# IEC 62481-7

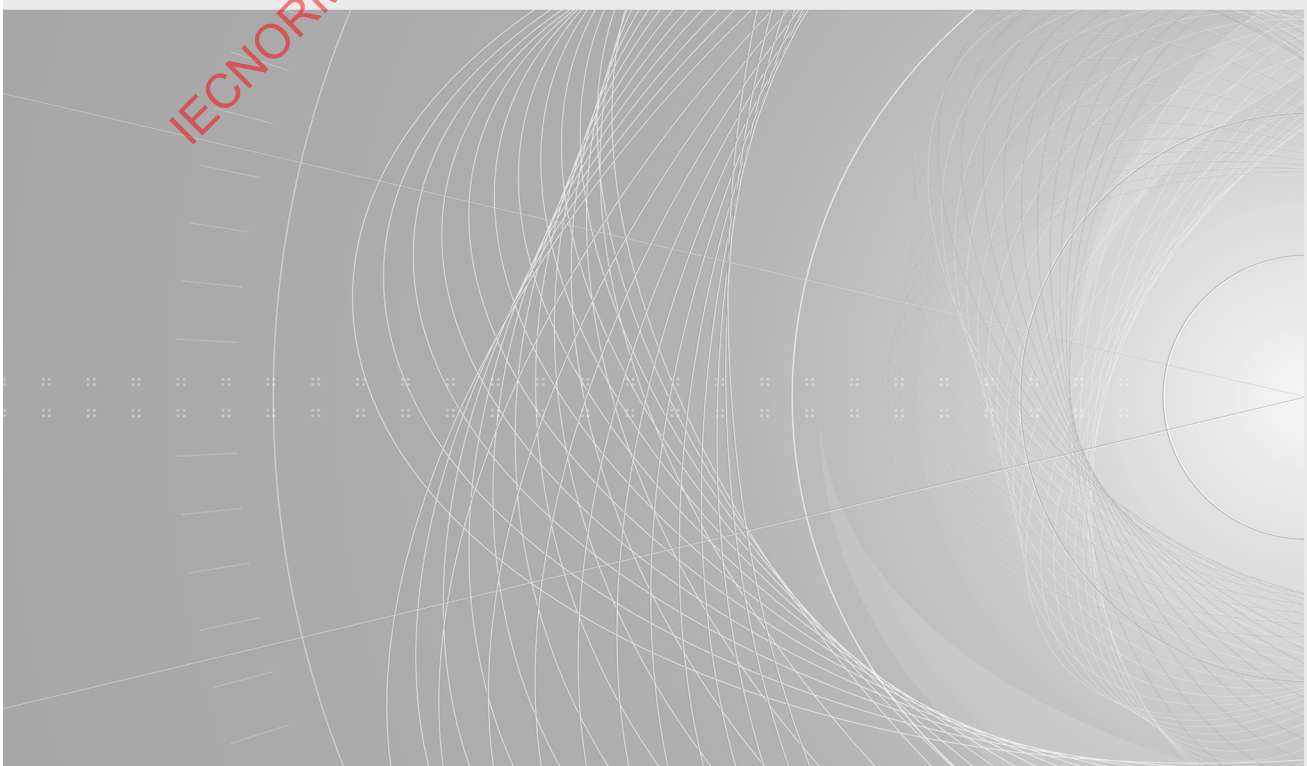
Edition 1.0 2017-07

# INTERNATIONAL STANDARD

colour inside



## Digital living network alliance (DLNA) home networked device interoperability guidelines –
## Part 7: Authentication



IEC 62481-7:2017-07(en)

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

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

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

IEC 62481-7

Edition 1.0 2017-07

# INTERNATIONAL STANDARD





## Digital living network alliance (DLNA) home networked device interoperability guidelines – Part 7: Authentication

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 33.160; 35.100.05; 35.110

ISBN 978-2-8322-4630-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

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

## Part 7: Authentication

## 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 62481-7 has been prepared under technical area 8: Multimedia home systems and applications for end-user network, of IEC technical committee 100: Audio, video and multimedia systems and equipment.

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

| CDV | Report on voting |
|---|---|
| 100/2744/CDV | 100/2889/RVC |

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

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

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

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

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

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

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

# INTRODUCTION

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

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

# Part 7: Authentication

## 1 Scope

This part of IEC 62481 specifies DLNA interoperability guidelines for device authentication.

