BS IEC 62766-7:2017

BSI Standards Publication

Consumer terminal function for access to IPTV and open internet multimedia services

Part 7: Authentication, content protection and service protection

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

National foreword

This British Standard is the UK implementation of IEC 62766-7:2017.

The UK participation in its preparation was entrusted to Technical Committee EPL/100, Audio, video and multimedia systems and equipment.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 88964 6

ICS 35.240.95; 33.170

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 28 February 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

IEC 62766-7

Edition 1.0 2017-07

INTERNATIONAL STANDARD

colour inside

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.

® Registered trademark of the International Electrotechnical Commission

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

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

AVA Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

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 OMArlin 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

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

Figure 12 – Outline of DRMControlInformationtype 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

AVA Documents
Document Sharing Hub

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

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

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.

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

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.

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

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.

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

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*

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

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 Assoviation 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.CI Plus.com/data/CI Plus_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

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62766-1 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

3.1.1
business token
collection of information defined in BNSP that contains the service-specific information for a given business model

3.1.2
content and service protection gateway
optional gateway function that provides a conversion from a (proprietary) content and service protection solution in the network to one that is supported by an OITF, as defined in IEC 62766-7

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

3.1.3
content and service protection gateway
optional gateway function that provides a conversion from a (proprietary) content and service protection solution in the network to one that is supported by an OITF, as defined in this document

3.1.4
client function
function that interacts with the Marlin client function in a content and service protection

3.1.5
content and service key management function
entity responsible for storing and providing service, programme, content keys and ECM attached information

Note 1 to entry: This function may be physically co-located with other functions (e.g. the content delivery network controller for content on demand services), see Annex B of IEC 62766-1:2017.

Note 2 to entry: This entity has been identified to illustrate informatively the separation between content encryption, which is part of content preparation, and content delivery.

3.1.6
content on demand encryption management function
back office content on demand function in charge of launching content on demand encryption

Note 1 to entry: This entity has been identified to illustrate informatively the separation between content encryption, which is part of content preparation, and content delivery.

3.1.7
content and service protection
function that handles service protection and content protection for the client in the OITF

3.1.8
CSP-G server
functional entity in the network that handles content protection and service protection for the content and service protection gateway (CSPG) in the residential network

3.1.9
CSP-T server
functional entity in the network that handles service protection and content protection for the CSP-T client in the OITF

3.1.10
Marlin action token
token defined either in BNSP or in Marlin MS3 that is used to trigger the Marlin protocols from the Marlin client function in CSP, and from which some information (e.g., business token) is used in the Marlin protocols

Note 1 to entry: The mimeType attribute is used to qualify which Marlin token type is returned

3.1.11
Marlin client function
compliant implementation of the Marlin client that is defined in BNSP and that enables secure communications (Marlin Protocols) with the Marlin server function in a CSP-T server

3.1.12
Marlin configuration token
token defined in BNSP that includes the location information of the Marlin server function in CSP-T server with which the CSP communicates

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

3.1.13
Marlin server function
compliant implementation of the Marlin server that is defined in BNSP and that enables secure communications (Marlin protocols) with the Marlin client function in a CSP

3.1.14
output control information
output control information as defined in BNSP and BBTS

3.1.15
programme key
symmetric key defined in IEC 62455 that encrypts an ECM

3.1.16
scramble key
symmetric key that is used to scramble the content

3.1.17
server function
function that interacts with the Marlin server function in a CSP-T server

3.1.18
serviceBaseCID
part of the content ID that is the same for all content in a service

3.1.19
service key
symmetric key defined in IEC 62455 that is used to encrypt an ECM or a programme key

3.1.20
single sign on
method of service access control that enables the user to authenticate once and gain access to the resources of multiple services

3.2 Abbreviated terms

3GPP	Third Generation Partnership Project
AES	Advanced Encryption Standard
AKE	Authentication and Key Exchange
APDU	Application Protocol Data Unit
ATIS	Alliance for Telecommunications Industry Solutions
BBTS	Broadband Transport Stream – MPEG-2 transport stream as defined by BBTS
BNS	Broadband Network Service
BSF	Bootstrapping Server Function
bslbf	bit string, left bit first
B-TID	Bootstrapping Transaction Identifier
CA	Conditional Access
CAD	Content Access Descriptor
CAM	Conditional Access Module
CAT	Conditional Access Table
CBC	Cipher-Block Chaining
CE-HTML	Consumer Electronics – HTML

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

CI	Common Interface
CSKMF	Content and Service Key Management Function
CSPG	Content and Service Protection Gateway
CSPG-CI+	CSPG based on CI+
CSPG-DTCP	CSPG based on DTCP-IP
CSP-T	Content and Service Protection – terminal-centric Approach
DCF	DRM Content Format
DMZ	Dynamic Media Zones
DNR	Do Not Record
DNTS	Do Not Time Shift
DTCP	Digital Transmission Content Protection
DTLA	Digital Transmission Licensing Administrator
DVB	Digital Video Broadcasting
ECM	Entitlement Control Message
EMM	Entitlement Management Message
ETSI	European Telecommunications Standards Institute
FF	File Format
FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
HDCP	High-bandwidth Digital Content Protection
HDD	Hard Disk Drive
HNI-AMNI	Home Network Interface – Additional Managed Network Interface
HNI-CSP	Home Network Interface – Content and Service Protection
HNI-IGI	Home Network Interface – IMS Gateway Interface
HNI-INI	Home Network Interface – ITF (IPTV Terminal Function) Network Interface
ID	Identity
IDSA	IIF Default Scrambling Algorithm
IETF	Internet Engineering Task Force
IIF	IPTV Interoperability Forum
IPMC	IP Multicast
IPMP	Intellectual Property Management Protocol
IV	Initialization Vector
KDF	Key Derivation Function
KSM	Key Stream Message
M-CID	Marlin Content ID
MIME	Multipurpose Internet Mail Extensions
MP4	MPEG-4
MPEG	Moving Pictures Experts Group
MS3	Marlin Simple Secure Streaming
NAF	Network Application Function
NPI	Network Provider Interface
OASIS	Organization for the Advancement of Structured Information Standards
PCMCIA	Personal Computer Memory Card International Association

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

PCP	Protected Content Packet
PDCF	Packetized DRM Content Format
PES	Packetized Elementary Stream
PID	Packet Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PMT	Programme Map Table
SAML	Security Assertion Markup Language
SAS	Specific Application Support
SRM	System Renewability Message
TEK	Traffic Encryption Key
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TLS	Transport Layer Security
TLV	Type Length Value
TS	Transport Stream
uimsbf	unsigned integer most significant bit first
UNIS-CSP-G	User Network Interface Specific – Content and Service Protection Gateway
UPnP	Universal Plug and Play
URI	Usage Rules Information

4 Content and service protection

4.1 General

This clause specifies the content and service protection (CSP) functionality. It consists of a specification of:

- the terminal-centric approach, see 4.2, and
- the gateway-Centric approach, see 4.3.

4.2 Terminal-centric approach

4.2.1 General

Subclause 4.2 specifies the functionality for the terminal-centric approach to content and service protection. In order to do this, a mapping is provided from all relevant functions and interfaces from Annex B of IEC 62766-1 to specific clauses of Marlin specifications BNSP and Marlin MS3. The Marlin Core System Specification provides a specification for the parts of Marlin DRM that are common for all Marlin delivery system specifications.

All normative statements in 4.2 apply only in case the terminal-centric approach is supported by the OITF.

OITFs that support the OIPF terminal-centric approach to content and service protection shall be compliant with BNSP and may be compliant with Marlin MS3.

NOTE 1 The criteria that determine under which circumstances the terminal-centric approach is implemented are out of the scope of the present document.

NOTE 2 The criteria that determine under which circumstances the support for Marlin metering for content or rights owner settlement is implemented in the OITF are out of the scope of the present document.

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

4.2.2 Interfaces for CSP and CSP-T server

4.2.2.1 General

Subclause 4.2.2 describes the interfaces related to a CSP and CSP-T Server in the functional architecture described in Annex B of IEC 62766-1:2017.

