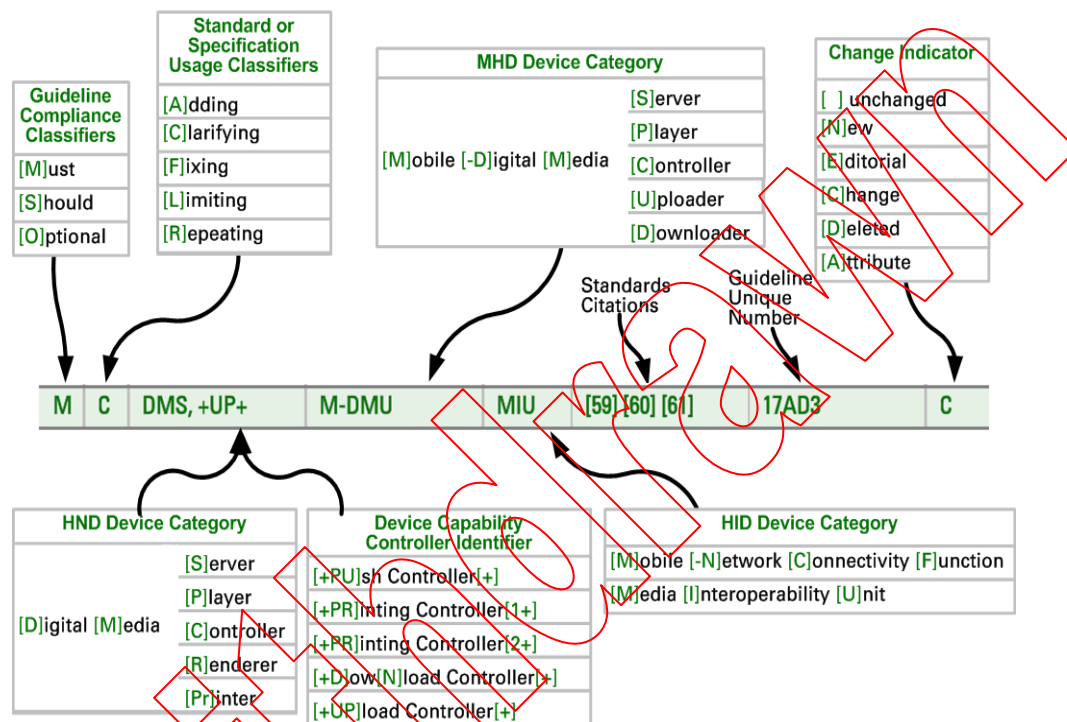
Figure 1 – Guideline layout and definitions

The following list describes the content of Figure 1.

- Name:** A unique label for the guideline. The label is preceded with a sequentially increasing number to allow easy lookup.
- Requirements:** The actual description of a guideline. A guideline is preceded with a sequentially increasing number in each volume to allow easy lookup.
- Attribute table:** A summary of the essential attributes of a requirement. The table is a single row with the following definitions for the columns.
 - Compliance classifier: M/S/O (See 6.1 for the definition of guideline compliance classifiers).
 - The specification usage classifier: A/C/F/L/R: for the guideline. (See 6.2 for the definition of specification usage classifiers.)
 - HND device classes with device capabilities (see Table 2 and Table 3 of IEC 62481-1 for definitions). Device capabilities listed in the HND column of the attribute table. Device capabilities can also apply equally to the MHD device category but have been omitted from the MHD column in the attribute table to provide for better readability.
 - MHD device classes (see Table 4 of IEC 62481-1 for definitions).
 - HID device classes (see Table 5 of IEC 62481-1 for definitions).
 - Standards citation: Standards that are referenced by the guideline. Standards citations are by number and are referenced in Clause 2.
 - Guideline unique number: an alpha-numeric string that uniquely identifies a requirement.
 - Change indicator: documents the change in the requirement that occurred since the last edition of the guideline (see Table 2 for definitions).

- Guideline attribute columns that do not have a value have the designation "n/a" (not applicable). A visual map of possible values for the attribute tables is in Figure 2.
- d) Comment: Supplementary information about a guideline such as a justification for the guideline, the specific interoperability issue that is addressed, etc.

Note that many guidelines do not explicitly list MIU since guidelines which apply to a device class also apply to the virtualized variants.



