

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**



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It also gives information on projects, replaced and withdrawn publications.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.

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.

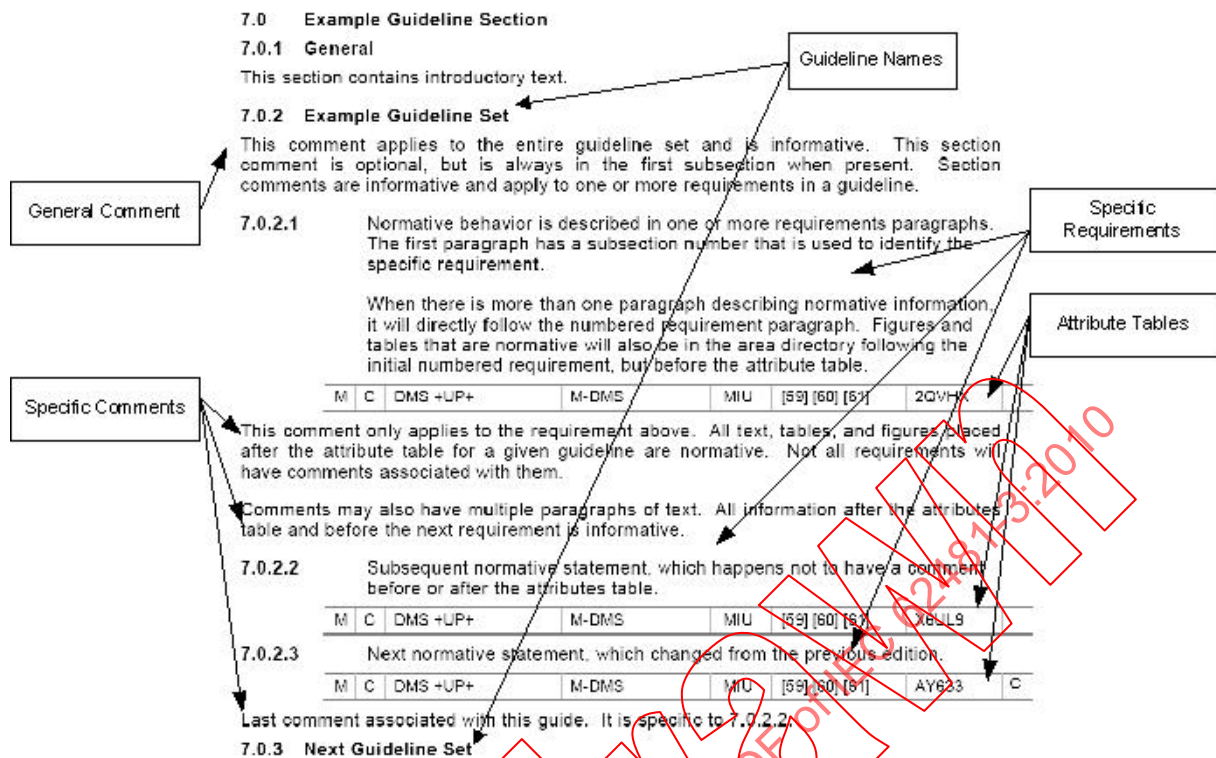


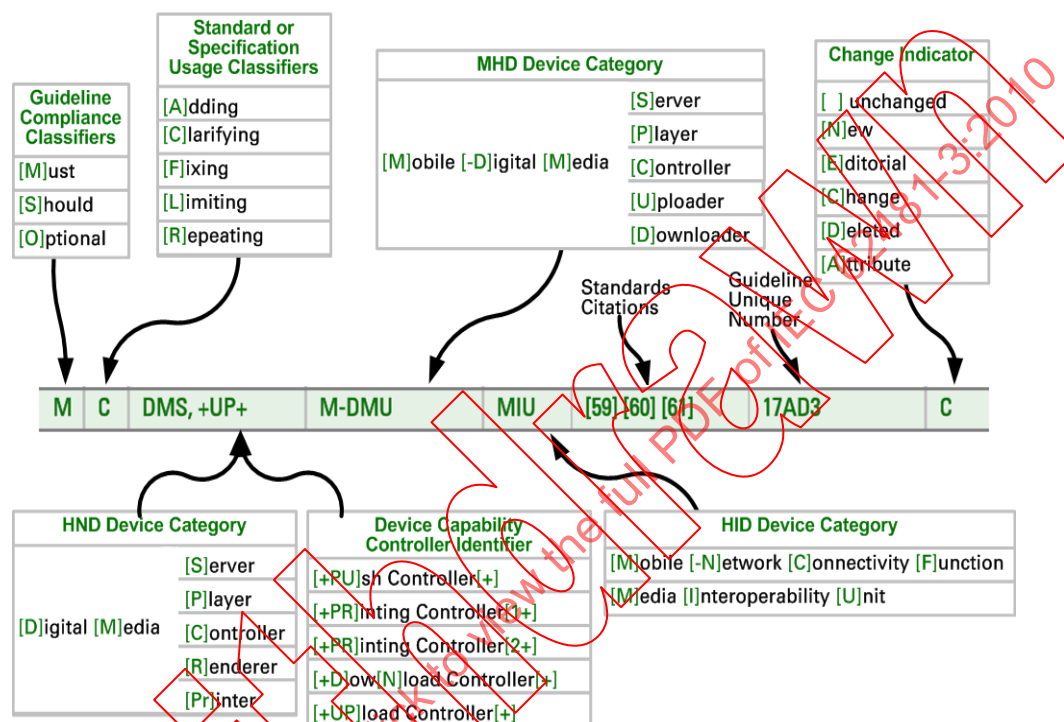
Figure 1 – Guideline layout and definitions

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.

**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 npt-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	KJVVW4	
---	---	-----	-------	-----	-------------	--------	--

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	TW5CS	
---	---	------	--	--	-----	--	-----	-----	-------	--

- 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	
---	---	-----	-----	-----	---	-------	--

8.8.2.3 The profile ID of DTCP-IP protected content shall comply with the following syntax:

ProfileID_Protected = "DTCP_" Original_ProfileID

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

Example: If a content binary that complies with the MPEG_PS_NTSC profile ID is transferred with DTCP-IP link protection, then the profile ID of the protected content shall be DTCP_MPEG_PS_NTSC.

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

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

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

8.8.2.5 A content binary using a DTCP_ Profile ID shall only be transferred using the DTCP-IP link protection system.

M	A	HND	MHD	n/a	n/a	FW2J3	
---	---	-----	-----	-----	-----	-------	--

8.8.3 CP DTCP-IP – Profile MIME type definition

8.8.3.1 General

Profile: DTCP_*

8.8.3.2 When used to describe a content binary, the MIME type used for profiles based on the DTCP-IP link protection system shall be as follows:

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

<MIME-type> is the MIME type of the original content before DTCP-IP packetization.

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

M	C	DMS +PU+	M-DMS	n/a	DTCP Volume 1, DTCP Volume 1 Supplement E	VS3EY	
---	---	----------	-------	-----	---	-------	--

Example would be in protocolInfo values that are used in <res> elements.

8.8.3.3 The <host> value in the MIME type specified by 8.8.3.1 shall be an absolute IP address in the a.b.c.d IPv4 address format (i.e. quad-form network byte order).

M	R	DMS +PU+	M-DMS	n/a	n/a	XR7U7	
---	---	----------	-------	-----	-----	-------	--

8.8.3.4 When used to describe a capability of a device, the MIME type used for profiles based on the DTCP-IP link protection system shall be as follows:

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

<MIME-type> is the MIME-type, as listed in DTCP Volume 1 Supplement E, for the content format profile before DTCP encryption.

M	C	DMS DMR	M-DMS	n/a	DTCP Volume 1, DTCP Volume 1 Supplement E	YGDM2	
---	---	---------	-------	-----	---	-------	--

Example would be in protocolInfo values that are used in the response to the CMS:GetProtocolInfo action.

8.8.4 CP DTCP-IP – Profile protected and unprotected content portions

8.8.4.1 General

Profile: DTCP_*

8.8.4.2 If a content binary contains both a protected portion and a non-protected portion, then the entire content shall be transferred by the serving endpoint using a DTCP-IP profile.

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

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

8.8.4.3 If a content binary is known to never contain any protected content portions, then the serving endpoint should not use the DTCP-IP format profile to describe the content.

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

For instance, a server that is capturing a stream that it knows will never have a protected portion should send this content as unprotected content and not use the DTCP-IP link protection system.

8.8.4.4 A rendering endpoint shall continue to render the input stream correctly in the presence of dynamic changes of E-EMI values during the transfer of the content stream.

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

8.8.4.5 If a serving endpoint can not determine if the content item will ever contain a protected content portion, then the entire content shall be transferred using the Protected Content Packet (PCP) format.

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

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

8.8.5 CP DTCP-IP – Profile HTTP encapsulation

Profile: DTCP_*

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

For DTCP encapsulated content, the link protection alignment element is a PCP packet consisting of a properly formed PCP header, payload, and any necessary padding.

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

8.8.6 DTCP-IP profile encapsulation

8.8.6.1 DTCP-IP encapsulated content

Mandatory alignment element for cleartext.

Profiles:

DTCP_MPEG_PS_NTSC,
DTCP_MPEG_PS_PAL,
DTCP_MPEG_PS_NTSC_XAC3,
DTCP_MPEG_PS_PAL_XAC3

The media format alignment element for cleartext bitstreams conformant to these profiles shall be the MPEG-2 pack.

M	A	n/a	n/a	n/a	ISO/IEC 13818-1 ISO/IEC 13818-2 ISO/IEC 14496-2	GDM2L	
---	---	-----	-----	-----	--	-------	--

This entry clarifies the transport alignment of MPEG-2 program streams encapsulated within the DTCP-IP link protection system.

8.8.6.2 DTCP-IP encapsulated content

Mandatory decoder friendly alignment position for cleartext.

Profiles:

DTCP_MPEG_PS_NTSC,
DTCP_MPEG_PS_PAL,
DTCP_MPEG_PS_NTSC_XAC3,
DTCP_MPEG_PS_PAL_XAC3

The decoder friendly alignment position for bitstreams conformant to these profiles shall be the VOB boundary.

M	A	n/a	n/a	n/a	ISO/IEC 13818-1 ISO/IEC 13818-2 ISO/IEC 14496-2	BIVE3	
---	---	-----	-----	-----	--	-------	--

This entry clarifies the transport alignment of MPEG-2 program streams encapsulated within the DTCP-IP link protection system when a Range.dtcp.com is performed.

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

8.8.6.3 DTCP-IP encapsulated content

Mandatory decoder friendly alignment position for cleartext.

Profiles:

DTCP_MPEG_PS_NTSC,
DTCP_MPEG_PS_PAL,
DTCP_MPEG_PS_NTSC_XAC3,
DTCP_MPEG_PS_PAL_XAC3

For content with the MPEG2-PS profile transferred with the HTTP transport protocol, the size of each PCP shall be one VOBU except when transferring a specific range of content requested with the Range.dtcp.com or TimeSeekRange.dlna.org header or when transferring the last VOBU in a content stream.

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

8.8.6.4 DTCP-IP encapsulated content

Mandatory alignment element for cleartext.

Profiles:

DTCP_MPEG_TS_SD_NA,
DTCP_MPEG_TS_SD_NA_T,
DTCP_MPEG_TS_SD_NA_ISO,
DTCP_MPEG_TS_HD_NA,
DTCP_MPEG_TS_HD_NA_T,
DTCP_MPEG_TS_HD_NA_ISO,
DTCP_MPEG_TS_SD_EU,
DTCP_MPEG_TS_SD_EU_T,
DTCP_MPEG_TS_SD_EU_ISO,
DTCP_MPEG_TS_SD_KO,
DTCP_MPEG_TS_SD_KO_T,
DTCP_MPEG_TS_SD_KO_ISO,
DTCP_MPEG_TS_HD_KO,
DTCP_MPEG_TS_HD_KO_T,
DTCP_MPEG_TS_HD_KO_ISO

The media format alignment element for cleartext bitstreams conformant to these profiles shall be the DLNA transport packet.

M	A	n/a	n/a	n/a	IEC 62481-2	V86HW	
---	---	-----	-----	-----	-------------	-------	--

This entry clarifies the transport alignment of MPEG-2 transport streams encapsulated within the DTCP-IP link protection system.

8.8.6.5 DTCP-IP encapsulated content

Mandatory decoder friendly alignment position for cleartext.

Profiles:

DTCP_MPEG_TS_SD_NA,
DTCP_MPEG_TS_SD_NA_T,
DTCP_MPEG_TS_SD_NA_ISO,
DTCP_MPEG_TS_HD_NA,
DTCP_MPEG_TS_HD_NA_T,
DTCP_MPEG_TS_HD_NA_ISO,
DTCP_MPEG_TS_SD_EU,
DTCP_MPEG_TS_SD_EU_T,
DTCP_MPEG_TS_SD_EU_ISO,
DTCP_MPEG_TS_SD_KO,
DTCP_MPEG_TS_SD_KO_T,
DTCP_MPEG_TS_SD_KO_ISO,
DTCP_MPEG_TS_HD_KO,
DTCP_MPEG_TS_HD_KO_T,
DTCP_MPEG_TS_HD_KO_ISO

The decoder friendly alignment position for cleartext bitstreams conformant to these profiles shall be the DLNA transport packet boundary.

M	A	n/a	n/a	n/a	IEC 62481-2	2CKL6	
---	---	-----	-----	-----	-------------	-------	--

8.9 General requirements

8.9.1 General

This subclause contains general requirements for devices that implement DTCP-IP.

8.9.2 CP DTCP-IP – Requirements

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

M	R	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	DTCP Volume 1, DTCP Volume 1 Supplement E, DTCP Audio Compliance Rules EXHIBIT B-2, [10]	5GV8W	N
---	---	---------------------	-------------	-----	---	-------	---

Reference [10] defines a grace period that allows vendors to ship products which are conformant with previous specifications.

9 WMDRM-ND link protection system guidelines

9.1 General

This subclause contains guidelines that are specific to the WMDRM-ND link protection system. The guidelines only apply to DLNA devices that implement the WMDRM-ND link protection system. These guidelines are based on WMDRM-ND in IEC 62481-1.

9.2 General requirements

9.2.1 General

This subclause contains general requirements for devices that implement WMDRM-ND.

9.2.2 CP WMDRM-ND – Requirements

9.2.2.1 Content receivers that implement WMDRM-ND shall comply with all requirements in the WMDRM-ND specification [2] at the time the product is offered to the market.

M	A	DMP DMR	M-DMP	MIU	[2]	I2CKL	
---	---	---------	-------	-----	-----	-------	--

The section entitled "Common Cryptographic Elements for Receivers" in [2] lists requirements on the use of encryption algorithms and on output formats, which shall be satisfied by all rendering endpoints that use WMDRM-ND. The section entitled "Protocol Requirements for Receivers" in [2] lists protocol requirements.

9.2.2.2 Content sources that implement WMDRM-ND shall comply with all requirements in the WMDRM-ND specification [2] at the time the product is offered to the market.

M	A	DMS +PU+	M-DMS	n/a	[2]	6WAWI	
---	---	----------	-------	-----	-----	-------	--

The section entitled "common cryptographic elements for transmitters" in [2] lists requirements on the use of encryption algorithms, random number generation and on clock accuracy, which shall be satisfied by all serving endpoints that use WMDRM-ND. The section entitled "protocol requirements for transmitters" in [2] lists protocol requirements.

9.2.3 CP WMDRM-ND – Support for HTTP

9.2.3.1 Content receivers that implement WMDRM-ND shall support the guidelines for the use of WMDRM-ND with the HTTP media transport defined in 9.6.1.

M	A	DMP DMR	M-DMP	MIU	[2]	I6WAW	
---	---	---------	-------	-----	-----	-------	--

9.2.3.2 Content sources that implement WMDRM-ND shall support the guidelines for the use of WMDRM-ND with the HTTP media transport defined in 9.6.1.

M	A	DMS +PU+	M-DMS	n/a	[2]	86HW6	
---	---	----------	-------	-----	-----	-------	--

9.2.4 CP WMDRM-ND – Support for RTP

9.2.4.1 Content receivers that implement WMDRM-ND and that support the RTP media transport for non link protected content should implement WMDRM-ND for the RTP media transport.

S	A	DMP DMR	M-DMP	MIU	[2]	YKV4V	
---	---	---------	-------	-----	-----	-------	--

Content receivers and content sources that implement WMDRM-ND, and also support the optional RTP media transport, are recommended to extend their support for WMDRM-ND to include the RTP media transport.

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

9.2.4.2 Content receivers that implement WMDRM-ND for the RTP media transport shall adhere to the guidelines defined in 9.6.2.

M	A	DMP DMR	M-DMP	MIU	[2]	89TV8	
---	---	---------	-------	-----	-----	-------	--

- 9.2.4.3** Content sources that implement WMDRM-ND and that support the RTP media transport for non link protected content should implement WMDRM-ND for the RTP media transport.

S	A	DMS +PU+	M-DMS	n/a	[2]	KV4VE	
---	---	----------	-------	-----	-----	-------	--

- 9.2.4.4** Content sources that implement WMDRM-ND for the RTP media transport shall adhere to the guidelines defined in 9.6.2.

M	A	DMS +PU+	M-DMS	n/a	[2]	Q89TV	
---	---	----------	-------	-----	-----	-------	--

9.2.5 CP WMDRM-ND – Registration and revalidation procedures

- 9.2.5.1** Content receivers that implement WMDRM-ND shall implement the mapping of the WMDRM-ND registration and revalidation procedures to UPnP, as defined in the section entitled "registration using UPnP" in [2].

M	R	DMP DMR	M-DMP	MIU	[2]	9TV86	
---	---	---------	-------	-----	-----	-------	--

The WMDRM-ND registration procedure allows the content source to uniquely identify the content receiver. It also allows the content source to discover content receivers that do not otherwise announce their presence on the network (e.g., by sending ssdp:alive messages.)

Content receivers invoke the register device action of the X-MS_MediaReceiverRegistrar:1 service (defined in [2]) on the content source as part of the WMDRM-ND registration procedure.

This guideline also applies to the DMR device class.

- 9.2.5.2** Content sources that implement WMDRM-ND shall implement the mapping of the WMDRM-ND registration and revalidation procedures to UPnP, as defined in the section entitled "Registration Using UPnP" in [2].

M	R	DMS +PU+	M-DMS	n/a	[2]	4VEJX	
---	---	----------	-------	-----	-----	-------	--

The WMDRM-ND registration procedure is required to have been completed successfully before a content source is allowed to deliver content (using any media transport) to a content receiver.

- 9.2.5.3** A content source that implements WMDRM-ND shall expose the X-MS_MediaReceiverRegistrar:1 service as one of the services offered by the device.

M	A	DMS +PU+	M-DMS	n/a	[2]	TV86M	C
---	---	----------	-------	-----	-----	-------	---

The mapping of the WMDRM-ND registration and revalidation procedures to UPnP require implementing the X-MS_MediaReceiverRegistrar:1 service. This service shall be implemented on the UPnP device implemented by the content source and invoked by the content receiver. A push controller needs to implement a UPnP device in order to expose the service if it is combined with a DLNA device class that does not require a UPnP device.

- 9.2.5.4** A content receiver that implements WMDRM-ND shall implement an X-MS_MediaReceiverRegistrar:1 service control point.

M	A	DMP DMR	M-DMP	MIU	[2]	V4VEJ	C
---	---	---------	-------	-----	-----	-------	---

9.2.6 CP WMDRM-ND – Discovery of content receivers

Content sources that implement WMDRM-ND shall perform the WMDRM-ND authorization procedure defined in the "Authorization" section of [2] before starting the transfer of a content binary to a content receiver, and shall not transfer content binaries to a content receiver which has not been authorized.

M	R	DMS +PU+	M-DMS	n/a	[2]	WAWIF	
---	---	----------	-------	-----	-----	-------	--

Content sources may discover content receivers by listening for ssdp:alive messages or through the optional mapping of the WMDRM-ND authorization procedure to UPnP. DMRs are required to send ssdp:alive messages, and can be discovered that way. If a content receiver chooses to invoke the IsAuthorized UPnP action (part of the mapping of the WMDRM-ND authorization procedure to UPnP), then this also allows the content source to discover the receiver. content receivers that do not send ssdp:alive messages (such as DMPs) may not be discovered until they perform the WMDRM-ND registration procedure.

9.3 Networking and connectivity

9.3.1 Networking and connectivity – General capability requirements

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

9.3.2 CP WMDRM-ND – QoS requirements

If DLNA QoS as defined in 7.2 of IEC 62481-1 is implemented, all WMDRM-ND proximity detection messages shall be tagged as DLNAQOS_3 or a lower DLNAQOS_UP value, in accordance with Table 3.

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

Proximity detection messages are used to measure the round trip time between the content source and the content receiver. Allowing DLNAQOS_3 for such messages reduces the likelihood that other network traffic will skew the round trip time measurement.

9.4 Device discovery and control

9.4.1 General

This subclause covers the guidelines for implementing device discovery and control using the UPnP device architecture that are specific to the WMDRM-ND link protection system. For detailed information, see 7.3 of IEC 62481-1.

