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

IEC 62766-7:2017-07(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 It also gives information on projects, replaced and withdrawn publications.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 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.

CONTENTS

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 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

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

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

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

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

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.

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.

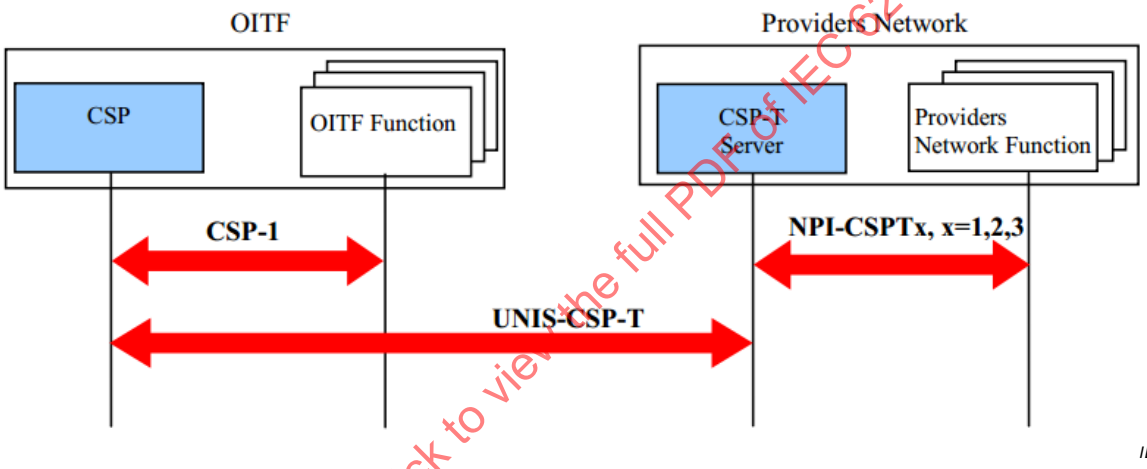

Figure 1 – CSP-T system overview

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

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.

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.

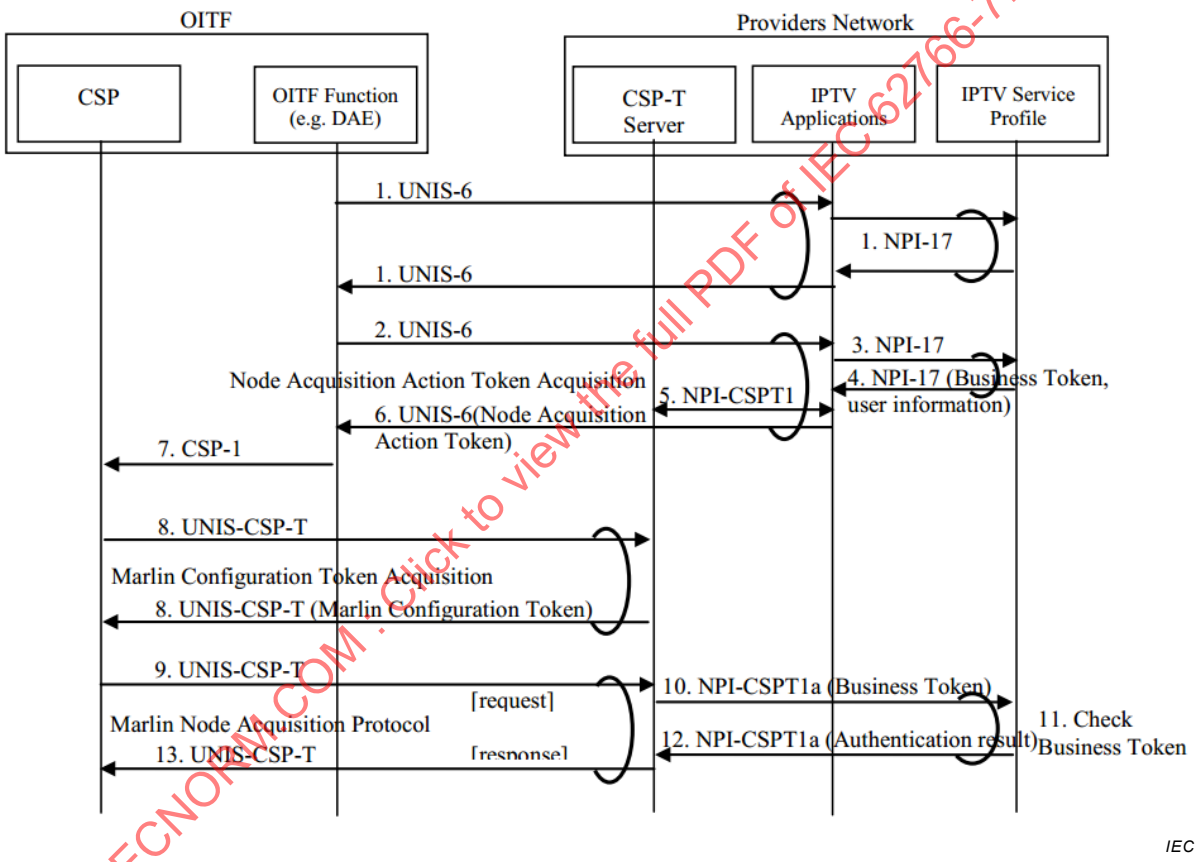

Figure 2 – Node acquisition sequence

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.

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.

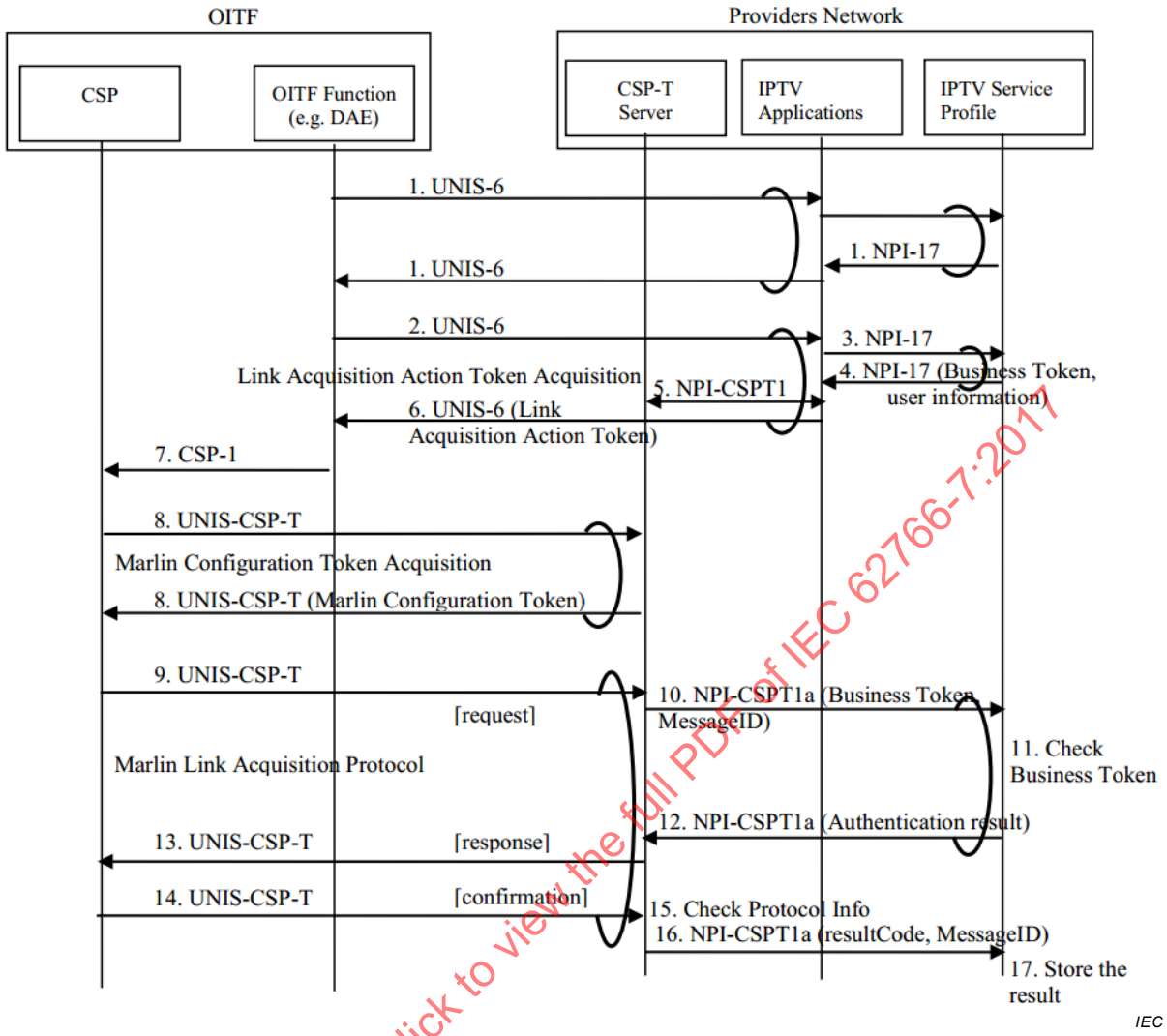

Figure 3 – Link acquisition sequence

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.

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.

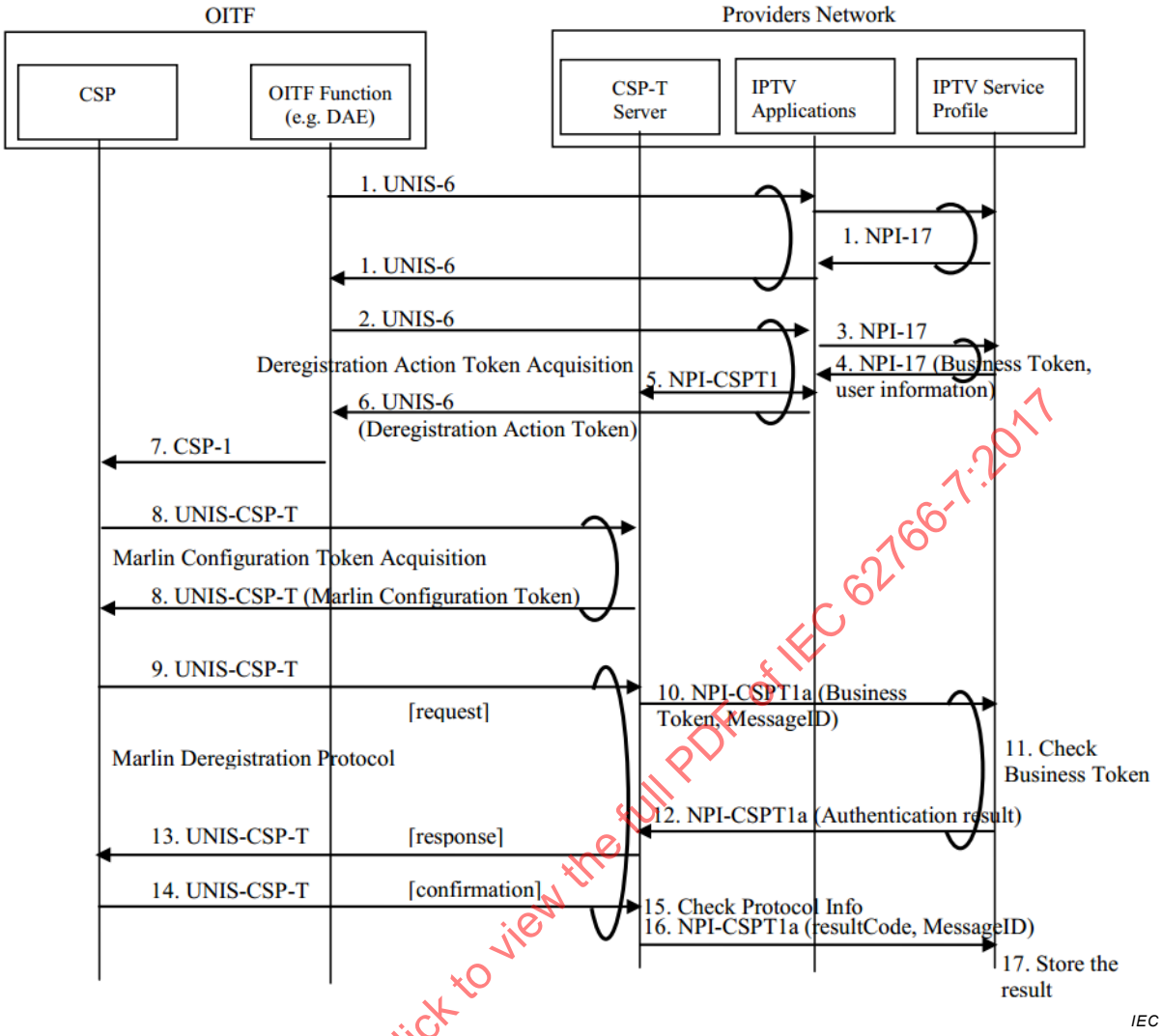

Figure 4 – Deregistration sequence

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.

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.

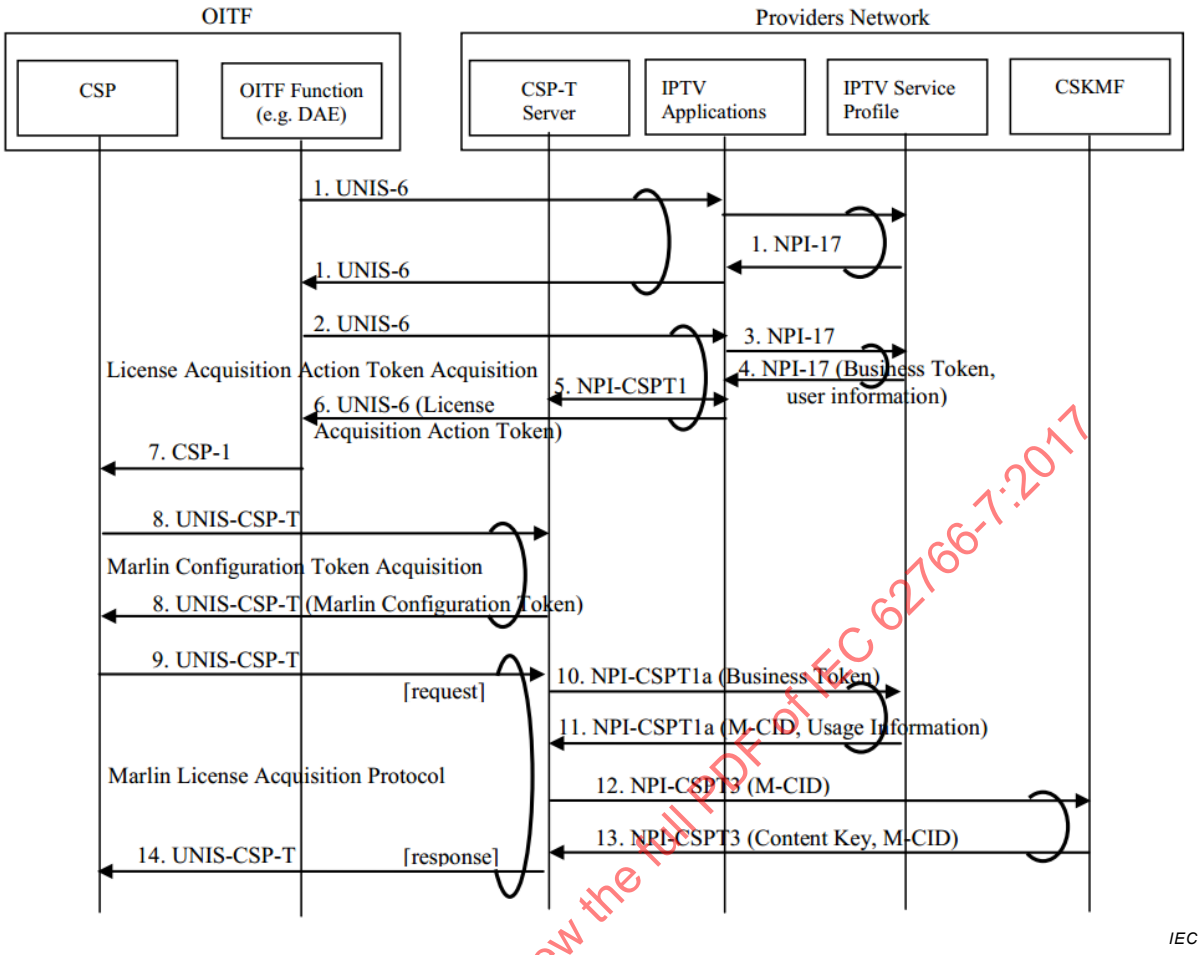

Figure 5 – Licence acquisition sequence

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.

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.

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.

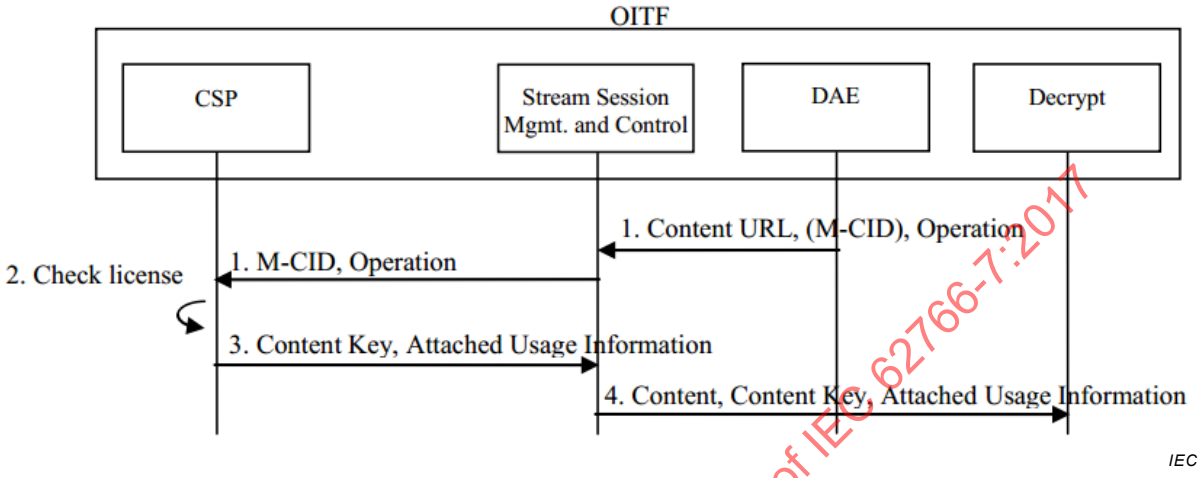

Figure 6 – Licence evaluation sequence

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.

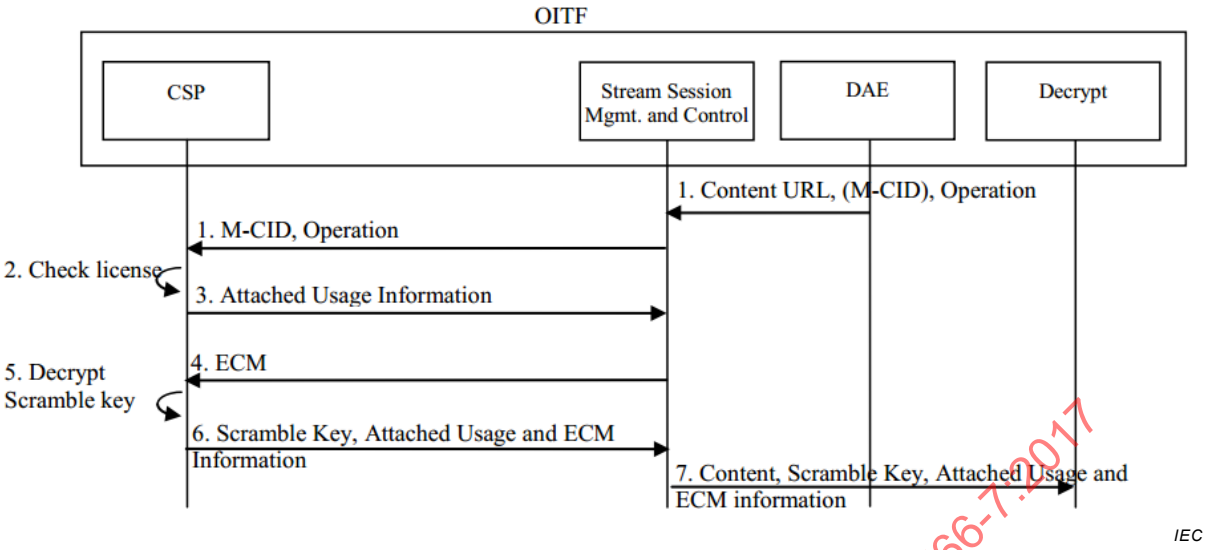

Figure 7 – Scramble key decryption sequence

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.

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.

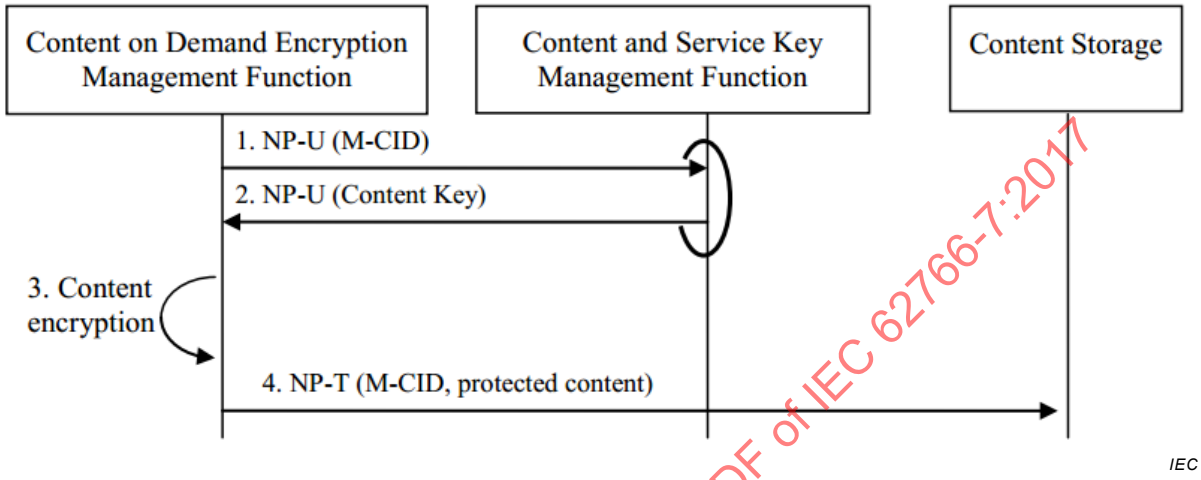

Figure 8 – Content on demand encryption sequence using content key (for (P)DCF OMArlin or Marlin IPMP Marlin FF)

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.