IEC 2345/10

Figure 2 – Visual map of possible values for the attribute tables

Table 2 – Allowed values for change indicator field in attribute table

Value	Meaning
<blank>	No changes in the text or figures from the immediately-preceding version of this requirement.
A	Attribute table itself, excluding the change indicator, has changed. E.g. a new device class was added.
C	Changes made to the requirement modify the testing, intent, or other normative behavior relative to the immediately-preceding version of this requirement.
D	Requirement has been deleted. These requirements are moved to the deleted requirements document. Note that the change indicator for the requirement is marked deleted only the first time it appears in the deleted requirements' document; in subsequent versions of the deleted requirements' document the change indicator is reset to blank.
E	Changes made that do not modify testable requirements, intent, or other normative behavior.

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. For this reason, this subclause includes recommendations for conditions at the time of making these measurements, as follows.

- 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

7.3.1 General

The guidelines in this subclause provide requirements for general and device specific capabilities for networking that are independent of the link protection system used. For DTCP-IP specific requirements, see 8.2. For WMDRM-ND specific requirements, see 9.3.

The following additions shall be made to Table 8 of IEC 62481-1 to include the normative DLNA QoS levels for link protection messages.

Table 3 – Normative priorities for dlina traffic types for link protection

DLNAQOS_UP	DLNA traffic types	IEEE 802.1Q user priority	WMM access category	DSCP	Clause details
DLNAQOS_3 (Highest)	DLNA link protection key exchange	7	VO	0x38	8.2.2 9.3.2

7.3.2 New general capability requirements – Bluetooth NC CP – Power saving modes

If the NC-PS bearer level power saving scheme is supported and the network link is in 'Standby' mode, then the MHD device should request the transition from 'Standby' to 'Active' NC-PS mode before any required link protection communication.

S	A	n/a	M-DMS M-DMP	n/a	IEC 62481-1	67G8Y
---	---	-----	-------------	-----	-------------	-------

Refer to IEC 62481-1, 7.2.3.4.3.

This is to ensure that the link is in the highest bandwidth and lowest delay state before starting a link protection exchange that may depend on the timing of individual message. For example, DTCP-IP measures the RTT between the content source and the content receiver to determine if the endpoints are on the user's home network. If this operation occurs while the link is in the 'Standby' mode, the delay can be artificially high.

7.4 Device discovery and control

This subclause covers the guidelines for implementing device discovery and control using the UPnP device architecture. There are no changes to this subclause for the support of DLNA link protection. For DTCP-IP specific requirements, see 8.3. For WMDRM-ND specific requirements, see 9.4.

7.5 Media management

7.5.1 Media management – AV media management

This subclause covers the guidelines for implementing media management using the UPnP AV architecture with DLNA link protection. This subclause gives detailed information on media management. For DTCP-IP specific requirements, see 8.4. For WMDRM-ND specific requirements, see 9.5.

Many of the guidelines for this subclause as well as 7.6 have to do with the structures necessary to perform seek operations over the link protected content. IEC 62481-1 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 4 and Table 5 summarize the structures used for each of the domains and seek models. Table 6 contains the guidelines that define the media management requirements for devices using DLNA link protection.

WATERMARK

**Table 4 – Summary of domain elements
for full random access data availability mode**

Model	Function	Time domain	Network byte domain	Cleartext byte domain
Full random access data availability	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:cleartext Size
	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 5 – Summary of domain elements
for limited random access data availability model**

Model	Function	Time domain	Network byte domain	Cleartext byte domain
Limited random access data availability	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 not-range)	availableSeekRange.dlna.org (with byte-range)	availableSeekRange.dlna.org (with cleartextbyte-range)
	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
	S0 is increasing	flags-param Bit 27 : s0-increasing		
	SN is increasing	flags-param Bit 26 : sN-increasing		

7.5.2 AV media management guidelines

7.5.2.1 Updates to existing general AV media management guidelines

7.5.2.1.1 General

Table 6 – AV media management guideline changes

Requirement updated	Location in IEC 62481-1
MM flags-param (flags parameter)	7.4.1.3.23.2
MM lop-npt, lop-bytes, and lop cleartextbytes (limited operations flags): Common	7.4.1.3.28.1
MM lop-npt lop-bytes, and lop-cleartextbytes (limited operations flags): HTTP	7.4.1.3.29
MM lop-npt, lop-bytes, and lop-cleartextbytes (limited operations flags): RTP	7.4.1.3.30
MM IFO file	7.4.1.4.8.1
	7.4.1.4.8.2
	7.4.1.4.8.3
	7.4.1.4.8.4
	7.4.1.4.8.5

7.5.2.1.2 MM IFO file

7.5.2.1.2.1 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.

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

Refer to IEC 62481-1, 7.4.1.4.8. The IFO file shall be available as cleartext.

7.5.2.1.2.2 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.