9.4.2 CP WMDRM-ND – Additional rules for DMRs

If WMDRM-ND is supported by a DMR, then its implementation of the control point for the X-MS_MediaReceiverRegistrar:1 service shall comply with all guidelines in 7.3 of IEC 62481-1 for the DMP device class.

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

DMRs are required to invoke the RegisterDevice action of the X-MS_MediaReceiverRegistrar:1 service (defined in Appendix 1 of [2]) on the content source as part of the WMDRM-ND registration procedure.

This means that the DMR is a UPnP control point for the X-MS_MediaReceiverRegistrar:1 service. Subclause 7.3 of IEC 62481-1 specifies rules for UPnP control points. Those guidelines also apply to the implementation of the X-MS_MediaReceiverRegistrar:1 control point.

9.5 Media management

There are no WMDRM-ND specific changes to the guidelines in 7.4 of IEC 62481-1.

9.6 Media transport

9.6.1 HTTP transport

9.6.1.1 General

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

9.6.1.2 CP WMDRM-ND – HTTP support

9.6.1.2.1 When using the WMDRM-ND link protection system, HTTP client endpoints shall implement the mapping of WMDRM-ND to HTTP as specified in the "HTTP Mappings" section of [2].

M	A	DMP DMR	M-DMP	MIU	[2]	KL6LR	
---	---	---------	-------	-----	-----	-------	--

HTTP client endpoints and HTTP server endpoints that implement WMDRM-ND and use the HTTP media transport shall follow the rules for how WMDRM-ND is used with HTTP. Those rules are defined in the subclause called "HTTP Mappings" in the WMDRM-ND specification.

9.6.1.2.2 When using the WMDRM-ND link protection system, HTTP server endpoints shall implement the mapping of WMDRM-ND to HTTP as specified in the "HTTP Mappings" section of [2].

M	A	DMS +PU+	M-DMS	n/a	[2]	6HW6W	
---	---	----------	-------	-----	-----	-------	--

9.6.1.3 CP WMDRM-ND – Media format profiles that use ASF when using HTTP

When using the WMDRM-ND link protection system with the HTTP media transport, a DLNA endpoint transferring a content binary that uses ASF encapsulation shall follow the rules below.

- The rules in the "Data Transfer" section of [2].
- The rules in the section entitled "Rules Common to All Content" in the "Data Transfer Using HTTP" section of [2].
- The rules in the section entitled "Windows Media-based Content" in the "Data Transfer Using HTTP" section of [2].

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	IEC 62481-2 [2]	E369K	
---	---	---------------------	-------------	-----	--------------------	-------	--

Content encapsulated in ASF uses ASF sample encryption (defined in [2]). It involves adding the advanced encryption object in the ASF file header, and including a sample ID ASF packet extension in each encrypted ASF packet.

Media format profiles that use ASF encapsulation are defined in IEC 62481-2.

Examples of such profiles include the WMA profiles in Table 10 and the WMV9 profiles in Table 15 of IEC 62481-2 and all profiles whose name starts with MPEG4_PS_ASF_.

9.6.1.4 CP WMDRM-ND – MPEG-2 transport stream content when using HTTP

When using the WMDRM-ND link protection system with the HTTP media transport, a DLNA Endpoint transferring a content binary that uses MPEG-2 transport stream shall follow the rules below.

- The rules in the "Data Transfer" section of [2].

- The rules in the section entitled "Rules Common to All Content" in the "Data Transfer Using HTTP" section of [2].
- The rules in the section entitled "MPEG-2 Transport Stream Content" in the "Data Transfer Using HTTP" section of [2].

M	A	DMS +PU+	DMP	DMR	M-DMS M-DMP	MIU	IEC 62481-2 [2]	HW6WF	
---	---	-------------	-----	-----	-------------	-----	--------------------	-------	--

For content that uses MPEG-2 transport stream encapsulation, additional MPEG-2 transport packets, called TAG packets, are inserted in front of each protected PES packet in the transport stream.

Media format profiles that use MPEG-2 transport stream encapsulation are defined in IEC 62481-2.

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

9.6.1.5 CP WMDRM-ND – Link encryption mode when using HTTP

When using the WMDRM-ND link protection system with the HTTP media transport, a DLNA endpoint transferring a content binary that does not use ASF or MPEG-2 transport stream encapsulation shall follow these rules:

- The rules in the "Data Transfer" section of [2].
- The rules in the section entitled "Rules Common to All Content" in the "Data Transfer Using HTTP" section of [2].
- The rules in the section entitled "Other Content Types" in the "Data Transfer Using HTTP" section of [2].

M	A	DMS +PU+	DMP	DMR	M-DMS M-DMP	MIU	IEC 62481-2 [2]	VE369	
---	---	-------------	-----	-----	-------------	-----	--------------------	-------	--

In this case, the WMDRM-ND link encryption mode is used. It is defined in the "Link Encryption Mode" section of [2]. The content source partitions the content binary into an arbitrary number of data segments. Each data segment is encrypted independently and transmitted together with a data segment descriptor (defined in [2]).

9.6.1.6 CP WMDRM-ND – Link protection alignment element when using HTTP

When using the WMDRM-ND link protection system with the HTTP media transport, a link protection alignment element is defined as follows.

- For ASF sample encryption: An ASF packet or the ASF file header.
- For content that use MPEG-2 transport stream: A MPEG-2 TS packet.
- For content that use the WMDRM-ND link encryption mode: The framing header defined in the "HTTP framing headers" section of [2] followed by the number of bytes indicated in the framing header.

M	A	DMS +PU+	DMP	DMR	M-DMS M-DMP	MIU	IEC 62481-2 [2]	DM2LQ	
---	---	-------------	-----	-----	-------------	-----	-----------------	-------	--

IEC 62481-2 defines which media format profiles use MPEG-2 transport stream.

9.6.1.7 CP WMDRM-ND – Cleartext byte seek request header

9.6.1.7.1 When using the WMDRM-ND link protection system, HTTP client and server endpoints shall use the Cleartext-Range.dlna.org header as the cleartext byte seek request header.

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

9.6.1.7.2 The notation of the Cleartext-Range.dlna.org header field for HTTP media transport of WMDRM-ND link protected content shall be as stated below:

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

first-cleartextbyte-pos and last-cleartextbyte-pos apply to the cleartext byte domain, the content binary immediately before WMDRM-ND processing, i.e. before encryption.

Note that the literal "bytes" is case sensitive.

Examples:

- Cleartext-Range.dlna.org: bytes=1539686400-
- Cleartext-Range.dlna.org: bytes=1539686400-1540210688

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

9.6.1.8 CP WMDRM-ND – Cleartext byte seek response header

9.6.1.8.1 When using the WMDRM-ND link protection system, HTTP client and server endpoints shall use the Cleartext-Content-Range.dlna.org header as the cleartext byte seek response header.

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

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

- Cleartext-Content-Range.dlna.org = "Cleartext-Content-Range.dlna.org" ":" content-range-spec;
- content-range-spec = byte-content-range-spec;
- byte-content-range-spec = bytes-unit SP byte-range-resp-spec "/" (instance-length | "**");
- bytes-unit = "bytes";
- byte-range-resp-spec = first-cleartextbyte-pos "-" last-cleartextbyte-pos;
- first-cleartextbyte-pos = 1*DIGIT;
- last-cleartextbyte-pos = 1*DIGIT;
- instance-length = 1*DIGIT;

first-clear-text-byte-pos, last-clear-text-byte-pos and instance-length apply to the clear-text byte domain, the content binary immediately before WMDRM-ND processing, i.e. before encryption.

Note that the literal "bytes" is case sensitive.

Example :

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

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

The positions specified in this header refer to positions in the clear-text byte domain.

9.6.2 RTP transport

9.6.2.1 General

This subclause covers the guidelines for the RTP transport protocol for DLNA devices using the WMDRM-ND link protection system. The guidelines in this subclause apply only to DLNA devices that implement both the RTP media transport and the WMDRM-ND link protection system.

9.6.2.2 CP WMDRM-ND – RTP support

- 9.6.2.2.1** When using the WMDRM-ND link protection system, receiving endpoints shall implement the mapping of WMDRM-ND to RTP and RTSP defined in the "RTSP Mappings" section of [2].

M	A	DMP DMR	M-DMP	MIU	[2] [6] [7]	FS8VM	
---	---	---------	-------	-----	-------------	-------	--

Receiving endpoints and serving endpoints that implement WMDRM-ND and use it with the RTP media transport shall follow the rules for how WMDRM-ND is used with RTSP and RTP. Those rules are defined in the section called "RTSP Mappings" in the WMDRM-ND specification.

- 9.6.2.2.2** When using the WMDRM-ND link protection system, serving endpoints shall implement the mapping of WMDRM-ND to RTP and RTSP defined in the "RTSP Mappings" section of [2].

M	A	DMS +PU+	M-DMS	n/a	[2] [6] [7]	8V5U9	
---	---	----------	-------	-----	-------------	-------	--

9.6.2.3 CP WMDRM-ND – RTP license update procedure

Serving endpoints shall satisfy the following requirements when performing a WMDRM-ND license update procedure by sending an ANNOUNCE request to the content receiver.

- Follow the requirements for the WMDRM-ND license update procedure in the "License Update Details for Transmitters" section of the "License Updates Using RTSP" section in [2].
- The EVENT-TYPE.DLNA.ORG header (7.5.8.2.17 in IEC 62481-1) shall be included in the ANNOUNCE request and its event-code parameter shall be set to 4000.
- The ANNOUNCE request shall include the CSEQ header.
- The ANNOUNCE request shall include the SESSION header.

M	A	DMS +PU+	M-DMS	n/a	IEC 62481-1 [2] [6] [7]	5U96O	
---	---	----------	-------	-----	----------------------------	-------	--

9.6.2.4 CP WMDRM-ND – WMA and WMV media format profiles when using RTP

When using the WMDRM-ND link protection system with the RTP media transport, content that is derived from WMA or WMV media format profiles shall follow the rules below.

- The rules in the section entitled "Data Transfer" in [2].
- The rules in the section entitled "Windows Media-based Content" in the "Data Transfer Using RTSP" section of [2].
- The guidelines in 7.5.7.8 of IEC 62481-1.

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	IEC 62481-1 IEC 62481-2 [2] [3] [6] [7]	8VM6S	
---	---	---------------------	-------------	-----	---	-------	--

WMA and WMV content uses ASF sample encryption (defined in [2]) and is encapsulated using the RTP payload format for WMA and WMV in [3]. The guidelines in 7.5.7.8 of IEC 62481-1 for this RTP payload format still apply.

Media format profiles that use WMA and WMV are defined in Table 10 and Table 15 of IEC 62481-2.

9.6.2.5 CP WMDRM-ND – MPEG-2 ES media format profiles when using RTP

When using the WMDRM-ND link protection system with the RTP media transport, content that is derived from MPEG elementary stream media format profiles shall follow the rules below.

- The rules in the section entitled "Data Transfer" in [2].
- The rules in the section entitled "MPEG-2 Elementary Stream Content" in the "Data Transfer Using RTSP" section of [2].

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	IEC 62481-2 [2] [6] [7]	V5U96	
---	---	---------------------	-------------	-----	----------------------------	-------	--

The "Data Transfer Using RTSP" section of [2] specifies how MPEG-2 elementary stream content is encrypted and encapsulated with the RTP payload format in [3].

This guideline applies to MPEG_ES media format profiles, e.g., WMDRM_MPEG_ES_NTSC and WMDRM_ND_MPEG_ES_PAL_XAC3.

Media format profiles for MPEG-2 elementary streams are defined in IEC 62481-2.

9.6.2.6 CP WMDRM-ND – MPEG-2 transport stream content when using RTP

When using the WMDRM-ND link protection system with the RTP media transport, content that use MPEG-2 transport stream encapsulation shall follow the rules below.

- The rules in the section entitled "Data Transfer" in [2].
- The rules in the section entitled "MPEG-2 Transport Stream Content" in the "Data Transfer Using RTSP" section of [2].
- The guidelines in 7.5.6.3 of IEC 62481-1.

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	IEC 62481-2 [2] [6] [7]	S8VM6	
---	---	---------------------	-------------	-----	----------------------------	-------	--

For content that uses MPEG-2 transport stream encapsulation, additional MPEG-2 transport packets, called TAG packets, are inserted in front of each protected PES packet in the transport stream.

Media format profiles that use MPEG-2 transport stream encapsulation are defined in IEC 62481-2.

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

9.6.2.7 CP WMDRM-ND – Link encryption mode when using RTP

When using the WMDRM-ND link protection system with the RTP media transport, content that is not derived from WMA, WMV, MPEG elementary stream, or MPEG-2 transport stream media format profiles, shall follow the rules below.

- The rules in the section entitled "Data Transfer" in [2].
- The rules in the section entitled "Other Content Types" in the "Data Transfer Using RTSP" section of [2].
- The guidelines in 7.5.6.3 of IEC 62481-1.

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	IEC 62481-2 [2] [6] [7]	344ZV	
---	---	---------------------	-------------	-----	----------------------------	-------	--

In this case, the WMDRM-ND link encryption mode is used. It is defined in the "Link Encryption Mode" section of [2].

The payload of each RTP packet is encrypted independently and transmitted together with a data segment descriptor (defined in [2]).

9.7 Content conversion device virtualization

There are no guidelines specific to WMDRM-ND for content conversion and device virtualization.

9.8 Media interoperability unit (MIU)

There are no guidelines specific to WMDRM-ND for media interoperability units.

9.9 Media format – WMDRM-ND profiling guidelines

9.9.1 General

This subclause contains additions to IEC 62481-2, defining the WMDRM-ND media format profiles. This subclause contains guidelines that are specific to the WMDRM-ND link protection system. The guidelines only apply to DLNA devices that implement the WMDRM-ND link protection system.

9.9.2 CP WMDRM-ND – Identification of content transferred using WMDRM-ND

- 9.9.2.1** The profile ID of WMDRM-ND protected content shall comply with the following syntax.

ProfileID_Protected = "WMDRM_" Original_ProfileID.

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

Example: If content that complies with the WMABASE profile ID is transferred with WMDRM-ND protection, then the profile ID of the protected content shall be WMDRM_WMABASE.

M	A	MHD	HND	n/a	IEC 62481-2 [2]	J344Z	
---	---	-----	-----	-----	--------------------	-------	--

The "WMDRM_" prefix is added to the original profile ID to make it possible to determine that the content is transferred with WMDRM-ND link protection.

- 9.9.2.2** A content object that represents a link protected form of one of the DLNA media classes shall use the media class value of the cleartext content.

M	L	DMS +PU+	M-DMS	MIU	IEC 62481-2	YAO6A	
---	---	----------	-------	-----	-------------	-------	--

For example, link protected content that, in its cleartext form, conforms to the DLNA "AV" media class shall use object.item.videoItem or a derived class for the upnp:class value.

9.9.3 CP WMDRM-ND – Media format requirements

- 9.9.3.1** Content using a WMDRM_ Profile ID shall only be transferred using the WMDRM-ND link protection system [2].

M	A	DMS +PU+	M-DMS	MIU	[2]	EYAO6	
---	---	----------	-------	-----	-----	-------	--

- 9.9.3.2** Devices that transfer or receive content using WMDRM_ profile ID shall adhere to all mandatory requirements of the WMDRM-ND link protection system [2] at the time the product is offered to the market.

M	A	MHD	HND	n/a	[2]	U7QOS	
---	---	-----	-----	-----	-----	-------	--

- 9.9.3.3** If content using a WMDRM_ profile ID contains both a cleartext portion and a non-cleartext portion, then the entire content binary shall be transferred with WMDRM-ND [2] encapsulation.

M	A	DMS +PU+	M-DMS	MIU	[2]	7QOSM	
---	---	----------	-------	-----	-----	-------	--

It is not permitted to switch from protected mode to unprotected mode, or vice versa, during the transfer of a single content binary.

9.9.4 CP WMDRM-ND – MIME type

For content that is transferred using WMDRM-ND, the third field of protocolInfo shall be set to the same value as it would be set to if the content did not use DLNA link protection.

M	L	DMS +PU+	M-DMS	MIU	IEC 62481-1	2LQ77	
---	---	----------	-------	-----	-------------	-------	--

The third field of protocolInfo shall be used in the same way as it is for cleartext content.

9.9.5 CP WMDRM-ND – Decoder friendly alignment position

The decoder friendly alignment position for content using a WMDRM_ profile ID shall be the same as would be used for the cleartext version of the same content.

M	A	MHD	HND	n/a	IEC 62481-2	369K5	
---	---	-----	-----	-----	-------------	-------	--

9.9.6 CP WMDRM-ND – Media format alignment element

The media format alignment element for content using a WMDRM_ profile ID shall be the same as would be used for the cleartext version of the same content.

M	A	MHD	HND	n/a	IEC 62481-2	W6WFS	
---	---	-----	-----	-----	-------------	-------	--

Annex A (informative)

An introduction to DLNA seek operations

A.1 General

Seek operations are a key element to DLNA guidelines used to support many of the core media operations. In DLNA there are two domains in which a seek operation can be performed. There is the time domain, where positions within the content binary are specified as time offsets from the beginning. And the network byte domain, where positions are specified by a byte offset from the start of the content binary as it was transmitted by the media transport. When link protected content is transmitted, the situation is complicated in that the network byte domain contains protected bytes. As will be shown, this introduces difficulties to the rendering endpoint of specifying the correct position within the content stream. This clause introduces the seek models used within DLNA and how they are adapted in the link-protected.

A.2 UCDAM and seek operations

The uniform content data availability model as specified in the DLNA guideline appendix is a conceptual framework used to describe the bytes of the content stream and the ranges over which the content receiver can perform seek operations. Figure A.1 shows the core elements of the UCDAM as they relate to seek operations.

A content binary always starts at position d_X and ends at position d_Y . For content that is stored in a file $d_X = 0$ and $d_Y =$ the length of the file. For live content, $d_X = -8$ and $d_Y = 8$. Within this range of content, there is a restricted set of the content that the server can source at any time; this is the range $[S_0, S_N]$. This is the range that we will typically be interested in for seek operations, since it represents the range of content that the server can make available at any time. For some models of seek operations, there is also a reduced range $[R_0, R_N]$. The range $[R_0, R_N]$ represents the content that the server can make available for random seek operations in a timely fashion. For most seek models the range $[S_0, S_N] = [R_0, R_N]$. However, for one seek mode, defined below, the ranges are not equal.

These ranges are conceptual in that the minimum value of the ranges is not specified by the DLNA guidelines. These guidelines are typically dependent on the buffering model of the content and the type of the content. These ranges allow us to discuss content that is stored on a disk in the same way that we discuss "live", unbuffered content. For example, in the former case $[S_0, S_N]$ will equal the entire content binary. In the latter case, $S_0=S_N =$ the byte that is available at this moment. This provides a common notation for describing the important attributes of the content stream within the guidelines.