4.2.2.2 Overview

The main purpose of 4.2.2 is to describe CSP interfaces (CSP-1, UNIS-CSP-T) and CSP-T Server interfaces (NPI-CSPTx, x = 1, 2, 3). CSP-1 is the interface between CSP and OITF functions. NPI-CSPTx, x = 1, 2, 3, are the interfaces between the CSP-T server and providers network functions. Subclause 4.2.2 informatively touches upon the Marlin licence evaluation and content encryption.

Only the UNIS-CSP-T interface and the interface to DAE in CSP-1 are normative. The other interfaces are informatively described for comprehension. Figure 1 shows the message flow overview.

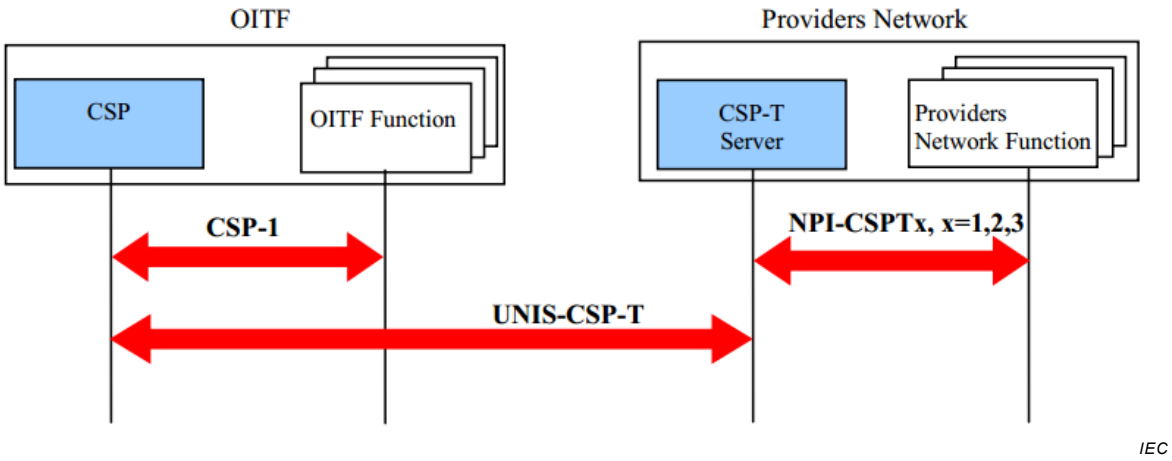

Figure 1 – CSP-T system overview

The four functional entities in Figure 1 are described below.

- CSP in this document consists of Marlin client function and a part of the client function that deals with Marlin elements.
- CSP-T server in this document consists of Marlin server function and a part of the server function that deals with Marlin elements.
- OITF function is the function in the OITF that interacts with the CSP. The OITF function also interacts with a providers network function to acquire the necessary information for the CSP. How the providers network function is called in this document depends on the process to be performed.
- Providers network function is the function in the providers network that interacts with the CSP-T server. How the providers network function is called in this document depends on the process to be performed.

NOTE The OITF function with which the CSP communicates is not limited as described in this document and may vary depending on the implementation of the OITF.

4.2.2.3 Interface CSP – CSP-T server (UNIS-CSP-T)

When requested from a native application or from the DAE application to handle a Marlin action token or a MIPPVControlMessage (see 4.2.8.3), the CSP shall act as a Marlin DRM client and shall perform Marlin protocols as specified in BNSP or Marlin MS3 as applicable. Furthermore, in the context of BNSP, if there are no available rights when trying to use

AVA Documents Document Sharing Hub

content, the CSP shall comply with BBTS and OMArlin and shall try to use the URL specified in the content to acquire new rights.

In both cases, the CSP-T server shall comply with Marlin protocols as specified in BNSP.

These protocols are:

- Marlin registration: node acquisition and link acquisition;
- Marlin de-registration;
- Marlin licence acquisition.

If Marlin simple secure streaming feature is supported, the CSP-T server may comply with MS3 protocols as specified in Marlin MS3:

- MS3 protocol.

Marlin protocols are described in 4.2.2.5.

4.2.2.4 Interface CSP – OITF function (CSP-1)

The DAE DRM agent API, as defined in 7.6.2 of IEC 62766-5-1:2017, triggers the handling of a DRM message, for example a Marlin action token, MIPPVControlMessage or Marlin licence. When the sendDRMMessage API is called for a DRMSystemID set to the value defined for Marlin, OITF shall forward the DRM message to the CSP function. The result of calling sendDRMMessage is notified through the onDRMMessageResult event handler.

Typical DRM events shall be triggered by CSP to DAE via A/V or video/broadcast object when content cannot be played, recorded or time shifted, due to a lack of rights (no licence, invalid licence) or parental control locking. These events are defined in 7.13.6 and 7.14.7 of IEC 62766-5-1:2017. The DRMSystemID of these events shall be set to the value defined for Marlin.

A DAE application or native application may use DRMControlInformation, defined as an extension to purchaseItem in IEC 62766-3, present in the BCG and SD&S retrieved by the metadata client. SilentRightsURL, PreviewRightsURL and RightsIssuerURL in DRMControlInformation may be used to get updated rights. If the DRMSystemID in DRMControlInformation is set to the value defined for Marlin, the application shall forward the DRMPrivateData, if present, to the CSP. A DAE application shall use sendDRMMessage, defined in 7.6.2.2 of IEC 62766-5-1:2017, to forward the DRMPrivateData.

All objects defined in IEC 62766-5-1 that are requested to handle a content access descriptor, defined in IEC 62766-5-1, shall check if the content-access descriptor includes DRMControlInformation. These objects or the underlying functions shall forward the available DRMPrivateData in the DRMControlInformation to the CSP if the DRMSystemID is set to the value defined for Marlin.

The DRMSystemID for Marlin is defined in 4.2.8.1.

4.2.2.5 Marlin protocol sequences

4.2.2.5.1 Marlin registration

4.2.2.5.1.1 General

Marlin registration provides functions which enable a Marlin client function in CSP to register to a Marlin domain. Marlin registration consists of node acquisition and link acquisition.

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

4.2.2.5.1.2 Node acquisition

Node acquisition provides an octopus node object from a Marlin server function in CSP-T server to a Marlin client function in CSP.

Note that node acquisition is performed prior to the respective link acquisition to provide the octopus node objects necessary for the link acquisition.

Marlin node acquisition protocol is triggered by a Marlin action token for node acquisition (hereafter "node acquisition action token") from CSP. The OITF function acquires the node acquisition action token and then the OITF function feeds it to CSP. After CSP acquires corresponding Marlin configuration token from CSP-T Server, CSP executes Marlin node acquisition protocol with CSP-T server. Note that Marlin node acquisition protocol is to provide one octopus node object per its request and response. The message flow in case of node acquisition is shown in Figure 2.

