BCAST Distribution System Adaptation - 3GPP/MBMS
Candidate Version 1.2 – 14 Jan 2014

Open Mobile Alliance
OMA-TS-BCAST_MBMS_Adaptation-V1_2-20140114-C

Contents

Figures

Tables

1. Scope

This document specifies how the BCAST 1.2 enabler is implemented over a specific BDS (BCAST Distribution System).

The BCAST 1.2 Enabler supports the global interoperability among different BCAST Distribution Systems, and can also be adapted according to the characteristics of BCAST Distribution Systems for BCAST 1.2 enabler implementation over a certain BDS. In this document, two types of adaptation are presented.

All functions of the BCAST 1.2 Enabler can be implemented over the specific BDS with minimal adaptation. This is referred to as "generic adaptation", which can be applied for any kind of BDS.

The underlying BDS may already have a method for a function defined in the BCAST 1.2 Enabler. This specification defines the cases where this method selected in the underlying BDS is utilised for the BCAST function also. In this case BCAST functionality is adapted, as described in this document. This is referred to as "BDS specific adaptation".

This is further explained in Section 4 Introduction.

2. References

2.1 Normative References

[3GPP TS 22.246] "Multimedia Broadcast/Multicast Service (MBMS) user services; Stage 1", 3rd Generation Partnership Project, Technical Specification 3GPP TS 22.246 Release 8,
URL:http://www.3gpp.org/

[3GPP TS 23.003] "Numbering, Addressing and Identification"; 3rd Generation Partnership Project, Technical Specification 3GPP TS 23.003 Release 8,
URL:http://www.3gpp.org/

[3GPP TS 23.246] "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description", 3rd Generation Partnership Project, Technical Specification 3GPP TS 23.246 Release 8,
URL:http://www.3gpp.org/

[3GPP TS 25.331] "Radio resource control(RRC); Protocol specification", 3rd Generation Partnership Project, Technical Specification 3GPP TS 25.331 Release 8,
URL:http://www.3gpp.org/

[3GPP TS 25.346] "Introduction of the Multimedia Broadcast Multicast Service(MBMS) in the Radio Access Network (RAN); Stage 2", 3rd Generation Partnership Project, Technical Specification 3GPP 25.346 Release 8,
URL:http://www.3gpp.org/

[3GPP TS 25.401] "UTRAN overall description", 3rd Generation Partnership Project, Technical Specification 3GPP TS 25.401 Release 8,
URL:http://www.3gpp.org/

[3GPP TS 26.346] "Multimedia Broadcast/Multicast Service (MBMS), Protocols and codecs", 3rd Generation Partnership Project, Technical Specification 3GPP TS 26.346 Release 8,
URL:http://www.3gpp.org/

[3GPP TS 33.246] "3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)", 3rd Generation Partnership Project, Technical Specification 3GPP 33.246 Release 8,
URL:http://www.3gpp.org/

[BCAST12-Distribution] "File and Stream Distribution for Mobile Broadcast Services ", Open Mobile Alliance™, OMA-TS-BCAST_Distribution-V1_2,
URL:http://www.openmobilealliance.org/

[BCAST12-ServContProt] "Service and Content Protection for Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_SvcCntProtection-V1_2,
URL:http://www.openmobilealliance.org/

[BCAST12-Services] "Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_Services-V1_2,
URL:http://www.openmobilealliance.org/

[BCAST12-SG] "Service Guide for Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_ServiceGuide-V1_2,
URL:http://www.openmobilealliance.org/

[DRM20-Broadcast-Extensions] "OMA DRM v2.0 Extensions for Broadcast Support", Open Mobile Alliance™, OMA-TS-DRM-XBS-V1_2,
URL:http://www.openmobilealliance.org/

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1,
URL:http://www.openmobilealliance.org/

[RFC 3711] "The Secure Real-time Transport Protocol (SRTP)", M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman,
URL: http://www.ietf.org/rfc/rfc3711.txt

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997,
URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997,
URL:http://www.ietf.org/rfc/rfc2234.txt

[RFC4234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005, URL:http://www.ietf.org/rfc/rfc4234.txt

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/

2.2 Informative References

[3GPP TS 23.060] "General Packet Radio Service (GPRS); Service description; Stage 2", 3rd Generation Partnership Project, Technical Specification 3GPP TS 23.060 Release 8, URL:http://www.3gpp.org/

[OMADICT] "Dictionary for OMA Specifications", Version x.y, Open Mobile Alliance™, OMA-ORG-Dictionary-Vx_y, URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

BCAST Distribution System	A system typically but not necessarily containing the ability to transmit the same IP flow to multiple Terminal devices simultaneously. A BCAST Distribution System (BDS) typically uses techniques that achieve efficient use of radio resources. A BDS consists of Network functionality up to the IP layer and optional Service Distribution/Adaptation functionality above the IP layer. Most BDSs support broadcast/multicast distribution in the network. Some BCAST Distribution Systems have the capability to deliver the IP flows in the network via unicast.
Cell_Group_ID	Identifier for a group of cells sharing protocol entities for point-to-multipoint MBMS transmission, as described in [3GPP TS 25.346] (section 5.2.2) and [3GPP TS 25.331] (section 10.2.16h)
Cell_ID	Cell Identifier as defined in [3GPP TS 25.401] chapters 6.1.5

3.3 Abbreviations

BCMCS	Broadcast Multicast Service (3GPP2)
BDS	BCAST Distribution System
DVB-H	Digital Video Broadcasting - Handheld
IMB	Integrated Mobile Broadcast (3GPP)
MBMS	Multimedia Broadcast Multicast Service (3GPP)
MBSFN	MBMS over a Single Frequency Network
MKI	Master Key Identifier
MSK	MBMS Service Key
MTK	MBMS Traffic Key
OMA	Open Mobile Alliance
SG	Service Guide
SRTP	Secure Real-time Transport Protocol
TDD	Time Division Duplexing

4. Introduction

This technical specification specifies how the OMA Mobile Broadcast Services (BCAST) Enabler can be implemented in 3GPP MBMS network.

4.1 Version 1.0

BCAST ERP 1.0 has two modes of adaptation for MBMS:

1. Generic adaptation over an underlying MBMS IP transmission network

   In this mode, this Technical Specification explains how the BCAST Enabler has access to the IP transport layer so that BCAST services can be provided from BCAST Network entities to BCAST Terminal. Furthermore, this allows a common behaviour across multiple BCAST enabled BCAST Distribution Systems (BDSes)

   However, in generic adaptation mode, it may be impossible to share broadcast services with a native MBMS terminal (a terminal that supports MBMS as specified by 3GPP) due to differences between the technologies selected in the specific BDS and the Generic adaptation. For example, file delivery mechanisms may be different or service and content protection mechanisms may be different. In practice this means file delivery sessions and streaming sessions are most likely to be provided in parallel in order to cater for BCAST Terminals and MBMS terminals.

2. BDS specific adaptation to MBMS functionality

   In this mode, this Technical Specification explains how various BCAST functionalities are adapted in a MBMS IP transmission network taking in consideration the specific technical aspects of the underlying BCAST Distribution System (BDS). In this mode, it is possible that broadcast services can be shared between BCAST terminals and MBMS terminals. Hence BCAST Network entities and MBMS servers can provide services to both types of terminals.

   For example, file delivery mechanisms and protection mechanisms would be those defined by 3GPP MBMS specifications. In practice this means file delivery sessions and streaming sessions would cater for both BCAST terminals and MBMS terminals, without the need for providing sessions in parallel.