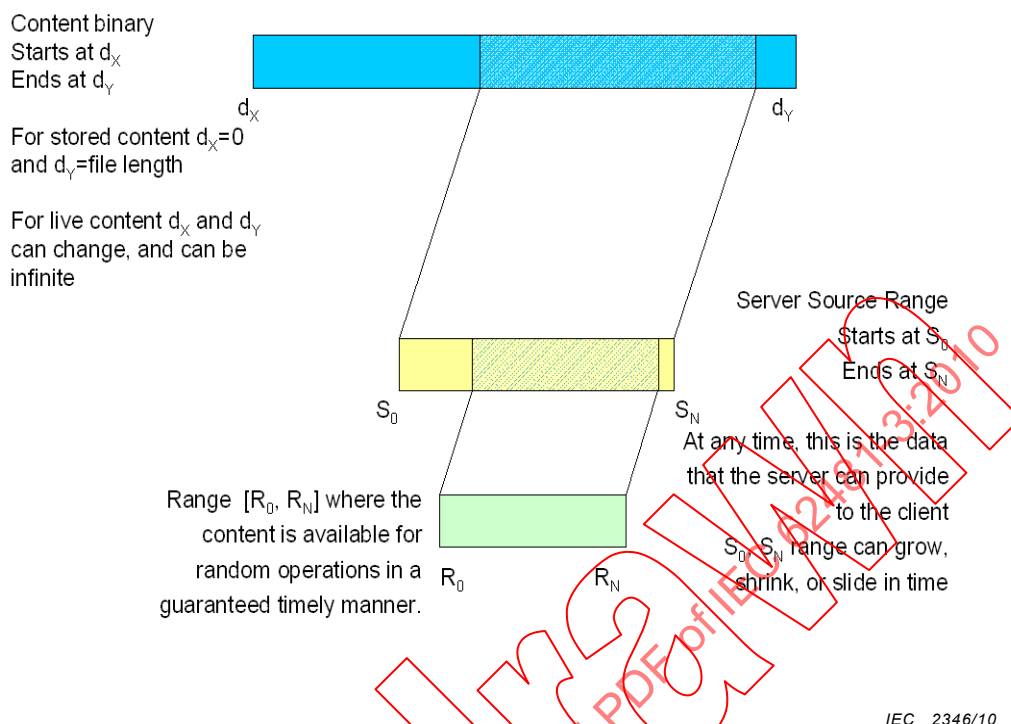


Figure A.1 – UCDAM definitions for seek operations

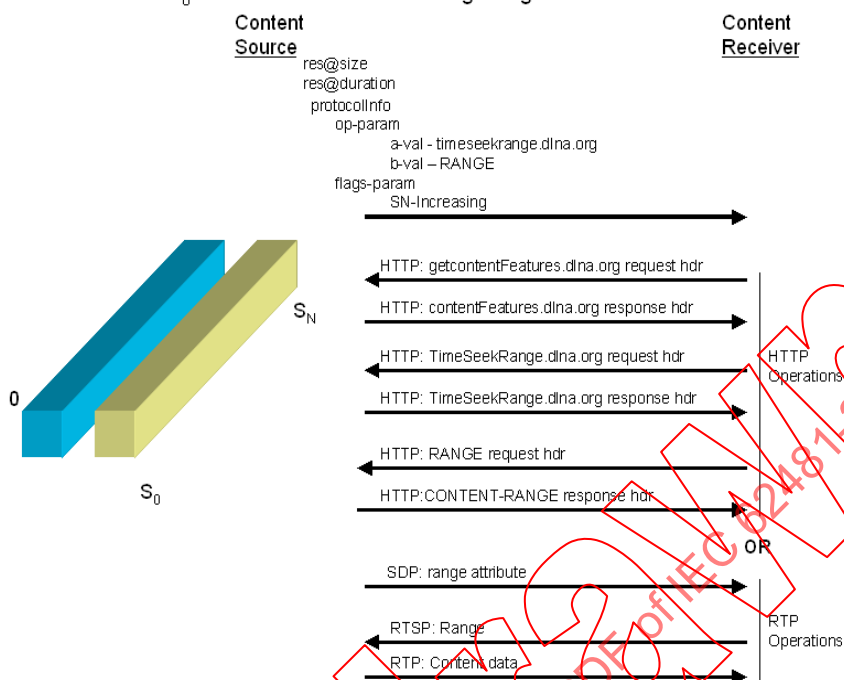
A.3 Seek models

There are two seek models defined in the DLNA guidelines. The full random access data availability model is used when the range $[S_0, S_N]$ equals the entire content binary. The limited random access data availability model is used when the range $[S_0, S_N]$ is a limited subset of the content binary. The limited random access data availability model can also be used in two modes. Mode 0 is used when S_0 is changing. Mode 1 is used when only a restricted range, $[R_0, R_N]$, can guarantee timely responses to seek requests.

A.4 Full random access data availability

In DLNA V1.0, the only seek model was the full random access data availability model. It is defined when the range $[S_0, S_N] = [R_0, R_N]$ and is the entire content binary. The DLNA constructs that are used to implement it are shown in Figure A.2. This clause contains the full model as it is specified in the DLNA current guidelines, for the initial DLNA guidelines for devices, the case where S_N is increasing is not allowed and the RTP transport is not allowed.

Source range = the entire content binary at any given time. S_N may increase with time but S_0 must remain fixed at the beginning



IEC 2347/10

Figure A.2 – Full random access data availability model

The metadata attributes and headers used to implement this model are shown in Table A.1.

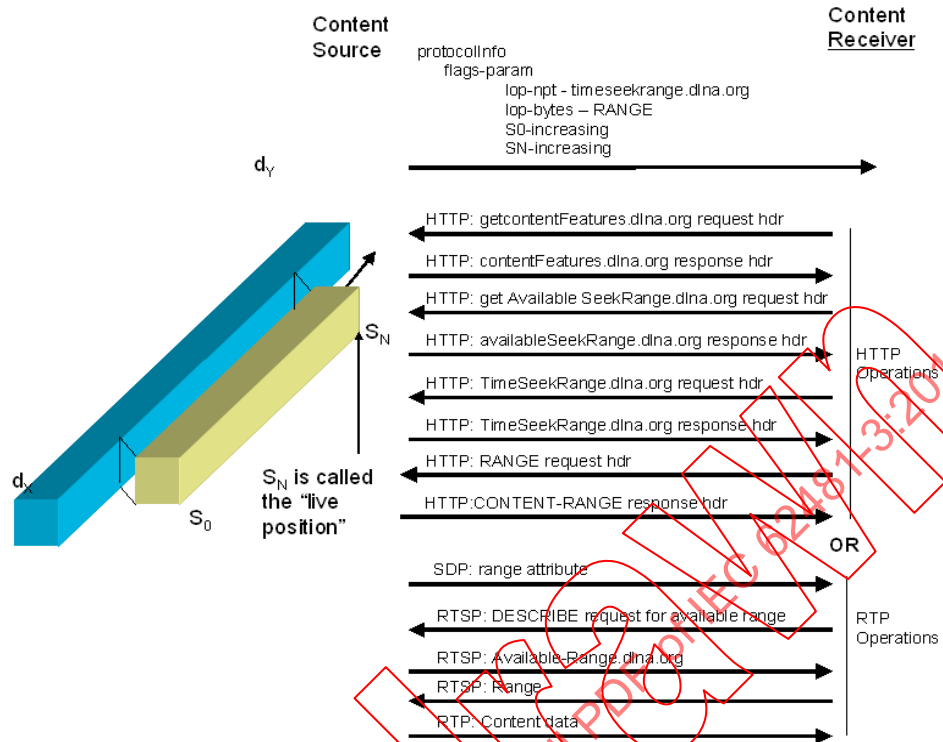
Table A.1 – DLNA constructs of full random access data availability mode

Construct	Use	IEC 62481-1
Definition of full random data availability model	Defines the requirements for the model	7.5.4.2.14 7.5.5.2.18 7.5.4.2.15 7.5.5.2.19
Op-param	Specifies if byte or time seek are available.	7.4.1.3.18 7.4.1.3.19 7.4.1.3.20
Flags-param	sN-increasing = S _N boundary moving	7.4.1.3.23 7.4.1.3.33
res@size res@duration	Defines the ending point of the search range	7.4.1.3.11
getcontentFeatures.dlna.org contentFeatures.dlna.org	Requests the Op-param to verify seek operations are available in HTTP	7.4.1.3.12
TimeSeekRange.dlna.org	Time domain seek operation for HTTP	7.5.5.2.24
RANGE HTTP request header	Byte domain seek operation for HTTP	7.5.5.2.21 7.5.5.2.22
CONTENT-RANGE resp. header	Response to byte seek operation for HTTP	7.5.5.2.19 7.5.5.2.22
CONTENT-LENGTH resp. header	Specifies the length of the response in HTTP	7.5.5.2.15
Range SDP attribute	Specifies that the server will support time seek operations in RTP	7.5.8.2.41
Range RTSP header	Time domain seek operation for RTP	7.5.8.2.41 7.5.8.2.42 7.5.8.2.43

A.5 Limited random access data availability

The limited random access data availability model was added after the initial version of the DLNA guidelines. Under it, the range [S0, SN] does not equal the entire content binary. In this model, there are two modes. The DLNA constructs for the modes are shown in the following diagrams, see Figure A.3 and Figure A.4.

Source range = the searchable range at any time, both S_0 and S_N change with time.



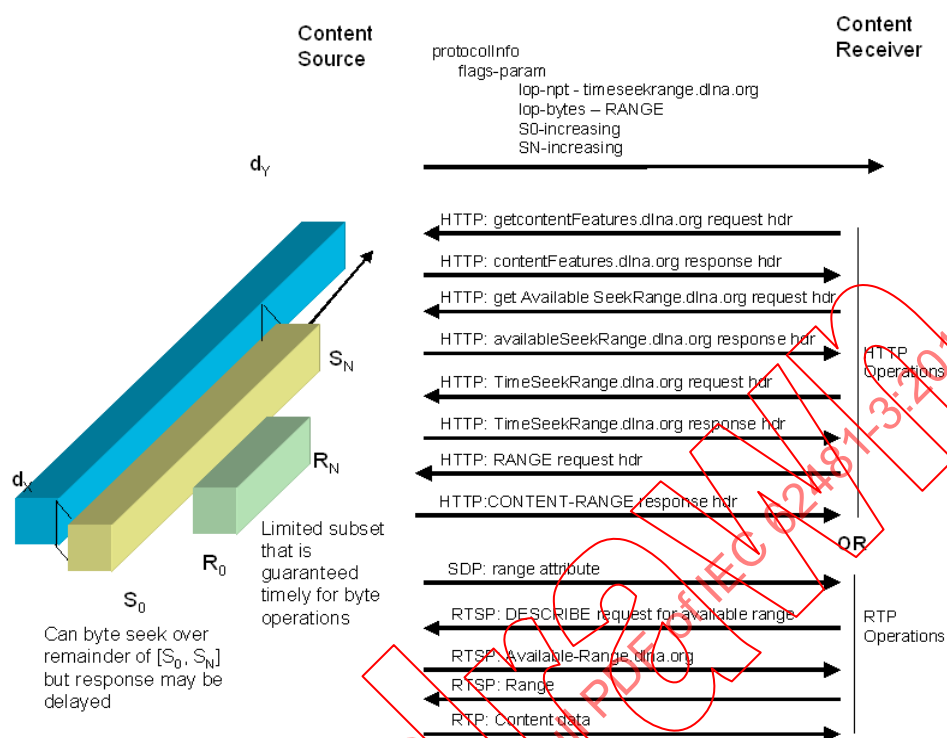
IEC 2348/10

Figure A.3 – Limited random access data availability model mode 0

In mode 0, $[S_0, S_N] = [R_0, R_N]$ and S_0 changes with time, S_N may also change with time to implement a sliding window of content that is available. This model is typically used with live captured content on the server that has a certain amount of the content stored in a temporary buffer. The key difference between the DLNA constructs used for this model are the `getAvailableSeekRange.dlna.org` request header and the `availableSeekRange.dlna.org` header used to request and reply with the range $[S_0, S_N]$.

Mode 1 and the DLNA constructs used to implement it are shown in the following Figure A.4.

Source range = the searchable range at any time, S_0 is fixed at the beginning and S_N changes with time.



IEC 2349/10

Figure A.4 – Limited random access data availability mode 1

In this model, $[S_0, S_N] \supset [R_0, R_N]$. The range $[R_0, R_N]$ represents the content that the server can respond with in a guaranteed timely manner. The range $[S_0, S_N]$ can be accessed, but the server cannot guarantee that it will be able to quickly respond to a request in this range. The DLNA constructs used to define and operate within this seek mode are the same as for mode 1. All of the DLNA constructs are outlined in Table A.2.

Table A.2 – DLNA constructs of limited random access data availability model

Construct	Use	IEC 62481-1
Definition of limited random data availability model	Defines the requirements for the model	7.5.4.2.14 7.5.5.2.18 7.5.4.2.16 7.5.5.2.20
Flags-param	Specifies the parameters of the model lop-npt = limited time seek lop-bytes = limited byte seek sN-increasing = S_N boundary moving s0-increasing = S_0 boundary moving	7.4.1.3.23 7.4.1.3.32 7.4.1.3.28 7.4.1.3.33 7.4.1.3.29
getContentFeatures.dlna.org contentFeatures.dlna.org	HTTP requests for the Flags- param to verify seek operations are available	7.5.5.2.10
getavailableSeekRange.dlna.org availableSeekRange.dlna.org	HTTP request for the available byte and time range [S_0 , S_N]	7.5.5.2.20
TimeSeekRange.dlna.org	HTTP time domain seek on [S_0 , S_N]	7.5.5.2.24
RANGE request header	HTTP byte domain seek on [S_0 , S_N]	7.5.5.2.21 7.5.5.2.22
CONTENT-RANGE resp. header	HTTP response to byte domain seek	7.5.5.2.19 7.5.5.2.22
CONTENT-LENGTH resp. header	Specifies the length of the response in HTTP	7.5.5.2.15
range SDP attribute	Specifies that the server will support time seek operations in RTP	7.5.8.2.41
DESCRIBE RTSP request	Request the available seek range [S_0 , S_N]	7.5.8.2.29
Available-Range.dlna.org RTSP header	Return the available seek range [S_0 , S_N]	7.5.8.2.20 7.5.8.2.30
Range RTSP header	Time domain seek operation for RTP	7.5.8.2.41 7.5.8.2.42 7.5.8.2.43

A.6 Seek operations on link protected content

For unprotected content, the following diagram shows the content flowing from the source server to the content receiver, here shown as a rendering engine for playback.

Unprotected Content

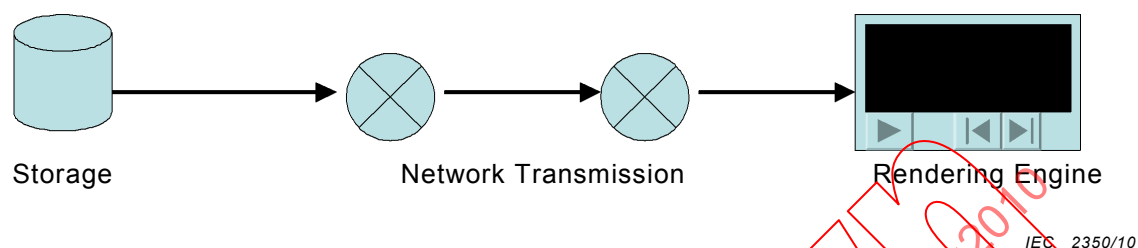


Figure A.5 – Content flow unprotected content

In this case, the rendering engine receives the bytes of the content from the network transmission and can perform a byte seek to a particular location. This request can flow back to the server as a request using the HTTP RANGE headers. The bytes that the rendering engine are displaying are unaltered from the bytes that are flowing across the network so no transformation has to occur between the rendering engine requesting "byte 500" and the network transmission requesting "byte 500".

With link protected content, the situation is different. The following diagram shows a hypothetical content flow for link protected content. The black arrows represent unprotected content while the red arrows show content that has had link protection applied.

Protected Content

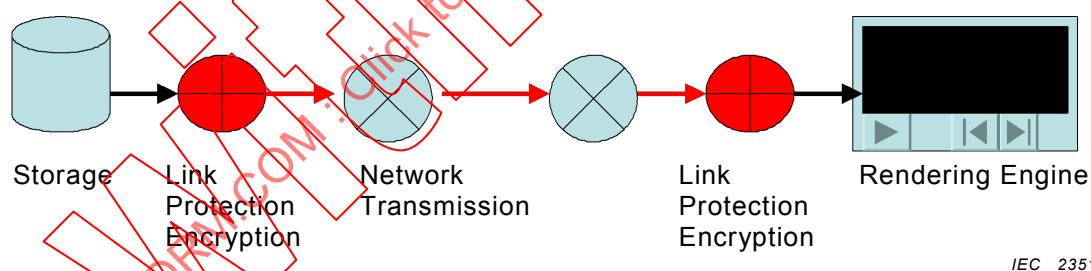


Figure A.6 – Content flow link protected content

In this case, a link protection transformation has been placed between the rendering engine and the network transmission. Now, when the rendering engine requests "byte 500" the network transmission HTTP RANGE header cannot necessarily be used. The link protection system may have added headers or padding bytes. It may not be possible to determine the correct network bytes to request. It is important for the rendering engine to be able to seek on the unprotected content. Hypothetically, suppose the same content binary were being transmitted in each of the above Figure A.5 and Figure A.6, the first without link protection and the second with. The rendering engine should be able to expect the same set of bytes when requesting "byte 500" on the content streams since it may or may not be aware of the presence of link protection in the implementation.

In DLNA guidelines there are 2 seek domains; the time domain, where locations are specified in time units and the byte domain where units are specified in bytes. The use of the network RANGE header in DLNA guidelines make the assumption that the byte domain rendered by the receiver is the same as the network byte domain.

The way that these guidelines solve the problem of seeking in the link protected content stream is to recognize that byte seeking in DLNA guidelines is the "network byte seek domain" and to introduce an additional domain, the "cleartext byte domain". Thus there are three seek domains with their own headers to transfer the necessary values.

- Time domain – ranges and positions are specified in time units.
- Network byte domain – ranges and positions are specified in bytes and are positions and ranges as seen in the content flowing across the network transport.
- Cleartext byte domain – ranges and positions are specified in bytes and are positions and ranges specified within the unprotected content stream.

All three of these domains are available on any of the random access data availability models, however, as in DLNA current guidelines only one random access data availability model applies at any time to all domains. For protected content, there are no changes to previous DLNA guideline headers for the time seek domain, or the network byte seek domain. However, it shall be understood that use of the network byte seek domain implies that the seek occurs within the protected content stream after application of the link protection system. These guidelines define the cleartext byte domain, the metadata used to specify the availability of the operations in this domain and the headers used to convey the necessary information.

For link protected content, the three domains listed above operate independently under the same data availability model. For non-link protected content, the content receiver can perform a seek operation in either the time domain or the network byte domain. For link protected content, the content receiver can perform a seek operation in the time domain, the network byte domain, or the cleartext byte domain. In this case, the network byte domain represents a byte position within the protected content stream and the cleartext byte domain represents a byte position within the content stream before link protect has been applied.

Bibliography

- [1] IETF RFC 1191, *Path MTU Discovery*, J. Mogul, DECWRL, S. Deering, Stanford University, November 1990
<http://www.ietf.org/rfc/rfc1191.txt>
- [2] WMDRM-ND, *Windows Media DRM for Network Devices*
<http://wmlicense.smdisp.net/licenserequest/default.asp>
- [3] *RTP Payload format for WMV and WMA, RTP Payload Format for Windows Media Audio and Video*, Microsoft Corporation
http://download.microsoft.com/download/5/5/a/55a7b886-b742-4613-8ea8-d8b8b5c27bbc/RTPPayloadFormat_for_WMAandWMV_v1.doc
- [4] IETF RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1*, R. Fielding, UC Irvine, J. Gettys, Compaq/W3C, J. Mogul, Compaq, H. Frystyk, W3C/MIT, L. Masinter, Xerox, P. Leach, Microsoft*, T. Berners-Lee, June 1999
<http://www.ietf.org/rfc/rfc2616.txt?number=2616>
- [5] *UPnP ConnectionManager:1, ConnectionManager:1 Service Template Version 1.01*, UPnP Forum, June 25, 2002
<http://www.upnp.org/standardizeddcps/documents/ConnectionManager1.0.pdf>
- [6] IETF RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*, H. Schulzrinne, Columbia University, S. Casner, Packet Design, R. Frederick, Blue Coat Systems Inc., V. Jacobson, Packet Design, July 2003
<http://www.ietf.org/rfc/rfc3550.txt>
- [7] IETF RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*, H. Schulzrinne, Columbia University, S. Casner, Packet Design, July 2003
<http://www.ietf.org/rfc/rfc3551.txt>
- [8] *UPnP AVTransport:1, AVTransport:1 Service Template Version 1.01*, UPnP Forum, June
<http://www.upnp.org/standardizeddcps/documents/AVTransport1.0.pdf>
- [9] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, S. Bradner, March 1997
<http://www.ietf.org/rfc/rfc2119.txt>
- [10] DTCP Adopter Agreement Digital Transmission Protection License Agreement, May 2005
<http://www.dtcp.com/data/AA05312005.pdf>
- [11] *UPnP ContentDirectory:1, ContentDirectory:1 Service Template Version 1.01*, UPnP Forum, June 25, 2002
<http://www.upnp.org/standardizeddcps/documents/ContentDirectory1.0.pdf>
-

SOMMAIRE

AVANT PROPOS	71
1 Domaine d'application	73
2 Références normatives	73
3 Termes, définitions et acronymes	74
3.1 Termes et définition	74
3.2 Abréviations	79
4 Architecture de réseau domestique DLNA	79
5 Modèle de dispositif DLNA	79
6 Terminologie et conventions des directives	80
6.1 Classifieurs de conformité des directives	80
6.2 Norme des classifieurs d'utilisation de spécification	80
6.3 Conventions d'utilisation des polices de caractères des directives	81
6.4 Convention de notation de syntaxe des directives	81
6.5 Conventions de textes normatifs et informatifs des directives	81
6.6 Espaces de nom et schémas XML DLNA	81
7 Directives communes pour la protection de liaison	82
7.1 Généralités	82
7.2 Conditions relatives au temps de mesure dans les échanges de messages	86
7.3 Mise en réseau et connectivité	86
7.3.1 Généralités	86
7.3.2 Nouvelles exigences de capacité générales– «Bluetooth» NC CP – Modes d'économie d'énergie	86
7.4 Découverte et pilotage de dispositif	87
7.5 Gestion du support	87
7.5.1 Gestion du support – Gestion du support AV (Audio avec vidéo)	87
7.5.2 Directives pour la gestion des supports AV (Audio avec vidéo)	90
7.6 Transport du support	94
7.6.1 Généralités	94
7.6.2 Protocoles de transport du support	94
7.6.3 Transport HTTP	95
7.6.4 Directives concernant le transport de support HTTP pour le transfert en flux continu	103
7.6.5 Directives concernant le transport de support HTTP pour transfert interactif	104
7.6.6 Transport RTP (Protocole en temps réel)	105
7.7 Virtualisation du dispositif de conversion de contenu	105
7.8 Unité d'interopérabilité de support (MIU)	106
7.9 Exigences des directives concernant la technologie de protection de liaison	106
7.9.1 Système de protection de liaison– DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)	106
7.9.2 Système de protection de liaison – DRM (gestion des droits numériques) «Windows media» pour dispositifs réseau	107
8 Directives concernant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)	108
8.1 Généralités	108
8.2 Mise en réseau et connectivité	108