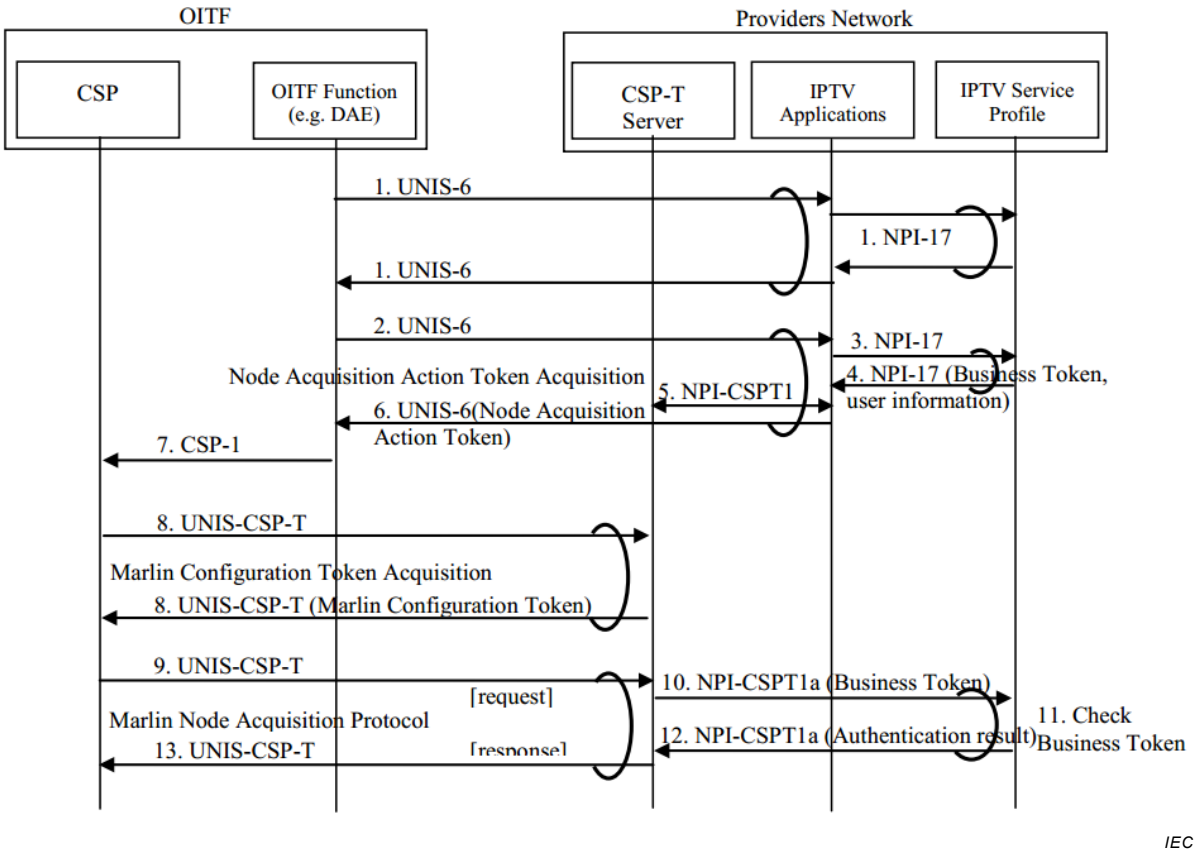

Figure 2 – Node acquisition sequence

In node acquisition sequence, the following steps are performed:

1) The OITF function (e.g. DAE) communicates with IPTV applications and IPTV service profile function via UNIS-6 and NPI-17 for node acquisition. Although NPI-17 is assumed as the interface for communication between IPTV applications and IPTV service profile, in the case of the managed network model, NPI-2 and NPI-6 may be used instead.

2) Given the Marlin action token URL (e.g. embedded into the webpage obtained in step 1), the OITF function (e.g. DAE application) sends the request for the node acquisition action token to the IPTV applications by UNIS-6.

3) When receiving the request from the OITF function, the IPTV applications sends a request to the IPTV service profile function via NPI-17 to get the necessary information to generate the node acquisition action token.

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

4) Receiving the request from IPTV applications, the IPTV service profile function sends business token and user information to IPTV applications.

5) Given the information from the IPTV applications, when there is no octopus node for the given user information, the CSP-T server generates octopus node and correlates user information with the octopus node, so that CSP-T server can check for the existence of the octopus node next time from the user information. Then the CSP-T server correlates the business token with octopus node so that the CSP-T server can provide the corresponding octopus node from the business token included in the (Marlin node acquisition protocol) request.

6) IPTV applications sends the node acquisition action token to the OITF function by UNIS-6.

7) The OITF function sends the node acquisition action token to the CSP by CSP-1.

8) When the CSP does not have a corresponding Marlin configuration token, the CSP gets the Marlin configuration token from the CSP-T server by referring to the URL specified in the node acquisition action token.

9) Given the node acquisition action token, the CSP sends a (Marlin node acquisition protocol) request to CSP-T server by UNIS-CSP-T.

10) To check the request from the CSP, the CSP-T server sends the business token (and possibly other client data such as client version or model extracted from the request) to the IPTV service profile function.

11) The IPTV service profile function validates the data received from the CSP-T server.

12) If validation succeeds, the IPTV service returns to CSP-T server the data necessary to fulfil the CSP request. If validation fails, an error is returned to the CSP-T server.

13) The CSP-T server sends a Marlin (node acquisition) response message to the CSP. This response includes either the octopus node correlated to the business token sent in the original CSP request, or an error message as defined in BNSP.

4.2.2.5.1.3 Link acquisition

Link acquisition provides an octopus link from Marlin server function in CSP-T server to Marlin client function in CSP.

NOTE This sequence assumes that the corresponding node acquisition has already been performed between the CSP and CSP-T server.

Marlin link acquisition protocol is triggered by a Marlin action token for link acquisition (hereafter "link acquisition action token") from the CSP. The OITF function acquires the link acquisition action token, and then the OITF function feeds it to the CSP. After the CSP acquires corresponding Marlin configuration token from the CSP-T server, the CSP executes Marlin link acquisition protocol with the CSP-T server.

The message flow in case of link acquisition is shown in Figure 3.

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017

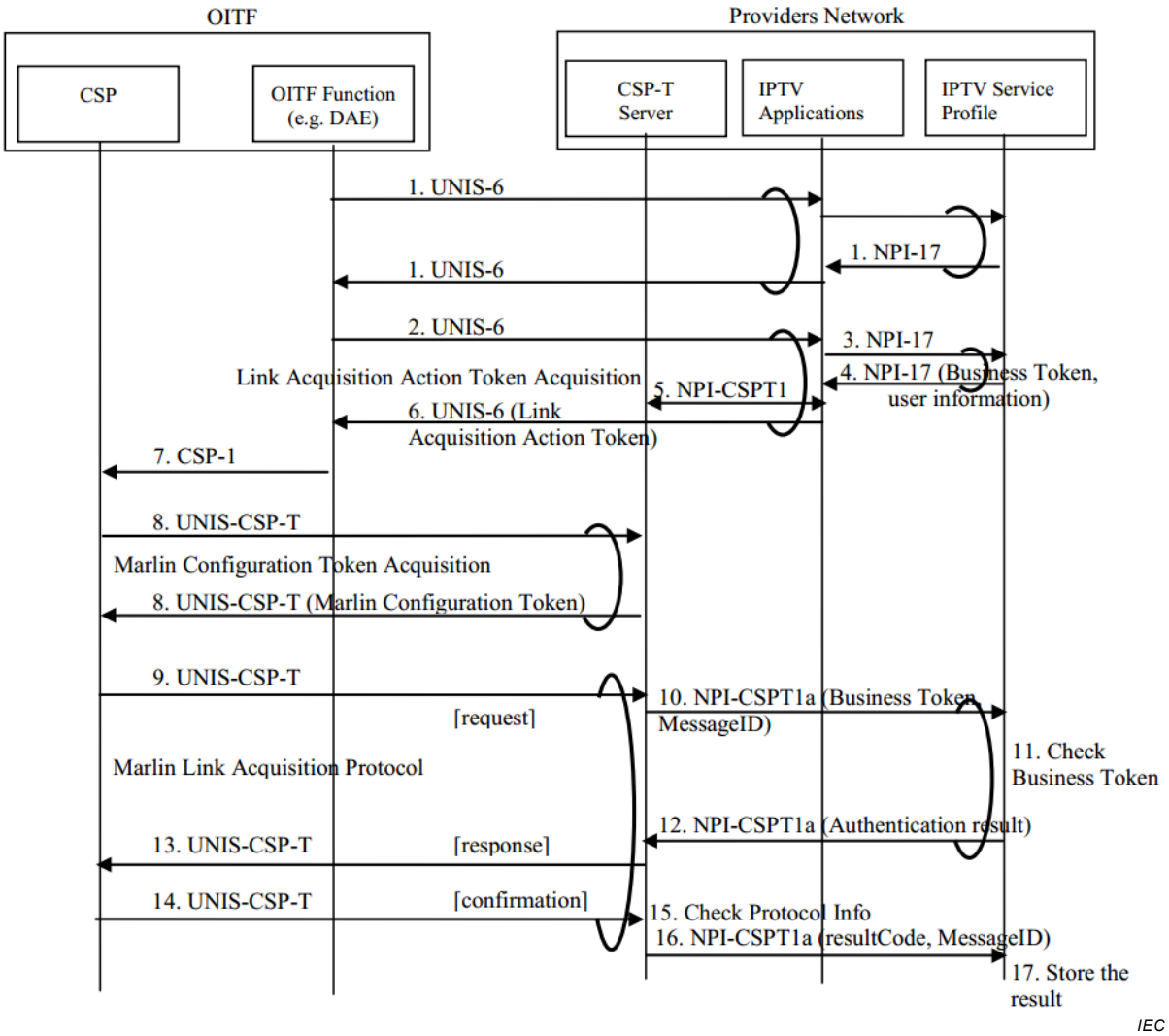

Figure 3 – Link acquisition sequence

In link acquisition sequence, the following steps are performed:

1) The OITF function (e.g. DAE) communicates with IPTV applications and IPTV service profile function via UNIS-6 and NPI-17 for link acquisition. Although NPI-17 is assumed as the interface for communication between IPTV applications and IPTV service profile, in the case of the managed network model, NPI-2 and NPI-6 may be used instead.