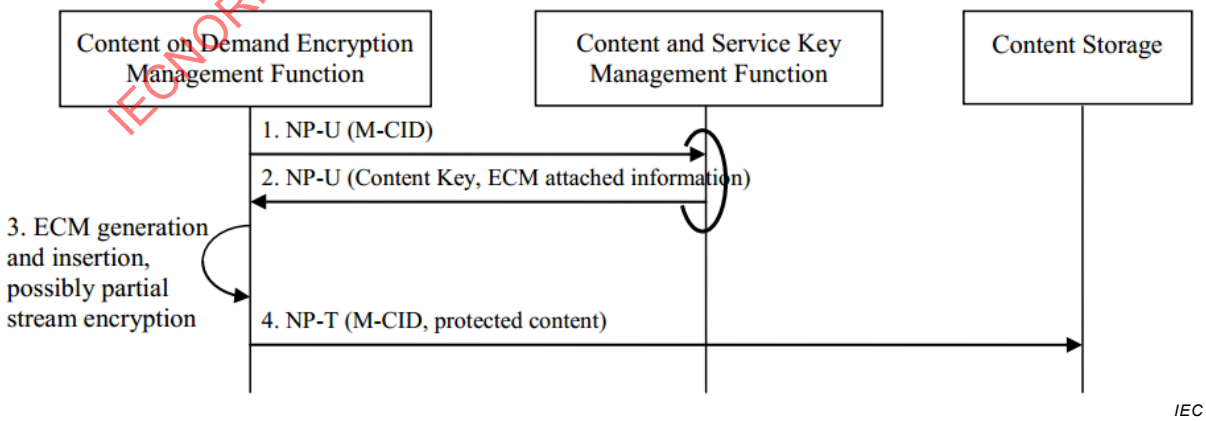

Figure 9 – Content on demand encryption sequence using content key (for MPEG-2 TS)

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

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.

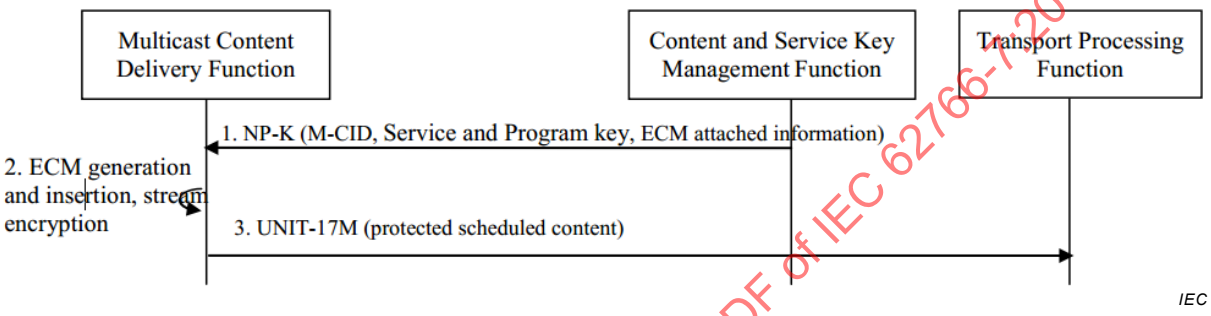

Figure 10 – Scheduled content encryption sequence using scramble key (for MPEG-2 TS)

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.

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.

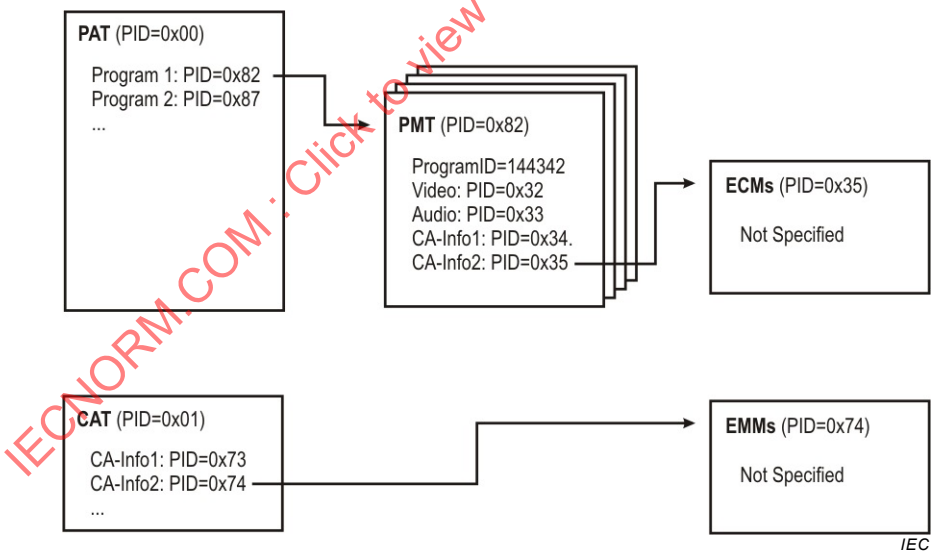

Figure 11 – Conditional access descriptors signalling ECM and EMM messages

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.

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.

Table 1 – Recording Control access_criteria_descriptor

recording control information access_criteria_descriptor	Tag	Length (in bits)	Type
recording_control_information_byte	0x010	8	Bslbf

Table 2 shows the syntax of the recording_control_information_byte.

Table 2 – Bit assignments of recording_control_information_byte

Bit #	7	6	5	4	3	2	1	0
Assignment	rsvd	rsvd	rsvd	rsvd	rsvd	rsvd	DNTS	DNR

The DNR (do not record) bit signals that a BBTS is not allowed to be stored for PVR function. The OITF shall not store for the PVR function the TS packets of a BBTS that are received after receipt of a BBTS packet carrying an IEC 62455 ECM that includes a recording control access_criteria_descriptor in which the DNR bit is set to 1.

The OITF may store for the PVR function the TS packets of a BBTS that are received after receipt of a BBTS packet carrying an IEC 62455 ECM that does not include a recording control access_criteria_descriptor or does include a recording control access criterion in which the DNR bit is set to 0.

The DNTS (do not time shift) bit signals that a BBTS is not allowed to be stored for time shifting. The OITF shall not store for time shifting the TS packets of a BBTS that are received after receipt of a BBTS packet carrying an IEC 62455 ECM that includes a recording control access_criteria_descriptor in which the DNTS bit is set to 1.

The OITF may store for time shifting the TS packets of a BBTS that are received after receipt of a BBTS packet carrying an IEC 62455 ECM that does not include a recording control access_criteria_descriptor or does include a recording control access criteria in which the DNTS bit is set to 0.

The time shifting period shall not exceed 90 min if the DNR bit is set to 1 and the DNTS bit is set to 0.

The combination of DNR equals 0 (PVR allowed) and DNTS equals 1 (time shift not allowed) should not be set.

For an overview of the combinations, see Table 3.

Table 3 – DNR and DNTS combinations

DNR	DNTS	Description
0	0	Time shifting allowed for infinite period; PVR allowed
0	1	Should not occur
1	0	Time shift limited to 90 min; PVR not allowed
1	1	Time shift not allowed; PVR not allowed

The rsvd (reserved for future use) bits shall be set to 0.

4.2.6.4 PMT table

When creating transport streams that are formatted as specified in BBTS, the content delivery shall include a BBTS CA_descriptor BBTS in each PMT pointing to a stream protected by Marlin and shall include the serviceBaseCID, see BBTS, into the BBTS CA_descriptor. The socID BBTS used by the content delivery shall be "marlin" (without the double quotes).

In case DVB-SimulCrypt is used with other CA systems as defined in TS 103 197 and/or with the gateway-centric approach then the content_key_index field in the IEC 62455 ECM as defined in BBTS shall match the scrambling_mode of the other CA system. If the cipher_mode field is 0x1 (CBC) then the initial_vector and next_initial_vector fields in the IEC 62455 ECM shall be set to 0 as specified in ATIS-0800006.

4.2.6.5 CAT table

When creating transport streams that are formatted as specified in BBTS, the content delivery function may include a BBTS CA_descriptor BBTS in the CAT for streams protected by Marlin, in order to provide Marlin rights URLs. If several Marlin rights URL sets are provided for different service operators, the content delivery shall include several BBTS CA_descriptor and each BBTS CA_descriptor shall include a different serviceBaseCID.

The rights issuer URL clause, defined in BBTS, may contain a parental control URL, as defined in this subclause. Use of the parental control URL is described in 4.2.6.2.

The coding of the parental control URL parameter in the TLV format is shown in Table 4.

Table 4 – Parental_Control_URL parameter syntax

Syntax	Mnemonic	No. of bits
Parental_Control_URL () {		
Parental_Control_URL_tag = 0x05	uimsbf	8
Parental_Control_URL_length	uimsbf	8
For (i=0; i<N; i++){		
Parental_Control_URL_data_byte	bslbf	8
}		
}		

Parental_Control_URL_tag: this specification has defined the value of 0x05 for the parental control URL parameter.

Parental_Control_URL_length: specifies the length of the Parental_Control_URL_data_byte in bytes (N).

Parental_Control_URL_data_byte: the parental control URL for this content.

NOTE The syntax of Table 4 and similar tables in subsequent clauses follows conventions outlined in ISO/IEC 13818-1 (e.g. mnemonics, use of C-language like loop descriptors).

Before accessing the rights issuer URL specified in BBTS, the OITF, or the DAE application that receives an "onDRMRightsError" event, as defined in 7.13.7 and 7.14.7 of IEC 62766-5-1:2017, shall obtain user consent to access the web page. When a service receives an HTTP request to the Rights Issuer URL, the service should respond with an HTML page and not with a Marlin action token or with a Marlin licence. This HTML shall comply with CE-HTML. After

user interaction via the HTML pages, the service may return a Marlin action token or Marlin licence.

Before accessing the parental control URL specified in this clause, OITF shall obtain user consent to access the web page. When receiving an HTTP request to the parental control URL, the service should respond with an HTML page. This HTML shall comply with CE-HTML.

4.2.6.6 System renewability messages

In the scope of this specification, DTCP and HDCP system renewability messages (SRM) can be transported in a Marlin protected MPEG-2 TS. The signalling and transport of SRM in Marlin protected MPEG-2 TS shall comply with ETSI TS 102 770.

If an OITF supports HDCP output and receives Marlin protected MPEG2-TS format, the OITF shall detect the presence of HDCP system renewability messages and install them, as defined in HDCP.

If an OITF supports DTCP output and receives Marlin protected MPEG2-TS format, the OITF shall detect the presence of DTCP system renewability messages and install them, as defined in DTCP.

4.2.7 Operation of Marlin technologies

4.2.7.1 General

Subclause 4.2.7 specifies the operation of Marlin technologies to support certain type of use cases.

4.2.7.2 Status of Marlin licence support

A usage rule which uses status information (such as count) is supported in the Marlin licence (e.g. burn usage rule by allowing Export action to a certain target system). When the Marlin licence requires status management in the client, the corresponding Marlin licence should also have a 'not after' condition specified in the absolute validity period. The value specified by 'not after' should be no later than 1 month from the issuance of the Marlin licence. For example, when the Marlin licence issued on 24 November 2008 00:00 allows some operation to be performed 3 times, this Marlin licence should only be valid until 24 December 2008 00:00.

4.2.7.3 Subscription support

A CSP function that implements this specification shall support BNS Extended topology for Subscription Nodes as defined in BNSP. It means that the CSP shall support following Marlin protocols for subscription node, which are originally defined as optional functions in BNSP:

– Marlin licence acquisition to bind Marlin licence to subscription node;

– Marlin deregistration from a domain represented by subscription node where a corresponding subscription link shall have the following properties:

  - LinkFrom: personality node or user node;
  - LinkTo: subscription node.

The CSP shall signal this support of the BNS Extended topology by using the mechanism defined in 6.2 of BNSP.

4.2.8 DRM data

4.2.8.1 DRMSystemID

DRMSystemID, used to signal the type of DRM, is defined in IEC 62766-3. DRMSystemID is used in metadata structures, defined in IEC 62766-3, in APIs defined in IEC 62766-5-1 and in protocols defined in IEC 62766-4-1. For Marlin, since the DVB CA_System_ID is assigned as 0x4AF4, the value for the DRMSystemID to signal Marlin shall be set to the following value: "urn:dvb:casystemid:19188". In addition to the DRMSystemID "urn:dvb:casystemid:19188" signaling Marlin, URN "urn:marlin:ms3:1-0" defined in 1.3.1 of Marlin MS3 may be used as a second DRMSystemID to signal that Marlin Simple secure streaming feature is supported.

4.2.8.2 Metadata – DRM control information

A DRM control Information structure to hold DRM dependant control parameters is defined in IEC 62766-3 as an extended element included in content access descriptor, defined in IEC 62766-5-1 and extension of purchaseItem element of BCG and SD&S metadata, defined in IEC 62766-3.

For Marlin protected content, the element of DRMControlInformation shall be mapped as specified in Table 5.

Table 5 – DRMControlInformation mapping for Marlin

Element / Attribute Name	Element / Attribute Mapping for Marlin
DRMControlInformation	
DRMSystemID	Shall be set to the value defined for the Marlin System ID, in 4.2.8.1.
DRMContentID	Shall be set Marlin content ID. For Marlin protected MPEG-2 TS or timespamped MPEG2-TS, the content ID is derived from the socID; together with serviceBaseCID as defined in BBTS.
RightsIssuerURL	Should be set to the RightsIssuerURL present in Marlin protected content formats, defined in 4.2.5 and 4.2.6.
SilentRightsURL	Should be set to the SilentRightsURL present in Marlin protected content formats, defined in 4.2.5 and 4.2.6. When accessing to this SilentRightsURL, Marlin action Token or MIPPVControlMessage may be returned.
PreviewRightsURL	Should be set to the PreviewRightsURL present in Marlin protected content formats, defined in 4.2.5 and 4.2.6.
DoNotRecord	Should be set to the same value as the DNR (do not record) bit in recording control access criteria defined in 4.2.6.3.
DoNotTimeShift	Should be set to the same value as the DNTS (do not time shift) bit in recording control access criteria defined in 4.2.6.3.
DRMGenericData	Placeholder element for which currently no mapping is defined.
DRMPrivateData	DRMPrivateData shall be an instance of a MarlinPrivateDataType structure, see B.2.
mimeType	Shall be set to the mime type of the DRMPrivateData. For Marlin, it shall therefore be set to MIME type of a Marlin licence, see BNSP or to the MIME type of a Marlin Token, see BNSP.

If Marlin Simple secure streaming feature is supported, in addition to the DRMControlInformation structure given in Table 5, a second DRM control Information structure may be present with parameters mapped as specified in Table 6.

Table 6 – DRMControlInformation mapping for Marlin simple secure streaming

Element / Attribute Name	Element / Attribute Mapping for Marlin
DRMControlInformation	
DRMSystemID	Shall be set to the value defined for the Marlin Simple secure streaming feature, in 4.2.8.1.
DRMContentID	Shall be set Marlin content ID. In the case of scheduled content over IP, the content ID is derived from the socID; together with serviceBaseCID as defined in BBTS.
RightsIssuerURL	Placeholder element for which currently no mapping is defined.
SilentRightsURL	Placeholder element for which currently no mapping is defined.
PreviewRightsURL	Placeholder element for which currently no mapping is defined.
DoNotRecord	Should be set to the same value as the DNR (do not record) bit in recording control access criteria defined in 4.2.6.3.
DoNotTimeShift	Should be set to the same value as the DNTS (do not time shift) bit in recording control access criteria defined in 4.2.6.3.
DRMGenericData	Placeholder element for which currently no mapping is defined.
DRMPrivateData	Placeholder element for which currently no mapping is defined.
mimeType	Shall be set to the mime type of the DRMPrivateData. For Marlin Simple secure streaming feature, it shall be set to MIME type of a Marlin Token, Marlin MS3.

Both MarlinPrivateDataType and HexBinaryPrivateDataType extend DRMPrivateDataType, defined in IEC 62766-3; and so the element DRMPrivateData can be substituted by either MarlinPrivateData or HexBinaryPrivateData as defined in Figure 12.

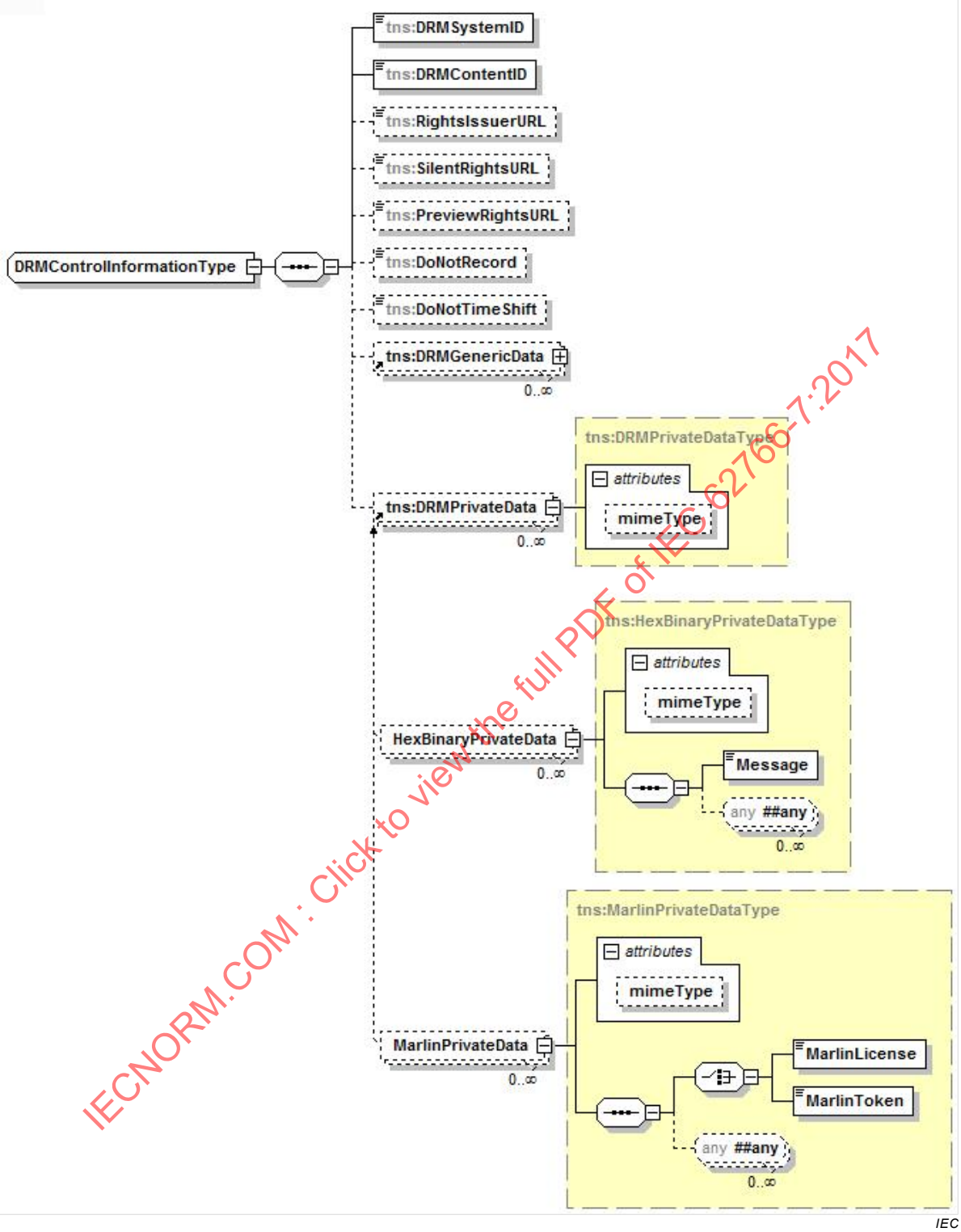

Figure 12 – Outline of DRMControlInformationtype with MarlinPrivateData

The XML schema for the MarlinPrivateDataType is defined in B.2.

Table 7 specifies the format of the Marlin private data structure.

Table 7 – MarlinPrivateData structure

Element / Attribute Name	Element / Attribute description
MarlinPrivateData	

MarlinLicense	A Base64 encoded XML Document containing an instance of a Marlin licence, typically used for channel preview.
MarlinToken	A Base64 encoded XML document containing an instance of a Marlin token, to be used for triggering Marlin protocol.

4.2.8.3 DAE Marlin messages

4.2.8.3.1 General

The CSP shall support receiving the following messages via the sendDRMMessage API defined in 7.6.2 of IEC 62766-5-1:2017:

- Marlin action token, format and mime type defined in BNSP;
- MIPPVControlMessage, format and mime type defined in 4.2.8.3.2;
- Marlin licence, format and mime type defined in BNSP.

For these messages, the DRMSystemID shall be set to the value defined for the Marlin system ID in 4.2.8.1.

4.2.8.3.2 MIPPVControlMessage format

This subclause describes the usage of MIPPVControlMessage, which is used for pay-per-view cases, and defines the message structure of MIPPVControlMessage. MIPPVControlMessage is used in a pay-per-view use case where a large number of users try to acquire a Marlin licence just before a pay-per-view programme begins. To avoid such simultaneous accesses to the CSP-T (DRM server), a service can apply MIPPVControlMessage which includes common Marlin licence (i.e. common for OITFs), Marlin action token, and Marlin licence acquisition timing information. These three data items are used as follows in a typical pay-per-view case:

1) When an OITF function (e.g. DAE application) receives a MIPPVControlMessage, the OITF Function (e.g. DAE application) passes the MIPPVControlMessage to CSP. CSP uses common Marlin licence embedded in MIPPVControlMessage to play a pay per view programme until it gets the Marlin licence that is valid only for that OITF. Since a common Marlin licence is valid for any OITF, the common Marlin licence expires during the pay per view programme.
2) By following the timing information in MIPPVControlMessage, the client executes the Marlin action token in MIPPVControlMessage, and then it acquires the Marlin licence for the OITF.
3) After acquisition of the Marlin licence for the OITF, the OITF can play the pay-per-view programme even after the expiration of the common Marlin licence.

The MIPPVControlMessage, as shown in Figure 13, includes Marlin licence, which is common among clients, Marlin action token, which is used to acquire the unique Marlin licence, and timing information, which indicates the timing to initiate Marlin licence acquisition protocols.

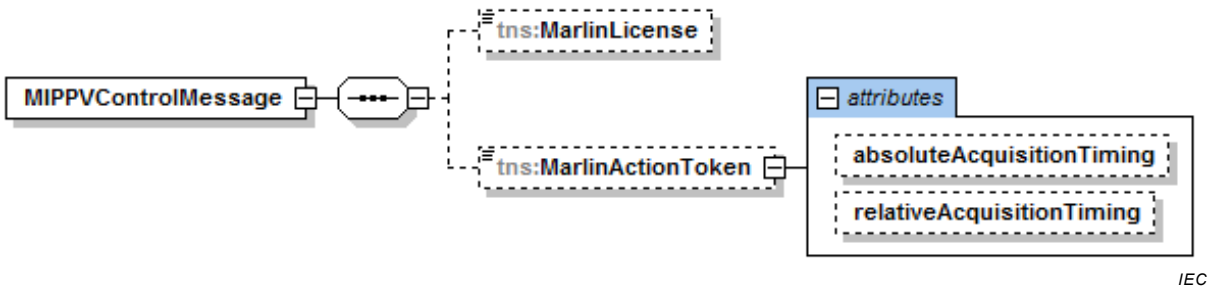

Figure 13 – Outline of MIPPVControlMessage

The XML schema for the MIPPVControlMessage is defined in Clause B.2.

Each element has the semantics as shown in Table 8.

Table 8 – MIPPVControlMessage format

Element / Attribute Name	Element / Attribute description
MIPPVControlMessage	
MarlinLicense	A Base64 encoded XML Document containing an instance of a Marlin licence.
MarlinActionToken	A Base64 encoded XML document containing an instance of a Marlin action token.
absoluteAcquisitionTiming	Licence acquisition timing in absolute time
relativeAcquisitionTiming	Licence acquisition timing in relative time from the start of the content

MIME type of MIPPVControlMessage is defined as follows:

```
application/vnd.oipf.mippvcontrolmessage+xml
```

4.3 Gateway-centric approach

4.3.1 General

Subclause 4.3 specifies the functionality for the OIPF Gateway-centric approach to content and service protection. It elaborates on the CSPG functional entity and UNIS-CSP-G, HNI-CSP, HNI-AGC reference points introduced in the functional architecture described in Annex B of IEC 62766-1:2017.