8.2.1	Mise en réseau et connectivité – Exigences de capacité générales	108
8.2.2	Nouvelles exigences de DLNAQOS exigence de QoS (Qualité de service) pour le trafic DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)	108
8.2.3	Nouvelles exigences des dispositifs – NC CP commun – Sécurité sans fil.....	108
8.3	Découverte et pilotage de dispositif.....	108
8.4	Gestion du support.....	109
8.4.1	Gestion du support – Gestion du support AV (Audio avec vidéo)	109
8.4.2	MM CP - URI (Identificateur uniforme de ressource) DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).....	109
8.5	Transport de support.....	109
8.5.1	Transport HTTP.....	109
8.5.2	Transport RTP (Protocole en temps réel).....	111
8.6	Virtualisation du dispositif de conversion de contenu.....	113
8.7	Unité d'interopérabilité de support (MIU)	113
8.8	Format de support – Directives de profilage DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).....	113
8.8.1	Généralités.....	113
8.8.2	CP DTCP-IP – Profil.....	113
8.8.3	CP DTCP-IP – Définition du type de profil MIME (Extension de courrier Internet à fonctions multiples).....	114
8.8.4	CP DTCP-IP – Parties de contenu de profil protégé et non protégé	115
8.8.5	CP DTCP-IP – Encapsulation de profil HTTP.....	116
8.8.6	Encapsulation de profil DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)	116
8.9	Exigences générales.....	119
8.9.1	Généralités.....	119
8.9.2	CP DTCP-IP – Exigences	119
9	Directives concernant le système de protection de liaison WMDRM-ND.....	119
9.1	Généralités.....	119
9.2	Exigences générales.....	119
9.2.1	Généralités.....	119
9.2.2	CP WMDRM-ND – Exigences	119
9.2.3	CP WMDRM-ND – Prise en charge pour HTTP.....	120
9.2.4	CP WMDRM-ND – Prise en charge pour RTP (Protocole en temps réel).....	120
9.2.5	CP WMDRM-ND – Modes opératoires d'enregistrement et de revalidation.....	121
9.2.6	CP WMDRM-ND – Découverte de récepteurs de contenu	121
9.3	Mise en réseau et connectivité	122
9.3.1	Mise en réseau et connectivité – Exigences de capacité générales	122
9.3.2	CP WMDRM-ND – Exigences de QoS (Qualité de service)	122
9.4	Découverte et pilotage de dispositif.....	122
9.4.1	Généralités.....	122
9.4.2	CP WMDRM-ND – Règles supplémentaires pour les DMR.....	122
9.5	Gestion du support.....	122
9.6	Transport du support.....	123
9.6.1	Transport HTTP.....	123
9.6.2	Transport RTP (Protocole en temps réel).....	126

9.7	Virtualisation du dispositif de conversion de contenu	129
9.8	Unité d'interopérabilité de support (MIU)	129
9.9	Format de support - Directives de profilage WMDRM-ND	129
9.9.1	Généralités.....	129
9.9.2	CP WMDRM-ND – Identification du contenu transféré en utilisant WMDRM-ND.....	129
9.9.3	CP WMDRM-ND – Exigences concernant le format de support	129
9.9.4	CP WMDRM-ND – Type MIME (Extension de courrier Internet à fonctions multiples).....	130
9.9.5	CP WMDRM-ND – Position d'alignement approprié au décodeur	130
9.9.6	CP WMDRM-ND – Élément d'alignement de format de support.....	130
Annexe A (informative) Introduction aux opérations de recherche DLNA.....		131
Bibliographie.....		142
Figure 1 – Configuration et définition des directives		83
Figure 2 – Carte visuelle des valeurs possibles pour les tableaux d'attributs.....		85
Figure A.1 – Définitions de l'UCDAM (Modèle de disponibilité des données de contenu uniforme) pour les opérations de recherche		132
Figure A.2 – Modèle de disponibilité complète des données à accès aléatoire		134
Figure A.3 – Modèle de disponibilité limitée des données à accès aléatoire, mode 0		136
Figure A.4 – Modèle de disponibilité limitée des données à accès aléatoire, mode 1		137
Figure A.5 – Contenu non protégé de flux de contenu.....		139
Figure A.6 – Contenu protégé de liaison de flux de contenu.....		140
Tableau 1 – Valeurs d'espace de nom DLNA		82
Tableau 2 – Valeurs autorisées pour le champ d'indicateur de modification dans le tableau d'attributs		85
Tableau 3 – Priorités normatives pour les types de trafic dlina pour la protection de liaison.....		86
Tableau 4 – Résumé des éléments de domaine pour le mode de disponibilité complète des données à accès aléatoire.....		88
Tableau 5 – Résumé des éléments de domaine pour le mode de disponibilité limitée de données à accès aléatoire		89
Tableau 6 – Modifications des directives de gestion des supports AV (Audio avec vidéo)		90
Tableau 7 – Propriétés recommandées des métadonnées.....		91
Tableau 8 – Type de propriété et valeur multiple.....		92
Tableau 9 – Mises à jour des directives générales existantes concernant le transport de support		94
Tableau 10 – Mises à jour des directives générales existantes concernant le transport de support HTTP		96
Tableau 11 – Mises à jour des directives générales existantes concernant le transport de support HTTP pour le transfert en flux continu		104
Tableau A.1 – Constructions DLNA du mode de disponibilité complète des données à accès aléatoire		135
Tableau A.2 – Constructions DLNA du mode de disponibilité complète des données à accès aléatoire		138

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

**LIGNES DIRECTRICES POUR L'INTEROPÉRABILITÉ
DES DISPOSITIFS DOMESTIQUES DLNA
(DIGITAL LIVING NETWORK ALLIANCE) –****Partie 3: Protection des liaisons****AVANT PROPOS**

- 1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) La CEI ne fournit elle-même aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains domaines, l'accès à des marques de conformité CEI. La CEI n'est responsable d'aucun des services proposés par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de l'identification de l'un quelconque ou de la totalité de ces droits de propriété industrielle.

La Norme internationale CEI 62481-3 a été élaborée par le domaine technique 9: Applications audio, vidéo et multimédia pour réseau d'utilisateur final, du comité d'études 100 de la CEI: Systèmes et appareils audio, vidéo et multimédia.

La présente version bilingue (2012-09) correspond à la version anglaise monolingue publiée en 2010-11.

Le texte anglais de cette norme est issu des documents 100/1617/CDV et 100/1739/RVC.

Le rapport de vote 100/1739/RVC donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Une liste de toutes les parties de la série CEI 62481, présentées sous le titre général *Directives pour l'interopérabilité des dispositifs domestiques de la DLNA (Digital Living Network Alliance)*, peut être consultée sur le site web de la CEI.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de la CEI sous «<http://webstore.iec.ch>» dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

LIGNES DIRECTRICES POUR L'INTEROPÉRABILITÉ DES DISPOSITIFS DOMESTIQUES DLNA (DIGITAL LIVING NETWORK ALLIANCE) –

Partie 3: Protection des liaisons

1 Domaine d'application

La présente partie de la CEI 62481 spécifie les directives de la protection de liaison DLNA, qui constituent une extension des directives DLNA. La protection de liaison DLNA est définie comme la protection d'un flux de contenu entre deux dispositifs sur un réseau DLNA contre une observation ou une interception illégitime, utilisant les protocoles définis dans la présente norme.

La protection de contenu est un mécanisme important pour garantir que le contenu commercial est protégé contre le piratage et une redistribution illégitime. La protection de liaison est une technique permettant la distribution sur un réseau domestique d'un contenu commercial protégé, procurant ainsi une plus grande souplesse pour le consommateur tout en préservant toujours les droits des détenteurs de droits d'auteur et des fournisseurs de contenu.

Les lignes directrices présentées dans la présente norme référencent les technologies existantes pour la protection de liaison et fournissent des mécanismes assurant l'interopérabilité entre différentes mises en œuvre ainsi que l'intégration avec l'architecture DLNA.

La présente Norme est organisée de manière à être alignée avec la structure globale de la CEI 62481-1 et de la CEI 62481-2.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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/CEI 13818-2, *Technologies de l'information – Codage générique des images animées et du son associé: Données vidéo*

ISO/CEI 14496-2:2004, *Technologies de l'information – Codage des objets audiovisuels – Partie 2: Codage visuel*

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

ISO/CEI 29341-3-10:2008, *Technologies de l'information – Architecture de dispositif UPnP – Partie 3-10: Protocole de contrôle de dispositif audio-vidéo – Service de transport audio-vidéo*

ISO/CEI 29341-3-11:2008, *Technologies de l'information – Architecture de dispositif UPnP – Partie 3-11: Protocole de contrôle de dispositif audio-vidéo – Service de gestionnaire de connexion*

ISO/CEI 29341-3-12:2008, *Technologies de l'information – Architecture de dispositif UPnP – Partie 3-12: Protocole de contrôle de dispositif audio-vidéo – Service d'annuaire de contenu*

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 Supplément E (version informative)

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 Termes, définitions et acronymes

Pour les besoins du présent document, les termes, définitions et acronymes suivants s'appliquent.

3.1 Termes et définition

3.1.1

authentification et échange de clé

AKE

dans un système de protection de liaison, étape dans laquelle le dispositif récepteur est authentifié et reçoit les clés correctes pour le contenu

3.1.2

format de système avancé

ASF

encapsulation de format de support pour la transmission de contenu

3.1.3

audio avec vidéo

AV

tout contenu de support contenant à la fois une image animée et du son

3.1.4**transport AV****AVT**

service UPnP (Universel prêt à fonctionner) assurant un pilotage basé sur un réseau pour les opérations de transport courantes telles que la lecture, l'arrêt, la pause, la plage suivante, la plage précédente et la recherche, norme UPnP DCP

3.1.5**texte en clair**

flux de contenu non chiffré après déchiffrement par le système de protection de contenu amont et avant chiffrement par le système de protection de liaison

3.1.6**domaine des octets de texte en clair**

spécification d'une position d'octet dans le flux de contenu de texte en clair, expliquant complètement les opérations de recherche sur le contenu de liaison protégé, voir Annexe A

3.1.7**en-tête de requête de recherche d'octet de texte en clair**

utilisée pour représenter l'un quelconque des en-têtes de requête de la couche transport; implique que la directive s'applique à toutes les utilisations de l'un quelconque des en-têtes de requête

3.1.8**en-tête de réponse à une recherche d'octet de texte en clair**

utilisée pour représenter l'un quelconque des en-têtes de réponse de la couche transport; implique que la directive s'applique à toutes les utilisations de l'un quelconque des en-têtes de requête

3.1.9**service gestionnaire de connexion****CMS**

service UPnP (Universel prêt à fonctionner) fournissant des informations concernant les protocoles de transport pris en charge et les formats de support d'un dispositif UPnP, une norme UPnP DCP

3.1.10**source contributive****CSRC**

source utilisée pour le transport de support RTP (Protocole en temps réel)

3.1.11**position d'alignement approprié au décodeur**

dans le flux de bits défini, position pour un alignement approprié au décodeur; toujours le début d'un élément d'alignement de format de support pouvant commencer à traiter des données sans autre information sur l'état interne concernant le flux de façon que le décodeur puisse commencer le traitement en ce point et créer un rendu de sortie valable

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

organisme ayant élaboré cette norme à l'origine

3.1.13**protection de liaison DLNA**

protection, utilisant des éléments de protocole DLNA comme défini dans ces directives, d'un flux de contenu entre deux dispositifs sur un réseau DLNA, contre une observation ou une interception illégitime

3.1.14

priorité d'utilisateur QoS (Qualité de service) DLNA

DLNAQOS_UP

étiquette de QoS (Qualité de service) définie par DLNA, utilisée pour effectuer une corrélation d'une priorité d'utilisateur IEEE 802.1Q sous-jacente et d'une catégorie d'accès WMM à un ou plusieurs types de trafic DLNA

3.1.15

protection du contenu d'une transmission numérique

DTCP

l'un des systèmes de protection de liaison

3.1.16

protection du contenu d'une transmission numérique sur des réseaux IP (Protocole Internet)

DTCP-IP

DTCP (Protection du contenu d'une transmission numérique) appliquée à un réseau IP (Protocole Internet)

3.1.17

groupe d'images

GOP

groupement défini d'informations dans le format de support MPEG-2

3.1.18

protocole de transfert hypertexte

HTTP

protocole pour transférer des fichiers sur Internet

NOTE Nécessite un programme client HTTP à une extrémité et un programme serveur HTTP à l'autre extrémité.

3.1.19

élément d'alignement de protection de liaison

unité de contenu transporté dans un flux de contenu de liaison protégé commençant par un en-tête de paquet défini par le système de protection de liaison et contenant les octets du flux de liaison protégé

3.1.20

protection de liaison

protection d'un flux de contenu entre deux dispositifs sur un réseau DLNA contre une observation ou une interception illégitime

3.1.21

système de protection de liaison

collection spécifique de technologies avec des règles correspondantes permettant un transfert sûr de contenu entre deux points d'extrémité

3.1.22

élément d'alignement de format de support

utilisation d'un contenu transporté dans un flux de contenu non protégé, commençant par une position d'alignement approprié au décodeur pour le format de support donné et contenant un nombre entier d'unités de contenu, comme défini par le format de support utilisé

3.1.23

extension de courrier Internet à fonctions multiples

MIME

système normalisé pour identifier le type de données contenues dans un fichier

NOTE MIME est un protocole Internet permettant d'envoyer des fichiers binaires sur Internet sous forme de pièces jointes à des messages de courrier électronique. Celui-ci comporte des dessins, des photographies, des fichiers son et vidéo ainsi que des documents de textes formatés.

3.1.24

domaine des octets de réseau

spécification d'une position d'octet dans le flux de contenu transporté sur le réseau de transport

NOTE Pour un contenu binaire utilisant un système de protection de liaison, ceci comporte le chiffrement et tous les en-têtes ou remplissages nécessaires requis par le système de protection de liaison.

3.1.25

connectivité de réseau – économie d'énergie

NC-PS

modes de fonctionnement avec économie d'énergie, comme défini dans la CEI 62481-1

3.1.26

paquet de contenu protégé

PCP

format de paquet pour le contenu de liaison protégé DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) comme défini dans le Volume 1 de DTCP (Protection du contenu d'une transmission numérique) et le Supplément E du Volume 1 de DTCP

3.1.27

flux de programme

PS

flux de contenu binaire se référant habituellement à un format de flux AV (Audio avec vidéo) MPEG-2

3.1.28

protocole en temps réel

RTP

transport de support fournissant des fonctions de transport de réseau bout-à-bout pour transmettre des données en temps réel, par exemple AV (Audio avec vidéo)

NOTE Il fournit des services tels que l'identification du type de charge utile, la numérotation des séquences, l'horodatage et la surveillance de la fourniture.

3.1.29

protocole de transfert en flux continu en temps réel

RTSP

protocole appartenant à la série de protocoles RTP (Protocoles en temps réel)

3.1.30

temps d'aller et retour

RTT

temps s'écoulant entre l'envoi d'un paquet de réseau à un hôte distant et le temps nécessaire à la réception de la réponse

3.1.31

protocole de description de session

SDP

protocole appartenant à la série de protocoles RTP (Protocoles en temps réel)

3.1.32

protocole simple d'accès aux objets

SOAP

protocole de messagerie basé sur XML utilisé pour échanger des requêtes de service et des réponses sur un réseau

3.1.33

domaine temporel

spécification d'une position dans le flux de contenu en unités de temps

3.1.34

flux de transport

TS

flux de contenu binaire se référant habituellement à un format de flux AV (Audio avec vidéo) MPEG-2

3.1.35

modèle de disponibilité de données de client uniforme

UCDAM

modèle pour représenter les octets d'un contenu binaire qui sont disponibles sur un serveur pour des opérations de recherche

NOTE Voir 7.5 de la CEI 62481-1 pour une définition complète.

3.1.36

UPnP (Universel prêt à fonctionner)

architecture pour connectivité universelle du réseau poste-à-poste de dispositifs de tous les facteurs de forme

NOTE 1 Voir ISO/CEI 29341-1 pour la description de l'architecture.

NOTE 2 Il est conçu pour procurer une connectivité facile à utiliser, souple, basée sur des normes, à des réseaux ad hoc ou non gérés, à domicile, dans une petite entreprise, dans des espaces publics ou reliés à Internet. Il s'agit d'une architecture de réseau ouverte distribuée mettant à niveau les techniques TCP/IP et Web pour permettre une mise en réseau de proximité en plus du contrôle et du transfert de données parmi les dispositifs en réseau à domicile, au bureau et dans des espaces publics.

3.1.37

identificateur uniforme de ressource

URI

codification W3C de la syntaxe du nom et de l'adresse des objets actuels et futurs sur Internet

NOTE Dans sa forme la plus fondamentale, un URI est constitué d'un nom de schéma (par exemple http, ftp, news, mailto, gopher) suivi d'une virgule, suivi d'un chemin dont la nature est déterminée par le schéma qui le précède. URI est le terme générique pour les URN (Nom uniforme de ressource), URL (localisateur uniforme de ressource) et tous les autres identificateurs uniformes de ressources.

3.1.38

unité d'objet vidéo

VOBU

groupement défini d'informations dans le format de support MPEG-2

3.1.39

confidentialité à équivalence câblée

WEP

norme de confidentialité sans fil utilisée conjointement avec les réseaux IEEE 802.11

3.1.40

Format «Windows media audio»

WMA

format binaire de compression audio

3.1.41

DRM (gestion des droits numériques) «Windows media» pour dispositif réseau

WMDRM-ND

l'un des systèmes de protection de liaison

3.1.42**format «Windows media video»****WMV**

format binaire de compression AV (Audio avec vidéo)

3.1.43**accès protégé WiFi****WPA**

système pour sécuriser un réseau sans fil IEEE 802.11

3.1.44**accès protégé WiFi, version 2****WPA2**

système pour sécuriser un réseau sans fil IEEE 802.11, version 2

3.2 Abréviations

BNF	Forme de Backus-Naur
LWS	Espace blanc linéaire
MPEG-2	Groupe d'experts en images animées, phase 2
MIU	Unité d'interopérabilité média
MTU	Unité de transmission maximale
UCDAM	Modèle de disponibilité de données de contenu uniforme
UPnP	Universel prêt à fonctionner
W3C	Consortium «World Wide Web»

4 Architecture de réseau domestique DLNA

Se référer à l'Article 4 de la CEI 62481-1, pour des descriptions détaillées de l'architecture de réseau domestique DLNA.

5 Modèle de dispositif DLNA

Se référer à l'Article 5 de la CEI 62481-1, pour des descriptions détaillées de l'architecture de réseau domestique DLNA. Cette norme s'étend aux dispositifs DLNA existants et aux utilisations de système, incluant un contenu de liaison protégé utilisé pour ce qui suit:

- utilisation du système «2 box pull»;
- utilisation du système «2 box push»;
- utilisation du système «3 box»;

pour le transfert et le rendu des éléments de contenu. Il s'agit des seules utilisations de système actuellement envisagées pour utiliser la protection de liaison DLNA.

6 Terminologie et conventions des directives

6.1 Classifieurs de conformité des directives

La référence [9]¹ donne une description des conventions de terminologie utilisées dans tous les documents IETF RFC. La terminologie et les conventions utilisées par les directives d'interopérabilité des dispositifs de réseau domestique DLNA sont adaptées à partir de cette référence. Les détails de chaque directive comportent un classifieur de conformité appartenant à l'ensemble suivant.

[D]oit, Requis: Il s'agit de l'ensemble minimal d'exigences assurant l'interopérabilité et/ou un fonctionnement robuste entre dispositifs. On s'attend à ce que tous les dispositifs soient conformes à ces exigences, exprimées sous forme inconditionnelle. Une exigence conditionnelle exprimée sous la forme, «Si X, alors Y doit être mis en œuvre», signifie que l'exigence «Y» doit être satisfaite lorsque l'aspect conditionnel «X» s'applique à une mise en œuvre donnée.

[C]onvient, Recommandé: Les éléments recommandés sont des éléments facultatifs dont il est fortement recommandé qu'ils soient inclus dans les produits. La différence entre les éléments «recommandés» et les éléments «facultatifs», voir ci-dessous, est une différence de priorité. Considérant les caractéristiques d'inclusion dans un produit, il convient d'inclure les éléments recommandés en premier.

[F]acultatif, Peut: Les éléments facultatifs sont des suggestions de caractéristiques améliorant l'expérience de l'utilisateur ou proposés comme choix moins préféré par rapport à une autre caractéristique recommandée. Si des caractéristiques facultatives sont incluses, elles doivent satisfaire aux exigences garantissant l'interopérabilité avec les autres mises en œuvre.

