ETSI TS 183 063 V2.8.1 (2011-02)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based IPTV stage 3 specification

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or
perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF).
In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive
within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

ETSI

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1   Scope

The present document describes the Procedures on the Functional Entities and Call Flows for the protocols and their possible enhancements to support IPTV services based on the architecture and stage 2 information flows described in TS 182 027 [2].

The possible enhancements of protocols will define the scope of new or enhanced protocol specifications.

Besides, the interaction with other Simulation Service will be considered.

> NOTE: The present document relies on the architectural framework defined in TS 182 027 [2] for IMS-based IPTV Stage 2 and may need to be updated once the open issues identified in the present document are resolved.

The present document is applicable to:

- the interface between the User Equipment (UE) and the Call Session Control Function (CSCF);

- the interface between the S-CSCF and IPTV Service Control Functions (SCF);

- the interface between the S-CSCF and IPTV Service Discovery Functions (SDF);

- the interface between the S-CSCF and the Media Control Functions (MCF);

- the interface between the User Equipment (UE) and IPTV Service Selection Functions(SSF);

- the interface between the User Equipment (UE) and Elementary Control Functions (ECF)/Elementary Forwarding Functions (EFF);

- the interface between the User Equipment (UE) and IPTV Service Control Functions (SCF).

2   References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

> NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1   Normative references

The following referenced documents are necessary for the application of the present document.

[1]   ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[2]   ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".

[3]   ETSI TS 102 034 (V1.3.1): "Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks".

[4]   ETSI TS 102 471: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Electronic Service Guide (ESG)".

[5]   ETSI TS 102 472: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Content Delivery Protocols".

[6]   OMA-TS-BCAST-ServiceGuide-V1-0: "Open Mobile Alliance: Service Guide for Mobile Broadcast Services".

[7]   OMA-TS-BCAST-DVB-Adaptation-V1-0: "Open Mobile Alliance: Broadcast Distribution System Adaptation - IPDC over DVB-H".

[8]   IETF RFC 2326: "Real Time Streaming Protocol (RTSP)".

[9]   IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[10]   ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

[11]   ETSI TS 124 109: "Universal Mobile Telecommunications System (UMTS); Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details (3GPP TS 24.109 Release 7)".

[12]   ETSI TS 183 023: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating NGN PSTN/ISDN Simulation Services".

[13]   ETSI TS 102 539: "Digital Video Broadcasting (DVB); Carriage of Broadband Content Guide (BCG) information over Internet Protocol (IP)".

[14]   ETSI TS 133 222: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (3GPP TS 33.222 Release 7)".

[15]   IETF RFC 5874: "An Extensible Markup Language (XML) Document Format for Indicating A Change in XML Configuration Access Protocol (XCAP) Resources".

[16]   ETSI TS 184 009: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) Rules covering the use of TV URIs for the Identification of Television Channels".

[17]   IETF RFC 3925: "Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[18]   IETF RFC 1035: "Domain names - implementation and specification".

[19]   IETF RFC 1034: "Domain names - concepts and facilities".

[20]   ETSI ES 283 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 modified]".

[21]   ETSI ES 283 030: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Presence Service Capability; Protocol Specification [3GPP TS 24.141 V7.0.0, modified and OMA-TS-Presence-SIMPLE-V1-0, modified]".

[22]   Void.

[23]   OMA-TS-Presence-SIMPLE-V1-0-20060725-A: "Open Mobile Alliance: Presence SIMPLE Specification".

[24]   ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 Release 8)".

[25] IETF RFC 4756: "Forward Error Correction Grouping Semantics in Session Description Protocol".

[26] IETF RFC 5875: "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package".

[27] Void.

[28] IETF RFC 3376: "Internet Group Management Protocol, Version 3".

[29] IETF RFC 3810: "Multicast Listener Discovery Version 2 (MLDv2) for IPv6".

[30] IETF RFC 2616: "Hypertext Transfer Protocol - HTTP/1.1".

[31] IETF RFC 2782: "A DNS RR for specifying the location of services (DNS SRV)".

[32] IETF RFC 2246: "The TLS Protocol Version 1.0".

[33] ETSI TS 102 822-3-1: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 3: Metadata; Sub-part 1: Phase 1 - Metadata schemas".

[34] ETSI TS 101 154: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream".

[35] ETSI TS 102 822-4: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 4: Phase 1 - Content referencing".

[36] ETSI ES 283 035: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol".

[37] DSL Forum TR-069 Amendment 2: "CPE WAN Management Protocol v1.1".

[38] ETSI TS 183 060: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Subsystem (RACS); Re interface based on the DIAMETER protocol".

[39] IETF draft-ietf-sipping-config-framework-18: "A Framework for Session Initiation Protocol User Agent Profile Delivery".

NOTE: Available at draft-ietf-sipping-config-framework-18.

[40] IETF RFC 5234: "Augmented BNF for Syntax Specifications: ABNF".

[41] IETF RFC 3261: "SIP: Session Initiation Protocol".

[42] IETF RFC 4566: "SDP: Session Description Protocol".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Void.

[i.2] ETSI TS 183 017: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification".

[i.3]   ETSI TS 183 033: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia; Diameter based protocol for the interfaces between the Call Session Control Function and the User Profile Server Function/Subscription Locator Function; Signalling flows and protocol details [3GPP TS 29.228 and 3GPP TS 29.229, modified]".

[i.4]   ETSI TS 129 329: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329 Release 7)".

[i.5]   IEEE 1003.1-2004: "Standard for information technology - portable operating system interface (POSIX). Shell and utilities".

[i.6]   IETF draft-stiemerling-rtsp-announce-01: "RTSP 2.0 Asynchronous Notification".

[i.7]   IETF draft-ietf-sip-ipv6-abnf-fix-05: "Essential correction for IPv6 ABNF and URI comparison in RFC 3261".

[i.8]   IETF RFC 4395: "Guidelines and Registration Procedures for New URI Schemes".

[i.9]   IETF RFC 3406: "Uniform Resource Names (URN) Namespace Definition Mechanisms".

[i.10]   draft-ietf-sip-xcapevent-00.

NOTE: Available at http://tools.ietf.org/html/draft-ietf-sip-xcapevent-00.

3   Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACK	ACKnowledge character
AP	Authentication Proxy
AS	Application Server
AUID	Application Unique ID
B2BUA	Back To Back UA
BC	BroadCast
BCG	Broadband Content Guide
CNGCF	Customer Network Gateway Configuration Function
CoD	Content on Demand
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVB	Digital Video Broadcasting
DVBSTP	DVB SD&S Transport Protocol
ECF	Elementary Control Functions
ECF/EFF	Elementary Control Function/Elementary Forwarding Function
EFF	Elementary Forwarding Functions
EPG	Electronic Program Guide
ERE	Extended Regular Expressions
ESG	Electronic Service Guide
FEC	Forward Error Correction
HTTP	Hypertext Transfer Protocol
I-CSCF	Interrogation - Call Session Control Function
ICSI	IMS Communication Service Identities
ID	Identifier
IFC	Initial Filter Criteria
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol TeleVision
MCF	Media Control Function
MDF	Media Delivery Function

MF	Media Function
MLD	Multicast Listener Discovery
NGN	Next Generation Network
NPT	Normal Play Time
N-PVR	Network-Personal Video Recorder
nPVR	network-side Personal Video Recorder
OMA	Open Mobile Alliance
P-CSCF	Proxy - Call Session Control Function
PSI	Public Service Identity
RACS	Resource and Admission Control Subsystem
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SAD	Service Action Data
SCF	Service Control Function
S-CSCF	Serving - Call Session Control Function
SD&S	Service Discovery and Selection
SDF	Service Discovery Function
SDP	Session Description Protocol
SGDD	Service Guide Delivery Descriptors
SGDU	Service Guide Delivery Units
SIP	Session Initiation Protocol
SNTP	Simple Network Time Protocol
SOAP	Simple Object Access Protocol
SRV	SerVice Records
SSF	Service Selection Function
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TsTV	Time shift TV
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
UPSF	User Profile Server Function
URI	Uniform Resource Identifier
VoD	Video on Demand
XCAP	XML Configuration Access Protocol
XDM	XML (extensible markup language) Data Management Server
XML	eXtensible Markup Language

4 Applicability

4.1 Overview

The overall functional architecture for the IMS-based IPTV service conforms to TS 182 027 [2].

This clause provides the list of protocols and related reference points.
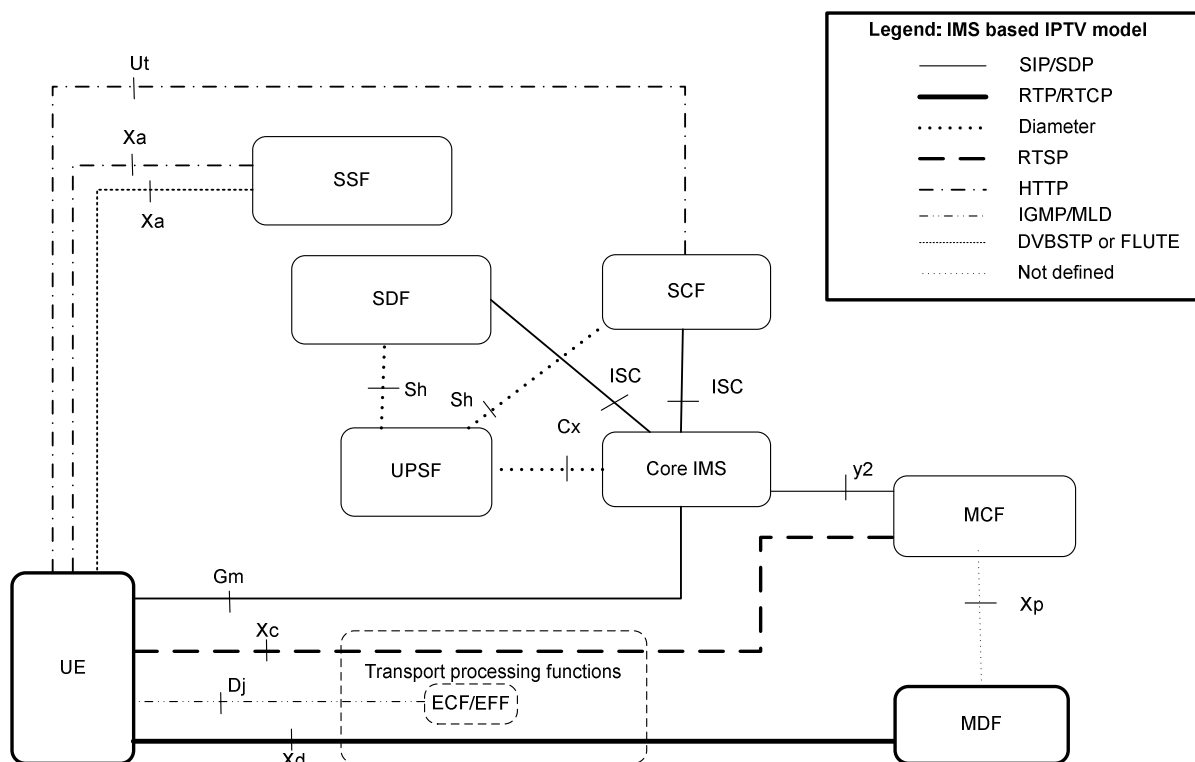
Figure 4.1: Protocols used in functional architecture for the IMS-based IPTV service

Table 4.1: IMS based IPTV functional entities and protocols used on reference points

FE/ Reference point (protocol)	UE	IMS core	UPSF	SDF	SSF	SCF	MCF	MDF	ECF/ EFF
UE	---	Gm (SIP/SDP)	---	via Core IMS (SIP/SDP)	Xa (HTTP, DVBSTP, FLUTE)	Ut (HTTP), via Core IMS (SIP/SDP)	Xc (RTSP) (Note 1)	Xd (UDP/RT) (Note 1)	Dj, Di IGMP/ MLD
IMS core	Gm (SIP/SDP)	---	Cx (Diameter)	---	---	ISC (SIP/SDP)	y2 (SIP/SDP)	---	---
UPSF	---	Cx (Diameter)	---	Sh (Diameter)	---	Sh (Diameter)	---	---	---
SDF	via Core IMS (SIP/SDP)	---	Sh (Diameter)	---	---	---	---	---	---
SSF	Xa (HTTP, DVBSTP, FLUTE)	---	---	---	---	---	---	---	---
SCF	Ut (HTTP), via Core IMS (SIP/SDP)	ISC (SIP/SDP)	Sh (Diameter)	---	---	---	via Core IMS and y2 (SIP/SDP)	---	---
MCF	Xc (RTSP) (Note 1)	y2 (SIP/SDP)	---	---	---	via Core IMS and y2 (SIP/SDP)	---	Xp (not defined)	---
MDF	Xd (UDP/RTP) (Note 1)	---	---	---	---	---	Xp (not defined)	---	---
ECF/ EFF	---	---	---	---	---	---	---	---	---
NOTE 1: As described in TS 182 027 [2], clauses 6.4 and 6.5, Xc and Xd are logical reference points that can be decomposed into Dj and possibly Di, Ds or Iz reference points depending on the location of the MCF or MDF.									
NOTE 2: Annex H lists compliance requirements for the protocols listed in this table.									

Use the SIP/SDP protocol across the following interfaces is described in clause 5:

- interface Gm;

- interface ISC;

- interface y2.

Usage of the HTTP protocol across the following interfaces is described in clause 6:

- interface Xa;

- interface Ut.

Usage of the RTSP protocol across the following interfaces is described in clause 7:

- interface Di, Dj, Ds or lz.

Usage of the UDP/RTP/RTCP protocol across the following interfaces is described in clause 11:

- interface Di, Dj, Ds or Iz.

Usage of the IGMP/MLD protocol across the following interfaces is described in clause 8:

- interface Dj, Di.

NOTE: Whether usage of multicast protocols (IGMP,MLD) is supported on Xc, Xd interface or how MDF joins
          multicast streams (e.g. for nPVR or BC with trick mode services) is out of the scope of the present
          document.

Usage of the DVBSTP protocol across the following interface is described in clause 9:

- interface Xa.

Usage of the FLUTE protocol across the following interface is described in clause 10:

- interface Xa.

4.2   Functional entities

4.2.1   User Equipment (UE)

The UE is a functional entity that provides the user with access to IPTV services.

4.2.2   Service Control Function (SCF)

The SCF is a functional entity that provides IPTV service logic and the functions required to support execution of such
logic.

4.2.3   Service Discovery Function (SDF)

An SDF is a functional entity that provides service attachment information to the UE.

4.2.4   Service Selection Function (SSF)

An SSF is a functional entity that provides service selection information to the UE.

4.2.5   Media Control Function (MCF)

The MCF is a functional entity that provides the UE with functions required to control media flows and manages the
MDFs under its control.

4.2.6   Media Delivery Function (MDF)

The MDF is a functional entity that delivers content data to the UE.

4.2.7   Core-IMS

The Core IMS includes a number of functional entities identified in ES 282 007 [1]. For the purpose of supporting IPTV services, the following functional entities of the Core IMS are involved:

- the P-CSCF;

- the S-CSCF;

- the I-CSCF;

- the IBCF in case the P-CSCF and the I/S-CSCF or the CSCF and the MCF are in different administrative domains.

The behaviour of these functional entities with regards to SIP and SDP shall conform to ES 283 003 [20].

5   Procedures using SIP/SDP for IMS-based IPTV

Use the SIP/SDP protocol across the following interfaces is described in this clause:

- interface Gm;

- interface ISC;

- interface y2.

SIP/SDP capable functional entities are following:

- UE.

- SCF.

- SDF.

- MCF.

- Core IMS.

   NOTE: Summary of compliancy requirements and referred specification are listed in clause H.1.

5.1   User Equipment (UE)

5.1.1   Procedure for IMS registration

As specified in TS 182 027 [2], clause 8.2 the UE shall perform IMS registration before launching a service attachment procedure.

The behaviour of the UE with regards to IMS registration shall comply with ES 283 003 [20].

5.1.2   Procedure for service attachment

If the SDF is known as per annex I the Pull mode as in clause 5.1.2.2 shall be used, else the UE shall be preconfigured to use the public user identity of the user to send a SIP SUBSCRIBE request according to the Pull mode or to expect a SIP MESSAGE request according to Push mode as in clause 5.1.2.1.

5.1.2.1 Push mode

Upon receipt of a SIP MESSAGE request from the SDF, the UE shall parse the XML document as described in clause 5.1.2.2.2.

5.1.2.2 Pull mode

Service Attachment, the UE shall generate a SUBSCRIBE request. The behaviour of the UE when processing a SUBSCRIBE request shall conform to ES 283 003 [20], clause 5.1.2A.1.

5.1.2.2.1 Subscription

When the UE intends to retrieve service attachment information from the SDF, it shall generate a SUBSCRIBE request for the "ua-profile" event package defined in annex Y.

The contents of the SUBSCRIBE request shall be as follows:

- The value of the Request-URI shall be set to one of following:

    - The PSI of the SDF which is retrieved using SDF Discovery procedures specified in annex I, or

    - When the SDF identify is not present the public user identity of the IPTV end user.

- The From and To header shall be set to the public user identity of the IPTV end user.

- The Accept header shall include the content-type identifier that corresponds to the registered MIME type of XML documents representing IPTV profiles: "application/vnd.etsi.iptvdiscovery+xml".

- The Event header shall be set to the "ua-profile" event package.

- The Event parameters shall be set as follows:

    - The "profile-type" parameter shall be set to "application".

    - The "vendor", "model" and "version" parameter values shall be set to values specified by the implementer of the user equipment, as specified in ES 283 003 [20].

    - The "appids" parameter shall be set to " urn:org:etsi:ngn:applications:ims-iptv-service-discovery".

The UE may include a SIP SUBSCRIBE message body associated with the appid " urn:org:etsi:ngn:applications:ims-iptv-service-discovery ". The message body includes the capabilities of the UE which is sent to the SDF.

NOTE: Process of registering the appid is aligned with IETF specification in annex Y.

If the SIP SUBSCRIBE contains a message body, the details of the SIP SUBSCRIBE are as follows:

- Content Type header shall be set to "application/vnd.etsi.iptvueprofile+xml".

- A message body shall be present for conveying UE-specific information as defined in annex P. This includes:

    - User Equipment ID.

    - User Equipment Class: Specifies the type of UE. The currently defined types are "STB", "Mobile" and "PC".

    - UE Capabilities: This defines the set of UE capabilities and could include:

        ▪ Physical resolution of the screen of the rendering device (defined in vertical and horizontal number of pixels).

        ▪ Supported coding formats (defined using the Coding XML element from TV-Anytime (TS 102 822-3-1 [33]), and using the classification schemes from MPEG7 and DVB).

        ▪ Optionally, supported Video Frame Rates (defined as per TS 101 154 [34]) associated with the encoding format.

■ Supported transport protocols (MPEG2TS over UDP, MPEG2TS over RTP, direct RTP).

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header of the received response.

The UE shall automatically refresh the subscription, either 600 seconds before the expiration time if the initial subscription was for greater than 1 200 seconds, or when half of the time has expired if the initial subscription was for 1 200 seconds or less. If a SUBSCRIBE request to refresh a subscription fails with a non-481 response, the UE shall still consider the original subscription valid for the duration of the most recently known "Expires" value according to ES 283 003 [20]. Otherwise, the UE shall consider the subscription invalid and start a new initial subscription according to ES 283 003 [20].

5.1.2.2.2 Receiving notifications

Upon receipt of a NOTIFY request on the dialog which was generated during subscription, the UE shall look for a message body with a content-type header indicating "application/vnd.etsi.iptvdiscovery+xml ". The IPTV application within the UE shall parse the XML document contained in the message body.

The list of parameters which are described in clause 5.2.2.3 shall be used for service selection information retrieval according to clause 6.1.1 in unicast mode and clause 8.1.1 in multicast mode.

When parsing the list of parameters the UE shall take the following action:

- Information relates to SSF whom the UE has already an entree.

    - If the "@version" attribute is present and has not the same value or if not present, then the UE performs the following actions:

        ■ For parameters related to this SSF already present in the UE: the UE shall update these parameters with the new values sent by the SSF. If the Segment@Version has not the same value, the UE shall update service selection information from the SSF before using it.

        ■ For parameters related to this SSF not present in the UE: the UE shall store the new parameters.

    - If the "@version" attribute is present and has the same value, the UE shall not update the stored SSF information.

- Information relates to an SSF not known by the UE: the UE creates a new entry for this SSF with all indicated parameters.

After all elements have been processed, the UE shall return a SIP 200 OK response to the NOTIFY request.

Failure to perform subscription refresh does not imply that there is a loss of communication to SSF or SCF. The UE has an option to continue using the lists of parameters from the last NOTIFY.

After deregistration, the UE may keep stored information on per user basis. As for subscription refresh, the UE may use the stored information if initial subscription fails after a new registration.

5.1.3 Procedure for BC service

5.1.3.1 Session initiation

The UE shall support the procedures specified in ES 283 003 [20] for originating sessions.

Upon a request for a BC session initiation, the UE shall generate an initial INVITE request as specified in ES 283 003 [20] for an originating UE. The Request-URI in the INVITE request shall be the well known PSI (Public Service Identifier) of the BC Service.

An SDP Offer shall be included in the request. The SDP offer shall be done in accordance with the parameters received during UE service selection procedure and with media capabilities and required bandwidth available for the BC session. If the user desires to join a BC service outside of this negotiated set of channels, a session modification is required.

The SDP offer at media level shall include the following elements:

- The m-line(s) shall be set according to the mapping defined in clause L.2 for the BC service which the UE intends to join first.

- The c-line(s) shall be set according to the mapping defined in clause L.2 for the BC service which the UE intends to join first.

- An a=bc_service:BCServiceId line to indicate the BC service which the UE intends to join first.

- Optionally one or more a=bc_service_package attributes (see below) as defined in annex N. In the first initial offer it shall not contain mult_list and bc_service_id list parameters. If the initiation is the result of a previously denied initiation the UE may restrict the BC services by including mult_list.

- If the UE has knowledge of the largest bandwidth of all the BC services included in the session, the b-line shall be included and set to this value.

- An a=recvonly line.

Additionally, FEC streams may be defined, as described in clause 5.1.3.1.1.

When the UE receives any SIP request or response, the UE shall examine the media parameters in the received SDP. The UE shall restrict the BC services that it joins according to the a=bc_service_package parameters received from the SCF. If the UE has retrieved the IPTV User profile prior to BC session initiation, it may ignore the a=bc_service_package parameters, if present (see clause 5.3.1.1).

If the user desires to join a BC service outside of this negotiated set, a session modification is required.

If the UE receives a 488 error code with warning 370 Insufficient Bandwidth the UE may perform a new SIP INVITE with a lower maximum bandwidth for BC service the UE intends to join. This procedure may be repeated. If no agreement can be reached the UE may display a failure message to the user.

When the UE receives the SIP final response, the UE shall joins the multicast channel according to the a=bc_service line.

5.1.3.1.1 Additional SDP lines for FEC streams

When the UE decides to connect to FEC stream(s) associated to the original BC stream(s), it shall include additional SDP lines in the SDP offer as follows:

- One or more m line(s) for each FEC stream exposed through the SSF:

  - It shall be set according to the mapping defined in clause L.2.

  - It shall contain a c-line according to the mapping defined in clause L.2.

If the BC content is defined through a single m-line, a grouping line may be included.

If the BC content is defined through several m-lines, grouping line(s) shall be included, one for each BC m-line that is associated to a FEC stream.

The grouping line uses the "FEC" semantic as defined in RFC 4756 [25]:

- a=group:FEC:<original stream id> <FEC stream id>
  The present document supports only the DVB-IP AL-FEC Base layer, so there can be only one <FEC stream id> associated to an original stream.

  - The original stream id shall reflect the value hold by the media description of one stream in its a=mid attribute.

  - The FEC stream id shall reflect the value hold by the media description of the DVB-IP AL-FEC Base layer FEC stream (associated to the original stream) in its a=mid attribute.

Furthermore, when grouping line is included, there shall be an additional media identification attribute within the m-line of the original stream that is within the grouping:

- a=mid:<original stream id>.

5.1.3.2   Session modification

When there is a need for BC session modification, the UE shall generate a re-INVITE request or an UPDATE request, depending on the dialogue state, as specified in ES 283 003 [20] for an originating UE.

The UE shall include SDP offer in session modification request. When the modified session is also a broadcast session the format of the SDP shall be the same as for a session initiation.

Upon receipt of a re-INVITE request or an UPDATE request, the UE shall follow the procedures defined in ES 283 003 [20] for an originating UE.

When receiving SDP offer, the SDP answer shall reflect the media capabilities and required bandwidth as available for the BC session. The selection of the channels that are above the negotiated bandwidth may require a new session modification in accordance with the behaviour of the UE.

5.1.3.3   BC service with trick-play mode

In case of supporting BC service with trick play, the BC session can observe two special cases:

- The Broadcast session is modified to change from Multicast to unicast flow. This is the case in which the UE activates the trick play mode.

- The Broadcast session with trick play mode is modified to return to normal Broadcast TV. This is the case in which the UE deactivates the trick play mode by, e.g. switching channels from a paused channel to another live Broadcast TV channels.

5.1.3.3.1   Trick-play mode activation

Upon activation of trick-play mode, the UE shall perform session modification as described in clause 5.1.3.2.

The UE shall include an SDP offer with previously negotiated media descriptions with the port set to zero and two or more additional media descriptions: one for RTSP control and one or more for the unicast streams. The RTSP control media descriptor shall follow ES 283 003 [20]. The SDP offer for media delivery shall be identical to the previous SDP offer done for broadcast in term of codecs and transport protocol.

The UE shall also include the following Service Action Data:

- IPTVActionDataCommand shall be set to "SwitchToTM".

- SwitchToTM shall be set to "IPTVBcActionData".

BCServiceId shall present only if the UE has not informed the SCF of the selected channel prior to this procedure (as defined in clause 5.1.3.5) and set to the value of the current channel.

When the UE acknowledges the SIP 200 OK with an ACK message, the UE may start playback (see clause 7).

5.1.3.3.2   Trick-play mode deactivation

Upon deactivation of trick-play mode, the UE shall perform session modification as described in clause 5.1.3.2.

The UE shall include an SDP offer with previously negotiated RTSP and unicast media descriptions with the port set to zero. The SDP corresponding to the broadcast session shall be reactivated (i.e. port not set to zero).

The UE shall also include the following Service Action Data:

- IPTVActionDataCommand shall be set to "SwitchtoBC".

- SwitchToBC shall be set to "IPTVBcActionData".

- BCServiceId is set to the value of the selected channel.

The UE deactivates trick-play mode when it receives an indication from the network that it has caught up with the live BC service.

The UE shall go back to normal BC session if it does not receive any delivery data anymore and has not paused playback.

5.1.3.4   Session termination

Upon a request for a BC session termination, the UE shall generate a BYE request as specified in ES 283 003 [20] for an originating UE.

Upon receipt of a BYE request the UE shall follow the procedure specified in ES 283 003 [20] for an originating UE.

5.1.3.5   Session Information

During the procedures for join multicast group (clause 8.1.1) the UE may inform SCF of the selected channel.

If the UE informs the SCF of the selected channel it shall reset a delay timer after successfully viewing a new channel using the procedure for joining multicast group (clause 8.1.1). The delay timer is a preconfigured value in the UE with a default value of 10 seconds. When the delay timer expires, the network shall be informed of the currently viewed channel with a SIP INFO message.

- The SIP INFO message shall be sent by the UE on the same dialogue as the Broadcast TV session initiation and shall contain an XML file with the channel change information. The message body carries the service action data: the matching "BC Bookmarks" object shall be created so that:

    - IPTVActionDataCommand shall be set to "Notify".

    - Notify shall be set to "IPTVBcActionData".

    - BCServiceId is set to the value of the current channel.

    - ProgrammeId is optionally set to the value of the current programme.

- Bookmark is set to the current timestamp if the UE has the knowledge of such timestamp (e.g. through SNTP). If the UE is not aware of such current timestamp, Bookmark is set to a default value: "NOW".

The Content-Type header shall be set to "application/vnd.etsi.iptvcommand +xml". The body content of the message is described in annex D.

5.1.4   Procedure for CoD service

5.1.4.1   Procedure for retrieving missing parameters before session initiation

In case of procedure for establishing the content control and content delivery at the same time see clause 5.1.4.2.1, if the UE does not have all transport parameters (RTP or UDP transport for MPEG2TS encapsulation or direct RTP, FEC layers addresses and ports) the UE shall send a SIP OPTIONS message,

   NOTE: It is an operator choice to provide preconfigured transport parameters values, manual configuration mechanisms, etc., if the transport information is not retrieved from the SSF.

The "Request-URI" is related to the CoD session that the user wants to activate. The Request-URI shall be composed of a user and domain part as defined as follows:

- The user part contains the content identifier in a free string format, as defined in TS 182 027 [2].

- The domain part is the Service Provider domain name, obtained from SSF.

The content identifier shall be retrieved from service selection information (cf. annex L concerning the mapping between service selection information and SIP/SDP parameters).

The TO header shall contain the same URI as in the "Request-URI" parameter.

The FROM header shall indicate the public user identity of the user.

Upon reception of the SIP 200 OK including SDP, the UE shall initiate COD session as described in clause 5.1.4.2.

5.1.4.2   Session initiation

The UE shall support the procedures specified in ES 283 003 [20] for originating sessions.

Upon a request for a COD session initiation, the UE shall generate an initial INVITE request as specified in
ES 283 003 [20] for an originating UE.

The "Request-URI" is related to the CoD session that the user wants to activate. The Request-URI shall be composed of
a user and domain part as defined as follows:

- The user part contains the content identifier in a free string format, as defined in TS 182 027 [2].

- The domain part is the Service Provider domain name, obtained from SSF.

The content identifier shall be retrieved from service selection information (cf. annex L concerning the mapping
between service selection information and SIP/SDP parameters).

The TO header shall contain the same URI as in the "Request-URI" parameter.

The FROM header shall indicate the public user identity of the user.

5.1.4.2.1   Procedure for establishing the RTSP content control and content delivery channel

5.1.4.2.1.1   UE as SDP offerer

An SDP Offer shall be included in the initial INVITE request. the SDP offer shall be done in accordance with media
capabilities and policies available for the CoD session and with the parameters received from the SSF during UE
service selection procedure (cf. annex L concerning the mapping between service selection information and SIP/SDP
parameters) or from the SIP OPTIONS response.

The SDP offer from the UE shall contain a media description for the RTSP content control channel and one for the
content delivery channel.

SDP session level parameters shall be used as specified in ES 283 003 [20].

The RTSP content control media description shall be carried by TCP and follow ES 283 003 [20]. The SDP parameters
for the RTSP content control channel shall be set as follows:

- a "m" line for an RTSP stream of format: m=<media> <port> <transport> <fmt>:

    - The media field shall have a value of "application".

    - The port field shall be set to a value of 9, which is the discard port.

    - The transport field shall be set to TCP or TCP/TLS. The former is used when RTSP runs directly on top
      of TCP and the latter is used when RTSP runs on top of TLS, which in turn runs on top of TCP.

    - The fmt parameter shall be included and shall be set to *iptv_rtsp*
      (ex. m=application 9 tcp iptv_rtsp).

- An "a=setup" attribute shall be present and set to "active" as defined in ES 283 003 [20]
  (ex. a=setup:active).

- An "a= connection" attribute shall be present and set as "new" as defined in ES 283 003 [20]
  (ex. a=connection:new).

- A "c" line shall include the network type with the value set to IN, the address type set to IP4 or IP6 and IP address of the flow of the related RTSP content control
  (ex. `c=IN IP4 <IP_ADDRESS>`).

NOTE: RTSP over UDP is out of scope of the present document.

For each media stream controlled by the RTSP content control channel the SDP offer shall include a content delivery channel media description set as follows:

- The "m=" line indicates the type of the media, the transport protocol and the port of the related content delivery channel. It may also include a fmt parameter which shall indicate the format given by the SSF, a subset of them or the format offered by the UE if none is given by the SSF.

- The "c=" line shall include the network type with the value set to IN, the address type set to IP4 or IP6 and unicast address of the flow of the related content delivery channel,
  (ex. `c=IN IP4 <IP_ADDRESS>`).

- The "b=" line shall contain the proposed bandwidth. If the user has fetched the bandwidth required for this particular content delivery channel during service selection procedure, the bandwidth attribute at media level shall be set to this value. Otherwise, this attribute shall be set to a pre-configured value
  (ex. `b=AS:15000`).

- An "a=" line with a "recvonly"
  (ex. `a=recvonly`).

Additionally, FEC streams may be defined, as described in clause 5.1.4.2.3.

When receiving any SIP response, the UE shall examine the media parameters in the received SDP: the UE shall fetch the RTSP session ID from the "fmtp:iptv_rtsp h-session" attribute if present in the received in the SDP answer contained in the SIP response. This RTSP session ID shall be used for in RTSP media control messages and the UE shall subsequently use RTSP Method 1 for CoD playback control as described in clause 7.1.1. If fmtp:iptv_rtsp h-offset is specified in the SDP from MCF, the UE may use this as appropriate in subsequent RTSP media control messages.

In case no "fmtp:iptv_rtsp h-session" parameter was received in the SDP answer, the UE shall use RTSP method 2 for CoD playback control as described in clause 7.1.2.

5.1.4.2.2   Procedure for establishing the RTSP channel separately

5.1.4.2.2.1   UE as SDP offerer

The INVITE request shall contain an SDP offer of media description only for the RTSP channel.

The SDP session level parameters shall be used as specified in ES 283 003 [20].

The SDP parameters for the RTSP channel shall be set as follows:

- A "m" line for an RTSP stream of format: m=<media> <port> <transport> <fmt>:

  - The media field shall have a value of "application".

  - The port field shall be set to a value of 9, which is the discard port.

  - The transport field shall be set to TCP or TCP/TLS. The former is used when RTSP runs directly on top of TCP and the latter is used when RTSP runs on top of TLS, which in turn runs on top of TCP:

    - The fmt parameter shall be set to iptv_rtsp.

- An "a=setup" attribute shall be present and set to "active" as defined in ES 283 003 [20].

- An "a= connection" attribute shall be present and set as "new" as defined in ES 283 003 [20].

NOTE: RTSP over UDP is out of scope of the present document.

5.1.4.2.3 Additional SDP lines for FEC streams

When the UE decides to connect to FEC stream(s) associated to the COD original stream, it shall include additional SDP lines in the SDP offer as follows:

- One or more m-line(s) for each FEC stream exposed through the SSF:

    - It shall be set according to the mapping defined in clause L.3.

    - It shall contain a c-line according to the mapping defined in clause L.3.

If the COD content is defined through a single m-line, a grouping line may be included.