Note that the purpose of BDS specific adaptation is to enable sharing a service between BCAST terminals and native BDS terminals. In contrast, generic adaptation allows to share a BCAST service across different BDSs. As described above, BCAST Network entities and BCAST Terminals will be able to handle the two types of adaptation, providing maximum deployment flexibility for the Service Provider. This allows BCAST terminal to work automatically in both situations, as signalling is provided to indicate to the terminal the type of adaptation provided. As not all underlying BDS functionality is adopted by BCAST, BCAST Enabler may be adapted to both types, i.e. BDS specific adaptation (optimized for BDS) for certain functions whilst using generic adaptation (BCAST-specific functionality) for other functions.

Note that in the context of ‘MBMS IP transmission network’, the ‘IP transmission’ means IP multicast or IP unicast between BM_SC and UE.

4.2 Version 1.1

In BCAST 1.1 ERP, TS-MBMS adaptation has three main changes.

- Version of some normative references was updated according to the provision of the latest versions.
- Technical description of BDS specific entry points was updated.
- MBSFN Integrated Mobile Broadcast (IMB) was added. IMB is one of enhanced technologies in the latest version of 3GPP MBMS. The detail information of MBMS is provisioned at 3GPP Release 8 [3GPP TS 25.346]. IMB provides capabilities for broadcast services in 3G TDD bands in a way that is integrated with existing 3G FDD unicast technology.

4.3 Version 1.2

In BCAST 1.2 ERP, the change in TS-MBMS adaptation is only editorial, to refer to the BCAST1.2 specifications.

5. Overview of MBMS (Informative)

MBMS (Multimedia Broadcast / Multicast Service) has been developed by 3GPP as mobile broadcast technology. It is a mechanism for delivering the same content to several users more efficiently over existing cellular networks than using dedicated channel and will be available to both the 2.5G (GSM / EDGE) radio access network and the 3G radio access network. MBMS follows a toolbox approach, where different applications can be delivered over a combination of different delivery methods (namely download and streaming) and bearers (point-to-point bearers and MBMS bearers, providing multicast/broadcast transmission down to radio layer), as shown in Fig. 1.

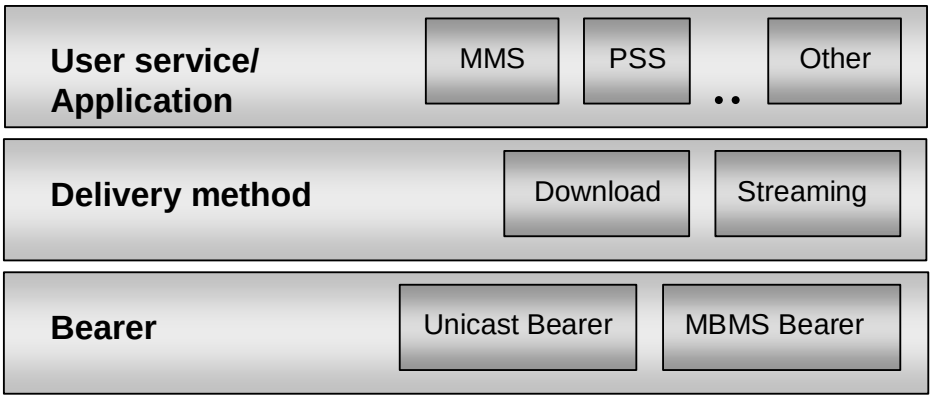

Figure 1: Functional Layers for MBMS User Service

MBMS bearers (shown at the bottom in Fig. 1) provide the mechanism by which IP data is transported. MBMS bearers as defined in [3GPP TS 23.246] and [3GPP TS 22.146] are used to transport multicast and broadcast traffic in an efficient one-to-many manner and are the foundation of MBMS-based services. MBMS bearers may be used jointly with unicast PDP contexts in offering complete service capabilities. An MBMS bearer (identified by IP multicast address and APN) might be used in providing data to more than one MBMS download or streaming session ([3GPP TS 22.246], section 5). The different session are identified by different UDP ports.

When delivering MBMS content to a receiving application one or more delivery methods are used. The delivery layer provides functionality such as security and key distribution, reliability control by means of forward-error-correction techniques and associated delivery procedures such as file-repair, and delivery verification. Two delivery methods are defined, namely download and streaming. Delivery methods may be added beyond release 8. Delivery methods may use MBMS bearers and may make use of point-to-point bearers through a set of MBMS associated procedures.

In addition to the MBMS bearer there are also service layer functions specified for MBMS. This includes the definition of MBMS user services, media codecs, formats and transport/application protocols using MBMS. The MBMS User service enables applications. Different applications impose different requirements when delivering content to MBMS subscribers and may use different MBMS delivery methods. As an example a messaging application such as MMS would use the download delivery method while a streaming application such as PSS would use the streaming delivery method. An MBMS user service is an entity that is used in presenting a complete service offering to the end-user and allowing him to activate or deactivate the service. It is typically associated with short descriptive material presented to the end-user, which would potentially be used by the user to decide whether and when to activate the offered service.

A single service entity can contain multiple distinct multimedia objects or streams, which may need to be provided over various MBMS download or MBMS streaming sessions. A download session or a streaming session is associated with its MBMS bearers and a set of delivery method parameters specifying how content is to be received on the mobile side. A set of one or more MBMS bearers can be used for delivering data as part of an MBMS download or streaming session. As an example, the audio and visual part of video stream can be carried on separate MBMS bearers. However, it is recommended to

transfer MBMS download and/or streaming sessions, which belong to the same MBMS user service on the same MBMS bearer service.

Figure 2 depicts the MBMS network architecture showing MBMS related entities involved in providing MBMS user services.

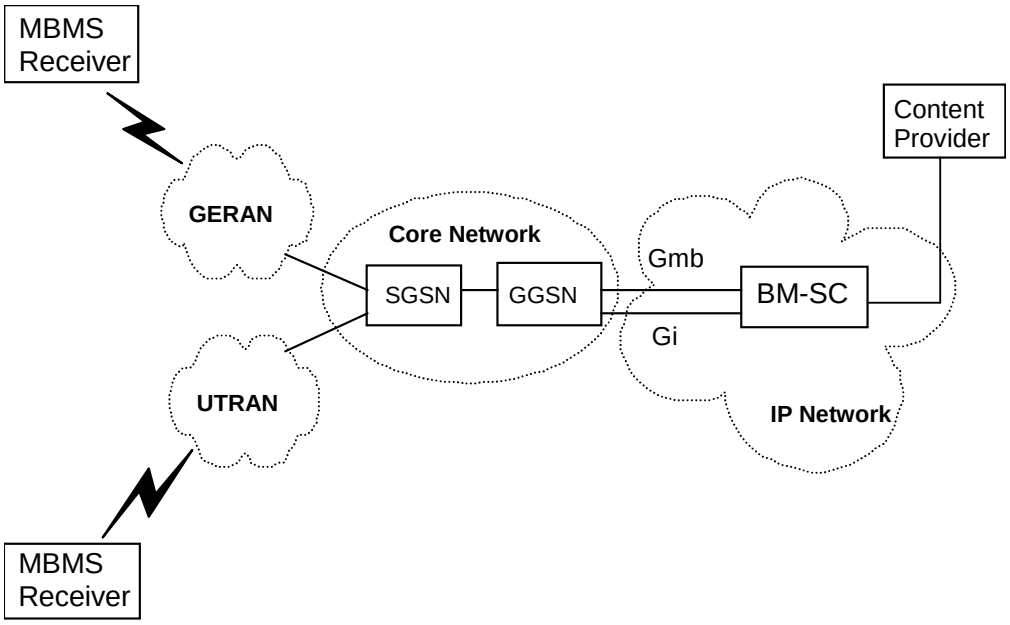

Figure 2: MBMS network architecture model

MBMS User Service architecture is based on an MBMS receiver on the UE (i.e., terminal) side and a BM-SC on the network side. Details about the BM-SC functional entities are given in Fig. 3.