2) Given the Marlin action token URL (e.g. embedded into the webpage obtained in step 1), the OITF function (e.g. DAE application) sends the request for the link acquisition action token to IPTV applications by UNIS-6.

3) When receiving the request from the OITF function, the IPTV applications sends a request to the IPTV service profile function by NPI-17 to get necessary information to generate the link acquisition action token.

4) Receiving the request from IPTV applications, the IPTV service profile function sends business token and user information to IPTV applications.

5) Given the user information from the IPTV applications, the CSP-T server finds the information of octopus node which corresponds to "From Node" and "To Node". Then the CSP-T server correlates the business token with "From Node" and "To Node" so that the CSP-T server can check the information in the (Marlin link acquisition protocol) request.

6) IPTV application sends the link acquisition action token to the OITF function by UNIS-6.

AVA Documents
Document Sharing Hub

7) Given the link acquisition action token, the OITF function sends it to the CSP by CSP-1.

8) When the CSP does not have a corresponding Marlin configuration token, the CSP gets the Marlin configuration token from the CSP-T server by referring to the URL specified in the link acquisition action token by UNIS-CSP-T.

9) Given the link acquisition action token, the CSP sends a (Marlin link acquisition protocol) request to the CSP-T server.

10) To check the request from the CSP, when the request includes the correct combination of business token, "From Node", and "To Node", the CSP-T server sends a business token and MessageID to the IPTV service profile function by NPI-CSPT1a. The MessageID is a unique id, and the same MessageID is set among request, response, and confirmation, so that IPTV service profile function can use the MessageID to correlate request, response, and confirmation.

11) The IPTV service profile function validates the data received from the CSP-T server.

12) If validation succeeds, the IPTV service profile function returns to CSP-T server the data necessary to fulfil the CSP request. If validation fails, an error is returned to the CSP-T server.

13) The CSP-T server sends a Marlin (Registration) response message to the CSP. This response includes either the registration agent correlated to the Business token sent in the original CSP request, or a fault message as defined in BNSP.

14) The CSP sends a (Marlin link acquisition protocol) confirmation to the CSP-T server by UNIS-CSP-T.

15) The CSP-T server checks the resultCode (i.e. success or failure for registration in CSP), and then stores the "From Node" and "To Node" information by correlating with the user information so that CSP-T server can manage Marlin domain information for the user.

16) The CSP-T server sends the resultCode and the MessageID to the IPTV service profile function by NPI-CSPT1a.

17) The IPTV service profile function stores the resultCode in connection with the user information from step 4).

4.2.2.5.2 Marlin deregistration

Marlin deregistration provides functions which enable Marlin client function in CSP to deregister from a Marlin domain.

NOTE This sequence assumes that the corresponding node acquisition and link acquisition have already been performed between the CSP and CSP-T server.

Marlin deregistration protocol is triggered by a Marlin action token for deregistration (hereafter "deregistration action token") from the CSP. The OITF function acquires the deregistration action token, and then the OITF function feeds it to the CSP. After the CSP acquires the corresponding Marlin configuration token from the CSP-T server, the CSP executes Marlin deregistration protocol with the CSP-T server. The sequence of deregistration messages is shown in Figure 4.

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

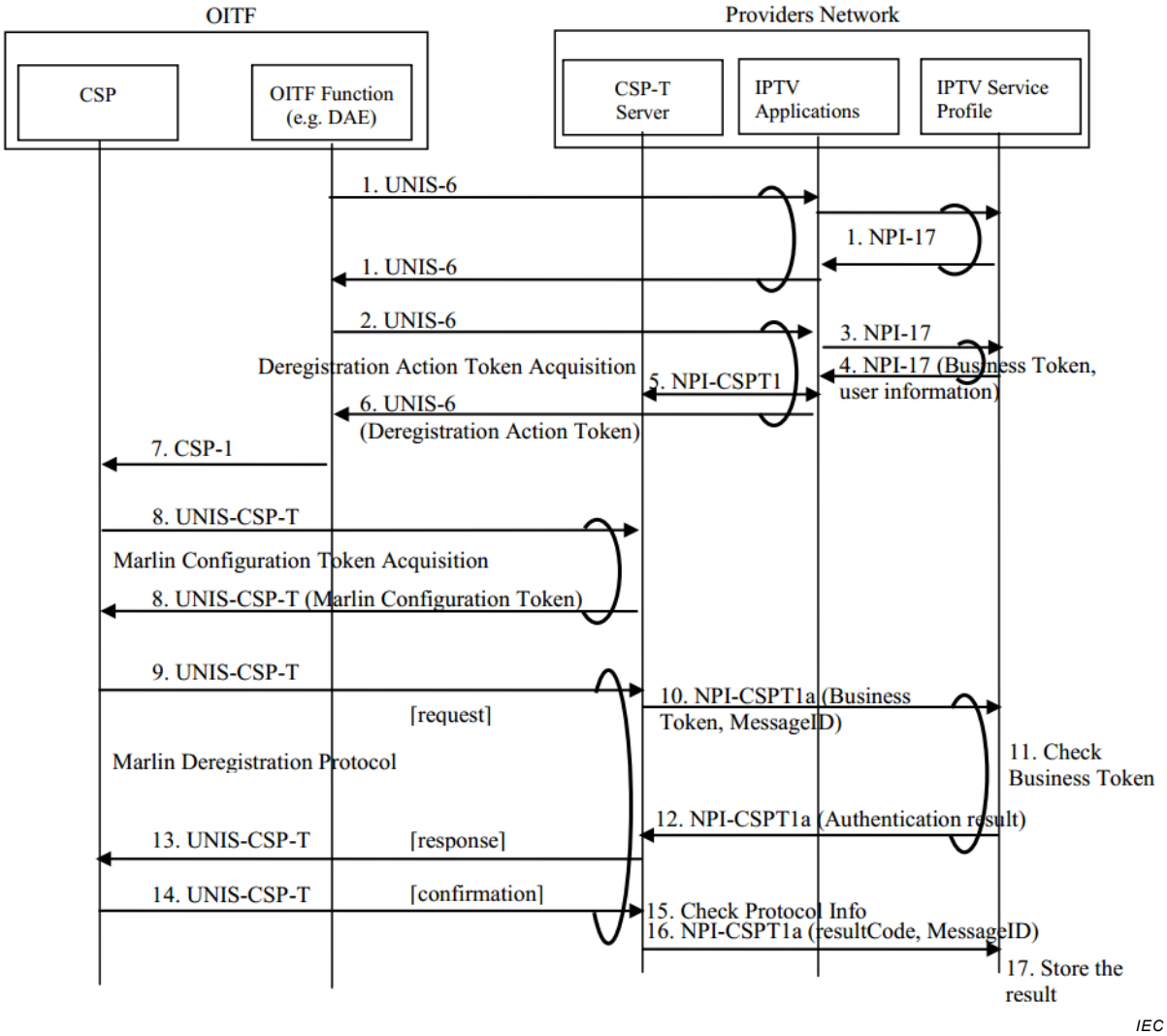

Figure 4 – Deregistration sequence

In this deregistration sequence, the following steps are performed:

1) The OITF function (e.g. DAE) communicates with IPTV applications and the IPTV service profile function via UNIS-6 and NPI-17 for Marlin deregistration. Although NPI-17 is assumed as the interface for communication between IPTV applications and the IPTV service profile, in the case of the managed network model, NPI-2 and NPI-6 may be used instead.

2) Given the Marlin action token URL (e.g. embedded into the web page obtained in step 1), the OITF function (e.g. DAE application) sends the request for the deregistration action token to the IPTV applications by UNIS-6.