6.2 Norme des classifieurs d'utilisation de spécification

Lors de la spécification des détails des directives, il est souvent utile de réitérer ou de clarifier certains aspects d'une norme ou d'une spécification qui sont souvent violés ou incompris. De plus, des exigences de directives peuvent exister, contredisant ou restreignant volontairement la mise en œuvre de certains aspects d'une norme ou d'une spécification pour garantir l'interopérabilité entre des dispositifs DLNA. Les classifieurs suivants sont utilisés dans les directives d'interopérabilité des dispositifs de réseau domestique DLNA pour indiquer la relation d'une exigence de directive spécifique avec une norme ou spécification source.

[A]ddition: Exigence de directive s'ajoutant à une norme ou spécification ou la complétant pour améliorer l'interopérabilité. Une exigence de directive ne faisant pas référence à une norme ou spécification utilise également ce classifieur.

[C]larification: Exigence de directive traitant des aspects vagues ou ambigus d'une norme ou spécification.

[F]ixation: Exigence de directive remplaçant et fixant volontairement les aspects d'une norme ou spécification incorrecte et fournissant par ailleurs une mauvaise expérience de l'utilisateur ou empêchant l'interopérabilité du dispositif.

[L]imitation: Exigence de directive restreignant ou spécifiant un comportement exact dans des domaines où une norme ou spécification procure de plus grands degrés de latitude dans la mise en œuvre.

[R]épétition: Exigence de directive répétant ce qui se trouve déjà dans une norme ou spécification en raison de problèmes observés et répétés avec les mises en œuvre. À chaque

¹ Les nombres entre crochets se réfèrent à la Bibliographie.

fois qu'une exigence de directive avec ce classifieur d'utilisation semble être en conflit avec la norme réelle, la norme prévaut sur l'exigence de la directive.

6.3 Conventions d'utilisation des polices de caractères des directives

Les conventions d'utilisation suivantes des polices sont utilisées avec les directives d'interopérabilité des dispositifs de réseau domestique DLNA afin de procurer une clarté supplémentaire.

- Les hyperliens sur des références sont indiqués sous la forme [nombre] Par exemple [1], [20], ...
- les en-têtes et méthodes HTTP sont toujours en caractères gras, par exemple CACHE-CONTROL.
- les noms d'action UPnP sont indiqués ainsi: [Acronyme de service].[nom d'action], par exemple CDS: Exploration.
- Des termes particuliers peuvent être *en italique*. Une exigence de directive définit parfois un terme à utiliser dans cette directive et le terme est *en italique*.

6.4 Convention de notation de syntaxe des directives

Les conventions de notation de syntaxe (BNF (Forme de Backus-Naur)) suivantes sont utilisées avec les directives d'interopérabilité des dispositifs de réseau domestique DLNA pour assurer la lisibilité.

- Les caractères d'espaces blancs linéaires (LWS), tels que les retours chariot, les espaces, les tabulations ou les sauts de lignes, ne sont impliqués nulle part dans les définitions de la syntaxe (BNF) utilisées dans les directives d'interopérabilité.
- L'utilisation des caractères LWS est limitée à la directive d'interopérabilité DLNA sauf spécification explicite dans l'une quelconque des définitions de syntaxe en référence aux communications HTTP UPnP (Universel prêt à fonctionner).
- Par défaut, les jetons et valeurs de texte ont un traitement sensible à la casse, sauf indication explicite dans les directives. Cette convention s'applique également aux définitions de BNF, nom de balises XML, valeurs de balises XML, identificateurs de capacité et valeurs d'en-tête HTTP pour les en-têtes HTTP utilisés par les directives DLNA. L'une des exceptions à cette règle s'applique aux noms des en-têtes HTTP. les noms des en-têtes HTTP ont un traitement insensible à la casse. Par exemple, TimeSeekRange.dlna.org est similaire à timeseekrange.dlna.org. (Voir CEI 62481-1-7.5.5.2.6). D'autres exceptions sont décrites dans chaque directive définissant la syntaxe BNF.

6.5 Conventions de textes normatifs et informatifs des directives

Tous les textes apparaissant dans les directives d'interopérabilité DLNA doivent être considérés comme normatifs sauf spécification contraire explicite, telle que les références informatives et les annexes informatives. Un texte normatif comporte un texte introductif avant les tableaux d'exigences des directives, mais les exigences pouvant être vérifiées ne sont contenues que dans les entrées des tableaux d'exigences de directives.

6.6 Espaces de nom et schémas XML DLNA

Les directives d'interopérabilité DLNA font de nombreuses références à des éléments et attributs XML qui sont définis pour les classes de dispositif et les capacités de dispositif DLNA. Toutefois, volontairement ces noms d'espace ne sont pas définis au moyen d'un schéma de format XML DLNA. Ceci permettra dans l'avenir aux directives d'interopérabilité DLNA de définir de nouveaux éléments et attributs XML sans devoir définir un nouvel espace de nom ou une nouvelle définition de schéma. on s'attend à ce que les classes de dispositif et les capacités de dispositif DLNA présentent un comportement tolérant lorsqu'elles rencontreront des éléments ou des attributs XML qui seront attribués dans l'avenir, comme requis par la norme existante CEI 62481-1, 7.3.24 et 7.4.1.3.1. Le Tableau 1 énumère les

valeurs d'espace de nom qui sont utilisées par les directives DLNA et le contexte de leur utilisation.

Tableau 1 – Valeurs d'espace de nom DLNA

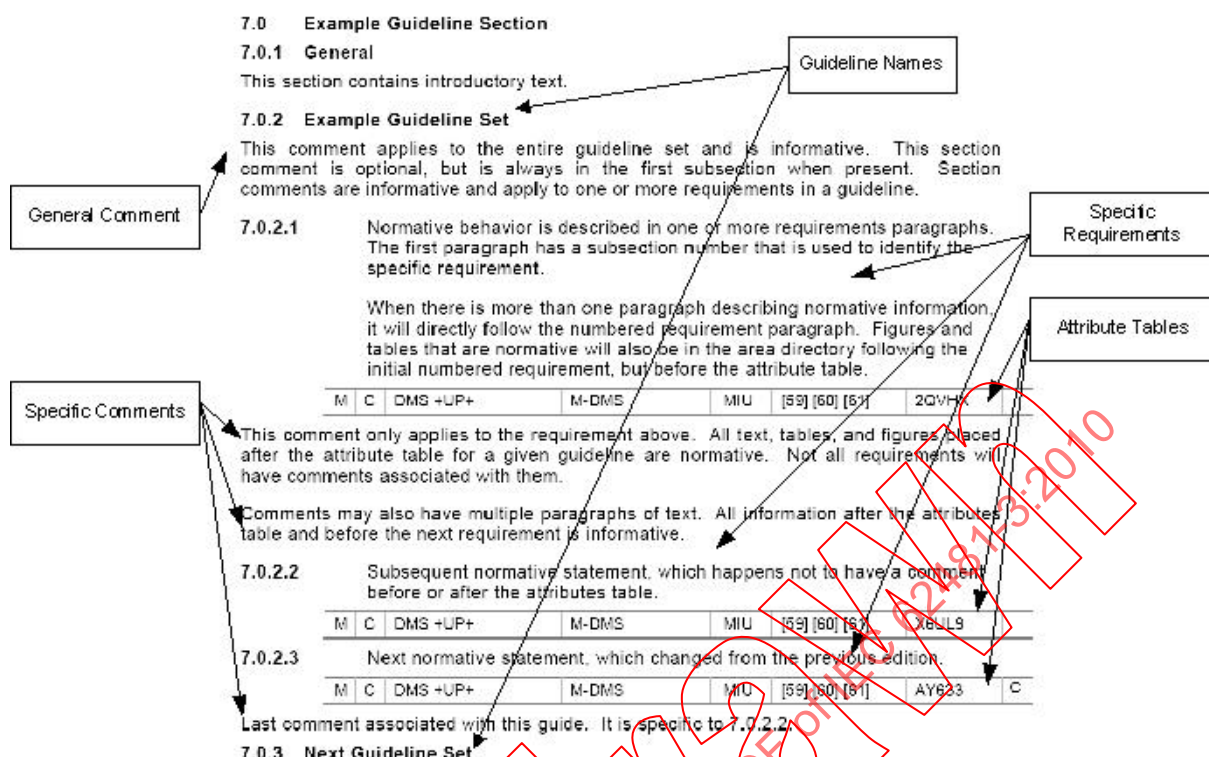
Valeur d'espace de nom	Contexte d'utilisation
urn:schemas-dlna-org:device-1-0	Utilisée pour les éléments et attributs XML définis par les directives d'interopérabilité DLNA pour être utilisés dans les fichiers de description de dispositif UPnP (Universel prêt à fonctionner).
urn:schemas-dlna-org:metadata-1-0/	Utilisée pour les éléments et attributs XML définis par les directives d'interopérabilité DLNA pour être utilisés dans les documents et fragments DIDL-Lite.

7 Directives communes pour la protection de liaison

7.1 Généralités

Ce paragraphe contient les directives indépendantes du système de protection de liaison sous-jacent. Les paragraphes 7.3 à 7.8 concernent les paragraphes correspondants 7.2 à 7.7 de la CEI 62481-1. Le paragraphe 7.9 contient des informations ne concernant pas cette partie et il convient de le lire en premier pour fournir le contexte pour 7.3 à 7.8.

Ces directives sont présentées dans un format article/paragraphe, comme représenté à la Figure 1.



IEC 2344/10

Légende

Anglais	Français
Guideline Names	Noms des directives
General Comments	Commentaires généraux
Specific comments	Commentaires spécifiques
Specific Requirements	Exigences spécifiques
Attribute Tables	Tableaux d'attributs

Figure 1 – Configuration et définition des directives

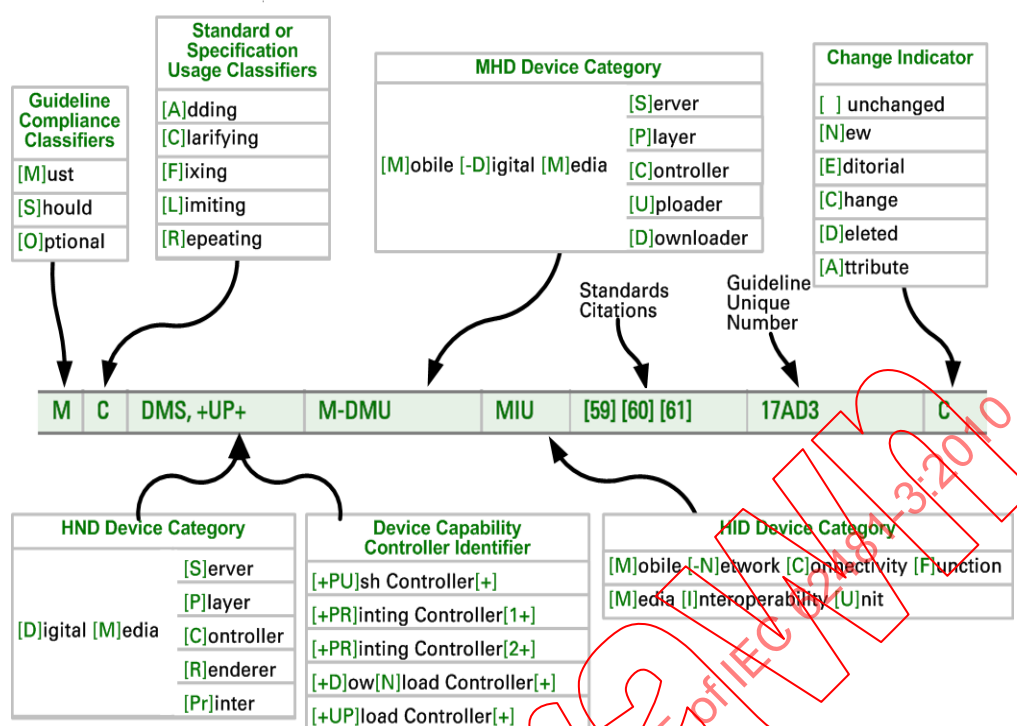
La liste suivante décrit le contenu de la Figure 1.

- Nom: Etiquette unique pour la directive. L'étiquette est précédée d'un numéro croissant en séquence pour permettre une consultation aisée.
- Exigences: Description réelle d'une directive. Une directive est précédée d'un numéro croissant en séquence dans chaque volume pour permettre une consultation aisée.
- Tableau d'attributs: Résumé des attributs essentiels d'une exigence. Le tableau est constitué d'une ligne unique avec les définitions suivantes pour les colonnes.
 - Classifieur de conformité: M/S/O (Voir 6.1 pour la définition des classifieurs de conformité des directives).
 - Le classifieur d'utilisation de spécification: A/C/F/L/R: pour la directive. (Voir 6.2 pour la définition des classifieurs d'utilisation de spécification.)
 - Classes de dispositif HND avec capacités de dispositif (voir Tableau 2 et Tableau 3 de la CEI 62481-1 pour les définitions). Capacités de dispositif énumérées dans la colonne HND du tableau d'attributs. Les capacités du dispositif peuvent également

s'appliquer à la catégorie de dispositif MHD mais ont été omises de la colonne MHD du tableau d'attributs pour permettre une meilleure lisibilité.

- Classes de dispositif MHD (voir Tableau 4 de la CEI 62481-1 pour les définitions).
 - Classes de dispositif HID (voir Tableau 5, de la CEI 62481-1 pour les définitions).
 - Citation de normes: Normes référencées par la directive. Les citations de normes s'effectuent par numéro et son référencées à l'Article 2.
 - Numéro unique de directive: chaîne alphanumérique identifiant une exigence de manière unique.
 - Indicateur de modification: documente la modification de l'exigence qui est apparue depuis la dernière édition de la directive (voir les définitions au Tableau 2).
 - Les colonnes d'attributs de directives n'ayant pas de valeur comportent la désignation «n/a» (non applicable). Une carte visuelle des valeurs possibles pour les tables d'attributs se trouve à la Figure 2.
- d) Commentaire: Informations supplémentaires relatives à une directive, telles qu'une justification de la directive, le problème d'interopérabilité spécifique traité, etc.

Noter qu'un grand nombre de directives n'énumèrent pas explicitement les MIU (Unités d'interopérabilité), car les directives s'appliquant à une classe de dispositifs s'appliquent également aux variantes virtualisées.



IEC 2345/10

Légende

Anglais	Français
Guideline Compliance Classifiers	Classifieurs de conformité aux directives
Standard or Specification Usage Classifiers	Classifieurs d'utilisation des normes ou spécifications
MHD Device Category	Catégorie de dispositif MHD
Change Indicator	Indicateur de changement
Standard Citations	Citations de normes
Guideline Unique Number	Numéro unique de directive
HND Device Category	Catégorie de dispositif HND
Device Capability Control Identifier	Identificateur de contrôle de capacité de dispositif
HID Device Category	Catégorie de dispositif HID

Figure 2 – Carte visuelle des valeurs possibles pour les tableaux d'attributs

Tableau 2 – Valeurs autorisées pour le champ d'indicateur de modification dans le tableau d'attributs

Valeur	Signification
<vierge>	Aucun changement au texte ou aux figures par rapport à la version immédiatement précédente de cette exigence.
A	Le tableau d'attributs lui-même, à l'exclusion de l'indicateur de modification, a changé. Par exemple, une nouvelle classe a été ajoutée.
C	Les changements effectués par rapport à l'exigence modifient l'essai, le souhait ou un autre comportement normatif par rapport à la version immédiatement précédente de cette exigence.
D	L'exigence a été supprimée. Ces exigences sont déplacées dans le document des exigences supprimées. Noter que l'indicateur de modification pour l'exigence n'est marqué comme supprimé que la première fois qu'il apparaît dans le document des exigences supprimées: dans les versions suivantes du document des exigences supprimées, l'indicateur de modification est remis à blanc.
E	Changements effectués ne modifiant pas les exigences pouvant être soumises à essai, les souhaits ou autre comportement normatif.

7.2 Conditions relatives au temps de mesure dans les échanges de messages

Ces directives définissent dans certains cas les contraintes de temps pour l'échange de messages entre deux points d'extrémités qui communiquent. Ces contraintes de temps ont été définies comme un moyen pour assurer une certaine cohérence de fonctionnement entre les deux points d'extrémités qui communiquent. Toutefois, dans les réseaux de meilleur effort, les mesures en temps réel pour l'échange de messages montrent de larges variations selon les perturbations déterminées à partir des conditions du réseau, du trafic, de la bande passante disponible, ainsi que d'autres raisons. Pour cette raison, ce paragraphe comporte des recommandations relatives aux conditions au moment de l'exécution de ces mesures, comme suit.

- Il convient que les deux points d'extrémités qui communiquent établissent des communications dans des conditions idéales du réseau.
- Les mesures de temps sur une couche donnée supposent que les couches sous-jacentes préservent le canal de communication. Par exemple, les mesures de temps sur la couche HTTP ne peuvent pas être valables si le canal TCP/IP sous-jacent est coupé pendant les mesures.
- Sauf spécification contraire, les mesures de temps supposent que les dispositifs qui communiquent sont tous deux en mode actif. Ceci signifie qu'il convient que les mesures de temps n'incluent pas les transitions entre le mode sommeil et le mode actif.

7.3 Mise en réseau et connectivité

7.3.1 Généralités

Les directives de ce paragraphe fournissent des exigences concernant les capacités générales et spécifiques du dispositif pour la mise en réseau, qui sont indépendantes du système de protection de liaison utilisé. Pour les exigences spécifiques à DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.2. Pour les exigences spécifiques à WMDRM-ND, voir 9.3.

Les ajouts suivants doivent être effectués dans le Tableau 8 de la CEI 62481-1 pour inclure les niveaux de QoS (Qualité de service) DLNA normatifs pour les messages de protection de liaison.

Tableau 3 – Priorités normatives pour les types de trafic dlina pour la protection de liaison

DLNAQOS_UP	Types de trafic DLNA	Priorité d'utilisateur IEEE 802.1Q	Catégorie d'accès WMM	DSCP	Détails de l'Article
DLNAQOS_3 (Le plus haut)	Échange de clé de protection de liaison DLNA	7	VO	0x38	8.2.2 9.3.2

7.3.2 Nouvelles exigences de capacité générales– «Bluetooth» NC CP – Modes d'économie d'énergie

Si le schéma d'économie d'énergie au niveau du support NC-PS (Connectivité de réseau - Économie d'énergie) est pris en charge et la liaison de réseau est dans le mode «Attente», il convient alors que le dispositif MHD demande la transition du mode NC-PS «Attente» au mode «Actif» avant toute communication de protection de liaison requise.

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

Se référer à la CEI 62481-1, 7.2.3.4.3.

Ceci est destiné à garantir que la liaison est dans l'état de plus grande bande passante et de plus faible retard avant de démarrer un échange de protection de liaison pouvant dépendre du

séquençement de chaque message. Par exemple, DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) mesure le RTT (Temps d'aller et retour) entre la source de contenu et le récepteur de contenu afin de déterminer si les points d'extrémité se trouvent sur le réseau domestique de l'utilisateur. Si l'opération s'effectue pendant que la liaison est dans le mode «Attente», le retard peut être artificiellement élevé.

7.4 Découverte et pilotage de dispositif

Ce paragraphe traite des directives pour mettre en œuvre la découverte et le pilotage de dispositif en utilisant l'architecture de dispositif UPnP (Universel prêt à fonctionner). Il n'y a aucune modification à ce paragraphe pour la prise en charge de la protection de liaison DLNA. Pour les exigences spécifiques à DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.3. Pour les exigences spécifiques à WMDRM-ND, voir 9.4.

7.5 Gestion du support

7.5.1 Gestion du support – Gestion du support AV (Audio avec vidéo)

Ce paragraphe traite des directives pour mettre en œuvre la gestion de support en utilisant l'architecture AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) avec protection de liaison DLNA. Ce paragraphe donne des informations détaillées sur la gestion de support. Pour les exigences spécifiques à DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.4. Pour les exigences spécifiques à WMDRM-ND, voir 9.5.

Un grand nombre des directives de ce paragraphe ainsi que 7.6 ont un rapport avec les structures nécessaires pour effectuer des opérations de recherche sur le contenu de liaison protégé. La CEI 62481-1 définit deux modèles d'opération de recherche: le modèle de disponibilité complète de recherche de données et le modèle de disponibilité limitée de recherche de données. Ces deux modèles continuent à fonctionner pour un contenu utilisant la protection de liaison DLNA. On introduit toutefois pour ce contenu le concept de domaine des octets de réseau (flux de contenu protégé à mesure qu'il circule sur le réseau) et de domaine des octets de texte en clair (représentant des positions dans le contenu avant chiffrement par le système de protection de liaison). Ceci permet au récepteur de contenu de rechercher les positions d'octet dans le contenu comme si aucune protection de liaison n'avait été appliquée. Pour les contenus binaires utilisant la protection de liaison DLNA, si le récepteur de contenu effectue une opération de recherche d'octet dans le domaine des octets de texte en clair, il peut délivrer des requêtes pour les mêmes positions d'octet que ce qu'il ferait si le contenu était envoyé sans aucune protection de liaison. Il n'est pas nécessaire que le récepteur de contenu effectue une conversion entre les positions dans le texte en clair et les positions dans le contenu chiffré. Pour une explication détaillée sur la recherche et le contenu de liaison protégé, voir Annexe A. Le Tableau 4 et le Tableau 5 résument les structures utilisées pour chacun des domaines et modèles de recherche. Le Tableau 6 contient les directives définissant les exigences de gestion de support pour les dispositifs utilisant la protection de liaison DLNA.