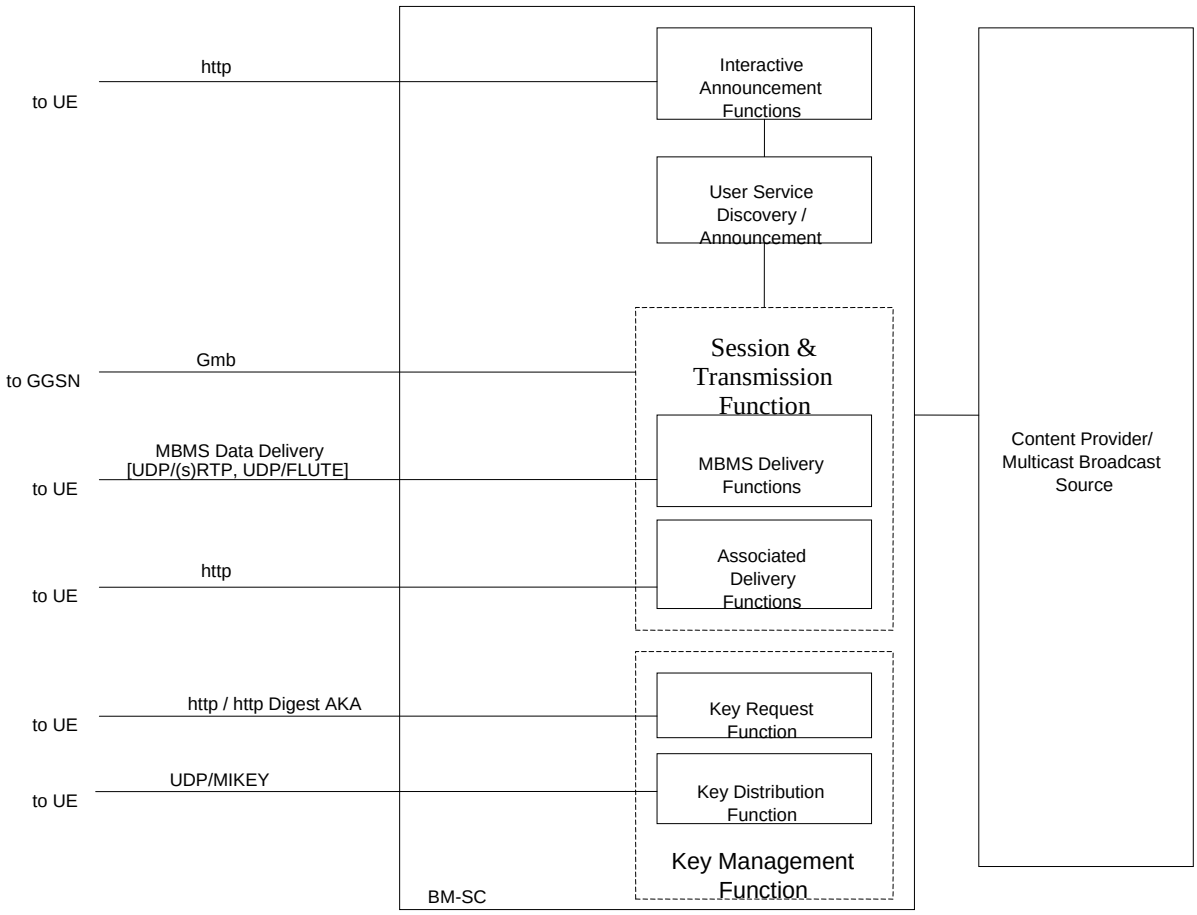

Figure 3: BM-SC sub-functional structure

The Session and Transmission function is further subdivided into the MBMS Delivery functions and the Associated Delivery functions. The BM-SC and UE may exchange service and content related information either over point-to-point bearers or MBMS bearers whichever is suitable. To that end the following MBMS procedures are provided:

- User Service Discovery / Announcement providing service description material to be presented to the end-user as well as application parameters used in providing service content to the end-user.
- MBMS-based delivery of data/content from the BM-SC to the UE over IP multicast or over IP unicast.
  - The data/content is optionally confidentiality and/or integrity protected
  - The data/content is optionally protected by a forward error correction code
- Key Request and Registration procedure for receiving keys and key updates.
- Service specific key distribution procedures whereby the BM-SC distributes service specific key material required to access service data and delivered content.
- Associated Delivery functions are invoked by the UE in relation to the MBMS data transmission. The following associated delivery functions are available:

- File repair for download delivery method used to complement missing data.
- Delivery verification and reception statistics collection procedures.

The interfaces between internal BM-SC functions are outside the scope of 3GPP.

The Content Provider/Multicast Broadcast Source (see Fig. 3) may provide discrete and continuous media, as well as service descriptions and control data, to the BM-SC to offer services via MBMS broadcast- and multicast bearer services at a time. An MBMS User Service may use one or several MBMS delivery methods simultaneously. The Content Provider/Multicast Broadcast Source may also be a 3rd Party Content Provider/Multicast Broadcast Source.

The Content Provider/Multicast Broadcast Source function may reside within the broadcast service provider's network or may be provided from outside the broadcast service provider's network. The Content Provider/Multicast Broadcast Source can also configure the Session and Transmission functions (e.g. delivery or associated delivery). The interface between the Content Provider/Multicast Broadcast Source and the BM-SC is outside the scope of 3GPP.

There exist several realizations of the MBMS bearer. MBSFN Integrated Mobile Broadcast (IMB) is an optional realization of MBMS bearers which was introduced in 3GPP Release 8 [3GPP TS 25.346]. IMB provides capabilities for broadcast services in 3G TDD bands in a way that is integrated with existing 3G FDD unicast technology.

The following specification describes the MBMS service requirements:

3GPP TS 21. 246	Multimedia Broadcast/Multicast Service user services
3GPP TS 22.146	Multimedia Broadcast/Multicast Service; Stage 1

The following specification describes the MBMS architecture:

3GPP TS 23.246	Multimedia Broadcast Multicast Service; Architecture and Functional Description
3GPP TS 25.346	Introduction of the Multimedia Broadcast/Multicast Service (MBMS) in the Radio Access Network (RAN); Stage 2
3GPP TS 43.246	Multimedia Broadcast/Multicast Service (MBMS) in the GERAN; Stage 2

The following specifications and reports describe service layer aspects of MBMS:

3GPP TS 26.346	MBMS; Protocols and Codecs
3GPP TR 26.946	MBMS user service guidelines
3GPP TS 32.273	MBMS Charging
3GPP TS 33.246	3G Security; Security of MBMS

6. Generic Adaptation over MBMS' IP transmission network

This Section describes how BCAST specifications (namely [BCAST12-Services], [BCAST12-SG], [BCAST12-ServContProt], [BCAST12-Distribution] and [DRM20-Broadcast-Extensions]) are used over an MBMS network. The provisions in this Section thus complement the ones in the generic specifications so that BCAST services can be distributed over MBMS IP transmission network, without re-using the MBMS functionality and hence without the ability for sharing services with native MBMS terminals (unlike the adaptation specified in Section 7 below).