3) When receiving the request from the OITF function, the IPTV applications sends a request to the IPTV service profile function by NPI-17 to get necessary information to generate the deregistration action token.

4) Receiving the request from IPTV applications, the IPTV service profile function sends business token and user information to IPTV applications.

5) Given the user information from the IPTV applications, the CSP-T server finds the information of octopus node which corresponds to "From Node" and "To Node". Then the CSP-T server correlates the business token with "From Node" and "To Node" so that the CSP-T server can check the information in (Marlin deregistration protocol) request.

6) IPTV applications sends the deregistration action token to the OITF function by UNIS-6.

AVA Documents
Document Sharing Hub

7) Given the deregistration action token, the OITF function sends it to the CSP by CSP-1.

8) When the CSP does not have a corresponding Marlin configuration token, the CSP gets the Marlin configuration token from the CSP-T server by referring to the URL specified in the deregistration action token.

9) Given the deregistration action token, the CSP sends a (Marlin deregistration protocol) request to the CSP-T server by UNIS-CSP-T.

10) To check the request from the CSP by the IPTV service profile function, when the request includes the correct combination of business token, "From Node", and "To Node", the CSP-T server sends a business token and MessageID to the IPTV service profile function by NPI-CSPT1a. The MessageID is a unique id and the same MessageID is set among request, response, and confirmation so that IPTV service profile function can use the MessageID to correlate request, response, and confirmation.

11) The IPTV service profile function validates the data received from the CSP-T server.

12) If validation succeeds, the IPTV service profile function returns to the CSP-T server the data necessary to fulfil the CSP request. If validation fails, an error is returned to the CSP-T server.

13) The CSP-T server sends a Marlin (Deregistration) response message to the CSP. This response includes either the deregistration agent correlated to the business token sent in the original CSP request, or an error message as defined in BNSP.

14) The CSP sends a (Marlin deregistration protocol) confirmation to the CSP-T server by UNIS-CSP-T.

15) The CSP-T server checks the resultCode (i.e. success or failure for deregistration in CSP) and MessageID, and then stores the "From Node" and "To Node" information by correlating it with the user information, so that CSP-T server can manage Marlin domain information for the user.

16) The CSP-T server sends the resultCode and the MessageID to the IPTV service profile function by NPI-CSPT1a.

17) The IPTV service profile function stores the resultCode in connection with the user information from step 4).

4.2.2.5.3 Marlin licence acquisition

Licence acquisition provides functions which enable Marlin client function in CSP to obtain a Marlin licence.

Marlin licence acquisition protocol is triggered by a Marlin action token for licence acquisition (hereafter "licence acquisition action token") from CSP. The OITF function acquires the licence acquisition action token, and then the OITF function feeds it to the CSP. After the CSP acquires the corresponding Marlin configuration token from CSP-T server, CSP executes the Marlin licence acquisition protocol with CSP-T server. The sequence of licence acquisition messages is shown in Figure 5.

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

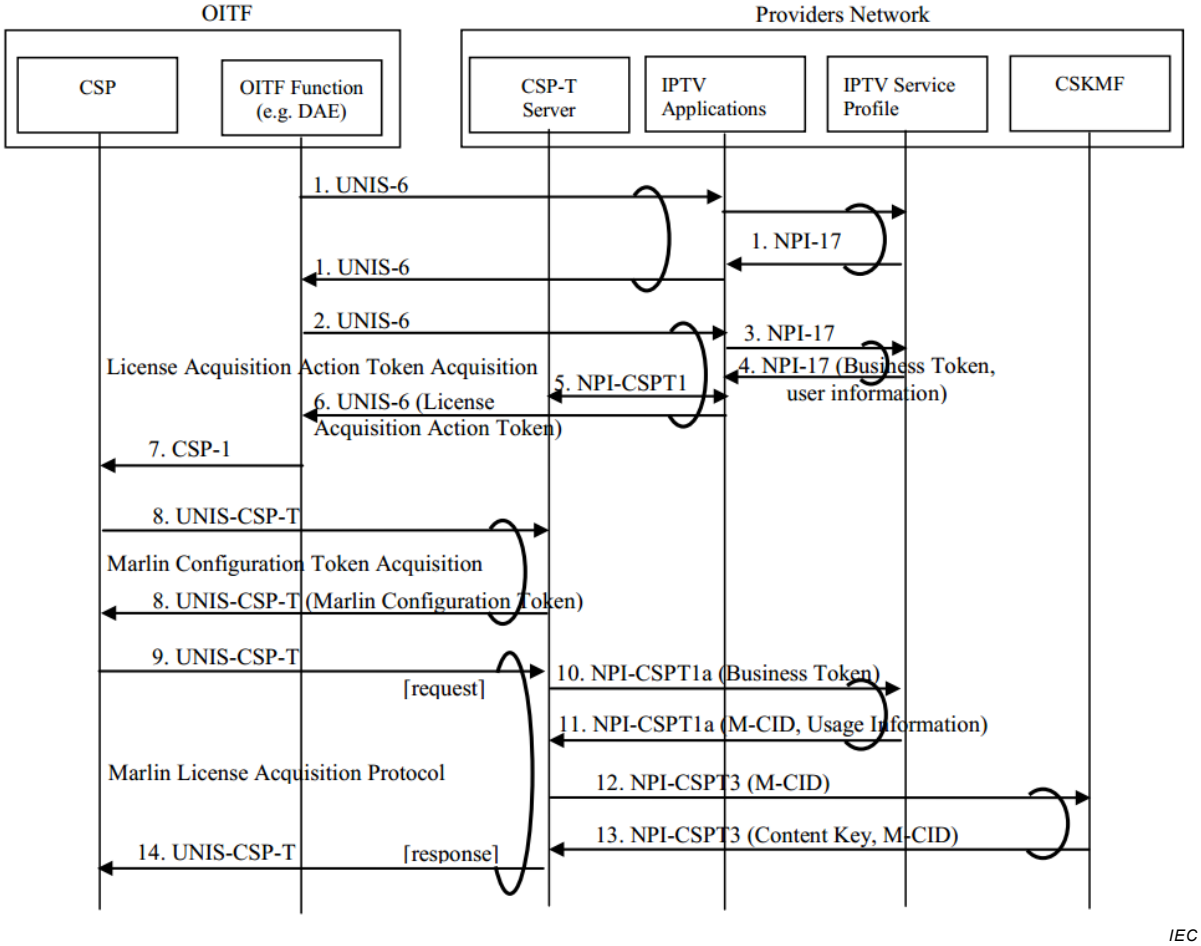

Figure 5 – Licence acquisition sequence

In this sequence, the following steps are performed:

1) The OITF function (e.g. DAE) communicates with IPTV applications and IPTV service profile function via UNIS-6 and NPI-17 for licence acquisition. Although NPI-17 is assumed as the interface for communication between IPTV applications and IPTV service profile, in the case of the managed network model, NPI-2 and NPI-6 may be used instead.

2) Given the Marlin action token URL (e.g. embedded into the webpage obtained in step1), the OITF function (e.g. DAE application) sends the request for the licence acquisition action token to the IPTV applications by UNIS-6.

3) When receiving the request from the OITF function, the IPTV applications sends a request to the IPTV service profile function by NPI-17 to get the information necessary to generate the licence acquisition action token.

4) Receiving the request from IPTV applications, the IPTV service profile function sends business token and user information to IPTV applications. This user information for licence acquisition also indicates "Bound to Node" of the Marlin licence.

5) Given the information from the IPTV applications, the CSP-T server correlates the business token with the "Bound to Node" so that the CSP-T server can check the information in a (Marlin Licence acquisition protocol) request.

6) IPTV applications sends the licence acquisition action token to the OITF function by UNIS-6.

7) Given the licence acquisition action token, the OITF function sends it to the CSP by CSP-1.

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

8) When the CSP does not have a corresponding Marlin configuration token, the CSP obtains the Marlin configuration token from the CSP-T server by referring to the URL specified in the licence acquisition action token.

9) Given the licence acquisition action token, the CSP sends a (Marlin licence acquisition protocol) request to the CSP-T server by UNIS-CSP-T.

10) To check the request from the CSP, when the request includes the correct combination of business token and "Bound to Node", the CSP-T server sends a business token to the IPTV service profile function by NPI-CSPT1a.