Tableau 4 – Résumé des éléments de domaine pour le mode de disponibilité complète des données à accès aléatoire

Modèle	Fonction	Domaine temporel	Domaine des octets de réseau	Domaine des octets de texte en clair
Disponibilité complète des données à accès aléatoire	Domaine et prise en charge de modèle	op-param a-val	op-param a-val	flags-param Bit 15: CleartextByteSeek- full
	Indication SDP de prise en charge de domaine	Portée	Domain non disponible	Domain non disponible
	Taille de fichier	res@duration	res@size	Taille res@dlna:cleartext
	En-tête de requête HTTP pour exécuter opération de recherche	TimeSeekRange.dlna.org	Portée	En-tête de requête de recherche d'octet de texte en clair DTCP-IP: Range.dtcp.com WMDRM-ND: Cleartext-Range.dlna.org
	En-tête de réponse HTTP pour opération de recherche	TimeSeekRange.dlna.org	Content-Range	En-tête de réponse à une recherche d'octet de texte en clair DTCP-IP: Content-Range.dtcp.com WMDRM-ND: Cleartext-Content-Range.dlna.org
	En-tête RTSP pour exécuter opération de recherche	Portée	Domain non disponible	Domain non disponible
	Taille du corps de message HTTP	Non défini	Content-Length	La taille du contenu du corps de message HTTP Content-Length est toujours spécifiée par l'en-tête de réponse Content-Length

Tableau 5 – Résumé des éléments de domaine pour le modèle de disponibilité limitée de données à accès aléatoire

Modèle	Fonction	Domaine temporel	Domaine des octets de réseau	Domaine des octets de texte en clair
Disponibilité limitée des données à accès aléatoire	Prise en charge de domaine et modèle	flags-param Bit 30: lop-npt	flags-param Bit 29: lop-bytes	flags-param Bit 14: lop- cleartextbytes
	Indication SDP de prise en charge de domaine	Portée	Domain non disponible	Domain non disponible
	En-tête de requête HTTP pour exécuter opération de recherche	TimeSeekRange. dlina.org	Portée	En-tête de requête de recherche d'octet de texte en clair DTCP-IP: Range.dtcp.com WMDRM-ND: Cleartext-Range.dlina.org
	En-tête de réponse HTTP pour opération de recherche	TimeSeekRange. dlina.org	Content-Range	En-tête de réponse à une recherche d'octet de texte en clair DTCP-IP: Content- Range.dtcp.com WMDRM-ND: Cleartext-Content- Range.dlina.org
	En-tête RTSP pour exécuter opération de recherche	Portée	Domain non disponible	Domain non disponible
	En-tête HTTP pour demander la plage disponible	getAvailableSeekRange.dlina.org		
	En-tête de réponse HTTP pour la plage disponible	availableSeekRange.dlina.org (avec npt-range)	availableSeekRange.dlina.org (avec byte-range)	availableSeekRange.dlina.org (avec cleartextbyte-range)
	En-tête RTSP pour demander la plage disponible	DESCRIBE	Domain non disponible	Domain non disponible
	En-tête RTSP pour spécifier la plage disponible	Available- Range.dlina.org	Domain non disponible	Domain non disponible
	S0 augmente	flags-param Bit 27: s0-increasing		
	SN augmente	flags-param Bit 26: sN-increasing		

7.5.2 Directives pour la gestion des supports AV (Audio avec vidéo)

7.5.2.1 Mises à jour des directives générales existantes concernant la gestion des supports AV (Audio avec vidéo)

7.5.2.1.1 Généralités

Tableau 6 – Modifications des directives de gestion des supports AV (Audio avec vidéo)

Exigence mise à jour	Emplacement dans la CEI 62481-1
MM flags-param (paramètre d'indicateurs)	7.4.1.3.23.2
MM lop-npt, lop-bytes, and lop cleartextbytes (indicateurs de fonctionnement limité): Common	7.4.1.3.28.1
MM lop-npt lop-bytes, and lop-cleartextbytes (indicateurs de fonctionnement limité): HTTP	7.4.1.3.29
MM lop-npt, lop-bytes, and lop-cleartextbytes (indicateurs de fonctionnement limité): RTP	7.4.1.3.30
Fichier MM IFO	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 Fichier MM IFO

7.5.2.1.2.1 Si un fichier IFO est fourni par le MediaServer (Serveur de support) AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) ou un contrôleur de poussée pour un quelconque contenu binaire correspondant à un profil de format de support utilisant la protection de liaison DLNA, alors l'IFO ne doit pas être chiffré ou encapsulé par le système de protection de liaison utilisé pour le contenu binaire.

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

Se référer à la CEI 62481-1, 7.4.1.4.8. Le fichier IFO doit être disponible sous forme de texte en clair.

7.5.2.1.2.2 Si un fichier IFO est fourni par le MediaServer (Serveur de support) AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) ou un contrôleur de poussée pour un quelconque contenu binaire correspondant à un profil de format de support utilisant la protection de liaison DLNA, les données des octets et les données temporelles dans le fichier IFO doivent se référer à la position d'octet et à la position temporelle dans le flux de contenu non protégé.

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

Se référer à la CEI 62481-1, 7.4.1.4.8. Les positions d'octet sont considérées par rapport au flux de contenu non protégé et ne sont pas une position d'octet dans le flux de contenu protégé.

7.5.2.2 Nouvelles exigences générales de gestion des supports AV (Audio avec vidéo)

7.5.2.2.1 Classe de supports MM de contenu de liaison protégé

Un objet de contenu représentant une forme de liaison protégée de l'une des classes de supports DLNA doit utiliser la valeur de classe de supports du contenu non protégé.

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

Se référer à la CEI 62481-1, 7.4.1.3.11. Par exemple, le contenu de liaison protégé qui, dans sa forme non protégée, est conforme à la classe de supports DLNA «AV» doit utiliser `object.item.videoItem` ou une classe dérivée pour la valeur `upnp:class`.

7.5.2.2.2 Propriétés des métadonnées d'octet MM DIDL-Lite

Pour des ressources spécifiant un contenu binaire utilisant la protection de liaison DLNA, toutes les métadonnées avec des unités d'octet doivent se référer au domaine des octets de réseau (c'est-à-dire, le contenu de liaison protégé à mesure qu'il est transmis entre les points d'extrémité de serveur et de restitution) sauf spécification par la définition de l'élément de métadonnées à se référer au domaine des octets de texte en clair.

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

Se référer à la CEI 62481-1, 7.4.1.3.11. La longueur du flux de contenu protégé peut être supérieure en raison des en-têtes de chiffrement supplémentaires pour la mise en paquet et de tous les remplissages nécessaires.

7.5.2.2.3 MM CP – `res@dlina:cleartextSize`

Il convient qu'un MediaServer (Serveur de support) AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) fournisse, de plus, des valeurs non vides et non-espaces blancs pour les propriétés des métadonnées, comme représenté dans le Tableau 7 pour les éléments <res> décrivant des contenus binaires utilisant un système de protection de liaison

Tableau 7 – Propriétés recommandées des métadonnées

Valeur <code>upnp:class</code>	Noms des propriétés
<code>object.item.audioItem</code>	<code>res@dlina:cleartextSize</code>
<code>object.item.imageItem</code>	<code>res@dlina:cleartextSize</code>
<code>object.item.videoItem</code>	<code>res@dlina:cleartextSize</code>

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

Se référer à la CEI 62481-1, 7.4.1.3.11. Cette directive facilite la résolution des problèmes de dépendance de la restitution des points d'extrémité, connaissant la taille en octets du flux de contenu non protégé.

Si le MediaServer (Serveur de support) AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) spécifie la valeur `res@dlina:cleartextSize` du contenu binaire, celle-ci doit être de la taille en octets du contenu binaire non protégé avant d'avoir ajouté de quelconques en-têtes de protection de liaison, un remplissage ou un chiffrement.

Tableau 8 – Type de propriété et valeur multiple

Nom de propriété	Type de propriété	Valeur multiple
res@dlna:cleartextSize	unsigned long	Non

Le préfixe de res@dlna:cleartextSize doit être «dlna» et le namespace doit être "urn:schemas-dlna-org:metadata-1-0/".

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

7.5.2.2.4 MM CP – Valeur de DIDL-Lite protocolInfo

Un MediaServer (Serveur de support) AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) peut contenir des ressources spécifiant des contenus binaires chiffrés si le profil de format le spécifie.

O	A	DMS	M-DMS	n/a	CEI 62481-1	KJVVW4	
---	---	-----	-------	-----	-------------	--------	--

Se référer à la CEI 62481-1, 7.4.1.3.15.5. Il interdit le chiffrement de la couche transport sauf si le profil de format de support indique explicitement qu'il est requis. Cette directive clarifie le fait que certains profils de format de support peuvent utiliser une protection de liaison et sont donc chiffrés. Le système de protection de liaison est spécifié dans le profil de format de support du contenu.

7.5.2.2.5 MM CP – Indicateur LP (Indicateur de protection de liaison)

7.5.2.2.5.1 Si le contenu binaire décrit par protocolInfo utilise la protection de liaison DLNA pendant qu'il est transmis, l'indicateur LP doit alors être à vrai.

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

Se référer à la CEI 62481-1, 7.4.1.3.37. La spécificité du système de protection de liaison utilisé et les paramètres pour établir la connexion peuvent se trouver dans les paramètres de type MIME (Extension de courrier Internet à fonctions multiples) ou d'autres paramètres de protocolInfo.

7.5.2.2.5.2 Si le contenu binaire décrit par protocolInfo n'utilise pas la protection de liaison DLNA pendant qu'il est transmis, l'indicateur LP doit alors être à faux.

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

7.5.2.2.6 MM CP – cleartextbyseek-full

Octet basé sur la disponibilité complète des données de recherche avec l'en-tête de requête de recherche d'octet de texte en clair.

Si un contenu binaire utilise un système de protection de liaison sur le protocole de transport de support HTTP, la signification de l'indicateur cleartextbyseek-full doit être la suivante.

Vrai = La source du contenu prend en charge l'en-tête de requête de recherche d'octet de texte en clair selon le modèle de disponibilité complète des données à accès aléatoire.

Faux = La source du contenu ne prend pas en charge l'en-tête de requête de recherche d'octet de texte en clair selon le modèle de disponibilité complète des données à accès aléatoire.

Les exigences du modèle de disponibilité complète des données d'accès aléatoire pour le contenu de liaison protégé sont définies en 7.6.2.3.2 ci-dessous.

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

Se référer à la CEI 62481-1, 7.4.1.3.37. L'en-tête de requête de recherche d'octet de texte en clair peut être différent selon le système de protection de liaison utilisé. Pour les exigences générales de l'en-tête, voir 7.6.6.2.2, pour le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.5.1.2, pour le système de protection de liaison WMDRM-ND, voir 9.6.1.7, pour la définition de cet en-tête. L'en-tête de requête de recherche d'octet de texte en clair permet à un point d'extrémité de spécifier une plage d'octets dans le domaine des octets de texte en clair à retourner par le serveur.

7.5.2.2.7 MM CP – Indicateur lop-cleartextbytes

Octet basé sur la disponibilité limitée de données de recherche avec l'en-tête de requête de recherche d'octet de texte en clair.

Si un contenu binaire utilise un système de protection de liaison sur le protocole de transport de support HTTP, la signification de l'indicateur lop-cleartextbytes doit être la suivante.

Vrai = La source du contenu prend en charge l'en-tête de requête de recherche d'octet de texte en clair selon le modèle de disponibilité limitée de données à accès aléatoire.

Faux = La source du contenu ne prend pas en charge l'en-tête de requête de recherche d'octet de texte en clair selon le modèle de disponibilité limitée de données à accès aléatoire.

Les exigences du modèle de disponibilité limitée de données à accès aléatoire pour le contenu de liaison protégé sont définies en 7.6.2.3.3 ci-dessous.

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

Se référer à la CEI 62481-1, 7.4.1.3.37. L'en-tête de requête de recherche d'octet de texte en clair peut être différent selon le système de protection de liaison utilisé. Pour les exigences générales de l'en-tête, voir 7.6.6.2.2, pour le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.5.1.2, pour le système de protection de liaison WMDRM-ND, voir 9.6.1.7, pour la définition de cet en-tête. L'en-tête de requête de recherche d'octet de texte en clair permet à un point d'extrémité de spécifier une plage d'octets dans le domaine des octets de texte en clair à retourner par le serveur.

7.5.2.3 Exigences de dispositif MediaRenderer

7.5.2.3.1 MM CP – Erreur d'état de protection de liaison

Il convient que la variable d'état de l'instance AVT:TransportStatus soit mise à «"ERROR_OCCURRED» si la méthode AVT:SetAVTransportURI échoue en raison de l'échec d'authentification d'un dispositif ou de restrictions de la protection de liaison (par exemple RTT (Temps d'aller et retour)) qui n'ont pas été satisfaites entre la source de contenu et le récepteur de contenu.

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

Se référer à la CEI 62481-1, 7.4.1.6.11. Les MediaRenderers UPnP (Universel prêt à fonctionner) définissent de nouvelles valeurs autorisées pour la variable d'état de l'instance AVT:TransportStatus pour représenter une condition d'erreur de protection de liaison.

7.5.2.3.2 MM CP – Message d'erreur de protection de liaison lisible par un être humain

7.5.2.3.2.1 Si la liaison du support au récepteur de contenu (par exemple MediaRenderer AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner)) échoue avec l'erreur 403 (Interdit) HTTP ou RTSP (Protocole de transfert en flux continu en temps réel), il convient que le récepteur de contenu réponde à une requête AVT:SetAVTransportURI AVT:Play AVT:Seek AVT:Previous ou AVT:Next

avec un code d'erreur 722 UPnP AV avec la description d'erreur lisible par un être humain: «Impossible de déterminer les utilisations autorisées».

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

Se référer à la CEI 62481-1, 7.4.1.6.11.

7.5.2.3.2.2 Si le MediaRenderer AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) connaît la raison spécifique de l'échec, il peut utiliser un message d'erreur localisé lisible par un être humain dans errorDescriptiontag de la réponse SOAP (Protocole simple d'accès aux objets) indiquant l'échec d'authentification du dispositif ou le fait que les restrictions de protection de liaison (par exemple RTT (Temps d'aller et retour)) n'ont pas été satisfaites.

O	A	DMR	n/a	n/a	[8]	JVW41	
---	---	-----	-----	-----	-----	-------	--

7.6 Transport du support

7.6.1 Généralités

Ce paragraphe traite des exigences pour la couche transport du support. Il donne également des informations détaillées sur le transport du support. Pour les exigences spécifiques à DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.5. Pour les exigences spécifiques à WMDRM-ND, voir 9.6.

7.6.2 Protocoles de transport du support

7.6.2.1 Généralités

Les paragraphes suivants contiennent des directives pour l'utilisation de transports de support dans les dispositifs DLNA. Les directives sont organisées dans un tableau traitant des exigences communes parmi tous les transports de support, puis des articles/tableaux traitant des exigences pour des protocoles de transport de support spécifiques, par exemple HTTP et d'autres. Pour des informations détaillées, voir 7.5 de la CEI 62481-1.

Un grand nombre des directives de ce paragraphe définissent les opérations de recherche d'octets disponibles sur le contenu. Voir en 7.5.1 un résumé des en-têtes et indicateurs utilisés pour représenter les divers domaines d'octets et modèles de recherche.

7.6.2.2 Mises à jour des directives générales existantes concernant le transport de support

Le Tableau 9 fait référence à la CEI 62481-1.

Tableau 9 – Mises à jour des directives générales existantes concernant le transport de support

Exigence mise à jour	Emplacement dans la CEI 62481-1
Modèles de disponibilité de données MT normatives à accès aléatoire	7.5.4.2.14.1
Modèles de «disponibilité complète des données MT à accès aléatoire»	7.5.4.2.15.1
	7.5.4.2.15.2
Modèles de «disponibilité limitée des données MT à accès aléatoire»	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 Nouvelles exigences générales de transport de support

7.6.2.3.1 MT CP – Contenu de liaison protégé

Tout échange de clé requis pour décoder un contenu binaire de liaison protégé doit suivre les exigences du système de protection de liaison utilisé.

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

Se référer à la CEI 62481-1, 7.5.4.2.3.

7.6.2.3.2 MT CP – Prêt pour la lecture

Il convient que l'initialisation des opérations de mise en place spécifique de la protection de liaison s'effectue pendant l'exploration du contenu ou lors de l'appel d'AVT:SetAVTransportURI.

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

Se référer à la CEI 62481-1, 7.5.4.2.3. Les opérations de mise en place de protection de liaison (par exemple essai RTT (Temps d'aller et retour) et authentification du point d'extrémité et de l'échange de clé) peuvent prendre un temps considérable. Il convient que le point d'extrémité de restitution n'attende pas un établissement de liaison HTTP pour initialiser ces opérations, mais il convient qu'il les démarre aussitôt que possible.

7.6.2.3.3 MT CP – En-têtes de métadonnées et de transport pour la protection de liaison

Pour les ressources spécifiant un contenu binaire utilisant la protection de liaison DLNA, sauf spécification contraire, tous les en-têtes de la couche transport avec des unités d'octets doivent se référer au contenu de liaison protégé tel qu'il est transmis entre les points d'extrémité de serveur et de restitution (c'est-à-dire, avec chiffrement, en-têtes de protection de liaison et tout remplissage nécessaire ajouté).

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

Se référer à la CEI 62481-1, 7.5.4.2.13.

7.6.3 Transport HTTP

7.6.3.1 Généralités

Un grand nombre de protocoles de transport possibles peuvent être utilisés pour le transfert du contenu. Le protocole de transport de support obligatoire de référence pour les dispositifs DLNA est HTTP. Le reste de ce paragraphe contient les directives concernant le transport HTTP et elles sont organisées en exigences communes à tous les transferts HTTP, exigences spécifiques à un transfert de flux en continu, exigences spécifiques à un transfert interactif et exigences spécifiques à un transfert en arrière-plan. Pour des informations détaillées, voir 7.5.5 de la CEI 62481-1.

7.6.3.2 Mises à jour des directives générales existantes concernant le transport de support HTTP

7.6.3.2.1 Généralités

Tableau 10 – Mises à jour des directives générales existantes concernant le transport de support HTTP

Exigence mise à jour	Emplacement dans CEI 62481-1
En-tête MT HTTP: contentFeatures.dlna.org	7.5.5.2.10.7
Exigences communes de disponibilité des données à accès aléatoire MT HTTP	7.5.5.2.18.1
Plage de données MT HTTP de «disponibilité complète des données à accès aléatoire»	7.5.5.2.18.2
Plage de données MT HTTP de «disponibilité limitée des données à accès aléatoire»	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
	7.5.5.2.20.16
En-tête MT HTTP: RANGE (Server)	7.5.5.2.22.3
	7.5.5.2.22.4
MT HTTP time-based seek (Serveur)	7.5.5.2.24.1

7.6.3.2.2 Exigences communes de disponibilité des données à accès aléatoire MT HTTP

Si un point d'extrémité de serveur HTTP prend en charge l'en-tête de requête de recherche d'octet de texte en clair pour l'URI (Identificateur uniforme de ressource) spécifié, il doit traiter en même temps toutes les plages demandées dans la plage de données à accès aléatoire.

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

Se référer à la CEI 62481-1, 7.5.5.2.18. Ceci est une exigence générale pour que les requêtes à accès aléatoire soient prises en charge sur toute la plage de données [r0, rN] sur le domaine des octets de texte en clair.

7.6.3.2.3 Plage de données MT HTTP de «disponibilité complète des données à accès aléatoire»

7.6.3.2.3.1 La position d'octet à 0 pour le champ d'en-tête de requête de recherche d'octet de texte en clair doit se référer au début du contenu binaire.

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

Se référer à la CEI 62481-1, 7.5.5.2.19.

7.6.3.2.3.2 Si un point d'extrémité de serveur HTTP reçoit une requête HTTP GET pour un contenu binaire utilisant un système de protection de liaison et omettant

tous les en-têtes utilisés pour les opérations de recherche (c'est-à-dire, l'en-tête RANGE HTTP, l'en-tête de requête de recherche d'octet de texte en clair et l'en-tête TimeSeekRange.dlna.org HTTP), le point d'extrémité de serveur HTTP doit alors produire une position d'octet demandée de 0 (c'est-à-dire répondre à partir du début du contenu binaire). Cette directive doit également s'appliquer lorsque l'augmentation de s0 est fausse et si aucun des en-têtes ci-dessus n'est pris en charge par le serveur HTTP.

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

Se référer à la CEI 62481-1, 7.5.5.2.19.