The sentence "as defined by BCAST Enabler specifications" is a shorthand notation that indicates both BCAST server and terminal SHALL respect the relevant BCAST specification (listed above).

Generic adaptation MAY be supported by BCAST Network entities and SHALL be supported by BCAST Terminal.

All normative statements in this specification are only applicable in the case OMA BCAST services are distributed over 3GPP MBMS.

6.1 Access to the MBMS IP layer

3GPP MBMS specification SHALL apply. See chapter 5 for a list of specifications.

6.2 MBMS adaptation related to OMA-TS-BCAST_Services

6.2.1 Interaction

Note that MBMS itself specifies the broadcast/multicast capability of a cellular 3GPP network. It does not itself include an interaction channel, but it is assumed that MBMS is always part of a cellular network that provides interaction channel capabilities. For purposes of MBMS adaptation, the "MBMS interaction channel" should be understood as a dedicated signalling connection established between the BCAST network entities (BSM/BSDA) and the BCAST Terminal (e.g. as specified by [3GPP TS 23.060]). The MBMS interaction channel may be realized using access-independent transport protocols (e.g. HTTP, TCP, UDP) over an IP bearer and/or access-dependent mechanisms (e.g. telephony, SMS, MMS). Since the interaction channel exists and is used in MBMS, the BCAST Terminal SHALL support interaction defined by [BCAST12-Services].

The Terminal SHOULD support SMS for service interaction.

6.2.2 Service Provisioning

As defined by [BCAST12-Services].

6.2.3 Terminal Provisioning

As defined by [BCAST12-Services].

Note: SG bootstrap information is provisioned using Terminal Provisioning.

6.2.4 Notification

The specification in section 5.14 of [BCAST12-Services] SHALL apply.

When using 3GPP MBMS as the underlying BCAST Distribution System the Notification functionality is enabled as specified in [BCAST12-Services].

6.3 MBMS adaptation related to OMA-TS-BCAST_ServiceGuide

6.3.1 Service Guide Delivery over Broadcast Channel

As defined by [BCAST12-SG].

6.3.2 Service Guide Delivery over Interaction Channel

As defined by [BCAST12-SG].

6.3.3 Service Guide Encoding

As defined by [BCAST12-SG].

6.3.4 Session Description

As defined by [BCAST12-SG].

6.3.5 Service Guide Data Model

As defined by [BCAST12-SG].

6.3.5.1 CellTargetArea in MBMS

See section 7.3.5.1.

6.3.5.2 BDSSpecificEntryPointInfo definition

Section 5.4.1.5.2 of [BCAST12-SG] specifies how SGDDs can include the definition of SGEntryPoints over BCAST BDS broadcast channels. Each broadcast SGEntryPoint (i.e. SG Announcement Channel) in a BCAST BDS is declared partially by generic parameters (such as 'srcIpAddress', 'port', etc.) and partially by BDS-specific parameters, provided in each BDS Adaptation TS via the extension by derivation of the abstract type of BDSSpecificEntryPointInfo element.

For the MBMS BDS, the abstract type of BDSSpecificEntryPointInfo element is derived as follows:

Name	Type	Category	Cardinality	Description	Data Type
BDSSpecificEntryPointInfo	E5	NM/TM	0..1	The placeholder for the supplementary information that is required in order to retrieve the broadcast SG entry point in BCAST BDS, i.e. in MBMS BDS for the present specification.	complexType deriving from abstract type of BDSSpecificEntryPointInfo element
BCBearer	E6	NM/TM	0..1	MBMS bearer parameter used for reception of a broadcasted SG (both SG Announcement Channel and SG Delivery Channels). This element SHALL be present in case the mode of the MBMS bearer is Broadcast Mode, and SHALL be absent otherwise. Contains the following attributes: TMGI isCounting	

TMGI	A	NM/TM	1	Temporary Mobile Group Identity (TMGI) as defined in [3GPP TS 23.003]. An MBMS Bearer service is uniquely identified by the TMGI. The value is encoded as a decimal number which in hexadecimal form represent octets 3 to 8 of the TMGI information element structure defined in [3GPP TS 24.008]. Octet 3 is the most significant octet.	string
isCounting	A	NM/TM	1	MBMS Counting Information as defined in [3GPP TS 25.413]. It indicates whether the RAN level counting procedures is applicable or not for the MBMS broadcast mode. The value “true” corresponds to the information element value of “counting” and the value “false” corresponds to the information element value “not counting”. It is OPTIONAL for the terminal to act on to the information provided in this attribute, e.g., if it has received the counting information out-of-band of the Service Guide.	boolean

6.3.6 Service Guide Bootstrap for SG Delivery over Broadcast Channel

The entry point information according to [BCAST12-SG] section 6.1.1 SHALL be provisioned to the terminal using OMA DM as specified in [BCAST12-Services] and using the BCAST MO specified in [BCAST12-Services].

6.3.7 Service Guide Bootstrap for SG Delivery over Unicast Channel

The entry point information , i.e. the BSDA URL, SHALL be provisioned to the terminal using OMA DM as specified in [BCAST12-Services] and using the BCAST MO specified in [BCAST12-Services].

6.4 MBMS adaptation related to OMA-TS-BCAST_SvcCntProtection and OMA-TS-DRM_XBS

As defined by [BCAST12-ServContProt] and [DRM20-Broadcast-Extensions].

6.4.1 DRM Profile

The Terminal MAY support service protection using the DRM Profile. IF the DRM Profile based service protection is supported, the Terminal SHALL support the reception and processing of keys transported in OMA DRM 2.0 Rights Objects (ROs).

The Terminal MAY support content protection using the DRM Profile as defined in [BCAST12-ServContProt].

The Terminal MAY support extensions for service protection and content protection of broadcast-only devices as defined in [DRM20-Broadcast-Extentions].

6.4.2 OMA BCAST Smartcard Profile

The Terminal SHALL support service protection using the Smartcard profile as defined in [BCAST12-ServContProt] section 4.1 and 6.

The Terminal MAY support content protection using the Smartcard Profile as defined in [BCAST12-ServContProt].

6.5 MBMS adaptation related to OMA-TS-BCAST_Distribution

6.5.1 File Distribution

As defined by [BCAST12-Distribution].

The FEC RAPTOR scheme MAY be supported by the BSDA and SHALL be supported by terminal as specified in [3GPP TS 26.346] Annex B (there called MBMS FEC).

6.5.1.1 Signalling of parameters with FLUTE

FLUTE FDT Instances SHALL comply with [BCAST12-Distribution], with the following restrictions:

- FEC-OTI-FEC-Encoding-ID attribute SHALL be included in <FDT-Instance> element ;
- Content-Type attribute SHALL be included in <FDT-Instance> element ;
- Content-Length attribute SHALL be included in each <File> element.

6.5.1.2 FDT Instance schema

FLUTE FDT Instances SHALL comply with BCAST FDT Instance schema defined in [BCAST12-Distribution].

In addition, MBMS adaptation restrictions defined in section 6.5.1.1 SHOULD be enforced in BCAST FDT Instances, using the ‘xsi:type’ attribute as follows:

- Type of <FDT-Instance> element SHOULD be ’FDT-InstanceType-BdsMbmsDvb’ from BCAST FDT namespace ;
- Type of each <File> element SHOULD be ’FileType-BdsMbmsDvb’ from BCAST FDT namespace.

6.5.2 Associated Delivery Procedures

As defined by [BCAST12-Distribution].

6.5.3 Stream Distribution

As defined by [BCAST12-Distribution], with the following exceptions:

Terminals SHALL implement the streaming services as defined in [3GPP 26.234].