The gateway-centric approach provides a content protection solution whereby the service provider is able to deploy any preferred protection system to deliver protected content to the user, but the delivery protection is terminated in the CSP Gateway (CSPG) function and a common local protection solution is used to maintain protection of the content on the final link between the CSPG and the OITF. CSPG are specified for CI+ (4.3.4) and for DTCP-IP (4.3.5).

It is permitted that the CSPG and OITF functional entities are implemented in the same device. In this case, the CA/DRM system used for content delivery will be terminated directly at the terminal device. Also, the OITF-CSPG communication is a device-internal interface that does not need to conform to the HNI-CSP interface, i.e. there is a "virtual" CSPG embedded in the terminal device. This is conceptually equivalent to the implementation of any chosen CA/DRM in the device hosting the OITF. This approach is documented informatively in Annex F.

4.3.2 Capabilities

The DAE shall signal which CA_System_ID values ISO/IEC 13818-1, and optionally the type of CSP gateway, are supported in the OITF including those available via gateway-centric approach as defined in Clause 9 of IEC 62766-5-1:2017.

The list of supported CA_System_ID values and optionally the type of CSP gateway shall also be retrieved by the service platform provider using one of the following methods:

- the OITF remote management interface as defined in IEC 62766-4-1;
- as part of the service provider discovery subscribe message as defined in IEC 62766-4-1.

4.3.3 CSPG-DAE interface

When a DAE application uses the DRM agent API and event, sendDRMMessage and onDRMMessageResult, defined in 7.6.2 of IEC 62766-5-1:2017, to handle a DRM message for a given CA_System_ID that is supported by a CSPG, the OITF shall forward these messages to the appropriate function, CSP or CSPG.

When protected content is used (played, time-shifted, recorded) from a DAE application, the OITF shall forward events (no rights or parental control locking) from the CSPG to the DAE application via the A/V or video/broadcast object. The DRM events onDRMRightsError, onParentalRatingChange and onParentalRatingError are defined in 7.13.6, 7.13.7, 7.14.8 and 7.14.7 of IEC 62766-5-1:2017. The DRM events (no rights or parental control locking) shall include the CA_System_ID information.

4.3.4 CI+ based gateway

4.3.4.1 General

All normative statements in 4.3.4 apply only in case the CI+ based gateway-centric approach is supported.

NOTE The criteria that determine under which circumstances the CI+ based gateway-centric approach is implemented are out of the scope of the present document.

4.3.4.2 Overview

The CSPG-CI+ is an optional entity handling security for the OITF. It shall make any specific content protection solution transparent to the OITF. This is achieved by the use of a standard secure channel between the OITF and the CSPG-CI+. The CSPG-CI+ acts as a bridge between a specific protection solution and one standard secure channel. Once the OITF and the CSPG-CI+ are mutually authenticated, the OITF is seamlessly able to receive any content that was initially secured by the different content protection solutions that the CSPG-CI+ handles. The incoming stream to the CSPG-CI+ is associated with the generic media format label "PF", as defined in IEC 62766-2-1.

The protected content stream is sent from the OITF to the CSPG-CI+ and then sent back to the OITF protected in such a way that only authenticated OITF can gain access to it. Incoming and outgoing streams format are based on MPEG-2 transport stream. Protected file formats based on MP4 file format (i.e. OMA (P)DCF and Marlin IPMP) are not supported.

The definition of the interfaces is based on the DVB CI specification (EN 50221 and TS 101 699) and the CI+ specification (CI Plus V1.3).

Figure 14 presents an overview of the functions and interfaces of the CSPG-CI+.

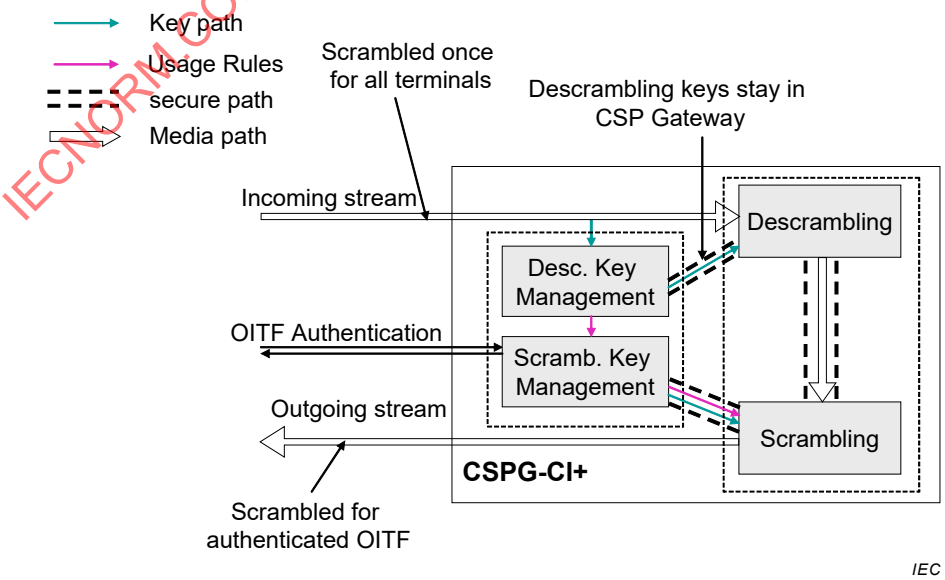

Figure 14 – CSPG-CI+ overview

In order to provide seamless behaviour to the end user (e.g. for service selection operation), the incoming stream in Figure 14 shall be delivered through the UNIT-17 reference point as

for the terminal-centric approach. Figure 15 describes CSPG-CI+ in the home network context and maps interfaces from Figure 14 to home network interfaces defined in Annex B of IEC 62766-1:2017.

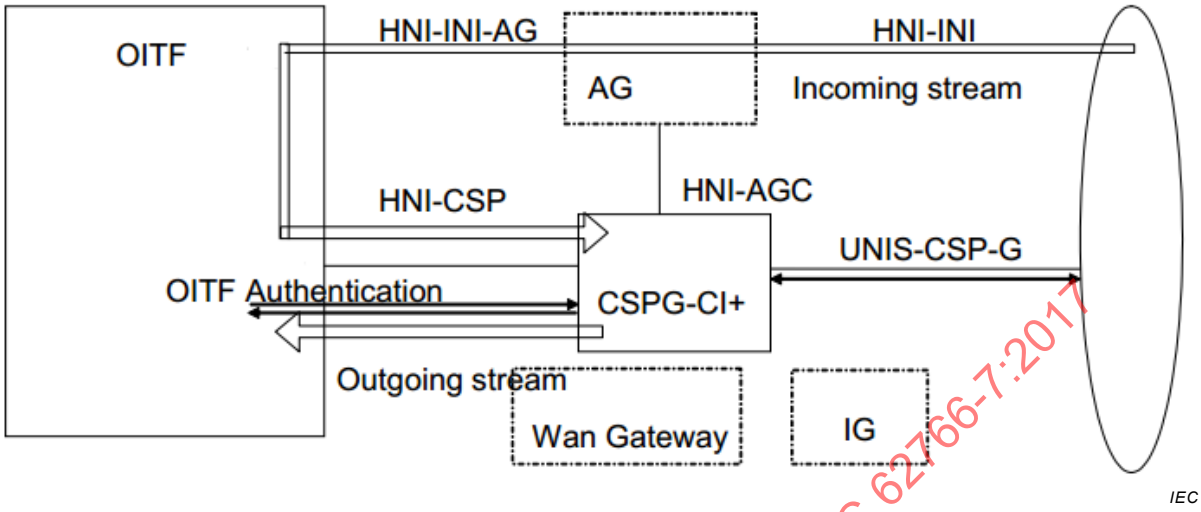

Figure 15 – CSPG-CI+ context

The OITF and CSPG-CI+ shall comply with CI+ specifications (CI Plus V1.3).

4.3.4.3 CSPG-CI+ connectivity

The physical interface is based on a PCMCIA slot as specified by the DVB-CI specification (EN 50221 and TS 101 699) and the CI+ specification (CI Plus V1.3).

4.3.4.4 CSPG-CI+ discovery

The CSPG-CI+ discovery shall be performed at OITF start-up and CSPG-CI+ initialization. The setup of the session to the CI Plus V1.3 Specific application Support (SAS) resource and the connection to the Open IPTV Forum private application are described in 4.3.4.5.1.2. A successful connection means that a CSPG-CI+ has been discovered.

4.3.4.5 Residential network interfaces

4.3.4.5.1 HNI-CSP

4.3.4.5.1.1 General

HNI-CSP is an interface to exchange control information and media between the CSPG-CI+ and the OITF.

4.3.4.5.1.2 Control channel

####### 4.3.4.5.1.2.1 General

OITF controls the CSPG-CI+ using resources defined in EN 50221 and TS 101 699 as well as resources as defined in Clause 11 of CI Plus V1.3.

OITF and CSPG-CI+ shall use the SAS resource, defined in 11.4 of CI Plus V1.3, to handle messages as specified in 4.3.4.5.1.2.

The OITF shall send a ***SAS_connect_rqst()*** APDU CI Plus V1.3 to the CSPG-CI+ with the specific Open IPTV forum private_host_application_ID defined in Table 9. The CSPG-CI+ shall acknowledge the connection by sending back a ***SAS_connect_cnf()*** APDU CI Plus V1.3. The highest private_host_application_ID value known by the host shall be tried first. If the

SAS_session_status returned by the ***SAS_connect_cnf()*** APDU is not 0x00 ("Connection established") then a lower value shall be tried and so on until success.

Table 9 – OIPF private_host_application_ID

private_host_application_ID	Value (64 bits)
OIPF_APPLICATION_ID for legacy versions	0x0108113101190000
OIPF_APPLICATION_ID for version compliant with the present part	0x0108113101190001

Then any further exchanges between the OITF and the CSPG-CI+ are completed through the use of the ***SAS_async_msg()*** APDU. Syntax of this APDU is reminded in Table 10.

Table 10 – *SAS_async_msg*() APDU syntax

Syntax	No. of Bits	Mnemonic
SAS_async_msg() {		
SAS_async_msg_tag	24	uimsbf
length_field()		
message_nb	8	uimsbf
message_length	16	uimsbf
for (i=0; i<message_length; i++) {		
message_byte	8	uimsbf
}		
}		

4.3.4.5.1.2.2 Specific messages

The OITF and CSPG-CI+ shall support the messages listed in Table 12. For each of the messages the message_byte payload takes the generic syntax given in Table 11. The message data may be broken into a number of records containing the same or different types of data identified by the datatype_id.

Table 11 – Generic message_byte() syntax

Syntax	No. of Bits	Mnemonic
message_byte() {		
command_id	8	uimsbf
ca_system_id	16	uimsbf
transaction_id	32	uimsbf
send_datatype_nbr	8	uimsbf
for (i=0; i<send_datatype_nbr; i++) {		
datatype_id	8	uimsbf
datatype_length	16	uimsbf

Syntax	No. of Bits	Mnemonic
data_type() } }	8 * datatype_length	bslbf

command_id: 8-bit value that identifies the message. The values are defined in Table 12.

ca_system_id: 16-bit integer that identifies the CA system being queried.

transaction_id: 32-bit value, generated by the OITF, provided in a message to the CSPG-CI+ that will be returned in any corresponding reply message from the CSPG-CI+. The transaction_id allows the OITF to match the CSPG-CI+'s replies with the corresponding requests. The OITF should increment the value, modulo 2^{32}, with every message it sends. The transaction_id should be ignored in messages sent spontaneously (events) by the CSPG-CI+ (i.e. rights_info, parental_control_info, system_info).

send_datatype_nbr: 8-bit integer that gives the number of data type items included in the message.

datatype_id: 8-bit integer that identifies the type of the data contained in the data type loop. The values are defined in Table 13.

datatype_length: 16-bit integer that gives the length of the data_type() field in bytes.

data_type: data type payload. The data type loop shall only contain the specified data type, but may contain multiple records of the same type; the number of records may be determined by computation of the datatype_length field.

Table 12 – OIPF specific messages and command_id values

Message	command_id value (hexadecimal)	Direction	
		OITF	CSPG-CI+
send_msg	0x01	→	
reply_msg	0x02	←	
parental_control_info	0x03	←	
rights_info	0x04	←	
system_info	0x05	←	
can_play_content_req	0x06	→	
can_play_content_reply	0x07	←	
can_record_content_req	0x08	→	
can_record_content_reply	0x09	←	
(reserved)	0x0A-0x7F		
(user defined)	0x80-0xFF		

Table 13 – OIPF specific datatype_id values

Data type	datatype_id value (hexadecimal)
oipf_ca_vendor_specific_information	0x01

oipf_country_code	0x02
oipf_parental_control_url	0x03
oipf_rating_type	0x04
oipf_rating_value	0x05
oipf_rights_issuer_url	0x06
oipf_access_status	0x07
oipf_status	0x08
oipf_drm_private_data	0x09
oipf_can_play_status	0x0A
oipf_can_record_status	0x0B
(reserved)	0x0C-0x7F
(user defined)	0x80-0xFF

4.3.4.5.1.2.3 Mapping of messages to DAE API or events

The OITF shall map the specific messages listed in Table 12 to DAE API or events as described in Table 14:

Table 14 – Mapping to DAE API or events

Message	DAE API or event
send_msg	sendDRMMessage
reply_msg	onDRMMessageResult
parental_control_info	onParentalRatingChange, onParentalRatingError
rights_info	onDRMRightsError
system_info	onDRMSystemMessage
can_play_content_req	canPlayContent
can_play_content_reply	canPlayContent
can_record_content_req	canRecordContent
can_record_content_reply	canRecordContent

The DRMSystemID attribute in DAE API or events are mapped to the ca_system_id field in the SAS_async_msg APDU. The ca_system_id field is filled by extracting the numeric value from the DRMSystemID string, such that "urn:dvb:casystemid:" is removed and the remaining number is converted from a string to a 16-bit integer. The DRMSystemId is built by prefixing the 16-bit integer converted to a decimal number string with "urn:dvb:casystemid:" as described in IEC 62766-3.

Private data are array of bytes encoded for DAE API or events attributes in a string using a hexadecimal representation, as defined for xs:hexBinary type used in XML schemas. In CI+ SAS_async_msg fields, the private data is encoded in bytes.

Precise mapping of DAE API or events and attributes are described in the following clauses.

4.3.4.5.1.2.4 send_msg

A native application or DAE application should use the *send_msg* message to provide DRM specific messages to the CSPG-CI+.

When requested by either a native or DAE application, the OITF shall send the *send_msg* message to the CSPG-CI+ to exchange DRM messages. Examples of usage are:

- Service provider handles the purchase of content at the server side and then uses the *send_msg* message via a DAE application to ask the CSPG-CI+ to retrieve the associated licence.
- Service provider sends the *send_msg* message via a DAE application to the CSPG-CI+ to force the CSPG-CI+ to purchase a specific programme.

The data types for the *send_msg* message are listed in Table 15.

Table 15 – *send_msg* message data types

Syntax	Occurrence number
oipf_ca_vendor_specific_information	1

oipf_ca_vendor_specific_information: vendor-specific information. The maximum length is 65 000 bytes.

When a DAE application calls the sendDRMMessage API with msgType set to the MIME type "application/vnd.oipf.cspg-hexbinary" and a DRMSystemId set to a ca system id supported by the CSPG-CI+, the OITF shall send a *send_msg* message to the CSPG-CI+.

The prototype of the sendDRMMessage API defined in IEC 62766-5-1 is recalled here:

String sendDRMMessage(String msgType, string msg, string DRMSystemID)

The OITF shall map the attributes of the called DAE API as follows:

- the DRMSystemId attribute is mapped to the ca_system_id field as described in 4.3.4.5.1.2.3.
- the private data in msg attribute encoded in a string using a hexadecimal representation, as defined for xs:hexBinary type used in XML schemas is decoded to bytes before passing it to *send_msg* message in the oipf_ca_vendor_specific_information field as described in 4.3.4.5.1.2.3.

4.3.4.5.1.2.5 reply_msg

The CSPG-CI+ shall send the *reply_msg* message to the OITF to provide the status of the *send_msg* message.

The data types for the *reply_msg* message are listed in Table 16.

Table 16 – *reply_msg* message data types

Syntax	Occurrence number
oipf_status	1
oipf_ca_vendor_specific_information	0..1

oipf_status: if equal to 0, the *send_msg* message has been successfully handled by the CSPG-CI+ and a oipf_ca_vendor_specific_information may be available.

- If equal to 1, the *send_msg* message failed because an unspecified error occurred.
- If equal to 2, the *send_msg* message failed because the CSPG-CI+ was unable to complete the necessary computations in the time allotted.

- If equal to 3, the *send_msg* message failed because oipf_ca_vendor_specific_information has a wrong format.
- If equal to 4, the *send_msg* message failed because user consent is needed for that action.
- If equal to 5, the *send_msg* message failed because the specified CA system in ca_system_id is unknown.

Unspecified status values should be considered as, message failed because an unspecified error occurs.

oipf_ca_vendor_specific_information: vendor specific information. The maximum length is 65 000 bytes.

NOTE The service provider should not provide a DRM message in metadata (BCG, SD&S, CAD) and expect a response in oipf_ca_vendor_specific_information of ***reply_msg*** message, if these metadata are handled by a native application. The native application sending the DRM message to the CSPG-CI+ will not know how to handle a response.

When receiving a *reply_msg* message with a transaction_id mapping to a send_msg message issued from a DAE application call to sendDRMMessage, the OITF shall issue an onDRMMessageResult event to the DAE application

The prototype of the onDRMMessageResult event defined in IEC 62766-5-1 is recalled here:

function onDRMMessageResult(String msgID, string resultMsg, Integer resultCode)

The OITF shall set the attributes of the issued DAE event as follows:

- the msgID attribute set to the value returned to the called sendDRMMessage;
- the resultCode attribute is mapped to oipf_status field as shown in Table 17;

Table 17 – resultCode and oipf_status mapping

oipf_status field	Description	resultCode attribute	Description
0	Succesful	0	Successful
1	Unspecified error	1	Unknown error
2	Out of time	2	Cannot process request
3	Wrong format	6	Wrong format
4	User Consent Needed	4	User Consent Needed
5	Unknown DRM system	5	Unknown DRM system

- the resultMsg attribute set to the private data in oipf_ca_vendor_specific_information encoded in a string as described in 4.3.4.5.1.2.3.

4.3.4.5.1.2.6 parental_control_info

The CSPG-CI+ shall send a *parental_control_info* message to advise the OITF whenever the selected programme's rating changes. If the new 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 programme is not descrambled anymore. If the new rating meets the parental rating criterion (e.g. rating is under a certain threshold for a rating system that is ordered from lower viewer age to higher viewer age), the programme is descrambled again.

The data types for the *parental_control_info* message are listed in Table 18.

Table 18 – *parental_control_info* message data types

Syntax	Occurrence number
oipf_access_status	1
oipf_rating_type	1
oipf_rating_value	1
oipf_country_code	0..*n*
oipf_parental_control_url	0..1

oipf_access_status: if equal to 0, the programme is no longer being descrambled, access conditions to the programme are no longer being met. A oipf_parental_control_url may be provided. If equal to 1, the programme is descrambled again.

oipf_rating_type: rating_type as defined in the parental_rating access_criteria_descriptor in IEC 62455.

oipf_rating_value: 1-byte rating_value as defined in the parental_rating access_criteria_descriptor in IEC 62455.

oipf_country_code: 2-byte optional country_codes as defined in the parental_rating access_criteria_descriptor in IEC 62455.

oipf_parental_control_url: optional URL for connecting to the service provider, for unlocking the parental control.

The OITF shall support at least the parental rating system identified by the oipf_rating_type 0, which maps to the parental rating system in DVB Systems, specified in EN 300 468.

If an oipf_parental_control_url is provided and the event is raised to a native application, the native application should launch the DAE with the oipf_parental_control_url that might allow to unlock parental control in the CSPG-CI+.

When the *parental_control_info* message is received and a DAE application is launched, the OITF shall issue the relevant event to the DAE application:

- onParentalRatingChange event, if the parental rating system specified by the oipf_rating_type is supported by the OITF.
- onParentalRatingError event, if the parental rating system specified by the oipf_rating_type is not supported by the OITF.

The prototype of the onParentalRatingChange and onParentalRatingError events defined in IEC 62766-5-1 are recalled here:

function onParentalRatingChange(String contentID, ParentalRatingCollection ratings, String DRMSystemID, Boolean blocked);

function onParentalRatingError(String contentID, ParentalRatingCollection ratings, String DRMSystemID).

The OITF shall set the attributes of the issued event as follows.

– The contentId attribute is set to null or undefined.

– The ratings attribute (ParentalRatingCollection object) is filled out with a single ParentalRating object. This ParentalRating object is initialized as follows.
  - If the oipf_rating_type is supported by the OITF, the oipf_rating_type field is mapped into the scheme property of the ParentalRating object. If the oipf_rating_type is not supported by the OITF, the scheme is set to null or undefined.
  - The oipf_rating_value field is mapped into the value property of the ParentalRating object. If the oipf_rating_type is supported by the OITF, the name property of the ParentalRating object is filled with the string representation of the parental rating value. If the oipf_rating_type is not supported by the OITF, the name property is set to null or undefined.
  - The oipf_country_code field is mapped into the region property of the ParentalRating object
– The DRMSystemID attribute is mapped to the ca_system_id field as defined in 4.3.4.5.1.2.3.
– The blocked attribute is mapped to oipf_access_status as shown in Table 19.

Table 19 – oipf_access_status field and blocked attribute mapping

oipf_access_status field	Description	Blocked attribute	Description
0	Programme not descrambled	True	Content blocked
1	Programme descrambled	False	Content not blocked

A DAE application should use a proprietary method using sendDRMMessage to unlock parental control.

If the programme is no longer being descrambled (oipf_access_status=0), the native or DAE application should not stop playing the programme, as the programme may become descrambled again later (access criteria change, parental unlocking, etc.).

4.3.4.5.1.2.7 rights_info

The CSPG-CI+ shall send a *rights_info* message to advise the OITF that access conditions or rights changed and that the CSPG-CI+ is no longer able or is able again to descramble all requested elementary streams. Once this message is received and if a DAE application is launched, the OITF shall send the relevant event onDRMRightsError, as defined in 7.13.7 and 7.14.7 IEC 62766-5-1:2017, to the DAE application.

If the programme is descrambled again, the OITF should display the programme again. If the programme is no longer being descrambled, the OITF may decide to stop the programme and should use the oipf_rights_issuer_url, which may provide for the CSPG-CI+ information to let it retrieve missing rights.

The data types for the *rights_info* message are listed in Table 20.

Table 20 – *rights_info* message data types

Syntax	Occurrence number
oipf_access_status	1
oipf_rights_issuer_url	0..1

oipf_access_status: if equal to 0, the programme is no longer being descrambled; access conditions to the programme are no longer being met. An oipf_rights_issuer_url may be

provided.
If equal to 1, the programme is descrambled again.

oipf_rights_issuer_url: optional URL for connecting to the service provider.

The prototype of the onDRMRightsError event defined in IEC 62766-5-1 is recalled here:

function onDRMRightsError(Integer errorState, string contentID, string DRMSystemID, string rightsIssuerURL)

When the *right_info* message is received and a DAE application is launched, the OITF shall issue the *onDRMRightsError* event to the DAE application.

The OITF shall set the attributes of the issued event as follows.

- The errorState attribute is mapped to oipf_access_status field as shown in Table 21.

Table 21 – oipf_access_status field and errorStatte attribute mapping

oipf_access_status field	Description	errorState attribute	Description
0	Programme not descrambled	0	No licence
1	Programme descrambled	2	Valid licence

- The contentId attribute is set to null or undefined.
- The DRMSystemID attribute is mapped to the ca_system_id field as defined in 4.3.4.5.1.2.3.
- The rightsIssuerURL is mapped to oipf_rights_issuer_url if this field is present. If the oipf_rights_issuer_url is not present, rightIssuerURL is set to null or undefined.