The DLNA interoperability guidelines are based on a device authentication solution, which is defined as methods to enable authentication of a client device as DLNA Certified. Methods are included to allow a client device to authenticate a server device as trusted by a Certificate Authority.

The guidelines are intended to supplement other interoperability mechanisms already defined for DLNA link protection and DLNA DRM interoperability solutions.

## 2 Normative references

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

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

IETF RFC 2616, *Hypertext Transfer Protocol*,
http://www.ietf.org/rfc/rfc2616.txt

IETF RFC 2818, *HTTP over TLS, Informational*,
http://tools.ietf.org/html/rfc2818

IETF RFC 4680, *TLS Handshake Message for Supplemental Data*,
http://tools.ietf.org/html/rfc4680

IETF RFC 5246, *Transport Layer Security (TLS) Protocol*,
http://tools.ietf.org/html/rfc5246

IETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*,
http://tools.ietf.org/html/rfc5280

IETF RFC 5878, *Transport Layer Security (TLS) Authorization Extensions*,
http://tools.ietf.org/html/rfc5878

IETF RFC 7562, *Authentication Credential Exchange Using TLS Supplemental Data*,
https://tools.ietf.org/html/rfc7562

DTCP Volume 1 (informational version), *Digital Transmission Content Protection Specification Volume 1, Revision 1.7*.
http://www.dtcp.com/documents/dtcp/info-20111214-dtcp-v1-rev-1-p-7.pdf

# 3 Terms, definitions and conventions

For the purposes of this document, the terms and definitions given in IEC 62481-1-1:2017 and the following apply.

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

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

## 3.1 General terms

**3.1.1**
**Authentication Client**
set of device functions that, as part of the Client Authentication Device Option, provides the protocols to allow a client to be authenticated and the protocols to authenticate an Authentication Server by verifying the server credentials

**3.1.2**
**Authentication Server**
Device Function that, as part of the Server Authentication Device Option, provides the protocols to allow a server to be authenticated and the protocols to authenticate an Authentication Client by verifying the client credentials

**3.1.3**
**Client Authentication**
process or action where the Authentication Client initiates the authentication request for the Authentication Server to authenticate the Client

**3.1.4**
**DTCP Method**
process that occurs when a device uses a device certificate for itself during DLNA Authentication

**3.1.5**
**Server Authentication**
process or action where the Authentication Server is authenticated by the Authentication Client

**3.1.6**
**X.509 Method**
process that occurs when a device uses an X.509 credential for itself during DLNA Authentication

Note 1 to entry: No DTCP device certificate is used with this method.

## 3.2 Conventions

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

# 4 Networking architecture and guideline conventions

## 4.1 DLNA home networking architecture

This document extends the DLNA home networking architecture that is defined in Clause 4 of IEC 62481-1-1:2017.

## 4.2 Document conventions

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

## 4.3 Guideline structure

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

# 5 DLNA Device Model

## 5.1 General

Refer to Clause 5, IEC 62481-1-1:2017 for detailed descriptions of existing DLNA Home Networking Architecture Device Model. This document extends the existing DLNA system usages.

## 5.2 Authentication Device Functions

The architecture consists of system elements in the home and outside the home used to implement the DLNA authentication feature. These elements support both service provider and home owner use cases. Figure 1 is an overview of the architecture.