The FEC RAPTOR scheme MAY be supported by the BSDA and SHALL be supported by the terminal as specified in [3GPP TS 26.346] Annex B (there called MBMS FEC).

Note: See annex G of [3GPP TS 26.346] for a description of some methods to improve channel tune-in and switching times for stream distribution when using REC RAPTOR scheme.

6.5.4 Media codecs

While BCAST Enabler does not define support of any media codecs, BCAST Terminals SHALL follow support of media codecs as defined in 3GPP MBMS specifications. See Section .7.5.4.

7. BCAST enabler adapting to MBMS functionality

This Section describes which BCAST technologies are chosen from MBMS and how the BCAST Functions are adapted for MBMS network. The adaptation can be implemented via restrictions and extensions of the BCAST specifications (namely OMA-TS-BCAST_Services, OMA-TS-BCAST_ServiceGuide, OMA-TS-BCAST_SvcCntProtection, OMA-TS-BCAST-Distribution, and OMA-TS-DRM-XBS). The provisions in this section take precedence over the ones in the BCAST specifications to enable BCAST services using MBMS adopted functionality to be distributed over MBMS network allowing service sharing for MBMS terminals.

BDS Specific adaptation MAY be supported by BCAST Network entities and SHALL be supported by BCAST Terminal.

All normative statements in this specification are only applicable in the case OMA BCAST services are distributed over MBMS network.

7.1 Access to the MBMS IP layer

See Section 6.1.

7.2 MBMS adaptation related to OMA-TS-BCAST_Services

7.2.1 Interaction

As defined by [BCAST12-Services].

For specific adaptation, MBMS is understood as MBMS user service, thus including interaction capability e.g. for file repair.

In this context, the “MBMS interaction channel” SHALL be understood as a dedicated signalling connection established between the BCAST network entities (BSM/BSDA) and the BCAST Terminal. The MBMS interaction channel SHALL be supported using access-independent transport protocols (e.g. HTTP, TCP, UDP, IP) over an IP bearer and/or access-dependent mechanisms (e.g. telephony, SMS, MMS). Since the interaction channel exists and is used in MBMS, the BCAST Terminal SHALL support interaction defined by [BCAST12-Services].

The Terminal SHOULD support SMS for service interaction.

7.2.2 Service Provisioning

As defined in [BCAST12-Services].

7.2.3 Terminal Provisioning

As defined in [BCAST12-Services].

Note: SG bootstrap information is provided using Terminal Provisioning.

7.2.4 Notification

See section 6.2.4.

7.3 MBMS adaptation related to OMA-TS-BCAST_ServiceGuide

7.3.1 Service Guide Delivery over Broadcast Channel

As defined by [BCAST12-SG].

If the Service guide is delivered over the broadcast channel, it SHALL be delivered using an MBMS download session and using FLUTE as the transport protocol.

7.3.2 Service Guide Delivery over Interaction Channel

As defined by [BCAST12-SG].

7.3.3 Service Guide Encoding

As defined by [BCAST12-SG].

The Service Guide Delivery Unit carrying a set of fragments for Service Guide SHOULD be compressed for the delivery using the GZIP algorithm.

7.3.4 Session Description

The Session Description fragment SHALL be provided using either SDP or the session description as defined by MBMS user service bundle description (MBMS-USBD) as specified in [3GPP TS 26.346] section 5.2. MBMS-USBD refers to one or several SDP description(s), formatted according to [BCAST12-SG] section 5.1.2.5 and [BCAST12-ServContProt] section 10.

Note: The min-buffer-time attribute appears also in MBMS. However, it appears as parameter of “mbms-repair” SDP attribute and serves a different purpose. Therefore is not recommended to use it for signaling Initial buffering time when used for stream distribution over MBMS.

MBMS USBD SHALL NOT contain security description.

7.3.5 Service Guide Data Model

As defined by [BCAST12-SG].

7.3.5.1 CellTargetArea/BDSLocationID in MBMS

Underlying MBMS functionality is re-used, as explained below.

OMA BCAST Service Guide allows describing the target area for Service and Content and specific SG request from terminal based upon its BDSLocationID as specified in [BCAST12-SG] in terms of BDS-specific cell identification. In the case of MBMS, the value of “CellTargetArea” element of “TargetArea” element and “BDSType” as specified in [BCAST12-SG] is expressed as defined in [BCAST12-SG], but can only assume the following values for “type”: 1 (3GPP Cell Global Identifier), 2 (3GPP Routing Area Identifier), 3 (3GPP Location Area Identifier), 4 (3GPP Service Area Identifier), 5 (3GPP MBMS Service Area Identity).

7.3.6 Service Guide Bootstrap

See sections 6.3.6. and 6.3.7

7.4 MBMS adaptation related to OMA-TS-BCAST_SvcCntProtection and OMA-TS-DRM_XBS

The Terminal SHALL support service protection using the Smartcard Profile using (U)SIM as defined in [BCAST12-ServContProt] sections 4.1 and 6.

For streaming services, the CS ID map type subfield SHALL be set to “SRTP-ID” in LTKMs as defined in [3GPP TS 33.246].

The Terminal MAY support service protection using the DRM Profile as defined in [BCAST12-ServConProt].

As defined by Section 9 Encryption Protocols of [BCAST12-ServContProt] with the constraints indicated below in Section 7.4.1.1.

7.4.1 Content Encryption

The specification in Section 9 "Encryption Protocols" of [BCAST12-ServContProt] with the constraints indicated below in Section 7.4.1.1 SHALL apply.

SRTP is the common content encryption method included in [3GPP TS 33.246] and [BCAST12-ServContProt].

If IPsec or ISMACryp are used, BCAST specifications apply i.e. without constraints.

7.4.1.1 Constraints on content encryption

This section sets specific restrictions on the use of SRTP relative to what is described in [BCAST12-ServContProt] so that compliance to [3GPP TS 33.246] is achieved, i.e., so that a common encryption layer is achieved, allowing both BCAST Terminals and MBMS Terminals to access the same encrypted stream.

SRTP

A 128 bit Master Key SHALL be used, as per BCAST and MBMS specifications.

A 112 bit Master Salt SHALL be used.

MKI length SHALL be 6 bytes to provide compatibility with DRM Profile, Smartcard Profile and MBMS.

The Table below summarises constraints required for SRTP to allow BCAST and MBMS Terminals to share access to a common encrypted data stream.

Parameter	DRM Profile STKM Key ID	Smartcard Profile 3GPP MBMS MIKEY
TEK ID for SRTP	MKI (6 bytes)	MKI = MSK ID || MTK ID 6 bytes
MK for SRTP	128 bits	128 bits
MS for SRTP	112 bits	112 bits

Table 1: Encryption parameters for shared BCAST/MBMS SRTP encrypted content stream

7.4.1.2 SRTP encryption: Sharing a protected media stream between BCAST and 3GPP- MBMS terminals

This subsection describes how a number of broadcast service providers can share an SRTP protected media stream while maintaining compatibility with the 3GPP MBMS specifications. The solution allows MBMS only terminals to share a protected media stream with BCAST terminals using the DRM or Smartcard Profile.

The use of SRTP is mandatory with respect to 3GPP MBMS [3GPP TS 33.246]. This means that IPSec and ISMACryp protected media streams, which are supported in BCAST, can not be shared with MBMS only terminals.

A protected media stream is encrypted using a single set of Traffic Encryption Keys (TEKs). Broadcast service providers wishing to share a protected media stream must provide their subscribers with STKMs containing the TEKs required for decryption of the content. The STKMs must also contain an identifier to allow the terminal to determine which protected packets the TEK can be used to decrypt.