If the programme is no longer being descrambled (oipf_access_status=0), the native or DAE application should not stop playing the programme, as the programme may become descrambled again later (access criteria change, rights update etc).

4.3.4.5.1.2.8 system_info

The CSPG-CI+ shall send a *system_info* message to advise the OITF of any DRM related event, for example the removal of a smartcard. Once this message is received and if a DAE application is launched, the OIPF shall send the relevant event onDRMSystemMessage, as defined in 7.6.2 of IEC 62766-5-1:2017, to the DAE application.

The data types for the *system_info* message are listed in Table 22.

Table 22 – *system_info* message data types

Syntax	Occurrence number
oipf_ca_vendor_specific_information	1

oipf_ca_vendor_specific_information: Vendor specific information. The maximum length is 65 000 bytes.

When the *system_info* message is received and if a DAE application is launched, the OITF shall issue the onDRMSystemMessage event to the DAE application.

The prototype of the onDRMSystemMessage event defined in IEC 62766-5-1 is recalled here:

function onDRMSystemMessage(String DRMSystemID, string msg)

The OITF shall set the attributes of the issued event as follows:

- The DRMSystemID attribute is mapped to the ca_system_id field as defined in 4.3.4.5.1.2.3.
- The msg attribute set to the private data in oipf_ca_vendor_specific_information encoded in a string as described in 4.3.4.5.1.2.3.

4.3.4.5.1.2.9 can_play_content_req and can_play_content_reply

The following messages are supported only for a private_host_application_ID greater or equal to 0x0108113101190001.

When requested by either a native or DAE application, the OITF shall send the *can_play_content_req* message to the CSPG-CI+ to check the local availability of a valid licence for playing content protected by a DRM integrated in the CSPG-CI+.

The data types for the *can_play_content_req* message are listed in Table 23.

Table 23 – can_play_content_req message data types

Syntax	Occurrence number
oipf_drm_private_data	1

oipf_drm_private_data: DRM proprietary private data. The maximum length is 16 384 bytes.

When a DAE application calls the canPlayContent API with a DRMSystemId set to a ca system id supported by the CSPG-CI+, the OITF shall send a *can_play_content_req* message to the CSPG-CI+ and wait for a *can_play_content_reply* message from the CSPG-CI+.

The data types for the *can_play_content_reply* message are listed in Table 24.

Table 24 – *can_play_content_reply* message data types

Syntax	Occurrence number
`oipf_can_play_status`	`1`

oipf_can_play_status: if equal to 1, the CSPG_CI+ has a valid licence available that may allow playing the content associated to the DRM metadata. If equal to 0, the CSPG-CI+ has no licence available.

When the CSPG-CI+ receives a *can_play_content_req* message, then it shall check whether it owns a valid licence for playing the protected content which oipf_drm_private_data relates to and reply to the OITF with a *can_play_content_reply* message with an oipf_can_play_status that indicates whether or not the CSPG-CI+ has a valid licence available.

The prototype of the canPlayContent API defined in IEC 62766-5-1 is recalled here:

Boolean canPlayContent (String DRMPrivateData, string DRMSystemID)

The OITF shall map the attributes of the called DAE API as follows:

- The DRMSystemId attribute is mapped to the ca_system_id field as described in 4.3.4.5.1.2.3.
- The DRMPrivateData is mapped to oipf_drm_private_data.
- The returned Boolean is mapped from the oipf_can_play_status.

4.3.4.5.1.2.10 can_record_content_req and can_record_content_reply

The following messages are supported only for a private_host_application_ID greater or equal to 0x0108113101190001.

When requested by either a native or DAE application, the OITF shall send the *can_record_content_req* message to the CSPG-CI+ to check the local availability of a valid licence for recording a content protected by a DRM integrated in the CSPG-CI+.

The data types for the ***can_record_content_req*** message are listed in Table 25.

Table 25 – *can_record_content_req* message data types

Syntax	Occurrence number
`oipf_drm_private_data`	1

oipf_drm_private_data: DRM proprietary private data. The maximum length is 16 384 bytes.

When a DAE application calls the canRecordContent API with a DRMSystemId set to a ca system id supported by the CSPG-CI+, the OITF shall send a *can_record_content_req* message to the CSPG-CI+ and wait for a *can_record_content_reply* message from the CSPG-CI+.

The data types for the *can_record_content_reply* message are listed in Table 26.

Table 26 – *can_record_content_reply* message data types

Syntax	Occurrence number
`oipf_can_record_status`	1

oipf_can_record_status: if equal to 1, the CSPG_CI+ has a valid licence available that may allow recording the content associated to the DRM metadata. If equal to 0, the CSPG-CI+ has no licence available.

When the CSPG-CI+ receives a *can_record_content_req* message, then it shall check whether it owns a valid licence for recording the protected content that oipf_drm_private_data relates to and reply to the OITF with a *can_record_content_reply* message with an oipf_can_record_status that indicates whether or not the CSPG-CI+ has a valid licence available.

The prototype of the canRecordContent API defined in IEC 62766-5-1 is recalled here:

Boolean canRecordContent (String DRMPrivateData, string DRMSystemID)

The OITF shall map the attributes of the called DAE API as follows:

- the DRMSystemId attribute is mapped to the ca_system_id field as described in 4.3.4.5.1.2.3;
- the DRMPrivateData is mapped to oipf_drm_private_data;

- the returned Boolean is mapped from the oipf_can_record_status.

4.3.4.5.1.3 Media channel

Media are exchanged as defined in the CI Plus V1.3 specification.

For streamed content, in either scheduled content case or content on demand case, the transmission of the protected content from the OITF to the CSPG-CI+ is performed by using MPEG-2 Transport stream.

For downloaded content, the OITF shall stream the content to the CSPG-CI+ at consumption time.

4.3.4.5.2 UNIS-CSP-G

This reference point is used to exchange with the network. Since the CSPG-CI+ does not have network connectivity, it uses the OITF to reach the network.

4.3.4.5.2.1 Low-speed communication resource

The OITF shall support the low-speed communications resource with IP extension as specified in 14.2 of CI Plus V1.3.

4.3.4.5.3 HNI-AGC

In case there is an application gateway, control flow is handled through the OITF, via HNI-INI-AG and HNI-CSP control channel. The HNI-AGC reference point introduced in Annex B of IEC 62766-1 is not used.

4.3.4.6 Provider network interfaces

The scrambler on network side shall have an interface with the CSP-G server functional entity so that ECMs can be provided during content encryption. This interface is not described in the present specification.

4.3.4.7 Protected streaming and file formats

4.3.4.7.1 General

The CSPG-CI+ supports the MPEG-2 transport stream format. The CSPG-CI+ supports the MPEG-2 transport stream format. The generically protected incoming transport stream to the CSPG-CI+ is associated with the media format label "PF", as defined in IEC 62766-2-1.

The CSPG-CI+ does not support the time stamped MPEG-2 Transport stream format.

However, in the case content is received by the OITF under a time stamped MPEG-2 transport stream format and if the OITF supports the unprotected time stamped MPEG-2 TS format:

- the OITF may first use the timestamps provided through the 4 additional bytes of each time stamped MPEG-2 TS packet as defined in IEC 62766-2-1 to eliminate network jitter and restore the original packet arrival times before sending the content to the CSPG-CI+; and
- the OITF shall remove the 4 additional bytes from each time stamped MPEG-2 TS packet as defined in IEC 62766-2-1 before sending the content to the CSPG-CI+.

If the OITF does not support the unprotected time stamped MPEG-2 TS format, the support of the above two operations is optional.

4.3.4.7.2 Protection of MPEG-2 transport streams

MPEG-2 transport stream can be streamed or downloaded. Based on the CA_descriptor found in the PMT table, the OITF knows if it can handle the stream or if it has to send it to the CSPG-CI+.

If the CA_descriptor found in the PMT is a Marlin CA_descriptor (with CA_system_ID value assigned for Marlin) and the terminal-centric approach is supported by the OITF, then the OITF shall manage the content with the CSP function described in 4.2.

If the CA_descriptor found in the PMT is a Marlin CA_descriptor and the terminal-centric approach is not supported by the OITF, then the OITF shall ignore it unless Marlin is supported by a CSPG-CI+, in which case the OITF shall provide the protected content to the relevant CSPG-CI+.

If the CA_descriptor found in the PMT is not a Marlin CA_descriptor, then the OITF shall compare the CA_system_ID value with the CA_system_ID supported by the CSPG-CI+. A CSPG-CI+ may support more than one CA_system_ID. If a CA_system_ID value matches, then the OITF shall provide the protected content to the CSPG-CI+. In case several CSPG-CI+ gateways are connected to the OITF, the OITF shall provide the protected content to only one CSPG-CI+.

If there are several CA_descriptors in the PMT, i.e. referring to different content protection systems (Marlin and/or those offered by the CSPG-CI+ gateways), and if the user is already granted with a valid right or licence through one of these content protection systems, the OITF shall select the corresponding content protection system as a priority.

NOTE If simulcrypting with the terminal-centric solution is desired, the algorithm used for content encryption in the gateway-centric approach has to be the same as for the terminal-centric approach.

The scrambling algorithm shall be signalled in the PMT at programme loop level by the scrambling_descriptor specified in EN 300 468. Within the scrambling_descriptor, the algorithm is specified by the scrambling_mode field. The scrambling_modes referenced by the present document are listed in Table 27.

Table 27 – Scrambling modes

scrambling_mode	Description
0x01	DVB-CSA1
0x02	DVB-CSA2
0x70	AES 128-bit key using the Cipher Block Chaining (CBC) encryption mode with the IV setting and the residual termination block process as specified in ATIS-0800006.

4.3.4.7.3 Downloaded content usage

Downloaded content shall be stored locally as it is received by the OITF not going through the CSPG-CI+.

Downloaded content shall be provided to the CSPG-CI+ at consumption time only. Consequently, any conversion e.g. from a time stamped MPEG-2 TS as defined in IEC 62766-2-1 to a non-time-stamped TS is performed at consumption time as well.

4.3.4.8 Personal video recorder

PVR functionality is supported by using URI (Usage Rule Information) as defined in 5.7 of CI Plus V1.3.

When the OITF is asked to store content, it shall send the content to CSPG-CI+. The content is returned from CSPG-CI+ and recorded in accordance with the URI associated with the content.

4.3.4.9 Time shifting

Time shifting functionality is supported by using URI (usage rule information) as defined in 5.7 of CI Plus V1.3.

When the OITF is asked to time shift content, it shall store the content returned from CSPG-CI+ before rendering in accordance with the URI associated to the content.

4.3.4.10 CI+ specification usage

4.3.4.10.1 Module deployment

As the network offered in the OIPF context is a bi-directional communication channel, the optional registered service mode (RSM) in the CI+ specification CI Plus V1.3 is recommended in the CSP specification. The RSM should be supported by CSPG-CI+.

4.3.4.10.2 Host service shunning

As no DVB-CI backward compatibility is needed, the OITF shall make the CSPG-CI+ operate in a CI+ mode CI Plus V1.3 only (thus preventing CSPG-CI+ gateways from operating with the unencrypted DVB-CI link). CI+ protected service signalling defined in 10.1 of CI Plus V1.3 is not used.

4.3.4.11 DRM data

4.3.4.11.1 DRMSystemID

DRMSystemID, used to signal the type of DRM, is defined in IEC 62766-3. DRMSystemID is used in metadata structures in APIs defined in IEC 62766-5-1 and in protocols defined in IEC 62766-4-1. For CSPG-CI+, the DVB CA_System_ID in DRMSystemID shall be the one of the specific content protection solution in the CSPG-CI+.

4.3.4.11.2 Metadata – DRM control information

A DRM control information structure to hold DRM dependant control parameters is defined in IEC 62766-3 as an extended element included in content access descriptor, defined in IEC 62766-5-1 and extension of purchaseItem element of BCG and SD&S metadata, defined in IEC 62766-3.

For specifically protected content, the element of DRMControlInformation shall be mapped as specified in Table 28.

Table 28 – DRMControlInformation mapping for CSPG-CI+

Element / Attribute name	Element / Attribute mapping for CSPG-CI+
DRMControlInformation	
DRMSystemID	Shall be set to the value defined for the specific protection system in the CSPG-CI+, in 4.3.4.11.1
DRMContentID	Vendor specific information.
RightsIssuerURL	Should be set to the RightsIssuerURL which is provided in the ***rights_info*** message defined in 4.3.4.5.1.2.7.
SilentRightsURL	May be set to an URL allowing retrieval of a message to be forwarded to the CSPG-CI+ in order to silently get updated rights. The MIME type or the HTTP response shall be "application/vnd.oipf.cspg-hexbinary" and the body of the HTTP response shall be a hexadecimal string as described in 4.3.4.5.1.2.3.

PreviewRightsURL	May be set to an URL allowing retrieval of a message to be forwarded to the CSPG-CI+ in order to get preview rights. The MIME type or the HTTP response shall be "application/vnd.oipf.cspg-hexbinary" and the body of the HTTP response shall be a hexadecimal string as described in 4.3.4.5.1.2.3.
DoNotRecord	Vendor specific mapping
DoNotTimeShift	Vendor specific mapping
DRMPrivateData	DRMPrivateData structure shall be substituted by the HexBinaryPrivateData structure.
mimeType	Shall be set to the mime type of the DRMPrivateData. For CSPG-CI+, it shall therefore be set to the following MIME type: "application/vnd.oipf.cspg-hexbinary".

Both MarlinPrivateDataType and HexBinaryPrivateDataType extend DRMPrivateDataType, which is defined in IEC 62766-3, and so the element DRMPrivateData can be substituted by either MarlinPrivateData or HexBinaryPrivateData as described in DRMControlInformation outline in Figure 12.

The syntax of the HexBinaryPrivateData structure is shown in Table 29. The XML schema for HexBinaryPrivateData is defined in B.4.

Table 29 – HexBinaryPrivateData structure

Element / Attribute name	Element / Attribute description
HexBinaryPrivateData	
Message	A hexadecimal encoded sequence of bytes to be sent to the CSPG-CI+ using ***send_msg*** message

4.3.5 DTCP-IP based gateway

4.3.5.1 General

All normative statements in 4.3.5 apply only if the DTCP-IP based gateway-centric approach is supported.

NOTE The criteria that determine under which circumstances the DTCP-IP based gateway-centric approach is implemented are out of the scope of the present document.

4.3.5.2 Overview

The CSP gateway based on DTCP-IP (CSPG-DTCP) is an optional entity handling security for the OITF. The CSPG-DTCP resides in the residential network and makes any specific content protection solution transparent. This is achieved by transforming a service proprietary content protection format into standard protection formats, which are sent by a secure channel. OITF and CSPG-DTCP mutually authenticate each other, and the CSPG-DTCP transfers content and its usage rule information to OITF in a secure manner. The definition of this interface is based on DTCP (DTCP) and DTCP over IP (DTCP-IP). An overview of CSPG-DTCP is shown in Figure 16. Figure 17 elaborates on the involved reference points.

Browsing interactions are executed between DAE and IPTV applications.

OITF discovers CSPG-DTCP in a home IP network by the use of the UPnP device discovery protocol as specified in 11.4 of IEC 62766-4-1:2017.

For managed network relying on the IMS, CSPG-DTCP is co-located with the IG to share session management information between the IG and the CSPG-DTCP. If it supports multicast IPTV services, it is co-located with WAN gateway to intercept IGMP messages from the OITF.

CSPG-DTCP acts as an HTTP proxy or RTSP proxy. The CSPG-DTCP identifies the location of the content through an input URL from the OITF.

The CSPG-DTCP transforms service-specific content protection formats and usage information format to DTCP over IP content protection format and usage information format respectively.

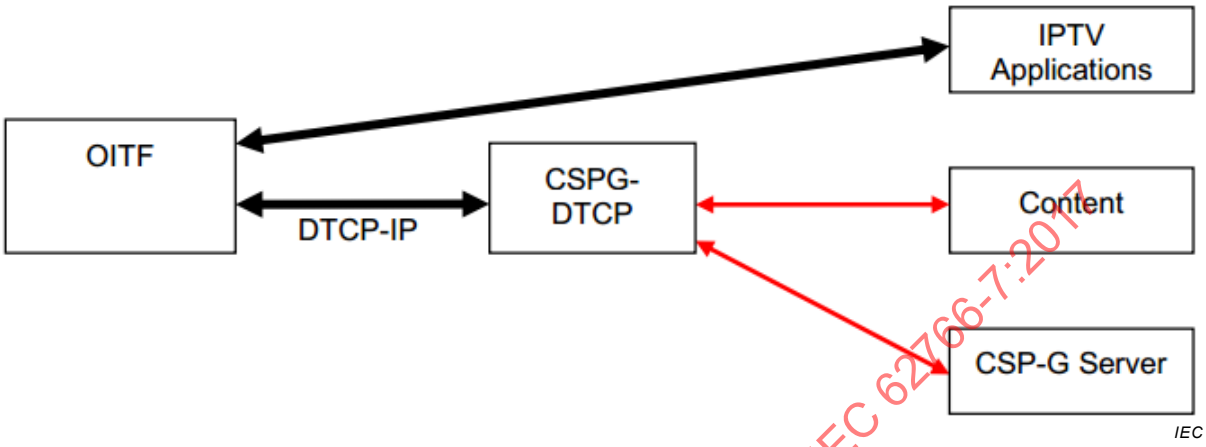

Figure 16 – CSPG-DTCP overview

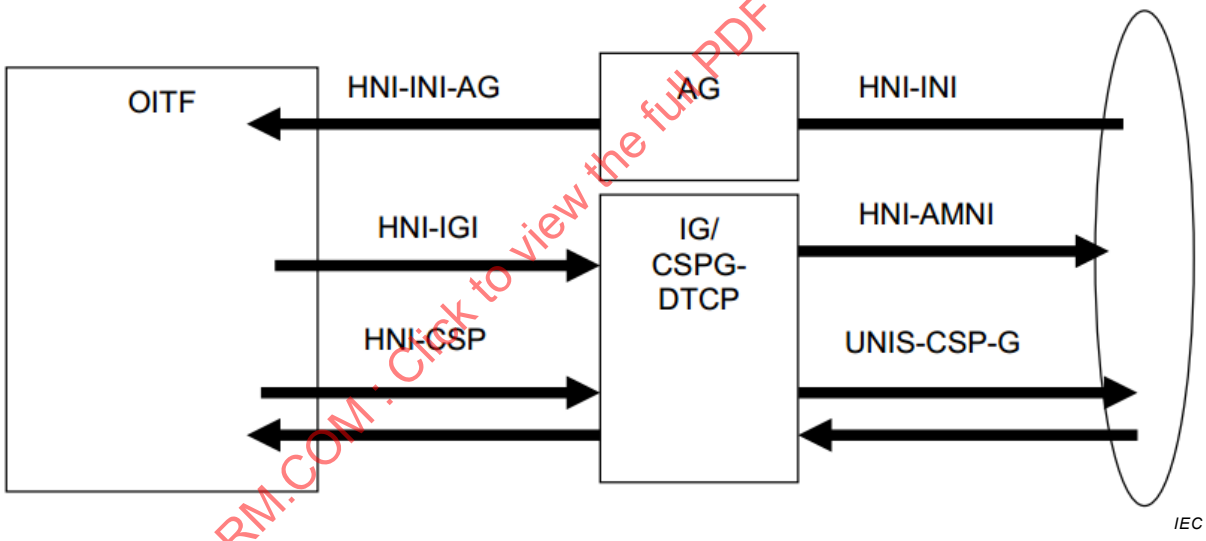

Figure 17 – Overview of involved reference points

NOTE HNI-AGC and HNI-AGI are not involved for the CSPG-DTCP.

4.3.5.3 CSPG-DTCP connectivity

The CSPG-DTCP is an IP connected device, and uses the same physical interface used for other IP devices such as IG, AG or home router.

4.3.5.4 HNI-CSP

4.3.5.4.1 General

The main functionalities of the HNI-CSP are to provide:

- CSPG-DTCP discovery (as described in IEC 62766-4-1);
- content access through CSPG-DTCP;
- DTCP AKE, content stream and usage rule transmission.

4.3.5.4.2 Content access through CSPG-DTCP

When an OITF determines, for example by inspecting the information in the DRMType element (see IEC 62766-3), from the content guide, content access descriptor or SD&S, that the content is protected by a service specific protection scheme, it shall access the content through the CSPG-DTCP, which acts as an HTTP proxy or RTSP proxy. The CSPG-DTCP receives content and shall transform the protection scheme to DTCP-IP. When the OITF receives error code of 403 from the CSPG-DTCP, the error code is interpreted as a DRM rights error. Then a DAE application accesses the error handling web page as an action of onDRMRightsError event defined in IEC 62766-5-1, or a native application accesses the RightsIssuerURL described in BCG or SD&S metadata, as defined in IEC 62766-3.

Refer to Annex E for examples of session setup sequences with a CSPG-DTCP.

For HTTP streaming and download, the OITF shall send the HTTP GET request through the HTTP proxy in CSPG-DTCP. Note that other HTTP transactions shall not use the HTTP proxy in CSPG-DTCP.

4.3.5.4.3 DTCP AKE, content streaming and usage rule transmission

DTCP AKE (Authentication and Key Exchange), DTCP content streams and DTCP usage rules are defined in DTCP and DTCP-IP. The usage rule is provided to the OITF from the CSPG-DTCP considering appropriate mapping, which depends on the service provider's business models. Content type of HTTP response/request shall be set to DTCP application media type as defined by DTCP-IP.

4.3.5.5 UNIS-CSP-G

This interface is out of scope because of applied service-specific protection schemes.

4.3.5.6 Protected streaming and file formats

4.3.5.6.1 General

The CSPG-DTCP supports either or both of the following formats protected by DTCP-IP encryption on HNI-CSP. The supported format depends on the CA system supported by the CSPG-DTCP. Media format on UNIS-CSP-G is out of scope of this specification.

- MPEG-2 TS and/or time stamped MPEG-2 TS, or
- MP4 File format.

If the OITF supports the unprotected MPEG-2 TS, the OITF shall support the DTCP-IP protected MPEG-2 TS format, as defined in 4.3.5.6. Otherwise, the support of the DTCP-IP protected MPEG-2 TS format as defined in 4.3.5.6 is optional.

If the OITF supports the unprotected time stamped MPEG-2 TS format, the OITF shall support the DTCP-IP protected time stamped MPEG-2 TS format, as defined in 4.3.5.6. Otherwise, the support of the DTCP-IP protected time stamped MPEG-2 TS format as defined in 4.3.5.6 is optional.

If the OITF supports the unprotected MP4 file format, the OITF shall support the DTCP-IP protected MP4 file format, as defined in 4.3.5.6. Otherwise, the support of the DTCP-IP protected MP4 file format as defined in 4.3.5.6 is optional.

4.3.5.6.2 Protection of MPEG-2 transport streams

4.3.5.6.2.1 General

An MPEG-2 Transport stream can be streamed or downloaded through CSPG-DTCP. CSPG-DTCP shall transmit the content in the DTCP PCP format. The DTCP PCP format

encapsulates the MPEG-2 Transport stream format, which is defined in IEC 62766-2-1. For the avoidance of doubt, transport stream level scrambling or PES level scrambling are not used. Both transport_scrambling_control bits and pes_scrambling control bits shall be set to "00".

For content with parental rating control, CSPG-DTCP shall transmit MPEG-2 TS with CA descriptor and KSM table as specified in 4.3.5.6.2.2 and 4.3.5.6.2.3. The access_criteria_descriptor carries information for parental rating control.