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

Refer to IEC 62481-1, 7.4.1.4.8. Byte positions are with respect to the unprotected content stream and not a byte position within the protected content stream.

7.5.2.2 New general AV media management requirements

7.5.2.2.1 MM media class of link protected content

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.

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

Refer to IEC 62481-1, 7.4.1.3.11. For example link protected content that in its unprotected form conforms to the DLNA "AV" media class shall use object.item.videoItem or a derived class for the upnp:class value.

7.5.2.2.2 MM DIDL-Lite byte metadata properties

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.

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

Refer to IEC 62481-1, 7.4.1.3.11. The length of the protected content stream may be longer due to encryption additional headers for packetization and any necessary padding.

7.5.2.2.3 MM CP – res@dlina:cleartextSize

7.5.2.2.3.1 A UPnP AV MediaServer should additionally provide non-empty and non-whitespace values for metadata properties as shown in the Table 7 for <res> elements that describe content binaries that use a link protection system

Table 7 – Recommended metadata properties

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

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

Refer to IEC 62481-1, 7.4.1.3.11. This guideline helps resolve dependency issues that rendering endpoints have on knowing the size in bytes of the unprotected content stream.

7.5.2.2.3.2 If the UPnP AV MediaServer specifies the res@dlina: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.

Table 8 – Property type and multi value

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

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

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

7.5.2.2.4 MM CP – DIDL-Lite protocolInfo value

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

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

Refer to IEC 62481-1, 7.4.1.3.15.5. It prohibits transport layer encryption unless the media format profile explicitly states it is required. This guideline clarifies that some media format profiles may use link protection and are hence encrypted. The link protection system is specified within the media format profile of the content.

7.5.2.2.5 MM CP – LP-flag (link protection flag)

7.5.2.2.5.1 If the content binary described by the protocolInfo uses DLNA link protection when it is transmitted then the LP-flag shall be true.

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

Refer to IEC 62481-1, 7.4.1.3.37. The specifics of the link protection system used and parameters for setting up the connection may be found in the MIME type or other protocolInfo parameters.

7.5.2.2.5.2 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.

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

7.5.2.2.6 MM CP – cleartextbyte seek-full

Byte-based on full seek data availability with the cleartext byte seek request header.

If a content binary uses a link protection system over the HTTP media transport protocol the meaning of the cleartextbyte seek-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 requirements of the full random access data availability model for link protected content are defined in 7.6.2.3.2 below.

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

Refer to IEC 62481-1, 7.4.1.3.37. The cleartext byte seek request header can be different depending on the link protection system used. For the general requirements of the header, see 7.6.6.2.2, for the DTCP-IP link protection system, see 8.5.1.2, 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.

7.5.2.2.7 MM CP – lop-cleartextbytes flag

Byte-based limited seek data availability with cleartext byte seek request header.

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 requirements of the limited random access data availability model for link protected content are defined by 7.6.2.3.3 below.

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

Refer to IEC 62481-1, 7.4.1.3.37. The cleartext byte seek request header can be different depending on the link protection system used. For the general requirements of the header, see 7.6.6.2.2, for the DTCP-IP link protection system, see 8.5.1.2, 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.

7.5.2.3 MediaRenderer device requirements

7.5.2.3.1 MM CP – Link protection state error

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 link protection restrictions (e.g. RTT) were not met between the content source and the content receiver.

S	A	DMR	n/a	n/a	[8]	WDR47	
---	---	-----	-----	-----	-----	-------	--

Refer to IEC 62481-1, 7.4.1.6.11. UPnP MediaRenderers define new allowed values for the AVT:TransportStatus instance state variable to represent a link protection error condition.

7.5.2.3.2 MM CP – Link protection human readable error message

7.5.2.3.2.1 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 with the human readable error description "Can't determine allowed uses".

S	A	DMR	n/a	n/a	[8]	G8YKV	
---	---	-----	-----	-----	-----	-------	--

Refer to IEC 62481-1, 7.4.1.6.11.

7.5.2.3.2.2 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.

O	A	DMR	n/a	n/a	[8]	JVW4I	
---	---	-----	-----	-----	-----	-------	--

7.6 Media transport

7.6.1 General

This subclause covers the requirements for the media transport layer. It also gives detailed information on media transport. For DTCP-IP specific requirements, see 8.5. For WMDRM-ND specific requirements, see 9.6.

7.6.2 Media transport protocols

7.6.2.1 General

The following subclauses contain guidelines for the use of media transports in DLNA devices. The guidelines are organized into a table that covers requirements common among all media transports and then clauses/tables that cover requirements for specific media transport protocols such as HTTP and others. For detailed information, see 7.5 of IEC 62481-1.