The Master Key Identifier (MKI) identifies the correct Traffic Encryption Key (TEK) to use to decrypt the protected media stream. The MKI is included in the SRTP packets of the protected media stream and SHALL be used as defined in [RFC 3711].

According to [3GPP TS 33.246] the MKI is formatted as follows where MSK is the MBMS Service Key and MTK is the MBMS Traffic Key:

MKI = MSK ID || MTK ID

The MSK ID and MTK ID are constructed as follows:

- MSK ID (4 bytes): is split into 2 sub parameters: the Key Group part and the Key Number part.
  - Key Group part (2 bytes): is used to group keys toghether in order to allow the efficient management of stored MSKs.
  - Key Number part (2 bytes): is used to distinguish MSKs that have the same Key Domain ID and Key Group part.
- MTK ID (2 bytes): is used to distinguish MTKs that have the same MSK ID and Key Domain ID.

In BCAST the SEK is the functional equivalent of the MBMS MSK and the TEK is the functional equivalent of the MTK. The SEK ID and TEK ID are constructed as per the MSK ID and MTK ID respectively.

If several broadcast service providers share the same SRTP protected media stream, distributed by a single BSDA, the MKI value transmitted in SRTP packets will also be shared.

This in turn means that the SEK IDs (MSK IDs) and TEK IDs (MTK IDs) included in the STKMs transmitted by each of the broadcast service providers must be the same. For the SEK ID (MSK ID) this means that both the Key Group part and the Key Number part must be the same.

The requirement to synchronise the SEK IDs (MSK IDs) and TEK IDs (MTK IDs) between broadcast service providers implies that the update frequency of both SEKs (MSKs) and TEKs (MTKs) must also be synchronised.

[3GPP TS 33.246] mandates that when a new MSK is taken into use, the MTK ID of the first MTK protected by that MSK must be set to an initial value greater than zero. Additionally, for each new MTK protected by a specific MSK, the value of the MTK ID must be greater than the value used for the previous MTK. In most situations the practical choice for the initial value and the MTK ID increment will be one. However, this does not prevent the use of different values. If the MTK ID is used as part of the MKI for a protected media stream which is shared between broadcast service providers addressing BCAST and MBMS only terminals, the rules defined in [3GPP TS 33.246] for the update of MTK IDs must be respected by the BSDA.

In summary to share a protected media stream and maintain compatibility with MBMS:

- In order for the terminal to identify the correct TEK (MTK) to use to decrypt the protected media stream, all broadcast service providers must distribute STKMs that include the SEK ID (MSK ID) and TEK ID (MTK ID) used to generate the MKI value used by the shared SRTP stream.
- The MKI must be constructed as follows: MKI = (MSK ID || MTK ID)
- A single set of TEKs (MTKs) must be used. It follows that the STKMs provided by each broadcast service provider for the shared protected media stream will necessarily contain the same TEKs (MTKs) and that the TEK (MTK) update period will be the same for all broadcast service providers.
- Broadcast service providers don't have to use the same SEKs (MSKs) to protect their STKMs. However, broadcast service providers must all update their SEKs (MSKs) at the same time and use the same SEK IDs.
- The BSDA must use the following SRTP parameters values:

Parameter / Profile	DRM Profile	Smartcard Profile
MKI	same as Smartcard	MSK ID || MTK ID (6 bytes)
MK	same as Smartcdard	random 128 bits
MS	same as Smartcard	random 112 bits or NULL
derivation rate r	0	0 or non-zero

Table 2: BCAST SRTP Parameters – sharing common stream with MBMS terminals

It should be noted that even though SEK (MSK) update periods must be synchronised between the broadcast service providers sharing a protected media stream, each broadcast service provider can independently define key validity periods for the SEKs (MSKs) that they issue to their users. The key validity periods defined by the broadcast service provider cannot

exceed the lifetime of the SEK (MSK). SEK (MSK) key validity periods can be updated without updating the SEK (MSK) , cf. section 6.5.3 [3GPP TS 33.246]. The SEK ID (MSK ID) must be changed when a new SEK (MSK) is used.

The following can then be considered:

Assuming that there is a single shared protected media stream, the SEK renewal period is one month, and that there are two broadcast service providers (A and B):

- Subscribers from broadcast service provider A can access the shared media stream using SEK_A1 to decrypt the TEKs in the STKMs sent by broadcast service provider A.Broadcast service provider A issues its subscribers with LTKMs that include SEK_A1, with a key validity period of one week and a SEK ID = SEK_1. Broadcast service provider A can issue a second LTKM to provide their subscribers with an additional week's access to the protected media stream. In this case the second LTKM would contain the same SEK (SEK_A) and the same SEK_ID (SEK_1) but with a key validity period extended to cover the additional week.
- Subscribers from broadcast service provider B can access the shared media stream using SEK_B1 to decrypt the TEKs in the STKMs sent by broadcast service provider B, Broadcast service provider B issues its subscribers with LTKMs that include SEK_B1, with a key validity period of one month and a SEK ID = SEK_1.

In the above example, the value of the SEK_ID is shared between the broadcast service providers, while theSEK and the key validity periods are different. Using different key validity periods allows the broadcast service providers to offer their subscribers customised service offerings related to the same shared protected media stream.

Broadcast service providers A and B have to periodically update the SEK used to protect the STKMs. SEK updates must be completed at the same time by A and B. Furthermore, A and B must use the same SEK_ID for each new SEK.

With the above solution, different use cases are possible, depending on the number of BSDAs and key management systems implemented by the Broadcast service providers.

7.4.1.2.1 A single SRTP stream shared by three broadcast service providers using the Smartcard Profile

The first use case deals with sharing a single protected SRTP stream between three broadcast service providers implementing the Smartcard Profile for key management. Figure 4 outlines this use case.

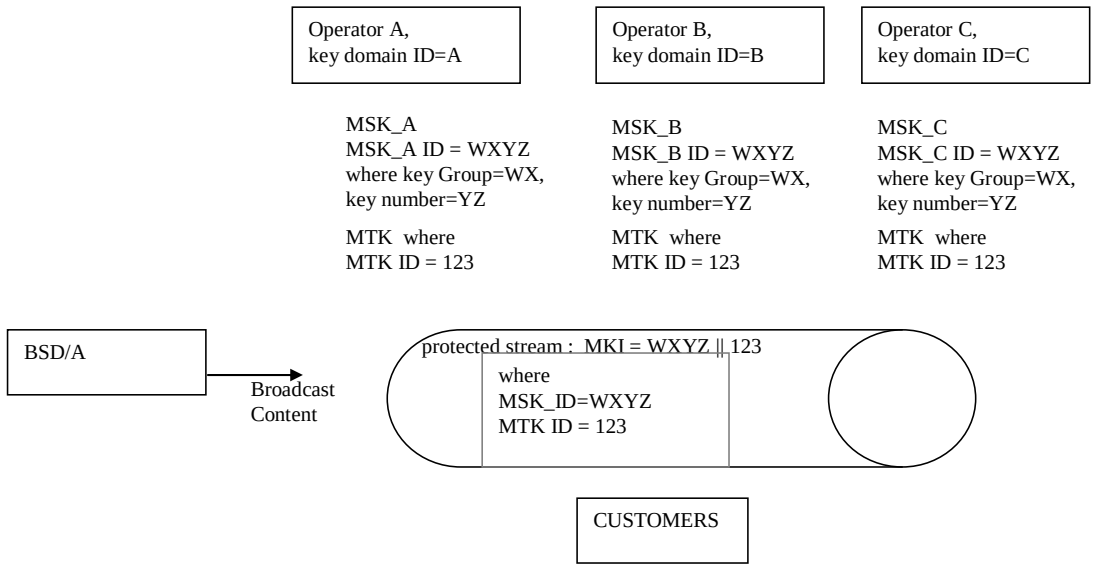

Figure 4: Sharing a single SRTP stream between three broadcast service providers implementing the Smartcard Profile for key management

Figure 4 illustrates how a single protected media stream distributed by the can be shared between broadcast service providers A, B and C, all of whom implement the Smartcard Profile.