11) The IPTV service profile function validates the data received from the CSP-T server. If validation fails, an error is returned to the CSP-T server. If validation succeeds, the IPTV service profile function returns to CSP-T server the data necessary to generate the Marlin licence, consisting at a minimum of:

- M-CID (Marlin Content ID);
- usage information, which includes the content usage rules.

12) To get the corresponding content key, the CSP-T server sends the M-CID to the CSKMF by NPI-CSPT3.

13) When receiving the information, the CSKMF looks for the corresponding content key by M-CID, and then sends the content key and M-CID to the CSP-T server by NPI-CSPT3. When the content is protected by scramble key and service key (or programme key), the service key (or programme key) is provided from CSKMF to CSP-T server instead of content key. See 4.2.4 for a brief explanation of such encryption scheme.

14) The CSP-T server sends a Marlin (licence) response message to the CSP. This response includes either the licence correlated to the business token sent in the original CSP request, or an error message as defined in BNSP.

4.2.3 Protected content usages

4.2.3.1 General

Protected content usages include: playback, recording, time shifting.

Protected content can be played from a native application or from a DAE application using A/V plug-in or video/broadcast object as defined in IEC 62766-5-1.

Protected content can be time-shifted from a native application or from a DAE application using video/broadcast object as defined in IEC 62766-5-1.

Protected content can be recorded from a native application or from a DAE application video/broadcast object as defined in IEC 62766-5-1.

The CSP shall control protected content usages as defined in BNSP for licence evaluation, Marlin MS3 for evaluation of stream access statements, and BBTS for ECM control. See also 4.2.4 for an overview.

If usages are not allowed, the CSP shall block the consumption of programmes (i.e. stop descrambling) and shall generate the appropriate event (no rights, parental control locking) to the calling application, i.e. native application or DAE object. The DAE AV or video/broadcast object shall trigger the event to the calling DAE application as specified in 4.2.2.4.

For MPEG-2 TS, usages shall be controlled at each ECM change. For other file formats, usages are controlled only when requesting the usage.

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

4.2.3.2 Marlin licence evaluation

4.2.3.2.1 Licence evaluation (for (P)DCF OMArlin or Marlin IPMP Marlin FF)

Subclause 4.2.3.2 describes the informative overview of how Marlin data objects acquired via Marlin protocols are used for consumption of protected contents, such as rendering or exporting. Figure 6 shows the message flow of licence evaluation.

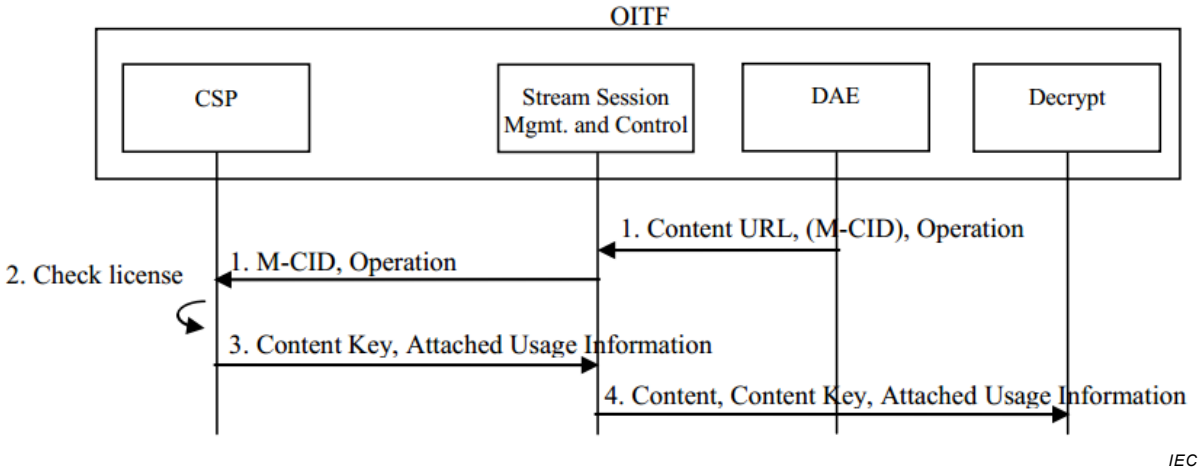

Figure 6 – Licence evaluation sequence

In order to gain access to a protected content, steps below are performed:

1) An OITF function such as DAE triggers the evaluation of a corresponding Marlin licence at CSP via stream session management and control by providing following information:
   - Content URL: the protected content to be accessed.
   - Optionally, M-CID (Marlin Content ID): ID of the protected content to be accessed. The M-CID can also be retrieved from the content, ContentAccessDescriptor IEC 62766-5-1, BCG, or SD&S (see IEC 62766-3).
   - Operation: operation to perform with the protected content (e.g. render, export).

   NOTE Although DAE is used as a function to trigger the licence evaluation, this is only for illustrative purposes and other OITF function can be used, such as OITF embedded application depending on the design of the OITF.
2) The Marlin client function in the CSP is required to check the following:
   - The PKI signatures on the Marlin data objects related to the protected content are validated. For trust management of Marlin, see Clause 9 of the Marlin core specification.
   - The usage rule specified in the Marlin data objects for the protected content is valid for the CSP.
3) If the licence evaluation succeeds, the CSP returns the corresponding content key and attached usage information such as output control information (if any) to the stream session management and control. Otherwise, the CSP responds with an error.
4) The stream session management sends the received content, content key and attached usage information, to the decrypt function.

4.2.3.2.2 Licence evaluation (for MPEG-2 transport stream)

Figure 7 shows the message flow of licence evaluation with scramble key decryption.

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

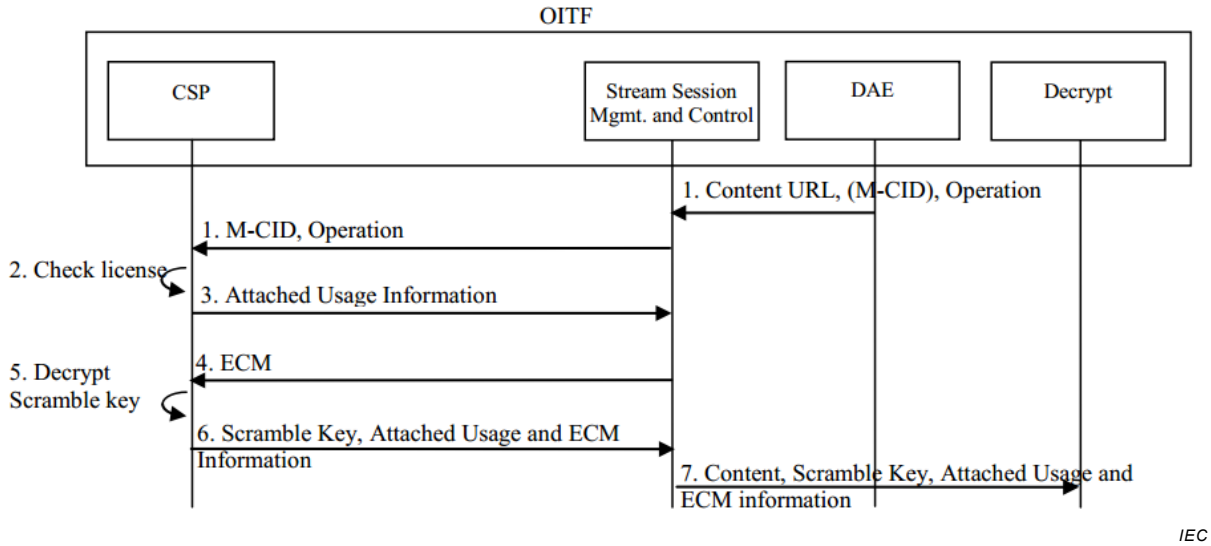

Figure 7 – Scramble key decryption sequence

When the content is encrypted by scramble key, the licence evaluation and scramble key decryption sequence below is followed:

1) OITF function such as DAE triggers the evaluation of a corresponding Marlin Licence at CSP via stream session management and control by providing following information:
   - Content URL: the protected content to be accessed (Local or remote URL).
   - Optionally, M-CID (Marlin Content ID): ID of the protected content to be accessed. The M-CID can also be retrieved from the content, ContentAccessDescriptor IEC 62766-5-1, BCG, or SD&S (see IEC 62766-3).
   - Operation: operation to perform with the protected content (e.g. render, export).