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

7.6.2.2 Updates to existing general media transport guidelines

Table 9 gives references to IEC 62481-1.

Table 9 – Updates to existing general media transport guidelines

Requirement updated	Location in IEC 62481-1
MT normative random access data availability models	7.5.4.2.14.1
MT "full random access data availability" model	7.5.4.2.15.1
	7.5.4.2.15.2
MT "limited random access data availability" model	7.5.4.2.16.1
	7.5.4.2.16.2
	7.5.4.2.16.3
	7.5.4.2.16.4

7.6.2.3 New general media transport requirements

7.6.2.3.1 MT CP – Link protected content

Any key exchange required to decode a link protected content binary shall follow the requirements of the link protection system in use.

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

Refer to IEC 62481-1, 7.5.4.2.3.

7.6.2.3.2 MT CP – Play ready

Initiation of link protection specific setup operations should occur while browsing for content or upon invocation of AVT:SetAVTransportURI.

S	A	DMP DMR	M-DMP	n/a	[5] [8]	R6EOV	
---	---	---------	-------	-----	---------	-------	--

Refer to IEC 62481-1, 7.5.4.2.3. link protection setup operations (such as RTT testing and authentication of the endpoint and key exchange) may take considerable time. The rendering endpoint should not wait until the HTTP connection is established to initiate these operations, but should start them as soon as possible.

7.6.2.3.3 MT CP – Metadata and transport headers for link protection

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).

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

Refer to IEC 62481-1, 7.5.4.2.13.

7.6.3 HTTP transport

7.6.3.1 General

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. The remainder of this subclause contains the guidelines that pertain to the HTTP transport and are organized into requirements that are common to all HTTP transfers, requirements specific to a streaming transfer, requirements specific to an interactive transfer, and requirements specific to a background transfer. For detailed information, see 7.5.5 of IEC 62481-1.

7.6.3.2 Updates to existing general HTTP media transport guidelines

7.6.3.2.1 General

Table 10 – Updates to existing general HTTP media transport guidelines

Requirement updated	Location in IEC 62481-1
MT HTTP header: contentFeatures.dlna.org	7.5.5.2.10.7
MT HTTP common random access data availability requirements	7.5.5.2.18.1
MT HTTP data range of "full random access data availability"	7.5.5.2.18.2
MT HTTP data range of "limited random access data availability"	7.5.5.2.20.1
	7.5.5.2.20.2
	7.5.5.2.20.4
	7.5.5.2.20.8
	7.5.5.2.20.9
	7.5.5.2.20.11
	7.5.5.2.20.12
MT HTTP header: RANGE (Server)	7.5.5.2.20.16
	7.5.5.2.22.3
	7.5.5.2.22.4
MT HTTP time-based seek (Server)	7.5.5.2.24.1

7.6.3.2.2 MT HTTP common random access data availability requirements

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 time.

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

Refer to IEC 62481-1, 7.5.5.2.18. This is a general requirement that random access requests be supported on the entire [r0, rN] data range over the cleartext byte domain.

7.6.3.2.3 MT HTTP data range of "full random access data availability"

7.6.3.2.3.1 The byte position of 0 for the cleartext byte seek request header field shall refer to the beginning of the content binary.

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

Refer to IEC 62481-1, 7.5.5.2.19.

7.6.3.2.3.2 If a 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 s0-increasing is false and none of the above headers are supported by the HTTP server.

M	A	DMS	M-DMS	MIU	[4]	T5GV8	
---	---	-----	-------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.5.2.19.

7.6.3.2.3.3 For a content binary that uses a link protection system, if a 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.

S	C	DMS +PU+	M-DMS	n/a	[4]	W4I6W	
---	---	----------	-------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.5.2.19.

The cleartext byte seek request header can be different depending on the link protection system used. For the general requirements of the header, see 7.6.6.2.2, for the DTCP-IP link protection system, see 8.5.1.2, for the WMDRM-ND link protection system, see 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 8.4.2; for the WMDRM-ND link protection system, see 9.6.1.8 for the definition of this header.

7.6.3.2.3.4 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.

S	C	DMP DMR	M-DMP	MIU	[4]	47I2C	
---	---	---------	-------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.5.2.19.

The response will include the cleartext byte seek response header. If the instance length is known, then it will be number of bytes in the UCDAM [s0, sN] 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 7.6.6.2.2, for the DTCP-IP link protection system, see 8.5.1.2, for the WMDRM-ND link protection system, see 9.6.1.7 for the definition of this header.

- 7.6.3.2.3.5** 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.