Broadcast service providers A, B and C generate their own SEKs, SEK_A, SEK_B and SEK_C respectively. The SEKs are all different. The update frequency of the SEKs is synchronised amongst broadcast service providers. The identifier used for each of the broadcast service provider'sSEK is synchronised. For SEK_A, SEK_B and SEK_C the MKI used is WXYZ || 123 (SEK_ID ||TEK ID. Each broadcast service provider distributes the common TEK, in an STKM protected by the relevant SEK, over the broadcast bearer. Each broadcast service provider broadcasts their own STKM stream.

The BSDA broadcasts the protected media stream encrypted with the common TEK. Upon reception of the protected media stream the Terminal retrieves the correct TEK to decrypt the content based on the SEK ID and the TEK ID extracted from the MKI.

7.4.1.2.2 Two SRTP streams, provided by two different BSDAs and shared by three broadcast service providers all using the Smartcard Profile

The second use case illustrates how two SRTP protected media streams, provided by different BSDAs (BSDA_1 and BSDA_2), can be shared between three broadcast service providers implementing the Smartcard Profile. Figure 5 outlines this use case.

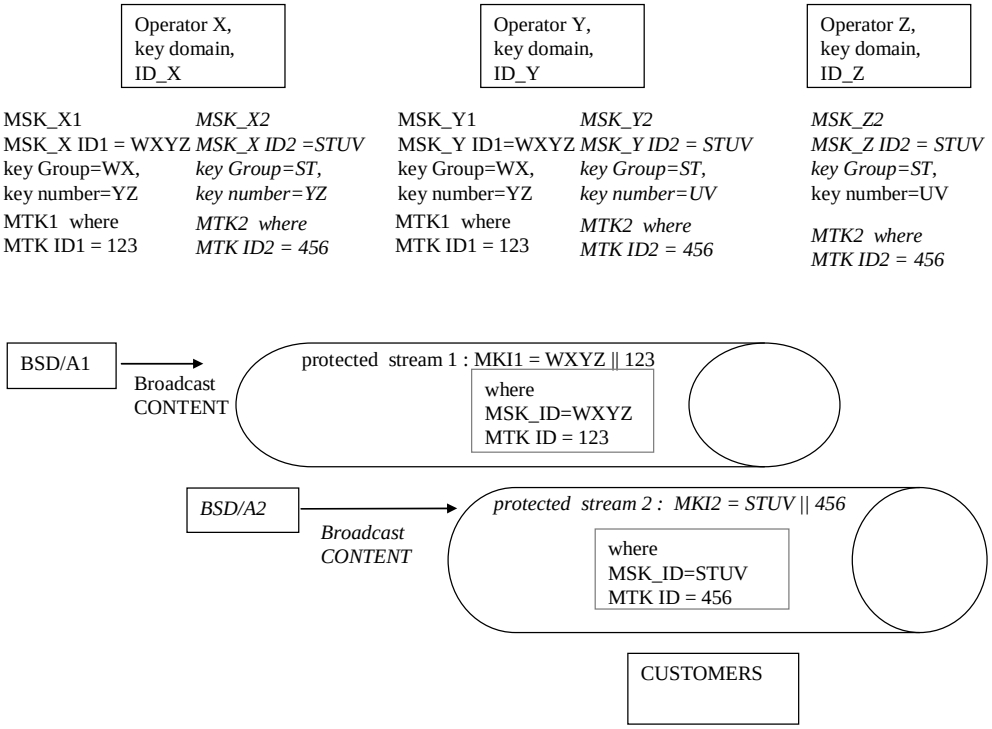

Figure 5: Sharing two SRTP streams between three broadcast service providers using the Smartcard Profile for key management

Figure 5 illustrates how two SRTP protected streams provided by BSDA_1 and BSDA_2 can be shared between three broadcast service providers X, Y and Z, all of whom implement the Smartcard Profile. The protected media stream broadcast by BSDA_1 is shared by X and Y while the protected media stream broadcast by BSDA_2 is shared by X,Y and Z.

Broadcast service providers X, Y and Z generate their own SEKs for each of the protected media streams that they are sharing, SEK_X1/SEK_X2, SEK_Y1/SEK_Y2 and SEK_Z2. The SEKs generated by each broadcast service provider are different, as are SEKs used by X and Y for the protected media streams provided by BSDA_1 and BSDA_2.

The SEK IDs used for each protected media is synchronised between the broadcast service provders, e.g. SEK_ID = "WXYZ" is used for stream 1 and SEK ID = "STUV" is used for stream 2. The update frequencies of the SEKs for each protected media stream are synchronised between broadcast service providers. Each protected media stream uses a common TEK and TEK ID, e.g. for TEK_1, which is used for stream 1, the TEK_ID = "123 ", while for TEK_2, which is used for stream 2, the TEK_ID = "456". Each broadcast service provider distributes the common TEKs (TEK_1 and TEK_2), in an STKM protected by the relevant SEK, over the broadcast bearer.. Each broadcast service provider broadcasts their own STKM stream.

BSDA_1 and BSDA_2 broadcast the protected media stream encrypted with the corresponding common TEK, e.g. TEK_1 for stream 1 and TEK_2 for stream 2. Upon reception of the protected media stream the terminal retrieves the TEK required to decrypt the content based on TEK ID and MTK ID extracted from the MKI.

7.4.1.2.3 A single SRTP stream shared by broadcast service providers using the DRM profile and (U)SIM and (R-)UIM/CSIM variants of the Smartcard profile