7.6.3.2.3.3 Pour un contenu binaire utilisant un système de protection de liaison, si un point d'extrémité de serveur HTTP prend en charge l'en-tête de requête de recherche d'octet de texte en clair avec le modèle «disponibilité complète des données à accès aléatoire», il convient que le point d'extrémité de serveur HTTP spécifie la longueur en octets de l'entité retournée (dans le domaine des octets de texte en clair) par l'intermédiaire de la longueur d'instance incluse dans l'en-tête de réponse à une recherche d'octet de texte en clair appropriée de la réponse de cible à une requête HTTP GET/HEAD avec l'en-tête de requête de recherche d'octet de texte en clair.

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

Se référer à la CEI 62481-1, 7.5.5.2.19.

L'en-tête de requête de recherche d'octet de texte en clair peut être différent selon le système de protection de liaison utilisé. Pour les exigences générales de l'en-tête, voir 7.6.6.2.2, pour le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.5.1.2, pour le système de protection de liaison WMDRM-ND, voir 9.6.1.7, pour la définition de cet en-tête.

De façon similaire, l'en-tête de réponse à une recherche d'octet de texte en clair peut également être différent selon le système de protection de liaison utilisé. Pour le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir directive 8.4.2; pour le système de protection de liaison WMDRM-ND, voir 9.6.1.8 pour la définition de cet en-tête.

7.6.3.2.3.4 Pour un contenu binaire utilisant un système de protection de liaison, si un point d'extrémité client HTTP souhaite obtenir la longueur d'instance d'un contenu binaire dans le domaine des octets de texte en clair, il convient alors qu'il utilise une requête HTTP HEAD, l'en-tête de requête de recherche d'octet de texte en clair spécifiant 0 pour le first-cleartextbyte-pos et omettant le last-cleartextbyte-pos.

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

Se référer à la CEI 62481-1, 7.5.5.2.19.

La réponse comportera l'en-tête de réponse à une recherche d'octet de texte en clair. Si la longueur d'instance est connue, c'est alors le nombre d'octets dans la plage de données UCDAM [s0, sN] pour le domaine des octets de texte en clair. Sinon, le jeton de longueur d'instance sera de «*».

L'en-tête de requête de recherche d'octet de texte en clair peut être différent selon le système de protection de liaison utilisé. Pour les exigences générales de l'en-tête, voir 7.6.6.2.2, pour le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.5.1.2, pour le système de protection de liaison WMDRM-ND, voir 9.6.1.7, pour la définition de cet en-tête.

7.6.3.2.3.5 Pour un contenu binaire utilisant un système de protection de liaison, si un point d'extrémité de serveur HTTP connaît la longueur d'instance d'un

contenu binaire, il doit alors fournir la longueur d'instance dans l'en-tête de réponse à une recherche d'octet de texte en clair.

Noter que cette directive est obligatoire pour les scénarios où le serveur HTTP fournit un contenu mémorisé.

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

Se référer à la CEI 62481-1, 7.5.5.2.19.

7.6.3.2.4 MT HTTP – Plage de données de «disponibilité limitée des données à accès aléatoire»

Pour un contenu binaire utilisant un système de protection de liaison, si un point d'extrémité de serveur HTTP prend en charge la requête de recherche d'octet de texte en clair pour un contenu binaire fonctionnant selon le modèle de «disponibilité limitée des données à accès aléatoire», il doit fournir cleartextbyte-range dans le champ d'en-tête availableSeekRange.dlna.org HTTP de la réponse cible à une requête HTTP avec le champ d'en-tête HTTP de l'en-tête getAvailableSeek.Range.dlna.org et ce cleartextbyte-range doit se référer à une plage d'octets dans le domaine des octets de texte en clair.

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

Se référer à la CEI 62481-1, 7.5.5.2.20.

7.6.3.2.5 MT HTTP – Plage de données de «disponibilité limitée des données à accès aléatoire»

Pour un contenu binaire utilisant un système de protection de liaison, l'en-tête de requête de recherche d'octet de texte en clair doit être utilisé comme mécanisme pour les opérations de recherche par octet sur le protocole de transport HTTP, qui sont spécifiées dans le domaine des octets de texte en clair.

L'en-tête RANGE doit être utilisé comme mécanisme pour spécifier les opérations de recherche d'octet sur le protocole de transport HTTP, qui sont spécifiées dans le domaine des octets de réseau. La plage de données pouvant être recherchée doit être équivalente à la plage de données d'accès aléatoire [r0, rN].

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

Se référer à la CEI 62481-1, 7.5.5.2.21.

L'en-tête de requête de recherche d'octet de texte en clair peut être différent selon le système de protection de liaison utilisé. Pour les exigences générales de l'en-tête, voir 7.6.6.2.2, pour le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.5.1.2, pour le système de protection de liaison WMDRM-ND, voir 9.6.1.7, pour la définition de cet en-tête.

7.6.3.2.6 Recherche MT HTTP basée sur le temps (serveur)

Si un point d'extrémité de serveur HTTP prend en charge à la fois les opérations de recherche basée sur le temps et les opérations basées sur les octets dans le domaine des octets de texte en clair sur une ressource utilisant le système de protection de liaison, il doit alors spécifier une valeur cleartextbyte-range en utilisant l'en-tête de réponse à une recherche d'octet de texte en clair et une valeur npt-range utilisant l'en-tête TimeSeekRange.dlna.org dans la réponse cible HTTP à la requête HTTP.

L'en-tête `TimeSeekRange.dlna.org` doit inclure la valeur `instance-duration`. L'en-tête de réponse à une recherche d'octet de texte en clair doit inclure la valeur `instance-length` appropriée sauf si l'exception suivante s'applique.

Exception:

- Si toutes les conditions suivantes sont vraies.
- Le modèle d'accès de données est le modèle de «disponibilité limitée des données à accès aléatoire».
- L'indicateur de mode (comme indiqué dans `availableSeekRange.dlna.org`) est à «1».
- La requête a omis l'en-tête de requête de recherche d'octet de texte en clair et a spécifié uniquement `TimeSeekRange.dlna.org`.

Exemple 1:

- `TimeSeekRange.dlna.org: npt=335.1-336.1/40445.4`
- `Content-Range.dtcp.com: octets 1539686400-1540210688/304857907200`

Exemple 2:

- `TimeSeekRange.dlna.org: npt=00:05:35.2-00:05:38.1/*`
- `Content-Range.dtcp.com: octets 1539686400-1540210688/*`

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

Se référer à la CEI 62481-1, 7.5.5.2.24.

Pour le contenu de liaison protégé, la plage d'instance est retournée en utilisant l'en-tête de réponse à une recherche d'octet de texte en clair et en n'utilisant pas l'en-tête `TimeSeekRange.dlna.org`. En conséquence, les deux en-têtes doivent être retournés pour indiquer la position d'octet dans le domaine des octets de texte en clair.

Les valeurs `instance-duration` et `npt-range` de `TimeSeekRange.dlna.org` sont définies en 7.5.5.2.24.3.

Les valeurs `cleartextbyte-range` et `instance-length` pour l'en-tête de réponse à une recherche d'octet de texte en clair sont définies dans le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) en 8.5.1.2, pour le système de protection de liaison WMDRM-ND en 9.6.1.7.

7.6.3.2.7 Directives de mise en antémémoire MT pour HTTP 1.0

Un point d'extrémité de serveur HTTP transférant un contenu en utilisant la protection de liaison DLNA comme réponse à une requête HTTP/1.0 GET doit empêcher une mise en antémémoire intermédiaire en incluant la directive parmi les en-têtes de réponse HTTP.

- `Pragma: no-cache`

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

Se référer à la CEI 62481-1, 7.5.5.2.34.

7.6.3.2.8 Directives de mise en antémémoire MT pour HTTP 1.1

Un point d'extrémité de serveur HTTP transférant un contenu en utilisant la protection de liaison DLNA comme réponse à une requête HTTP/1.1 GET doit empêcher une mise en mémoire intermédiaire en incluant la directive parmi les en-têtes de réponse HTTP.

- `Pragma: no-cache`

- Cache-control: no-cache

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

Se référer à la CEI 62481-1, 7.5.5.2.35.

7.6.3.3 Nouvelles exigences générales de transport de support HTTP

7.6.3.3.1 Codes d'erreur HTTP pour contenu indisponible

Si un point d'extrémité de serveur HTTP reçoit une requête pour un contenu binaire avec une requête HTTP GET ou HEAD et que le point d'extrémité de serveur ne peut pas rendre disponible ce contenu en raison d'un problème de licence de protection du contenu, il convient que le point d'extrémité de serveur HTTP réponde avec un code d'erreur 403 (interdit).

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

Se référer à la CEI 62481-1, 7.5.5.2.4.

Au moyen de la spécification HTTP, le point d'extrémité de serveur HTTP peut disposer des informations supplémentaires concernant la cause de l'erreur dans le corps d'entité de la réponse.

7.6.3.3.2 Définitions des positions d'octet MT

Pour un contenu utilisant une protection de liaison DLNA, sauf spécification contraire, toutes les références de la CEI 62481-1 se référant aux positions d'octet aux opérations de recherche basée sur les octets (par exemple les en-têtes Range, Content-Range, et Content-Length, ainsi que les valeurs d'unité d'octet de instance-length et byte-range de l'en-tête TimeSeekRange.dlna.org) doivent se référer aux positions d'octets dans le domaine des octets de réseau (c'est-à-dire, après avoir ajouté le chiffrement et toutes les en-têtes de protection de liaison ainsi que le remplissage).

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

Se référer à la CEI 62481-1, 7.5.5.2.7.

7.6.3.3.3 En-tête MT HTTP – En-tête de requête de recherche d'octet de texte en clair (serveur)

7.6.3.3.3.1 Si le point d'extrémité de serveur HTTP transporte un contenu utilisant une protection de liaison DLNA, il convient que le point d'extrémité de serveur HTTP prenne en charge la réception de l'en-tête de requête de recherche d'octet de texte en clair comme défini dans les directives ci-dessous pour les méthodes HTTP GET et HEAD.

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

Se référer à la CEI 62481-1, 7.5.5.2.24.

7.6.3.3.3.2 Si le point d'extrémité de serveur HTTP transporte un contenu en utilisant la protection de liaison DLNA et le point d'extrémité de serveur HTTP reçoit l'en-tête de requête de recherche d'octet de texte en clair dans une requête HEAD, alors le serveur HTTP peut répondre sans l'en-tête de réponse à une recherche d'octet de texte en clair.

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

7.6.3.3.3.3 Si le point d'extrémité de serveur HTTP transporte un contenu en utilisant la protection de liaison DLNA et le point d'extrémité de serveur HTTP retourne la

plage de données demandée avec l'en-tête de requête de recherche d'octet de texte en clair, il doit spécifier l'en-tête de réponse à une recherche d'octet de texte en clair dans la réponse cible. De plus, le code de réponse HTTP doit être: 200 (OK).

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

Les positions spécifiées dans cet en-tête se réfèrent aux positions dans le domaine des octets de texte en clair.

7.6.3.3.3.4 Si le point d'extrémité de serveur HTTP transporte un contenu en utilisant la protection de liaison DLNA, il doit répondre avec l'en-tête de requête à une réponse d'octet de texte en clair pour une requête spécifiée avec l'en-tête de requête de recherche d'octet de texte en clair dans la requête HTTP GET.

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

7.6.3.3.3.5 Si le point d'extrémité de serveur HTTP transporte un contenu en utilisant la protection de liaison DLNA et le point d'extrémité de serveur HTTP utilise l'en-tête de réponse à une recherche d'octet, alors les valeurs fournies doivent être précises sur la plage demandée sur le domaine des octets de texte en clair permettant l'alignement sur les frontières à l'intérieur du contenu binaire. De façon spécifique,

- la position du premier octet spécifiée dans l'en-tête de réponse à une recherche d'octet de texte en clair doit correspondre au premier octet demandé dans l'en-tête ou le début de requête de recherche d'octet de texte en clair dans une position d'alignement approprié au décodeur pour le profil de format donné contenant l'octet demandé;
- la position du dernier octet spécifiée dans l'en-tête de réponse à une recherche d'octet de texte en clair doit bien correspondre du dernier octet demandé dans l'en-tête ou la fin de requête de recherche d'octet de texte en clair au point d'extrémité d'un élément d'alignement de format de support pour le profil de format donné utilisé.

La valeur indiquant instance-length doit indiquer la longueur de l'ensemble du contenu binaire d'origine sur le domaine des octets de texte en clair (c'est-à-dire avant chiffrement et toute mise en paquet de protection de liaison) ou un astérisque (*) si elle est inconnue.

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

La position d'alignement approprié au décodeur est définie pour chacun des profils de format de support spécifiés en 8.8, directives de profil DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) de format de support et en 9.9 directives de profil WMDRM-ND de format de support.

L'élément d'alignement de format de support est défini pour chacun des profils de format de support spécifiés en 8.8, directives de profil DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) de format de support et en 9.9 directives de profil WMDRM-ND de format de support.

7.6.3.3.3.6 Si le point d'extrémité de serveur HTTP transporte un contenu en utilisant la protection de liaison DLNA et que le point d'extrémité de serveur HTTP utilise l'en-tête de réponse à une recherche d'octet de texte en clair pour retourner une plage de données spécifiques, le premier octet du corps de l'entité HTTP doit correspondre au début d'un élément d'alignement de protection de liaison pour le système de protection de liaison donné utilisé.

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

Il y a eu généralement une opération de recherche lorsque les octets retournés ne correspondent pas aux octets qui suivent le paquet précédent. Pour permettre au déchiffrement de fonctionner correctement, le client doit être capable de démarrer le déchiffrement au début du corps de l'entité HTTP.

- 7.6.3.3.3.7** Si la plage demandée avec l'en-tête de requête de recherche d'octet de texte en clair n'est pas valable pour la ressource avec un URI (Identificateur uniforme de ressource) spécifié dans la requête HTTP, le point d'extrémité de serveur HTTP doit alors répondre avec le code de réponse HTTP 416 (plage demandée non validable).

Lorsqu'on rencontre des erreurs de syntaxe avec l'en-tête de requête de recherche d'octet de texte en clair, le serveur HTTP doit utiliser le code de réponse HTTP 400 (mauvaise requête).

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

Le code de réponse HTTP 416 est utilisé lorsque le point d'extrémité du serveur HTTP prend en charge une recherche dans le domaine des octets de texte en clair pour le contenu binaire spécifié mais est incapable de satisfaire à la requête car la plage demandée n'est pas actuellement disponible sur le serveur.

- 7.6.3.3.3.8** Si une requête HTTP avec un en-tête de requête de recherche d'octet de texte en clair pour l'URI ne peut jamais être traitée/satisfaite par le point d'extrémité de serveur HTTP, par exemple dans le cas d'un transcodage en temps réel ou d'un contenu en direct, le point d'extrémité de serveur HTTP doit alors répondre avec 406 (non acceptable).

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

Le code de réponse HTTP 406 est utilisé lorsque le point d'extrémité de serveur HTTP ne prend pas en charge la recherche dans le domaine des octets de texte en clair pour le contenu binaire spécifié et la requête comporte l'en-tête de requête de recherche d'octet de texte en clair.

Noter que l'utilisation d'un en-tête de requête de recherche d'octet de texte en clair avec une position de début à 0 et demandant toute la plage de contenus disponibles utilise toujours l'en-tête de requête de recherche d'octet de texte en clair.

Noter que ceci inclut le cas où l'en-tête incorrect de requête de recherche d'octet de texte en clair est utilisé pour le type de contenu binaire. Pour la spécification de l'en-tête requis pour le système de protection de liaison donné utilisé, voir 8.5.1.3, pour le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP); pour le système de protection de liaison WMDRM-ND, voir 9.6.1.8.

- 7.6.3.3.3.9** Si un point d'extrémité de serveur HTTP reçoit une requête GET ou HEAD à la fois avec l'en-tête de requête de recherche d'octet de texte en clair et l'en-tête RANGE, le point d'extrémité de serveur HTTP doit alors répondre par 406 (non acceptable).

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

Le client ne peut pas spécifier cette situation, voir 7.6.3.3.4.3. Si un point d'extrémité de serveur HTTP peut prendre en charge des requêtes HTTP avec une plage d'octets spécifiée, comme exprimé dans l'en-tête de requête de recherche d'octet de texte en clair pour un URI (Identificateur uniforme de ressource) particulier, alors il convient que le point d'extrémité de serveur HTTP prenne en charge des connexions persistantes (HTTP/1. 1) pour cet URI.

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

Le contenu demandé avec l'option de plages d'octets peut souvent obtenir un grand nombre de requêtes en utilisant l'en-tête de requête de recherche d'octet de texte en clair en une courte période de temps, provoquant potentiellement l'épuisement des connexions disponibles pour les dispositifs serveurs de contenus.

- 7.6.3.3.3.10** Il convient qu'un point d'extrémité de serveur HTTP prenne en charge des requêtes HTTP spécifiant l'en-tête de requête de recherche d'octet de texte

en clair en mettant en œuvre un comportement retournant le corps d'entité demandé avec l'en-tête HTTP 200 (OK).

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

7.6.3.3.4 En-tête MT HTTP – En-tête de requête de recherche d'octet de texte en clair (client)

- 7.6.3.3.4.1** Les points d'extrémité de client HTTP ne doivent pas fournir de requête HTTP GET et HEAD avec l'en-tête de requête de recherche d'octet de texte en clair pour des éléments de contenu n'indiquant pas explicitement une prise en charge de l'en-tête de requête de recherche d'octet de texte en clair par l'intermédiaire de l'indicateur cleartextbytesseek-full du quatrième champ ou de l'indicateur lop-cleartextbytes ou de flags-param comme défini en 7.5.2.1.2.

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

Se référer à la CEI 62481-1, 7.5.5.2.24.

Cette interdiction inclut les requêtes HTTP GET et HEAD avec une plage incluant tout le contenu binaire.

- 7.6.3.3.4.2** Les points d'extrémité de client HTTP doivent spécifier les positions d'octet dans le domaine des octets de texte en clair (avant d'ajouter le chiffrement de protection de liaison, les en-têtes ou le remplissage) lors de l'utilisation de l'en-tête de requête de recherche d'octet de texte en clair.

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

- 7.6.3.3.4.3** Les points d'extrémité de client HTTP ne doivent pas spécifier de requête HTTP GET ou HEAD indiquant à la fois l'en-tête de requête de recherche d'octet de texte en clair et l'en-tête HTTP RANGE.

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

Il est peu probable que la requête puisse être satisfaite avec des spécifications à la fois pour la position d'octet dans le domaine des octets de réseau et le domaine des octets de texte en clair.

7.6.4 Directives concernant le transport de support HTTP pour le transfert en flux continu

7.6.4.1 Mises à jour des directives générales existantes concernant le transport de support HTTP pour le transfert en flux continu

7.6.4.1.1 Généralités

Le Tableau 11 fait référence à la CEI 62481-1.

Tableau 11 – Mises à jour des directives générales existantes concernant le transport de support HTTP pour le transfert en flux continu

Exigence mise à jour	Emplacement dans la CEI 62481-1
Fonctionnement du support en balayage en avance rapide MT HTTP	7.5.5.3.8
Fonctionnement du support en balayage en avance lente de transfert en flux continu MT HTTP	7.5.5.3.9
Fonctionnement du support en balayage en retour rapide en flux continu MT HTTP	7.5.5.3.10
Fonctionnement du support en balayage en retour lent en flux continu MT HTTP	7.5.5.3.11
Fonctionnement du support en balayage en flux continu MT HTTP	7.5.5.3.12
Fonctionnement du support MT HTTP dans un profil	7.5.5.3.15.2
RANGE MT combiné, recherche basée sur le temps et requêtes HTTP de vitesse de lecture	7.5.5.3.17.2
En-tête MT HTTP: realTimeInfo.dlna.org	7.5.5.3.18.6

7.6.4.1.2 Fonctionnement du support en recherche MT HTTP

Il convient qu'un point d'extrémité de client HTTP en flux continu mette en œuvre le fonctionnement de support en recherche sur un contenu utilisant une protection de liaison DLNA en utilisant l'en-tête de requête de recherche d'octet de texte en clair RANGE ou l'en-tête TimeSeekRange.dlna.org, si ces en-têtes sont pris en charge par le serveur HTTP pour le contenu binaire.

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

Se référer à la CEI 62481-1, 7.5.5.3.7.

L'en-tête de requête de recherche d'octet de texte en clair peut être différent selon le système de protection de liaison utilisé. Pour les exigences générales de l'en-tête, voir 7.6.6.2.2, pour le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), voir 8.5.1.2, pour le système de protection de liaison WMDRM-ND, voir 9.6.1.7, pour la définition de cet en-tête.

7.6.5 Directives concernant le transport de support HTTP pour transfert interactif

7.6.5.1 Généralités

Ce paragraphe fournit des mises à jour des directives générales existantes concernant le transport de support HTTP pour le transfert interactif.

7.6.5.2 Comportement de MT RANGE pour le contenu interactif transféré

Pour un contenu binaire utilisant un système de protection de liaison, l'en-tête de requête de recherche d'octet de texte en clair peut être utilisé pour des transferts interactifs lorsque le modèle «disponibilité complète des données à accès aléatoire» ou le modèle «disponibilité limitée des données à accès aléatoire» avec mode-flag=1 s'applique au point d'extrémité de serveur HTTP desservant le contenu binaire.

