



IEC 62766-7

Edition 1.0 2017-07

INTERNATIONAL STANDARD



**Consumer terminal function for access to IPTV and open internet
multimedia services –
Part 7: Authentication, content protection and service protection**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 33.170 35.240.95

ISBN 978-2-8322-4555-2

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	9
2 Normative references	9
3 Terms, definitions and abbreviated terms	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms.....	13
4 Content and service protection	15
4.1 General.....	15
4.2 Terminal-centric approach	15
4.2.1 General	15
4.2.2 Interfaces for CSP and CSP-T server	16
4.2.3 Protected content usages	25
4.2.4 Content encryption	28
4.2.5 Protected file formats.....	29
4.2.6 Protection of MPEG-2 transport streams.....	30
4.2.7 Operation of Marlin technologies	34
4.2.8 DRM data	35
4.3 Gateway-centric approach	39
4.3.1 General	39
4.3.2 Capabilities.....	39
4.3.3 CSPG-DAE interface	39
4.3.4 CI+ based gateway	40
4.3.5 DTCP-IP based gateway.....	55
5 User identification, authentication, authorisation and service access protection.....	60
5.1 General principles.....	60
5.2 Interfaces.....	61
5.2.1 General	61
5.2.2 HNI-INI	61
5.2.3 HNI-IGI.....	62
5.2.4 Common requirements.....	62
5.3 Service access protection	62
5.3.1 SAA co-located with service	62
5.3.2 SAA standalone	63
5.4 OITF authentication mechanisms	64
5.4.1 HTTP basic and digest authentication.....	64
5.4.2 Network-based authentication.....	65
5.4.3 Web-based authentication	65
5.4.4 HTTP digest authentication – Using IMS gateway	67
5.4.5 GBA authentication – Using IMS gateway	72
5.5 IMS registration – OITF.....	75
5.5.1 General	75
5.5.2 Relevant functional entities and reference points	75
5.5.3 Prerequisites	76
5.5.4 SIP digest message flows.....	77
5.5.5 IMS AKA message flows.....	78

5.6	Session management and single sign on	80
5.6.1	General	80
5.6.2	Cookie session	80
5.6.3	URL parameters	81
5.6.4	HTTP authentication session	82
5.6.5	SAML Web-based SSO.....	83
6	Forced play-out using media zones	84
Annex A (informative)	Link of user authentication and DRM device authentication	86
Annex B (normative)	XML schemas	88
B.1	General.....	88
B.2	XML schema for MarlinPrivateDataType structure	88
B.3	XML schema for MIPPVControlMessage format	89
B.4	XML schema for HexBinaryPrivateDataType structure	89
Annex C (informative)	DRM messages used in DAE.....	90
Annex D (informative)	CSPG-CI+ usage examples.....	91
D.1	General.....	91
D.2	CSPG-CI+ initial power-on	91
D.3	CSPG-CI+ normal power-on.....	91
D.4	Live session example.....	92
D.5	Parental control management example	93
D.6	No-rights event and purchase example	94
D.7	VoD session example	95
Annex E (informative)	CSPG-DTCP session setup sequence examples	96
E.1	General.....	96
E.2	Multicast streaming with SIP session management	96
E.3	Unicast streaming with SIP session management	98
E.4	Unicast streaming with RTSP session management.....	99
E.5	HTTP streaming and download	100
Annex F (informative)	Embedded CSPG	101
F.1	General.....	101
F.2	Application to simple and secure streaming	103
Bibliography	105
Figure 1	– CSP-T system overview	16
Figure 2	– Node acquisition sequence	18
Figure 3	– Link acquisition sequence	20
Figure 4	– Deregistration sequence	22
Figure 5	– Licence acquisition sequence.....	24
Figure 6	– Licence evaluation sequence	26
Figure 7	– Scramble key decryption sequence	27
Figure 8	– Content on demand encryption sequence using content key (for (P)DCF OMArIn or Marlin IPMP Marlin FF)	28
Figure 9	– Content on demand encryption sequence using content key (for MPEG-2 TS) 28	
Figure 10	– Scheduled content encryption sequence using scramble key (for MPEG-2 TS) 29	
Figure 11	– Conditional access descriptors signalling ECM and EMM messages	30