   NOTE Although DAE is used as a function to trigger the licence evaluation, this is only for illustrative purposes and other OITF function can be used, such as OITF embedded application depending on the design of the OITF.
2) The Marlin client function in the CSP is required to check the following:
   - The PKI signatures on the Marlin data objects related to the protected content are validated (signature O.K. and certificate chain is successfully chained up to the Marlin trust anchors).
   - The usage rule specified in the Marlin data objects for the protected content is valid for the CSP.
3) If the licence evaluation succeeds, the CSP returns attached usage information such as output control information (if any) to the stream session management and control. Otherwise, the CSP responds with an error.
4) The stream session management and control provides an ECM to the CSP. The ECM includes a scramble key encrypted by a service or programme key and attached ECM information including the encryption algorithm type, parental control information, recording control Information and output control information.
5) The CSP checks the ECM on integrity. If this is OK, the CSP decrypts encrypted scramble key with the appropriate key, and, based on the combined output control information in the ECM and licence, the CSP determines updated output control information as specified in BBTS.
6) The CSP sends scramble key and attached usage and ECM information to the stream session management and control.
7) The stream session management sends the received content, scramble key and attached usage and ECM information to the decrypt.

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

NOTE The sequence assumes that stream session management and control is trusted by the CSP and that the scramble key, permission to perform the requested operation and attached usage information are transferred over a secure channel.

4.2.4 Content encryption

This subclause contains an informative overview of content encryption to clarify sequences related to content key, service or programme key, and scramble key in 4.2.2.5.3 and 4.2.3.2. Figure 8, Figure 9 and Figure 10 show the message flows of content encryption.

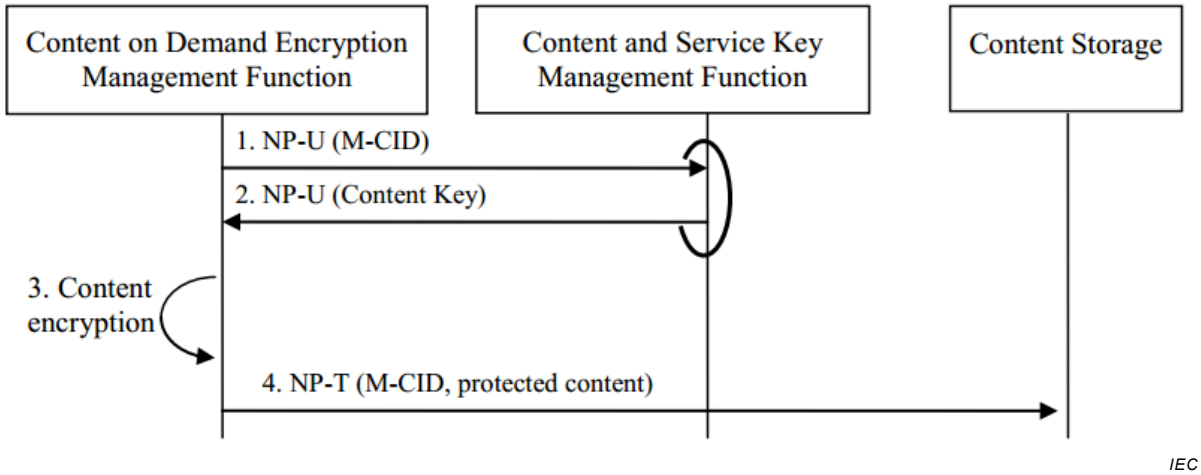

Figure 8 – Content on demand encryption sequence using content key (for (P)DCF OMArlin or Marlin IPMP Marlin FF)

When (P)DCF OMArlin or Marlin IPMP Marlin FF content on demand is encrypted using a content key, the following steps are performed in the content encryption sequence:

1) The content on demand management requests for a content specified by M-CID (Marlin content ID), the content key to use.
2) The content and service key management function returns the content key.
3) The content on demand encryption management function launches encryption of the content in the clear using the M-CID (Marlin content ID) and content key. The protected content is generated.
4) The content on demand management stores the protected content in the content storage.

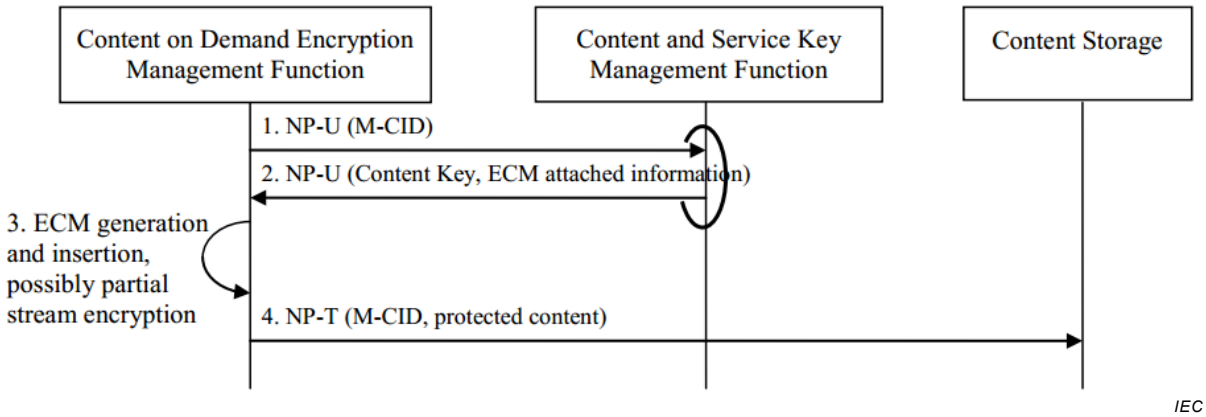

Figure 9 – Content on demand encryption sequence using content key (for MPEG-2 TS)

When MPEG-2 TS content on demand is encrypted using a content key, the following steps are performed in the content encryption sequence:

Documents
Document Sharing Hub
Full document details: BS IEC 62766-7:2017

1) The content on demand management requests, for the content item specified by M-CID (Marlin content ID), the content key and ECM attached information, including the encryption algorithm, parental control information and output control information, to use.
2) The content and service key management function returns the content key and ECM attached information.
3) The content on demand encryption management function launches encryption of the content in the clear. Scramble keys are generated and the content is encrypted using these scramble keys. The scramble keys are encrypted using the content key. ECMs that include scramble keys and provided ECM attached information are inserted into the protected content.
4) The content on demand encryption management function stores the protected content in the content storage.

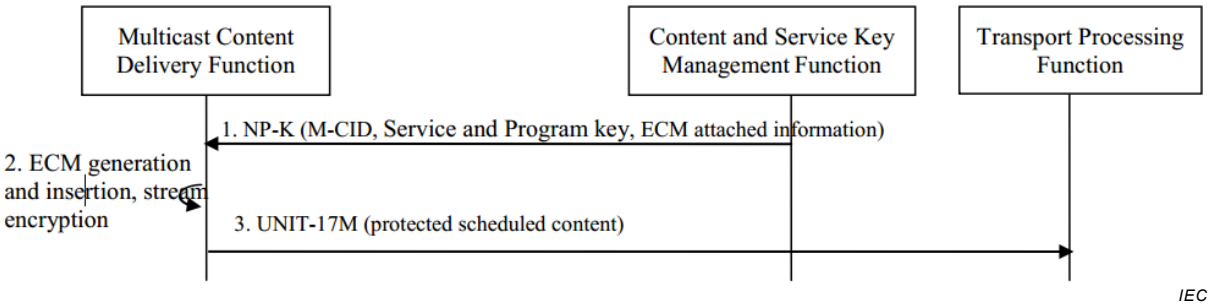

Figure 10 – Scheduled content encryption sequence using scramble key (for MPEG-2 TS)

When MPEG-2 TS scheduled content is encrypted by scramble keys, then the scramble keys are encrypted by a service or programme key, the following steps are performed in Content Encryption sequence:

1) The content and service key management function sends the M-CID (Marlin Content ID), service key and possibly a programme key, ECM attached information including encryption algorithm, parental control information and output control information to the multicast content delivery function.
2) The multicast content delivery function generates scramble keys and then encrypts clear content using these scramble keys. Then the multicast content delivery function encrypts the scramble keys using the service key or programme key. When the programme key is used for encryption of scramble keys, the multicast content delivery function encrypts the programme key using the service key. An ECM that includes the encrypted scramble keys and provided ECM attached information is inserted into the protected content.
3) Protected scheduled content is sent to the transport processing function through UNIT-17M.