Note that this guideline is mandatory for scenarios where the HTTP server is serving stored content.

M	A	DMS	M-DMS	n/a	[4]	R47I2	
---	---	-----	-------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.5.2.19.

7.6.3.2.4 MT HTTP – Data range of "limited random access data availability"

For a content binary that uses a link protection system, if an HTTP server endpoint supports the cleartext byte seek request for a content binary that operates under the "limited random access data availability" model, it shall provide the cleartextbyte-range in the availableSeekRange.dlna.org HTTP header field of the target response to an HTTP request with the getAvailableSeekRange.dlna.org header HTTP header field and that cleartextbyte-range shall refer to a byte range within the cleartext byte domain.

M	A	DMS +PU+	M-DMS		[4]	F3M2V	
---	---	----------	-------	--	-----	-------	--

Refer to IEC 62481-1, 7.5.5.2.20.

7.6.3.2.5 MT HTTP – Data range of "limited random access data availability"

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 [r0, rN].

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	[4]	3M2V8	
---	---	------------------	-------------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.5.2.21.

The cleartext byte seek request header can be different depending on the link protection system used. For the general requirements of the header, see 7.6.6.2.2, for the DTCP-IP link protection system, see 8.5.1.2, for the WMDRM-ND link protection system, see 9.6.1.7 for the definition of this header.

7.6.3.2.6 MT HTTP time-based seek (server)

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 and an npt-range value using the TimeSeekRange.dlna.org header in the HTTP target response to the HTTP request.

The TimeSeekRange.dlna.org header shall include the instance-duration value. The cleartext byte seek response header shall include the appropriate instance-length value unless the following exception applies.

Exception:

- If all of the following conditions are true.
- The data access model is the "limited random access data availability" model.

- The mode-flag (as indicated in availableSeekRange.dlna.org) is "1".
- The request omitted the cleartext byte seek request header and only specified TimeSeekRange.dlna.org.

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/*

M	A	DMS +PU+	M-DMS	n/a	[4]	M2V86
---	---	----------	-------	-----	-----	-------

Refer to IEC 62481-1, 7.5.5.2.24.

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 shall be returned to indicate the byte position within the cleartext byte domain.

The instance-duration and npt-range values of TimeSeekRange.dlna.org is defined in 7.5.5.2.24.3.

The cleartextbyte-range and instance-length values for the cleartext byte seek response header are defined for the DTCP-IP link protection system in 8.5.1.2, for the WMDRM-ND link protection system in 9.6.1.7.

7.6.3.2.7 MT caching directives for HTTP 1.0

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

M	A	DMS +PU+	M-DMS	n/a	[4]	VLBIV
---	---	----------	-------	-----	-----	-------

Refer to IEC 62481-1, 7.5.5.2.34.

7.6.3.2.8 MT caching directives for HTTP 1.1

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

M	A	DMS +PU+	M-DMS	n/a	[4]	JYDYG
---	---	----------	-------	-----	-----	-------

Refer to IEC 62481-1, 7.5.5.2.35.

7.6.3.3 New general HTTP media transport requirements

7.6.3.3.1 HTTP error codes for unavailable content

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).

S	A	DMS	M-DMS	n/a	[4]	6EOVL	
---	---	-----	-------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.5.2.4.

By the HTTP specification, the HTTP server endpoint may place additional information about the cause of the error in the entity body of the response.

7.6.3.3.2 MT byte position definitions

For content that uses DLNA link protection, unless otherwise stated, all references in IEC 62481-1 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).

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

Refer to IEC 62481-1, 7.5.5.2.7.

7.6.3.3.3 MT HTTP header – Cleartext byte seek request header (server)

7.6.3.3.3.1 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.

S	L	DMS +PU+	M-DMS	n/a	[4]	3PVBR	
---	---	----------	-------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.5.2.24.

7.6.3.3.3.2 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.

O	A	DMS +PU+	M-DMS	n/a	[4]	EOVLB	
---	---	----------	-------	-----	-----	-------	--

7.6.3.3.3.3 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).

M	A	DMS +PU+	M-DMS	n/a	[4]	5JYDY	
---	---	----------	-------	-----	-----	-------	--

The positions specified in this header refer to positions in the cleartext byte domain.

7.6.3.3.3.4 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.

M	A	DMS +PU+	M-DMS	n/a	[4]	X5JYD	
---	---	----------	-------	-----	-----	-------	--

7.6.3.3.3.5 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 a 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.

M	A	DMS +PU+	M-DMS	n/a	[4]	OVLBI	
---	---	----------	-------	-----	-----	-------	--

The decoder friendly alignment position is defined for each of the media format profiles specified in 8.8 Media format DTCP-IP profiling guidelines and 9.9 Media format WMDRM-ND profiling guidelines.