If the COD content is defined through several m-lines, grouping line(s) shall be included, one for each COD m-line that is associated to a FEC stream.

- a=group:FEC:<original stream id> <FEC stream id>
  The present document supports only the DVB-IP AL-FEC Base layer, so there can be only one <FEC stream id> associated to an original stream:

    - The original stream id shall reflect the value hold by the media description of one stream in its a=mid attribute.

    - The FEC stream id shall reflect the value hold by the media description of the DVB-IP AL-FEC Base layer FEC stream (associated to the original stream) in its a=mid attribute.

Furthermore, when grouping line is included, there shall be an additional media identification attribute within the m-line of the original stream that is within the grouping:

- a=mid:<original stream id>.

5.1.4.3 Session modification

In order to modify the session from the UE side, the UE shall send a re-INVITE or an UPDATE request as specified in ES 283 003 [20] for an originating UE.

The UE shall not modify RTSP channel m-line description in the SDP if the media delivery streams controlled by RTSP are not removed (port not set to zero in m-lines) in the SDP.

Upon receipt of a re-INVITE request or an UPDATE request, the UE shall modify the session as specified in ES 283 003 [20] if the request is acceptable to the UE.

5.1.4.3.1 Procedure for establishing the content delivery channel

5.1.4.3.1.1 UE as SDP offerer

The UE shall send a re-INVITE or an UPDATE request containing SDP offer after acquiring the network parameters via RTSP DESCRIBE as specified in clause 7.1.2.2 in order to establish the content delivery channels. The media descriptions of content delivery channels shall be populated as follows:

- Media descriptions acquired by DESCRIBE response are appended after the media description of RTSP channel.

- The port number in "m=" line shall be replaced by the real receiving port of the UE.

- "a=recvonly" attribute shall be inserted if the attribute is not specified.

- Remove "a=" lines specific to RTSP (a=control, a=range, and a=etag).

- If "c=" lines are specified in media descriptions, the addresses of "c=" lines shall be replaced by the address of the UE.

The SDP parameters for the RTSP channel shall be set to the same parameters as specified in clause 5.1.4.2.1 except for the "a=connection" attribution. The attribution shall be set to "existing" as defined in ES 283 003 [20].

The SDP offer shall include one or more media description sets as follows:

- The "m=" line indicates the type of the media, the transport protocol the port on which the UE has to received the flows of the related content delivery channel. It may also include a fmt parameter which shall indicate the format given by the network parameters.

- The "c=" line shall include the network type with the value set to IN, the address type set to IP4 or IP6, and unicast address of the flow of the related content delivery channel. These values are given by the network parameters.

- The "b=" line shall contain the bandwidth. The bandwidth attribute shall be set to this value given by the network parameters.

- An "a=" line with a "recvonly".

Additionally, FEC streams may be defined, as described in clause 5.1.4.3.2.

5.1.4.3.2   Additional SDP lines for FEC streams

When the UE decides to connect to FEC stream(s) associated to the COD original stream, it shall include additional SDP lines in the SDP offer as follows:

- One or more m-line(s) for each FEC stream exposed through the SSF:

    - It shall be set according to the mapping defined in clause L.3.

    - It shall contain a c-line according to the mapping defined in clause L.3.

- If the COD content is defined through a single m-line, a grouping line may be included.

If the COD content is defined through several m-lines, grouping line(s) shall be included, one for each COD m-line that is associated to a FEC stream.

The grouping line uses the "FEC" semantic as defined in RFC 4756 [25]:

- a=group:FEC:<original stream id> <FEC stream id>.
  The present document supports only the DVB-IP AL-FEC Base layer, so there can be only one <FEC stream id> associated to an original stream:

    - The original stream id shall reflect the value hold by the media description of one stream in its a=mid attribute.

    - The FEC stream id shall reflect the value hold by the media description of the DVB-IP AL-FEC Base layer FEC stream (associated to the original stream) in its a=mid attribute.

Furthermore, when grouping line is included, there shall be an additional media identification attribute within the m-line of the original stream that is within the grouping:

- a=mid:<original stream id>.

5.1.4.4   Session termination

The session termination will differ when using RTSP "Method 1" or RTSP "Method 2" as described in clauses 5.1.4.4.1 and 5.1.4.4.2. The different RTSP methods are described in clause 7 and annex Q.

5.1.4.4.1   Session termination using RTSP Method 1

In order to terminate the session, the UE shall first close the RTSP session that was established during session initiation by closing the underlying TCP connection and then send a BYE request as specified in ES 283 003 [20].

Upon receipt of a BYE request, the UE shall then terminate the session as specified in ES 283 003 [20].

5.1.4.4.2   Session termination using RTSP Method 2

In order to terminate the session, the UE shall send a BYE request as specified in ES 283 003 [20]. The media teardown procedures using RTSP TEARDOWN as described in clause 7.1.2.6 shall be executed before the BYE is sent out. This would ensure that the BYE request does not close the RTSP content control channel ports at transport layer before RTSP TEARDOWN is sent.

Upon receipt of a BYE request, the UE shall send a TEARDOWN request to terminate the RTSP session if non-persistent RTSP connection is used or if the TCP connection is open. The UE shall then send a SIP 200 OK response to the BYE request as specified in ES 283 003 [20].

> NOTE: The UE may not be able to send TEARDOWN or receive a response for TEARDOWN when the resource in the network for RTSP session has been released when of receiving SIP BYE.

5.1.4.5   Procedures for handling COD Service action data

When a user requests to stop viewing a CoD with the intention of resuming it later, the UE may send a SIP INFO request to the SCF. The content of that INFO request shall be as follows:

- The value of the Request-URI shall be set to the one used in the related session.

- From and To headers shall be set to the one defined during the session initiation procedure.

- Call-ID shall be set to the same value as that of the CoD session.

- CSeq shall be generated by UE following rules defined in ES 283 003 [20] for request within a dialog.

- The Content-type header shall include the registered MIME type of XML documents representing IPTV service action data: "application/vnd.etsi.iptvcommand+xml".

- The message body carries the service action data:

    - IPTVActionDataCommand shall be set to "Notify".

    - Notify shall be set to "IPTVCodActionData".

    - The matching "Available CoD" object shall be updated so that CoDDeliveryStatus is set to "Parked" and CoDOffset is set to the current reading cursor of the content.

> NOTE: The XML schema mapping to the MIME type: "application/vnd.etsi.iptvsad-cod+xml" is available in annex K of the present document.

5.1.5   Procedure for Service Configuration

The UE uses the XCAP to manage the IPTV user profile (see clause 6.1.2). In order to keep the IPTV User Profile data synchronized with the network elements and other terminals that the user might be using, the UE should subscribe from the SCF to changes in the XCAP IPTV documents.

> NOTE: Changes may result from XCAP manipulation and/or operator's action.

5.1.5.1   Subscription to notification of changes

If subscription to notification of changes is used, the UE shall generate a SUBSCRIBE request in accordance with RFC 5875 [26] and RFC 5874 [15].

The contents of the SUBSCRIBE request shall be as follows:

- The value of the Request-URI shall be set to the IMS public user identity associated to the profile or to a pre-configured value or to a value received from the CNGCF.

- The From header shall be set to the IMS public user identity associated to the profile.

- The To header shall be set to a URI that identifies the IPTV service provider (e.g. PSI).

- The Accept header shall include the following values:

    - application/xcap-diff+xml.

- The Event header shall be set to the "xcap-diff" event package.

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header of the received response.

The UE shall automatically refresh the subscription, either 600 seconds before the expiration time if the initial subscription was for greater than 1 200 seconds, or when half of the time has expired if the initial subscription was for 1 200 seconds or less. If a SUBSCRIBE request to refresh a subscription fails with a non-481 response, the UE shall still consider the original subscription valid for the duration of the most recently known "Expires" value according to ES 283 003 [20]. Otherwise, the UE shall consider the subscription invalid and start a new initial subscription according to ES 283 003 [20].

5.1.5.2   Processing of notifications

Upon receipt of a NOTIFY request on the dialog which was generated during subscription, the UE shall look for a message body with a content-type header indicating "application/xcap-diff+xml" stores its contents for further processing. and return a SIP 200 OK response to the NOTIFY request.

5.1.6   Procedure for IPTV presence service

If presence service is used, the UE shall implement the role of a PUA as specified in ES 283 030 [21].

Publication of IPTV specific information in presence document depends on user-configurable data stored in the user equipment.

Depending on the user configuration, the UE may send a SIP PUBLISH request in the following case:

- On receipt of a final SIP 200 OK concerning a BC session initiation procedure.

- On receipt of a final SIP 200 OK concerning CoD session initiation procedure.

- On receipt of a final SIP 200 OK concerning N-PVR content session initiation procedure.

During a BC session, the UE may also send a PUBLISH request after having performed a channel-change (i.e. sending IGMP or MLD request for a particular BC service) or after the timer Tcc associated to the channel change has elapsed if this timer is activated as described in annex M.

When activated, the timer Tcc is triggered at every channel-change.

The content of the PUBLISH request shall be as follows:

- The Request-URI and of the To and From headers shall be set to the public user identity of the user.

- The Event header shall be set to the "presence" event package.

- The content type shall be set to "application/pidf +xml".

The presence XML document included in the PUBLISH body shall conform to ES 283 030 [21].

The "Entity" element shall be present and set to the public user identity of the user.

The "Activity" element shall be present and set to "TV".

Additional IPTV presence elements are defined in annex E and may be included in the presence documents published by the UE:

- The "BCServicePresence" element is part of the "tuple" component according to the presence data model. It is composed of:

    - "CurrentBCServiceID" element: it indicates the current activated BC service.

    - "CurrentBCProgramID" element: it indicates the currently watched program.

- The "CoDServicePresence" element is part of the "tuple" component according to the presence data model. It is composed of:

    - "CurrentCoDContentID" element: it indicates the currently watched CoD content.

- The "NPVRServicePresence" element is part of the "tuple" component according to the presence data model. It is composed of:

    - "CurrentNPVRContentID" element: it indicates the currently watched N-PVR content.

In the XML document, each service is described thanks to the "service-description" OMA parameter as specified in OMA-TS-Presence-SIMPLE-V1 [23]. A new "service-id" is defined for this purpose with the following values IPTV-BC, IPTV-CoD, IPTV-NPVR.

A "class" parameter can also be added with the value "IPTV".

The activation/deactivation of this service is reported thanks to the "status parameter present in the relevant "tuple.

An example of the use of this parameter in the XML document is described in annex E.

5.1.7   Procedure for NPVR Service

5.1.7.1   Procedures for NPVR Service Capture Request

The SIP MESSAGE method is used here to achieve what is described in the architectural document (TS 182 027 [2]) as "N-PVR content capture request". This request may be done in an impulsive way or offline.

5.1.7.1.1   Procedures for Impulsive Request

This use case is itself divided in two sub-cases:

Case 1: The user does not specify any end date and time for the recording. This can be seen as a case of "Park and pickup TV" as described in TS 182 027 [2]:

In this case the UE shall send a SIP MESSAGE request to SCF requiring Bookmark setting. The contents of the SIP MESSAGE request shall be as follows:

- The Request-URI in the MESSAGE request shall be the well known PSI (Public Service Identifier) of the BC Service.

    NOTE 1: This is the same value as the Request-URI for BC service session initiation.

- From and To headers shall be set to the public identity of the user issuing the MESSAGE message.

- Call-ID shall be generated by UE.

- CSeq shall be generated by UE.

- The Content-type header shall include the registered MIME type of XML documents representing IPTV service action data: "application/vnd.etsi.iptvcommand+xml".

- The message body carries the service action data: the matching "BC Bookmarks" object shall be created so that:

    - IPTVActionDataCommand shall be set to "Record".

    - Record shall be set to "IPTVBcActionData".

    - BCServiceId is set to the value of the current channel.

    - ProgrammeId is optionally set to the value of the current programme.

    - Bookmark is set to the current timestamp if the UE has the knowledge of such timestamp (e.g. through SNTP). If the UE is not aware of such current timestamp, Bookmark is set to a default value: "NOW" which implies that the content capture is initiated as soon as the NPVR SCF gets the request.

  NOTE 2: BookmarkExpiryTime may be updated in two ways. It can be updated according to the user preference pre-set by the user, or according to the service policy defined by the service provider.

Case 2: The user specifies an end date and time for the recording:

In this case the UE shall send a MESSAGE request to the SCF. The contents of the SIP MESSAGE request shall be as follows:

- The user-part value of the Request-URI shall be set to the BC Service Package ID that the BC service to be recorded belongs to.

- From and To headers shall be set to the public identity of the user issuing the MESSAGE message.

- Call-ID shall be generated by UE.

- CSeq shall be generated by UE.

- The Content-type header shall include the registered MIME type of XML documents representing IPTV service action data: "application/vnd.etsi.iptvcommand+xml".

- The message body carries the service action data: the matching "NPVR item" object shall be created so that:

    - IPTVActionDataCommand shall be set to "Record";

    - Record shall be set to "IPTVNpvrActionData";

    - NPVRContentId is not set;

    - BCServiceId is set to the BC Service to be recorded;

    - RecordStartDate is set to the current timestamp if the UE has the knowledge of such timestamp (e.g. thanks to SNTP). If the UE is not aware of such current timestamp, RecordStartDate should be set to a default value: "NOW" which implies that the content capture is started as soon as the NPVR SCF gets the request;

    - RecordEndDate is set to the end date/time when the recording should stop and would correspond to what the user has specified;

  NOTE 3: NPVRContentExpiryTime may be updated in two ways. It can be updated according to the user preference pre-set by the user, or according to the service policy defined by the service provider.

5.1.7.1.2   Procedures for Offline Request

A user may request to record a live programme that has not started yet. In this case the UE shall send a SIP MESSAGE request to the SCF. The content of the SIP MESSAGE request shall be as follows:

- The user-part of the Request-URI shall be set to the BC Service Package ID that the BC service belongs to.

- From and To headers shall be set to the public identity of the user issuing the MESSAGE message.

- CSeq shall be generated by UE.

- The Content-type header shall include the registered MIME type of XML documents representing IPTV service action data: "application/vnd.etsi.iptvcommand+xml".

- The message body carries the service action data: the matching "NPVR item" object shall be created so that:

  - IPTVActionDataCommand shall be set to "Record".

  - Record shall be set to "IPTVNpvrActionData".

  - If the recording is requested on a specific entry in the EPG:

    ▪ NPVRContentId is set to the matching ProgrammeId.

  - If the recording do not match a specific entry in the EPG:

    ▪ NPVRContentId is not set.

    ▪ BCServiceId is set to the BC Service to be recorded.

    ▪ RecordStartDate is set to the date/time when the recording has to start as specified by the user.

    ▪ RecordEndDate is set to the date/time when the recording has to be terminated and is specified by the user.

NOTE: NPVRContentExpiryTime may be updated in two ways. It can be updated according to the user preference pre-set by the user, or according to the service policy defined by the service provider.

5.1.7.2   Procedures for NPVR Session

The UE follows procedures outlined in clause 5.1.4 for COD to stream a previously captured NPVR content.

The user part of the "Request-URI" parameter shall contain the NPVRContentId retrieved from the SSF as defined in clause 6.1.1.5 and shall correspond to the content that was captured via impulsive or offline request.

The UE shall build the SDP offer as defined in clause 5.1.4.2 for CoD session initiation and shall include media control line for RTSP control channel. The SDP offer for the media delivery lines shall specify the transport and codec parameters for the corresponding BC ServiceId.

5.2   Service Discovery Function (SDF)

5.2.1   Procedure for IMS registration

If delivery of service discovery information using push mode is supported, the SDF acts as a third-party registrar and receive REGISTER requests from the Core-IMS during the IMS registration phase.

The SDF shall store the public user identity of the user as received in the To header and use it to initiate delivery of service discovery information in push mode towards this user. The SDF shall answer to the REGISTER request with a SIP 200 OK response as specified in ES 283 003 [20].

If delivery of service discovery information in push mode is not used, the SDF shall send a 501 error response to the Core-IMS.

5.2.2   Procedure for service attachment

5.2.2.1   Push mode

In the push mode, after the regular third-party registration, the SDF shall generate a SIP MESSAGE to the UE, and the service attachment information is taken in the message body of the SIP MESSAGE.

The SDF uses the SIP MESSAGE to transport the service attachment information, and the SDF shall generate a SIP MESSAGE request in accordance with ES 283 003 [20] and TS 124 229 [24] as used in ES 283 003 [20].

The contents of the SIP method request shall be as follows:

- The Request-URI of the SIP MESSAGE request shall be set to the public user identity of the intended recipient.

- The From head shall be set to the SIP URI of the SDF.

- The To head shall be set to the public user identity of the intended recipient.

- The content type shall be set to "application/vnd.etsi.iptvdiscovery+xml".

- The message body shall conform to the XML schema described in annex M and shall be according to clause 5.2.2.3.

The SDF shall send the SIP MESSAGE request towards the Core IMS according to the procedures of the Core IMS.

When the SDF generates and sends the service attachment information to the UE, it can check IPTV profile of the user, and provides the custom/personalize service attachment information to the UE. IPTV profile including:

- Location information, e.g. the SDF can retrieve the location of the UE and send the address of the SSF based on the location of the UE.

- User subscription information.

- UE capabilities, including the model, vender, version, coding format etc., and the SDF can send the service attachment information to the UE based the UE capabilities, When the service attachment information is changed, the SDF may generate a SIP method request including new service attachment information.

5.2.2.2   Pull mode

The SDF addresses may be determined by the UE using any of the alternatives as defined in annex I.

When the SDF receives a SUBSCRIBE request, if personalized information is required it shall perform user's identity verification as defined in ES 283 003 [20], clause 5.7.1.4. After successful user identification if an IPTV User Profile is available it is possible to perform personalization of the body (Service Attachment Information) of the NOTIFY. Filtering may also be performed if device capabilities are available to the SDF.

If the SDF receives a SIP SUBSCRIBE message body from the UE carrying UE capabilities, the SDF shall process the SIP request as follows - if the content-type in the request does not match "application/vnd.etsi.iptvueprofile+xml:, then the SDF shall respond with a 415 Unsupported Media Type error.

The SDF shall examine the parameters specified in the SIP SUBSCRIBE body and shall then record UE capabilities information as part of the IPTV user profile data.

> NOTE 1: The UE capabilities that are recorded as part of the IPTV user profile may be used by the SSF for personalization purposes.

In case of successful subscription, the SDF shall generate a SIP 200 OK in response to the SUBSCRIBE request. The SDF shall then send a NOTIFY request immediately.

> NOTE 2: The SDF can select personalized SSF information based on IPTV user profile. For example, the SDF will send only addresses of SSF(s) that contain information (e.g. EPG) related to the BC service package(s) subscribed by the user.

The contents of the NOTIFY request shall be as follows:

- The Event header shall be set to the "ua-profile" event package.

- The "effective-by" parameter for the event header shall be set to 0.

- The content type shall be set to "application/vnd.etsi.iptvdiscovery+xml".

- The message body shall conform to the XML schema described in annex M and shall be according to clause 5.2.2.3.
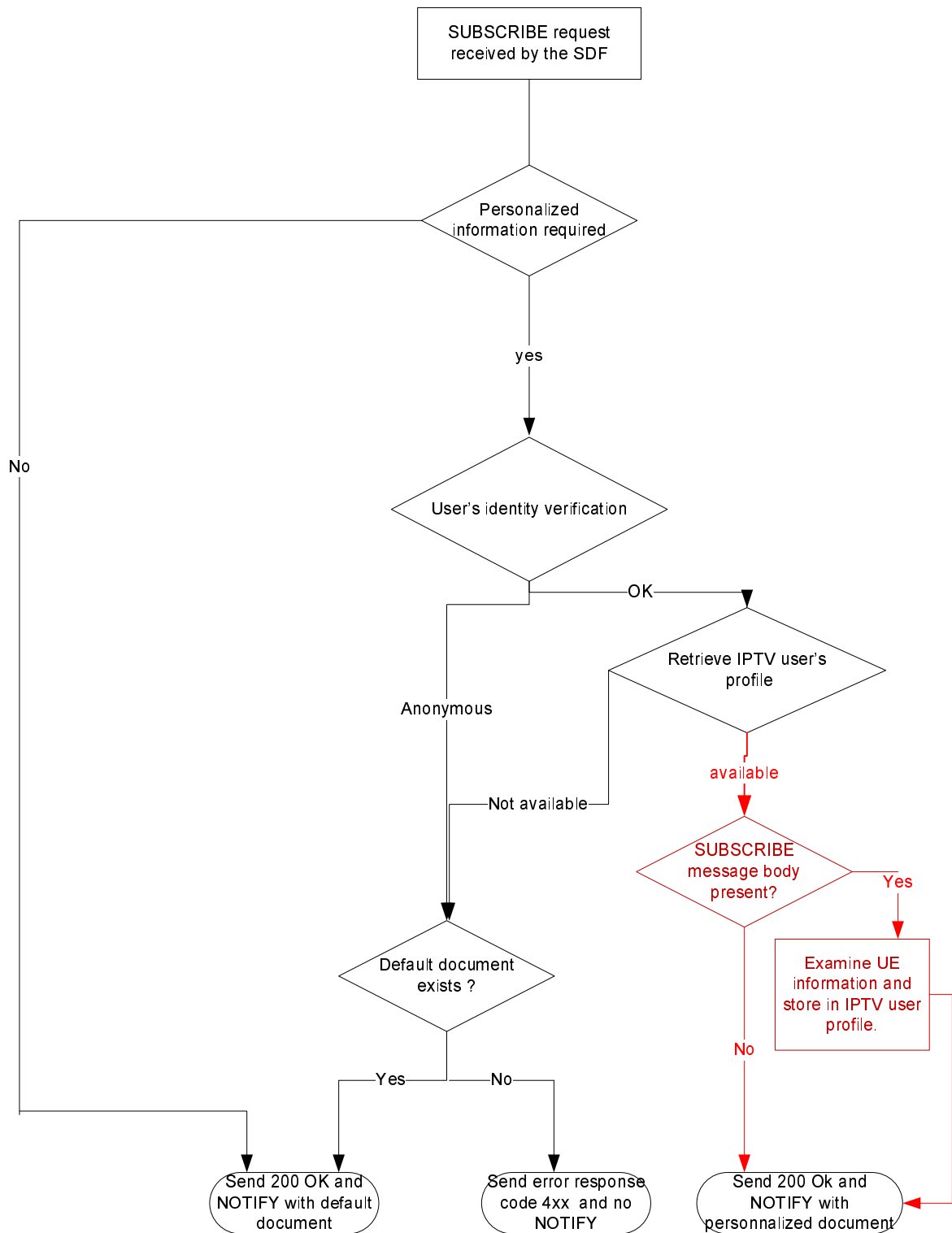
Figure 5.2.2.2: SDF logic for processing SUBSCRIBE requests

When any parameter of service configuration information has changed, the SDF may generate a NOTIFY request including new service configuration information.

5.2.2.3 Service Attachment Information

The body of the SIP message from SDF shall include an XML document as defined in annex M listing SSF addresses and the means of connecting to the SSFs for retrieving service selection information.

For each SSF, the following sub-elements are populated as follows:

Table 5.2.2.3: SSF information sending by SDF during service attachment procedure

Element Name	Description	Mandatory(M)/ Optional (O)	Many = several instances are possible
SSF	Root element	M	Many
@ID	Identifier for SSF defined uniquely for a given SDF	M	
@Technology	Indicates the technology used for delivering service selection information. Currently defined technologies are "dvb.org_iptv""openmobilealliance.org_bcast" and "tispan.org_sad" Refer to annex L for the mapping of Technologies defined in the present document Refer to annex O for the definition procedure of new technologies	M	
@Version	This is incremented when one or more fields in SSF element have changed		
Description	Description of the SSF for potential display in one or more languages. One description is allowed per language	O	Many
ServiceProvider	Provides information about IPTV service provider	O	
@DomainName	The IPTV service provider domain name	M	
@LogoURI	Link for the IPTV Service Provider Logo	O	
Name	Name of the IPTV Service Provider for potential display in one or more languages. One name is allowed per language	M	Many
Description	Description of the IPTV Service Provider for potential display in one or more languages. One description is allowed per language	O	Many
Pull	Provide information to access SSF via Pull Mode	O	Many
@Location	URI of the SSF	M	
DataType	Specifies the type of service selection information available at the SSF (e.g. COD, BC)	M	Many
@Type	The type of service selection information. The exact format is determined by the Technology	M	
Segment	Used to logically separate service selection information	The mandatory/optional nature of this parameter depends on the SSF Technology and is detailed in annex L	M
@ID	Identifier for segment. The exact format is determined by the Technology	M	
@Version	This is incremented when the information in segment changes	O	
Push	Provide information to access SSF via Push Mode	O	Many
@IPVersion	Specifies the IP Version (4 or 6). If omitted, then version 4 is assumed	O	
@MulticastAddress	The address to join to in order to retrieve service selection data	M	
@MulticastAddress	The address to join to in order to retrieve service selection data	M	

Element Name	Description	Mandatory(M)/ Optional (O)	Many = several instances are possible
@SourceAddress	The address of the sender of the service selection data	O	
DataType	Specifies the type of service selection information available at the SSF (e.g. COD, BC)	M	Many
@Type	The type of service selection information. The exact format is determined by the Technology	M	
Segment	Used to logically separate service selection information	The mandatory/optional nature of this parameter depends on the SSF Technology and is detailed in annex L	M
@ID	Identifier for segment. The exact format is determined by the Technology	M	
@Version	This is incremented when the information in segment changes	O	

NOTE 1: The mechanism used by the SDF to gather SSF information belonging to multiple service providers is outside the scope of Release 2.

The following constraints apply to XML documents as described by table 5.2.2.3:

- There shall be at least one Pull or Push element specified for a SSF.

- When an optional element is included in the XML document, then all mandatory attributes and sub-elements related to this element shall be included as well.

- Extensions to the elements are possible (refer to the XML schema defined in annex M).

NOTE 2: Alternatively, annex J describes the optional case, when using a non-SIP AS based SDF (e.g. for legacy purpose) as described in annex A of TS 182 027 [2].

5.3   Service Control Function (SCF)

5.3.1   Procedure for BC service

5.3.1.1   Session initiation

The SCF shall support the procedures specified in ES 283 003 [20] applicable to an AS acting as a terminating UA.

Upon receipt of SIP INVITE request, the SCF shall examine the Request-URI to determine that it is a BC session initiation request. According to the user subscription information, the SCF shall check the service rights of requested broadcast service packages and multicast addresses. The SCF shall examine the SDP parameters. In particular:

- It shall examine the a=bc_service parameter. This parameter contains the channel the UE intends to join. If the bc_service parameter does not point to a channel that the UE is allowed to join the SCF shall not accept the offer and shall answer with a 403 error code.

- If present it shall examine the a=bc_service_package attributes and verify that the referred service packages are allowed in the user profile. The SCF shall limit the service packages and the BC services according to the user subscription (see below). If none of the service packages are subscribed, the SCF shall answer with a 403 error code.

- It shall examine the c-line(s) to determine that it is a multicast session. It may also check that it corresponds to the bc_service parameter. If not, the SCF shall answer with an 403 error code.

- It shall examine the b parameter if present to verify that it is the largest bandwidth of the BC services the UE intends to join. If not, the SCF shall answer with a 403 error code.

If the SDP parameters are examined successfully, the SCF shall answer with a SIP 200 OK, indicating the SDP answer as follows:

- The c-lines and m-lines shall be identical to ones indicated in the SDP offer.

- It shall include an a=recvonly attribute.

- It shall include a b-line parameter with the same value as in the offer, if present. If the b-lines were not present in the offer, the SCF shall include one with a value set to the largest bandwidth of all the BC services contained in the indicated service packages attribute.

- If the SDP offer includes one or more a=bc_service_package attribute the SDP answer shall include the same number of attributes or less. The SCF shall remove service packages not subscribed by the user. If no bc_service_package attributes are included in the SDP offer the SCF shall include in the SDP answer one or more a=bc_service_package attribute, except if the SCF knows that the RACS is pre-provisioned with the list of subscribed channels and if all the subscribed channels are allowed for the session. In that case, the inclusion of a=bc_service_package is optional.

    NOTE: How the resources are pre-provisioned is a deployment issue; these attributes may be included for updating dynamically the RACS with new service packages or multicast address, when the UE knows its profile.

The service packages shall be populated according to the user profile to indicate the service packages and BC services that can be used for the session according to annex N.

If a=bc_service_package attribute is included the SCF shall include one or more mult_list parameter(s) if the user has not subscribed to the entire service package. It may also include the bc_service_id_list containing the list of subscribed BC service ids. If the user has subscribed to the entire service package, the inclusion of mult_list parameter is optional (e.g. depending on SCF local policies).

5.3.1.2   Session modification

Upon receipt of a re-INVITE request or an UPDATE request, the SCF shall follow the procedures defined in ES 283 003 [20] concerning the AS acting as a terminating UA or a B2BUA.

When receiving an SDP offer, the SCF may modify the SDP answer in accordance to the user subscription. If the SCF finds a media line not compatible with the user's subscription, it shall set the port of this media line to 0. If none of the media lines are acceptable, it shall reply with a 403 error response.

Upon request of a BC session modification, the SCF shall send a re-INVITE or an UPDATE request, depending on the dialogue state, and follow the procedures defined in ES 283 003 [20] concerning the AS acting as an originating UA.

5.3.1.3   BC service with trick-play mode

In case of supporting BC service with trick play, the BC session can observe two special cases:

- The Broadcast session is modified to change from Multicast to unicast flow. This is the case in which the UE activates the trick play mode.

- The Broadcast session with trick play mode is modified to return to normal Broadcast TV. This is the case in which the UE deactivates the trick play mode by, e.g. switching channels from a paused channel to another live Broadcast TV channels.

5.3.1.3.1   Trick-play mode activation

Within the existing Broadcast TV session, if the session modification request contains Service Action Data with IPTVActionDataCommand set to "SwitchToTM", the SCF shall determine the modify request is for transition from Broadcast TV to Broadcast TV with trick mode and shall act as a B2BUA, terminating the re-INVITE request and sending a INVITE request to initiate a session setup to the MCF in charge of recording the BC service that the user has selected. When sending the initial INVITE message to MCF, SCF shall follow the procedures defined in ES 283 003 [20] concerning the AS acting as originating UA or B2BUA.

Prior to that procedure, the SCF shall check that the SDP in the re-INVITE contains the unicast streams description for content control and content delivery channels to be sent to the MCF to have the necessary parameter to initiate a session towards the MCF. If not, the SCF shall answer to the UE with a 403 error code.

The value of Request-URI contained in the new session initiation request shall be set to the routable identifier of the MCF, i.e. the SIP URI of the MCF.

The TO header shall contain the identifier of the channel to be trick-played i.e. the BC ServiceId included in the Service Action Data XML document or retrieved during session information procedure as defined in clause 5.1.3.5.

If the content or channel that the user has selected is not enabled for trick play, a SIP error code 403 Forbidden, shall be generated as a response.

The SDP offer sent with the INVITE to the MCF will follow the same pattern as in the CoD session initiation.

The SDP answer shall contain the same number of media descriptors as in the offer, following the SDP offer/answer model as indicated in the CoD session initiation clause. The only difference with that is the inclusion of:

- h-offset attribute different than 0, as calculated by the MCF indicating the offset in a given program.

The SIP 200 OK message will be progressed from the SCF to the UE as the response to the session modification. The SDP answer in the SIP 200 OK shall contain the same number of media descriptors as the SDP offer in the re-INVITE.

5.3.1.3.2 Trick-play mode deactivation

Within the existing Broadcast TV session, if the session modification request Service Action Data with IPTVActionDataCommand set to "SwitchtoBC", the SCF shall determine the modify request is for transition from Broadcast TV with trick mode to Broadcast TV and shall act as a B2BUA, terminating the re-INVITE request and sending a BYE to terminate the session to the MCF.

When the trick play mode is deactivated by the UE, the SCF will need to unlink the MF from the session in order to return to the normal broadcast session.

Before answering to the UE, the SCF shall check that the m-lines containing the multicast streams have been added by the UE and those one containing the unicast media streams have been removed. If not, the SCF shall answer to the UE with a 403 error code.

NOTE: How to add or remove a media stream in SDP conforms to ES 283 003 [20].

The SCF will then answer back to the re-INVITE request with a SIP 200 OK for the session to be returned to broadcast TV as defined in clause 5.3.1.2.

5.3.1.4 Session termination

Upon receipt of a BC session termination request, the SCF shall follow the procedures defined in ES 283 003 [20] concerning the AS acting as a terminating UA.

Upon receipt of an internal indication that a BC session shall be terminated, the SCF shall send a BYE request and follow the procedures defined in ES 283 003 [20] concerning the AS acting as a terminating UA.

5.3.2 Procedure for CoD service

The SCF shall support the procedures specified in ES 283 003 [20] applicable to an AS acting as a proxy or B2B UA.

5.3.2.1 Procedure for handling missing parameters before session initiation

When receiving the SIP OPTIONS message, the SCF shall select the appropriate media function (see TS 182 027 [2]) and forward the SIP request to the appropriate MCF by changing the "Request-URI" accordingly.

The SCF shall not change the user-part of the TO header in order to keep the content-id in the OPTIONS request.

In certain cases, the SCF may also forward the SIP OPTIONS over to a default media function.

When receiving a 301 or 302 response from the MCF, the SCF shall not forward this message to the UE.

The SCF may check if the MCF indicated in the contact header is allowed destinations.

If allowed, the SCF shall use one of the MCF URI indicated in the contact header of this response and use it as a destination for the redirected OPTIONS.

5.3.2.2 Session initiation

When receiving any SIP request, the SCF may examine the request to see if it is compatible with the user's subscription (e.g. parental control level).

If the user is not allowed to initiate a session for the requested content, the SCF shall reply with appropriate, SIP error code 403 Forbidden, response.

The SCF shall select the appropriate media function (see TS 182 027 [2]) and forward the SIP request to the appropriate MCF by changing the "Request-URI" accordingly.

The SCF shall not change the user-part of the TO header in order to keep the content-id in the INVITE request.

In certain cases, the SCF may also forward the SIP INVITE over to a default media function.

When receiving a 301 or 302 response from the MCF, the SCF shall not forward this message to the UE.

The SCF may check if the MCF indicated in the contact header is allowed destinations.

If allowed, The SCF shall use one of the MCF URI indicated in the contact header of this response and use it as a destination for the redirected INVITE.

5.3.2.3 Session modification

Void.

5.3.2.4 Session termination

5.3.2.4.1 Session termination using RTSP method 1

In case of SCF-initiated CoD session termination, the SCF shall send a BYE Request towards the UE and a BYE request towards the MF as specified in ES 283 003 [20].