Figure 12 – Outline of DRMControllInformationtype with MarlinPrivateData	37
Figure 13 – Outline of MIPPVControlMessage	38
Figure 14 – CSPG-CI+ overview	40
Figure 15 – CSPG-CI+ context.....	41
Figure 16 – CSPG-DTCP overview	56
Figure 17 – Overview of involved reference points	56
Figure 18 – General message flow for service access protection and user authentication	60
Figure 19 – SAA co-located with requested service.....	63
Figure 20 – Standalone SAA, redirection mode	63
Figure 21 – HTTP basic and digest authentication	64
Figure 22 – Network-based authentication	65
Figure 23 – Web-based authentication with form.....	66
Figure 24 – Initial procedure	68
Figure 25 – Authentication between an OITF and an SAA based on HTTP credentials stored in IG.....	69
Figure 26 – Authentication between an OITF and an SAA based on GBA credentials.....	71
Figure 27 – Initial GBA registration	73
Figure 28 – Authentication between an OITF and an SAA based on GBA keys	74
Figure 29 – OIPF functional entities and reference points involved in IMS registration	76
Figure 30 – SIP digest message flow interlaced into IMS registration.....	77
Figure 31 – User identification and authentication based on the IMS AKA procedure	79
Figure 32 – Session management using cookie.....	81
Figure 33 – Session management using URL parameters	82
Figure 34 – HTTP authentication session.....	83
Figure 35 – SAML Web-based SSO	84
Figure A.1 – User authentication for CSP, CSP-T server communication	86
Figure D.1 – CSPG-CI+ first power-on	91
Figure D.2 – CSPG-CI+ normal power-on	92
Figure D.3 – CSPG-CI+ live session example	92
Figure D.4 – Parental control management example	93
Figure D.5 – No-rights event and purchase example	94
Figure D.6 – VoD session example	95
Figure E.1 – Session setup sequence for multicast streaming with SIP session management.....	97
Figure E.2 – CSPG-DTCP initiated teardown sequence for multicast streaming with SIP session management	98
Figure E.3 – Session setup sequence for unicast streaming with SIP session management.....	99
Figure E.4 – Session setup sequence for unicast streaming with RTSP session management.....	100
Figure E.5 – Session setup sequence for HTTP streaming and download	100
Figure F.1 – Possible CSPG deployments.....	101
Figure F.2 – CSPG embedded in the same device as OITF.....	102
Figure F.3 – Simple and secure streaming with CSPG	103

Table 1 – Recording Control access_criteria_descriptor	32
Table 2 – Bit assignments of recording_control_information_byte	32
Table 3 – DNR and DNTS combinations.....	32
Table 4 – Parental_Control_URL parameter syntax.....	33
Table 5 – DRMControlInformation mapping for Marlin	35
Table 6 – DRMControlInformation mapping for Marlin simple secure streaming	36
Table 7 – MarlinPrivateData structure	37
Table 8 – MIPPVControlMessage format.....	39
Table 9 – OIPF private_host_application_ID	42
Table 10 – SAS_async_msg() APDU syntax	42
Table 11 – Generic message_byte() syntax	42
Table 12 – OIPF specific messages and command_id values.....	43
Table 13 – OIPF specific datatype_id values.....	43
Table 14 – Mapping to DAE API or events	44
Table 15 – send_msg message data types.....	45
Table 16 – reply_msg message data types	45
Table 17 – resultCode and oipf_status mapping.....	46
Table 18 – parental_control_info message data types.....	47
Table 19 – oipf_access_status field and blocked attribute mapping.....	48
Table 20 – rights_info message data types	48
Table 21 – oipf_access_status field and errorStatte attribute mapping.....	49
Table 22 – system_info message data types	49
Table 23 – can_play_content_req message data types	50
Table 24 – can_play_content_reply message data types.....	50
Table 25 – can_record_content_req message data types.....	51
Table 26 – can_record_content_reply message data types	51
Table 27 – Scrambling modes.....	53
Table 28 – DRMControlInformation mapping for CSPG-CI+	54
Table 29 – HexBinaryPrivateData structure.....	55
Table 30 – CA_descriptor	58
Table C.1 – DRM messages used in the DAE	90

INTERNATIONAL ELECTROTECHNICAL COMMISSION

CONSUMER TERMINAL FUNCTION FOR ACCESS TO IPTV AND OPEN INTERNET MULTIMEDIA SERVICES –

Part 7: Authentication, content protection and service 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 62766 has been prepared by IEC technical committee 100: Audio, video and multimedia systems and equipment.

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

CDV	Report on voting
100/2551/CDV	100/2665/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.

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

A list of all parts in the IEC 62766 series, published under the general title *Consumer terminal function for access to IPTV and open Internet multimedia services*, 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.

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

The IEC 62766 series is based on a series of specifications that was originally developed by the OPEN IPTV FORUM (OIPF). They specify the user-to-network interface (UNI) for consumer terminals to access IPTV and open internet multimedia services over managed or non-managed networks as defined by OIPF.

CONSUMER TERMINAL FUNCTION FOR ACCESS TO IPTV AND OPEN INTERNET MULTIMEDIA SERVICES –

Part 7: Authentication, content protection and service protection

1 Scope

This part of IEC 62766 specifies functions for content protection, service protection, service access protection, user identification, user authentication, and user authorisation.