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

Se référer à la CEI 62481-1, 7.5.5.4.3.

7.6.6 Transport RTP (Protocole en temps réel)

7.6.6.1 Généralités

Ce paragraphe couvre les directives pour le protocole de transport RTP (Protocole en temps réel) pour un contenu transmis en utilisant une protection de liaison DLNA. Pour des informations détaillées, voir 7.5 de la CEI 62481-1.

7.6.6.2 Mise à jour des directives générales existantes concernant le transport RTP (Protocole en temps réel)

7.6.6.2.1 Taille des paquets MT RTP (Protocole en temps réel)

Il convient qu'un point d'extrémité de serveur limite la taille du contenu de transport RTP (Protocole en temps réel) en utilisant la protection de liaison DLNA de façon que la taille du paquet chiffré, incluant les en-têtes de protocole, les en-têtes de protection de liaison et tout remplissage nécessaire, ne dépasse pas l'Unité de transmission maximale (MTU) utilisée dans le réseau domestique.

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

Se référer à la CEI 62481-1, 7.5.6.3.5.

Une encapsulation de protection de liaison peut ajouter des en-têtes et un remplissage et augmente la taille de la charge utile.

7.6.6.2.2 Fonctionnement du support en lecture MT RTP (Protocole en temps réel)

Si un point d'extrémité de serveur RTSP (Protocole de transfert en flux continu en temps réel) reçoit une requête pour un contenu binaire avec une requête RTSP PLAY ou SETUP et que le point d'extrémité de serveur ne peut pas rendre disponible ce contenu en raison d'un problème de licence de protection du contenu, il convient que le point d'extrémité de serveur RTSP réponde avec un code d'erreur 403 (Interdit).

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

Se référer à la CEI 62481-1, 7.5.8.2.36.

7.6.6.3 Nouvelles directives générales de transport RTP (Protocole en temps réel) MT – RTP prise en charge du contenu de liaison protégé

Il convient que les points d'extrémité de desserte et les points d'extrémité de réception mettant en œuvre un système de protection de liaison et prenant en charge le transport de support RTP (Protocole en temps réel) pour le contenu de liaison non protégé mettent en œuvre le système de protection de liaison pour le transport de support RTP.

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

Se référer à la CEI 62481-1, 7.5.6.2.18.

Il est recommandé que les récepteurs de contenu et les sources de contenu mettant en œuvre un système de protection de liaison et prenant également en charge le transport facultatif de support RTP (Protocole en temps réel) étendent leur prise en charge au système de protection de liaison en incluant le transport de support RTP.

7.7 Virtualisation du dispositif de conversion de contenu

Il n'y a aucune modification au paragraphe correspondant de la CEI 62481-1 concernant la protection de liaison. Les directives contenues en 7.6 de la CEI 62481-1 sont identiques pour les dispositifs échangeant un contenu en utilisant une protection de liaison DLNA. De manière

correspondante, il n'y a pas de directive spécifique supplémentaire DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) ou WMDRM-ND à l'Article 8 ou à l'Article 9 pour la conversion de contenu et la Virtualisation de dispositif.

7.8 Unité d'interopérabilité de support (MIU)

Il n'y a aucune modification au paragraphe correspondant de la CEI 62481-1 concernant la protection de liaison. Les directives contenues en 7.7 de la CEI 62481-1 sont identiques pour les dispositifs échangeant un contenu en utilisant une protection de liaison DLNA. De manière correspondante, il n'y a pas de directive spécifique supplémentaire DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) ou WMDRM-ND à l'Article 8 ou à l'Article 9 pour les dispositifs MIU (Unité d'interopérabilité de support).

7.9 Exigences des directives concernant la technologie de protection de liaison

7.9.1 Système de protection de liaison – DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)

7.9.1.1 Si un dispositif prend en charge la protection de liaison DLNA il doit prendre en charge DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) comme défini dans ces directives.

M	A	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	DTCP Volume 1, DTCP Volume 1 Supplément E, Règles de conformité audio DTCP EXHIBIT B-2: [10]	BSTW5	
---	---	------------------	-------------	-----	---	-------	--

7.9.1.2 Si un serveur AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) prend en charge la protection de liaison DLNA, il doit être capable d'exposer et de transférer au moins l'un des profils de format de support DLNA avec protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).

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

7.9.1.3 Si un point de pilotage de rendu de support AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) prend en charge la protection de liaison DLNA il doit être capable de transférer au moins l'un des profils de format de support DLNA avec protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).

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

7.9.1.4 Si un MediaServer (Serveur de support) AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) prend en charge la protection de liaison DLNA les objets de contenu qu'il expose pour lesquels DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) est autorisé comme sortie doivent avoir un élément <res> avec un identificateur de profil utilisant le préfixe DTCP_.

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

La phrase «autorisé comme sortie» se réfère à une utilisation conforme aux exigences de la politique à laquelle est soumis le point d'extrémité et qui sont définies par l'entité régissant l'utilisation du contenu. Ceci exclut des décisions de conception du produit ou une politique du fabricant du produit. Bien que la définition de ces politiques ne fasse pas partie du

domaine d'application des directives concernant la protection de liaison DLNA, le comportement requis exprimé par cette directive produira une interopérabilité améliorée.

- 7.9.1.5** Si un contrôleur de poussée prend en charge la protection de liaison DLNA, le contenu qu'il achemine en continu autorisant DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) comme sortie doit être disponible avec la protection de liaison DTCP-IP.

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

- 7.9.1.6** Si un dispositif prend en charge le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) il doit prendre en charge toutes les directives de la CEI 62481-1, modifiées par les directives qui se trouvent à l'Article 7 de cette norme ainsi que 8.2, 8.4 et 8.5.1.2 à 8.5.1.3 et si le format de transport de support RTP (Protocole en temps réel) est pris en charge, 8.5.1.4 à 8.5.1.6.

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

7.9.2 Système de protection de liaison – DRM (gestion des droits numériques) «Windows media» pour dispositifs réseau

- 7.9.2.1** Si un dispositif prend en charge la protection de liaison DLNA il peut prendre en charge WMDRM-ND comme défini dans ces directives.

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

- 7.9.2.2** Si un serveur de support AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) prend en charge la protection de liaison DLNA les objets de contenu qu'il expose pour lesquels WMDRM-ND est autorisé comme sortie peuvent avoir un élément <res> avec un identificateur de profil utilisant le préfixe WMDRM_.

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

La phrase «autorisé comme sortie» se réfère à une utilisation conforme aux exigences de la politique à laquelle est soumis le point d'extrémité et qui sont définies par l'entité régissant l'utilisation du contenu. Ceci exclut des décisions de conception du produit ou une politique du fabricant du produit. Bien que la définition de ces politiques ne fasse pas partie du domaine d'application des directives de protection de liaison DLNA, le comportement facultatif exprimé par cette directive produira une interopérabilité améliorée. Les objets de contenu qui ne sont autorisés à sortir que sur WMDRM-ND peuvent facultativement être exposés sur le réseau avec la protection WMDRM-ND; les objets de contenu qui sont autorisés à sortir à la fois sur DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) et WMDRM-ND peuvent facultativement être exposés sur le réseau avec la protection WMDRM-ND en plus d'être exposés avec la protection DTCP-IP requise.

- 7.9.2.3** Si un contrôleur de poussée prend en charge la protection de liaison DLNA, le contenu qu'il achemine en continu autorisant WMDRM-ND comme sortie peut être disponible avec la protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).

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

- 7.9.2.4** Si un dispositif prend en charge le système de protection de liaison WMDRM-ND il doit prendre en charge toutes les directives de la CEI 62481-1, modifiées par les directives qui se trouvent à l'Article 7 de cette norme ainsi que 9.2, 9.3, 9.4, 9.6.1.2 à 9.6.1.8 et si le format de transport de support RTP (Protocole en temps réel) est pris en charge, 9.6.2.2 à 9.6.2.7.

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

8 Directives concernant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)

8.1 Généralités

Ce paragraphe contient les directives spécifiques au système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).

Voir 8.9 pour les exigences générales concernant les dispositifs mettant en œuvre DTCP-IP.

8.2 Mise en réseau et connectivité

8.2.1 Mise en réseau et connectivité – Exigences de capacité générales

Ce paragraphe contient les exigences spécifiques à l'utilisation DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) des capacités de mise en réseau décrites en 7.2 de la CEI 62481-1.

8.2.2 Nouvelles exigences de DLNAQOS exigence de QoS (Qualité de service) pour le trafic DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)

Si la QoS (Qualité de service) DLNA comme défini en 7.2 de la CEI 62481-1 est mise en œuvre, toutes les commandes et réponses DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) générée par les sources de contenu et les récepteurs de contenu doivent être marquées comme DLNAQOS_3, ou une valeur DLNAQOS_UP inférieure, conformément au Tableau 3.

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

DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) comporte un essai de RTT (Temps d'aller et retour) imposant des exigences rigoureuses au séquençement du réseau. Pour assurer que ces paquets obtiennent le meilleur service de réseau disponible, le niveau de DLNAQOS doit être fixé de manière appropriée. Il convient d'assigner aux messages DTCP-IP une priorité supérieure à celle du flux A/V (Audio avec vidéo) lui-même.

8.2.3 Nouvelles exigences des dispositifs – NC CP commun – Sécurité sans fil

Les dispositifs utilisant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) avec IEEE 802.11 intégré doivent assurer que WEP ou un autre mécanisme de protection équivalent (par exemple WPA (Accès protégé WiFi) ou WPA2) est mis en œuvre avant d'échanger des commandes d'AKE (Authentification et échange de clé) DTCP et un contenu protégé par l'intermédiaire de cette interface de réseau.

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

Ceci est une exigence de la spécification DTCP.

8.3 Découverte et pilotage de dispositif

Il n'y a pas de modification spécifique à DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) dans les directives de 7.3 de la CEI 62481-1.

8.4 Gestion du support

8.4.1 Gestion du support – Gestion du support AV (Audio avec vidéo)

Ce paragraphe traite des directives pour mettre en œuvre la gestion de support en utilisant l'architecture AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) qui sont spécifiques au système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP). Pour des informations détaillées, voir 7.5 de la CEI 62481-1.

8.4.2 MM CP – URI (Identificateur uniforme de ressource) DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)

Un dispositif DLNA ne doit pas se baser sur l'existence de paramètres d'URI (Identificateur uniforme de ressource) pour établir la connexion d'AKE (Authentification et échange de clé) DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).

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

La spécification DTCP permet de placer les paramètres d'AKE (Authentification et échange de clé) DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) pour l'hôte et le port, soit dans le type MIME (Extension de courrier Internet à fonctions multiples), soit dans l'URI (Identificateur uniforme de ressource) du contenu. Cette spécification exige que les serveurs publient l'hôte et le port dans le type MIME et les dispositifs de rendu ne doivent pas se baser sur les informations qui se trouvent également dans l'URI.

8.5 Transport de support

8.5.1 Transport HTTP

8.5.1.1 Généralités

Ce paragraphe traite des directives pour mettre en œuvre le transport de support en utilisant l'architecture AV (Audio avec vidéo) UPnP (Universel prêt à fonctionner) qui sont spécifiques au système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP). Pour des informations détaillées, voir 7.5 de la CEI 62481-1.

8.5.1.2 MT HTTP – En-tête de requête de recherche d'octet de texte en clair pour DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)

8.5.1.2.1 Le serveur HTTP et les points d'extrémité de client doivent utiliser l'en-tête Range.dtcp.com comme en-tête de requête de recherche d'octet de texte en clair pour le contenu utilisant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) transmis en utilisant le protocole de transport de support HTTP.

M	R	DMS DMP DMR +PU+	M-DMS M-DMP	MIU	DTCP Volume 1 Supplément E, [4]	4I6WA	
---	---	------------------	-------------	-----	--	-------	--

8.5.1.2.2 La notation du champ d'en-tête Range.dtcp.com pour le transport de support HTTP du contenu utilisant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) doit être comme indiqué ci-dessous:

- 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-clear-text-byte-pos "-" [last-clear-text-byte-pos];
- first-clear-text-byte-pos = 1*DIGIT;
- last-clear-text-byte-pos = 1*DIGIT;

first-clear-text-byte-pos et last-clear-text-byte-pos s'appliquent au contenu binaire d'origine qui précède immédiatement le traitement DTCP c'est-à-dire avant chiffrement et mise en paquet PCP (Paquet de contenu protégé).

Noter que «bytes» est sensible à la casse.

Exemples:

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

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

8.5.1.3 MT HTTP – En-tête de réponse à une recherche d'octet de texte en clair pour DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)

8.5.1.3.1 Le serveur HTTP et les points d'extrémité de client doivent utiliser l'en-tête Content-Range.dtcp.com comme en-tête de réponse à une recherche d'octet de texte en clair pour le contenu utilisant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) transmis en utilisant le protocole de transport de support HTTP.

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

8.5.1.3.2 La notation du champ d'en-tête Content-Range.dtcp.com pour le transport de support HTTP du contenu utilisant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) doit être comme indiqué ci-dessous:

- 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-clear-text-byte-pos "-" last-clear-text-byte-pos;
- first-clear-text-byte-pos = 1*DIGIT;
- last-clear-text-byte-pos = 1*DIGIT;
- instance-length = 1*DIGIT;

first-clear-text-byte-pos, last-clear-text-byte-pos et instance-length s'appliquent au contenu binaire sur le domaine des octets de texte en clair qui précède immédiatement le traitement DTCP c'est-à-dire avant chiffrement et mise en paquet PCP (Paquet de contenu protégé).

Noter que «bytes» est sensible à la casse.

Exemple d'en-tête Content-Range.dtcp.com.

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

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

8.5.2 Transport RTP (Protocole en temps réel)

8.5.2.1 Généralités

Ce paragraphe traite des directives pour le protocole de transport RTP (Protocole en temps réel) pour des dispositifs DLNA utilisant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).

8.5.2.2 MT RTP CP – Profils de formats de support de liaison protégée

Pour des valeurs d'identificateur de profil A/V (Audio avec vidéo), de 8.8 pour lesquelles ce qui suit est vérifié:

- le profil de format de support définit le contenu de liaison protégé,
- le système de protection de liaison utilisé est DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).

L'encapsulation RTP (Protocole en temps réel) de ce profil de format de support ne doit pas utiliser un type de charge utile statique, voir 8.5.2.4.

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

8.5.2.3 Profils de format de support encapsulé MT DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)

8.5.2.3.1 Pour un contenu binaire utilisant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), le contenu binaire de texte en clair doit d'abord être encapsulé dans une charge utile RTP (Protocole en temps réel) et un en-tête RTP doit être généré, conforme aux directives de 7.5.6.3 à 7.5.7.10 conformément au profil de format correspondant du contenu non chiffré.

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

8.5.2.3.2 Après encapsulation RTP (Protocole en temps réel) du contenu de texte en clair selon 8.5.1.2.1, la charge utile RTP ainsi générée doit être chiffrée dans un PCP (Paquet de contenu protégé) de DTCP (Protection du contenu d'une transmission numérique) unique, comme défini en [10].

La charge utile RTP (Protocole en temps réel) comporte la partie de support encapsulé, mais pas l'en-tête RTP, la liste CSRC (Source contributive), l'en-tête RTP étendu ou tout remplissage RTP appliqué.

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

8.5.2.3.3 Toutes les autres informations d'en-tête de RTP (Protocole en temps réel) pour la charge utile encapsulée DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) doivent correspondre à la valeur correspondante de l'en-tête de RTP de l'encapsulation du flux de contenu de texte en clair de 8.5.1.2.1.

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

Toutes les informations de séquençement transportées dans l'en-tête de RTP (Protocole en temps réel) d'un paquet encapsulé DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) doivent correspondre aux informations disponibles pour la charge utile RTP non chiffrée située à l'intérieur.

8.5.2.4 MT RTP CP

Si le système de protection de liaison est DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), le champ de support de SDP (Protocole de description de session) doit être «application» et on doit utiliser un type de charge utile dynamique.

Le champ d'attribut rtpmap doit avoir pour nom de codage «x-dtcp1».

Le champ fmt attribute doit avoir "CONTENTFORMAT=<MIME-Type> DTCP1HOST=<address> DTCP1PORT=<port>" comme paramètres spécifique de format.

Dans ce cas, <MIME-Type> représente le type MIME (Extension de courrier Internet à fonctions multiples) de l'encapsulation de RTP (Protocole en temps réel) avant d'appliquer la protection de liaison.

<address> représente l'adresse IP de l'hôte d'AKE (Authentification et échange de clé).

<port> représente le port sur lequel l'hôte d'AKE écoute les messages d'authentification et d'échange de clé.

Les paramètres d'AKE <address> et <port> pour tous les flux définis dans le SDP (Protocole de description de session) doivent être égaux.

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

Se référer à RFC 2327.

Exemple:

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

Si le flux vidéo et le flux audio sont séparés, il convient de décrire 2 types de charge utile dynamique comme suit.

```
m=application 0 RTP/AVP 96
a=rtpmap:96 x-dtcp1/90000
a=fmt: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 Virtualisation du dispositif de conversion de contenu

Il n'existe pas de directive spécifique à DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) pour la conversion de contenu et la virtualisation de dispositif.

8.7 Unité d'interopérabilité de support (MIU)

Il n'existe pas de directive spécifique à DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) pour les unités d'interopérabilité de support.

8.8 Format de support – Directives de profilage DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP)

8.8.1 Généralités

Ce paragraphe contient des additions à la CEI 62481-2 définissant les profils de format de support DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP). Ce paragraphe contient des directives spécifiques au système de protection de liaison DTCP-IP. Les directives ne s'appliquent qu'aux dispositifs DLNA mettant en œuvre le système de protection de liaison DTCP-IP.

8.8.2 CP DTCP-IP – Profil

8.8.2.1 Généralités

Profil: DTCP_*

8.8.2.2 Les principales caractéristiques des profils qui sont encapsulés en utilisant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) sont définies dans le Volume 1 de DTCP et dans le Supplément E du Volume 1 de DTCP.

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

8.8.2.3 L'identificateur de profil du contenu protégé DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) doit être conforme à la syntaxe suivante:

ProfileID_Protected = "DTCP_" Original_ProfileID

Original_ProfileID = identificateur de profil spécifié dans la CEI 62481-2 qui serait utilisé pour la version de texte en clair du même contenu.

Exemple: Si un contenu binaire conforme à l'identificateur de profil MPEG_PS_NTSC est transféré avec une protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP), l'identificateur de profil du contenu protégé doit alors être DTCP_MPEG_PS_NTSC.

M	A	HND	MHD	n/a	CEI 62481-2	S88V5	
---	---	-----	-----	-----	-------------	-------	--

- 8.8.2.4** Le support transporté dans le profil de format de support DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) après désencapsulation de DTCP-IP doit être conforme à l'identificateur de profil d'origine spécifié dans la partie Original_ProfileID de l'identificateur de profil de format.

M	A	HND	MHD	n/a	CEI 62481-2	B9FS8	
---	---	-----	-----	-----	-------------	-------	--

- 8.8.2.5** Un contenu binaire utilisant un identificateur de profil DTCP ne doit être transféré qu'en utilisant le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).

M	A	HND	MHD	n/a	n/a	FW2J3	
---	---	-----	-----	-----	-----	-------	--

8.8.3 CP DTCP-IP – Définition du type de profil MIME (Extension de courrier Internet à fonctions multiples)

8.8.3.1 Généralités

Profil: DTCP_*

- 8.8.3.2** Lorsqu'il est utilisé pour décrire un contenu binaire, le type MIME (Extension de courrier Internet à fonctions multiples) utilisé pour les profils basés sur le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) doit être comme suit:

application/x-

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

<MIME-type> est le type MIME (Extension de courrier Internet à fonctions multiples) du contenu d'origine avant mise en paquet DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP).

Où <host> et <port> sont l'hôte et le port où le point d'extrémité du serveur écoute tout échange d'AKE (Authentification et échange de clé) requis.

M	C	DMS +PU+	M-DMS	n/a	DTCP Volume 1, DTCP Volume 1 Supplément E	VS3EY	
---	---	----------	-------	-----	---	-------	--

Un exemple serait des valeurs de protocolInfo utilisées dans des éléments <res>.

- 8.8.3.3** La valeur de <host> dans le type MIME (Extension de courrier Internet à fonctions multiples) spécifié en 8.8.3.1 doit être une adresse IP absolue dans le format d'adresse IPv4 a.b.c.d (c'est-à-dire un ordre d'octet de réseau de forme quadruple).

M	R	DMS +PU+	M-DMS	n/a	n/a	XR7U7	
---	---	----------	-------	-----	-----	-------	--

- 8.8.3.4** Lorsqu'il est utilisé pour décrire la capacité d'un dispositif, le type MIME (Extension de courrier Internet à fonctions multiples) utilisé pour les profils basés sur le système de protection de liaison DTCP-IP (Protection du contenu d'une transmission numérique sur des réseaux IP) doit être comme suit:

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