5.3.2.4.2 Session termination using RTSP method 2

The SCF shall support the procedures specified in ES 283 003 [20] applicable to an AS acting as a proxy or B2B UA for call release.

In case of SCF-initiated CoD session termination, the SCF shall send a BYE Request towards the UE and a BYE request towards the MF as specified in ES 283 003 [20].

5.3.2.5 Procedures for handling COD Service action data

Upon receiving an INFO request with Content-type set to "application/vnd.etsi.iptvsad-cod+xml", the SCF retrieves the service action data from the INFO message body and either creates or updates the matching object instance.

A SIP 200 OK message with no body shall be sent to the originator if the INFO request is successfully received for an existing call; the service action data objects shall be created (or updated) according to the data retrieved from the INFO message body.

A "405 Method Not Allowed" shall be sent back to the originator if the SCF has no capability to process INFO message.

A "415 Unsupported Media Type" shall be sent back to the originator if the INFO request contains a body that the SCF does not understand.

A "481 Call Leg/Transaction Does Not Exist" shall be sent back to the originator if the INFO request does not match any existing session.

NOTE: The XML schema mapping to the MIME type: "application/vnd.etsi.iptvsad-cod+xml" is available in annex K of the present document.

5.3.3   Procedure for Service Configuration

The UE uses the XCAP to manage the IPTV user profile (see clause 6.1.2). In order to keep the IPTV services data synchronized with the network elements and other terminals that the user might be using, the UE should subscribe from the SCF to changes in the XCAP IPTV documents.

NOTE: Changes may result from XCAP manipulation and/or operator's actions.

When the SCF receives a SUBSCRIBE request having the Event header field value set to "xcap-diff", the SCF shall authorize the request based on the contents of the P-Asserted-Id. If the authorization is successful the SCF shall generate a SIP 200 OK response to the SUBSCRIBE request and generate notifications in accordance with RFC 5874 [15] and RFC 5875 [26].

5.3.4   Procedure for NPVR Service

5.3.4.1   Procedures for NPVR Service Capture Request

Upon receiving a SIP MESSAGE request, the SCF identifies the Content-type associated with the MESSAGE request and takes appropriate actions as specified below.

The SCF then checks whether the Service Package id is indeed authorized for the user issuing the request.

The actual BC service to be recorded/bookmarked is extracted from the XML body carried in the SIP MESSAGE. The SCF checks the rights granted to the user for this particular BC service.

A "415 Unsupported Media Type" shall be sent back to the originator if the MESSAGE request contains a body that the SCF does not understand.

5.3.4.1.1   Procedures for Impulsive Request

Case 1: In case of content_type set to "application/vnd.etsi.iptvsad-bc+xml".

Upon receiving a SIP MESSAGE request with Content-type set to "application/vnd.etsi.iptvsad-bc+xml", the SCF retrieves the service action data from the SIP MESSAGE message body and either creates or updates the matching object instance:

- If the Bookmark attribute is set to "NOW", the SCF should set it to the current timestamp.

NOTE: The XML schema mapping to the MIME type: "application/vnd.etsi.iptvsad-bc+xml" is available in annex K of the present document."

Case 2: In case of content_type set to "application/vnd.etsi.iptvsad-npvr+xml".

Upon receiving a SIP MESSAGE request with Content-type set to "application/vnd.etsi.iptvsad-npvr+xml", the SCF retrieves the service action data from the SIP MESSAGE message body and either creates or updates the matching object instance:

- If NPVRContentId is not present, it should be generated by the SCF itself.

- If the request is acknowledged by the proper entities (e.g. NPVR servers) RecordStatus is set to "Scheduled" by the SCF.

- If the RecordStartDate attribute is set to "NOW", the SCF should set it to the current timestamp.

The SCF may check the tNPVRStorageLimitInTime and tNPVRStorageLimitInVolume parameters associated with the user profile to decide whether to allow the user to capture the selected live content.

On both cases, a SIP 200 OK message with no body shall be sent to the originator if the MESSAGE request is successfully received for an existing call and the service action data objects shall be created (or updated) according to the data retrieved from the MESSAGE message body.

The SCF follows relevant procedures to initiate the recording of the content by the N-PVR-MF. Details of the procedures are outside scope of the present document.

5.3.4.1.2 Procedures for Offline Request

Upon receiving a SIP MESSAGE request, the SCF checks to see if the Content-type set to "application/vnd.etsi.iptvsad-npvr+xml". If so, it follows the procedures outlined in corresponding case 2 in clause 5.3.4.1.1.

5.3.4.2 Procedures for NPVR Session

The SCF follows procedures outlined in clause 5.3.2 for handling a COD session.

> NOTE: The XML schema mapping to the MIME type: "application/vnd.etsi.iptvsad-npvr+xml" is available in annex K of the present document.

5.4 Media Control Function (MCF)

5.4.1 Procedure for CoD service

The MCF shall support the procedures specified in ES 283 003 [20] applicable to a terminating UA.

5.4.1.1 Procedure for providing missing parameters before session initiation

When receiving SIP OPTIONS request, the MCF shall examine the CoD content identifier present in the user-part of the TO header.

The MCF may decide to redirect the request to another MCF as described in TS 182 027 [2], clause 5.1.3.3. In this case, the MCF shall return a 301 response if the content is not managed by this MCF and the MCF indicates one or more MCF addresses in the contact header as indicated in ES 283 003 [20].

In case the MCF responds to the request, the MCF shall answer with the SDP description of the content delivery channel conforming to clause 5.4.1.2.1.1, as requested by the request URI.

5.4.1.2 Session initiation

When receiving COD session initiation SIP request, the MCF shall examine the CoD content identifier present in the user-part of the TO header and the media parameters in the received SDP, if present.

The MCF may decide to redirect the request to another MCF as described in TS 182 027 [2], clause 5.1.3.3.

In this case, the MCF shall return a 301 response if the content is not managed by this MCF or 302 response for any other reasons (e.g. load-balancing).

The MCF indicates one or more MCF addresses in the contact header as indicated in ES 283 003 [20].

5.4.1.2.1 Procedure for establishing the RTSP content control and content delivery channel

5.4.1.2.1.1 MCF as SDP answerer

In the case when the MCF receives a session initiation request, the MCF shall examine the RTSP SDP parameters and shall allocate server ports for the CoD session. In case the MCF supports CoD RTSP playback control Method 1 as defined in clause 7.2.1, the MCF shall generate an RTSP session ID for the content control channel. The MCF shall also examine the media lines of the media channel SDP offer.

If none of the media lines in the SDP offer are acceptable, it shall reply with a SIP error code 488 Not Acceptable here, response. One reason may be that the SDP does not match the indicated content.

Else, the MCF shall answer with a SIP 200 OK, indicating the SDP answer. If the content that the user has selected cannot be found the MCF shall reply with appropriate, SIP error code 404 Not Found, response.

The SDP parameters for the RTSP channel shall be set as follows:

- An 'm' line for an RTSP stream of format: m=<media> <port> <transport> <fmt>:

  - The media field shall have a value of "application".

  - The port field is setup according to ES 283 003 [20]. The port number is set to the port allocated by the MCF. The "setup" attribute is set to 'passive' indicating that connection shall be initiated by the other endpoint (UE).

  - The transport field shall be identical to the one received in the SDP offer.

  - The fmt field shall be identical to the one received in the SDP offer.
    (ex. m=application 554 tcp iptv_rtsp).

- An "a=setup" attribute shall be present and set as "passive" as defined in ES 283 003 [20]
  (ex:a=setup:passive).

- An "a= connection" attribute shall be present and set as "new" as defined in ES 283 003 [20]
  (ex:a=connection:new).

NOTE: RTSP over UDP is out of scope of the present document.

- One or more a=fmtp lines representing RTSP specific attributes set as follows:

  - An "fmtp:iptv_rtsp h-uri" attribute shall be set to the RTSP URL to be used in the RTSP requests The h-uri can be in form of absolute or relative URI. If absolute URI is specified then it is used as-is in subsequent RTSP requests. If relative URI is specified in form of a media path, then the RTSP absolute URL could be constructed by the UE using the IPAddress (from c-line) and port (from m-line) as the base followed by h-uri value for the media path.

  - (a=fmtp:rtsp h-uri=<request-uri>).

  - In case the MCF supports CoD RTSP playback control Method 1 as defined in clause 7.2.1, the MCF shall include a "fmtp:iptv_rtsp h-session" attribute representing the session-id of the RTSP session to be created (ex. a=fmtp:iptv_rtsp h-session = <rtsp-session>).

  - For content related to BC service with trick-play mode the MCF shall include "fmtp:iptv_rtsp h-offset" attribute that indicates where the playback is to start from
    (ex. a=fmtp:iptv_rtsp h-offset = <media-offset>).

For each media stream controlled by the RTSP content control channel, SDP answer shall include a content delivery channel media description set as follows:

- the "m=" line indicates the type of the media, the transport protocol and the port of the related content delivery channel. If an fmt parameter is in the SDP offer it shall be completed with the supported format by the MDF;

- the "c=" line shall include the network type with the value set to IN, the address type set to IP4 or IP6 and unicast address of the flow related to the content delivery channel, (ex. c=IN IP4 <IP_ADDRESS>);

- the "b=" line shall contain the proposed bandwidth. Since the COD media stream is unidirectional the bandwidth shall be set to 0, except for the case that the transport is RTP and RTCP is allowed.
  (ex. b=AS:0);

- an "a=" line with a "sendonly"
  (ex. a=sendonly).

5.4.1.2.2   Procedure for establishing the RTSP channel separately

5.4.1.2.2.1   MCF as SDP answerer

When the MCF receives the SDP offer for establishing only the RTSP channel in the session initiation request, the MCF shall examine the SDP parameters.

If the SDP offer is not acceptable, the MCF shall reply with an SIP error response. Else, the MCF shall answer with a SIP 200 OK, indicating the SDP answer.

The SDP parameters for the RTSP channel shall be set as follows:

- An "m" line for an RTSP stream of format: m=<media> <port> <transport> <fmt>.

- The media field shall have a value of "application".

- The port field is setup according to ES 283 003 [20]. Typically, the port number is a port number of 554 (rtsp server port) on its "m" line, and the "setup" attribute is set to "passive" indicating that connection shall be initiated by the other endpoint (UE).

- The transport field shall be identical to the one received in the SDP offer.

- The fmt field shall be identical to the one received in the SDP offer.

- If "a=setup" attribute is present in the offer, it shall be present and set to "passive" as defined in ES 283 003 [20].

- If "a= connection" attribute is present in the offer, it shall be present and set to "new" as defined in ES 283 003 [20].

Optionally,an "a=fmtp:iptv_rtsp h-uri" attribute shall be set to the RTSP URL to be used in the RTSP requests The h-uri can be in form of absolute or relative URI. If absolute URI is specified then it is used as-is in subsequent RTSP requests. If relative URI is specified in form of a media path, then the RTSP absolute URL could be constructed by the UE using the IPAddress (from c-line) and port (from m-line) as the base followed by h-uri value for the media path. (a=fmtp:rtsp h-uri=<request-uri>).

5.4.1.3   Session modification

Upon receipt of a re-INVITE request or an UPDATE request, the MCF shall modify the session as specified in ES 283 003 [20] if the request is acceptable to the MCF in accordance with the user subscription.

In order to modify the session from the MCF side, the MCF shall send a re-INVITE or an UPDATE request.

The SDP parameters for the RTSP channel shall be set to the same parameters as specified in clause 5.4.1.2.2.1 except for the "a=connection" attribute. The attribute shall be set to "existing" as defined in ES 283 003 [20].

For each media stream controlled by the RTSP content control channel the SDP offer shall include a content delivery channel media description set as follows:

- The "m=" line indicates the type of the media, the transport protocol the port of the related content delivery channel.

- The "c=" line shall include the network type with the value set to IN, the address type set to IP4 or IP6, and unicast address of the flow of the related content delivery channel.

- The "b=" line shall contain the proposed bandwidth.

- An "a=" line with a "sendonly".

The MCF shall not modify RTSP channel m-line description in the SDP if the media delivery streams controlled by RTSP are not removed (port not set to zero in m-lines) in the SDP.

5.4.1.3.1   Procedure for establishing the content delivery channel

5.4.1.3.1.1   MCF as SDP answerer

When the MCF receives the SDP offer for establishing content delivery channel in the session modification request, the MCF shall examine the SDP parameters and answer with a SIP 200 OK, indicating the SDP answer.

The SDP parameters for the RTSP channel shall be set to the same parameters as specified in clause 5.4.1.2.2.1 except for the "a=connection" attribute. The attribute shall be set to "existing" as defined in ES 283 003 [20].

The SDP parameters shall include one or more media description sets as follows:

- The "m=" line indicates the type of the media, the transport protocol and the port. The type of the media, the transport protocol shall be identical to the one received in the SDP offer. The port shall be set to the value used for the content delivery channel.

- The "c=" line shall include the network type with the value set to IN, the address type set to IP4 or IP6 and unicast address of the flow of the related content delivery channel.

- The "b=" line shall contain the bandwidth. The bandwidth attribute shall be identical to the one received in the SDP offer.

- The "a=" line with a "sendonly".

5.4.1.4   Session termination

5.4.1.4.1   Session termination using RTSP method 1

Upon receipt of a BYE request, the MCF shall terminate the session as specified in ES 283 003 [20].

In order to terminate the session from the MCF side, the MCF shall first close the RTSP session that was established during session initiation by closing the underlying TCP connection if existing (e.g. in case of persistent TCP connection). The MCF shall then send a BYE request as specified in ES 283 003 [20].

5.4.1.4.2   Session termination using RTSP method 2

Upon receipt of a BYE request, the MCF shall terminate the session as specified in ES 283 003 [20].

In order to terminate the session from the MCF side, the MCF shall first close the RTSP session that was established during session initiation by closing the underlying TCP connection if existing (e.g. in case of persistent TCP connection). The MCF shall then send a BYE request as specified in ES 283 003 [20].

5.4.1.5   Procedures for handling COD Service action data

Upon receiving normal playback RTSP PLAY (scale header set to 1) (See note 1) request from UE, the MCF may send a SIP INFO request to the SCF containing the user related IPTV service action data. The content of INFO request shall be as follows:

- The value of the Request-URI shall be set to the one used in the related session.

- From and To headers shall be set to the one defined during the session initiation procedure.

- Call-ID shall be set to the same value as that of the CoD session.

- CSeq shall be generated by UE following rules defined in ES 283 003 [20] for request within a dialog.

- The Content-type header shall include the registered MIME type of XML documents representing IPTV service action data: "application/vnd.etsi.iptvsad-cod+xml".

- The message body carries the service action data: the matching "Available CoD" object shall be updated so that CoDDeliveryStatus is set to "Ongoing".

NOTE 1: This will only be performed when the very first RTSP PLAY (scale header=1) request is received by the MCF for a given CoD session (to avoid over flooding the network with unnecessary updates when user presses Play subsequently to FFW or FRW).

In the case of normal end of streaming, MCF may send a SIP INFO request to the SCF containing the related service action data. The content of INFO request shall be as follows:

- The value of the Request-URI shall be set to the one used in the related session.

- From and To headers shall be set to the one defined during the session initiation procedure.

- Call-ID shall be set to the same value as that of the CoD session.

- CSeq shall be generated by UE following rules defined in ES 283 003 [20] for request within a dialog.

- The Content-type header shall include the registered MIME type of XML documents representing IPTV service action data: "application/vnd.etsi.iptvsad-cod+xml".

- The message body carries the service action data: the matching "Available CoD" object shall be updated so that CoDDeliveryStatus is set to "Completed".

In the case of error occurring in streaming, MCF may send a SIP INFO request to the SCF containing the related service action data. The content of INFO request shall be as follows:

- The value of the Request-URI shall be set to the one used in the related session.

- From and To headers shall be set to the one defined during the session initiation procedure.

- Call-ID shall be set to the same value as that of the CoD session.

- CSeq shall be generated by MCF.

- The Content-type header shall include the registered MIME type of XML documents representing IPTV service action data: "application/vnd.etsi.iptvsad-cod+xml".

- The message body carries the service action data: the matching "Available CoD" object shall be updated so that CoDDeliveryStatus is set to "Failed".

NOTE 2: The XML schema mapping to the MIME type: "application/vnd.etsi.iptvsad-cod+xml" is available in annex K.

If the INVITE request received in session initiation contains an Allow header that does not describe INFO, the MCF shall not send INFO request of CoD service action data.

NOTE 3: INFO request may arrive at the UE if the SCF acts as a proxy. Handling of that case is not specified in the current release. If the SIP INFO request of service action data resulted in 405 or 415 response, the MCF does not send again the INFO request of service action data.

5.4.2   Procedure for support of BC service with trick play

As a general rule, the MCF is not involved in the BC service. Only in the case of a user initiating trick play mode of a Broadcast TV session, the MCF in charge of recording the requested channel will be linked to the session.

At receipt of an INVITE message from the SCF, the MCF will derive the content ID in real time and from the channel identifier it received in the TO header then carry out the same steps as described for the CoD session (see clause 5.4.1.2) before replying back, in a positive case, with the SIP 200 OK message.

In the SDP answer, the only difference with regards to the media descriptors compared to a normal CoD session is the inclusion of an h-offset attribute different than 0.

At receipt of the ACK message acknowledging the SIP 200 OK, trick mode can be initiated.

When the trick mode is deactivated by the UE, the MF will receive a BYE message as in the CoD session termination. The successful release of resources will imply responding with a SIP 200 OK to the SCF.

5.4.3   Procedure for NPVR Session

The MF follows procedures outlined in clause 5.4.1 for CoD session initiation, modification and termination procedures.

5.5   Core IMS

5.5.1   Procedure for Registration

The behaviour of Core IMS entities when supporting IMS registration shall conform to ES 283 003 [20].

5.5.2   Procedure for Service Attachment

5.5.2.1   Push mode

The behaviour of Core IMS entities when processing the third-party REGISTER and MESSAGE method shall conform to ES 283 003 [20].

The S-CSCF sends a third-party REGISTER request to the SDF that matches the Filter Criteria of the service profile from the UPSF for the REGISTER event.

The Initial Filter Criteria shall include the REGISTER method as the prime Service Trigger Point. Examples of service trigger points that may be used to build an appropriate IFC are available in annex R.

5.5.2.2   Pull mode

The behaviour of Core IMS entities when processing the SUBSCRIBE and NOTIFY methods shall conform to ES 283 003 [20].

SUBSCRIBE requests are routed to the SDF using one of the following methods:

1)   The SDF identity received in the Request URI matches a Public Service Identity (PSI) hosted by the SDF.

2)   The SUBSCRIBE request matches an Initial Filter Criteria (IFC) stored against the public user identity of the UE.

The present document does not place any restrictions on the procedures to be used for routing a session to a PSI nor on the list of service trigger points to use in building Initial Filter Criteria.

The Initial Filter Criteria shall include the SUBSCRIBE method as the prime Service Trigger Point. Examples of service trigger points that may be used to build an appropriate IFC are available in annex R.

5.5.3   Procedure for Service Configuration

Core IMS entities are not involved during service configuration procedures except if the UE subscribes to notifications to changes to its user profile, in which case the behaviour of Core IMS entities when processing the SUBSCRIBE and NOTIFY methods shall conform to ES 283 003 [20].

SUBSCRIBE requests are routed to the SDF using one of the following methods:

1)   The identity received in the Request URI matches a Public Service Identity (PSI) hosted by the SCF acting as a front end to manage the user profile.

2)   The SUBSCRIBE request matches an Initial Filter Criteria stored against the public user identity of the UE.

The present document does not place any restrictions on the procedures to be used for routing a session to a PSI nor on the list of service trigger points to use in building Initial Filter Criteria.

The Initial Filter Criteria shall include the SUBSCRIBE method as the prime Service Trigger Point. Examples of service trigger points that may be used to build an appropriate IFC are available in annex R.

5.5.4 Procedure for Service Selection

Core IMS entities are not involved during service selection procedures.

5.5.5 Procedure for CoD service

The behaviour of Core IMS entities shall conform to the procedure for handling an originating session as described in ES 283 003 [20].

INVITE requests are routed to the SCF using one of the following methods:

1) The SCF identity received in the Request URI matches a Public Service Identity (PSI) hosted by an SCF providing CoD service logic.

2) The INVITE request matches an Initial Filter Criteria stored against the public user identity of the UE.

The present document does not place any restrictions on the procedures to be used for routing a session to a PSI nor on the list of service trigger points to use in building Initial Filter Criteria.

The Initial Filter Criteria shall include the INVITE method as the prime Service Trigger Point. Examples of service trigger points that may be used to build an appropriate IFC are available in annex R.

5.5.6 Procedure for BC service

The behaviour of Core IMS entities conforms to the procedure for handling an originating session as described in ES 283 003 [20], with the additional capability that the P-CSCF transports the service package attributes as defined in annex N when present to the RACS as part of BC service resource reservation. It also handles appropriate error messages when bandwidth negotiation fails as defined in ES 283 003 [20].

INVITE requests are routed to the SCF using one of the following steps:

1) The well known Public Service Identity (PSI) received in the request URI is mapped to a set of SCFs providing BC service logic.

2) The SCF address is resolved by the INVITE request matching an Initial Filter Criteria stored against the public user identity of the UE.

The present document does not place any restrictions on the procedures to be used for routing a session to a PSI nor on the list of service trigger points to use in building Initial Filter Criteria.

The Initial Filter Criteria shall include the INVITE method as the prime Service Trigger Point. Examples of service trigger points that may be used to build an appropriate IFC are available in annex Q.

5.6 Common Procedures

NOTE: If the application contains a set of optional features and depending on the type of application (for example support of BC or CoD services have different application ids), there might be a need to have multiple IMS Application Reference Identifiers for that application that is one IMS Application Reference Identifier per sub-feature.

5.6.1 IMS Communication Service Identifier

The IMS Communication Service Identifier uniquely identifies the IMS service and associated SIP procedures. The IMS Communication Service Identifier defines restrictions to which SIP procedures are possible within a single SIP session or standalone transaction and how those SIP procedures are used. The IMS communication service contains an aggregation of zero, one, or several media components and the service logic managing the aggregation, represented in the protocols used, see ES 283 003 [20].

URN used to define the ICSI for the "IMS IPTV Service": urn:urn-7:3gpp-service.ims.icsi.iptv.

The URN is registered at http://www.3gpp.org/tb/Other/URN/URN.htm.

Summary of the URN: This URN indicates that the device supports the IMS IPTV Service.

5.6.2 Session Control Procedures

The ICSI may be supported to differentiate the procedures for IPTV service in relation to other IMS services. For example, an IPTV unicast media stream may require differentiation from other unicast streams for other services like telephony.

The "IMS IPTV Service" may support different types of media, including media types listed in the present document. The session control procedures for the different media types shall be in accordance with ES 283 003 [20] and the present document, with the following additions:

If the ICSI is used the following applies:

a) "IPTV" is an IMS communication service and the P-Preferred-Service and P-Asserted-Service headers shall be treated as described in ES 283 003 [20]. The coding of the ICSI value in the P-Preferred-Service and P-Asserted-Service headers shall be as described in clause 5.6.1.

b) The UE shall include the g.3gpp.icsi-ref feature tag equal to the ICSI value defined in clause 5.6.1 in the P-Preferred-Service header field in initial requests and responses as described in ES 283 003 [20].

c) The UE shall include the g.3gpp. icsi-ref feature tag equal to the ICSI value defined in clause 5.6.1 in the Contact header field in initial requests and responses as described in ES 283 003 [20].

d) The UE shall include an Accept-Contact header field containing the g.3gpp. icsi-ref feature tag containing the ICSI value as defined in clause 5.6.1 of ES 283 003 [20] in initial requests. If the user requests capabilities other than IPTV, the Accept-Contact header field may contain other feature parameters and feature parameter values, and other Accept-Contact header fields may be added to accurately express user preferences as per ES 283 003 [20].

e) The AS may include the g.3gpp. icsi-ref feature tag equal to the ICSI value defined in clause 5.6.1 in the P-Preferred-Service header field in initial requests and responses as described in ES 283 003 [20].

f) The AS may include the g.3gpp. icsi-ref feature tag equal to the ICSI value defined in clause 5.6.1 in the Contact header field in initial requests and responses as described in ES 283 003 [20].

NOTE: How the user indicates other feature parameters and feature parameter values are outside of the scope of the present document.

6 Procedures using HTTP for IMS-based IPTV

6.1 User Equipment (UE)

6.1.1 Procedures for service selection

6.1.1.1 Procedure for service personalization

For HTTP-based data retrieval, when sending the HTTP request to the SSFs, the UE may indicate personalization information to enable personalized answer. This shall be done by adding the following HTTP header to the request:

- X-3GPP-Intended-Identity to transmit the public identity.

- User-agent to transmit UE ID.

The authentication shall follow TS 187 003 [10], and may be performed either using the mechanisms specified in TS 133 222 [14] or HTTP Digest access authentication, as described in ES 283 003 [20].

The UE shall implement Transport Layer Security (TLS), as described in RFC 2246 [32].

NOTE: Authentication mechanism is specified in the present document.

6.1.1.2   Request of DVB SD&S

In the pull model of unicast delivery of a DVB SD&S data, the HTTP protocol shall be used conforming to
TS 102 034 [3], clause 5.4.2.2.

The payload id and segments to be retrieved shall be those advertised in the SDF attachment response.

6.1.1.3   Request of DVB BCG

6.1.1.3.1   Container-based request

In the pull model of unicast container-based delivery of DVB BCG, data the HTTP protocol shall be used conforming
to TS 102 539 [13], clause 4.1.2.2.2.

6.1.1.3.2   Query mechanism

In the pull model of unicast query mechanism of DVB BCG data, the HTTP protocol is used to transport SOAP
messages. This shall be conforming to TS 102 539 [13], clause 4.2.

6.1.1.4   Request of OMA BCAST ESG

In the pull model of unicast delivery of an OMA BCAST ESG, the HTTP protocol shall be used conforming to
OMA-TS-BCAST_Service_Guide, [6], clause 5.4.3.

6.1.1.5   Request of service action data

When the UE requests Service Action Data, it shall send HTTP GET request as defined in RFC 2616 [30].

The HTTP URL shall be /tispan/serviceactiondata?id=DomainName&Payload=Type where DomainName and Type are
retrieved from the SSF as defined in clause L.1.3.

If Payload is set to 0, it means that the UE requests all available Service Action Data.

When receiving HTTP 200 OK response, the UE shall evaluate the received XML document as defined in
clause 6.1.1.6.

6.1.1.6   Use of service selection information

The UE shall use parameters received from SSF as defined in clause L.2 for BC session initiation and L3 for CoD
session initiation.

   NOTE: There is no restriction on the UE to use any parameter received from SSF also for other purposes than
            session initiation, e.g. to present SSF information to the user.

Concerning broadcast service selection information, BC service package parameters are defined in Package Discovery
record as described in TS 102 034 [3], clause 5.2.6.5. for DVB SD&S, and in Purchase Item as described in
OMA-TS-BCAST_ServiceGuide [6], clause 5.1.2.6 for OMA ESG.BC service parameters are defined in
TS 102 034 [3], clause 5.2.6.2. for DVB SD&S and OMA-TS-BCAST_Service_Guide [6], clause 5.1.2.

For each BC service package, when parsing the list of related parameters the UE shall take the following action:

   •   information relates to BC Service Package whom the UE has already an entree. The UE shall update
        parameters related to the service package (e.g. the list of related BC services);

   •   information relates to BC Service Package not known by the UE. The UE shall store parameters related to the
        service package.

For each BC service, when parsing the list of related parameters the UE shall take the following action:

   •   information relates to a BC service whom the UE has already an entree. If present, the UE shall update stored
        BC services parameters;

- information relates to a BC service not known by the UE: the UE creates a new entree for this BC service. If present, it shall store at least multicast and source address(es), port, transport and codecs information related to the BC service.

The UE may store a part of the EPG information covering certain period of time and refresh this information periodically This avoid the UE to contact the SSF every time the user needs to consult the EPG.

If the UE is unable to contact any discovered SSF, it shall not delete stored information.

Concerning Service Action Data record, the UE shall use n-PVR, CoD and BC data as follows:

- if the data type indicates n-PVR service action data, the UE shall use the retrieved data as defined in clause 5.1.7;

- if the data type indicates CoD service action data, the UE may use "CoDoffset" parameter to initiate CoD session related to the indicated Content-Id as defined in clause 7.1.1.2;

- if the data type indicates BC service action data, the UE may use "BCServiceId" parameter to indicate the channel the UE intend to join in BC session initiation (see clause 5.1.3.1).

6.1.2   Procedure for service configuration

6.1.2.1   General

The UE implements the role of an XCAP client, as described in RFC 4825 [9], in accordance with the IPTV application usage specified in annex B.

The UE shall implement HTTP Digest access authentication, as described in ES 283 003 [20].

The UE shall implement Transport Layer Security (TLS), as described in RFC 2246 [32].

On sending an HTTP request, the UE may indicate the user's identity intended to be used with the SCF or stand-alone XDMS by adding a HTTP X-3GPP-Intended-Identity header (see TS 124 109 [11]) to the outgoing HTTP request.

6.1.2.2   Subscription for notification of state changes in XML document

In order to keep the IPTV services data synchronized with the network elements and other terminals that the user might be using, the UE should subscribe to changes in the XCAP IPTV documents by generating a SUBSCRIBE request in accordance with RFC 5874 [15] and RFC 5875 [26].

6.2   Service Control Function (SCF)

6.2.1   Procedure for service configuration

6.2.1.1   General

An Application Server implements the role of an XCAP server as described in RFC 4825 [9].

6.2.1.2   Manipulation acceptance

When the XCAP server receives an HTTP PUT, HTTP GET or HTTP DELETE request for manipulating or fetching a resource list, the XCAP server shall first authenticate the request and then perform authorization.

The SCF shall implement HTTP Digest access authentication as described in ES 283 003 [20].

The SCF shall implement Transport Layer Security (TLS) as described in see RFC 2246 [32].

Clause 6.2.1.3 provides more details on the authentication and authorization of HTTP requests.

Afterwards the XCAP server shall perform the requested action and generate a response in accordance with RFC 4825 [9] and the IPTV application usage specified in annex B.

6.2.1.3   Authentication and authorization

An Authentication Proxy (AP) may exist between the UE and the SCP, in which case the behaviour of the AP is assumed to conform to TS 183 023 [12].

If an Authentication Proxy (AP) is provided in the path of the HTTP request, then the SCF receives an HTTP request from a trusted source (the AP) and contains an HTTP X-3GPP-Asserted-Identity header (TS 124 109 [11]) that includes an asserted identity of the user. In this case the SCF does not need to authenticate the user, but just provide authorization to access the requested resource.

If an HTTP X-3GPP-Asserted-Identity header (TS 124 109 [11]) is not present in the HTTP request or if the request is received from a non-trusted source, then the SCF needs to authenticate the user prior to providing authorization to the XCAP resource by applying the following procedures.

On receiving an HTTP request that does not contain an Authorization header the SCF shall:

   a)   challenge the user by generating a 401 Unauthorized response that contains the proper Digest authentication parameters (e.g. realm), according to ES 283 003 [20]. Provisioning of credentials to authenticate the user is outside the scope of the present document; and

   b)   forward the 401 Unauthorized response to the sender of the HTTP request.

On receiving an HTTP request that contains an Authorization header, the SCF shall:

   a)   apply the authentication procedures defined in ES 283 003 [20]; and

   b)   authorize or deny authorization depending on the authenticated identity.

6.2.1.4   Subscription acceptance and notification of state changes in XML document

When the SCF receives a SUBSCRIBE request having the Event header field value set to "xcap-diff", the SCF shall authorize the request based on the contents of the P-Asserted-Id. If the authorization is successful the SCF shall generate a response to the SUBSCRIBE request and generate notifications in accordance with RFC 5874 [15] and RFC 5875 [26].

6.3   Service Selection Function (SSF)

6.3.1   Procedure for service selection

6.3.1.1   Authentication and authorization in case of personalized service selection information

In case of service selection personalization the SCF shall authenticate the user.

The authentication shall follow TS 187 003 [10], and may be performed either using the mechanisms specified in TS 133 222 [14] or HTTP Digest access authentication as described in ES 283 003 [20].

The SSF shall implement Transport Layer Security (TLS) as described in RFC 2246 [32].

An Authentication Proxy (AP) may exist between the UE and the SSF in which case the behaviour of the AP is assumed to conform to TS 183 023 [12] and TS 187 003 [10].

If an Authentication Proxy (AP) is provided in the path of the HTTP request, then the SSF receives an HTTP request from a trusted source (the AP) and the request contains an HTTP X-3GPP-Asserted-Identity header (TS 124 109 [11]) that includes an asserted identity of the user. In this case the SSF does not need to authenticate the user, but just provide authorization to access the requested resource.

If an HTTP X-3GPP-Asserted-Identity header (TS 124 109 [11]) is not present in the HTTP request or if the request is received from a non-trusted source, then the SSF needs to authenticate the user prior to providing personalize information by applying the following procedures:

On receiving an HTTP request that does not contain an Authorization header the SSF shall:

   a)   challenge the user by generating a 401 Unauthorized response that contains the proper Digest authentication parameters (e.g. realm), according to ES 283 003 [20]. Provisioning of credentials to authenticate the user is outside the scope of the present document; and

   b)   forward the 401 Unauthorized response to the sender of the HTTP request.

On receiving an HTTP request that contains an Authorization header, the SSF shall:

   a)   apply the authentication procedures defined in ES 283 003 [20]; and

   b)   authorize or deny authorization depending on the authenticated identity.

6.3.1.2   Procedure for service personalization

If personalization headers are present in the query from the UE, the SSF shall extract the UE ID and/or the public user identity information that is present in the query to customize/personalize the service information that is returned in the query response.

The SSF shall use the public user identity that is specified in the X-3GPP-Intended-Identity header or the X-3GPP-Asserted-Identity header (as defined in clause 6.3.1.1) if an authentication proxy is used to fetch the corresponding IPTV user profile associated with the user. For instance, the Parental Control level (if present) should be used to remove unsuitable elements from the COD listings that are returned to the UE.

The SSF shall use the public user identity that is specified in the X-3GPP-Intended-Identity header or the X-3GPP-Asserted-Identity header (as defined in clause 6.3.1.1) if an authentication proxy is used and the UE-ID that is specified in the user-agent header to fetch the corresponding UE profile information from the IPTV user profile associated with the specified IPTV user. If present, the SSF should use the UE capabilities to return back service information matching the capabilities supported by the specific UE. For example, The UE Capabilities information such as supported video frame rates and supported encodings can be used to identify the decoding and display capabilities of the UE and can be used to return back only SD content listings to UE that has no HD support.