If the OITF supports the DTCP-IP based gateway-centric approach, the OITF shall support the parental rating access_criteria_descriptor, specified in IEC 62455, and shall support at least the rating_type 0 within these criteria, which maps to the parental rating system in DVB Systems EN 300 468. Other descriptors in the key stream message should be ignored.

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 the programme 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 for the A/V content is detected that does not meet the parental rating criterion that is set for the parental system in use, and which has lead to blocking of the consumption of the content. The event shall provide the programme's rating. 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 case 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). If 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, the setting of which is usually restricted to privileged users, for example parents. 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 if the current programme's rating becomes lower than the current parental rating threshold.

4.3.5.6.2.2 CA_descriptor

Content with parental rating control shall include the CA descriptor in the PMT with restrictions as shown in Table 30.

Table 30 – CA_descriptor

Syntax	No. of bits	Mnemonic	Value
CA_descriptor() {			
descriptor_tag	8	uimsbf	9
descriptor_length	8	uimsbf	
CA_system_ID	16	uimsbf	0x0007
MPEG2_Reserved	3	bslbf	
CA_PID	13	uimsbf	
for (i=0; i<N; i++) {			
private_data_byte	8	uimsbf	

}			
}			

descriptor_tag: MPEG has defined the tag value of 9 for the CA-descriptor.

descriptor_length: the length of the descriptor.

CA_system_ID: 0x0007

CA_PID: the PID on which the KSM table can be found

MPEG2_reserved: bits reserved by ISO/IEC 13818-1.

private_data_byte: not used and shall be ignored.

4.3.5.6.2.3 Key stream message and KSM table

Content with parental rating control shall include key stream message in KSM table (IEC 62455, ETR 289).

Key stream message is defined in 7.2 of IEC 62455:2010 and the following usage restrictions shall be applied:

- access_criteria_flag is set to KSM_FLAG_TRUE for the content with parental rating control;
- traffic protection protocol is set to KSM_ALGO_MPEG2_TS_CRYPT;
- traffic_authentication_flag is set to KSM_FLAG_FALSE (traffic authentication is not used);
- next_traffic_key_flag is set to KSM_FLAG_FALSE;
- timestamp_flag is set to KSM_FLAG_FALSE;
- programme_flag is set to KSM_FLAG_FALSE;
- service_flag is set to KSM_FLAG_FALSE;
- content_key_index may be set to any value defined in IEC 62455; the OITF shall ignore this field;
- odd_even_flag may be set to any value defined in IEC 62455; the OITF shall ignore this field;
- cipher_mode may be set to any value defined in IEC 62455; the OITF shall ignore this field;
- encrypted_traffic_key_material_length is set to 0;
- traffic_key_lifetime is set to 0.

For content with parental rating control, the access_criteria_descriptor loop in the key stream message shall have at least one parental_rating access_criteria_descriptor. The OITF shall ignore other access_criteria_descriptors.

4.3.5.6.3 Protection of MP4 file format

MP4 file format can be downloaded through CSPG-DTCP. CSPG-DTCP shall transmit the content in DTCP PCP format which encapsulates MP4 file format, which is defined in IEC 62766-2-1.

4.3.5.7 Downloaded content usage

For downloaded content, content shall be transformed to DTCP-IP protection by CSPG-DTCP when content is being downloaded. Content shall be stored and played back by the OITF in a manner compliant to DTCP compliance rules DTCP Adopter Agreement.

4.3.5.8 PVR usage

For PVR usage for scheduled content service, content shall be transformed to DTCP-IP protection by CSPG-DTCP when content is being streamed or multicast. Content shall be stored and played back by OITF in a manner compliant to DTCP compliance rules DTCP Adopter Agreement.

5 User identification, authentication, authorisation and service access protection

5.1 General principles

For the syntax of the messages mentioned in Clause 5, see IEC 62766-4-1.

Clause 5 presents the general principles that govern service access protection and user authentication. In Clause 5, the requested service represents for example service provider discovery (SPD), service discovery (SD), or IPTV application.

Clause 5 also applies to services on the IG requested from the OITF over the HNI-IGI. In this case, the equivalent of SAA function and service function are co-located on the IG.

Figure 18 shows the generic message flow for service access protection and user authentication.

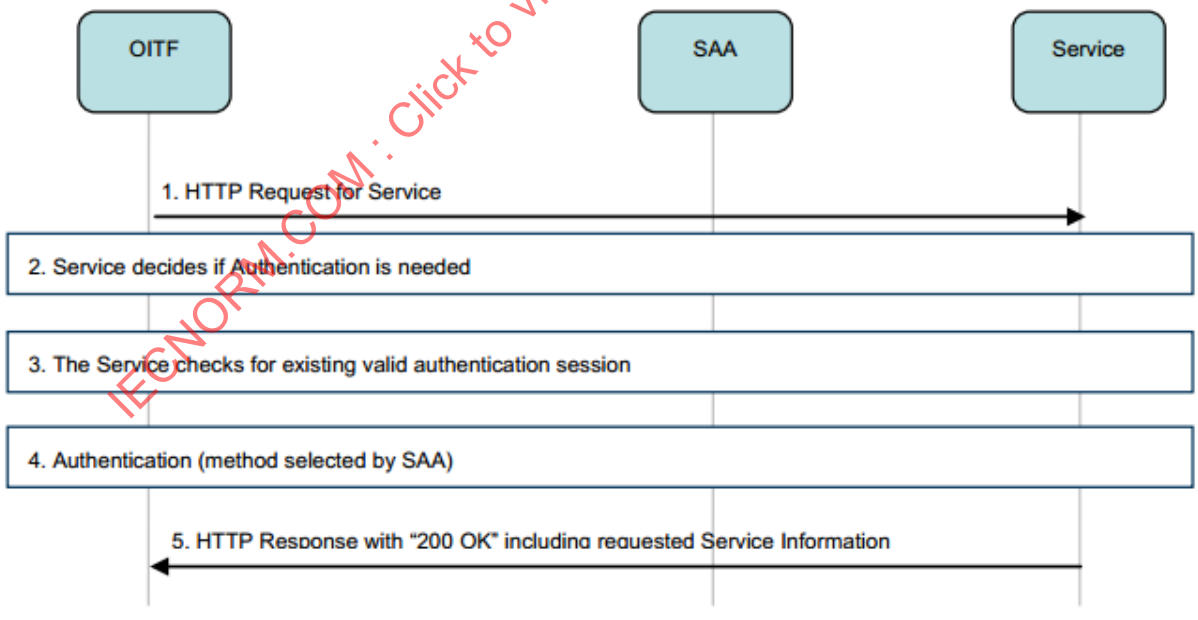

Figure 18 – General message flow for service access protection and user authentication

The steps are elaborated as follows:

1) The OITF requests a service.
2) The requested service decides whether the request needs to be authenticated or not.
   - If not, the service directly serves the request, go to step 5).

- If so, go on with step 3).

3) The requested service checks if the request is part of an existing valid authenticated service session (see 5.6).
   - If so, it directly serves the request, go to step 5).
   - If not, go on with step 4).
4) The requested service triggers SAA authentication. There are two cases: the SAA function is co-located with the requested service or the SAA function is standalone (see 5.3). The SAA decides what authentication mechanisms it uses (see 5.2 and 5.4).
   - If the authentication is successful, go on with step 5.
   - If not, the OITF may, for example, retry step 4 or display an error message, or return an HTTP error.
5) The requested service serves the request.

The requested service decides what security is needed for the service delivery: authentication needed or not, confidentiality needed (TLS/SSL) or not.

The SAA decides what authentication mechanisms it uses and what security is needed for the performed authentication: TLS/SSL or not.

5.2 Interfaces

5.2.1 General

Subclause 5.2 describes the impact of user identification, authentication, authorisation and service access protection on the HNI-INI and HNI-IGI interfaces.

5.2.2 HNI-INI

The following authentication mechanisms are supported for HTTP protocol on HNI-INI interface between OITF and the network (see 5.4 for their specification):

- no authentication;
- HTTP authentication, see 5.4.1;
- network based authentication (this requires no action on the OITF), see 5.4.2;
- web-based authentication, see 5.4.3;
- HTTP digest authentication using an IG (this requires an IG to be present in the home network), see 5.4.4;
- GBA authentication using an IG (this requires an IG to be present in the home network), see 5.4.5.

The OITF shall support all the mechanisms listed above.

The SAA may use any of the mechanisms listed above.

Note that 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.

5.2.3 HNI-IGI

In this case, the equivalent of SAA function and service function are co-located on the IG. The following authentication mechanisms are supported for HTTP protocol on HNI-IGI interface between OITF and IG:

- no authentication;
- HTTP authentication, see 5.4.1;
- web-based authentication, see 5.4.3.

The OITF shall support all the mechanisms listed above.

On the HNI-IGI interface, the IG shall support at least one of the following authentication mechanisms:

- no authentication;
- HTTP authentication, see 5.4.1.

The IG may use any of the above-listed mechanisms (no authentication, HTTP authentication or web-based authentication).

The OITF and IG shall support and perform IMS registration as specified in 6.4.6 in IEC 62766-4-1:2017 and described in 5.5. They shall do so prior to any service access attempt in a managed network relying on IMS.

5.2.4 Common requirements

On both HNI-INI and HNI-IGI interface, the OITF shall support all of the following mechanisms, redirection, and security for the HTTP protocol and HTML support:

- standard HTTP requirements: HTTP redirection, HTTP cookies;
- URL parameters;
- HTML forms and HTTP Post in forms;
- TLS/SSL – TLS 1.2 should be supported, if not then TLS 1.1 should be supported, otherwise TLS 1.0 shall be supported. The OITF shall support TLS Renegotiation Extension as described in IETF RFC 5746.

NOTE The requirements above ensure the support of SAML web-based SSO, see 5.6.5.

To avoid extra message exchanges, the OITF shall provide in requests, when available (see 5.6):

- HTTP authentication header (authorization),
- HTTP cookie header (cookie).

5.3 Service access protection

5.3.1 SAA co-located with service

Figure 19 describes the sequences when the SAA function is co-located with the requested service.

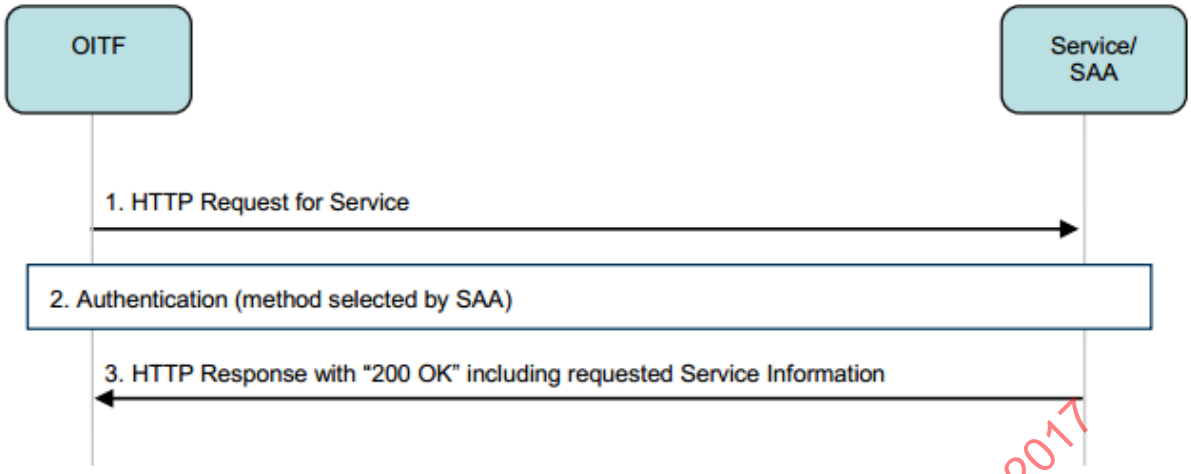

Figure 19 – SAA co-located with requested service

The steps are as follows:

1) The OITF requests a service. Authentication is needed and there is no valid authenticated service session.
2) The service/SAA performs authentication.
3) The requested service serves the request.

5.3.2 SAA standalone

Figure 20 describes the sequences when the SAA function is standalone, the OITF is redirected to the SAA for authentication.

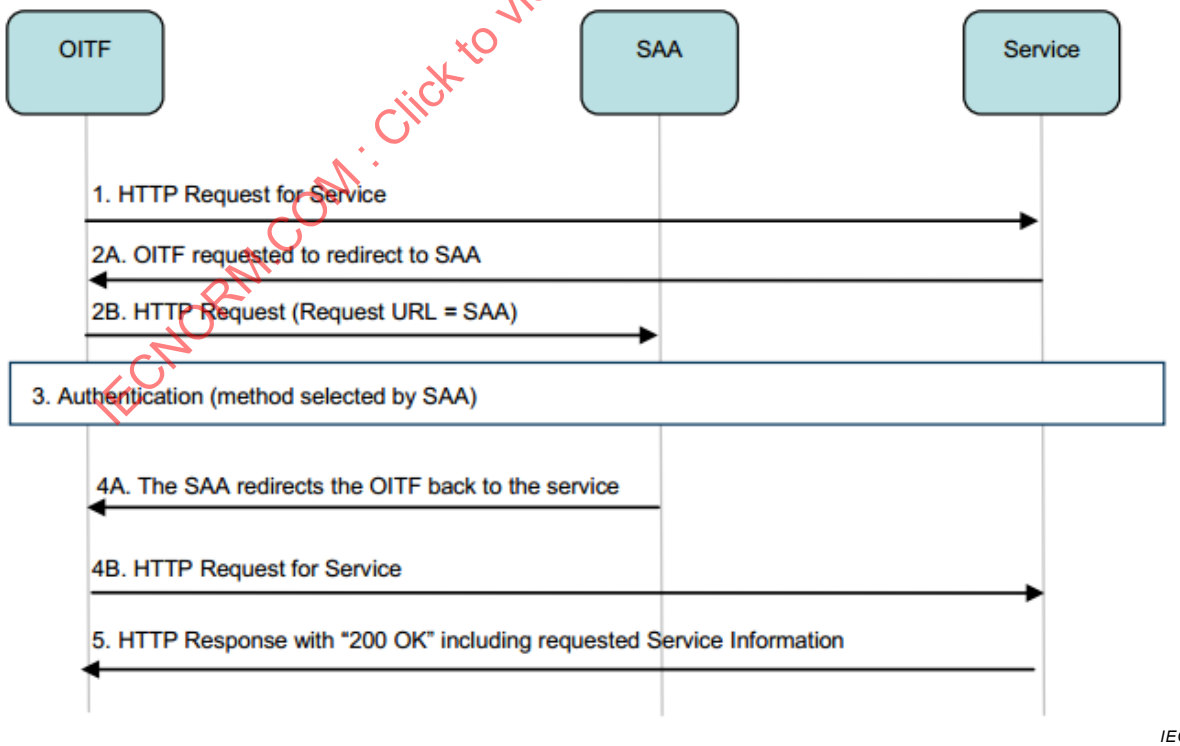

Figure 20 – Standalone SAA, redirection mode

The steps are as follows:

1) The OITF requests a service. Authentication is needed and there is no valid authenticated service session.
2) A. The requested service triggers SAA authentication. The service redirects the OITF to the SAA (e.g. using HTTP redirection (Location = SAA)).

   B. The OITF connects to the SAA, using the redirection obtained in step 2A.
3) The SAA performs authentication.
4) A. The SAA redirects the OITF back to the service (e.g. by using SAML HTTP-POST binding, SAML HTTP Post SimpleSign binding or HTTP redirection).

   B.The OITF requests the service again, using the redirection obtained in step 4A.
5) The requested service checks that authentication succeeded and serves the request.

5.4 OITF authentication mechanisms

5.4.1 HTTP basic and digest authentication

The OITF shall support HTTP basic and digest authentication as specified in RFC 2617. A possible message flow for HTTP basic and digest authentication is described in Figure 21. When HTTP basic or digest authentication RFC 2617 is used, it is assumed that user identifier and its secret information (e.g. password) are shared between OITF and Providers Network (SAA) in advance of the described sequence.

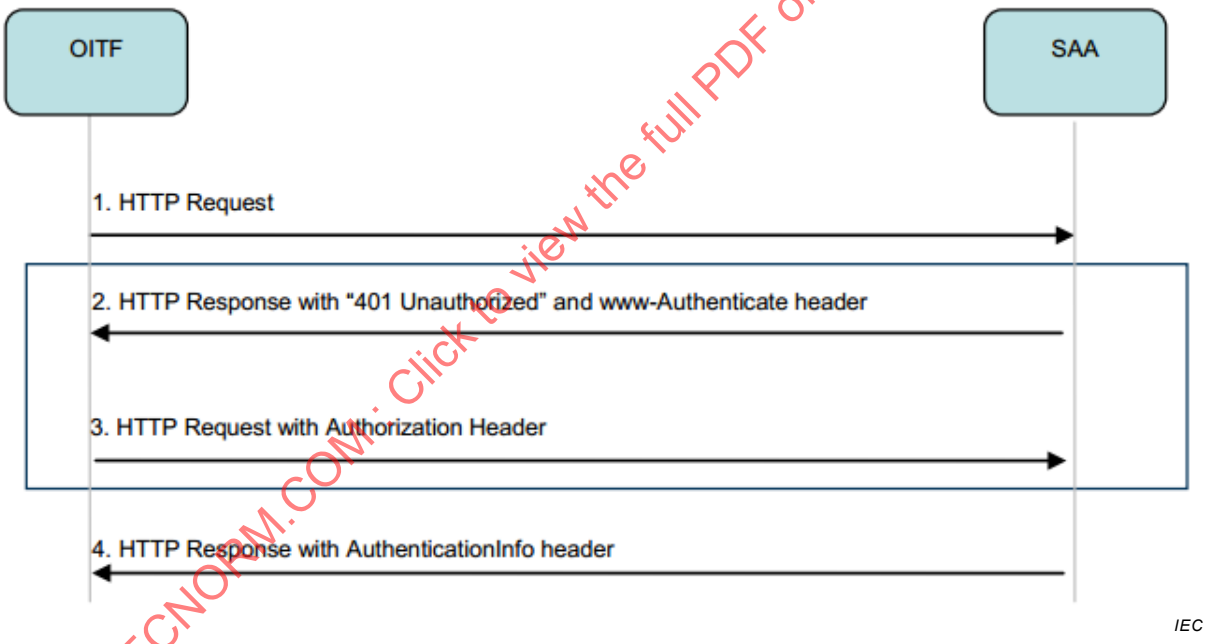

Figure 21 – HTTP basic and digest authentication

1) The OITF requests a service co-located with the SAA function or has requested a service and has been redirected to SAA function.
2) The SAA responds with a "401 Unauthorized" status code with a WWW-Authenticate header defined in RFC 2617.
3) The OITF re-sends the request with an authorization header as defined in RFC 2617. The user identifier and its secret information are used as username-value and password for the generation of the authorisation header.
4) The SAA checks the authorisation header. If the verification succeeds, the SAA/service serves the request or redirects the OITF to the service (e.g. by using SAML HTTP-POST binding, SAML HTTP Post SimpleSign binding or HTTP redirection). The response contains an AuthenticationInfo header. The response may contain session management information (cookie, URL parameter).

If no user and password are available at the OITF, a window may be displayed to the user for entering his credentials between steps 2 and 3. This is the standard working in a DAE application. As described in general principles, this situation shall occur only if no valid authentication session or credentials are available in the OITF. To protect the password that is in the clear in HTTP basic authentication, the SAA may additionally require TLS/SSL as stated in the general principles.

5.4.2 Network-based authentication

This subclause describes the message flows for network-based authentication. Network-based authentication is a silent authentication based on network information. This authentication is transparent to the OITF.

In the case of a managed network, the SAA can rely on (proprietary) network-specific information, whose information is out of scope of this specification, to authenticate an incoming request. The sequences are depicted in Figure 22.

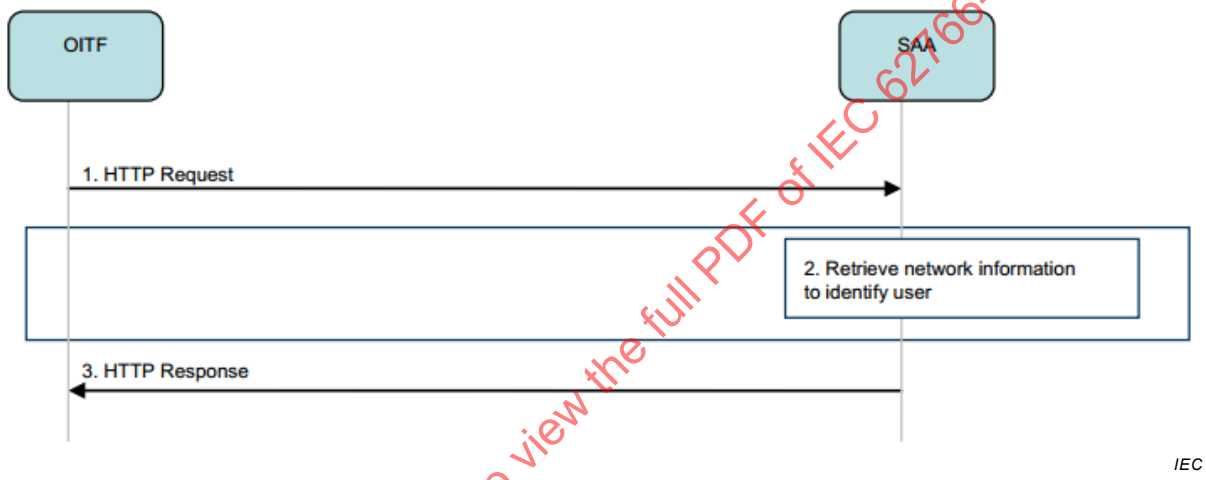

Figure 22 – Network-based authentication

The steps are elaborated in the following:

1) The OITF requests a service co-located with the SAA function or has requested a service and has been redirected to an SAA function.
2) The SAA links the request to the user based on network information.
3) If the operation succeeds, the SAA/service serves the request or redirects the OITF to the service (e.g. by using SAML HTTP-POST binding, SAML HTTP Post SimpleSign binding or HTTP redirection). The response may contain session management information (cookie, URL parameter).

5.4.3 Web-based authentication

The calling function in the OITF should support receiving a CE-HTML response for a service HTTP request and should launch the DAE for displaying it. If the calling function does not support receiving an CE-HTML, XHTML or HTML compatible response, it shall signal it to the server by including its acceptable media types without "application/xhtml+xml", "application/ce-html+xml", and "text/html" in the request's HTTP "accept" header explicitly, and by also not including CE-HTML/1.0 as part of the User-Agent header. If the calling function does not support receiving a CE-HTML, XHTML or HTML compatible response, the SAA shall return a "403 Forbidden" HTTP error.

As described in general principles, this situation shall occur only if no valid authentication session is available in the OITF (e.g. no cookie available).

The DAE within the OITF shall support CE-HTML forms and HTTP Post in forms.

The remainder of this subclause describes the message flows for web based authentication. Web based authentication can be explicit or implicit/silent.

- Explicit authentication: the user is prompted with a web page form to fill-in with a login and password: the result of the authentication can be persistent for later re-use (implicit/silent authentication).
- Implicit/silent authentication: the user is not prompted with any form but s/he is silently authenticated based on persistent data (session management).

Web based authentication mechanisms do not add requirements to the OITF besides supporting a DAE. They are based on optionally HTML forms and HTTP Post, HTTP redirection and HTTP cookies. Figure 23 shows the message flow for web-based authentication with form.