4.2.5 Protected file formats

The protected file formats supported in the present specification are:

– the MP4 file format as defined in 5.3 of IEC 62766-2-1:2016
  - encrypted according to the OMA (P)DCF file formats, including Marlin specific extensions in an OMA compatible way, as defined in clause 4 of OMArlin,
  - encrypted according to the Marlin IPMP file format as specified in 2.3 of Marlin FF,
  - encrypted as specified in ISO/IEC 23001-7,
– the MPEG-2 TS file format as specified in 4.2.6.

NOTE This clause lists four different protected file formats supported by this specification. The criteria that determine under which circumstances which one or more of these is implemented are out of the scope of the present document.

AVA Documents
Document Sharing Hub

4.2.6 Protection of MPEG-2 transport streams

4.2.6.1 General

If the OITF supports the unprotected MPEG-2 TS format, the OITF shall support the Marlin protected MPEG-2 TS format, as defined in 4.2.6. Otherwise, the support of the Marlin protected MPEG-2 TS format as defined in 4.2.6 is optional.

If the OITF supports the unprotected time stamped MPEG-2 TS format, the OITF shall support the Marlin protected time stamped MPEG-2 TS format, as defined in 4.2.6. Otherwise, the support of the Marlin protected time stamped MPEG-2 TS format as defined in 4.2.6 is optional.

4.2.6.2 Context

Transport of conditional access messages in MPEG-2 TS is defined by DVB. CA_descriptors (conditional access descriptor) are used to signal the presence of conditional access information in the stream. Conditional access messages are transported in short MPEG-2 TS private clause (clause_syntax_indicator = 0). Two types of messages are considered:

- ECM messages, which are linked to descrambling, access criteria and control words (TEK). These messages are signalled in the CA_descriptor in the PMT. ECM messages should have a high repetition rate in order to allow quick programme access.
- EMM messages, which are linked to rights management. These messages are signalled in the CA_descriptor in the CAT. These messages' repetition rate should be set at head end level in order to comply with the operator QoS requirements.

Figure 11 provides an overview of the relevant signalling defined by DVB, using example PID values.

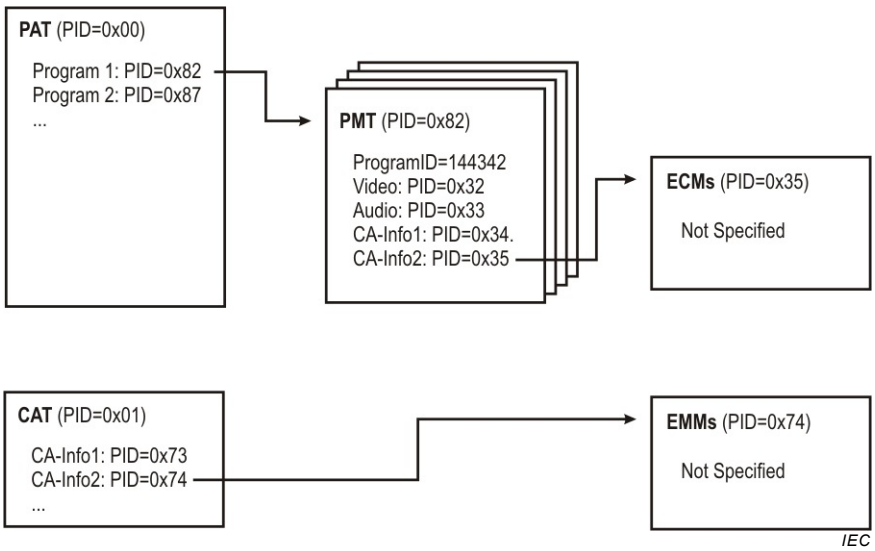

Figure 11 – Conditional access descriptors signalling ECM and EMM messages

Marlin is used to protect MPEG-2 transport streams and time stamped transport streams as specified in BBTS. If an OITF supports Marlin protected MPEG-2 TS, the OITF shall implement the functions of the DRM client as specified in BBTS. For Marlin protected MPEG-2 TS the content delivery function shall deliver transport streams or time-stamped transport streams that are formatted as specified in BBTS.

If an OITF supports Marlin protected MPEG-2 TS, the OITF shall support the parental_rating access_criteria_descriptor as specified in IEC 62455, the recording control access_criteria_descriptor as specified in 4.2.6.3 and shall support at least the rating_type 0 in these criteria, which maps to the parental rating system in DVB systems, as defined in EN 300 468.

AVA Documents
Document Sharing Hub

For the recording control, refer also to 4.2.6.3, the OITF shall compare the required operation with the allowed operations (PVR and time shifting) in the recording control criteria and refuse the requested operation to the calling application (native or DAE) if the requested operation is not allowed.

For the parental rating control, the OITF shall compare the programme's rating from the parental rating access_criteria_descriptor with the current parental rating criterion set in the OITF by the application (either native application or DAE) and shall block the consumption of programme (i.e. stop descrambling), if the parental rating system is supported by the OITF and the programme's rating does not meet the parental rating criterion (e.g. rating is at or above a certain threshold, for a rating system that is ordered from lower viewer age to higher viewer age). The OITF shall raise an event to the application controlling the playback or other operation, whenever a parental rating is discovered for the A/V content that does not meet the parental rating criterion that is set for the parental system in use, which has led to blocking of the consumption of the content. The event shall provide the programme's rating. In case the application is a native application and if the MPEG-2 TS provides a parental control URL, as defined in 4.2.6.5, the native application should launch the DAE with the Parental Control URL for the management of parental control. In case the application is a DAE application, the event is called onParentalRatingChange and is defined in 7.13.6 and 7.14.6 of IEC 62766-5-1:2017.

If the OITF does not support the particular parental rating system used in the programme, the OITF shall raise an event to the application controlling the playback or other operation. The event shall provide the programme's rating. In the case that the application is a DAE application, the event is called onParentalRatingError and is defined in 7.13.6 and 7.14.6 of IEC 62766-5-1:2017. The event may be managed via the DAE application (see 4.6 of IEC 62766-5-1:2017 for more information). In the case that the application is a native application, the event is managed through an OITF vendor-dependent user interface. In both cases, consumption may be unblocked by setting a new parental rating threshold. This threshold setting is usually restricted to privileged users, e.g. parents and a successful PIN input by a user may be used to control the parental rating threshold setting. The OITF should continue monitoring the MPEG-2 TS, taking into account parental rating criteria changes in ECM streams or new settings for the parental rating threshold in the OITF, and shall unblock consumption (i.e. re-start descrambling) if the current programme's rating becomes lower than the current parental rating threshold.

When no valid rights are available for the MPEG-2 TS, the OITF shall block the consumption of the programme (i.e. stop descrambling) and shall raise an event to the application controlling the playback or other operation. In case the application is a DAE application, the event is called onDRMRightsError and is defined in 7.13.7 and 7.14.7 of IEC 62766-5-1:2017. The OITF should continue monitoring the MPEG-2 TS, taking into account criteria changes in ECM streams or rights changes in OITF and shall unblock consumption (i.e. re-starting descrambling) if there are valid rights for the requested operation.

For the avoidance of doubt, the OITF shall support the presence of descriptors (for a general description of descriptors, see ISO/IEC 13818-1 which are not defined in this specification) but shall ignore these descriptors. In particular, to allow DVB-SimulCrypt with other CA systems as defined in TS 103 197 and gateway-centric approach, the presence of the following descriptors shall be supported: CA descriptor for other CA systems than Marlin and than CA systems supported in a CSPG, scrambling descriptor EN 300 468, and copyright descriptor ISO/IEC 13818-1.

4.2.6.3 Recording control access criteria

This clause defines an access_criteria_descriptor that may be present in the IEC 62455 ECM as defined in BBTS, as shown in Table 1.

Documents
Document Sharing Hub

Full document details: BS IEC 62766-7:2017