The fetching of IPTV user profile shall be done towards a dedicated database or UPSF within a service provider domain as specified in TS 182 027 [2], clause 7.2.4.

   NOTE: The support of personalization for multiple service providers from a single UPSF as well as the interface between the SSF and the dedicated database is out of scope of the present document.

6.3.1.3   Delivery of DVB SD&S

When the SD&S SSF receives a HTTP GET request, if personalization headers are presents it shall use those headers in order to build a personalized response.

The SD&S SSF shall send an HTTP response conforming to TS 102 034 [3], clause 5.4.2.

The body of the HTTP response shall contain an XML document with the appropriate SD&S offering record, conforming to TS 102 034 [3], clause 5.2.6.

Available Offering records are:

   •   The Broadcast Discovery record (clause 5.2.6.2) is a list of IPTV services.

   •   The Package Discovery record (clause 5.2.6.5) is a list of packages, a package being a list of pointers to services that are advertised in the broadcast discovery record.

- The BCG Discovery record (clause 5.2.6.6) is a list of BCGs, and for each of them the location of the BCG SSF(s) to connect to the BCG server(s) (DVB multicast and unicast modes are available, plus a specific Query mechanism).

    - The type of TV-Anytime content carried in the Payload shall be advertised by the SSF, conforming to TS 102 539 [13], clause 4.1.2.1 table 2.

    - When present, the DVBSTP@Source or the HTTP@Location of the TransportMode parameter in BCG Discovery Record represent respectively the multicast address (when service selection data are multicasted) and the URI (when service selection is done through HTTP) used by the BCG SSF.

    - When using the DVB pull mode without SOAP, the SD&S SSF shall include the Segment information.

6.3.1.4   Delivery of DVB BCG

6.3.1.4.1   Container-based delivery

When the BCG SSF receives a HTTP GET request, if personalization headers are presents it shall use those headers in order to build a personalized response.

The BCG SSF shall send an HTTP response conforming to TS 102 539 [13], clause 4.1.2.

The body of the HTTP response shall contain an XML document with the appropriate BCG data, conforming to TS 102 539 [13].

6.3.1.4.2   Query response

When the BCG SSF receives a BCG Query SOAP message, if personalization headers are present it shall use those headers in order to build a personalized response.

The BCG SSF shall send a SOAP response conforming to TS 102 539 [13], clause 4.2.

6.3.1.5   Delivery of OMA BCAST ESG

The procedure for retrieving OMA BCAST service selection information is employed to retrieve one or more Service Guide Delivery Descriptors (SGDD) and/or Service Guide Delivery Units (SGDU). The SGDD describes service level information as well as access information to the Service Guide fragments. The SGDU is the transport-independent network structure for encapsulating Service Guide fragments.

When the ESG SSF receives a HTTP POST request, if personalization headers are presents (in the form of key-value pairs) it shall use those headers in order to build a personalized response. For instance, the ESG SSF may use the provided user identity to retrieve the associated Parental Control Level in the IPTV user profile. This Parental Control Level would then be used to remove non suitable elements from the ESG data that are sent back. The provided user identity may also be used to retrieve a personalized ESG using the method in OMA-TS-BCAST_Service_Guide-V1_0 [6], clause 5.4.3.3.The ESG SSF shall send an HTTP response conforming to OMA-TS-BCAST_Service_Guide-V1_0 [6], clause 5.4.3.1. The body of the HTTP response shall contain an XML document with SGResponse data, conforming to OMA-TS-BCAST_Service_Guide-V1_0, clause 5.4.3.1.1 [6].

6.3.1.6   Delivery of Service Action Data

When receiving HTTP GET request for service action data, the SSF shall evaluate "Payload" parameter in the HTTP query and respond with the appropriate XML document as defined in annex D.

If the "Payload" parameter indicates BC service action Data, the message body carries the following parameters:

- IPTVActionDataCommand shall be set to "Notify".

- Notify shall be set to "IPTVBcActionData".

- BCServiceId is set to the value of the channel previously reported by the UE in BC session information procedure as defined in clause 5.1.3.5.

- If available, the following parameters shall be present: ProgrammeID, Bookmark, BookmarkExpiryTime. It means that a record exists for such a bookmark and that the UE can use it as an NPVR content.

If the "Payload" parameter indicates CoD service action Data, the message body carries the following parameters:

- IPTVActionDataCommand shall be set to "Notify".

- Notify shall be set to "IPTVCodActionData".

- For each content identified by a CoDId:

  - CoDDelivery status shall be present and set to the value stored for that content;

  - CoDOffset shall be present and set to the value stored for that content.

If the "Payload" parameter indicates NPVR service action Data, the message body carries the following parameters:

- IPTVActionDataCommand shall be set to "Notify".

- Notify shall be set to "IPTVNpvrActionData".

- For each NPVR content identified by a NPVRContentId, the following parameters shall be present if available: BCServiceId, RecordStartDate, RecordEnDate, RecordStatus, RecordOffset and RecordExpiryTime shall be present if available.

If the "Payload" parameter is set to "ALL", the SSF shall send all available Service Action Data as defined above.

If no information is available for the requested type, the SSF shall answer with a 404 error code.

6.4   Stand-Alone XMDS

6.4.1   Procedure for service configuration

6.4.1.1   General

The stand-alone XDMS implements the role of an XCAP server as described in RFC 4825 [9].

6.4.1.2   Manipulation acceptance

The behaviour of a stand-alone XDMS server with regards to XCAP is identical to the behaviour of an SCF as described in clause 6.2.

6.4.1.3   Authentication and authorization

The behaviour of a stand-alone XDMS server with regards to XCAP is identical to the behaviour of an SCF as described in clause 6.2.

6.4.1.4   Subscription acceptance and notification of state changes in XML document

A stand-alone XDMS does not support subscriptions to profile changes. Subscriptions to profile changes are directed to the SCF acting as a front-end to the XDMS.

7   Procedures using RTSP for IMS-based IPTV

This clause specifies how the playback control, e.g. in the CoD Service, through RTSP is achieved. Two approaches have been identified:

- "Method 1": Clauses 7.1.1 and 7.2.1 describe a protocol which uses a subset of the RTSP methods defined in RFC 2326 [8], interpreting SIP INVITE and SIP BYE as triggers for RTSP Session Initiation and termination.

- "Method 2": Clauses 7.1.2 and 7.2.2 describe a protocol which follows RFC 2326 [8].

7.1   User Equipment (UE)

7.1.1   Procedures for RTSP playback control (Method 1)

7.1.1.1   Introduction

The UE shall support the following RTSP methods for RTSP playback control:

- PLAY (UE to MCF).

- PAUSE (UE to MCF).

- GET_PARAMETER (UE to MCF).

- SET_PARAMETER (UE to MCF).

- ANNOUNCE (MCF to UE).

- OPTION (UE to MCF).

  NOTE: The UE is not required to use OPTION method since all the specified methods are mandatory. The OPTION method is included simply to allow for future compatibility and easier introduction of new optional methods.

The methods shall use the same session id as specified in the SDP h-session attribute.

7.1.1.2   Media playback initiation procedure

Upon a request to start playback the UE shall send an RTSP PLAY message to the MCF using the h-uri attribute received in the SDP. If a domain address is used in the RTSP URL the UE shall not perform DNS lookup. The IP header for the RTSP PLAY message shall be set to the IP address from the connection line ("c=") in the SDP answer and the port from the media line ("m=").

  NOTE: The UE does not perform DNS lookup in order to avoid misaligning the information conveyed in the SDP.

The RTSP fields in the RTSP PLAY message shall be filled as follows:

- The RTSP URL shall be set to the value retrieved from the SDP h-uri attribute in the case of an absolute URI. If the value of h-url is a relative URI that is in the form of a media path, then the RTSP absolute URL is constructed by the UE using the SDP IPAddress (from c-line) and port (from m-line) as the base followed by h-uri value for the media path.
  (e.g. `rtsp://10.5.1.72:22554/TV3/823527`).

- If the h-offset attribute is present in the SDP, then the Range parameter in the first RTSP PLAY message shall be included and set to the value retrieved from this SDP h-offset attribute. Else:

  - the Range parameter may be included and set to the value retrieved in the CoD SAD from the SSF in case the user wants to resume a pending CoD at the time it was previously stopped.

- If Range parameter is not sent by the UE, the stream will play from the beginning.
  (e.g. `Range: npt=<OFFSET>-`).

7.1.1.3   Media playback modification procedure

Upon a request to modify playback the UE shall send an RTSP PLAY message with a request to modify the position, speed and/or direction of playback. The UE changes the direction and/or speed of playback by including a `Scale` header or change the position of playback by including a `Range` header.

- Scale header is set as follows:

  -    1 indicates normal play.

  -    If not 1, the value corresponds to the rate with respect to normal viewing rate.

  -    A negative value indicates reverse direction.

If the request is to pause playback, the UE shall send an RTSP PAUSE message.

7.1.1.4   Media playback information retrieval and setting procedure

Upon a request to retrieve playback information the UE shall send an RTSP GET_PARAMETER message. The UE may retrieve the following information:

- position:

  -    The position in the media in seconds.

- scales:

  -    The allowed scales that can be used in the PLAY request.

Any other parameter that is used in GET_PARAMETER request will be rejected by the MCF. An empty body is allowed for RTSP keep alive.

The UE may also set the position parameter (ex. to jump to a bookmark position within a video) by sending the RTSP SET_PARAMETER message. Any other parameter that is used in SET_PARAMETER request will be rejected by the MCF.

7.1.1.5   Handling of media events

Upon the reception of the RTSP ANNOUNCE with indication of end-of-stream the UE may take relevant actions to handle the end of stream event (e.g. Terminating session, rewinding the media stream, etc.). The UE shall respond with a RTSP 200 OK.

In case of BC sessions with trick-play, if the UE receives a RTSP ANNOUNCE request with an end-of-stream indication, the UE may initiate a session modification procedure in order to go back to a normal BC session in multicast mode or may alternatively take other actions (e.g. rewind, pause, terminate session, etc.).

If the UE does not understand any of the headers or the notice-code value in the ANNOUNCE request, it simply shall ignore the request.

7.1.2   Procedure for content control (Method 2)

7.1.2.1   Introduction

After CoD session setup, RTSP as defined in RFC 2326 [8] is used to control media delivery. It includes media setup, media control and media teardown. RTSP header fields shall conform to TS 102 034 [3], clause 6.3.2.

The UE shall support the following RTSP methods:

- DESCRIBE (UE to MCF).

- SETUP (UE to MCF).

- PLAY (UE to MCF).

- PAUSE (UE to MCF).

- TEARDOWN (UE to MCF).

- ANNOUNCE (MCF to UE).

For transport parameters, the ones conveyed over SIP shall always take precedence over the ones conveyed over RTSP.

7.1.2.2   Media description procedure

In case the UE did not get content delivery description information (from the SSF or from the SCF/MCF during the SIP session initiation), it shall request description of the media via the DESCRIBE message. The RTSP URL to send the DESCRIBE message to is retrieved from the SSF data or from the MCF during the SIP session initiation.

If a domain address is used in the RTSP URL the UE shall not perform DNS lookup. The IP header for the RTSP DESCRIBE message shall be set to the IP address from the connection line ("c=") in the SDP answer and the port from the media line ("m=").

- The RTSP URL shall be set to the value retrieved from the SDP h-uri attribute in the case of an absolute URI. If the value of h-url is a relative URI that is in the form of a media path, then the RTSP absolute URL is constructed by the UE using the SDP IPAddress (from c-line) and port (from m-line) as the base followed by h-uri value for the media path.
  (e.g. rtsp://10.5.1.72:22554/TV3/823527).

  NOTE: The UE does not perform DNS lookup in order to avoid misaligning the information conveyed in the SDP.

The UE shall include an Accept header in the request with "application/sdp" and "text/xml".

7.1.2.3   Media setup procedure

On sending a SETUP request, the UE shall populate the header fields as follows:

- RTSP URL header shall be set to the a=control parameter if present in the answer to the DESCRIBE sent by the MCF. If not present, RTSP URL shall be set to the corresponding media RTSP URL which has been obtained from the SSF data, or from the CoD session initiation. If a domain address is used in the RTSP URL the UE shall not perform DNS lookup. The IP header for the RTSP SETUP message shall be set to the IP address from the connection line ("c=") in the SDP answer and the port from the media line ("m=").

- CSeq header shall be generated by the UE.

On receiving a RTSP 200 OK response to the SETUP request, the UE shall retrieve and store the Session header for issuing the PLAY request later.

7.1.2.4   Media playback initiation procedure

After SETUP request has been acknowledged as successful, UE shall start the playback of the content by sending an RTSP PLAY request.

The UE shall populate the header fields as follows:

- RTSP URL header shall be set to the a=control parameter if present in the answer to the DESCRIBE sent by the MCF. If not present, RTSP URL shall be set to the corresponding media RTSP URL which has been obtained from the SSF data, or from the CoD session initiation. If a domain address is used in the RTSP URL the UE shall not perform DNS lookup. The IP header for the RTSP SETUP message shall be set to the IP address from the connection line ("c=") in the SDP answer and the port from the media line ("m=").

- CSeq header shall be generated by the UE.

- Session header shall be set to the same value as that in the SETUP request.

- If Range header was present in the DESCRIBE response, then the UE shall use it. Otherwise, the UE may include a Range header. If Range header is not sent by the UE, the stream will play from the beginning.

7.1.2.5   Media playback modification procedure

Upon a request to modify playback the UE shall send an RTSP PLAY message with a request to modify the position, speed and/or direction of playback. The UE changes the direction and/or speed of playback by including a `Scale` header or change the position of playback by including a `Range` header.

The UE shall populate the header fields conforming to clause 7.1.2.4 with the following additions:

- Range header is optional.

- Scale header is optional: it is set as follows:

    - 1 indicates normal play.

    - If not 1, the value corresponds to the rate with respect to normal viewing rate.

    - A negative value indicates reverse direction.

If the request is to pause playback, the UE shall send an RTSP PAUSE message.

On sending a PAUSE request, the UE shall populate the header fields as follows:

- RTSP URL header shall be set to the same value as that in the previous PLAY request.

- CSeq header shall be set to the same value as that in the previous PLAY request.

- Session header shall be set to the same value as that in the PLAY request.

7.1.2.6   Media teardown procedure

On sending TEARDOWN request, the UE shall populate the header fields as follows:

- RTSP URL header shall be set to the a=control parameter if present in the answer to the DESCRIBE sent by the MCF. If not present, RTSP URL shall be set to the corresponding media RTSP URL which has been obtained from the SSF data, or from the CoD session initiation. If a domain address is used in the RTSP URL the UE shall not perform DNS lookup. The IP header for the RTSP SETUP message shall be set to the IP address from the connection line ("c=") in the SDP answer and the port from the media line ("m=").

- CSeq header shall be generated by the UE.

- Session header shall be set to the same value as that in the SETUP request.

7.1.2.7   Handling of media events

Upon the reception of the RTSP ANNOUNCE with indication of end-of-stream the UE may take relevant actions to handle the end of stream event (e.g. Terminating session, rewinding the media stream etc.). The UE shall respond with a RTSP 200 OK.

In case of BC sessions with trick-play, if the UE receives an RTSP ANNOUNCE request with an end-of-stream indication, the UE may initiate a session modification procedure in order to go back to a normal BC session in multicast mode or may alternatively take other actions (e.g. rewind, pause, terminate session, etc.).

If the UE does not understand any of the headers or the notice-code value in the ANNOUNCE request, it simply shall ignore the request.

7.2   Media Control Function (MCF)

7.2.1   Procedures for RTSP playback control (Method 1)

7.2.1.1   Introduction

The MCF shall support the following RTSP methods for RTSP playback control:

- PLAY (UE to MCF).

- PAUSE (UE to MCF).

- GET_PARAMETER (UE to MCF).

- SET_PARAMETER (UE to MCF).

- ANNOUNCE (MCF to UE).

- OPTION (UE to MCF).

All other methods that the MCF does not support will result in "405 Method not allowed" reply from the MCF.

The methods shall use the same session id as specified in the SDP h-session attribute.

7.2.1.2   Media Playback Initiation Procedure

Upon successful RTSP PLAY request the MCF responds with a RTSP 200 OK message except for the cases as follows:

- If the requested content is not ready for playing, the MCF shall reply with an RTSP error code 404 Not Found.

The contents of the RTSP 200 OK response shall be as follows:

- CSeq shall be set to the same value as that in the request.

- Date header may be generated by the MCF. It represents the date and time at which the message was originated.

- RTP-Info header may be generated by the MCF when the media packets are transported over the RTP layer. It indicates the RTP-specific parameters. The parameters url and rtptime shall be present. The parameter seq is recommended to be present. For non-MPEG2TS streams, the UE uses the parameter rtptime to calculate the mapping of RTP timestamp to NPT, and the UE may also use the parameter rtptime for inter-media synchronization.

7.2.1.3   Media playback modification procedure

Upon successful RTSP PLAY or PAUSE request the MCF responds with a RTSP 200 OK message.

The contents of the RTSP 200 OK response shall be as follows:

- CSeq shall be set to the same value as that in the request.

- Date header may be generated by the MCF. It represents the date and time at which the message was originated.

- RTP-Info header may be generated by the MCF when the media packets are transported over the RTP layer. It indicates the RTP-specific parameters. The parameters url and rtptime shall be present. The parameter seq is recommended to be present. For non-MPEG2TS streams, the UE uses the parameter rtptime to calculate the mapping of RTP timestamp to NPT, and the UE may also use the parameter rtptime for inter-media synchronization.

7.2.1.4   Media playback information retrieval and setting procedure

Upon successful RTSP GET_PARAMETER or SET_PARAMETER request the MCF responds with a RTSP 200 OK message with the requested values or with the successful setting of a parameter.

7.2.1.5   Handling of media events

Upon receipt of the end-of-stream indication from MDF, MCF may send an RTSP ANNOUNCE to the UE with an indication that the end-of-stream has been reached.

The "Notice" header shall be included with the notice code value set to "2101 End-of-Stream Reached".

> NOTE: The header and code are based draft-stiemerling-rtsp-announce-01 [i.6]. The use of other event types is outside the scope of the present document.

7.2.2   Procedure for content control (Method 2)

The MCF shall act as a media server as defined in RFC 2326 [8]. RTSP header fields shall conform to TS 102 034 [3], clause 6.3.2. The MCF shall not redirect the RTSP methods using either the REDIRECT method or Redirection status code (3xx).

> NOTE: It is recommended that the MCF does not perform redirection to avoid misaligning the information conveyed in the SDP. The problem occurs if the redirected ULR differs from the ones conveyed in the SDP connection and media line is that SIP is used for opening proxies and firewalls for the content control and the content delivery paths.

For transport parameters, the ones conveyed over SIP shall always take precedence over the ones conveyed over RTSP.

7.2.2.1   Introduction

After CoD session setup, RTSP as defined in RFC 2326 [8] is used to control media delivery. It includes media setup, media control and media teardown. RTSP header fields shall conform to TS 102 034 [3], clause 6.3.2.

The MCF shall support the following RTSP methods:

- DESCRIBE (UE to MCF).

- SETUP (UE to MCF).

- PLAY (UE to MCF).

- PAUSE (UE to MCF).

- TEARDOWN (UE to MCF).

- ANNOUNCE (MCF to UE).

All other methods that the MCF does not support will result in "405 Method not allowed" reply from the MCF.

7.2.2.2   Media description procedure

Upon successful RTSP DESCRIBE request the MCF responds with a RTSP 200 OK message.

The DESCRIBE response sent by the MCF shall have:

- Content-type header set to "application/sdp", or

- Content-type header set to "text/xml" and Content-encoding set to "utf8", conforming to TS 102 034 [3], clause 6.3.1.2.

7.2.2.3   Media setup procedure

Upon successful RTSP SETUP request the MCF responds with a RTSP 200 OK message.

The contents of RTSP 200 OK response shall be as follows:

-    CSeq shall be set to the same value as that in the SETUP request.

-    Date header may be generated by the MCF. It represents the date and time at which the message was originated.

-    Session header is generated by the MCF.

-    Transport header contains the transport parameters selected by the MCF.

7.2.2.4   Media playback initiationcontrol procedure

Upon successful RTSP PLAY request the MCF responds with a RTSP 200 OK message.

The contents of the RTSP 200 OK response shall be as follows:

-    CSeq shall be set to the same value as that in the request.

-    Date header may be generated by the MCF. It represents the date and time at which the message was originated.

-    RTP-Info header may be generated by the MCF when the media packets are transported over the RTP layer. It indicates the RTP-specific parameters. The parameters url and rtptime shall be present. The parameter seq is recommended to be present. For non-MPEG2TS streams, the UE uses the parameter rtptime to calculate the mapping of RTP timestamp to NPT, and the UE may also use the parameter rtptime for inter-media synchronization.

7.2.2.5   Media playback modification procedure

Upon successful RTSP control (PLAY, PAUSE) request the MCF responds with a RTSP 200 OK message.

The contents of the RTSP 200 OK response shall be as follows:

-    CSeq shall be set to the same value as that in the request.

-    Date header may be generated by the MCF. It represents the date and time at which the message was originated.

-    RTP-Info header may be generated by the MCF when the media packets are transported over the RTP layer. It indicates the RTP-specific parameters. The parameters url and rtptime shall be present. The parameter seq is recommended to be present. For non-MPEG2TS streams, the UE uses the parameter rtptime to calculate the mapping of RTP timestamp to NPT, and the UE may also use the parameter rtptime for inter-media synchronization.

7.2.2.6   Media teardown procedure

Upon successful RTSP TEARDOWN request the MCF responds with a RTSP 200 OK message.

The contents of RTSP 200 OK response shall be as follows:

-    CSeq shall be set to the same value as that in the TEARDOWN request.

7.2.2.7   Handling of media events

Upon receipt of the end-of-stream indication from MDF, MCF shall send an RTSP ANNOUNCE to the UE with an indication that the end-of-stream has been reached.

The "Notice" header shall be included with the notice code value set to "2101 End-of-Stream Reached".

NOTE: The header and code are based draft-stiemerling-rtsp-announce-01 [i.6]. The use of other event types is outside scope of release 2.

8   Procedures using IGMP/MLD for IMS-based IPTV

8.1   User Equipment (UE)

If IPv4 is used for the transport, the UE shall support IGMPv3 as described in RFC 3376 [28].

If IPv6 is used for the transport, the UE shall support MLDv2 as described in RFC 3810 [29].

Backward compatibility rules between the UE and the Transport Function have to be done conforming to RFC 3376 [28], clause 7 and RFC 3810 [29], clause 8.

8.1.1   Procedure for service selection

8.1.1.1   Procedure to start receiving service selection information

When the UE wishes to receive service selection information from the SSF in multicast mode, it shall send an IGMPv3 unsolicited Membership Report or a MLDv2 Multicast Listener Report Message to the Access Node as specified in RFC 3376 [28] and RFC 3810 [29].

The IGMPv3/MLDv2 request shall be populated as follows:

- the type shall be set to 0x22 "v3 Membership Report" in case of IGMPv3 or to 143 "Version 2 Multicast Listener Report" in case of MLDv2;

- in case of IGMPv3, the value of "Number of Group Records" is set to the number of group records present in the request. In case of MLDv2, the value of "Number of Multicast Address Records" is set to the number of multicast address records present in the request;

- the Group/Multicast Address Records shall be set as follows:

  - "Multicast Address" shall be set to the "Push@MulticastAddress" as specified in the XML document sent by the SDF.

  - In case one or more "Push@SourceAddress" elements are present in the XML document sent by the SDF, then:

    - "Record Type" shall be set to ALLOW_NEW_SOURCES with INCLUDE filter mode:

      - the value of "Number of Sources" is set to the number of source addresses present in the group record, i.e. number of "Push@SourceAddress" elements;

      - the "Source Address" fields shall be set to the "Push@SourceAddress" elements.

  - In case no "Push@SourceAddress" element is present in the XML document sent by the SDF (i.e. source address filtering is not used):

    - "Record Type" shall be set to CHANGE_TO_EXCLUDE_MODE with no "Source Address" fields.

The case when the UE has to use IGMP v2 for compatibility reason (i.e. the network does not support IGMPv3), the UE shall send v2 Membership report, set as follow:

- the type shall be set to 0x16 "v2 Membership Report";

- the Max response time shall be set to 0;

- the Group Address shall be set to the "Push@MulticastAddress" element as specified in the XML document sent by the SDF.

To cover the possibility of the initial Membership Report or Multicast Listener Report being lost or damaged, the UE may resend the request once or twice after short delays. If the UE does not receive service selection data as a result of sending these requests, it shall assume that the data are not available and shall stop attempting to join the multicast group.

8.1.1.2   Procedure to stop receiving service selection information

When the UE wants to stop receiving service selection information from an SSF in multicast mode, it shall send an IGMP v3 Membership Report Message or MLD v2 Multicast Listener Report Message for leaving a multicast group.

The IGMPv3/MLDv2 request shall be populated as follows:

- the type shall be set to 0x22 "v3 Membership Report" in case of IGMPv3 or to 143 "Version 2 Multicast Listener Report" in case of MLDv2;

- in case of IGMPv3, the value of "Number of Group Records" is set to the number of group records present in the request. In case of MLDv2, the value of "Number of Multicast Address Records" is set to the number of multicast address records present in the request;

- the Group/Multicast Address Records shall be set as follows:

  - "Multicast Address" shall be set to the "Push@MulticastAddress" as specified in the XML document sent by the SDF related to the service selection information that the user does not want to receive anymore.

  - In case one or more "Source Address" fields were set in the Join Operation, the same source address list shall be excluded from the listening interface: The "Record Type" shall be set to "BLOCK_OLD_SOURCES" and the "Source Address" fields shall be set to the source list being filtered.

  - In case no "Source Address" fields were set in the Join Operation, The "Record Type" shall be set to "CHANGE_TO_INCLUDE_MODE" with an empty source list.

The case when the UE has to use IGMP v2 for compatibility reason (i.e. the network does not support IGMPv3), the UE shall send v2 Leave, set as follow:

- the type shall be set to 0x17 "Leave Group";

- the Max response time shall be set to 0;

- the Group Address shall be set to the "Push@MulticastAddress" element as specified in the XML document sent by the SDF.

8.1.2   Procedure for BC service

8.1.2.1   Procedure for joining a BC service

After the BC session initiation procedure, when the UE wishes to join a particular BC service, an IGMP unsolicited v3 Membership Report or a MLD v2 Multicast Listener Report Message to the Access Node as specified in RFC 3376 [28] and RFC 3810 [29].

The IGMPv3/MLDv2 request shall be populated as follows:

- the type shall be set to 0x22 "v3 Membership Report" in case of IGMPv3 or to 143 "Version 2 Multicast Listener Report" in case of MLDv2;

- in case of IGMPv3, the value of "Number of Group Records" is set to the number of group records present in the request. In case of MLDv2, the value of "Number of Multicast Address Records" is set to the number of multicast address records present in the request;

- the Group/Multicast Address Records shall be set as follows:

  - "Multicast Address", as obtained from the SSF, shall be set to one of the allowed channels according to the session initiation.

- In case one or more source address elements are present in network parameters received during the BC session initiation procedure or received from the SSF, then:

  ▪ "Record Type" shall be set to ALLOW_NEW_SOURCES with INCLUDE filter mode:

    - the value of "Number of Sources" is set to the number of source addresses present in the group record;

    - the "Source Address" fields shall be set to the source address elements received during the BC session initiation procedure or received from the SSF.

- In case no source address elements are present in network parameters received during the BC session initiation procedure or received from the SSF, (i.e. source address filtering is not used):

  ▪ "Record Type" shall be set to CHANGE_TO_EXCLUDE_MODE with no "Source Address" fields.

The case when the UE has to use IGMP v2 for compatibility reason (i.e. the network does not support IGMPv3), the UE shall send v2 Membership report, set as follow:

- the type shall be set to 0x16 "v2 Membership Report";

- the Max response time shall be set to 0;

- the Group Address shall be set to the multicast address, as obtained from the SSF. It must be one of the allowed channels according to the session initiation.

To cover the possibility of the initial Membership Report or Multicast Listener Report being lost or damaged, the UE may resend the request once or twice after short delays. If after these attempts no BC media received, and an IGMP v3 Membership Report was sent, the UE shall revert to an IGMP v2 Multicast Listener Report and repeat the above procedure. If the UE does not receive BC media data as a result of sending these requests, it shall assume that the data is not available and shall stop attempting to join the multicast group.

8.1.2.2   Procedure for leaving BC service

When the UE wants to stops receiving content delivery data from the previously selected BC service, it shall send an IGMPv3 Membership Report Message or MLDv2 Multicast Listener Report Message for leaving a multicast group.

The IGMPv3/MLDv2 request shall be populated as follows:

- the type shall be set to 0x22 "v3 Membership Report" in case of IGMPv3 or to 143 "Version 2 Multicast Listener Report" in case of MLDv2;

- in case of IGMPv3, the value of "Number of Group Records" is set to the number of group records present in the request. In case of MLDv2, the value of "Number of Multicast Address Records" is set to the number of multicast address records present in the request;

- the Group/Multicast Address Records shall be set as follows:

  - "Multicast Address" shall be set to the multicast address of the BC service that the user does not want to receive anymore.

  - In case one or more "Source Address" fields were set in the Join Operation, the same source address list shall be excluded from the listening interface: The "Record Type" shall be set to "BLOCK_OLD_SOURCES" and the "Source Address" fields shall be set to the source list being filtered.

  - In case no "Source Address" fields were set in the Join Operation, The "Record Type" shall be set to "CHANGE_TO_INCLUDE_MODE" with an empty source list.

The case when the UE has to use IGMP v2 for compatibility reason (i.e. the network does not support IGMPv3), the UE shall send v2 Leave, set as follow:

- the type shall be set to 0x17 "Leave Group";

- the Max response time shall be set to 0;

- the Group Address shall be set to the multicast address of the BC service the UE wants to leave.

8.2   Transport Functions

For IPv4 multicast IPTV service distribution, the network transport functions shall support minimally IGMPv2 or higher. The use of IGMPv3 is recommended, in which case the backwards compatibility rules of RFC 3376 [28], clause 7 shall apply.

For IPv6 multicast IPTV service distribution, the network transport functions shall support minimally MLDv1 or higher. The use of MLDv2 is recommended, in which case the backwards compatibility rules of RFC 3810 [29], clause 8 shall apply.

8.2.1   Receiving IGMP/MLD request corresponding to a join operation

When receiving an IGMP/MLD request corresponding to a join, the ECF/EFF shall check, based on traffic policies, whether the sender of the request is allowed to join the targeted multicast group. If the multicast group is not allowed the ECF/EFF shall ignore the UE request. If the multicast group is allowed, the ECF/EFF may also check whether the resource level specified in the installed policy matches the resource level required by the requested multicast group. In case of a mismatch, the ECF/EFF node may request a new policy by querying the RACS. If fails no new policy is received or the new policy still does not match the request, the ECF/EFF shall ignore the UE request.

Traffic policies may be pre-configured in the ECF/EFF, received from the RACS when the UE attaches to the network (i.e. RACS push model), received from the RACS as a result of an IMS session being established (i.e. RACS push model) or received from the RACS in response to a query from the ECF/EFF (i.e. RACS pull model). Information received from the RACS takes precedence over pre-configured policies. Traffic policies supporting the decisions to forward traffic and traffic policies supporting admission control may be received using the same or different means. Whether the ECF/EFF queries the RACS depend on local policy rules and on the targeted multicast group. The ECF/EFF queries the RACS, by sending a DIAMETER CCR command as defined in TS 183 060 [38].

If the targeted multicast group is allowed and the resource reservation procedure is successful the ECF/EFF shall register the UE IP address as member of this multicast group and begin to forward content delivery data to the UE, when available.

If the ECF/EFF does not receive content delivery data from this multicast group yet, it shall subscribe to it.

8.2.2   Receiving IGMP/MLD request corresponding to a leave operation

When Receiving IGMP/MLD request corresponding to a leave operation, the ECF/EFF shall stop forwarding data to the UE corresponding to the multicast group indicated in the Leave operation and delete the subscription of the UE IP address to this group. If pull model is used, the ECF/EFF shall inform the RACS of the Leave operation to make the resources available to other services by sending a DIAMETER CCR command as defined in TS 183 060 [38].

9   Procedures using DVBSTP for IMS-based IPTV

This clause applies when using DVB-IPTV multicast delivery for service and content guide discovery.

9.1   User Equipment (UE)

9.1.1   Procedure for service selection

9.1.1.1   Request of DVB service discovery and selection data

In the DVB push model of multicast delivery of DVB SD&S data, the UE shall subscribe to the multicast DVBSTP streams identified within the response from the SDF. Refer to clause 8 for multicast connection mechanism.

9.1.1.2   Request of DVB broadband content guide

In the DVB push model of multicast delivery of a DVB BCG data, the UE shall subscribe-to the multicast DVBSTP streams identified within the response from the SDF or within the Service Selection information returned by the SSF. Refer to clause 8 for multicast connection mechanism.

9.1.1.3   Use of service selection information

The UE uses service selection information as defined in clause 6.1.1.5.

9.2   Service Selection Function (SSF)

9.2.1   Procedure for service selection

9.2.1.1   Delivery of DVB service discovery and selection data

In the DVB push model of multicast delivery of DVB SD&S data, the DVBSTP protocol shall be used conforming to TS 102 034 [3], clause 5.4.1.

9.2.1.2   Delivery of DVB broadband content guide

In the DVB push model of multicast delivery of a DVB BCG data, the DVBSTP protocol shall be used conforming to TS 102 539 [13], clause 4.1.2.2.1.

10   Procedures using FLUTE for IMS-based IPTV

> NOTE: This clause applies when using OMA BCAST multicast delivery for service provider and guide discovery.

10.1   User Equipment (UE)

10.1.1   Procedure for service selection

10.1.1.1   Request of OMA BCAST service discovery and selection data

In the OMA BCAST push model of multicast delivery of OMA BCAST ESG provider discovery data, the UE shall subscribe to the FLUTE streams identified within the response from the SDF, conforming to clause 9.2 in TS 102 471 [4] and clause 6 of TS 102 472 [5].

10.1.1.2   Request of OMA BCAST service guide

In the OMA BCAST push model of multicast delivery of an OMA BCAST ESG, the UE shall subscribe to the FLUTE streams identified within the response from SDF or within the Service Selection information returned by the SSF, conforming to TS 102 471 [4], clause 8.1, OMA-TS BCAST_DVB_Adaptation-V1_0 [6], clause 6.3.5 and OMA-TS-BCAST_Service_Guide-V1_0, clause 5.4 [5].

10.1.1.3   Use of service selection information

The UE uses service selection information as defined in clause 6.1.1.5.