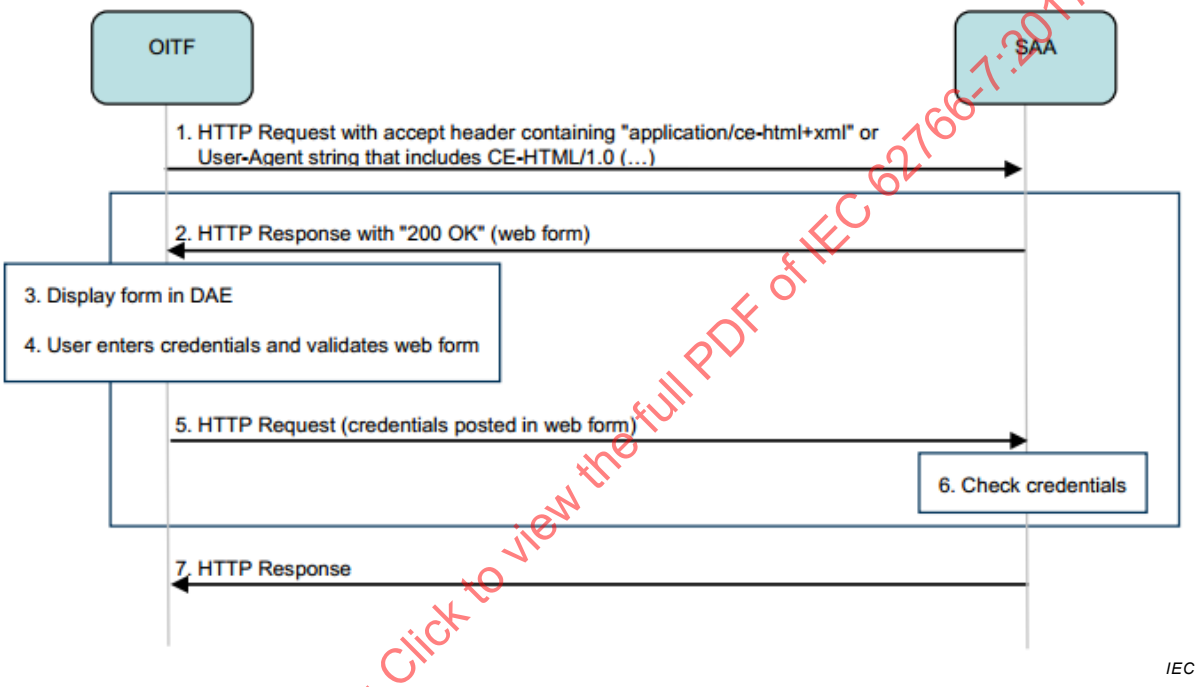

Figure 23 – Web-based authentication with form

1) The OITF requests a service co-located with the SAA function or has requested a service and has been redirected to SAA function.
2) If the HTTP request to the SAA has a User-Agent string that includes CE-HTML/1.0 as defined in CEA-2014-A, or the "accept" HTTP header includes (explicitly or implicitly) a CE-HTML accept header ("application/ce-html+xml"), the SAA responds with a CE-HTML compatible web form for requesting user credentials. User credentials provisioning are out of scope of this specification.
3) The web form is displayed in the DAE.
4) The user enters his credentials and validates the form.
5) The form validation posts the user credentials to the SAA.
6) The SAA checks the credentials.
7) If verification is successful, the SAA/service serves the request or redirects the OITF to the service (e.g. by using SAML HTTP-POST binding, SAML HTTP Post SimpleSign binding or HTTP redirection). The response may contain session management information (cookie, URL parameter).

5.4.4 HTTP digest authentication – Using IMS gateway

5.4.4.1 General

Subclause 5.4.4 specifies optional functionality by which an OITF can use HTTP digest credentials in an IG, if present in the home network, for user authentication to HTTP services relying on IMS credentials. The mechanism specified here allows the use of different types of credentials, depending on the capabilities of the IG, and in a way transparent to the OITF, including an extension mechanism to future authentication mechanisms. The OITF discovers the authentication mechanisms supported by IG and the associated credentials stored in the IG, and offers them towards an application server. The application server selects one of the offered authentication mechanisms.

The IG shall signal that it supports HTTP digest authentication in its description during UPnP discovery as specified in 11.2 of IEC 62766-4-1:2017.

HTTP basic authentication shall not be used.

NOTE The criteria that determine under which circumstances the functionality by which an OITF can use the HTTP digest credentials in a gateway Function is implemented in an OITF are out of the scope of the present document.

5.4.4.2 Initial procedure

When the OITF is powered up and if the IG supports HTTP digest authentication, the OITF shall request supported HTTP digest authentication realms from the IG as described in 6.4.6.3.2 of IEC 62766-4-1. Receiving this request:

- If the IG supports GBA as defined in TS 33.220, the IG shall perform a GBA bootstrapping for the current IMS registered user towards the GBA Single Sign-On Function (acting like a BSF in TS 33.220). The GBA registration is based on secrets shared between the ISIM and the network provider. The result of a successful GBA run is the establishment of a session identifier, B-TID, and a shared key, Ks. The decision on running GBA_U or GBA_ME is based on subscription information (i.e. UICC capabilities) as described in TS 33.220. Thus if the ISIM supports GBA, GBA_U bootstrap shall be run and in this case the key Ks is computed by the ISIM on the IG side and doesn't leave the UICC. If the ISIM doesn't support GBA, GBA_ME shall be run. The support of GBA by the ISIM is indicated in the ISIM service table as defined in 3GPP TS 31.103. This Ks key can later be re-used to derive server-side application (NAF) specific keys. These keys can also be passed on to trusted applications in the home network, and can later be used for authentication based on the GBA authentication, but without further need for IG-provider network communication.
- The IG shall provide the list of supported realms for HTTP digest authentication – using IMS Gateway. If the IG supports GBA, it shall include in this list the realm for GBA authentication, as defined in TS 24.109.
- The IG may provide a token to append to the HTTP user-agent of the OITF for signalling support of specific authentication scheme. The IG shall provide the token "3gpp-gba", as specified in TS 24.109, if it supports GBA.

The OITF may check the returned User-Agent token. The OITF shall accept unknown User-Agent tokens, in order to allow evolution of the authentication procedure.

The OITF shall append the returned user-agent token to its user-agent.

NOTE If the IG supports GBA authentication, as the IG adds "3gpp-gba" to the returned user-agent token, the OITF acts as a user equipment in TS 24.109 and signals in its user agent that it supports GBA authentication.

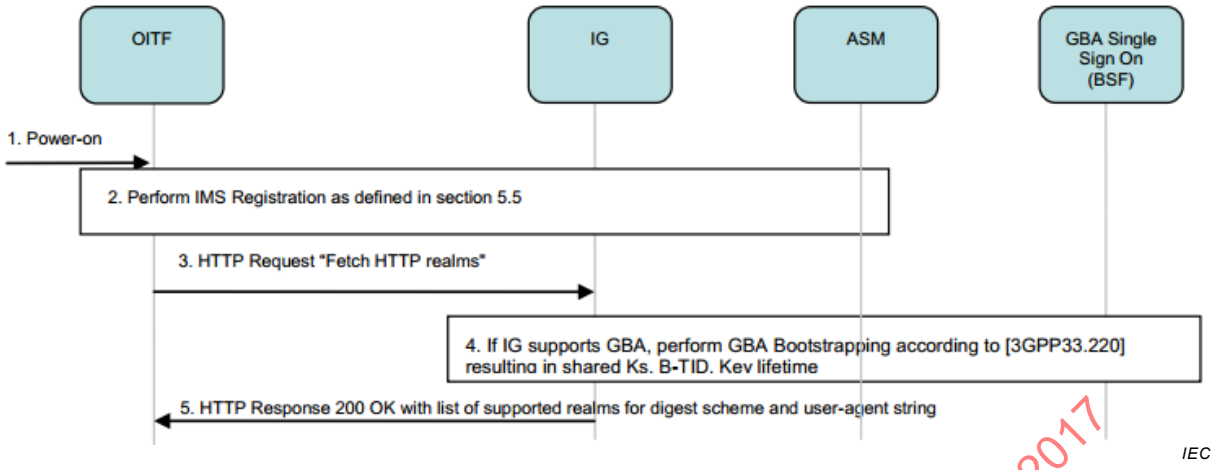

Figure 24 – Initial procedure

Figure 24 shows the message sequence for initial procedure to ensure HTTP digest authentication using IG. It contains the following steps:

1) The OITF is powered on.
2) The OITF performs a user registration as defined in 5.5.
3) The OITF sends a Fetch HTTP realms request to IG as defined in IEC 62766-4-1:2017, 6.4.6.3.2, step 1. The IG validates the request. The IG may require at that stage any authentication mechanism specified in 5.2.3 and/or any mechanism and security (i.e. TLS/SSL) specified in 5.2.4. For simplification, none of this mechanism is shown in Figure 24.
4) If IG supports GBA, the IG performs GBA Bootstrapping procedure according to TS 33.220 towards the GBA Single Sign-on (BSF) function in the provider's network. If successful, this results in establishing a shared key Ks on both ends. The GBA Single Sign-on function also sends the lifetime of the key Ks and a session identifier B-TID to the IG.
5) The IG returns the list of supported realm and user-agent string to the OITF as defined in 62766-4-1:2017, 6.4.6.3.2, step 2.

5.4.4.3 Authentication procedure

5.4.4.3.1 General

If the OITF has registered to an IG which supports HTTP digest authentication, each time the OITF needs to access a service offered by an application server that requires HTTP digest authentication, the OITF shall check the realm against the realms retrieved from IG in the initial procedure. If the realm matches to one of the IG supported realms, the OITF shall retrieve HTTP credentials and HTTP headers from the IG, as specified in 6.4.6.3.3 of IEC 62766-4-1:2017.

As a prerequisite to this procedure, the IMS registration shall have been successfully completed.

The IG may provide the following HTTP header:

- For 3GPP GBA authentication, a "X-3GPP-Intended-Identity" containing the identity of the current user, as specified in TS 24.109
- For HTTP digest authentication, a "X-OIPF-Intended-Identity" containing the identity of the current user.

The SAA may verify that the intended identity matches to the authenticated identity.

The intended identity is used to identify the user when credentials are shared among users. The service provider should define and enforce policies for sharing of credentials among users.

The OITF may check the returned HTTP Headers. The OITF shall accept unknown User-Agent tokens, in order to allow evolution of the authentication procedure.

The OITF shall use the returned credentials towards the application server, using HTTP digest authentication as specified by RFC 2617 and shall add the returned HTTP headers to the outgoing HTTP requests for this realm.

The service provider should define and enforce policies for sharing of credentials among application servers.

5.4.4.3.2 Authentication procedure using stored credentials

The same credentials and realm as for SIP digest may be used, this is an operator security and deployment choice (managed in the IG and the network). In this case:

- the userid shall be set to the value of the private user identity, and
- the realm shall be set to the domain name of the home network.

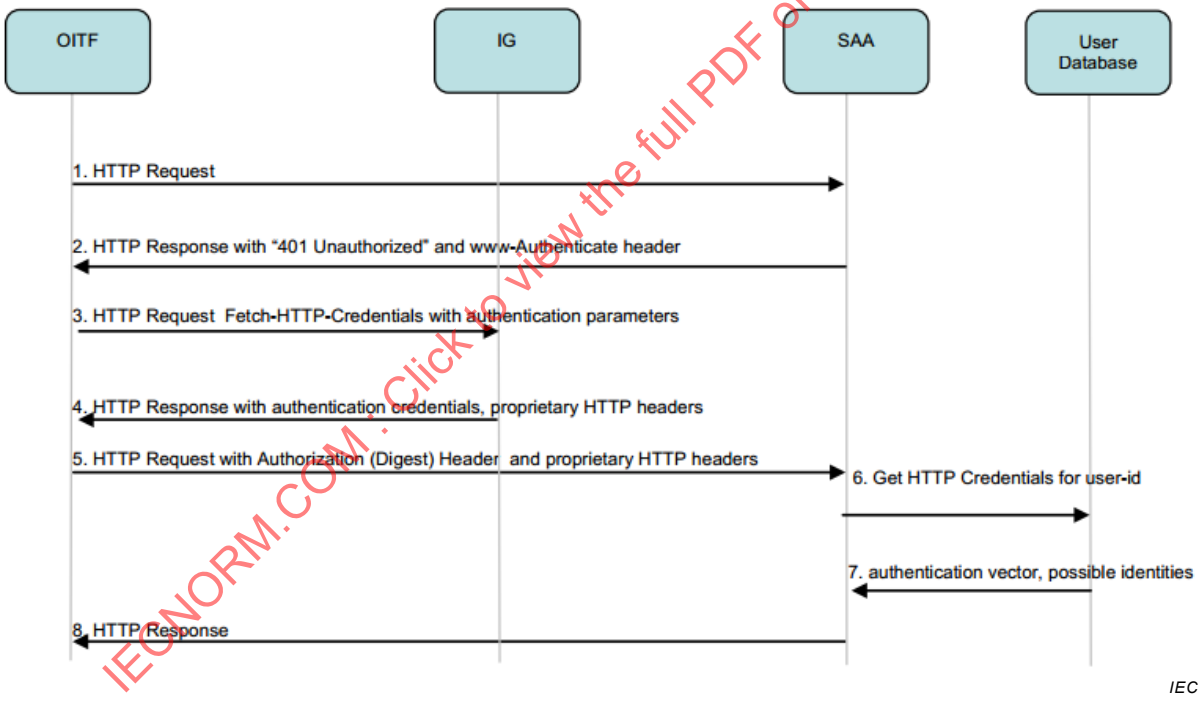

Figure 25 – Authentication between an OITF and an SAA based on HTTP credentials stored in IG

Figure 25 shows the message sequence for authentication between an OITF function and an SAA based on HTTP credentials retrieved from the IG. It contains the following steps:

1) OITF function sends a request for a resource (e.g. service) to the SAA. It is assumed here that the resource requires authentication.
2) The SAA returns a 401 unauthorized message as defined in RFC 2617.
3) The OITF checks the realms. The realm is one of the realms supported by the IG for HTTP digest authentication. The OITF sends a request including the IMPU, the auth-scheme and realm and additional authentication parameters in case of digest authentication to the IG to retrieve HTTP credentials for the registered user. The request format is specified in IEC 62766-4-1:2017, 6.4.6.3.3, step 1.

4) IG returns the authentication credentials and optionally HTTP headers. The nature of the authentication credentials and the response format are specified in IEC 62766-4-1:2017, 6.4.6.3.3, step 2. The IG may require at that stage any authentication mechanism specified in 5.2.3 and/or any mechanism and security (i.e. TLS/SSL) specified in 5.2.4 for access control and/or protection of the credentials. For simplification, none of this mechanism is shown in Figure 25.

5) The OITF function repeats step 1 with an authorisation header, using returned authentication credentials. The OITF adds the returned HTTP headers, if any, to the request.

6) SAA requests from the User Database for the subscriber specified via its user-id, its HTTP credentials (authentication vector) and possible identities.

7) The SAA gets the authentication vector and possible identities from the User Database. The SAA checks the user-id and password. The SAA may verify that the intended identity provided in the HTTP header belongs to the possible identities of the subscriber.

   NOTE It is assumed that there exists a trust relation between SAA and User Database. Details are out of scope of this specification.

8) Upon successful authentication, the SAA/service serves the request or redirects the OITF to the service (e.g. by using SAML HTTP-POST binding, SAML HTTP Post SimpleSign binding or HTTP redirection). The response may contain session management information (cookie, URL parameter).

The message format for steps 3 and 4 are specified in the 6.4.6.3.3 of IEC 62766-4-1:2017.

5.4.4.3.3 Authentication procedure using GBA credentials

The key Ks that was established during the GBA registration may be used later on for authentication between OITF functions and services (i.e., application servers). Each time an OITF needs to access a service offered by an AS (i.e., NAF) that requires GBA authentication, a specific key Ks_NAF in case of GBA-ME or Ks_ext_NAF in case of GBA-U shall be derived by the IG or ISIM in IG respectively and the server side GBA Single Sign-on function (acting like a BSF in TS 24.109). For clarity, this specific key is named in the rest of the document Ks_(ext)_NAF and will refer to Ks_NAF in case of GBA_ME and Ks_ext_NAF in case of GBA_U. This generated key shall be conveyed to the OITF function in the residential network by the IG and to the AS by the server side GBA Single Sign-on function (BSF). The key Ks_(ext)_NAF shall then be used for authentication between the OITF function and the AS, using HTTP digest authentication as specified by TS 24.109.

When an SAA (acting like a NAF in TS 24.109) requests GBA authentication (perceived as regular HTTP digest authentication by the OITF), the OITF shall retrieve HTTP credentials, in this case GBA credentials, and HTTP Headers and shall perform HTTP digest authentication.

As a prerequisite to this procedure, the GBA registration shall have been successfully completed by the IG in the initial procedure (see 5.4.4.2).

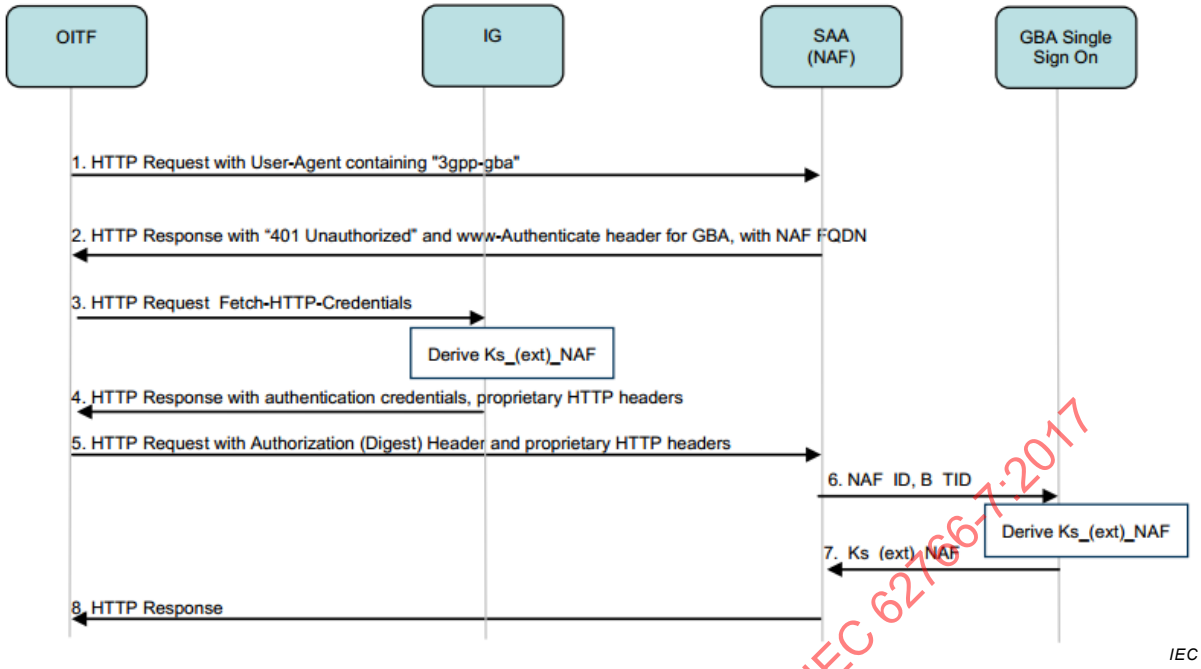

Figure 26 – Authentication between an OITF and an SAA based on GBA credentials

Figure 26 shows the message sequence for authentication between an OITF function and an SAA based on the previously established GBA bootstrapping. It contains the following steps:

1) OITF function sends a request for a resource (e.g., service) to the SAA (NAF). It is assumed here that the resource requires authentication. The User-Agent string in the HTTP request contains "3gpp-gba" indicating to the SAA that it supports GBA authentication.

   NOTE 1 The user-agent string has previously been sent from IG to OITF.

2) The SAA (NAF) returns a 401 "Unauthorized" message, the realm indicates that 3GPP bootstrapping is used and provides the NAF FQDN as defined in TS 24.109.

3) The OITF checks the realms. The realm is one of the realms supported by the IG for HTTP digest authentication. The OITF sends a request including the IMPU, the auth-scheme and realm and additional authentication parameters for digest authentication to the IG to retrieve HTTP credentials for the registered user. The request format is specified in IEC 62766-4-1:2017, 6.4.6.3.3, step 1. The IG identifies from the realm that GBA authentication is requested. IG generates Ks_NAF in the event of GBA_ME or Ks_ext_NAF with the co-operation of the ISIM in the event of GBA_U (Ks_(ext)_NAF).

   NOTE 2 According to TS 33.220, the NAF_ID is constructed as follows: NAF_ID = FQDN of the NAF || Ua security protocol identifier. The FQDN of the NAF is included in the realm. The identifier for Ua security protocol HTTP digest authentication according to TS 24.109 is (0x01,0x00,0x00, 0x00,0x02).

   Ks_(ext)_NAF is computed as Ks_(ext)_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_ID), where KDF is the key derivation function as specified in Annex B of TS 33.220, and the key derivation parameters consist of the user's IMPI, the NAF_ID and RAND.

4) IG returns the authentication credentials and optionally HTTP Headers. The B-TID is used as username and Ks_(ext)_NAF as password. The IG may return a "X-3GPP-Intended-Identity" HTTP header containing the identity of the current user, as specified in TS 24.109. The response format is specified in IEC 62766-4-1:2017, 6.4.6.3.3, step 2.

5) The OITF function repeats the request of step 1 with an authorisation header, using authentication credentials returned from IG in step 4. The OITF adds the returned HTTP headers, if any, to the request.

6) SAA (NAF) sends B-TID and its NAF_ID to the GBA Single Sign-on function (BSF) in provider network, the GBA single sign-on function retrieves Ks and calculates Ks_(ext)_NAF.

7) The GBA Single Sign-on function (BSF) in provider network returns Ks_(ext)_NAF, together with its lifetime, to SAA (NAF).

NOTE 3 The key lifetime returned by the GBA single Sign-on function (BSF) is equal to the lifetime of the corresponding Ks. But the SAA (NAF) may choose a shorter key lifetime based on local policy and/or application-specific needs.

8) If Ks_(ext)_NAF has expired, the SAA (NAF) shall send a suitable bootstrapping renegotiation request to the OITF, according to TS 33.220 and TS 24.109. Otherwise, the SAA (NAF) uses Ks_(ext)_NAF to authenticate the request. Upon successful authentication, the SAA (NAF)/service serves the request or redirects the OITF to the service (e.g. by using SAML HTTP-POST binding, SAML HTTP Post SimpleSign binding or HTTP redirection). The response may contain session management information (cookie, URL parameter).

The message format for steps 3 and 4 are specified in 6.4.6.3.3 of IEC 62766-4-1:2017.

5.4.5 GBA authentication – Using IMS gateway

5.4.5.1 General

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. Subclause 5.4.4 allows the use of different authentication mechanism 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.

Subclause 5.4.5 specifies optional functionality by which an OITF can use the ISIM in an IG, if present in the home network, for user authentication to services relying on IMS credentials. Subclause 5.4.5 is based on the principles described in Annex B of IEC 62766-1:2017 but extends that annex.

The IG shall signal that it supports GBA authentication in its description during UPnP discovery as specified in 11.2 of IEC 62766-4-1:2017.

NOTE The criteria that determine under which circumstances the functionality by which an OITF can use the ISIM in a Gateway Function is implemented in an OITF are out of the scope of the present document.