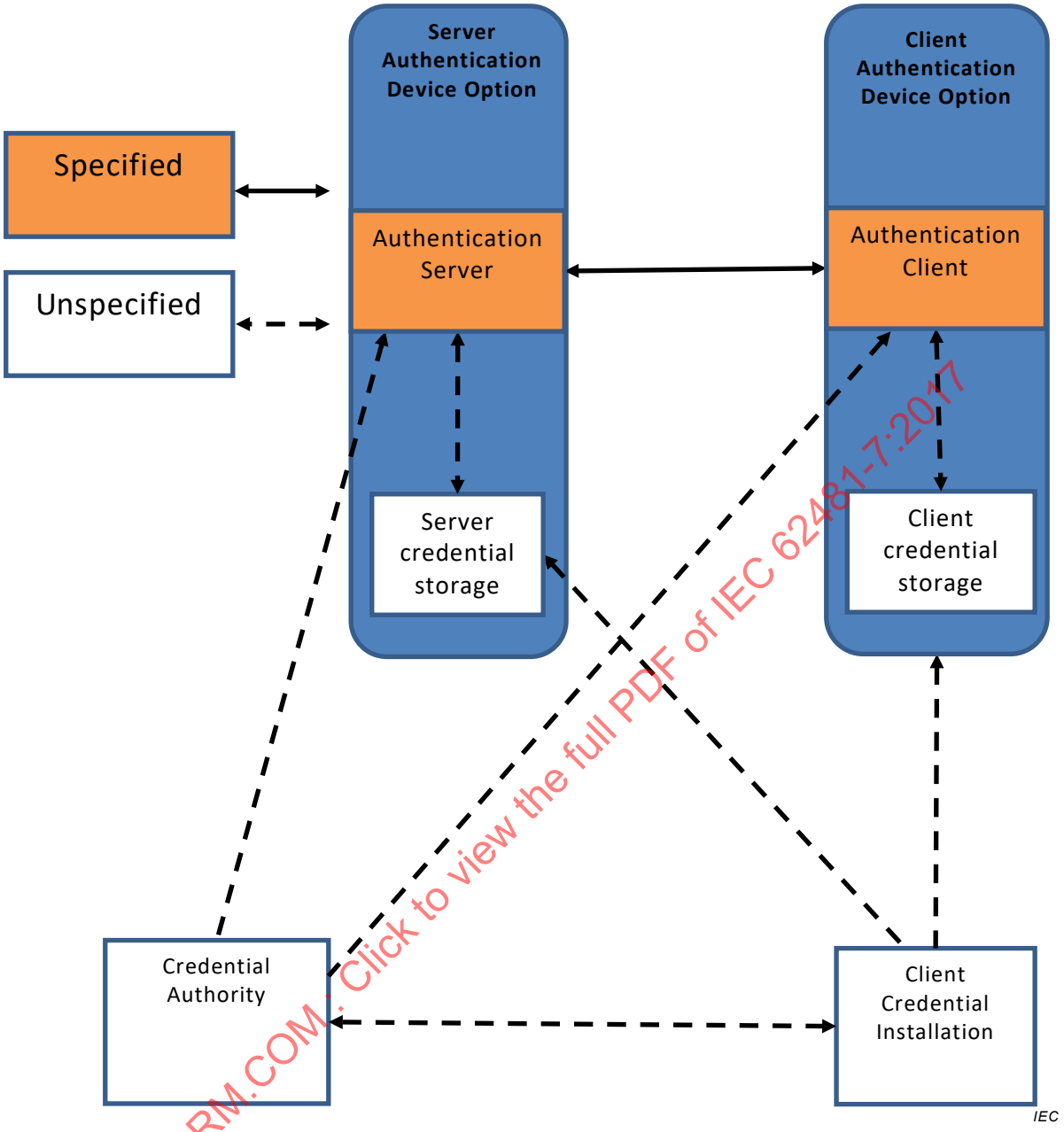



**Figure 1 – Authentication functions**



The architecture defines the following functions.

– Credential Authority: creates client and server credentials for use by manufacturers in their devices. Provides root certificate(s) to the Authentication Server and the Authentication Client. Defines the robustness requirements.

– Client Credential Installation: installs the credentials into the client device. Performed by the manufacturer.

– Client Credential Storage: stores the credentials according to the robustness requirements. Provides access to the credentials by the Authentication Server.

– Server Credential Storage: stores the credentials according to the robustness requirements. Provides access to the credentials by the Authentication Server.

– Authentication Client: authenticates with the Authentication Server and authenticates servers using the server credentials.

– Authentication Server: authenticates with the Authentication Client and authenticates clients using the client credentials.

The DLNA guidelines will cover interoperability between the Authentication Client Function and the Authentication Server Function.

### 5.3 Device Options

For the Authentication interoperability guidelines and system usages, the following Device Options are defined.

– Client Authentication: a Device Option that consists of an Authentication Client Function and client credentials.

– Server Authentication: a Device Option that consists of an Authentication Server Function and server credentials.

### 5.4 System usages

DLNA Authentication guidelines are designed to complement all DLNA Device Classes and Device Capabilities in all system usages, providing and enabling them the ability to authenticate each other securely before other functions, such as content transports, can be performed. Other than adding the authentication processes as described in 3.1.3 and 3.1.5, all DLNA system usages stay the same.

While some of the implementations of DLNA system usages require device authentication, many do not. As such, DLNA Authentication guidelines are optional (also known as Device Options) and it is an implementer's choice to implement them.