10.2   Service Selection Function (SSF)

10.2.1   Procedure for service selection

10.2.1.1   Delivery of OMA BCAST service discovery and selection data

In the OMA BCAST push model of multicast delivery of OMA BCAST ESG provider discovery data, the FLUTE
protocol shall be used, conforming to TS 102 471 [4], clause 9.2 and OMA-TS-BCAST_DVB_Adaptation-V1_0,
clause 6.3.5 [6].

10.2.1.2   Delivery of OMA BCAST service guide

In the OMA BCAST push model of multicast delivery of an OMA BCAST ESG, the FLUTE protocol shall be used,
conforming to TS 102 471 [4], clause 8.1, OMA-TS-BCAST_DVB_Adaptation-V1_0 [6], clause 6.3.5 and
OMA-TS-BCAST_Service_Guide-V1_0 [5], clause 5.4.

11   Procedures using UDP/RTP for IMS-based IPTV

The IPTV content is transported over the IP network. In order to do so, several encapsulation are possible:

- MPEG2TS: the content is encapsulated into MPEG2TS packets:

  - MPEG2TS over UDP: the MPEG2TS packets are directly transported over the UDP layer.

  - MPEG2TS over RTP: the MPEG2TS packets are transported over the RTP layer.

- Direct RTP: no MPEG2TS encapsulation is used, the Elementary streams are directly transported over the
  RTP layer.

11.1   User Equipment (UE)

11.1.1   Procedure for real-time transport

The UE shall support at least one of the following transport technologies:

- MPEG2TS encapsulation.

- Direct RTP transport.

11.1.1.1   Transport using MPEG2TS

The UE may be able to receive the content encapsulated in MPEG2TS packets.

When using the MPEG2TS encapsulation technology, the UE shall support both:

- MPEG2TS over UDP conforming to TS 102 034 [3], clause 7.1.2.

- MPEG2TS over RTP conforming to TS 102 034 [3], clause 7.1.1 excluding clause 7.1.1.1.

  - As specified in ES 283 003 [20], it is possible to negotiate RTCP bandwidth - and thus to control UE
    receiver report generation - for unicast IPTV services during SIP session setup.

NOTE 1: Handling of RTCP Receiver reports for BC services is out of scope of the present document.

NOTE 2: The default behaviour in case that - for m-lines indicating RTP/RTCP usage - no RTCP bandwidth
             negotiation is performed, is described in ES 283 003 [20].

11.1.1.2 Transport using direct RTP encapsulation

The UE may be able to receive the content directly over the RTP layer (e.g. H264 over RTP).

As specified in ES 283 003 [20], it is possible to negotiate RTCP bandwidth - and thus to control UE receiver report generation - for unicast IPTV services during SIP session setup.

NOTE 1: Handling of RTCP Receiver reports for BC services is out of scope of the present document.

NOTE 2: The default behaviour in case that - for m-lines indicating RTP/RTCP usage - no RTCP bandwidth negotiation is performed, is described in ES 283 003 [20].

11.1.2 Procedure for real-time transport eError correction

The UE may support a transport error correction mechanism.

11.1.2.1 Unidirectional transport error correction

When unidirectional transport error correction is used, the UE shall be able to receive an application Layer FEC, conforming to TS 102 034 [3], annex E.

NOTE: Only the base layer of the DVB-IP AL-FEC is supported in the present document, the enhancement layer support is out of scope.

11.2 Media Delivery Function (MDF)

11.2.1 Procedure for real-time transport

The MDF shall send the content using one of the following transport technologies:

- MPEG2TS encapsulation.

- Direct RTP transport.

11.2.1.1 Transport using MPEG2TS

The MDF may be able to send the content encapsulated into MPEG2-TS.In that case, one of the following shall be used:

- The transport of the IPTV content within MPEG2TS layer over RTP shall be done conforming to TS 102 034 [3], clause 7.1.1.

- The transport of the IPTV content within MPEG2TS layer over UDP shall be done conforming to TS 102 034 [3], clause 7.1.2.

11.2.1.2 Transport using direct RTP encapsulation

The MDF may be able to send the content directly over the RTP layer (e.g. H264 over RTP).

11.2.2 Procedure for real-time transport error correction

The MDF may support a transport error correction mechanism.

11.2.2.1 Unidirectional transport error correction

For unidirectional transport error correction the MDF shall use an application Layer FEC mechanism, conforming to TS 102 034 [3], annex E.

NOTE: Only the base layer of the DVB-IP AL-FEC is supported in the present document, the enhancement layer support is out of scope.

12   IPTV user profile schema

The IPTV user profile is described by an XML document. This XML document complies with the XML schema defined in annex C.

Although it is not explicit in the XML schema described in annex C, the IPTV user profile must comprise at least one BC profile or CoD profile.

The "Global Settings" element is set to "optional" in the IPTV user profile. However, in the case where this element would not be provided, default values should be used:

- the User Action Recordable Boolean should be assumed to be set to "false";

- the preferred language value should be assumed to be to one that is globally defined by the service provider (hence applicable to all users).

In the case where the ParentalControlLevel is not provided, its value is assumed to be the default level defined by the service provider (hence applicable to all users).

In the case where the quality definition is not provided, its default value shall be "SD".

13   IPTV service action data schema

For convenience purposes, each object class of the IPTV service action data is described by a separate XML documents. Those XML document comply with the XML schema defined in annex D.

Although they are defined as optional in the XML schema described for "NPVR items" in annex D, the "BCServiceId", "RecordStartDate" and "RecordEndDate" attributes are required in the case where the NPVRContentID attribute does not refer to a Programme Id (i.e. an entry in the EPG).

Bookmark and RecordStartDate attributes shall either take the form of an xs:dateTime type, or be equal to "NOW".

Annex A (informative):
Functional entity relations and example signalling flows of IMS based IPTV operations

A.1   Functional entities relations and overview of the IMS based IPTV procedures

NOTE 1:   Figure A.1 represents relationships and protocols between the functional entities at high level. The details of corresponding procedures and signalling flows are in the following clauses of this annex.

NOTE 2:   As described in TS 182 027 [2], clause 6.4 and 6.5, Xc and Xd are logical reference points that can be decomposed of Dj and possibly Di, Ds or Iz reference points depending on the location of the MCF or MDF.

Figure A.1: IMS based IPTV - protocol model with FE relation

0)   First of all it is needed to start or boot an UE (like a set-top-box, PC, mobile or any device with an IPTV client) and achieve network attachment to obtain network parameters (like an IP address, P-CSCF address, etc.).

1)   After network attachment the UE initiate the IMS registration process with core IMS (as described in clause 5.1.1).

2)   UE will perform IPTV service attachment functions including SIP based service discovery to perform SDF tasks (as described in clause 5.1.2).

3)   Then UE is able to initiate the service selection procedures with SSF via Xa (using HTTP over Xa as described in clause 6.1.1, using DVBSTP as in clause 9 or FLUTE 10) to receive service selection information.

4)   The IMS based IPTV UE needs to know and used received service selection information to establish appropriate multimedia session by generating SIP INVITE messages during service initiation procedure (over Gm towards home C-CSCF) send via IMS core to SCF.

NOTE 1:   SIP based request for service initiation (SIP procedures is applicable also for service termination or termination) is used for BC service (as in clause 5.1.3), CoD service (as in clause 5.1.4) or for NPVR Service (as in clause 5.1.7).

NOTE 2:   The core IMS is able to initiate resource reservation process for network resources needed by the IPTV streams according to the capabilities of the UE. The resource reservation and allocation is performed using standardized transport control functions of NGN RACS connected to the core IMS.

5) to 6)   After the successful session initiation, the SCF informs the MCF via core IMS and y2 interface (or UE in some case like BC) about identification of selected content from the Media Delivery Function (or ECF/EFF in case of BC services) to initiate start streaming the selected multimedia content (CoD, nPVR).

7)   The UE may control CoD media stream over the Xc (see note 2 for figure A.1) interface (between the UE and the MCF) to control media delivery with RTSP protocol (as in clause 7). The UE may control BC media stream over the Dj interface (between the UE and the ECF/EFF) to control media delivery with IGMP/MLD protocol (as in clause 8).

8)   The MDF performs media delivery over the Xd (see note 2 for figure A.1) interface is based on UDP/RTP stream delivery and several transport variants (as described in clause 11).

A.2   Example signalling flows of service discovery operation

A.2.1   Push mode

This clause describes an example of signalling flow of the service discovery based on the Push mode.
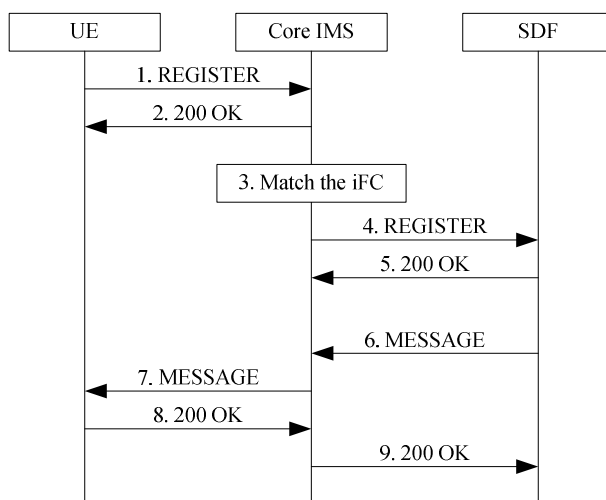
Figure A.2: Service discovery of Push mode operation

1)   The UE sends a REGISTER request to the Core IMS.

2)   Core IMS finishes the registration, and send the SIP 200 OK to the UE.

3)   Core IMS matches the iFC of the service profile belong to the user, and finds out the SDF that user has subscribed.

4)   Core IMS sends the third-party REGISTER request to the SDF.

5)   The SDF acquires the register status of the UE, and sends the SIP 200 OK to the Core IMS.

6)   The SDF sends the Service Attachment Information to the UE by the SIP MESSAGE request. The SDF could trigger service discovery logic, and configure the appropriate service attachment information for the user. Here the SDF could retrieve the user's location, UE's capability etc from IPTV user profile. for configure the service attachment information.

7)   The Core IMS relays the SIP MESSAGE to the UE.

8)   The UE receives the SIP MESSAGE with Service Attachment Information, and sends the SIP 200 OK to the SDF.

9)   The Core IMS relays the SIP 200 OK to the SDF.

A.2.2   Pull Mode

This clause describes an example of signalling flow of the service discovery based on the Pull mode.
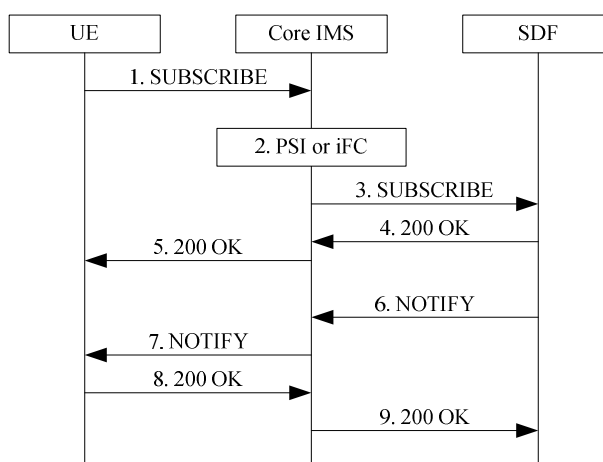
NOTE: The UE may retrieve the PSI/address of the SDF based on mechanisms defined in annex I.

Figure A.3: Service discovery of Pull mode operation

1)   The UE sends a SUBSCRIBE request to the Core IMS. The SUBSCRIBE could also contain a body to carry the UE's capabilities.

2) to 3) The Core IMS forwards the SUBSCRIBE to the SDF. The Core IMS could forwards the SUBSCRIBE based on the PSI or iFC.

4)   In case of the successful subscription, the SDF generates a SIP 200 OK in response to the SUBSCRIBE. When the SUBSCRIBE carry the UE's capabilities in the message body, the SDF examines and records UE capabilities information as part of the IPTV user profile data.

5)   The Core IMS relays the SIP 200 OK to the UE.

6)   The SDF generates the NOTIFY for the service attachment information. The SDF could retrieve the UE's capabilities to generate the personalized service attachment information.

7)   The Core IMS relays the NOTIFY to the UE.

8)   The UE receives the NOTIFY with the service attachment information, and sends the SIP 200 OK to the SDF.

9)   The Core IMS relays the SIP 200 OK to the SDF.

A.3 Example signalling flows of CoD operation

A.3.1 Session initiation

NOTE: As stated in TS 182 027 [2], the SCF may originate requests to the MF without involving the core-IMS.

A.3.1.1 Session initiation flows for case of establishing content control channel and content delivery channels separately

UE | RACS | Core-IMS | CoD-SCF | CoD-MF

content selection

1. INVITE
2. Resource Reservation
3. INVITE
4. select CoD-MCF
5. INVITE
6. INVITE
7. 200 OK
8. 200 OK
9. 200 OK
10. Resource Commit
11. 200 OK
12. ACK
13. ACK
14. ACK
15. ACK
16. Establish TCP Connection for RTSP
17. DESCRIBE
18. 200 OK
19. Extract SDP information
20. SETUP
21. 200 OK
22. re-INVITE
23. Resource Reservation
24. re-INVITE
25. re-INVITE
26. re-INVITE
27. 200 OK
28. 200 OK
29. 200 OK
30. Resource Commit
31. 200 OK
32. ACK
33. ACK
34. ACK
35. ACK
36. PLAY
37. 200 OK
38. Content stream(s)

NOTE 1: The procedure and flow between the CoD-MCF and CoD-MDF is out of scope of the current release.
NOTE 2: After successful authorization of the service initiation request, the delivery of the keying data (with security metadata) to the UE may be initiated. This would be done in accordance to the media content protection model for IPTV as described in TS 187 003 [10].

Figure A.4

1) Initial INVITE request to Core-IMS. The INVITE offers a SDP of a media description for RTSP connection.

2) Core-IMS requires for RACS to reserve resources of RTSP connection according to the Initial INVITE.

3) Core-IMS forwards the Initial INVITE to the CoD-SCF.

4) When the CoD-SCF receives the Initial INVITE request from the UE, the CoD-SCF may perform service authorization. The CoD-SCF selects a CoD-MF.

5) to 6) The initial INVITE request is sent to the CoD-MF selected by the CoD-SCF.

7) to 9) SIP 200 OK for Initial INVITE is sent from CoD-MF to the Core-IMS.

10) Core-IMS requires for RACS to commit the reservation.

11) SIP 200 OK response is sent back to the UE.

12) to 15) The UE sends ACK to CoD-MF.

16) A TCP connection for RTSP is established.

17) Since a SIP dialog is established and a TCP connection for RTSP is established, the UE invokes RTSP DESCRIBE request to the CoD-MF through the established TCP connection.

18) The CoD-MF sends SIP 200 OK with SDP. The SDP contains the media descriptions of RTP stream to be used.

19) The UE extracts the media descriptions from the SDP of SIP 200 OK.

20) The UE sends RTSP SETUP requests to the CoD-MF through the established TCP connection.

21) SIP 200 OK for SETUP is sent back to the UE.

22) The UE sends a re-INVITE request to Core-IMS. The SDP of re-INVITE contains as follows:

- The session description and media description for RTSP are same as that of Initial INVITE.

- The media descriptions for RTP content stream(s) are same as the media descriptions of SIP 200 OK (DESCRIBE) except for address, port number, and direction attribute. The address and port number are replaced by that of UE's, and "a=recvonly" direction attribute is inserted.

23) Core-IMS requires for RACS to reserve additional resources of RTP streams according to the re-INVITE.

24) to 26) re-INVITE is sent to CoD-MF.

27) to 29) SIP 200 OK for re-INVITE is sent back to UE.

30) Core-IMS requires for RACS to commit the reservation.

31) SIP 200 OK for re-INVITE is sent back to the UE.

32) to 35) The UE sends ACK to CoD-MF.

36) RTSP PLAY request is sent to the CoD-MF.

37) SIP 200 OK for PLAY is sent back to the UE.

38) The CoD-MF starts sending RTP content streams to the UE.

A.3.1.2　Session initiation flows for case of establishing content control channel and content delivery channels using RTSP method 2
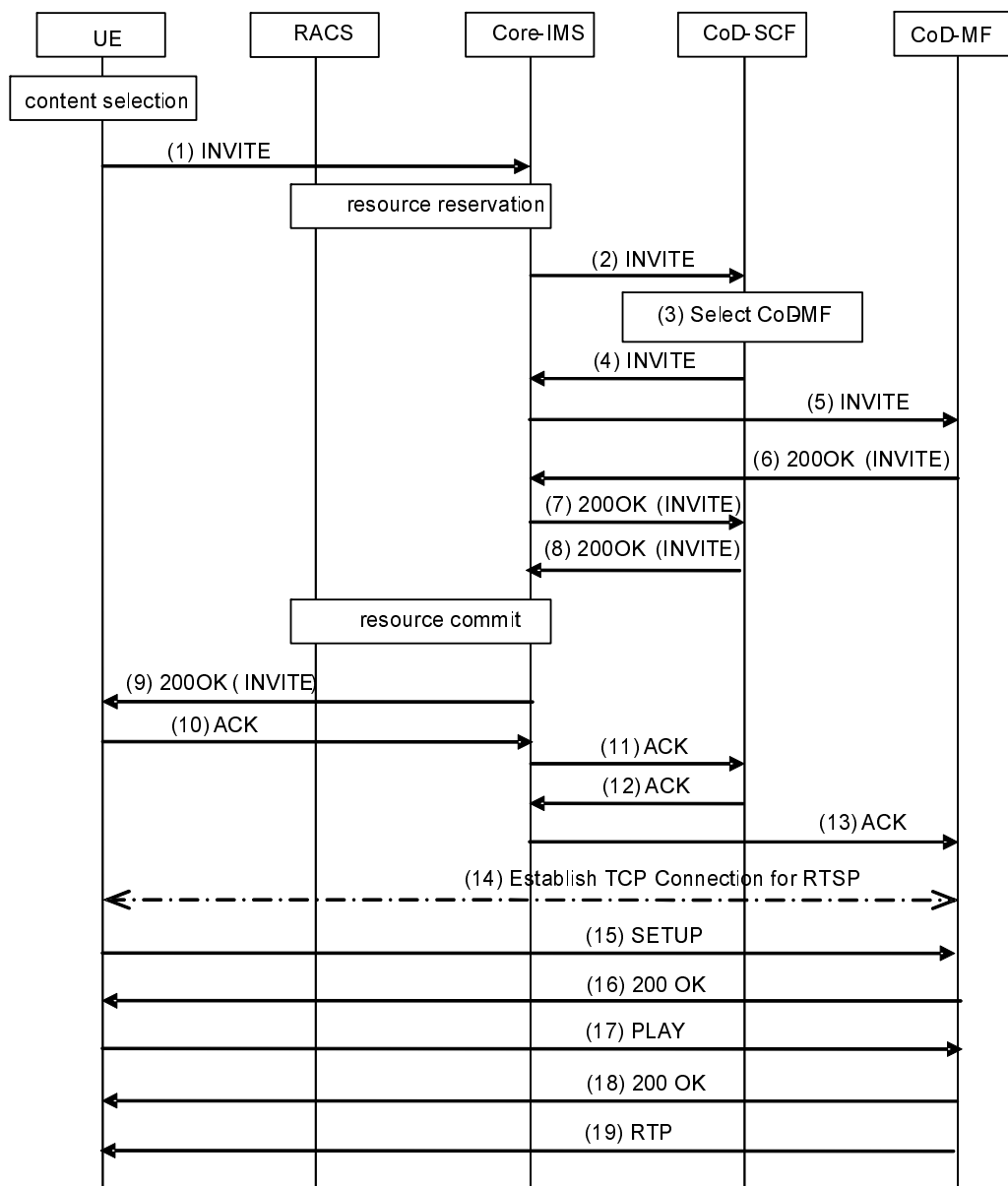
Figure A.5

1) to 2)　　The UE sends the initial SIP INVITE request to the SCF.

3)　　　　The SCF can deny service requests packages depending on operator policy e.g. based on UE location (provided by the NASS), UE capabilities or the User Profile. The SCF selects the appropriate MF.

4) to 5)　　The SCF sends initial SIP INVITE request to the selected MF.

6) to 9)　　SIP 200 OK of initial SIP INVITE is sent back to the UE as for final session agreement.

10) to 13)　SIP ACK is sent back to the MF.

14)　　　　TCP connection for the RTSP content control channel is established between the UE and the MF. The UE detects that the RTSP related SDP data negotiated during the preceding steps. If the RTSP session ID parameter is missing in this SDP, as described in clause 5.1.4.2.1, the UE knows that no RTSP session exists at the MF. Therefore the UE will use RTSP SETUP to trigger RTSP session initiation.

15)　　　　The UE sends an RTSP SETUP request to the MF.

16)   RTSP 200 OK for RTSP SETUP is sent back to the UE. The RTSP network parameters exchanged during
         steps 15 and 16 equal the RTSP network parameters as agreed in steps 1 to 13. If the MF or the UE detect
         deviating parameters they react with appropriate error messages and terminate SIP and RTSP sessions.

17)   RTSP PLAY request is sent to the MF.

18)   RTSP 200 OK for RTSP PLAY is sent back to the UE.

19)   The RTP stream is sent to the client IP address as indicated by SIP SDP and RTSP SETUP.

A.3.2   Session termination
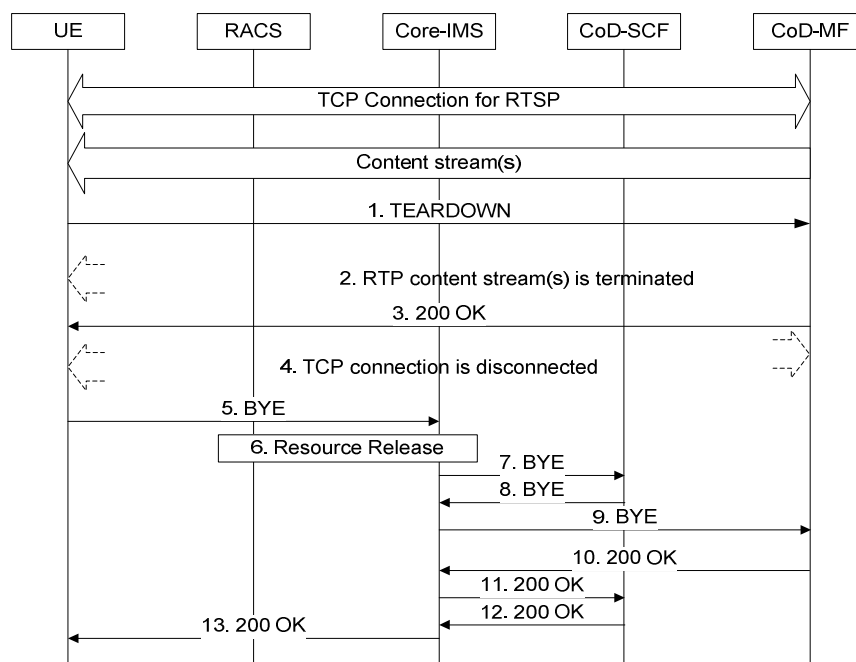
NOTE: The procedure and flow between the CoD-MCF and CoD-MDF is out of scope of the current release.

Figure A.6

1)   TEARDOWN request is sent to CoD-MF.

2)   CoD-MF stops sending RTP content streams.

3)   The CoD-MF responds with RTSP 200 OK response.

4)   The UE disconnects the TCP connection of RTSP.

5)   The UE sends the BYE request towards Core-IMS.

6)   Core-IMS requires for RACS to release resources.

7) to 9)   BYE is sent to CoD-MF.

10) to 13) SIP 200 OK is sent back to the UE.

A.3.3   Session modification

A.3.3.1   Session modification initiated by MF
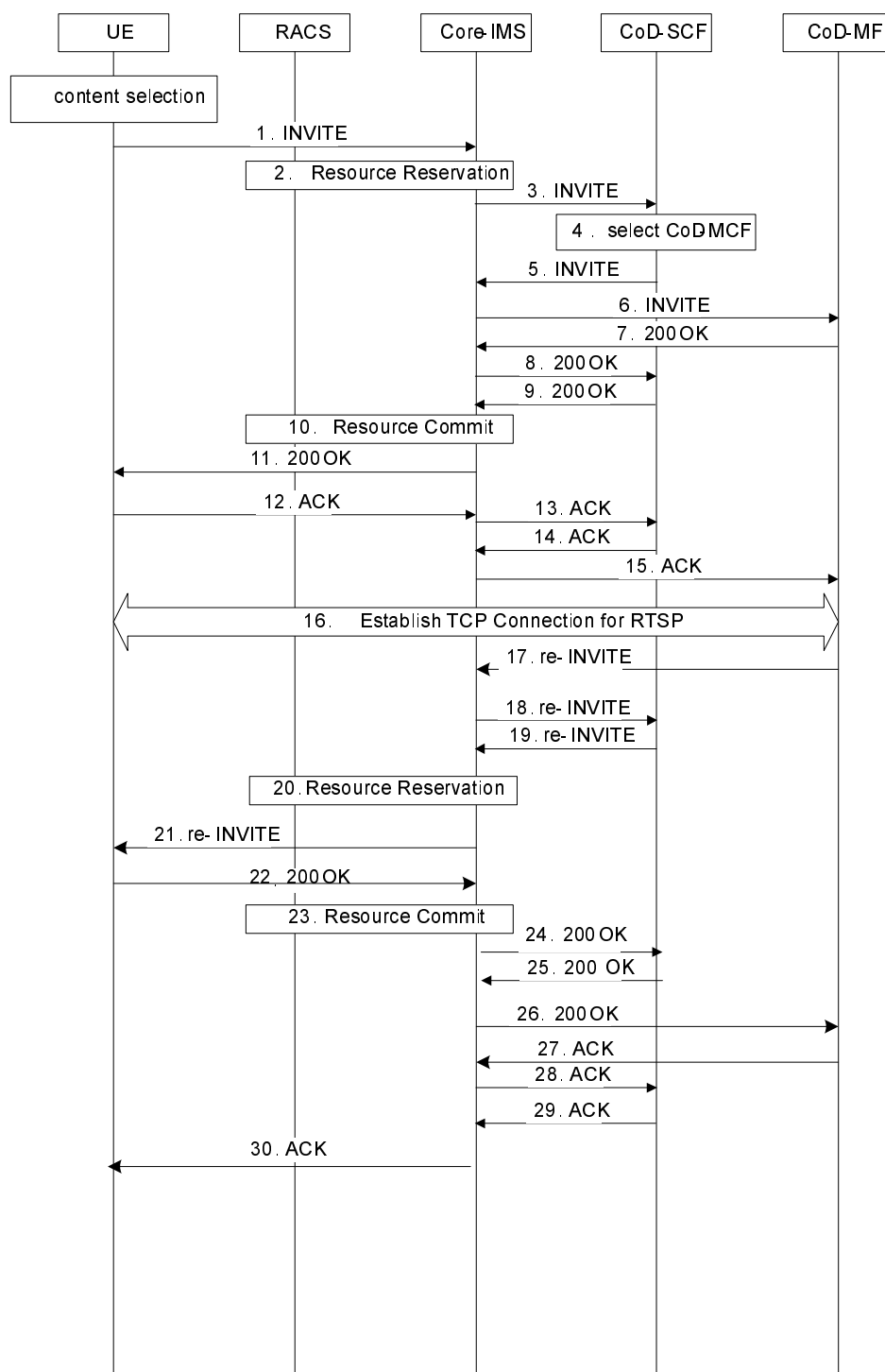
NOTE: The procedure and flow between the CoD-MCF and CoD-MDF is out of scope of the current release.

Figure A.7

1)   Initial INVITE request to Core-IMS. The INVITE offers a SDP of a media description for RTSP
          connection.

2)   Core-IMS requires for RACS to reserve resources of RTSP connection according to the Initial INVITE.

3)   Core-IMS forwards the Initial INVITE to the CoD-SCF.

4)   When the CoD-SCF receives the Initial INVITE request from the UE, the CoD-SCF may perform service authorization. The CoD-SCF selects a CoD-MF.

5) to 6)   The initial INVITE request is sent to the CoD-MF selected by the CoD-SCF.

7) to 9)   SIP 200 OK for Initial INVITE is sent from CoD-MF to the Core-IMS.

10)   Core-IMS requires for RACS to commit the reservation.

11)   SIP 200 OK response is sent back to the UE.

12) to 15) The UE sends ACK to CoD-MF.

16)   A TCP connection for RTSP is established.

17)   The CoD-MF sends a re-INVITE request to Core-IMS to establish the content delivery channel.

18) to 19) The re-INVITE request is routed back to Core-IMS via the CoD-SCF.

20)   Core-IMS requires for RACS to reserve additional resources of RTP streams according to the re-INVITE.

21)   re-INVITE is sent to the UE.

22)   The UE sends SIP 200 OK with SDP. The SDP contains the media descriptions of RTP stream to be used.

23)   Core-IMS requires for RACS to commit the reservation.

24) to 26) SIP 200 OK is sent to the CoD-MF.

27) to 30) The CoD-MF returns ACK to the UE.

A.4   Example signalling flows of BC operation

A.4.1   Session initiation

This clause describes an example of signalling flow of session initiation when the UE retrieves network parameters from the SSF.
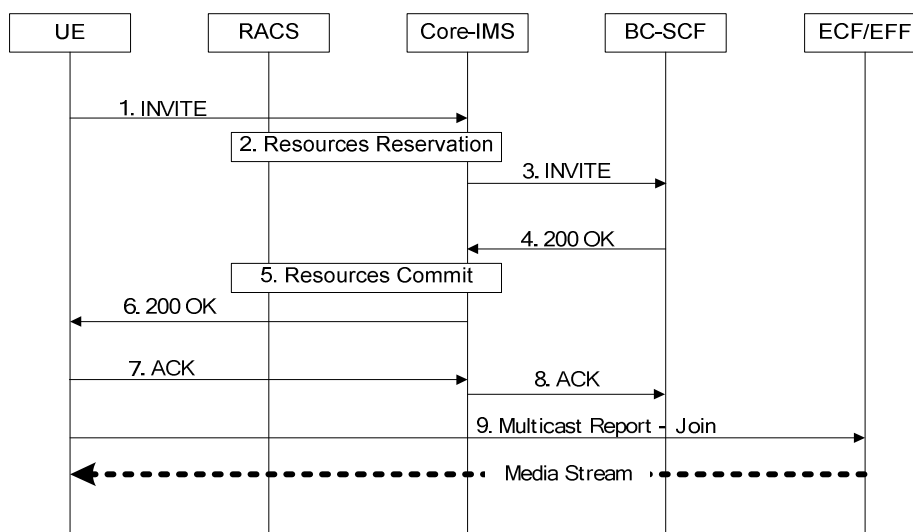
Figure A.8: Session initiation of BC operation

1) The UE initiates BC Service. The SIP INVITE message contains BW requirements for this session and a list of Service packages and multicast addresses to be authorized during the session.

2) Core IMS identifies this is as a BC service session initiation and reserves the resources with RACS.

3) The INVITE message is forwarded to the SCF. The SCF validates the list of requested service packages against the subscriber profile associated with the UE. The SCF may remove some service packages or replace one with a list of multicast addresses.

4) The IPTV application sends the positive result to the IMS core.

5) Core IMS modifies the reservation and aligns it with any modification the SCF made, as described in step 2. Core IMS commits the reservation with RACS.

6) Core IMS forwards the result to the UE.

7) UE sends ACK towards SCF.

8) Core-IMS routes the ACK message to SCF.

9) The UE joins the multicast address indicated in the response.

10) Content is delivered.

NOTE: After successful authorization of the service initiation request, the derivation and delivery of further necessary keying material to the UE may be initiated to enable decryption of BC streams in real time (in accordance to the media content protection model for IPTV as described in TS 187 003 [10]). This can be done statically prior to the content delivery or dynamically during the content delivery.

A.4.2   Session termination

This clause describes an example of signalling flow of session termination.
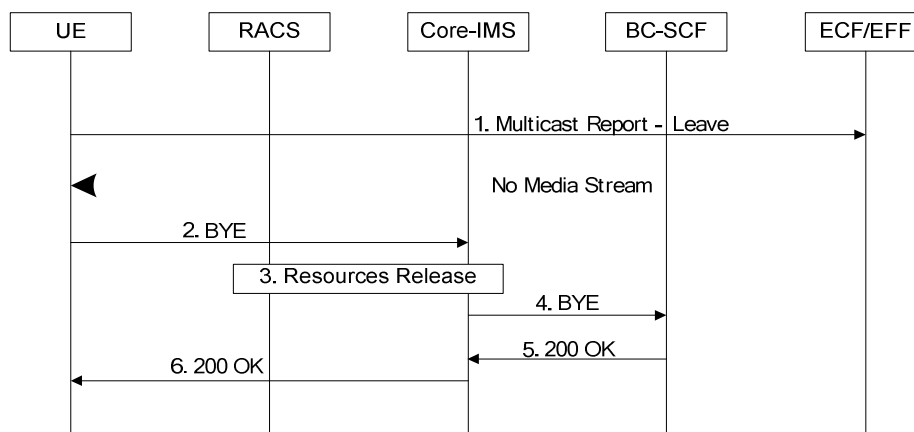
Figure A.9: Session termination of BC operation

1) The UE sends a multicast Leave request (Membership Report Message (IGMP) or Multicast Listener Report Message (MLD)) to stop receiving multicast media stream. The UE populates the message as follows:

  - Multicast Address field is set to the multicast address to be left.

  - If the protocol is IGMPv3 or MLDv2:

    ▪ If source addresses have been set in the Join message, the same source address list is excluded from the listening interface; the Record Type is set to "BLOCK_OLD_SOURCES" and Source list is set to the source address.

     ■ If no source address has been set in the Join message, Filter Change record is set to INCLUDE with an empty source list.

2)   The UE sends a BYE request to Core-IMS.

3)   Core-IMS requires for RACS to release resources.

4)   Core-IMS forwards a BYE to the BC-SCF.

5) to 6) The BC-SCF responds with SIP 200 OK response and the SIP session is terminated.

A.4.3 Channel switching

This clause describes two examples of signalling flow of channel switching.