5.4.5.2 Initial GBA registration

When the OITF is powered up or when the user initiates a registration, i.e. when the OITF requests a user registration from the IG, and if the IG supports GBA authentication, the OITF shall, after the user registration from the IG, request a GBA Registration from the IG as described in IEC 62766-4-1. Receiving this request, the IG shall perform a GBA registration for the current IMS registered user towards the GBA single Sign-On function (acting like a BSF), according to TS 33.220. The GBA registration is based on secrets shared between the ISIM and the network provider. The result of a successful GBA run is the establishment of a session identifier, B-TID, and a shared key, Ks. This key Ks can later be re-used to derive server side application (NAF) specific keys. These keys can also be passed on to trusted applications in the home network, and can later be used for authentication based on the GBA authentication, but without further need for IG-provider network communication.

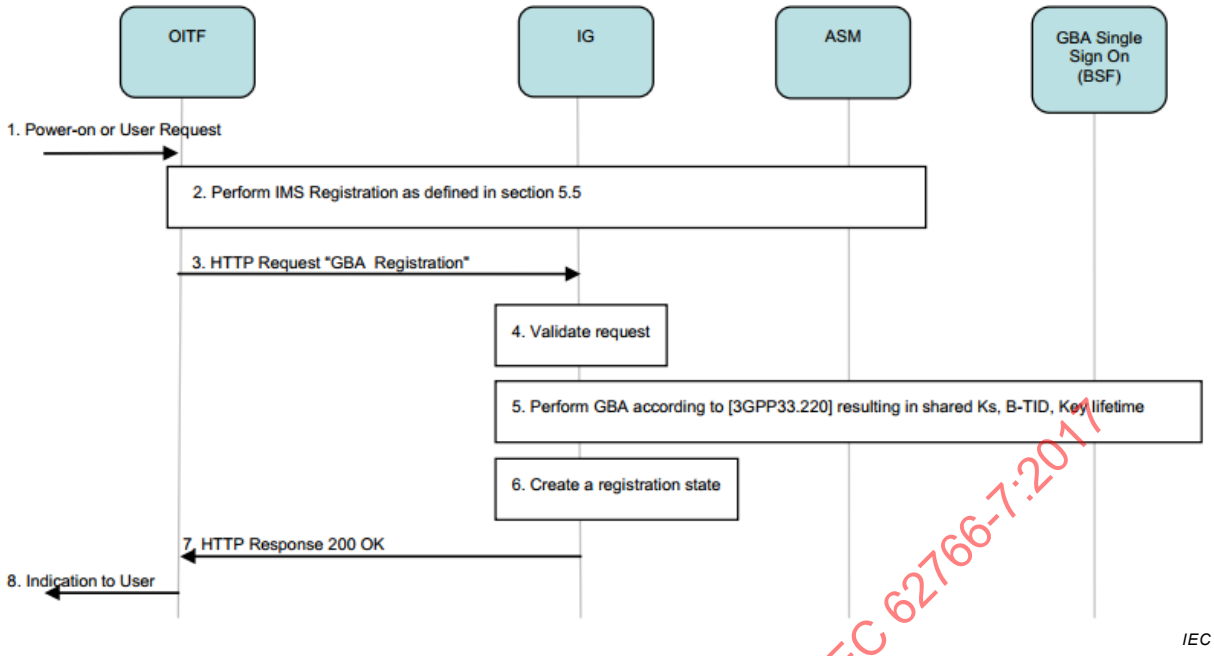

Figure 27 – Initial GBA registration

Figure 27 shows the message sequence for initial GBA registration. It contains the following steps:

1) The OITF is powered on (automatic default registration) or the user requests a personalised registration.
2) The OITF performs a user registration as defined in 5.4.5.
3) The OITF sends a GBA registration request to IG as defined in IEC 62766-4-1:2017 6.4.6.2.2, step 1.
4) The IG validates the request. The IG may require at that stage any authentication mechanism specified in 5.2.3 and/or any mechanism and security (i.e. TLS/SSL) specified in 5.2.4. For simplification, none of this mechanism is shown in Figure 27.
5) The IG performs GBA bootstrapping procedure according to TS 33.220 towards the GBA single Sign-on function (BSF) in the provider's network. If successful, this results in establishing a shared key Ks on both ends. The GBA Single Sign-on function (BSF) also sends the lifetime of the key Ks and a session identifier B-TID to the IG.
6) The IG returns the outcome of the GBA registration process to the OITF as defined in IEC 62766-4-1:2017, 6.4.6.2.2, step 2.
7) If the result of the registration procedure is successful, a registration state is created and maintained in IG.
8) An indication is sent to the user that includes the outcome of the registration process.

5.4.5.3 Re-use of GBA authentication – Using HTTP digest authentication

The key Ks that was established during the GBA registration may be used later on for authentication between OITF functions and services (i.e. application servers). Each time an OITF needs to access a service offered by an AS (i.e. NAF) that requires GBA authentication, a specific key Ks_(ext)_NAF shall be derived by the IG and the server side GBA Single Sign-on function (acting like a BSF in TS 24.109). This generated key shall be conveyed to the OITF function in the residential network by the IG, and to the AS by the server side GBA Single Sign-on function (BSF). The key Ks_(ext)_NAF shall then be used for authentication between the OITF function and the AS, using HTTP digest authentication as specified by TS 24.109.

If the OITF has registered to an IG which supports GBA authentication, the OITF shall act as a User Equipment in TS 24.109 and therefore shall signal in its User Agent that it supports GBA authentication.

When a SAA (acting like a NAF in TS 24.109) requests GBA authentication, the OITF shall retrieve GBA Credentials for the specified SAA (NAF) from the IG as specified in IEC 62766-4-1, and shall perform HTTP digest authentication as specified by TS 24.109.

If the OITF retrieves an X-HNI-IGI-Intended-Identity HTTP header from the IG, it shall use it as intended user identity and shall add an "X-3GPP-Intended-Identity" HTTP header to the outgoing HTTP requests to the SAA (NAF), as specified in TS 24.109. The SAA may verify that the intended identity belongs to the user (i.e. the identity matches one of the user's public identities indicated in the user security setting that was retrieved from the GBA Single Sign-On Function (BSF)).

As a pre-requisite to this procedure, the GBA registration (see 5.4.5.2) shall have been successfully completed.

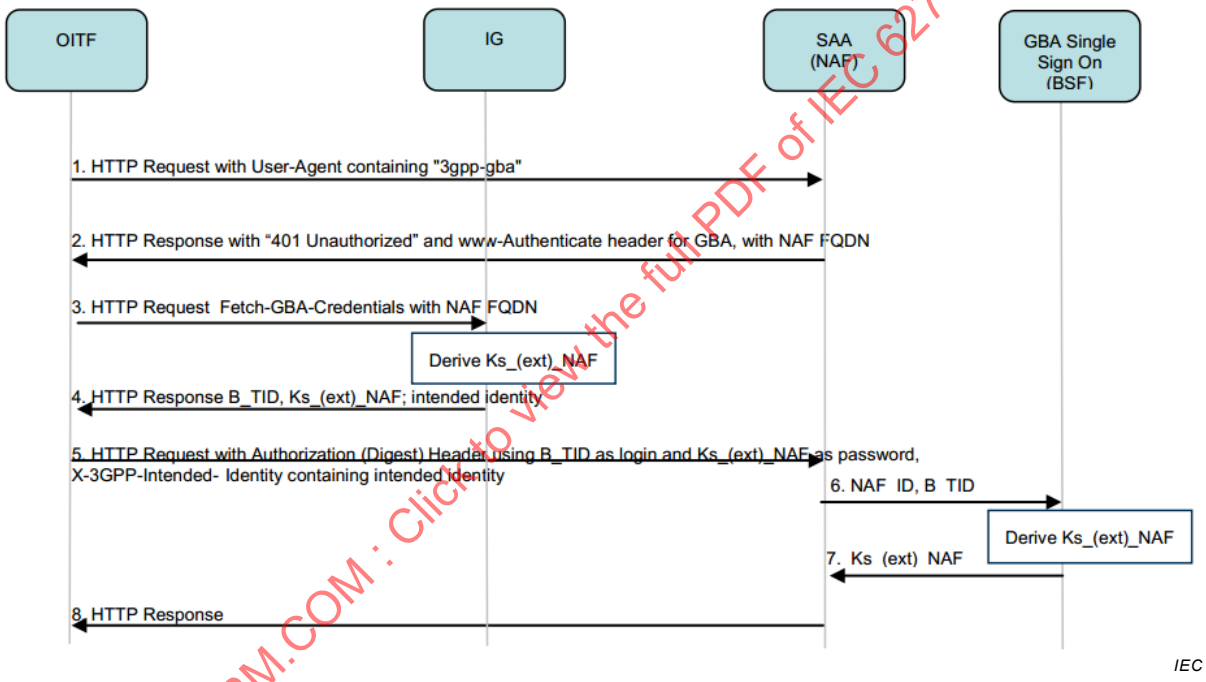

Figure 28 – Authentication between an OITF and an SAA based on GBA keys

Figure 28 shows the message sequence for authentication between an OITF function and an SAA based on the previously established GBA key. It contains the following steps:

1) OITF function sends a request for a resource (e.g. service) to the SAA (NAF). It is assumed here that the resource requires authentication. The User-Agent string in the HTTP request contains "3gpp-gba" indicating to the SAA (NAF) that it supports GBA authentication.
2) The SAA (NAF) returns a 401 unauthorized message, the realm indicates that 3GPP bootstrapping is used and provides the NAF FQDN as defined in TS 24.109.
3) OITF sends a request including the NAF FQDN to the IG to retrieve GBA credentials, and IG generates Ks_NAF in case of GBA_ME or Ks_ext_NAF with the co-operation of the ISIM in case of GBA_U (Ks_(ext)_NAF).

NOTE 1 According to TS 33.220, the NAF_ID is constructed as follows: NAF_ID = FQDN of the NAF || Ua security protocol identifier. The identifier for Ua security protocol HTTP digest authentication according to TS 24.109 is (0x01,0x00,0x00, 0x00,0x02). The request format is specified in IEC 62766-4-1:2017, 6.4.6.2.3, step 1.

Ks_(ext)_NAF is computed as Ks_(ext)_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_ID), where KDF is the key derivation function as specified in Annex B of TS 33.220, and the key derivation parameters consist of the user's IMPI, the NAF_ID and RAND.

4) IG returns Ks_(ext)_NAF, B-TID, the lifetime of the key Ks_(ext)_NAF and optionally the intended identity to OITF. The lifetime indicates the expiry time of the key Ks_(ext)_NAF and is equal to the lifetime of the key Ks (which was specified by the BSF during the GBA bootstrapping procedure). The response format is specified in IEC 62766-4-1:2017, 6.4.6.2.3, step 2.

5) The OITF function repeats the request with an authorisation header, using B-TID as username and Ks_(ext)_NAF as password. If a non-empty intended identity is returned from the IG, the OITF adds an X-3GPP-Intended-Identity HTTP Header containing the intended identity. If no intended identity is returned from the IG, the OITF shall not add an X-3GPP-Intended-Identity.

6) SAA (NAF) sends B-TID and its NAF_ID to the GBA Single Sign-on function (BSF) in provider network, the GBA Single Sign-on function (BSF) retrieves Ks and calculates Ks_(ext)_NAF.

7) The GBA Single Sign-on function (BSF) in provider network returns Ks_(ext)_NAF, together with its lifetime, to SAA (NAF).

   NOTE 2 The key lifetime returned by the GBA Single Sign-on function (BSF) is equal to the lifetime of the corresponding Ks. But the SAA (NAF) may choose a shorter key lifetime based on local policy and/or application-specific needs.

8) If Ks_(ext)_NAF has expired, the SAA (NAF) shall send a suitable bootstrapping renegotiation request to the OITF, according to TS 33.220. Otherwise the SAA (NAF) uses Ks_(ext)_NAF to authenticate the request. Upon successful authentication, the SAA (NAF)/service serves the request or redirects the OITF to the service (e.g. by using SAML HTTP-POST binding, SAML HTTP Post SimpleSign binding or HTTP redirection). The response may contain session management information (cookie, URL parameter).

The message format for steps 3 and 4 are specified in 6.4.6.2.3 of IEC 62766-4-1:2017.

5.4.5.4 Binding between GBA user authentication and DRM device authentication

GBA authenticates ISIM/IMPI, not the device. On the other hand, DRM (e.g. Marlin) relies on device authentication; the device shall have a valid certificate issued by the DRM trust authority. To avoid security issues, for example allowing a legitimate device (from a DRM point of view) that is not in fact authorised by a user accessing services, the GBA (user) authentication and the DRM device authentication need to be securely linked together.

5.5 IMS registration – OITF

5.5.1 General

Subclause 5.5 specifies the message flows for IMS registration using SIP digest authentication or IMS AKA authentication by means of which service platform Providers and IMS Gateways located in esidential Networks can authenticate each other. These message flows are based on TS 33.203 and TS 24.229 (stage 3 specification).

NOTE Subclause 5.5 specifies authentication-related details of certain SIP messages. Elsewhere, for example at ETSI TISPAN, this SIP authentication method is often called "HTTP digest" as SIP digest RFC 3261 is identical to HTTP digest [RFC2617] – despite the fact that the protocol in question is SIP and not HTTP. The authentication method treated in 5.5 is referred to as "SIP digest" since the name "HTTP digest" might lead to the wrong impression that the protocol in question is HTTP.

5.5.2 Relevant functional entities and reference points

Figure 29 extracts the functional entities and reference points relevant for IMS Registration from the OIPF provider and Residential Network Architectures (see Figures B.2 and B.4 in Annex B of IEC 62766-1:2017).

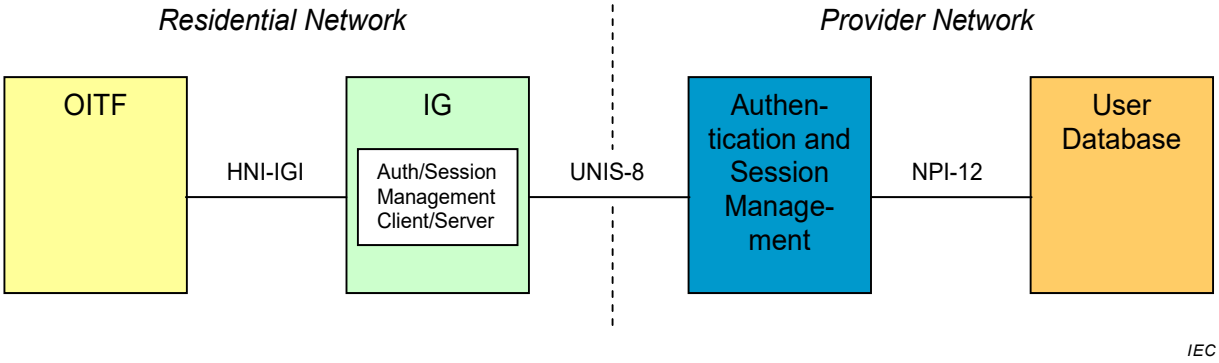

Figure 29 – OIPF functional entities and reference points involved in IMS registration

SIP digest authentication, and respectively IMS AKA authentication is interlaced into the IMS registration message exchange between the IMS Gateway (IG) and the authentication and Session Management (ASM) functional entities. IMS registration occurs either when the IG is powered up or when the IG receives a corresponding request from an OITF. The user database supplies the ASM with authentication vectors needed for SIP digest authentication, and respectively IMS AKA authentication.

5.5.3 Prerequisites

Prior to the first IMS Registration (and hence prior to the first SIP Digest or IMS AKA) protocol execution, the following parameters shall be provisioned:

a) to the IG:
   1) for SIP digest:
      - one or more IP Multimedia Private Identities (IMPI),
      - one or more IP Multimedia Public Identities (IMPU), each associated to one or more IMPIs,
      - one or more passwords, each assigned to one and only one of the IMPIs provisioned to the IG,
      - a service platform provider network domain name.

   NOTE In case of IMS AKA, the above parameters are in a UICC with an ISIM or USIM application.

   2) for IMS AKA, an ISIM or a USIM application shall always be used for authentication, as described in TS 33.203. For the purpose of this document, the ISIM is a term that indicates a collection of IMS security data and functions on a UICC.
      - The ISIM shall include:
        – one IMPI;
        – one or more IP Multimedia Public Identities (IMPU), associated with the IMPI;
        – a SPP network domain name referred as home network domain name in 3GPP specifications;
        – support for sequence number checking in the context of IMS Domain;
        – an authentication key;
        – the same framework for algorithms as specified for USIM.
      - There shall only be one ISIM for each IMPI.

b) and to the user database, the IMS subscription information comprising:
   1) the IMPI(s) and IMPU(s) provisioned to the IG,
   2) the association of the IMPU(s) to the IMPI(s),
   3) for SIP digest, the password(s) provisioned to the IG. The user database stores each password against the IMPI to which it is assigned,

4) for IMS AKA, the authentication key contained and protected within the UICC in the IG. The user database stores each authentication key against the IMPI to which it is assigned.

Methods for provisioning these parameters to IG and user database functional entities are outside the scope of this specification.

5.5.4 SIP digest message flows

Figure 30 shows the message flow for SIP digest authentication, which is interlaced into IMS registration messages.

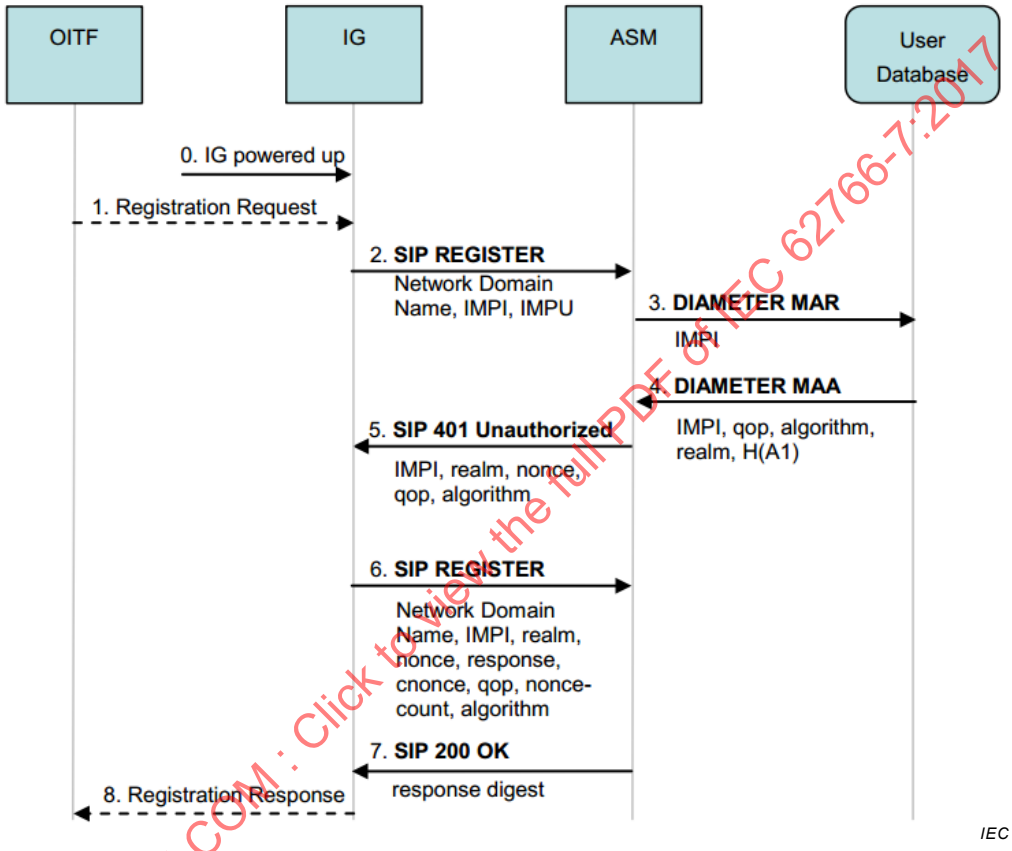

Figure 30 – SIP digest message flow interlaced into IMS registration

0) The IG is powered up. This can initiate the execution of steps 2 to 7.

1) OITF to IG: registration request
The OITF sends a request for registration to the IMS gateway (IG), when needed (the end user explicitly logs on for personalized services).

2) IG to ASM: SIP REGISTER
This request contains the SPP network domain name of the IG's IMS home network, an IMPI and an IMPU. If the ASM has a valid SIP digest authentication vector (SD-AV) for the specific IMPI, steps 3, 4 and 5 are omitted.

3) ASM to user database: DIAMETER MULTIMEDIA AUTH REQUEST (MAR)
The ASM requests a SD-AV from the user database with respect to the IMPI received in step 2.

4) User database to ASM: DIAMETER MULTIMEDIA AUTH ANSWER (MAA)
Along with the IMPI, the user database sends a SD-AV to the ASM containing the following data: qop value (quality of protection), the authentication algorithm, realm, and a hash value H(A1) of the IMPI, realm, and password. RFC 2617 provides additional information on the values in the authentication vector for SIP digest-based authentication. Upon reception of the MAA message, the ASM stores the H(A1) value and generates the nonce value needed to challenge the IG.

5) ASM to IG: SIP 401 unauthorized
The ASM denies the IG authentication but sends a SIP 401 unauthorized message to the IG in order to challenge the IG. This message contains the IMPI, the nonce, the authentication algorithm, and the realm and qop values.

6) IG to ASM: SIP REGISTER
After reception of message 5, the IG generates a client nonce (cnonce) and calculates an authentication response value using this cnonce and other values received in step 5 (see RFC 2617). The IG sends a new SIP REGISTER request to the ASM, this time with the authentication response along with the parameters IMPI, realm, nonce, response, cnonce, qop, nonce-count, and algorithm.

7) ASM to IG: SIP 200 OK (successful case)
After reception of the SIP REGISTER message containing the authentication response value, the ASM calculates the *expected* response value using the previously stored H(A1) and the stored nonce value together with other parameters (see RFC 2617). If the response value received from the IG equals the expected response value, the IG has been authenticated and the IMPU is registered in the ASM. In this successful case, the ASM sends the SIP 200 OK from ASM to the IG, enabling the IG to authenticate the SPP Network. This SIP 200 OK message contains a response digest calculated using the cnonce value generated by the IG prior to sending message 6.

8) IG to OITF: registration response
The IG informs the OITF about the result of the registration procedure (when step 1 was executed).

The details of the messages 2 to 7 are specified in TS 24.229.

5.5.5 IMS AKA message flows

To support IMS AKA, a UICC with an ISIM or USIM application shall be integrated into the IMS gateway (IG). From the IMS point of view, the IG thereby takes the role of an IMS subscriber. The UICC stores a long-term secret key K which is shared between the ISIM or USIM application and a user database belonging to the network operator that provides the ISIM or the USIM. Figure 31 shows the high-level message flows for user identification and authentication based on the IMS AKA procedure.