The media format alignment element is defined for each of the media format profiles specified in 8.8 Media format DTCP-IP profiling guidelines and 9.9 Media format WMDRM-ND profiling guidelines.

- 7.6.3.3.3.6** 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.

M	C	DMS +PU+	M-DMS	n/a	[4]	6X5JY	
---	---	----------	-------	-----	-----	-------	--

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 shall be able to start decryption at the start of the HTTP entity body.

- 7.6.3.3.3.7** 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).

M	C	DMS +PU+	M-DMS	n/a	[4]	VALG6	
---	---	----------	-------	-----	-----	-------	--

HTTP response code 416 is used when the HTTP 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.

- 7.6.3.3.3.8** 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).

M	L	DMS +PU+	M-DMS	n/a	[4]	ALG6N	
---	---	----------	-------	-----	-----	-------	--

HTTP response code 406 is used when the HTTP 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

Note, 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 required for the given link protect system used, see 8.5.1.3, for the DTCP-IP link protection system; for the WMDRM-ND link protection system, see 9.6.1.8.

7.6.3.3.3.9 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).

M	L	DMS +PU+	M-DMS	n/a	[4]	V3PVB	
---	---	----------	-------	-----	-----	-------	--

The client cannot specify this situation, see 7.6.3.3.4.3. 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.

	A	DMS +PU+	M-DMS	n/a	[4]	4N2GT	
--	---	----------	-------	-----	-----	-------	--

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

7.6.3.3.3.10 An HTTP server endpoint should support HTTP requests that specify the cleartext byte seek request header by implementing behavior that returns the requested entity-body with the 200 (OK) HTTP header.

S	A	DMS +PU+	M-DMS	n/a	[4]	YDYGD	
---	---	----------	-------	-----	-----	-------	--

7.6.3.3.4 MT HTTP Header – Cleartext byte seek request header (client)

7.6.3.3.4.1 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 fourth field cleartextbytesseek-full flag or the lop-cleartextbytes flag of the flags-param as defined in 7.5.2.1.2.

M	L	DMP DMR	n/a	MIU	[4]	6NXR7	
---	---	---------	-----	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.5.2.24.

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

7.6.3.3.4.2 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.

M	L	DMP DMR	n/a	MIU	[4]	G6NXR	
---	---	---------	-----	-----	-----	-------	--

7.6.3.3.4.3 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.

M	L	DMP DMR	n/a	MIU	[4]	PVBRV	
---	---	---------	-----	-----	-----	-------	--

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.

7.6.4 HTTP media transport for streaming transfer guidelines

7.6.4.1 Updates to existing general HTTP media transport for streaming transfer guidelines

7.6.4.1.1 General

Table 11 gives the references to IEC 62481-1.

Table 11 – Updates to existing general HTTP media transport for streaming transfer guidelines

Requirement updated	Location in IEC 62481-1
MT HTTP fast forward scan media operation	7.5.5.3.8
MT HTTP streaming slow forward scan media operation	7.5.5.3.9
MT HTTP streaming fast backward scan media operation	7.5.5.3.10
MT HTTP streaming slow backward scan media operation	7.5.5.3.11
MT HTTP streaming scan media operations	7.5.5.3.12
MT HTTP media operation support within a profile	7.5.5.3.15.2
MT combined RANGE, time based seek, and play speed HTTP requests	7.5.5.3.17.2
MT HTTP header: realTimeInfo.dlna.org	7.5.5.3.18.6

7.6.4.1.2 MT HTTP seek media operation

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.

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

Refer to IEC 62481-1, 7.5.5.3.7.

The cleartext byte seek request header can be different depending on the link protection system used. For the general requirements of the header, see 7.6.6.2.2, for the DTCP-IP link protection system, see 8.5.1.2, for the WMDRM-ND link protection system, see 9.6.1.7 for the definition of this header.

7.6.5 HTTP media transport for interactive transfer guidelines

7.6.5.1 General

This subclause provides updates to existing general HTTP media transport for interactive transfer guidelines.

7.6.5.2 MT RANGE behavior for interactive transferred content

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.

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

Refer to IEC 62481-1, 7.5.5.4.3.

7.6.6 RTP transport

7.6.6.1 General

This subclause covers the guidelines for the RTP transport protocol for content transmitted using DLNA link protection. For detailed information, see 7.5 of IEC 62481-1.

7.6.6.2 Update existing general RTP transport guidelines

7.6.6.2.1 MT RTP packet size

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.