A.4.3.1 Join after leave
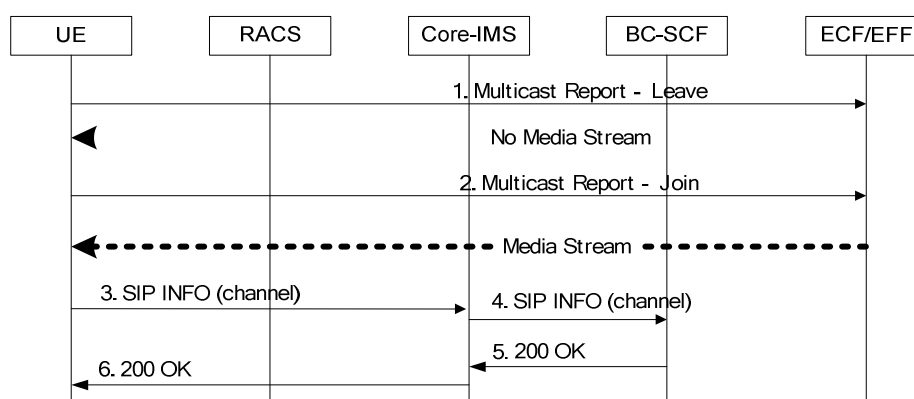
Figure A.10: Changing multicast channels of BC operation (2 messages)

1)   The UE sends a multicast Leave request (Membership Report Message (IGMP) or Multicast Listener Report Message (MLD)) to stop receiving the multicast media stream of the old channel.

2)   The UE sends a multicast Join request (Membership Report Message (IGMP) or Multicast Listener Report Message (MLD)) to start receiving the multicast media stream of the new channel.

3) to 4) If the UE remains on the selected channel for a period of time greater than a preconfigured value (example 10 seconds), the UE may inform the SCF of selected channel.

5) to 6) The SCF replies with a SIP 200 OK.

A.4.3.2 Leave and Join at the same time

If the Transport Function is using IGMPv3 or MLDv2, the UE may choose to send a single IGMP message containing the Leave request and the Join request, for leaving the old channel and joining the new channel. This is depicted in figure A.11.
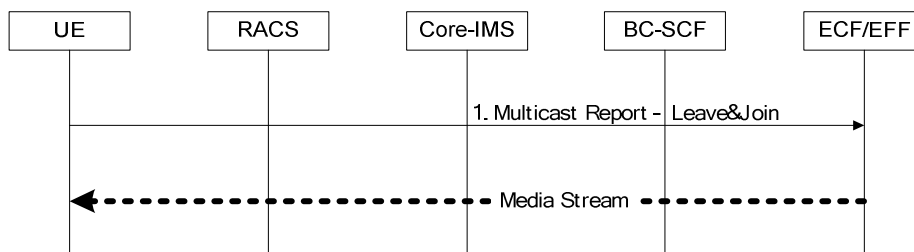
Figure A.11: Changing multicast channels of BC operation (single message)

1)   The UE sends a combined multicast Leave/Join request (Membership Report Message (IGMP) or Multicast
     Listener Report Message (MLD)) to stop receiving the multicast media stream of the old channel and start
     receiving the multicast media stream of the new channel.

Annex B (normative):
IPTV services XCAP application usage

B.1   General

For the purpose of manipulating data stored in an application server the XML Configuration Access Protocol (XCAP) defined in RFC 4825 [9] is used. XCAP allows a client to read, write and modify application configuration data, stored in XML format on a server. XCAP maps XML document sub-trees and element attributes to HTTP URIs, so that these components can be directly accessed by HTTP. XCAP uses the HTTP methods PUT, GET and DELETE to operating on XML documents stored in the server.

In the case of IPTV services, the data stored in a server is related to the execution of that given service. The present document defines a new XCAP Application Usage for the purpose of allowing a client to manipulate data related to IPTV services. This application usage defines the XML schema for the data used by the application, along with other key pieces of information.

XCAP defines two logical roles: XCAP client and XCAP servers. An XCAP client is an HTTP/1.1 compliant client. Similarly an XCAP server is an HTTP/1.1 compliant server. The XCAP server acts as a repository of XML documents that customize and modify the execution of IPTV services.

XCAP focuses on the definition of XML documents that are compliant with the XML schema and constrains defined for a particular XCAP application usage. XCAP allows application to provide XML documents that are common for all users or XML documents that affect the service of a given user.

Central to XCAP is the construction of the HTTP URI that points to particular XML document or certain components of it. A component in an XML document can be an XML element, attribute, or the value of it.

B.2   XCAP application usage

XCAP requires application usages to fulfil a number of steps in the definition of such application usage. The reminder of this clause specifies the required definitions of the IPTV services XCAP Application Usage.

Application Unique ID (AUID): Each XCAP application usage is associated with a unique name called the Application Unique ID (AUID). The AUID defined by this application usage falls into the vendor-proprietary namespace of XCAP AUID, where ETSI is considered a vendor.

The AUID allocated to the NGN IPTV services XCAP application usage is:

<div align="center">

`org.etsi.ngn.iptv`

</div>

XML schema: Implementations in compliance with the present document shall implement the XML schema defined in **annex C**

default namespace: XCAP requires application usages to declare the default namespace. The default namespace of the IPTV services XCAP application usage is:

<div align="center">

`urn:org:etsi:ngn:params:xml:ns:iptv`

</div>

MIME type: The MIME type of IPTV services XML documents is:

<div align="center">

`application/vnd.etsi.iptvprofile+xml`

</div>

validation constraints: The present document does not specify any additional constraint beyond those defined by XCAP.

data semantics: The XML schema does not accept URIs that could be expressed as a relative URI reference causing a resolution problem. However, each of the supplementary services should consider if relative URIs are allowed in the subdocument tree, and in that case, they should indicate how to resolve relative URI references. In the absence of further indications, relative URI references should be resolved using the document URI as the base of the relative URI reference.

naming conventions: By default, NGN IPTV services XML documents are stored under the user's Home Directory (which is located under the "users" sub-tree). In order to facilitate the manipulation of an NGN IPTV services XML document, we define a default XML file name:

<div align="center">

`iptvprofile.xml`

</div>

resource interdependencies: The present document does not specify additional resource interdependency beyond those specified in the XML schema.

authorization policies: The default XCAP authorization policy is used in the application usage defined by the present document.

  NOTE: The default policy indicates that the creator of the XML document is the one that is authorized to manipulate it.

Annex C (normative):
XML Schema for the IPTV profile

This annex specifies an XML schema for creating documents representing instances of the IPTV profile described in TS 182 027 [2]. This XML schema is used when IPTV profile is manipulated with the XCAP procedure described in clauses 6.1.2.1, 6.2.1.2, and annex B.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:uep="urn:org:etsi:ngn:params:xml:ns:iptvueprofile"
elementFormDefault="qualified"
attributeFormDefault="unqualified">

<xs:import namespace="urn:org:etsi:ngn:params:xml:ns:iptvueprofile"
schemaLocation="annexP-XML Schema for UE Profile.xsd"/>


<xs:element name="IPTVProfile">
    <xs:annotation>
        <xs:documentation> XML Schema for representing the IPTV Profile object identified in TS 182
027 clause 7.3.1
        </xs:documentation>
    </xs:annotation>
    <xs:complexType>
        <xs:sequence>
            <xs:element name="UEProfile" type="uep:tUEProfile" minOccurs="0"/>
            <xs:element name="GlobalSettings" type="tGlobalSettings" minOccurs="1"/>
            <xs:element name="BCProfile" type="tBCProfile" minOccurs="0"/>
            <xs:element name="CoDProfile" type="tCoDProfile" minOccurs="0"/>
            <xs:element name="PVRProfile" type="tPVRProfile" minOccurs="0"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ProfileId" type="xs:ID" />
        <xs:anyAttribute/>
    </xs:complexType>
</xs:element>


    <xs:complexType name="tBCProfile">
        <xs:sequence>
            <xs:element name="BCServicePackage" type="tBCServicePackage"
minOccurs="1" maxOccurs="unbounded"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>


    <xs:complexType name="tBCServicePackage">
        <xs:sequence>
            <xs:element name="BCPackageId" type="tBCServicePackageID" minOccurs="1"/>
            <xs:element name="Description" type="tBCServicePackageDescription" minOccurs="0"/>
            <xs:element name="BCService" type="tBCService" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>


    <xs:simpleType name="tBCServicePackageID" final="list restriction">
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="16"/>
        </xs:restriction>
    </xs:simpleType>
```

```xml
<xs:simpleType name="tBCServicePackageDescription" final="list restriction">
    <xs:restriction base="xs:string">
        <xs:minLength value="0"/>
        <xs:maxLength value="64"/>
    </xs:restriction>
</xs:simpleType>


<xs:complexType name="tBCService">
    <xs:sequence>
        <xs:element name="BCServiceId" type="tBCServiceID" minOccurs="1"/>
        <xs:element name="QualityDefinition" type="tQualityDefinition" minOccurs="0"/>
        <xs:element name="Extension" type="tExtension" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>


<xs:simpleType name="tBCServiceID" final="list restriction">
    <xs:restriction base="xs:string">
        <xs:minLength value="0"/>
        <xs:maxLength value="16"/>
    </xs:restriction>
</xs:simpleType>


<xs:simpleType name="tQualityDefinition" final="list restriction">
    <xs:restriction base="xs:unsignedByte">
        <xs:minInclusive value="0"/>
        <xs:maxInclusive value="1"/>
        <xs:enumeration value="0">
            <xs:annotation>
                <xs:documentation>
                    <label xml:lang="en">SD</label>
                    <definition xml:lang="en">Standard Definition</definition>
                </xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="1">
            <xs:annotation>
                <xs:documentation>
                    <label xml:lang="en">HD</label>
                    <definition xml:lang="en">High Definition</definition>
                </xs:documentation>
            </xs:annotation>
        </xs:enumeration>
    </xs:restriction>
</xs:simpleType>


<xs:complexType name="tCoDProfile">
    <xs:sequence>
        <xs:element name="ParentalControl" type="tParentalControlLevel" minOccurs="0"/>
        <xs:element name="Extension" type="tExtension" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>


<xs:simpleType name="tParentalControlLevel" final="list restriction">
    <xs:restriction base="xs:unsignedByte">
        <xs:minInclusive value="0"/>
        <xs:maxInclusive value="3"/>
        <xs:enumeration value="0">
            <xs:annotation>
                <xs:documentation>
                    <label xml:lang="en">ALL</label>
                    <definition xml:lang="en">All contents</definition>
                </xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="1">
            <xs:annotation>
                <xs:documentation>
                    <label xml:lang="en">Level 1</label>
                    <definition xml:lang="en">Level 1 contents</definition>
                </xs:documentation>
            </xs:annotation>
```

```
                </xs:enumeration>
                <xs:enumeration value="2">
                    <xs:annotation>
                        <xs:documentation>
                            <label xml:lang="en">Level 2</label>
                            <definition xml:lang="en">Up to level 2</definition>
                        </xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="3">
                    <xs:annotation>
                        <xs:documentation>
                            <label xml:lang="en">Level 3</label>
                            <definition xml:lang="en">Up to level 3</definition>
                        </xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="4">
                    <xs:annotation>
                        <xs:documentation>
                            <label xml:lang="en">Level 4</label>
                            <definition xml:lang="en">Up to level 4</definition>
                        </xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="5">
                    <xs:annotation>
                        <xs:documentation>
                            <label xml:lang="en">Level 5</label>
                            <definition xml:lang="en">Up to level 5</definition>
                        </xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
            </xs:restriction>
    </xs:simpleType>


    <xs:complexType name="tPVRProfile">
        <xs:sequence>
            <xs:annotation>
                <xs:documentation>
                    Unit of the StorageLimitInVolume element is the GigaOctet
                </xs:documentation>
            </xs:annotation>
            <xs:element name="PVRPreference" type="tPVRPreference"/>
            <xs:element name="StorageLimitInTime" type="tNPVRStorageLimitInTime" minOccurs="0"/>
            <xs:element name="StorageLimitInVolume" type="tNPVRStorageLimitInVolume" minOccurs="0"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:simpleType name="tPVRPreference" final="list restriction">
        <xs:restriction base="xs:unsignedByte">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="1"/>
            <xs:enumeration value="0">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">Network</label>
                        <definition xml:lang="en">Recording is done in the network</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="1">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">User_Equipment</label>
                        <definition xml:lang="en">Recording is done on the user
equipment</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="tNPVRStorageLimitInTime">
        <xs:restriction base="xs:duration">
```

```
            <xs:minInclusive value="PT0H"/>
            <xs:maxInclusive value="PT1000000000H"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="tNPVRStorageLimitInVolume">
        <xs:restriction base="xs:nonNegativeInteger"/>
    </xs:simpleType>

    <xs:complexType name="tGlobalSettings">
        <xs:sequence>
            <xs:element name="LanguagePreference" type="tLanguage" minOccurs="0"/>
            <xs:element name="UsersActionRecordable" type="tUserActionRecordable"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>


    <xs:simpleType name="tLanguage">
        <xs:restriction base="xs:string">
                <xs:annotation>
                <xs:documentation>
                  <definition xml:lang="en">ISO 639-2 Language code</definition>
                </xs:documentation>
            </xs:annotation>
            <xs:minLength value="3"/>
            <xs:maxLength value="3"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="tExtension">
        <xs:sequence>
            <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:simpleType name="tUserActionRecordable">
        <xs:restriction base="xs:boolean"/>
    </xs:simpleType>

</xs:schema>
```

NOTE 1: The list of parameter that could be sent to the UE over UT is specified in the procedures clause.

NOTE 2: The UE profile used for service discovery may be considered in the same XML schema, indicating explicitly which part to used for the different purposes.

Annex D (normative):
XML Schema for IPTV commands

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
targetNamespace="urn:org:etsi:ngn:params:xml:ns:iptvactiondatacommand"
xmlns="urn:org:etsi:ngn:params:xml:ns:iptvactiondatacommand"
xmlns:bc ="urn:org:etsi:ngn:params:xml:ns:iptvbcserviceactiondata"
xmlns:co ="urn:org:etsi:ngn:params:xml:ns:iptvcodserviceactiondata"
xmlns:np ="urn:org:etsi:ngn:params:xml:ns:iptvnpvrserviceactiondata"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">

<xs:import namespace="urn:org:etsi:ngn:params:xml:ns:iptvbcserviceactiondata"
schemaLocation="annexK-XML Schemas for the IPTV service action data-Part-1.xsd"/>

<xs:import namespace="urn:org:etsi:ngn:params:xml:ns:iptvcodserviceactiondata"
schemaLocation="annexK-XML Schemas for the IPTV service action data-Part-2.xsd"/>

<xs:import namespace="urn:org:etsi:ngn:params:xml:ns:iptvnpvrserviceactiondata"
schemaLocation="annexK-XML Schemas for the IPTV service action data-Part-3.xsd"/>


    <xs:element name="IPTVActionDataCommand">
        <xs:complexType>
            <xs:choice>
                <xs:element name="Notify" type="tNotify" minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="Record" type="tRecord" minOccurs="0" maxOccurs="unbounded"/>
                <xs:element name="SwitchToTM" type="tSwitchToTM" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="SwitchToBC" type="tSwitchToBC" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:choice>
        </xs:complexType>
    </xs:element>

    <xs:complexType name="tNotify">
        <xs:choice>
            <xs:element ref="bc:IPTVBcActionData" />
            <xs:element ref="co:IPTVCoDActionData" />
            <xs:element ref="np:IPTVNpvrActionData" />
        </xs:choice>
    </xs:complexType>

    <xs:complexType name="tRecord">
        <xs:choice>
            <xs:element ref="bc:IPTVBcActionData" />
            <xs:element ref="np:IPTVNpvrActionData" />
        </xs:choice>
    </xs:complexType>

    <xs:complexType name="tSwitchToTM">
        <xs:choice>
            <xs:element ref="bc:IPTVBcActionData" />
        </xs:choice>
    </xs:complexType>

    <xs:complexType name="tSwitchToBC">
        <xs:choice>
            <xs:element ref="bc:IPTVBcActionData" />
        </xs:choice>
    </xs:complexType>

</xs:schema>
```

NOTE: Table D.1 recaps the presence of each element in the three Service Action Data for the different commands.

Table D.1

	Notify UE - > CN	Notify UE < - CN	Record UE - > CN	SwitchToTM UE - > CN	SwitchToBC UE - > CN
IPTVBcActionData					
BCServiceId	O	M	M	M	M
ProgrammeId	O	O	O	x	x
Bookmark	O	O	M	x	x
BookmarkExpiryTime	O	O	O	x	x
IPTVCodActionData					
CoDId	M	M	NA	NA	NA
CoDDeliveryStatus	M(parked)	M			
CoDOffset	M	M			
CoDOffsetExpiryTime	x	O			
IPTVNpvrActionData					
NPVRContentId	NA	M	O	NA	NA
BCServiceId		M	M		
RecordStartDate		M	O		
RecordEndDate		M	O		
RecordStatus		M	x		
RecordOffset		M	O		
RecordOffsetExpiryTime		O	x		
RecordExpiryTime		O	x		
NOTE: M = Mandatory. 　　　　O = Optional. 　　　　X = Not included. 　　　　NA = Not Applicable.					

Annex E (normative):
XML schema for IPTV presence document extension

This XML schema is be used when the presence documents are published by the UE as described in clause 5.1.6.

```
<xs:schema targetNamespace="urn:org:etsi:ngn:params:xml:ns:iptvpresence"
xmlns:ns="urn:org:etsi:ngn:params:xml:ns:iptvpresence"
xmlns:oma="urn:oma:xml:prs:pidf:oma-pres"
xmlns:ss="urn:org:etsi:ngn:params:xml:ns:iptv"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified"
attributeFormDefault="unqualified">

<xs:complexType name="tBCServicePresence">
    <xs:sequence>
        <xs:element name="CurrentBCServiceID" type="ns:tBCServiceID" minOccurs="0"/>
        <xs:element name="CurrentBCProgramID" type="ns:tCurrentBCProgramID" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="tCoDServicePresence">
    <xs:sequence>
        <xs:element name="CurrentCODContentID" type="ns:tCurrentContentID" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="tNPVRServicePresence">
    <xs:sequence>
        <xs:element name="CurrentNPVRContentID" type="ns:tCurrentContentID" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:simpleType name="tCurrentBCProgramID" final="list restriction">
    <xs:restriction base="xs:string">
        <xs:minLength value="0"/>
        <xs:maxLength value="256"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="tCurrentContentID" final="list restriction">
    <xs:restriction base="xs:string">
        <xs:minLength value="0"/>
        <xs:maxLength value="256"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="tBCServiceID" final="list restriction">
    <xs:restriction base="xs:string">
        <xs:minLength value="0"/>
        <xs:maxLength value="16"/>
    </xs:restriction>
</xs:simpleType>

</xs:schema>
```

Annex F (informative):
Example of presence information update after channel-change
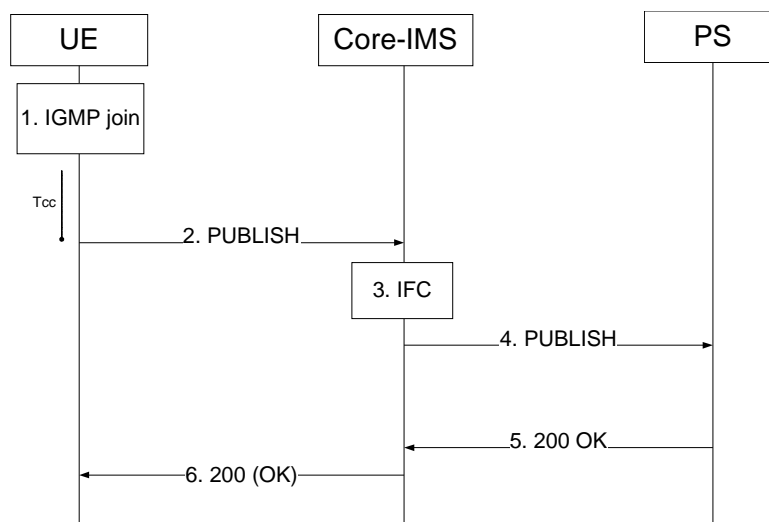
Figure F.1

1) **IGMP Join request (UE to Core-IMS):**

   The User wishes to change watching channel. The UE sends an IGMP join request to the multicast group corresponding to the selected channel.

   The timer Tcc is started.

2) **PUBLISH request (UE to Core-IMS):**

   After Tcc timer expiration, to initiate the publication, the UE generates a PUBLISH request according to ES 283 030 [21].

   The UE indicates the new watched channel in the present document.

3) **IFC:**

   The S-CSCF routes the request to the Presence Server according to the IFC.

4) **PUBLISH request (Core-IMS to Presence Server):**

   The Core-IMS forwards the PUBLISH request to the presence server thanks to the configured IFC. For example, for user1_public1@home1.net the Core-IMS has originating initial Filter Criteria with Service Point Trigger of Method = PUBLISH AND Event = "presence" AND
   Request-URI = "sip:user1_public1@home1.net" that informs the S-CSCF to route the PUBLISH request to the PS ps.home1.net.

5) **200 (OK) response (PS to Core-IMS):**

   The Presence Server evaluates the PUBLISH request and update presence information (i.e. currently watched channel).

   It replies with a SIP 200 OK to the Core IMS.

6) **200 (OK) response (Core-IMS to UE):**

   The Core-IMS forwards the SIP 200 OK to the UE.

Annex G (informative):
Example of presence document extension

The following example describes the particular case of a BC service:

```
<tuple id="serv11">
    <status>
        <basic>open</basic>
    </status>
    <oma:service-description>
        <oma:service-id>IPTV-BC</oma:service-id>
        <oma:version>x.y</oma:version>
        <oma:description>IPTV BroadCast service</oma:description>
    </oma:service-description>
    <caps:servcaps>
        <caps:audio>true</caps:audio>
        <caps:video>true</caps:video>
    </caps:servcaps>
    <BC>
        <currentBCServiceID>BCServiceId</currentBCServiceID>
        <currentBCProgramID>program1-id</currentBCProgramID>
    </BC>
    <rpid:class>IPTV</rpid:class>
    <dm:deviceID>mac:8asd7d7d70</dm:deviceID>
    <note>comment1</note>
</tuple>
```

Annex H (informative):
Summary of standards and protocols for IMS based IPTV

This informative annex provides summary of standards and protocols version (specification compliance) required by IMS based IPTV in mentioned reference points.

NOTE: In case of any inconsistencies with the normative text, the normative text applies.

H.1   SIP/SDP protocol

Usage the SIP/SDP protocol across the following reference points is described in clause 5:

- reference point Gm;

- reference point ISC;

- reference point y2.

Following functional entities are SIP/SDP capable:

- UE, SCF, SDP, MCF, Core IMS.

Following SIP protocol model explain which SIP request method are used for particular procedure.
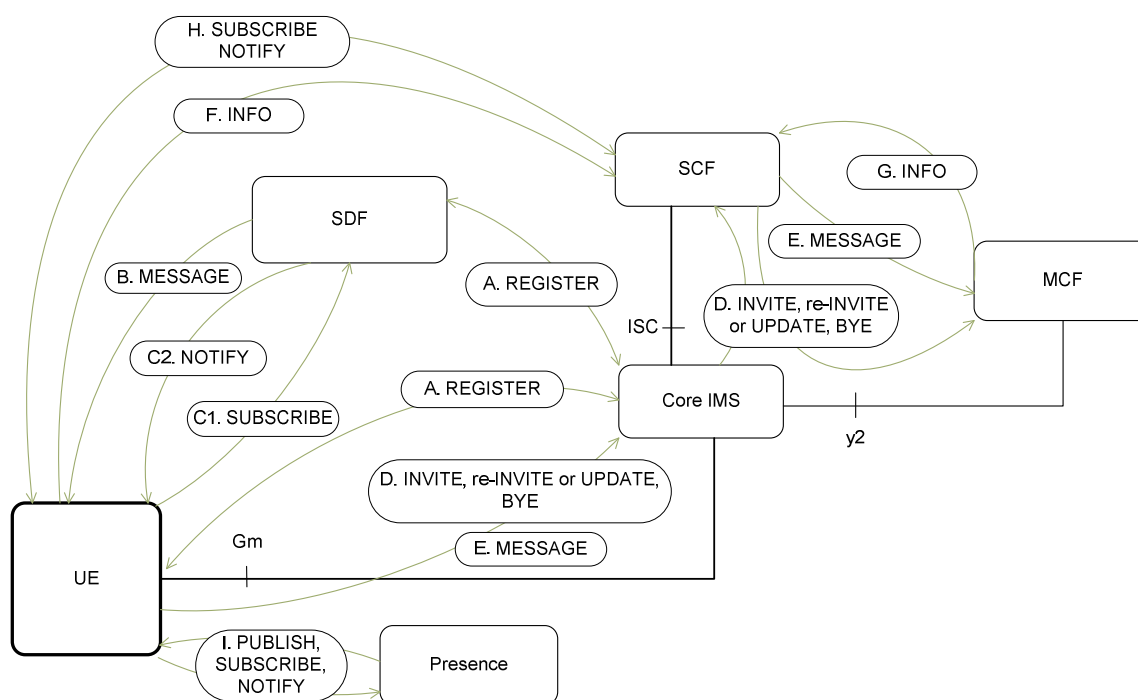
Figure H.1: IMS based IPTV - SIP protocol model

A.   UE send REGISTER to Core IMS and SDF.

B.   Service discovery Push mode - SDF send message MESSAGE with discovery information.

C.   Service discovery Pull mode - UE used SUBSCRIBE to SDF over Core IMS, SDF send NOTIFY with service discovery information (also when changed).

D.   Service initiation, modification and teardown from UE via Core IMS to SCF (INVITE, re-INVITE or UPDATE, BYE).

E.   UE sends a SIP MESSAGE request to SCF requiring NPVR service (SCF send MESSAGE to MCF).

F.   Optional - procedures for join multicast group (clause 8.1.1) the UE may inform SCF of the selected channel (sending INFO message).

G.   INFO message to send COD Service action data information to SCF.

H.   Service Attachment - PULL mode is used SUBSCRIBE and NOTIFY methods.

I.   Optional - Presence used for channel watching information.

H.1.1   Protocol specifications used for SIP/SDP

This clause contains list of protocol specifications required for IMS based IPTV implementation used as references in clause 5 or other related to SIP/SDP specifications. This clause contains also summary of methods required for implementation as mandatory and also optional.

Several Core IMS procedures are explicitly used by IMS based IPTV (not limited) like IMS registration, session initiation, modification and termination.

SIP methods like REGISTER, INVITE, UPDATE, PUBLISH, NOTIFY, MESSAGE, SUBSCRIBE are used in IMS based IPTV.

The following tables explain relation of used specification for specified function entity towards other entities. Last column summarizes requirements for implementation for specified functional entity (which specification are required for implementation).

Table H.1: SIP/SDP protocol related specification for UE

Specifications for: UE	IMS core	SDF	SCF	MCF	Summary of required implementation
Ref. point	Gm <->	Via IMS core <->	Via IMS core <->	---	UE
REGISTER [20]	(M)	(M) 3rd party			(M)
INVITE, re-INVITE or UPDATE, BYE [20]	(M)		(M)		(M)
MESSAGE [22] and [20] MESSAGE is used only by "Push mode" service discovery and "NPVR" service			(M)		(M)
PUBLISH [21] for IPTV presence (optional)			(O)		(O)
SUBSCRIBE [20] Pull mode		(M) clause 5.1.2A.1			(M)
NOTIFY [25] In pull mode			(M)		(M)
SIP INFO [20]			(O)		(O)
Annex Y in pull mode			(M)		(M)
OMA-TS-Presence-SIMPLE-V1 [23]			(O)		(O)
draft-ietf-sip-xcapevent-00 [i.10]			(O)		(O)
RFC 5874 [15]			(O)		(O)

Table H.2: SIP/SDP protocol related specification for Core IMS

Specification: IMS core	UE	SDF	SCF	MCF	Summary of required implementation
Ref. point	Gm <->	ISC <->	ISC <->	y2 <->	IMS core
ES 283 003 [20]	(M)	(M) ISC	(M) ISC	(M)	Core IMS entities
REGISTER, INVITE [20]	(M)	(M)			(M)
NOTIFY [25] [29] Pull mode	(M)	(M)			(M)
NOTE: Table mentions just SIP methods explicitly used in IMS based IPTV procedures but does not exclude any other usage of other methods.					

Table H.3: SIP/SDP protocol related specification for SDF

Specification: SDF	UE	IMS core	SCF	MCF	Summary of required implementation
Ref. point	Push mode -> Pull mode <-> Via IMS core	ISC <->	---	---	SDF
REGISTER [20]					third-party registration
Push mode [20]	(M)				(M)
Pull mode NOTIFY [29]	(M) clause 5.7.1.4				(M) clause 5.7.1.4
Pull mode user's identity verification [29]	(M)				(M)

Table H.4: SIP/SDP protocol related specification for SCF

Specification: SCF	UE	IMS core	SDF	MCF	Summary of required implementation
Ref. point	Ut <->	ISC <->	Via IMS core	Via IMS core	SCF
ES 283 003 [20]					SCF act as a terminating UA for BC service SCF act as a B2BUA when NPVR service is used (SIP dialog is established UA<=>SCF and SCF<=> MCF) SCF is a proxy or a B2BUA when CoD service is used
INVITE, re-INVITE or UPDATE, BYE [20]		(M)		(M)	(M) Via IMS core

Table H.5: SIP/SDP protocol related specification for MCF

Specification: MCF	UE	IMS core	SDF	SCF	Summary of required implementation
Ref. point		y2 <->		Via IMS core	MCF
ES 283 003 [20]		(M)		(M)	terminating UA (M)
REDIRECT SIP [2] BC with Trick play		(M)		(M)	(O) clause 5.1.3.3

ETSI

H.2   HTTP protocol

Usage of the HTTP protocol across the following interfaces is described in this clause:

- interface Xa;

- interface Ut.

HTTP capable functional entities:

- UE, SCF, SSF.

Table H.6: Summary of specifications compliancy for HTTP capable FEs

Specification:	UE	SSF	SCF
RFC 4825 [9]	XCAP client (M)	NA	XCAP sever (M) HTTP PUT, HTTP GET or HTTP DELETE
RFC 2246 [32]	(M)	(M)	(M)
TS 187 003 [10]	(M)	(M)	NA
TS 124 109 [11]	NA	(O)	(O)
TS 183 023 [12]	NA	(O)	(O)
TS 102 034 [3]	clause 5.4.2.2 (M)	clause 5.2.6 (M)	NA
TS 102 539 [13]	clauses 4.1.2.2.2 and 4.2 (M)	clauses 4.1.2 and 4.2 (M)	NA
TS 133 222 [14]	(O)	(O)	NA
RFC 5874 [15]	(O)	NA	(O)
OMA OMA-TS-BCAST_Service_Guide-V1_0 [6]	clause 5.4.3 (M)	clause 5.4.3.3 (M)	NA
NOTE: (M) - Mandatory. (O) - Optional. NA - NOT Applicable.			

H.3   RTSP/SDP protocol

Usage of the RTSP/SDP protocol across the following interfaces is described in clause 7:

- interface Di, Dj, Ds or lz.

RTSP/SDP capable functional entities:

- UE, MCF.

H.3.1   Protocol specifications used for RTSP/SDP

This clause contain summary of RTSP methods required for implementation in IMS based IPTV as mandatory or optional (as references to clause 7 or other related to RTSP/SDP). Table H.7 shows the differences by using RTSP method in compare with RFC 2326 [8].

Table H.7

RTSP Method	Direction: C = client - UE; S = Server - MCF;	RFC 2326 [8]	DVB Requirement TS 102 034 [3]		TISPAN IMS based IPTV	
			LMB	MBwTM and CoD	Method 1	Method 2
ANNOUNCE	C→S	MAY	MAY	MAY	N.A.	N.A.
ANNOUNCE	S→C	MAY	**SHOULD**	**SHOULD**	**(M)**	**(M)**
DESCRIBE	C→S	SHOULD	SHOULD	SHOULD	**N.A.**	**(M)**
GET_PARAMETER	C→S	MAY	**SHOULD**	**SHOULD**	**(M)**	N.A.
GET_PARAMETER	S→C	MAY	MAY	MAY	N.A.	N.A.
OPTIONS	C→S	SHALL	SHALL	SHALL	(M)	**N.A.**
OPTIONS	S→C	MAY	MAY	MAY	N.A.	N.A.
PAUSE	C→S	SHOULD	**N.A.**	**SHALL**	**(M)**	**(M)**
PLAY	C→S	SHALL	SHALL	SHALL	(M)	(M)
REDIRECT	S→C	MAY	**SHALL**	**SHALL**	**N.A.**	**N.A.**
SETUP	C→S	SHALL	SHALL	SHALL	**N.A.**	(M)
TEARDOWN	C→S	SHALL	SHALL	SHALL	**N.A.**	(M)
SET_PARAMETER	C→S	MAY	N.A.	N.A.	**(M)**	N.A.
SET_PARAMETER	S→C	MAY	N.A.	N.A.	N.A.	N.A.
RECORD	C→S	MAY	N.A.	N.A.	N.A.	N.A.
NOTE: (M) = Mandatory. (O) = Optional. N.A. = Not Applied. The text in **bold** shows differences comparing to RFC 2326 [8] table 2.						

H.4   RTP/RTCP protocol

Usage of the RTP/RTCP protocol across the following interfaces is described in clause 11:

- interface Di, Dj, Ds or Iz.

RTP/RFTCP capable functional entities:

- UE, MDF.

H.5   IGMP/MLD protocol

Usage of the IGMP/MLD protocol across the following interfaces is described in clause 8:

- interface Di.

IGMP/MLD capable functional entities:

- UE, Transporting functions (ECF/EFF), MDF.

If IPv4 is used for the transport, the UE conforms to RFC 3376 [28] (IGMPv3).

If IPv6 is used for the transport, the UE conforms to RFC 3810 [29] (MLDv2).

Backward compatibility rules between the UE and the Transport Function have to be done conforming to RFC 3376 [28], clause 7 and RFC 3810 [29], clause 8.

UE need to support at least:

- IGMP v3 unsolicited Membership Report or a MLDv2 Multicast Listener Report Message.

- IGMP v3 Membership Report Message or MLD v2 Multicast Listener Report Message.

H.6   Diameter protocol

Use of Diameter complies to the following specifications:

- TS 183 017 [i.2] in case of the Gq' interface.

- ES 283 035 [36] in case of the e2 interface.

- TS 183 033 [i.3] in case of the Cx and Dx' interfaces.

- TS 129 329 [i.4] in case of the Sh and Dh interfaces.

Diameter capable functional entities:

- CoreIMS, SCF, SDF.

H.7   DVBSTP protocol

Usage of the DVBSTP protocol across the following interface is described in clause 9:

- interface Xa.

DVBSTP capable functional entities (Optionally):

- UE, SSF.

H.8   FLUTE protocol

Usage of the FLUTE protocol across the following interface is described in clause 10:

- interface Xa.

FLUTE capable functional entities (Optionally):

- UE, SSF.

Annex I (normative):
Procedures for discovery of SDFs prior to service attachment

This annex describes a set of alternatives for the UE to identify the SDFs and/or the service provider domain information associated with them prior to service attachment procedures.