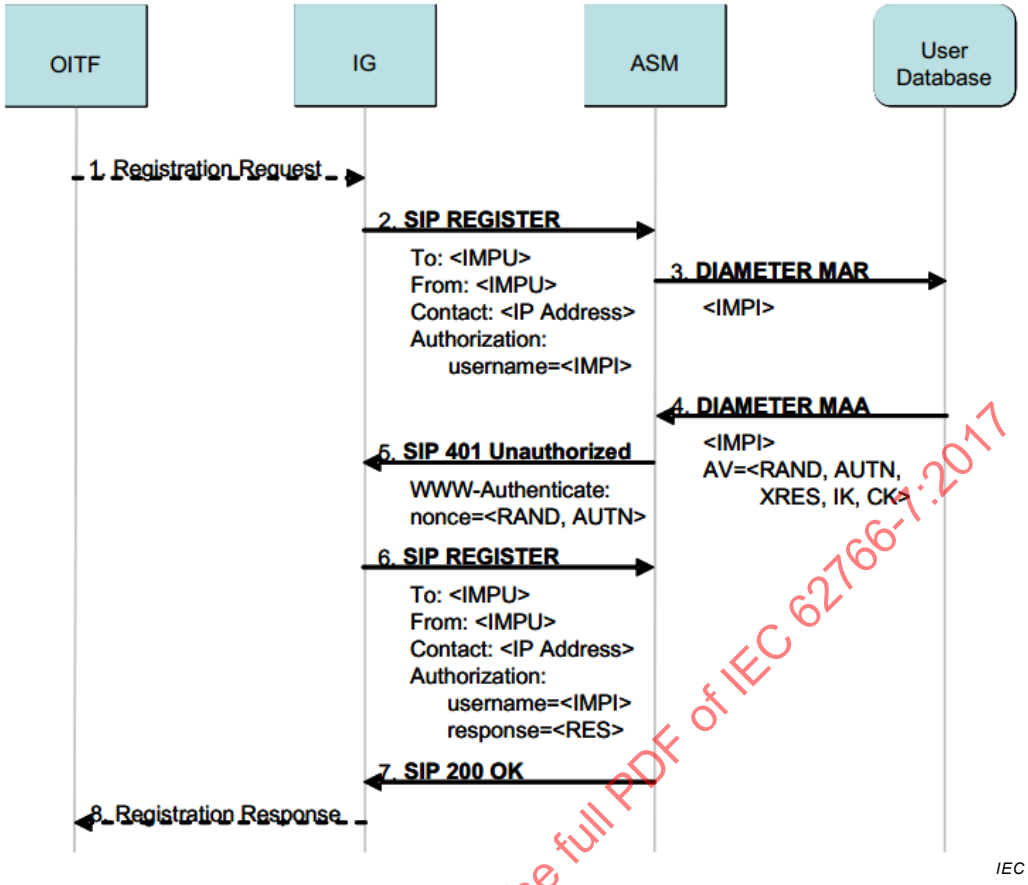

Figure 31 – User identification and authentication based on the IMS AKA procedure

The steps of the message flows are elaborated in the following manner:

0) The IG is powered up. This can initiate the execution of steps 2 to 7.

1) OITF to IG: Registration Request
The OITF sends a request for registration to the IMS gateway (IG), when needed (the end user explicitly logs on for personalized services).

2) IG to ASM: SIP REGISTER
This request contains the SPP network domain name of the IG's IMS home network, the IMPI and the IMPU. All this data is read from the ISIM.

3) ASM to user database: DIAMETER MULTIMEDIA AUTH REQUEST (MAR)
ASM requests authentication data from the User Database with respect to the IMPI received in step 2.

4) User database to ASM: DIAMETER MULTIMEDIA AUTH ANSWER (MAA)
The user database sends an Authentication Vectors (AV) to the ASM containing the following data: random challenge RAND, answer XRES expected by the IG in step 6, network authentication token AUTN, integrity key IK, and ciphering key CK. The authentication token AUTN contains a Message Authentication Code (MAC) enabling the IG to authenticate the SPP Network (see step 5).

5) ASM to IG: SIP 401 unauthorized
At this point in time, the ASM denies the IG authentication. Instead, it sends a SIP Unauthorized message with a WWW-authenticate header to the IG. This header contains RAND and AUTN. After reception of this message, the IG verifies the message authentication code contained in AUTN thereby authenticating its SPP Network.

6) IG to ASM: SIP REGISTER
ISIM computes the value RES on input of its version of the secret key K stored on the UICC of the IG. The IG sends a new SIP REGISTER request to the ASM, this time with RES as response to the challenge the ASM initiated in step 5.

7) ASM to IG: SIP 200 OK
If RES = XRES (successful case), ASM considers the IG as authenticated, and binds IMPU to the IP address <IP address>.

8) IG to OITF: Registration Response
The IG informs the OITF about the result of the registration procedure (when step 1 was executed).

In case of success, the ISIM of the IG is able, based on its knowledge of the secret key K and the authentication token AUTN, to calculate the same values of the integrity key IK and the ciphering key CK as those that the ASM received in step 4 from the User Database. The IG and the ASM use IK and CK to establish IPSec security Associations for protecting SIP signaling messages over the IG – ASM reference point.

The details of the messages 2 to 7 are specified in TS 24.229.

5.6 Session management and single sign on

5.6.1 General

User authentication does not need to be performed with each request. In order to avoid re-authentication at each request, a service (and/or SSA) can rely on authentication session management and single sign on. The following authentication session management can be used: cookies, URL parameters and HTTP authentication session, if HTTP or GBA authentication has been used. SAML web-based single sign on can be used.

5.6.2 Cookie session

The OITF shall support HTTP session management using cookies as described in RFC 2109. The cookie is opaque data to the OITF.

Persistent cookies shall be stored in non-volatile memory (Flash, HDD, etc.) in the OITF.

All OITF applications using HTTP (not only DAE) shall be able to create, read and delete **persistent** cookies with respect to domain restriction as specified in RFC 2109. Persistent cookies should be shared between all components in an OITF.

Users shall have the possibility to delete **persistent** cookies in OITF.

Figure 32 shows an example of sequences based using a cookie session.

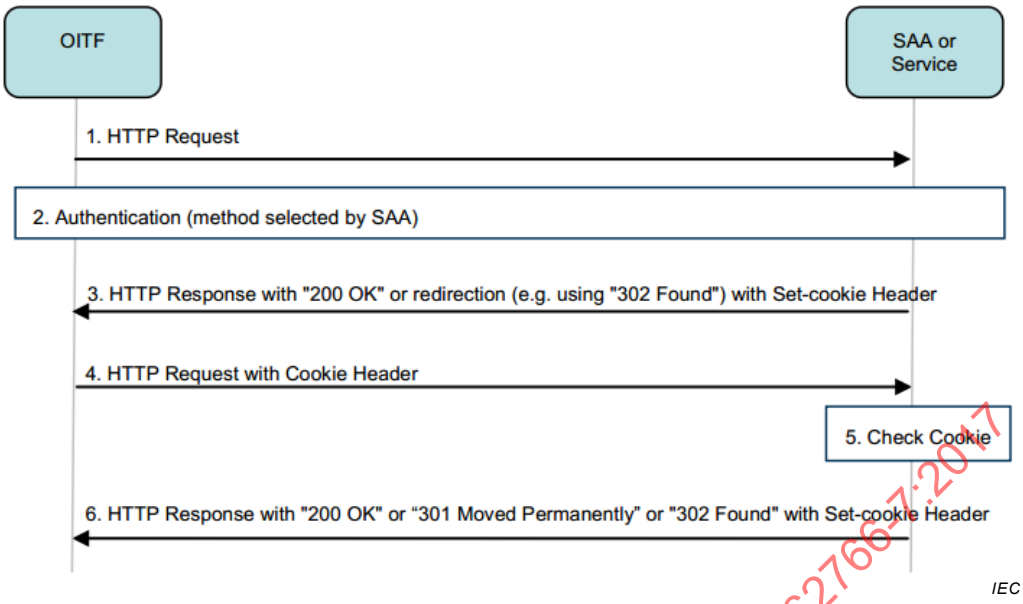

Figure 32 – Session management using cookie

The steps of the message flow are elaborated in the following manner:

1) The OITF requests a service with no valid cookie.
2) The service triggers the SAA authentication and the SAA performs the wanted authentication.
3) The service or SAA sets a cookie using set-cookie response header as specified in RFC 2109.
4) The OITF requests a service. Applicable cookies are provided in each HTTP request as specified in RFC 2109 (domain-match, port-match, path-match, Max_Age-match, etc.).
5) The service checks the cookie. Cookie checking is out of the scope of this specification.
6) The service optionally refreshes the cookie and sets it again using set-cookie response header as specified in RFC 2109.

Steps 4 to 6 are performed for each new HTTP request according to cookie matching.

5.6.3 URL parameters

An alternative to cookies for passing session data is the use of hidden input fields in forms or URL parameters in requests passed to the server. These mechanisms are transparent to the OITF. Figure 33 shows an example message flow using URL parameters. The use of hidden input fields can also be achieved with HTTP POST. The mechanism of using HTTP POST is not described in 5.6.3.

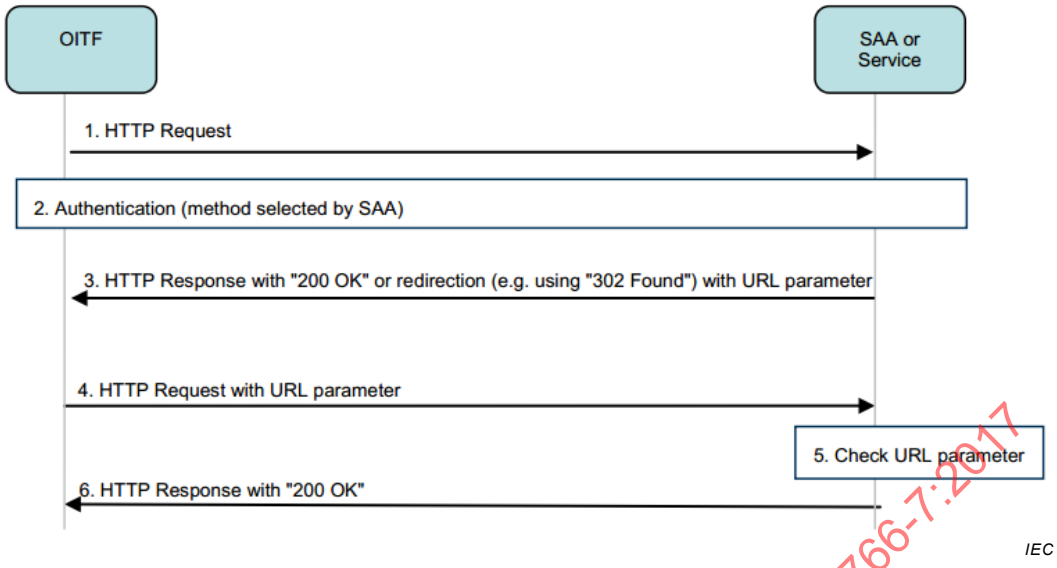

Figure 33 – Session management using URL parameters

The steps of the message flow are elaborated in the following manner:

1) The OITF requests a service with no valid authentication session.
2) The service triggers the SAA authentication and the SAA performs the wanted authentication.
3) The service or SAA redirects to the service with a new URL parameter for session data.
4) The OITF requests a service with the URL parameter.
5) The service checks the session data in the URL parameter. Session data is opaque data and out of the scope of this specification.
6) The service serves the request.

NOTE 1 URL parameters are often used to pass session information from an HTTP session to a session using another protocol (e.g. RTSP).

NOTE 2 A web server (service or SAA) can maintain an HTTP session using this technique. But the server is responsible for modifying every link URL, so that the session data is posted in a form or appended to the request.

NOTE 3 Passing information through URL parameters is highly insecure.

5.6.4 HTTP authentication session

When using HTTP authentication, a server can rely on HTTP authentication session as specified in RFC 2617.

The user may be prompted to allow OITF to store HTTP authentication parameters, i.e. username and password, in non-volatile memory.

All OITF applications using HTTP (not only DAE) should have access to HTTP authentication parameters, i.e. username and password.

All OITF applications using HTTP (not only DAE) should share the current HTTP authentication session (e.g. B-TID, Ks_NAF, nonce, cnonce, nonce-count and opaque values).

If username and password can be stored, the user shall have the possibility to change stored username and passwords in OITF for a given protection space as specified in RFC 2617.

Figure 34 shows an example of sequences based on HTTP authentication session.

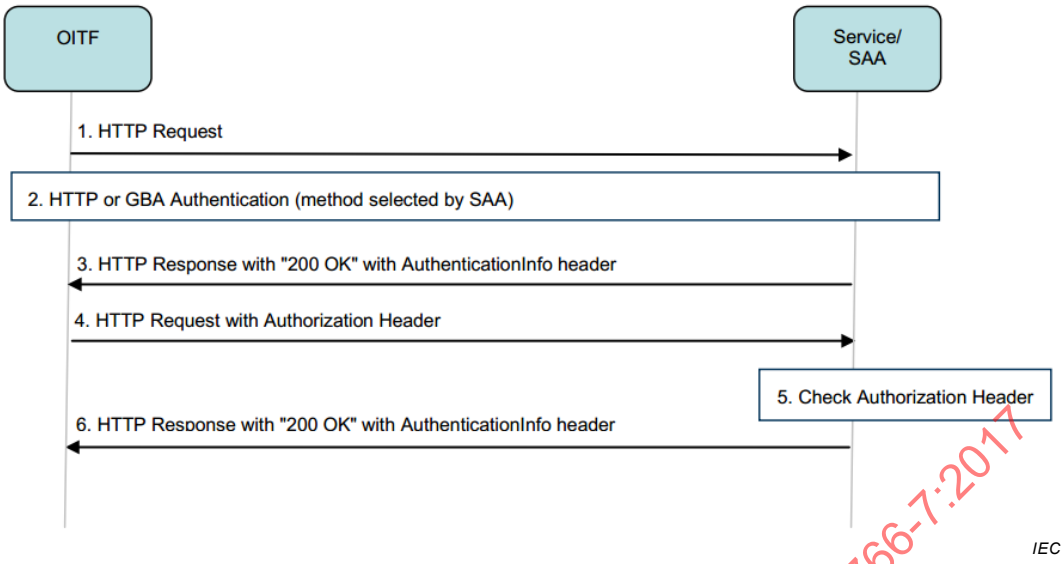

Figure 34 – HTTP authentication session

The steps of the message flow are carried out in the following order:

1) The OITF requests a service with no valid HTTP authentication session.
2) The service/SAA performs HTTP or GBA authentication.
3) The service/SAA serves the request including an authenticationInfo header as specified in RFC 2617.
4) The OITF requests again a service. Appropriate HTTP authorisation headers are provided in each HTTP request within the protection space (specified by domain) as specified in RFC 2617.
5) The service/SAA checks the authorisation header.
6) The service/SAA serves the request including an authenticationInfo header.

Step 4 to 6 may be performed for each new HTTP request within the protection space.

5.6.5 SAML Web-based SSO

Subclause 5.6.5 specifies the functionality and possible message flows for basic SAML web-based single sign-on.

SAML Web-based single sign-on shall adhere to 4.1 of OASIS SAML profiles, whereby either a SAML HTTP POST or a SAML HTTP SimpleSign binding of a SAML <Response> message from the SAA shall use MIME-type "application/ce-html+xml" as defined in CEA-2014-A. A standard CEA-2014-A compatible browser is able to handle the SAML HTTP redirect and POST bindings defined in 5.6.5, without requiring any extensions to CEA-2014-A. This profile of SAML therefore does not add requirements to the OITF besides supporting DAE functionality.

The remainder of 5.6.5 describes sequences of how SAML web-based single sign-on is handled between the different relevant entities, i.e. the service, the SAA, and the OITF.

The sequences assume that the SAA and service provider share a logical identification of the user in advance of the described sequence, which is shown in Figure 35. The user is known to the SAA. The SAA maintains knowledge of the user's authentication credentials.

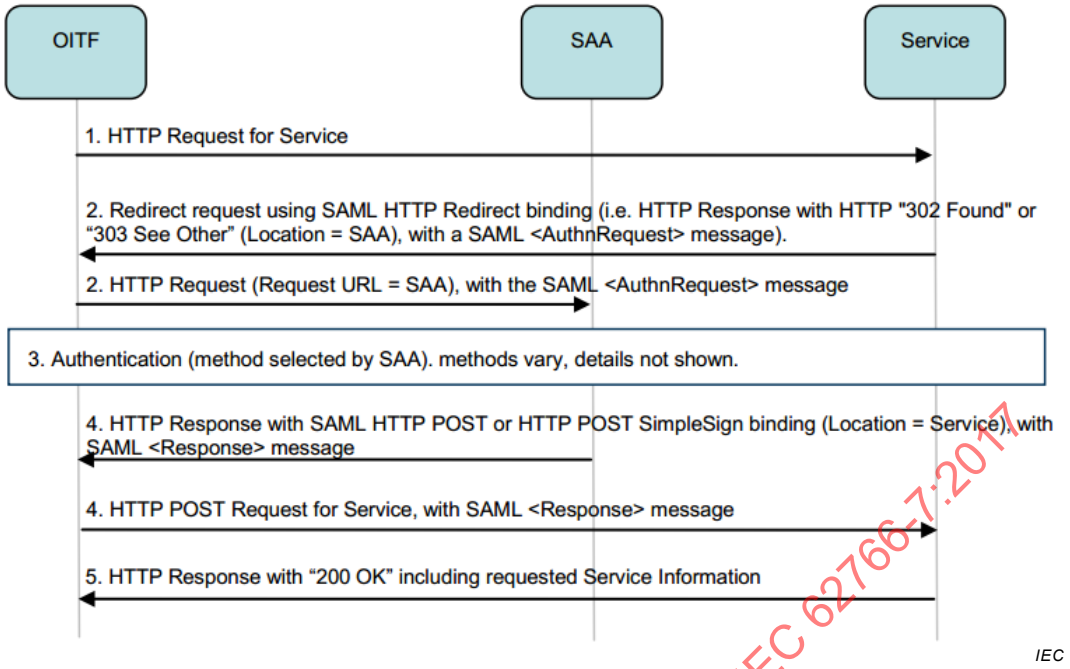

Figure 35 – SAML Web-based SSO

The steps of the message flow are carried out in the following order:

1) The OITF requests a service. Authentication is needed and there is no valid authenticated service session.
2) The requested service triggers SAA authentication by issuing a redirect request using SAML HTTP redirect binding, i.e. an HTTP response with HTTP "302 Found" or "303 See Other" (Location = SAA) , with a SAML <AuthnRequest> message (as defined in 3.4.1 of OASIS SAML).
3) The SAA authenticates the user. Various methods exist for this. Valid methods include the authentication methods as defined in 5.4.1 through 5.4.5 of this document.
4) The SAA responds with either an SAML HTTP POST or HTTP POST SimpleSign binding of a SAML <Response> message (as defined in 3.3.3 of OASIS SAML). Since the browser of the OITF is CE-HTML compliant, the SAA response message shall use MIME-type "application/ce-html+xml" as defined in CEA-2014-A. The CE-HTML browser will load the CE-HTML page with the SAML POST binding, after which it issues an HTTP POST request to the target service with the SAML <Response> message as payload.
5) The requested service checks the SAML <Response> message to see if authentication succeeded. If it did succeed, the service serves the request.

6 Forced play-out using media zones

Content may contain navigation constraints for forced play-out (see 5.2 and 5.3 of IEC 62766-2-1:2016).

If an OITF supports DMZ navigation constraints signalled in zone maps within MP4 files or MPEG-2 TS, it shall indicate this via the appropriate capability signalling as specified in IEC 61766-5-1. If an OITF does not understand the navigation constraints, this capability description is either absent or set to "false". If the capability description to support such DMZ navigation constraints is set to "true", an OITF shall obey the signalled constrains and shall not ignore the presence of navigation constraints.

NOTE 1 When this capability description is not sent or is set to "false", it is the choice of the service provider whether the content shall be sent to the OITF as there is no guarantee whether the navigation constraints will be obeyed.

For navigation constraints pertaining to protected content, the zone map information may be integrity protected using an included signature as described in [MRL_DMZ]. If the zone map is integrity protected using a signature, and if the terminal-centric approach is used for content protection, the key used for signature is derived as described in [MRL_DMZ] 2.1 and 2.3 for MP4 (using a key derived from the content key), and as described in Marlin DMZ 7.2.2 for MPEG-2 TS (using a signature key signalled in ECMs). Note that the Marlin DMZ specification contains normative language on what should happen if the integrity of the signalled constraints cannot be verified. If an OITF supports DMZ navigation constraints and if integrity protection is used, the OITF shall verify the integrity of the signalled constraints. If the integrity of the signalled constraints cannot be verified, the OITF shall not play the associated content.

NOTE 2 Server-based play-out control is described in 7.2.3.3 of IEC 62766-4-1:2017. The concept there is applicable to interactive streaming where the server may or may not grant requests for trick-mode commands like fast forward.

Annex A
(informative)

Link of user authentication and DRM device authentication

This annex describes the generic mechanism to link user authentication result with device authentication in OITF. Although the device authentication mechanism is provided by Marlin, the user authentication mechanism varies depending on the system environment.

The mechanism described in this annex uses HTTP digest authentication RFC 2617 and assumes that user identifier and its secret information (e.g. password, Ks_NAF) are shared between OITF and providers Network in advance of the sequences between CSP and CSP-T server.

Figure A.1 explains how the user authentication and device authentication are securely correlated with each other by Marlin action token acquisition and Marlin protocol.

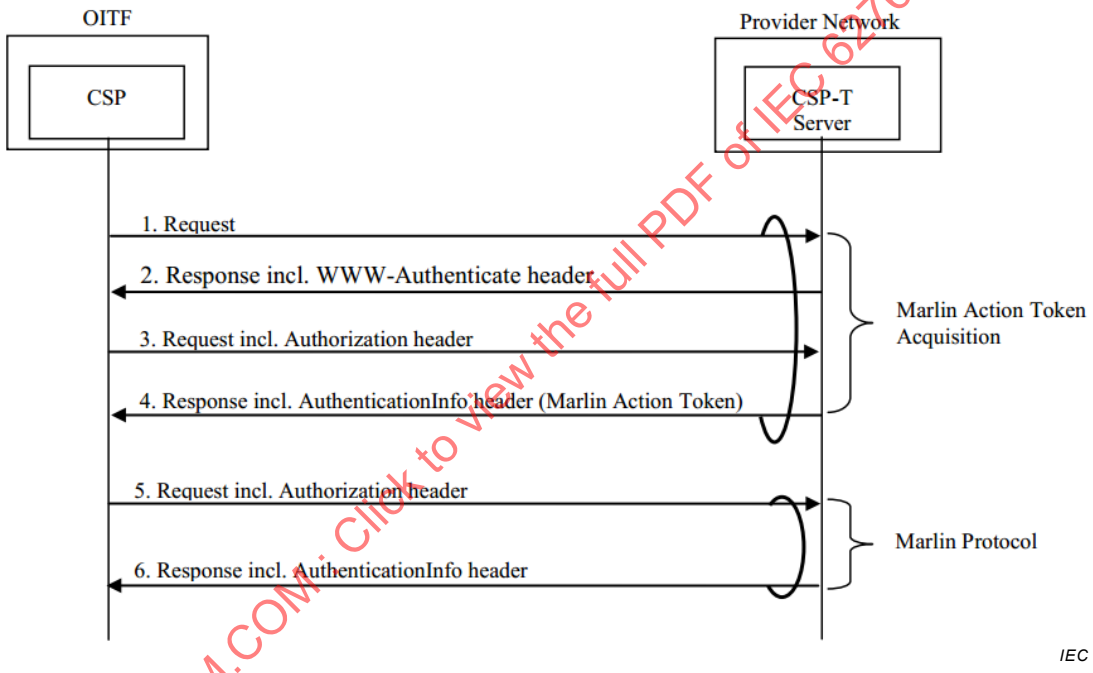

Figure A.1 – User authentication for CSP, CSP-T server communication

The steps of the message flow are carried out in the following order:

1) The CSP requests a Marlin action token to the CSP-T server.
2) When the CSP-T server receives the request from CSP for the Marlin action token, the CSP-T server responds with a "401 unauthorized" status code with a WWW-authenticate header defined in RFC 2617.
3) When the CSP receives the response, the CSP sends the request which includes an authorisation header defined in RFC 2617. The user identifier and its secret information are used as username and password for generation of the authorisation header.
4) When the CSP-T server receives the authorisation header:
   - the CSP-T server verifies the authorisation header;
   - if the verification succeeds, the CSP-T server generates user information to be included into the business token, and stores the combination of user identifier from the authorisation header and user information to be included into the business token;