The following clauses contain features for which the criteria that determine under which circumstances these features are implemented are out of the scope of the present document or contain conditional normative statements referring to other parts of IEC 62766:

- 4.2 Terminal-centric approach
- 4.2.5 Protected file formats
- 4.2.6 Protection of MPEG-2 transport streams
- 4.3.4 CI+ based gateway
- 4.3.4.7 Protected streaming and file formats
- 4.3.4.8 Personal video recorder
- 4.3.4.9 Time shifting
- 4.3.5 DTCP-IP based gateway
- 4.3.5.6 Protected streaming and file formats
- 5.4.4 HTTP digest authentication using IMS gateway
- 5.4.5 GBA authentication using IMS gateway

NOTE GBA authentication can be achieved using either the mechanism in 5.4.5 GBA authentication using IMS gateway or the, more general, mechanism in 5.4.4 HTTP digest authentication using IMS gateway. 5.4.4 allows the use of different authentication mechanisms in a way that is transparent to the OITF, including possible future authentication mechanisms, and should preferably be used. It is expected that 5.4.5 GBA authentication using IMS gateway will be deprecated and removed in future versions of this specification.

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 62455:2010, *Internet protocol (IP) and transport stream (TS) based service access*

IEC 62766-1:2017, *Consumer terminal function for access to IPTV and open Internet multimedia services – Part 1: General*

IEC 62766-2-1:2016, *Consumer terminal function for access to IPTV and open Internet multimedia services – Part 2-1: Media Formats*

IEC 62766-3:2016, *Consumer terminal function for access to IPTV and open Internet multimedia services – Part 3: Content Metadata*

IEC 62766-4-1:2017, *Consumer terminal function for access to IPTV and open Internet multimedia services – Part 4-1: Protocols*

IEC 62766-5-1:2017, *Consumer terminal function for access to IPTV and open Internet multimedia services – Part 5-1: Declarative Application Environment*

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

3GPP TS 24.109, *Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details*

3GPP TS 24.229, *IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 (Release 8)*

3GPP TS 33.203, *Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services (Release 8)*

3GPP TS 33.220, *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*

ATIS-0800006, *IIF Default Scrambling Algorithm (IDSA)*

Consumer Electronics Association CEA-2014-A (including the August 2008 Errata), *Web-based Protocol Framework for Remote User Interface on UPnP Networks and the Internet (Web4CE)*

CI Plus LLP, *CI Plus Specification V1.3 (2011-01), Content Security Extensions to the Common Interface*, available from:
http://www.CIPlus.com/data/CIPlus_specification_V1.3.1.pdf

DTLA, *DTCP Adopter Agreement, Digital Transmission Protection License Agreement*, available from:
<http://www.dtcp.com/agreements.aspx>

ETSI ETR 289, *Digital Video Broadcasting (DVB); Support for the use of scrambling and Conditional Access (CA) within digital broadcasting systems*

ETSI EN 50221, *Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications*

ETSI TS 101 699 V1.1.1, *Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification*

ETSI TS 103 197 V1.5.1, *Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt*

ETSI EN 300 468 V1.13.1, *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems*

ETSI TS 102 770 V1.1.1, *Digital Video Broadcasting (DVB); System Renewability Messages (SRM) in DVB Systems*

Marlin Developer Community, *Marlin Broadband Transport Stream Specification (BBTS), Version 1.0*, available from:
<http://www.marlin-community.com/develop/downloads>

Marlin Developer Community, *Marlin – Broadband Network Service Profile Specification (BNSP), Version 1.1*, available from:
<http://www.marlin-community.com/develop/downloads>

Marlin Developer Community, *Marlin – File Formats Specification (FF), Version 1.1*, available from: <http://www.marlin-community.com/develop/downloads>

Marlin Developer Community, *Marlin – Simple Secure Streaming Specification (MS3), Version 1.1.1*, available from:
<http://www.marlin-community.com/develop/downloads>

Marlin Developer Community, *OMArLin Specification, Version 1.0*, available from:
<http://www.marlin-community.com/develop/downloads>

IETF RFC 2109, *HTTP State Management Mechanism*

IETF RFC 2617, *HTTP Authentication: Basic and Digest Access Authentication*

IETF RFC 5746, *Transport Layer Security (TLS) Renegotiation Indication Extension*

OASIS, *Assertions and Protocols for the OASIS Security Markup Language (SAML) V2.0*, available from:
<https://www.oasis-open.org/standards#samlv2.0>

OASIS, *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*, available from:
<https://www.oasis-open.org/standards#samlv2.0>