The order in which these alternatives are executed or priority between the alternatives when executed simultaneously is outside of the scope of the present document.

I.1   Manual configuration based manual discovery

The UE may be manually configured with the one or more instances of the following information.

- The Service Provider Name: This provides the name of the Service Provider to connect to first. It is of variable length.

- ServiceProviderDomainName: This provides the domain name corresponding to Service provider. It is of variable length.

- ServiceDiscoveryServer: This specifies the address of the SDF associated with the SP and it is specified as an IMS Public Service Identifier or IP address or URL.

- The IMS PSI value shall be specified for IMS-based Service Discovery Function.

- The IPAddress or URL may be specified for non-SIP-AS based Service Discovery Function.

I.2   DHCP-based discovery

In addition to acquiring its IP address from the DHCP server, in this mechanism the UE can acquire information on SDFs and associated Service Provider(s) information using appropriate vendor class identifier DHCP options.

I.2.1   Using DHCP option 43/60

The client may send a Vendor class Identifier DHCP option 60 as specified in ES 283 003 [20] when it requests a DHCP lease for server. The option is specified with the vendor-class identifier as "ETSI_TISPAN_IPTV_SDS"

The DHCP server delivers the SDF information via Vendor-Specific Information DHCP option 43 packed in a binary buffer as defined in ES 283 003 [20]. The format of the binary buffer containing the SDF information is specified in clause I.2.3.

I.2.2   Using DHCP option 124/125

This vendor identifier specific DHCP option is recommended to be used when there is a need to support DHCP options from multiple vendors as specified in RFC 3925 [17].

The client may send a Vendor -Identifying Vendor Class option 124 as specified in RFC 3925 [17] when it requests a DHCP lease for server. The option is specified with an enterprise-number of 13019 (ETSI) and the vendor-class-data identifier as "ETSI_TISPAN_IPTV_SDS".

The DHCP server delivers the SDF information via Vendor-Identifying Vendor-Specific Information DHCP option 125 packed in a binary buffer as defined in RFC 3925 [17]. The enterprise-number shall be set as 13109 (ETSI). The format of the binary buffer containing the SDF information is specified in clause I.2.3.

I.2.3   Format of DHCP payload

The format of the vendor-specific binary buffer containing SDF addresses returned by the DHCP server is as follows.

It is a list of sub-options starting with sub-option number (one byte), its length (one byte) and its value (list of bytes).

The following vendor-specific sub-options are defined:

- Sub-Option: IMS_IPTV_SP: Code = 0x01. This option provides the name of the Service Provider to connect to first. It is of variable length and it is Optional.

- Sub-Option: IMS-IPTV-SPDOMAIN: Code= 0x02. This option provides the domain name corresponding to Service provider. It is of variable length and it is Optional.

- Sub-Option: IMS-IPTV-SDF: Code=0x03. This option carries either the (1) IMS PSI value, (2) the IPAddress of SDF or (3) the fully-qualified domain name of the Service Discovery Server associated with the Service Provider. This is Mandatory.

- A one byte "enc" field is used to indicate the type of encoding.

  - If the "enc" field has a value of _0x00, then this indicates an IMS PSI value. The "enc" field is followed by the bytes corresponding to the IMS PSI. This value shall be used for IMS-based service discovery function.

  - If the "enc" field has a value of _0x01, then this indicates an IP Address. The "enc" field is followed by 4 bytes corresponding to the IPAddress. This value may be used for non-SIP AS service discovery function.

  - If the "enc" field has a value of 0x02, then this indicates a DNS hostname. The "enc" field is followed by a sequence of labels, encoded according to clause 3.1 of RFC 1035 [18]. This value may be used for non-SIP AS service discovery function.

- The code of 0xFF is used to indicate end of the buffer.

The availability of the service provider SDF information at the Network Provider DHCP server is subject to business policies between the service provider and network provider.

I.3   DNS Service Records (SRV) - based discovery

In this case, the SD servers are discovered using the DNS SRV mechanism in accordance with RFC 2782 [31], with the following input parameters:

- Service: Defined as "tispan-iptv-service". This is the symbolic name of the desired service; to be defined and registered with IANA.

- Protocol: Can take values "http" or "sip". Specifies the protocol to contain the particular service.

- Domain name: the domain for which the returned records are valid; the value can be derived from the following:

  - Domain from manual configuration.

  - Domain from network attachment phase (DHCP server).

  - Domain from IMS home domain.

The output of the DNS SRV lookup is an ordered list of domain name, each pointing to a SDF server available within the specified Domain name.

I.4   TR-069 based discovery

In this case, the UE discovers the addresses of the SDFs and associated Service Provider information during remote configuration procedures using the TR-069 [37] protocol.

Specifically, upon successful UE network attachment and successful creation of a management session with the remote configuration server, the CNGCF may provide the UE with a listing of IPTV service providers and associated SDF servers that it knows about. How the remote configuration server at the CNGCF is provided with this information is beyond the scope of the present document.

An ordered listing of one or more instances of the following elements may be delivered:

- The Service Provider Name: This provides the name of the Service Provider to connect to first. It is of variable length.

- ServiceProviderDomainName: This provides the domain name corresponding to Service provider. It is of variable length.

- ServiceDiscoveryServer: This specifies the address of the SDF associated with the SP and it is specified as a IMS Public Service Identifier or IP address or URL:

    - The IMS PSI value shall be specified for IMS-based Service Discovery Function.

    - The IPAddress or URL may be specified for non-SIP-AS based Service Discovery Function.

NOTE: The exact object extension used to carry the above information during remote configuration is beyond scope of the present document.

Annex J (informative):
Integration of non SIP AS service discovery function

J.1 Integration of non SIP AS service discovery Function based on DVB IPTV

J.1.1 User Equipment (UE)

J.1.1.1 Procedure for service attachment

In order to discover the list of SDF, the UE will follow the entry points discovery steps as defined in TS 102 034 [3], clause 5.2.4.

The UE will use HTTP or DVBSTP protocols in order to retrieve the service provider discovery information, conforming to TS 102 034 [3], clause 5.4.

> NOTE: It is also possible that the UE holds a hard-coded parameter containing the entry point information, or that an out-of-band mechanism exists for the UE to retrieve this information.

J.1.1.2 Procedure for service selection

J.1.1.2.1 Request of DVB SD&S

The UE will use HTTP or DVBSTP protocols in order to retrieve the SD&S information, conforming to TS 102 034 [3], clause 5.4.

J.1.1.2.2 Request of DVB BCG

The UE will use HTTP, DVBSTP or HTTP/SOAP protocols in order to retrieve the BCG information, conforming to TS 102 539 [13], clause 4.

J.1.2 Service Discovery Function (SDF)

J.1.2.1 Procedure for service attachment

The SDF will provide to the UE the service provider discovery information conforming to TS 102 034 [3], clause 5.2.5.

The SDF will use HTTP and DVBSTP protocols, conforming to TS 102 034 [3], clause 5.4.

J.1.3 Service Selection Function (SSF)

J.1.3.1 Procedure for service selection

J.1.3.1.1 Delivery of DVB SD&S

The SSF will provide to the UE the SD&S information conforming to TS 102 034 [3], clause 5.2.6.

The SSF will use HTTP and DVBSTP protocols, conforming to TS 102 034 [3], clause 5.4.

J.1.3.1.2   Delivery of DVB BCG

The SSF will provide to the UE the BCG information conforming to TS 102 539 [13].

The SSF will use HTTP, DVBSTP, and HTTP/SOAP protocols, conforming to TS 102 539 [13], clause 4.

J.2   Integration of non SIP AS service discovery function based on OMA BCAST ESG

J.2.1   User Equipment (UE)

J.2.1.1   Procedure for service attachment

It is assumed that each service provider publishes a single ESG. Thus, an ESG provider is equal to a service provider. For discovering the available service providers the list of SDFs, the UE can follow the ESG bootstrapping method as defined in OMA-TS-BCAST_DVB_Adaptation-V1_0 [7], clause 6.3.5 or other signalling methods. It is assumed that there is an ESG bootstrap session where service guides are described with ESGProviderDiscovery Descriptors, as specified in clause 9 of TS 102 471 [4]. This also applies to describing OMA BCAST service guides [6]. In the push situation, the ESG bootstrap session will be a FLUTE session as specified in TS 102 471 [4]. In the pull situation, the bootstrap session uses HTTP.

  NOTE: It is also possible that the UE holds a hard-coded parameter containing the entry point information, or that an out-of-band mechanism exists for the UE to retrieve this information.

J.2.1.2   Procedure for service selection

J.2.1.2.1   Request of ESG provider discovery information

The UE uses the FLUTE protocol in order to retrieve the ESGProviderDiscovery Descriptor information, conforming to TS 102 471 [4], clause 9.2 and OMA-TS-BCAST_DVB_Adaptation-V1_0 [7], clause 6.3.5 or it uses the HTTP protocol.

J.2.1.2.2   Request of OMA BCAST ESG

The UE uses HTTP or FLUTE protocols in order to retrieve the ESG information, conforming to TS 102 471 [4], clause 8.1, OMA-TS-BCAST_DVB_Adaptation-V1_0 [7], clause 6.3.5 and OMA-TS-BCAST_Service_Guide-V1 [6], clause 5.4.

J.2.2   Service Discovery Function (SDF)

J.2.2.1   Procedure for service attachment

The SDF will provide to the UE the service provider discovery information in the form of ESGProviderDiscovery Descriptors, conforming to TS 102 471 [4], clause 9.1.1.

For providing the UE with this information, the SDF will use HTTP and FLUTE protocols, conforming to TS 102 471 [4], clause 9.2, OMA-TS-BCAST_DVB_Adaptation-V1_0 [7], clause 6.3.5 and OMA-TS-BCAST_Service_Guide-V1 [6], clause 5.4.

J.2.3   Service Selection Function (SSF)

J.2.3.1   Procedure for service selection

J.2.3.1.1   Delivery of ESG provider discovery information

The SSF will provide to the UE the ESGProviderDiscovery Descriptor conforming to TS 102 471 [4], clause 9.1.1. The SSF use the FLUTE protocol, conforming to TS 102 471 [4], clause 9.2 and OMA-TS-BCAST_DVB_Adaptation-V1_0 [7], clause 6.3.5. or it uses the HTTP protocol.

J.2.3.1.2   Delivery of OMA BCAST ESG

The SSF will provide to the UE the ESG information conforming to OMA-TS-BCAST_Service_Guide-V1_, clause 5.4.

The SSF will use HTTP or FLUTE protocols, conforming to TS 102 471 [4], clause 8.1, OMA-TS-BCAST_DVB_Adaptation-V1_0 [7], clause 6.3.5 and OMA-TS-BCAST_Service_Guide-V1 [6], clause 5.4.

Annex K (normative):
XML Schemas for the IPTV service action data

This annex specifies XML schemas for creating documents representing instances of the IPTV service action data.

XML Schema for BC service related data:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:org:etsi:ngn:params:xml:ns:iptvbcserviceactiondata"
xmlns="urn:org:etsi:ngn:params:xml:ns:iptvbcserviceactiondata"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
    <xs:element name="IPTVBcActionData">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="BCBookmark" type="tBCBookmark" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="tBCBookmark">
        <xs:sequence>
            <xs:element name="BCServiceId" type="xs:string"/>
            <xs:element name="ProgrammeId" type="xs:string" minOccurs="0"/>
            <xs:element name="Bookmark" type="xs:dateTime"/>
            <xs:element name="BookmarkExpiryTime" type="xs:dateTime" minOccurs="0"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tExtension">
        <xs:sequence>
            <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

XML Schema for CoD service related data:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:org:etsi:ngn:params:xml:ns:iptvcodserviceactiondata"
xmlns="urn:org:etsi:ngn:params:xml:ns:iptvcodserviceactiondata"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
    <xs:element name="IPTVCoDActionData">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="AvailableCoD" type="tAvailableCoD" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="tAvailableCoD">
        <xs:sequence>
            <xs:element name="CoDId" type="xs:string"/>
            <xs:element name="CoDDeliveryStatus" type="tCodDeliveryStatus"/>
            <xs:element name="CoDOffset" type="xs:string" minOccurs="0"/>
            <xs:element name="CoDOffsetExpiryTime" type="xs:dateTime" minOccurs="0"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="tCodDeliveryStatus" final="list">
        <xs:restriction base="xs:unsignedByte">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="3"/>
            <xs:enumeration value="0">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">Ordered</label>
                        <definition xml:lang="en">Content has been ordered</definition>
                    </xs:documentation>
                </xs:annotation>
```

```
                </xs:enumeration>
                <xs:enumeration value="1">
                    <xs:annotation>
                        <xs:documentation>
                            <label xml:lang="en">Ongoing</label>
                            <definition xml:lang="en">Streaming delivery has started</definition>
                        </xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="2">
                    <xs:annotation>
                        <xs:documentation>
                            <label xml:lang="en">Failed</label>
                            <definition xml:lang="en">Some error has occurred while delivering the
content</definition>
                        </xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="3">
                    <xs:annotation>
                        <xs:documentation>
                            <label xml:lang="en">Parked</label>
                            <definition xml:lang="en">The content was parked and will be pickep up
later</definition>
                        </xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
            </xs:restriction>
        </xs:simpleType>
        <xs:complexType name="tExtension">
            <xs:sequence>
                <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
</xs:schema>
```

XML Schema for NPVR service related data:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:org:etsi:ngn:params:xml:ns:iptvnpvrserviceactiondata"
xmlns="urn:org:etsi:ngn:params:xml:ns:iptvnpvrserviceactiondata"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">
    <xs:element name="IPTVNpvrActionData">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="NPVRItem" type="tNPVRItem" minOccurs="0" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:complexType name="tNPVRItem">
        <xs:sequence>
            <xs:element name="NPVRContentId" type="xs:string" minOccurs="0"/>
            <xs:element name="BCServiceId" type="xs:string" />
            <xs:element name="RecordStartDate" type="xs:string" minOccurs="0"/>
            <xs:element name="RecordEndDate" type="xs:dateTime" minOccurs="0"/>
            <xs:element name="RecordStatus" type="tRecordStatus" minOccurs="0"/>
            <xs:element name="PlaybackOffset" type="xs:string" minOccurs="0"/>
            <xs:element name="PlaybackOffsetExpiryTime" type="xs:dateTime" minOccurs="0"/>
            <xs:element name="NPVRContentExpiryTime" type="xs:dateTime" minOccurs="0"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="tRecordStatus">
        <xs:restriction base="xs:unsignedByte">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="3"/>
            <xs:enumeration value="0">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">Scheduled</label>
                        <definition xml:lang="en">Recording is scheduled</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="1">
                <xs:annotation>
```

```xml
                    <xs:documentation>
                        <label xml:lang="en">Started</label>
                        <definition xml:lang="en">Recording has started</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="2">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">Available</label>
                        <definition xml:lang="en">Recording is available</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="3">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">Failed</label>
                        <definition xml:lang="en">Recording has failed</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tExtension">
        <xs:sequence>
            <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

Annex L (normative):
Mapping of IPTV parameters to service selection

L.1 Mapping of service attachment

This clause presents how several IPTV technologies are mapped into TISPAN metadata (XML schema as specified in annex M) concerning the discovery of SSF entities. In the current release DVB and OMABCAST technologies mapping are described.

Within the XML schema, some fields are specific to TISPAN, they are marked as "*TISPAN defined field*" in the following tables.

L.1.1 Mapping of DVB SD&S SP discovery records to XML Schema for Service Attachment

This clause describes the mapping of DVB SD&S Service Provider discovery record to the generic XML schema for service attachment defined in annex M and clause 5.2.2.3.

TISPAN Element Name (copied from clause 5.2.2.3)	Corresponding DVB SD&S element in TS 102 034 [3], clause 5.2.5 table 2 (TS 102 034 [3] XML Schema clause reference)
SSF	
@ID	*TISPAN defined field*
@Technology	when a DVB SSF is advertised, this field must be "dvb.org_iptv"
@Version	*TISPAN defined field*
Description	*TISPAN defined field*
ServiceProvider	ServiceProvider *(Clause C.1.4.6)*
@DomainName	ServiceProvider@DomainName *(Clause C.1.4.6)*
@LogoURI	ServiceProvider@LogoURI *(Clause C.1.4.6)*
Name	ServiceProvider.Name *(Clause C.1.4.6)*
Description	ServiceProvider.Description *(Clause C.1.4.6)*
Pull	OfferingListType.Pull *(Clause C.1.3.15)*
@Location	Pull@Location *(Clause C.1.3.15)*
DataType	PayloadId There is a direct mapping between the DVB PayloadId values and this field. *(Clause C.1.3.19)*
@Type	PayloadId@Id refer to table 1 in TS 102 034 [3] and to table 2 in TS 102 539 [13] TS 102 034 [3] defines the values 0x00 to 0x06, TS 102 539 [13] defines the values 0xA1 to 0xA7. The present specification defines an additional value 0xA0: when using 0xA0, it means that the Pull@Location URL refers to a SSF that is a DVB-BCG server using the SOAP protocol, instead of the pull HTTP delivery. When 0xA0 is used, no Segment element shall be exposed. *(C.1.3.19)*
Segment	PayloadId.Segment *(Clause C.1.3.19)* This parameter is mandatory for DVB Pull mode
@ID	PayloadId.Segment@Id *(Clause C.1.3.19)*

TISPAN Element Name (copied from clause 5.2.2.3)	Corresponding DVB SD&S element in TS 102 034 [3], clause 5.2.5 table 2 (TS 102 034 [3] XML Schema clause reference)
@Version	PayloadId.Segment@Version *(Clause C.1.3.19)*
Push	OfferingListType.Push *(Clauses C.1.3.15 and C.1.3.4)*
@IPVersion	
@MulticastAddress	@Address *(Clause C.1.3.11)*
@MulticastPort	@Port *(Clause C.1.3.11)*
@SourceAddress	@Source *(Clause C.1.3.11)*
DataType	PayloadId (refer to table 1 in TS 102 034 [3] and to table 2 in TS 102 539 [13]) *(Clause C.1.3.19)*
@Type	PayloadId@Id There is a direct mapping between the DVB PayloadId values and this field *(Clause C.1.3.19)*
Segment	PayloadId.Segment *(Clause C.1.3.19)* This parameter is optional for DVB Push mode
@ID	PayloadId.Segment@Id *(Clause C.1.3.19)*
@Version	**PayloadId.Segment@Version** *(Clause C.1.3.19)*

L.1.2   Mapping of OMA BCAST ESG delivery descriptors to XML schema for service attachment

This clause describes the mapping of OMA BCAST ESG delivery descriptors to the generic XML schema for service attachment defined in annex M and clause 5.2.2.3. The mandatory/optional nature of the fields can be derived from there.

TISPAN Element Name (copied from clause 5.2.2.3)	Corresponding OMA BCAST ESG element in OMA-TS-BCAST_Service_Guide-V1_0 [REF9], clause 5.4 and TS 102 471 [4], clause 9.1
SSF	
@ID	*TISPAN defined field*
@Technology	When an OMA BCAST SSF is advertised, this field must be "openmobilealliance.org_bcast"
@Version	*TISPAN defined field*
Description	*TISPAN defined field*
ServiceProvider	
@DomainName	ProviderURI (TS 102 471 [4]*, clause 9.1.1*)
@LogoURI	ProviderLogo (*[REF7], clause 9.1.1*)
Name	ProviderName (TS 102 471 [4]*, clause 9.1.1*)
Description	
Pull	
@Location	This URI encodes the location of the Service Guide Delivery Descriptors and/or the Service Guide Delivery Units ([6]*, clause 5.4*)
DataType	Specifies the type of Service Guide data fragment. ([6]*, clause 5.4*)

TISPAN Element Name (copied from clause 5.2.2.3)	Corresponding OMA BCAST ESG element in OMA-TS-BCAST_Service_Guide-V1_0 [REF9], clause 5.4 and TS 102 471 [4], clause 9.1
@Type	Options are "sgdd", "sgdu" and "sgdd+sgdu". The value is used to populate the body of the HTTP request ([6], *clause 5.4.3.1*)
Segment	Service Guide Delivery Descriptor or Service Guide fragment. ([6], *clause 5.4.1*) This parameter is mandatory for OMABCAST Pull mode
@ID	Service Guide Delivery Descriptor or Service Guide fragment identifier. Can be mapped to "id", "fragmentID" or "fragmentTransportID". Format is anyURI ([6], *clause 5.4.1.1*)
@Version	Version of the Service Guide Delivery Descriptor or Service Guide fragment identifier. Can be mapped to "version" or "fragmentVersion". Format is unsignedInt ([6], *clauses 5.4.1.3 and 5.4.1.5.2*)
Push	
@IPVersion	IPVersion6, format is bit string. This is a binary flag, which, if set to "1", indicates IPv6 usage (TS 102 471 [4], *clause 9.1.2*)
@MulticastAddress	Specifies the IP address of the FLUTE session transporting the ESG (TS 102 471 [4], *clause 9.1.2*)
@MulticastPort	Specifies the port number of the IP stream of the FLUTE session transporting the ESG (TS 102 471 [4], *clause 9.1.2*)
@SourceAddress	Specifies the source IP address of the FLUTE session transporting the ESG (TS 102 471 [4], *clause 9.1.2*)
DataType	Specifies the type of Service Guide data fragment (TS 102 471 [4], *clause 5.4*)
@Type	Options are "application/vnd.oma.bcast.sgdd+xml" and "application/vnd.oma.bcast.sgdu" ([6], *clause 5.4.2*)
Segment	Service Guide Delivery Descriptor or Service Guide fragment (TS 102 471 [4], *clause 5.4.1*) This parameter is mandatory for OMABCAST Push mode
@ID	Service Guide Delivery Descriptor or Service Guide fragment identifier. Can be mapped to "id", "fragmentID" or "fragmentTransportID". Format is anyURI ([6], *clause 5.4.1.1*)
@Version	Version of the Service Guide Delivery Descriptor or Service Guide fragment identifier. Can be mapped to "version" or "fragmentVersion". Format is unsignedInt ([6], *clauses 5.4.1.3 and 5.4.1.5.2*)

L.1.3   Mapping of service action data record discovery records to XML schema for service attachment

This clause describes the mapping of **Service Action Data** record to the generic XML schema for service attachment defined in annex M and clause 5.2.2.3.

TISPAN Element Name (copied from clause 5.2.2.3)	Corresponding Service Action Data field
SSF	
@ID	TISPAN defined field
@Technology	when a Service Action Data record is advertised, this field must be "tispan.org_sad"
@Version	TISPAN defined field
Description	TISPAN defined field
ServiceProvider	Service Provider information
@DomainName	An internet DNS domain name registered by the Service Provider that uniquely identifies the Service Provider
@LogoURI	Pointer to a Service Provider logo for potential display
Name	Name of the Service Provider for display in one or more languages; one Service Provider name is allowed per language code, and at least one language shall be provided
Description	Description of the Service Provider for potential display in one or more languages; one description is allowed per language code
Pull	
@Location	Location of the Service Action data Record
DataType	Type of Service Action Data (BC bookmark, N-PVR, CoD)
@Type	0x00 defines All service action data 0x01 defines BC service action data 0x02 defines CoD service action data 0x03 defines N-PVR service action data
Segment	Not applicable
@ID	Not applicable
@Version	Not applicable
Push	Not applicable
@IPVersion	
@MulticastAddress	Not applicable
@MulticastPort	Not applicable
@SourceAddress	Not applicable
DataType	Not applicable
@Type	Not applicable
Segment	Not applicable
@ID	Not applicable
@Version	Not applicable

L.2   Mapping of BC service

L.2.1   Mapping of BC service for DVB technology

Table L.1: Mapping of SIP parameters for BC service

IPTV SIP parameters	DVB
Request-URI	Not retrieved from SSF

Table L.2: Mapping of SDP parameters for BC service

IPTV SDP parameters for each media stream	Corresponding DVB SD&S element in TS 102 034 [3], clause 5.2.6.2 tables 4, 5 and 8 *(TS 102 034 [3] XML Schema clause reference)*
BC content stream	
Connection Data c=<network type> <address type> <connection address>	
<network type>	Not retrieved from SSF
<address type>	Not retrieved form SSF
<connection address>	IPMulticastAddress@Address *(Clauses C.1.3.10, C.1.3.11)*
Media Announcements for content delivery m=<media> <port> <transport> <fmt list>	
<media>	"video", not retrieved from SSF
<port>	IPMulticastAddress@Port *(Clauses C.1.3.10 and C.1.3.11)*
<transport>	"RTP/AVP" if IPMulticastAddress@Streaming="rtp" or if IPMulticastAddress@Streaming is not present "UDP/H2221/MP2T" or "UDP/RAW/RAW" if IPMulticastAddress@Streaming="udp" *(Clauses C.1.3.10 and C.1.3.11)*
<fmt>	"33", not retrieved from SSF
Bandwidth b=AS:<bandwidth>	MaxBitrate *(Clause C.1.3.8)*
BCServiceId	TextualIdentifier@ServiceName ":"TextualIdentifier@DomainName *(Clause C.1.3.24)* Note that the TextualIdentifier@DomainName is an optional attribute; therefore if it's not present, the field is copied from the *OfferingBase@DomainName (Clause* C.1.3.14)
BCPackageId	Package@Id *(Clause C.1.3.16)*
FEC stream Note that the multicast address and source address of the FEC stream can be the same as the BC content stream	
Media Announcements for FEC delivery m=<media> <port> <transport> <fmt list>	see note
<media>	"application", not retrieved from SSF
<port>	IPMulticastAddress.FECBaseLayer@Port *(Clauses C.1.3.10 and C.1.3.6)*
<transport>	RTP/AVP
<fmt>	Dynamic payload type
a=rtpmap:<fmt> <encoding_name/clock_rate>	<encoding_name/clock_rate> referring to the DVB-IP AL-FEC Base layer and is equal to: "vnd.dvb.iptv.alfec-base/90000"
Connection Data at media level c=<network type> <address type> <connection address>	
<network type>	Not retrieved from SSF
<address type>	Not retrieved from SSF
<connection address>	IPMulticastAddress.FECBaseLayer@Address *(Clauses* C.1.3.10 and C.1.3.6)
NOTE: The FEC delivery can only be associated to a RTP delivered content.	

Table L.3: Mapping of IGMP parameters for BC service

IPTV IGMP parameters	Corresponding DVB SD&S element in TS 102 034 [3], clause 5.2.6.2, tables 4 and 5 *(TS 102 034 [3] XML Schema clause reference)*
BC content stream	
<Multicast Address>	IPMulticastAddress@Address *(Clauses C.1.3.10 and C.1.3.11)*
<Source Address>	IPMulticastAddress@Source *(Clauses C.1.3.10 and C.1.3.11)*
FEC stream Note that the multicast address and source address of the FEC stream can be the same as the Live content stream	
<Multicast Address>	If the FEC multicast address is not the same as the live stream address: IPMulticastAddress.FECBaseLayer@Address *(Clauses C.1.3.10 and C.1.3.6)*
<Source Address>	If the source address is not the same as the live stream: IPMulticastAddress.FECBaseLayer@Source *(Clauses C.1.3.10 and C.1.3.6)*

L.2.2   Mapping of BC service for OMA BCAST technology

Clause L.2.2 describes the mapping of OMA BCAST ESG delivery descriptors to the TISPAN XML schema for service attachment. This mapping procedure allows for retrieving OMA BCAST ESG fragments from an SSF. The various types of ESG fragments and the relation between them is described in clause 5.1.1 of OMA-TS-BCAST_ServiceGuide-V1_0 [6]" and shown in figure 1 of that clause. An ESG has separate fragments to describe the service (e.g. TV channel) and to describe the access to that service. From a Service fragment (clause 5.1.2.1 in [6]) a unique identifier can be obtained to map to the BCServiceID. The Access fragment can either contain or refer to an Session Description, which can take the form of an SDP. Thus, from an OMA BCAST SSF a UE can obtain TV channel identification, description and access information, where the latter is in the form of an SDP.

Table L.4: Mapping of SIP parameters for BC service

IPTV SIP parameters	OMA BCAST
Request-URI	Not retrieved from SSF

Table L.5: Mapping of SDP parameters for BC service

IPTV SDP parameters for each media stream	Corresponding OMA BCAST element in OMA-TS-BCAST_ServiceGuide-V1_0 [6]
Connection Data c=<network type> <address type> <connection address>	
<network type>	SDP
<address type>	SDP
<connection address>	SDP
Media Announcements for content delivery m=<media> <port> <transport> <fmt list>	
<media>	SDP
<port>	SDP
<transport>	SDP
<fmt list>	SDP
Bandwidth b=AS:<bandwidth>	SDP
BCServiceId	globalServiceID
BCPackageId	globalPurchaseItemID

Table L.6: Mapping of IGMP parameters for BC service

IPTV IGMP parameters	OMA BCAST
<Multicast Address>	SDP
<Source Address>	SDP

L.2.3   Use of the TV URI in the mapping of BC service for DVB technology and OMA BCAST technology

TS 184 009 [16] specifies the TV URI as globally unique identifier to identify broadcast television channels. The TV URI is used in the mapping of BC service for DVB technology and OMA BCAST technology as follows.

L.2.3.1   DVB technology

If DVB technology (see clause L.2.1) is used, then the ServiceName attribute of the TextualIdentifier should be populated with the TV URI identifying the television channel.

L.2.3.2   OMA BCAST technology

If OMA-BCAST technology is used (see clause L.2.2), then the globalServiceID should be populated with the TV URI identifying the television channel.

L.3   Mapping of CoD service

L.3.1   Mapping of CoD service for DVB technology

Table L.7: Mapping of SIP parameters for CoD service - DVB technology

IPTV SIP parameters	DVB BCG
Request-URI	Locator defined in TS 102 822-4 [35], in sip-uri format
NOTE: the user part of the Request-URI is a free string format corresponding to a unique content instance for one service provider, e.g. sip: cod_content1_hd@service_provider1.com.	

Table L.8: Mapping of SDP parameters for CoD service - DVB technology

IPTV SDP parameters	DVB BCG
Connection Data at session level c=<network type> <address type> <connection address>	Not retrieved from SSF
<network type>	Not retrieved from SSF
<address type>	Not retrieved from SSF
<connection address>	Not retrieved from SSF
Media Announcements for content delivery m=<media> <port> <transport> <fmt list>	
<media>	"video" - Not retrieved from SSF
<port>	Client port- Not retrieved from SSF
<transport>	"RTP/AVP" or "UDP/H2221/MP2T" or "UDP/RAW/RAW depending on the transport layer used for the content, see clause 5.1.4.1
<fmt>	"33" - Not retrieved from SSF
Bandwidth	BitRatetype as defined in TS 102 822-3-1 [33], clause 6.3.5
Media Announcements for FEC delivery m=<media> <port> <transport> <fmt list>	see note
<media>	"application", not retrieved from SSF
<port>	Client port, not retrieved from SSF
<transport>	RTP/AVP
<fmt>	Dynamic payload type
a=rtpmap:<fmt><encoding_name/clock_rate>	<encoding_name/clock_rate> referring to the DVB-IP AL-FEC Base layer and is equal to: "vnd.dvb.iptv.alfec-base/90000"
Connection Data at media level c=<network type> <address type> <connection address>	
<network type>	Not retrieved from SSF
<address type>	Not retrieved form SSF
<connection address>	Not retrieved from SSF
NOTE: The FEC delivery can only be associated to an RTP delivered content.	

L.3.2 Mapping of CoD service for OMA BCAST technology

Table L.9: Mapping of SIP Parameters for CoD Service

IPTV SIP parameters	OMA BCAST
Request-URI	-

Table L.10: Mapping of SDP Parameters for CoD Service

IPTV SDP parameters	OMA BCAST
Connection Data at session level c=<network type> <address type> <connection address>	
<network type>	N/A UE local data
<address type>	N/A UE local data
<connection address>	N/A UE local data
Media Announcements for content delivery m=<media> <port> <transport> <fmt list>	
<media>	FFS
<port>	N/A UE local data
<transport>	FFS
<fmt list>	

Annex M (normative):
XML Schema for Service Attachment Information

This annex describes the XML schema for the service attachment information to be returned to UE by SDF. This XML schema is used when the service attachment information is transported via SIP Push mode and Pull mode as described in clauses 5.2.2.1 (Push mode) and 5.2.2.2 (Pull mode).

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">

    <xs:element name="SSFList" type="tSSFList">
        <xs:annotation>
            <xs:documentation>XML Body of the SDF SIP Notify Response</xs:documentation>
        </xs:annotation>
    </xs:element>


    <xs:complexType name="tSSFList">
        <xs:sequence>
            <xs:element name="SSF" type="tSSF" maxOccurs="unbounded"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
    </xs:complexType>


    <xs:complexType name="tSSF">
        <xs:sequence>
            <xs:element name="Description" type="tMultilingual" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="ServiceProvider" type="tSSFServiceProvider" minOccurs="0"/>
            <xs:element name="Pull" type="tSSFPull" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="Push" type="tSSFPush" minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="ID" type="tHexadecimal16bit" use="required"/>
        <xs:attribute name="Technology" type="xs:string" use="required"/>
        <xs:attribute name="Version" type="tVersion">
            <xs:annotation>
                <xs:documentation>The version number is incremented when one or more attributes of
the SSF element have changed, so that the receiver knows whether it should update its data or
not.</xs:documentation>
            </xs:annotation>
        </xs:attribute>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
    </xs:complexType>

    <xs:simpleType name="tVersion">
        <xs:restriction base="xs:integer">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="255"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="tSSFServiceProvider">
        <xs:sequence>
            <xs:element name="Name" type="tMultilingual" maxOccurs="unbounded"/>
            <xs:element name="Description" type="tMultilingual" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
        </xs:sequence>
        <xs:attribute name="DomainName" type="tDomain" use="required">
            <xs:annotation>
                <xs:documentation>It is recommended that the DomainName complies with the "preferred
name syntax" of RFC1034 clause 3.5</xs:documentation>
            </xs:annotation>
        </xs:attribute>
        <xs:attribute name="LogoURI" type="xs:anyURI" use="optional"/>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
    </xs:complexType>
```

```
<xs:simpleType name="tDomain">
    <xs:restriction base="xs:string">
        <xs:pattern value="((.|\n|\r)*)?(\.(.|\n|\r)*)+"/>
    </xs:restriction>
</xs:simpleType>


<xs:complexType name="tSSFPull">
    <xs:complexContent>
        <xs:extension base="tDataTypeList">
            <xs:attribute name="Location" type="xs:anyURI" use="required"/>
            <xs:anyAttribute namespace="##other" processContents="lax">
                <xs:annotation>
                    <xs:documentation>Extension attribute to define further
data</xs:documentation>
                </xs:annotation>
            </xs:anyAttribute>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>


<xs:complexType name="tSSFPush">
    <xs:complexContent>
        <xs:extension base="tDataTypeList">
            <xs:attribute name="IpVersion" type="tVersion" use="optional"/>
            <xs:attribute name="MulticastAddress" type="xs:string" use="required"/>
            <xs:attribute name="MulticastPort" type="xs:unsignedShort" use="required"/>
            <xs:attribute name="SourceAddress" type="xs:string" use="optional"/>
            <xs:anyAttribute namespace="##other" processContents="lax">
                <xs:annotation>
                    <xs:documentation> Extension attribute to define further data
                    </xs:documentation>
                </xs:annotation>
            </xs:anyAttribute>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>


<xs:complexType name="tDataTypeList">
    <xs:sequence maxOccurs="unbounded">
        <xs:element name="DataType">
            <xs:complexType>
                <xs:sequence minOccurs="0" maxOccurs="unbounded">
                    <xs:element name="Segment">
                        <xs:annotation>
                            <xs:documentation>Segments are used to logically separate Service
Selection information</xs:documentation>
                        </xs:annotation>
                        <xs:complexType>
                            <xs:attribute name="ID" type="tHexadecimal16bit" use="required"/>
                            <xs:attribute name="Version" type="tVersion" use="optional"/>
                        </xs:complexType>
                    </xs:element>
                </xs:sequence>
                <xs:attribute name="Type" type="tHexadecimal8bit" use="required">
                    <xs:annotation>
                        <xs:documentation> Specify the type of Service Selection Information
that is delivered by the SSF
                        </xs:documentation>
                    </xs:annotation>
                </xs:attribute>
            </xs:complexType>
        </xs:element>
    </xs:sequence>
</xs:complexType>


<xs:complexType name="tExtension">
    <xs:sequence>
        <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>


<xs:complexType name="tMultilingual">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute name="Language" type="tLanguage" use="required"/>
        </xs:extension>
    </xs:simpleContent>
```

```
        </xs:complexType>

        <xs:simpleType name="tLanguage">
            <xs:restriction base="xs:string">
                <xs:annotation>
                    <xs:documentation>
                        <definition xml:lang="en">ISO 639-2 Language code</definition>
                    </xs:documentation>
                </xs:annotation>
                <xs:minLength value="3"/>
                <xs:maxLength value="3"/>
            </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="tHexadecimal8bit">
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-9a-fA-F]{1,2}"/>
            </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="tHexadecimal16bit">
            <xs:restriction base="xs:string">
                <xs:pattern value="[0-9a-fA-F]{1,4}"/>
            </xs:restriction>
        </xs:simpleType>

</xs:schema>
```

Annex N (normative):
Service Package SDP Attribute

N.0   General

IETF RFC 4566 [42] generically defines SDP attributes as follows:

    attribute-fields =   *("a=" attribute CRLF)

    attribute =   (att-field ":" att-value) | att-field

This annex specifies several IPTV attributes as special cases of this ABNF syntax.