S	A	DMS +PU+	M-DMS	n/a	[1]	2GTDF	
---	---	----------	-------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.6.3.5.

Link protection encapsulation may add headers and padding and will increase payload size.

7.6.6.2.2 MT RTP play media operation

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).

S	A	DMS +PU+	M-DMS	n/a	[1]	BRVS3	
---	---	----------	-------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.8.2.36.

7.6.6.3 New general RTP transport guidelines MT – RTP support for link protected content

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.

S	A	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	[2]	N2GTD	
---	---	---------------------	-------------	-----	-----	-------	--

Refer to IEC 62481-1, 7.5.6.2.18.

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

There are no changes to the corresponding subclause in IEC 62481-1 for link protection. The guidelines contained in 7.6 of IEC 62481-1 hold identically for devices exchanging content using DLNA link protection. Correspondingly, there are no additional DTCP-IP or WMDRM-ND specific guidelines in Clause 8 or Clause 9 for content conversion and device virtualization.

7.8 Media interoperability unit (MIU)

There are no changes to the corresponding subclause in IEC 62481-1 for link protection. The guidelines contained in 7.7 of IEC 62481-1 hold identically for devices exchanging content using DLNA link protection. Correspondingly, there are no additional DTCP-IP or WMDRM-ND specific guidelines in Clause 8 or Clause 9 for MIU devices.

7.9 Link protection technology guidelines requirements

7.9.1 Link protection system – DTCP-IP

7.9.1.1 If a device supports DLNA link protection it shall support DTCP-IP as defined in these guidelines.

M	A	DMS +PU+	DMP	DMR	M-DMS	M-DMP	MIU	DTCP Volume 1, DTCP Volume 1 Supplement E, DTCP audio compliance rules EXHIBIT B-2, [10]	BSTW5	
---	---	-------------	-----	-----	-------	-------	-----	---	-------	--

7.9.1.2 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.

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

7.9.1.3 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.

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

7.9.1.4 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.

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

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 required behavior expressed by this guideline will result in improved interoperability.

7.9.1.5 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.

M	A	+PU+			n/a		n/a	n/a	TW5	
---	---	------	--	--	-----	--	-----	-----	-----	--

- 7.9.1.6** If a device supports the DTCP-IP link protection system it shall support all guidelines in IEC 62481-1, modified by those guidelines found in Clause 7 of this standard and 8.2, 8.4 and 8.5.1.2 to 8.5.1.3 and if the RTP media transport format is supported 8.5.1.4 to 8.5.1.6.

M	A	DMS +PU+	DMP	DMR	M-DMS M-DMP	MIU	IEC 62481-1	GTDFW	E
---	---	-------------	-----	-----	-------------	-----	-------------	-------	---

7.9.2 Link protection system – Windows media DRM for network devices

- 7.9.2.1** If a device supports DLNA link protection it may support WMDRM-ND as defined in these guidelines.

O	A	DMS DMP DMR	M-DMS M-DMP	MIU	[2] [3]	3SNB9	
---	---	-------------	-------------	-----	---------	-------	--

- 7.9.2.2** If a UPnP AV media server 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.

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

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 behavior expressed by this guideline will result in improved interoperability. Content objects that are only permitted to be output over WMDRM-ND may 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 may be optionally exposed on the network with WMDRM-ND protection in addition to being exposed with the required DTCP-IP protection.

- 7.9.2.3** 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.

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

- 7.9.2.4** If a device supports the WMDRM-ND link protection system it shall support all guidelines in IEC 62481-1, modified by those guidelines found in Clause 7 of this standard and 9.2, 9.3, 9.4, 9.6.1.2 to 9.6.1.8 and if the RTP media transport is supported 9.6.2.2 - 9.6.2.7.

M	A	DMS DMP DMR	M-DMS M-DMP	MIU	IEC 62481-1	SNB9F	E
---	---	-------------	-------------	-----	-------------	-------	---

8 DTCP-IP link protection system guidelines

8.1 General

This subclause contains the guidelines that are specific to the DTCP-IP link protection system.

See 8.9 for general requirements for devices that implement DTCP-IP.

8.2 Networking and connectivity

8.2.1 Networking and connectivity – General capability requirements

This subclause contains the requirements that are specific to DTCP-IP use of the networking capabilities described in 7.2 of IEC 62481-1.

8.2.2 New DLNAQoS requirements QoS requirement for DTCP-IP traffic

If DLNA QoS as defined in 7.2 of IEC 62481-1 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 3.