Although an Authentication Server or an Authentication Client may be implemented as an independent entity that performs authentication only without any other function, this type of implementation does not make sense because there is no purpose to authenticate it. Therefore, the authentication services are designed as Device Options that shall be a part of a Device Class or Device Capability when implemented.

### 5.5 Theory of operation

The enclosed guidelines enable the ability for a server to authenticate a client as a DLNA certified device using either X.509 credentials or device certificates. Conversely, the ability for a client to authenticate a server is also supported. The TLS protocol using the SupplementalData payload mechanism is defined herein to support both client and server authentication using DTCP certificates.

The authentication scenarios covered are as follows.

1. Server uses trusted X.509 and client uses trusted X.509.
2. Server uses trusted X.509 and client uses DTCP.
3. Server uses (trusted or self-signed X.509) + DTCP, and client uses trusted X.509.
4. Server uses (trusted or self-signed X.509) + DTCP, and client uses DTCP.

The first scenario is supported by a standard TLS protocol. The rest of the scenarios require use of SupplementalData extensions to the TLS protocol. Scenario #3 is highly unlikely to occur in practice due to the typical nature of a TLS handshake. A TLS handshake is triggered by a TLS client sending a ClientHello message and if the TLS client does not indicate support for the DTCP method, a TLS server will not be allowed to send the DTCP certificate. So a TLS client is required to have a priori knowledge that a particular TLS server is using a DTCP certificate.

# 6 Guideline requirements

## 6.1 Device discovery and control

### 6.1.1 Authentication Server discovery

#### 6.1.1.1

**[GUIDELINE]** A DLNA Device Class or Device Capability that indicates support for the Server Authentication Device Option shall implement the requirements specified for Authentication Server.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMS, DMR, XDMR, +RUIHSRC+ | M-DMS | n/a | n/a | W3UP4 | |

**[COMMENT]** Support for Server Authentication Device Option is indicated at the time of registration for certification.

#### 6.1.1.2

**[GUIDELINE]** A DLNA Device Class or Device Capability that implements the Authentication Server shall have the capID value of "authentication-server" for the dlnacap-value in the <dlna:X_DLNACAP> element, as defined in IEC 62481-1-1:2017, of the Device Description document.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMS, DMR, XDMR, +RUIHSRC+ | M-DMS | n/a | IEC 62481-1-1:2017 | GX4I8 | |

**[COMMENT]** This is where a UPnP control point checks if the DLNA Device Class or Device Capability implemented the Authentication Server after retrieving the Device Description document of the UPnP Device.

### 6.1.2 Authentication Client discovery

**[GUIDELINE]** A DLNA Device Class or Device Capability that indicates support for the Client Authentication Device Option shall implement the requirements specified for Authentication Client.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | n/a | ENEWV | |

**[COMMENT]** Support for Client Authentication Device Option is indicated at the time of registration for certification.

## 6.2 Authentication guidelines

### 6.2.1 Authentication Server protocols

#### 6.2.1.1

**[GUIDELINE]** The Authentication Server shall implement the HTTP 1.1 Server.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMS, DMR, XDMR, +RUIHSRC+ | M-DMS | n/a | IETF RFC 2616 | 7LRZP | |

**[COMMENT]** The Device Class or Device Capability that implements the Authentication Server could already have the HTTP 1.1 Server implemented. This guideline establishes the basis for interoperability; however, other protocols could also be used.

#### 6.2.1.2

**[GUIDELINE]** The Authentication Server shall implement HTTPS (HTTP over TLS).

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMS, DMR, XDMR, +RUIHSRC+ | M-DMS | n/a | IETF RFC 2818 | ABKQG | |

**[COMMENT]** The Device Class or Device Capability that implements the Authentication Server could already have HTTPS implemented. This guideline establishes the basis for interoperability however other protocols could also be used.

#### 6.2.1.3

**[GUIDELINE]** The Authentication Server shall implement the TLS 1.2 protocol as defined in IETF RFC 5246.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMS, DMR, XDMR, +RUIHSRC+ | M-DMS | n/a | IETF RFC 5246 | WM9P4 | |

#### 6.2.1.4

**[GUIDELINE]** The Authentication Server shall implement the TLS SupplementalData handshake message as defined in IETF RFC 4680.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMS, DMR, XDMR, +RUIHSRC+ | M-DMS | n/a | IETF RFC 4680 | JY8N9 | |

**6.2.1.5**

**[GUIDELINE]** The Authentication Server shall implement the client_authz and server_authz TLS Hello message extensions as defined in IETF RFC 5878

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMS, DMR, XDMR, +RUIHSRC+ | M-DMS | n/a | IETF RFC 5878 | 7TRPH | |

**[COMMENT]** When a server uses the TLS SupplementalData message to send its credentials, it shall do so by indicating support for these extensions in the Hello message.