N.1   SDP attributes for BC Service

The SDP attribute a=bc_service is used to signal the BCServiceId (channel). The Augmented Backus-Naur Form [40]. specification of this SDP attribute is as follows.

    bc-service-attribute-field = "a=" bc-service-attribute CRLF

    bc-service-attribute = "bc_service" ":" BCServiceId

    BCServiceId =   *16(ALPHA / DIGIT / "-"); Zero up to 16 letters, digits or dashes

The following is an example of the SDP attribute for BC service identifier.

- a=bc_service:CCTV-5-Sports

N.2   SDP attributes for BC Service Package

The format of the a=bc_service_package attribute shall be the following:

- bc-service-package-attribute-field = "a=" bc-service-package-attribute CRLF

- bc-service-package-attribute = "bc_service_package" ":" BCPackage

- BCPackage = BCPackageId *1("[" mult-list "]") ; 0 or 1 mult_list

- BCPackageId = *16(ALPHA / DIGIT / "-"); Zero up to 16 letters, digits or dashes.

- mult-list = "mult_list:" source-unit *("/" source-unit) ; 1 or more source-unit

- source-unit = "[" 0*1("src_list:" source-addresses) "]" multicast-addresses "[" BCServiceId "]"

-   ; one BCService Id, one or more multicast addresses, and optionally one or more source addresses

- source-addresses = IPaddresses ; source addresses should be unicast IP addresses

- multicast-addresses = IPaddresses ; these should be multicast IP addresses

- IPaddresses = (IPaddress / IPaddress-range) *("," (IPaddress / IPaddress-range))

- IPaddress-range = IPaddress "-" IPaddress ; lowest and highest value of the IP address range

- IPaddress = IPv4address / IPv6address

BCServiceId is defined in clause N.1 (ABNF notation).

BCPackageId is the service package ID string.

IPv4 address and IPv6 address are specified in RFC 3261 [41], section 25.

NOTE: An essential correction to the ABNF of IPv6address is proposed in [i.7]. Implementers are advised to follow that guideline.

The following are examples of the SDP attribute for BC service package.

- a=bc_service_package:P25-News-Sports

- a=bc_service_package:P25-News-Sports[mult_list:[]225.10.3.0[CCTV-5-Sports]]

- a=bc_service_package:P25-News-Sports[mult_list:[src_list:192.168.10.1]225.10.3.0[CCTV-5-Sports]]

- a=bc_service_package:P25-News-Sports[mult_list:[src_list:192.168.10.1-192.168.10.255]225.10.3.0-225.10.4.255,FF02::2-FF02::8[CCTV-5-Sports]/[src_list:192.168.11.1,2001:cdba::3257:9652]FF02::10[CCTV-9-News]/[src_list:192.168.11.2]FF02::13[CCTV-8-News]/[]FF02::14[CCTV-6-Sports]]

As seen in this notation the multi_list parameter can contain one or more source_unit parameters with multicast addresses that can be separated with either "," or "-". When they are separated with "-" it means that it is a range of addresses. In addition there can optionally be a list of source addresses within the source unit parameter which is applicable for all the multicast addresses within the source unit parameter.

Annex O (normative):
Procedure for definition of new SSF technologies

New SSF technologies may be defined for support of the TISPAN IPTV services. Two technologies are defined so far in the present document, OMA BCAST and DVB-IPTV. This annex describes how new technologies (e.g. browser based technologies) can be defined by organizations willing to use the framework provided in the present document.

The following procedure specifies how to define new technologies:

1)   Definition of a technology. The Technology attribute of the XML schema defined in annex M is a string.

     The format of the Technology attribute shall be: <organization_name>_<subtechnology> where:

     -    The organization_name shall be the ICANN registered domain name of the organization that defines its technology.

     -    The subtechnology name identifies the SSF technology defined by the organization. It shall be unique within the context of the organization. It consists of one or more characters. Allowed characters are alphanumeric (i.e. 'a'-'z', 'A'-'Z', '0'-'9') plus the hyphen character ('-').

2)   Definition of the service attachment XML schema defined in annex M as applicable to the newly defined technology. The technology uses the XML structure to carry all relevant information, following the definition described in clause 5.2.2.3. For example, the DataType XML element is used to carry information which is meaningful only with regards to the technology. Example of completed XML schemas can be found in clause L.1.

3)   Definition of the service selection procedures associated with the newly specified technology, for the Pull mode and the Push mode, if used. Procedures defined within the present document may be reused.

4)   Mapping of the service selection information to the IPTV services defined in the present document. Below is the mapping that has to be completed (provided the IPTV service is defined with the technology).

     -    Mapping for BC Service (example is found in clause L.2).

     -    Mapping for CoD Service (example is found in clause L.3).

Annex P (normative): XML Schema for UE Profile

This XML Schema defines the UE information that is specified by UE during service attachment and may be carried within body of the SIP SUBSCRIBE request.

The format of the attributes UserEquipmentID and IPEncapsulation is outside of the scope of the present document.

The usage and personalization of the service selection data based on the attributes UserEquipmentClass and IPEncapsulation is outside of the scope of the present document.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
targetNamespace="urn:org:etsi:ngn:params:xml:ns:iptvueprofile"
xmlns:ns="urn:org:etsi:ngn:params:xml:ns:iptvueprofile"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:tva="urn:tva:metadata:2005"
 elementFormDefault="qualified" attributeFormDefault="unqualified">

<xs:import namespace="urn:tva:metadata:2005"
    schemaLocation="tva_metadata_3-1_v131.xsd"/>

    <xs:annotation>
        <xs:documentation xml:lang="en">
Defines the capabilities of the UE that is currently associated with the user
 </xs:documentation>
    </xs:annotation>

    <xs:element name="UEInformation" type="ns:tUEProfile"/>
        <xs:complexType name="tUEProfile">
            <xs:sequence>
                <xs:element name="UserEquipmentID" type="ns:tUEID"/>
                <xs:element name="UserEquipmentClass" type="ns:tUserEquipmentClass"/>
                <xs:element name="Resolution" type="ns:tResolution" minOccurs="0"/>
                <xs:element name="SupportedEncodings" type="ns:tSupportedEncodings" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="IPEncapsulations" type="ns:tIPEncapsulations" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="Extension" type="ns:tExtension" minOccurs="0"/>
                <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>

    <xs:simpleType name="tUEID" final="list restriction">
        <xs:annotation>
            <xs:documentation>
                <label xml:lang="en">User Equipment ID</label>
                <definition xml:lang="en">Unique Identifier for the UE(eg; Could be MAC address of
UE) </definition>
            </xs:documentation>
        </xs:annotation>

        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="16"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="tUserEquipmentClass" final="list restriction">
        <xs:annotation>
            <xs:documentation>
                <label xml:lang="en">User Equipment class</label>
                <definition xml:lang="en">Specifies the type of UE </definition>
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:enumeration value="STB"> </xs:enumeration>
            <xs:enumeration value="PC"> </xs:enumeration>
            <xs:enumeration value="Handset"> </xs:enumeration>
        </xs:restriction>

    </xs:simpleType>
```

```
<xs:complexType name="tResolution">
    <xs:attribute name="HorizontalSize" type="xs:integer">
        <xs:annotation>
            <xs:documentation>horizontal size in pixels of the screen</xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="VerticalSize" type="xs:integer">
        <xs:annotation>
            <xs:documentation>vertical size in pixels of the screen</xs:documentation>
        </xs:annotation>
    </xs:attribute>
    <xs:attribute name="Rotate" type="xs:boolean">
        <xs:annotation>
            <xs:documentation>set to TRUE if the screen can be rotated (horizontal becomes
vertical)</xs:documentation>
        </xs:annotation>
    </xs:attribute>
</xs:complexType>

<xs:complexType name="tSupportedEncodings">
    <xs:annotation>
        <xs:documentation>
            <label xml:lang="en">encodings</label>
            <definition xml:lang="en">Specifies the supported audio and video encodings (eg.
MPEG2,H264 AC3, AAC etc)</definition>
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="AudioEncoding" type="ns:tAudioEncoding" minOccurs="0"
maxOccurs="unbounded"/>
        <xs:element name="VideoEncoding" type="ns:tVideoEncoding" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="tAudioEncoding">
    <xs:annotation>
        <xs:documentation>
            <label xml:lang="en">Audio Encoding</label>
            <definition xml:lang="en">Specifies supported audio encoding properties</definition>
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="Encoding" type="tva:ControlledTermType"/>
        <xs:element name="Extension" type="ns:tExtension" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="tVideoEncoding">
    <xs:annotation>
        <xs:documentation>
            <label xml:lang="en">Video Encoding</label>
            <definition xml:lang="en"> Specifies supported video encoding properties
</definition>
        </xs:documentation>
    </xs:annotation>
    <xs:sequence>
        <xs:element name="Encoding" type="tva:ControlledTermType"/>
        <xs:element name="SupportedFrameRate" type="tva:FrameRateType" minOccurs="0"
maxOccurs="unbounded"/>
        <xs:element name="Extension" type="ns:tExtension" minOccurs="0"/>
        <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>

<xs:simpleType name="tIPEncapsulations" final="list restriction">
    <xs:annotation>
        <xs:documentation>
            <label xml:lang="en">encapsulation</label>
            <definition xml:lang="en">Specifies the IP encapsulation that is supported on device
(UDP/RTP, UDP/M2TS, UDP/RTP/M2TS)
            </definition>
        </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
        <xs:minLength value="0"/>
        <xs:maxLength value="16"/>
```

```
                </xs:restriction>
        </xs:simpleType>

        <xs:complexType name="tExtension">
                <xs:sequence>
                        <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
                </xs:sequence>
        </xs:complexType>

</xs:schema>
```

Example of XML document conforming to this structure. The SupportedEncoding field carries the list of the several coding format that the device can handle. The Name element is optional, it is presented herein for user readability.

```
<?xml version="1.0" encoding="UTF-8"?>
<UEInformation xmlns="?" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <UserEquipmentID>STB-dc14b2</UserEquipmentID>
    <UserEquipmentClass>STB</UserEquipmentClass>
    <Resolution Horizontal="720" Vertical="576" Rotate="FALSE"/>
    <SupportedEncodings>
        <AudioEncoding>
            <Encoding href="urn:mpeg:mpeg7:cs:AudioCodingFormatCS:2001:3">
                <Name>MPEG-1 Audio</Name>
            </Encoding>
        </AudioEncoding>
        <AudioEncoding>
            <Encoding href="urn:mpeg:mpeg7:cs:AudioCodingFormatCS:2001:5.4">
                <Name>MPEG-4 Main Audio Profile</Name>
            </Encoding>
        </AudioEncoding>
        <AudioEncoding>
            <Encoding href="urn:mpeg:mpeg7:cs:AudioCodingFormatCS:2001:5.5">
                <Name>MPEG-4 High Quality Audio Profile</Name>
            </Encoding>
        </AudioEncoding>
        <AudioEncoding>
            <Encoding href="urn:dvb:metadata:cs:AudioCodecCS:2007:1">
                <Name>MPEG-4 DVB Audio</Name>
            </Encoding>
        </AudioEncoding>
        <VideoEncoding>
            <Encoding href="urn:mpeg:mpeg7:cs:VisualCodingFormatCS:2001:1">
                <Name>MPEG-1 Video</Name>
            </Encoding>
        </VideoEncoding>
        <VideoEncoding>
            <Encoding href="urn:mpeg:mpeg7:cs:VisualCodingFormatCS:2001:2.2">
                <Name>MPEG-2 Video Main Profile</Name>
            </Encoding>
        </VideoEncoding>
        <VideoEncoding>
            <Encoding href="urn:dvb:metadata:cs:VideoCodecCS:2007:1.1">
                <Name>H264 Baseline Profile</Name>
            </Encoding>
            <SupportedFrameRate>30</SupportedFrameRate>
        </VideoEncoding>
        <VideoEncoding>
            <Encoding href="urn:dvb:metadata:cs:VideoCodecCS:2007:1.2">
                <Name>H264 Main Profile</Name>
            </Encoding>
            <SupportedFrameRate>30</SupportedFrameRate>
            <SupportedFrameRate>24</SupportedFrameRate>
        </VideoEncoding>
    </SupportedEncodings>
    <IPEncapsulation>M2TS/UDP,M2TS/RTP</IPEncapsulation>
</UEInformation>
```

Annex Q (informative):
Combination of SIP and RTSP protocols for content on demand

The SIP procedures described in clause 5 influence which of the two RTSP methods described in clause 7 to be used. Figures Q.1 and Q.2 specify the decision logic of the UE and the MCF respectively.

Q.1   User Equipment (UE) side RTSP method decision logic

Figure Q.1 shows the UE-side RTSP method decision logic.
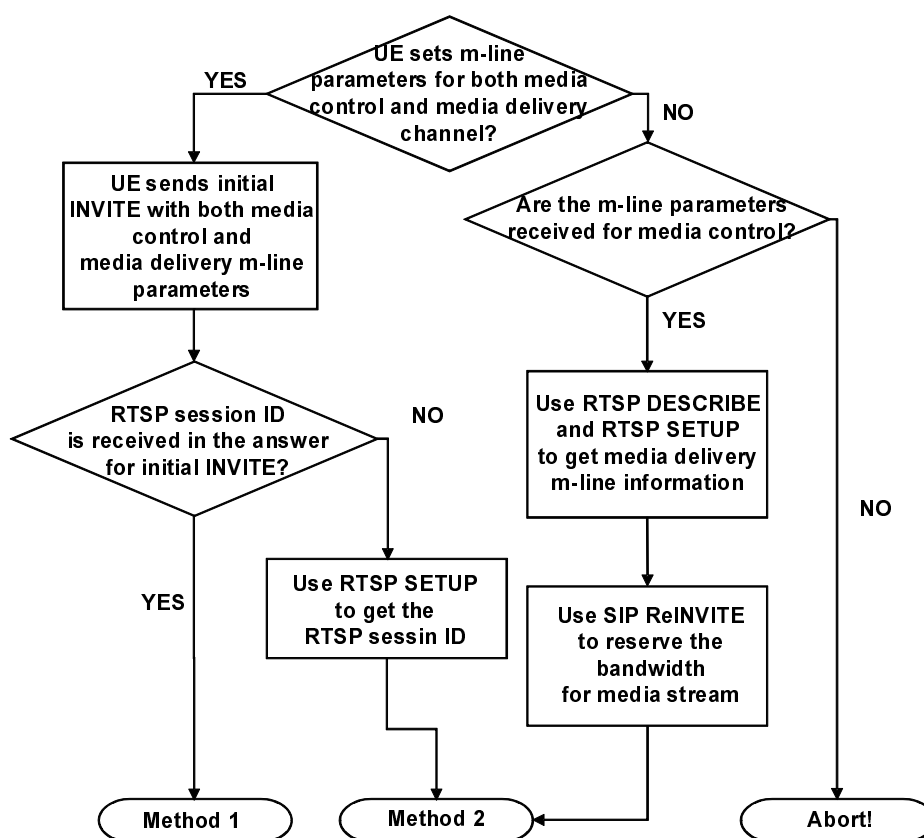

Figure Q.1: UE-side RTSP method decision logic

Q.2   Media Control Function (MCF) side RTSP method decision logic

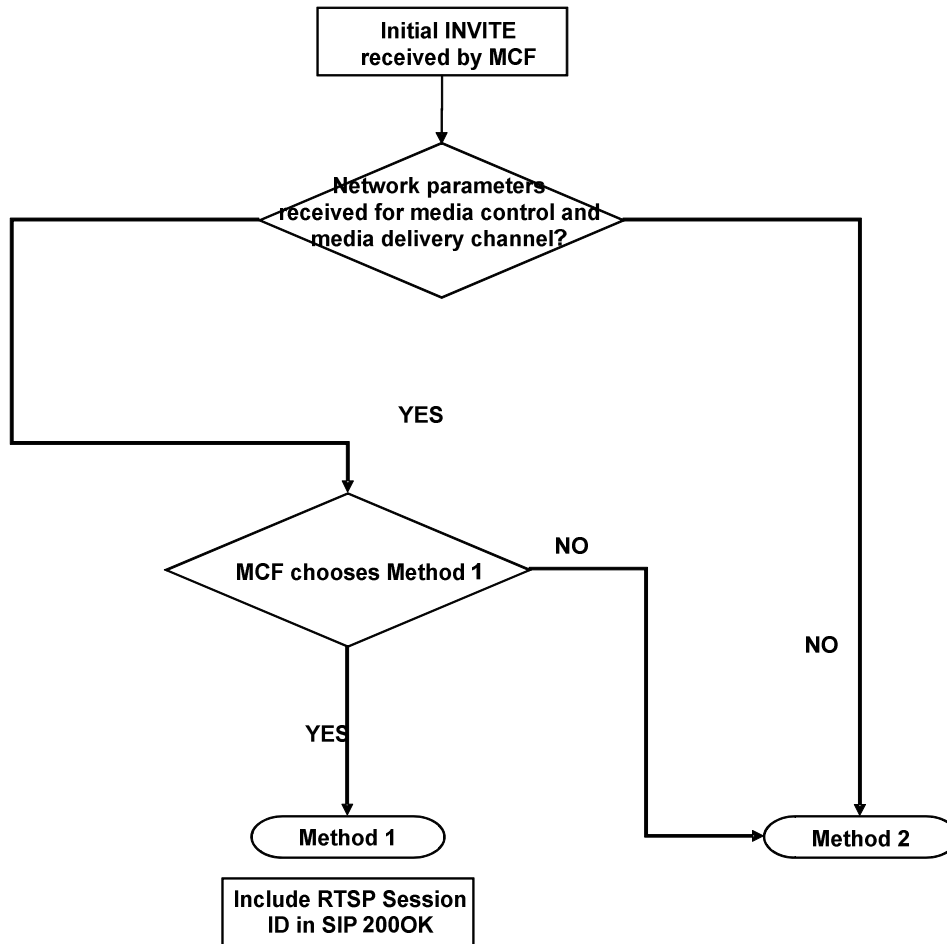Figure Q.2 shows the MCF-side RTSP method decision logic.

Figure Q.2: MCF-side RTSP method decision logic

Annex R (informative):
Initial Filter Criteria

Beyond the method name, (SUBCRIBE, INVITE, etc.), the following elements may be used a service trigger point to build initial filter criteria enabling Application Servers to be involved in the processing of IPTV procedures:

- The event name of a SUBSCRIBE request.

- The contents of the Accept header in a SUBSCRIBE request (e.g. MIME types).

- The contents of the P-Preferred-Service header or the Accept-Contact header (i.e. ICSI).

- The Request-URI, in which case the content tag will typically contain an Extended Regular Expressions (ERE) as defined in clause 9 in IEEE 1003.1-2004 [i.5] such that any Request-URI that includes a particular pattern (e.g. a domain name) matches the criteria.

The actual list of criteria depends on whether the public user identity is dedicated to the IPTV service or not.

The following example illustrates the case of an IFC used to trigger an application server that provides the SDF function only.

```
<InitialFilterCriteria>
    <Priority>0</Priority>
    <TriggerPoint>
        <ConditionTypeCNF>0</ConditionTypeCNF>
        <SPT>
            <ConditionNegated>0</ConditionNegated>
            <Group>0</Group>
            <Method>INVITE</Method>
        </SPT>
        <SPT>
            <ConditionNegated>0</ConditionNegated>
            <Group>0</Group>
            <RequestURI>@iptvdiscovery.homedomain.com$</RequestURI>
        </SPT>
    </TriggerPoint>
    <ApplicationServer>
        <ServerName>sip:SDF-AS1@homedomain.com</ServerName>
        <DefaultHandling>0</DefaultHandling>
    </ApplicationServer>
</InitialFilterCriteria>
```

Annexes S to X:
Void (defined in v3.y.z)

Annex Y (normative):
Support for an Application profile for SIP User Agents

This annex defines the normative text for a new application profile for a SIP User agent in addition to the 3 existing profiles currently defined in the SIP Config framework.

Y.1   Introduction

SIP User Agents require profile data to function properly. A mechanism to obtain profile data is specified by the Framework for SIP User Agent Profile Delivery I-D.ietf-sipping-config-framework [39]. The framework separates profile data into three categories, termed profile types, local-network, device and user. Each profile type deals with a specific data set, e.g. the device profile type is used to obtain device-specific configuration. The framework also allows for future extensions to support additional profile types. The present document specifies one such extension to support an additional profile type, application. This can be used by user agents for requesting profile data for one or more applications that they support.

Y.2   Motivation

The motivation for an independent application profile type can be demonstrated using the scenario described in figure Y.1. The scenario considers a device (not shown) that supports three applications (X, Y, Z). It also considers two users (A, B). Applications X and Y are user-specific, i.e. restricted to known end-users, where as Application Z can be used by any user (e.g. Weather Information).
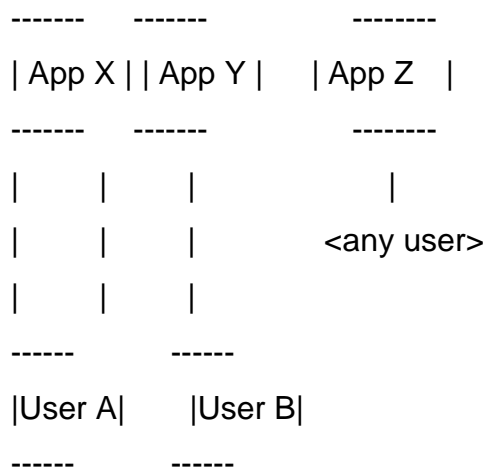
```
-------     -------              --------

| App X | | App Y |     | App Z   |

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

|       |     |                    |

|       |     |           <any user>

|       |     |

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

|User A|        |User B|

------          ------
```

Figure Y.1: Motivation for application profile type

Each application needs specific profile data to function. For instance, an application such as Video on Demand (VoD) would require VoD server information, codecs for rendering, minimum bandwidth requirements etc. It may also have requirements specific to users, such as rating and cost restrictions (parental controls). Further, the presence of an application does not always mean that it is enabled. For example, a Service Provider may disable VoD for certain subscription levels.

Profile data related to such applications, especially those that are unrelated to specific users, would need to be retrieved for successful operation. This profile data may be retrieved during device boot-up if it is configured to do so, e.g. via the device profile. The profile data can also be retrieved dynamically, e.g. when the application is enabled. Such profile data does not qualify under any existing profile types specified by the SIP UA configuration framework, viz. local-network, device and user. The only exception is application profile data that is specific to users, which can be provided via the user profile type. Thus the need for an additional profile type specific to applications.

Y.3   Overview

Y.3.1   Profile Type Definition

The present document specifies a new profile type for use with the SIP UA configuration framework. The name of the profile type is 'application'. The present document also defines an additional event header parameter for use with the application profile type. This parameter is termed "appids".

Y.3.2   Parameter 'appids'

The "appids" parameter describes the application profiles being requested. Its value is an identifier for the application, or a comma-separated list of such identifiers. Each application identifier is a unique value defined by the application specification, along with the profile content, and is in the form of a URI (RFC 4395 [i.8]), preferably a URN (RFC 3406). This parameter value SHOULD be provided in the SUBSCRIBE request for the 'application' profile-type only, along with the other three parameters (vendor, model and version) specified in I-D.ietf-sipping-config-framework [39]. This parameter is useful to the PDS to affect the profile provided. Behavior when the "appids" parameter is omitted is currently undefined and treated as an error. Future standards action may specify this behavior.

In the following ABNF defining the syntax, EQUAL and DQUOTE are defined in RFC 3261 [41]:

```
appids            = "appids=" list-of-app-ids
list-of-app-ids   = DQUOTE app-id *("," app-id) DQUOTE
app-id            = 1*(subset-print-chars)
subset-print-chars= %x21 /%x23-25 / %x27-29 / %x2D-3C / %x3E-7E
                    ;All printable characters except ", =, &, *, +
                    ;comma or white-space characters.
```

The "appids" parameter appears in the Event header of the NOTIFY request to specify the actual application the NOTIFY belongs to. In the initial NOTIFY following a SUBSCRIBE, the appids parameter SHOULD list all applications obtained in the subscription, which may be a subset of the applications listed in the SUBSCRIBE. The only case in which the "appids" parameter MAY be omitted from the initial NOTIFY is when only one application was listed in the SUBSCRIBE. If the SUBSCRIBE included an "appids" parameter, the "appids" parameter of the initial NOTIFY MUST NOT list applications not present in the SUBSCRIBE. If the parameter contains a list of applications, the order in the appids parameter MUST be the same as followed in the body (see below). Subsequent NOTIFY requests on a single application subscription MAY omit the "appids", since the application context is implied by the subscription dialog.

Y.3.3   Summary of Event Header

The following are example Event headers which may occur in SUBSCRIBE requests. The examples are not intended to show complete SUBSCRIBE requests.

```
Event: ua-profile;profile-type=application;
       vendor="vendor.example.com";model="Z100";version="1.2.3"

Event: ua-profile;profile-type=application;
       vendor="vendor.example.com";model="Z100";version="1.2.3";
       appids="myapplication"

Event: ua-profile;profile-type=application;
       vendor="vendor.example.com";model="Z100";version="1.2.3";
       appids="myapplication1,myapplication2,myapplication3"
```

The following are example Event headers which may occur in NOTIFY requests.   These example headers are not intended to be complete NOTIFY requests.

```
Event: ua-profile;profile-type=application

Event: ua-profile;profile-type=application;appids="myapplication1"

Event: ua-profile;profile-type=application;
```

```
        appids="myapplication2,myapplication3"
```

The table shows the use of Event header parameters in SUBSCRIBE requests for the application profile type:

```
        profile-type || application
        ===========================
        appids       ||     s
        vendor       ||     o
        model        ||     o
        version      ||     o
        effective-by ||

        m - mandatory
        s - SHOULD be provided
        o - optional
```

The table shows the use of Event header parameters in NOTIFY requests for the application profile type:

```
        profile-type || application
        ===========================
        appids       ||     s
        vendor       ||
        model        ||
        version      ||
        effective-by ||     o
```

Y.3.4   SUBSCRIBE Bodies

The present document defines an enhancement to the I-D.ietf-sipping-config-framework [39] by specifying a use for the SUBSCRIBE request body. If the appids parameter contains a single application identifier, the SUBSCRIBE message body MAY contain a single body part appropriate for the application. If the appids parameter contains a list of applications, the body of the SUBSCRIBE MAY contain a "multipart/mixed" content-type, with appropriate body parts for each of the applications for which the UA is subscribing.

The body parts MUST be in the same order in which they are listed in the "appids" parameter, and if any body parts are present, all applications must have a corresponding part, even if empty.

If present in the SUBSCRIBE request, the body SHALL be used by the application-specific PDS to tailor the NOTIFY responses to the subscribing UA for each of the applications listed. The meaning and form of the SUBSCRIBE body is specified by each application.

> NOTE: An alternative to requiring all applications to have body parts if any do, and to using "empty" parts where a body part is not needed, is to employ Content-Description to name the appid to which the part corresponds.

Y.3.5   NOTIFY Bodies

The NOTIFY message body contains a content type specific to the requested application (this type must be listed in the Accept header of the SUBSCRIBE). If the subscription is for multiple applications, the initial NOTIFY message body will contain a "multipart/mixed" content-type, and the ordering of the body-parts corresponds to the ordering of the "appids" application values.

Y.4   Example Usage

```
SUBSCRIBE sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB
           @example.com  SIP/2.0
   Event: ua-profile;profile-type=application;appids="sampleapplication"
   From: sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB
         @example.com;tag=1234
   To: sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB@example.com
   Call-ID: 3573853342923422@192.0.2.44
   CSeq: 2131 SUBSCRIBE
   Contact: sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB
         @example.com
     ;+sip.instance="<urn:uuid:00000000-0000-0000-0000-123456789AB0>"
   Via: SIP/2.0/TCP 192.0.2.41;
     branch=z9hG4bK6d6d35b6e2a203104d97211a3d18f57a
   Accept: message/external-body, application/x-z100-device-profile
   Content-Length: 0
```

Annex ZZ (informative):
Change history

Date	WG Doc.	CR	CRRev	CAT	Title/Comment	Current Version	New Version
30-05-08	17bTD204r3	001		F	Corrections for BC service	2.1.0	2.1.1
30-05-08	17bTD207r4	002		F	Improvement of the text for Session initiation of BC service	2.1.0	2.1.1
02-07-08	18WTD090r1	003		F	Acquiring of Request URI for RTSP DESCRIBE Message	2.1.1	2.1.2
02-07-08	18WTD127r1	004		F	Corrections on parameters for BC Service	2.1.1	2.1.2
02-07-08	18WTD136r1	005		F	Fixing XCAP section references	2.1.1	2.1.2
02-07-08	18WTD081r3	006		F	Correction of Mapping parameters for COD	2.1.1	2.1.2
07-08					TB approval of CRs 001 to 006	2.1.2	2.2.0
26-09-08	18bTD171r1	006		F	Correction of DVB IPTV ALFEC parameter	2.2.0	2.2.1
26-09-08	18bTD258r1	007		F	Fixing cross reference for Service Attachment	2.2.0	2.2.1
26-09-08	18bTD270r1	008		F	Correction of SSFAttachment XML schema (Annex M)	2.2.0	2.2.1
26-09-08	18bTD197r2	009		F	Use of CoD offset in RTSP PLAY	2.2.0	2.2.1
26-09-08	18bTD186r3	010		F	Modification of the text for acquiring of RTSP-URL	2.2.0	2.2.1
26-09-08	18bTD180r1	011		F	Correction of SDP formatting	2.2.0	2.2.1
05-11-08	19WTD117r1	012		F	Correction of BC session initiation at SCF side	2.2.1	2.2.2
05-11-08	19WTD214r1	013		F	Update of ICSI value	2.2.1	2.2.2
13-11-08					CRs 006 to 013 TB approved and clean-up by ETSI Secretariat	2.2.2	2.3.0
26-02-09	20WTD222r1	014		F	Resolving potential RTSP-SDP parameter conflicts	2.3.0	2.3.1
26-02-09	20WTD232r1	015		F	App_ref changed to icsi-ref	2.3.0	2.3.1
					CRs 014 and 015 TB approved at TISPAN#20, move of TS 183 060 to normative references clause and publication	2.3.1	2.4.1
27-05-09					Republication to insert back URIs unintentionally removed during publication of v2.4.1	2.4.1	2.4.2
29-09-09	22WTD68r1	016		F	Agreed contribution 22WTD68r1, some XML corrections to the TS document of version 2.4.2.	2.4.2	2.4.3
22-12-09	23WTD213r1	017		D	Modifying the value of maxLength attribute of tCurrentBCProgramID and tCurrentContentID elements in Annex E.	2.4.3	2.4.4
13-04-10	TISPAN03(10)0131r1	018		F	Modify text in 5.4.1.5 to populate From and To Headers for COD SAD signaling in line with COD session initiation signaling.	2.4.4	2.4.5
15-04-10	TISPAN03(10)0148r2	019		F	In Annex K, XML schema as to be modified: • Bookmark type is timestamp and shall not be minOccurs=0 • BCServiceId shall not be minOccurs=0	2.4.5	2.6.2 (To keep the version consistent to WG3 Report)
15-09-10	TISPAN03(10)0213r2	20		F	Rapporteur changes	2.7.0	2.7.1
15-09-10	TISPAN03(10)0241	21		F	New Normative Annex to replace draft-channabasappa-sipping-app-profile-type-02	2.7.0	2.7.1
					Some editorial refinements by Rappoteur	2.7.1	2.7.2
10-28-10	TISPAN03(10)0273r1	22		F	Reference to Sipping config. v18	2.7.2	2.7.3
12-14-2010	TISPAN03(10)0295r2	23	1	F	Annex_N_SDP_Correction	2.7.3	2.7.4
					publication	2.7.4	2.8.1

History

Document history		
V2.1.0	June 2008	Publication
V2.4.1	May 2009	Publication
V2.4.2	June 2009	Publication
V2.8.1	February 2011	Publication