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	IEC 62481-1	TDFW2	
---	---	---------------------	-------------	-----	-------------	-------	--

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, the DLNAQoS level shall be set appropriately. DTCP-IP messages should be assigned a priority higher than A/V stream itself.

8.2.3 New device requirements – Common NC CP – Wireless security

Devices which use the DTCP-IP link protection system with integrated IEEE 802.11 shall ensure that WEP or other such equivalent protection mechanism (e.g. WPA or WPA2) is engaged prior to exchanging DTCP AKE commands and protected content via that network interface.

M	R	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	DTCP Volume 1 Supplement E, [10]	LQ89T	
---	---	---------------------	-------------	-----	---	-------	--

This is a requirement of the DTCP specification.

8.3 Device discovery and control

There are no DTCP-IP specific changes to the guidelines in 7.3 of IEC 62481-1.

8.4 Media management

8.4.1 Media management – AV media management

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 7.5 of IEC 62481-1.

8.4.2 MM CP – DTCP-IP URI

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

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

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 rendering devices shall not rely on that information being within the URI also.

8.5 Media transport

8.5.1 HTTP transport

8.5.1.1 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 7.5 of IEC 62481-1.

8.5.1.2 MT HTTP cleartext byte seek request header for DTCP-IP

8.5.1.2.1 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.

M	R	DMS +PU+	DMP	DMR	M-DMS	M-DMP	MIU	DTCP Volume 1 Supplement E, [4]	416WA	
---	---	-------------	-----	-----	-------	-------	-----	--	-------	--

8.5.1.2.2 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:

- 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.

Examples:

- Range.dtcp.com: bytes=1539686400-
- Range.dtcp.com: bytes=1539686400-1540210688

M	L	DMP	DMR	M-DMP	MIU	DTCP Volume 1 Supplement E, [4]	712CK	C
---	---	-----	-----	-------	-----	--	-------	---

8.5.1.3 MT HTTP cleartext byte seek response header for DTCP-IP

8.5.1.3.1 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.

M	L	DMS +PU+	DMR	DMP	M-DMS M-DMP	MIU	DTCP Volume 1 Supplement E, [4]	2V86H	C
---	---	-------------	-----	-----	-------------	-----	--	-------	---

8.5.1.3.2 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

M	F	DMS +PU+	M-DMS	n/a	DTCP Volume 1 Supplement E, [4]	LBIVE	
---	---	----------	-------	-----	--	-------	--

8.5.2 RTP transport

8.5.2.1 General

This subclause covers the guidelines for the RTP transport protocol for DLNA devices using the DTCP-IP link protection system.

8.5.2.2 MT RTP CP – Link protected media format profiles

For A/V profile ID values in 8.8 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 8.5.2.4.

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1, DTCP Volume 1 Supplement E, [6] [7]	DYGDM	
---	---	---------------------	-------------	-----	---	-------	--

8.5.2.3 MT DTCP-IP encapsulated media format profiles

8.5.2.3.1 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 in 7.5.6.3 through 7.5.7.10 according to the corresponding format profile of the un-encrypted content.

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1, DTCP Volume 1 Supplement E, [6] [7]	NXR7U	
---	---	---------------------	-------------	-----	--	-------	--

8.5.2.3.2 After the RTP encapsulation of the cleartext content as per 8.5.1.2.1, the RTP payload thus generated shall be encrypted into a single DTCP PCP as defined in [10].

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.

M	C	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	DTCP Volume 1, DTCP Volume 1 Supplement E [6] [7]	RVS3E	
---	---	---------------------	-------------	-----	--	-------	--

8.5.2.3.3 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 8.5.1.2.1.

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	n/a	[6] [7]	DFW2J	
---	---	---------------------	-------------	-----	---------	-------	--

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.

8.5.2.4 MT RTP CP

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 fmtpp 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.

M	A	DMS DMP DMR	M-DMS M-DMP	n/a	[6] [7]	NB9FS	
---	---	-------------	-------------	-----	---------	-------	--

Refer to RFC 2327.

Example:

```
m=application 0 RTP/AVP 96
a=rtpmap:96 x-dtcp1/9000
a=fmtp:96 CONTENTFORMAT= video/mp2t DTCP1HOST=192.168.1.1
DTCP1PORT=37654
```

If the video stream and audio stream are separated, 2 kinds of dynamic payload types should be described 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
```

8.6 Content conversion device virtualization

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

8.7 Media interoperability unit (MIU)

There are no guidelines specific to DTCP-IP for media interoperability units.

8.8 Media format – DTCP-IP profiling guidelines

8.8.1 General

This subclause contains additions to IEC 62481-2 defining the DTCP-IP media format profiles. This subclause 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 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.

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