### 6.2.2 Authentication Client protocols

**6.2.2.1**

**[GUIDELINE]** The Authentication Client shall implement the HTTP 1.1 Client.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | IETF RFC 2616 | ME837 | |

**[COMMENT]** The Device Class or Device Capability that implements the Authentication Client could already have the HTTP 1.1 Client implemented. This guideline establishes the basis for interoperability; however, other protocols could also be used.

**6.2.2.2**

**[GUIDELINE]** The Authentication Client shall implement HTTPS (HTTP over TLS).

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | IETF RFC 2818 | 8USPH | |

**[COMMENT]** The Device Class or Device Capability that implements the Authentication Client could already have HTTPS implemented. This guideline establishes the basis for interoperability; however, other protocols could also be used.

**6.2.2.3**

**[GUIDELINE]** The Authentication Client shall implement the TLS 1.2 protocol as defined in IETF RFC 5246.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | IETF RFC 5246 | BC6YY | |

**6.2.2.4**

**[GUIDELINE]** An Authentication Client that implements the DTCP Method shall implement the TLS SupplementalData handshake message as defined in IETF RFC 4680.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | IETF RFC 4680 | GM2LB | |

**6.2.2.5**

**[GUIDELINE]** An Authentication Client that implements the DTCP Method shall implement the client_authz and server_authz TLS Hello message extensions as defined in IETF RFC 5878

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | IETF RFC 5878 | TCEMN | |

**[COMMENT]** When a client uses the TLS SupplementalData message to send its credentials, it will do so by indicating support for these extensions in the Hello message.

### 6.2.3 Client Authentication guidelines

**6.2.3.1**

**[GENERAL]** 6.2.3 defines all functionality required for performing Client Authentication.

**6.2.3.2**

**[GUIDELINE]** An Authentication Client shall implement one of the following authentication methods for client authentication:

– X.509 Method as defined in 6.2.3.3;

– DTCP Method as defined in 6.2.3.5 and 6.2.3.6.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | n/a | AQ7AC | |

**[COMMENT]** Authentication occurs via one of 2 separate credential mechanisms.

**6.2.3.3**

**[GUIDELINE]** If an Authentication Client implements the X.509 Method as defined in IETF RFC 5280 for Client Authentication, then it shall support TLS 1.2 for Client Authentication as defined in IETF RFC 5246.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | IETF RFC 5246<br>IETF RFC 5280 | LWI79 | |

**6.2.3.4**

**[GUIDELINE]** If an Authentication Client implements the DTCP Method, then it shall implement all client requirements defined in IETF RFC 7562 including generating, processing and error handling of SupplementalData messages.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR,, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | IETF RFC 7562 | 52ZEM | |

#### 6.2.3.5

**[GUIDELINE]** If an Authentication Client implements the DTCP Method, then it shall use the TLS SupplementalData Double Handshake as defined in IETF RFC 7562.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | IETF RFC 7562 | L8SLI | |

#### 6.2.3.6

**[GUIDELINE]** If an Authentication Client implements the DTCP Method, then it shall generate the SupplementalData message as defined in IETF RFC 7562 that includes the device certificate as defined in DTCP Volume 1.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMC, DMP, XDMR, +PU+, +RUIHPL+ | M-DMP M-DMC | n/a | IETF RFC 7562 DTCP Volume 1 | QA9QL | |

**[COMMENT]** The device certificate will include sufficient information that authenticates the client.

#### 6.2.3.7

**[GUIDELINE]** An Authentication Server shall implement the DTCP Method as defined in 0 for Client Authentication.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMS, DMR, XDMR, +RUIHSRC+ | M-DMS | n/a | IETF RFC 5246 | R9BVI | |

#### 6.2.3.8

**[GUIDELINE]** An Authentication Server shall implement the X.509 Method as defined in 6.2.3.3 for Client Authentication.

**[ATTRIBUTES]**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| M | A | DMS, DMR, XDMR, +RUIHSRC+ | M-DMS | n/a | IETF RFC 5246 | V224M | |

### 6.2.4 Server Authentication guidelines

#### 6.2.4.1

**[GENERAL]** This clause defines all functionality required for performing server authentication.