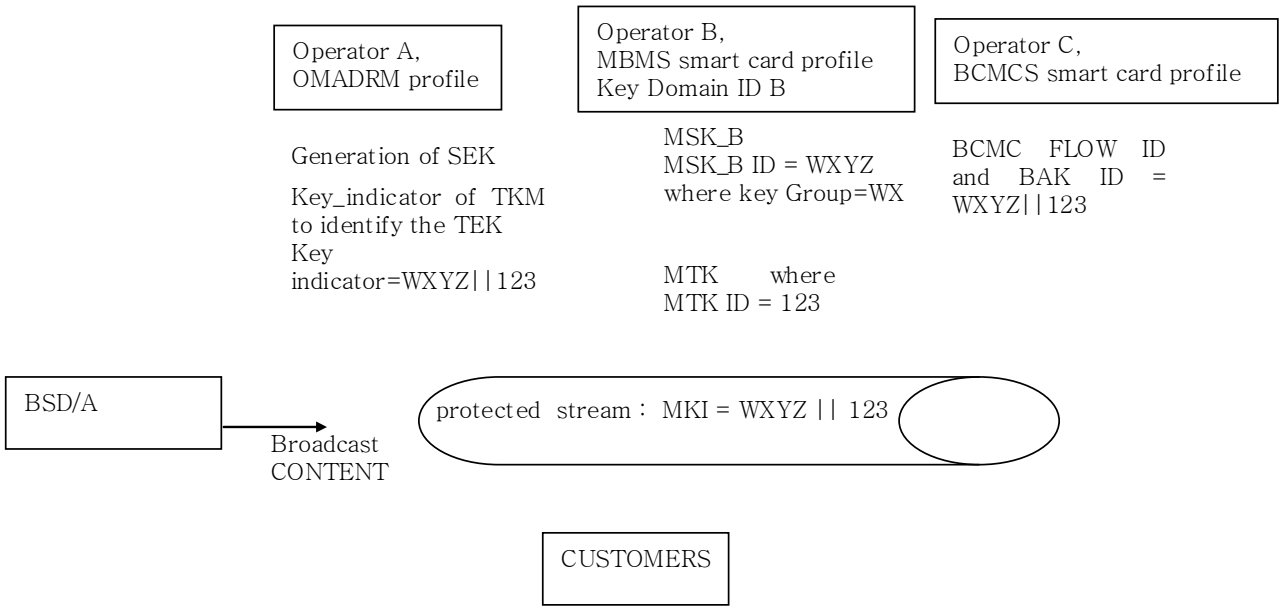

Figure 6: sharing a single SRTP stream between several Broadcast service providers, using the Smartcard profile and the DRM Profile for key management

The third use case illustrates how a single SRTP protected stream can be shared between broadcast service providers implementing the Smartcard profile and the DRM Profile. Figure 6 illustrates this use case.

Broadcast service providers A implements the DRM Profile, broadcast service provider B implements the (U)SIM variant of the Smartcard Profile and broadcast service provider C implements the (R-)UIM/CSIM variant of the Smartcard Profile.

Broadcast service providers A, B and C generate their own SEKs. The SEKs generated by each broadcast service provider are different. A TEK common to broadcast service providers A, B and C is used to protect the media stream..

The value of the MKI, which in the above example is " WXYZ || 123", has to be synchronised betweenthe broadcast service provider implementing the DRM Profile and the two broadcast service providers implementing the variants of the Smartcard Profile.

The BSDA broadcasts the protected media stream encrypted with common.

Upon reception of the protected media stream the terminal retrieves the TEK required to decrypt the content based on MKI.

7.4.2 Key Management

As defined by [BCAST12-ServContProt].

7.4.2.1 SDP Signaling of Key Management Information

As defined by [BCAST12-SG] and [BCAST12-ServContProt].

7.4.2.2 DRM Profile

The Terminal MAY support service protection using the DRM Profile. IF the DRM Profile based service protection is supported, the Terminal SHALL support the reception and processing of keys transported in OMA DRM 2.0 ROs.

The Terminal MAY support content protection using the DRM Profile as defined in [BCAST12-ServContProt].

The Terminal MAY support extensions for service protection and content protection of broadcast-only devices as defined in [DRM20-Broadcast-Extensions].

7.4.2.3 OMA BCAST Smartcard Profile

The Terminal SHALL support service protection using the Smartcard profile as defined in [BCAST12-ServContProt] section 4.1 and 6.

The Terminal MAY support content protection using the Smartcard profile as defined in [BCAST12-ServContProt].

7.4.3 File Protection

As defined by [BCAST12-ServContProt].

7.5 MBMS adaptation related to OMA-TS-BCAST_Distribution

7.5.1 File Distribution

As defined by [BCAST12-Distribution].

Split TOI SHALL NOT be used.

The BSDA SHALL use FLUTE for file distribution.

The FEC RAPTOR scheme MAY be supported by the BSDA and SHALL be supported by terminal as specified in [3GPP TS 26.346] Annex B (there called MBMS FEC).

7.5.1.1 Signalling of parameters with FLUTE

FLUTE FDT Instances SHALL comply with [BCAST12-Distribution], with the following restrictions:

- FEC-OTI-FEC-Encoding-ID attribute SHALL be included in <FDT-Instance> element ;
- Content-Type attribute SHALL be included in <FDT-Instance> element ;
- Content-Length attribute SHALL be included in each <File> element.

7.5.1.2 FDT Instance schema

FLUTE FDT Instances SHALL comply with BCAST FDT Instance schema defined in [BCAST12-Distribution].

In addition, MBMS adaptation restrictions defined in section 7.5.1.1 SHOULD be enforced in BCAST FDT Instances, using the ‘xsi:type’ attribute as follows:

- Type of <FDT-Instance> element SHOULD be ’FDT-InstanceType-BdsMbmsDvb’ from BCAST FDT namespace ;
- Type of each <File> element SHOULD be ’FileType-BdsMbmsDvb’ from BCAST FDT namespace.

7.5.2 Associated Delivery Procedures

As defined by [BCAST12-Distribution].

The Terminal and the BSDA SHALL implement file repair and reception reporting mechanisms as specified in [BCAST12-Distribution].

7.5.3 Stream Distribution

As defined by [BCAST12-Distribution], with the following exceptions;

Terminals SHALL implement the streaming service as defined in [3GPP 26.234].

The sender SHALL send RTCP sender reports as described in [3GPP TS 26.346].

The FEC RAPTOR scheme MAY be supported by the BSDA and SHALL be supported by the terminal as specified in [3GPP TS 26.346] Annex B (there called MBMS FEC).

Note: See annex G of [3GPP TS 26.346] for a description of some methods to improve channel tune-in and switching times for stream distribution when using REC RAPTOR scheme.

7.5.4 Media codecs

The Terminal SHALL be able to receive, decode and render the codecs and payload types that are MANDATORY according to [3GPP TS 26.346].

The Terminal SHOULD be able to receive, decode and render the codecs and payload types that are RECOMMENDED according to [3GPP TS 26.346].

The Terminal MAY be able to receive, decode and render the codecs and payload types that are OPTIONAL according to [3GPP TS 26.346].

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-BCAST_MBMS_Adaptation-V1_1-20131029-A	29 Oct 2013	Status changed to Approved by TP TP Ref # OMA-TP-2013-0332-INP_BCAST_V1_1_ERP_for_final_Approval

A.2 Draft/Candidate Version 1.2 History

Document Identifier	Date	Sections	Description
Draft Version OMA-TS-BCAST_MBMS_Adaptation-V1_2	10 Dec 2013	2.1; entire document	Version 1.2 Created from OMA-TS-BCAST_MBMS_Adaptation-V1_1-20131029-A. Implementation of CR OMA-BCAST-2013-0056-CR_CONR1.2_E001_E002.doc
Candidate Version OMA-TS-BCAST_MBMS_Adaptation-V1_2	14 Jan 2014	n/a	Status changed to Candidate by TP TP Ref # OMA-TP-2014-0002-INP_BCAST_NGH_V1_2_ERP_and_ETR_for_Candidate_approval

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [IOPPROC].

Note: BCAST adaptation specifications, in which it is specified how the BCAST 1.0 enabler is implemented over a specific BDS (BCAST Distribution System), may overrule or adapt requirements from this SCR or provide additional requirements.

B.1 SCR for BCAST MBMS Client

Item	Function	Reference	Status	Requirement
BCAST-MBMS-C-001	Support MBMS adaptation		O	BCAST-MBMS-C-002 AND BCAST-MBMS-C-003 AND BCAST-MBMS-C-006 AND BCAST-MBMS-C-007 AND BCAST-MBMS-C-008 AND BCAST-MBMS-C-015 AND BCAST-MBMS-C-018
BCAST-MBMS-C-002	Support CODECS for 3GPP MBMS	TS MBMS Adaptation 6.5.4 and 7.5.4	O	
BCAST-MBMS-C-003	Support Service Interaction btw Network and Terminal	TS MBMS Adaptation 6.2.1 and 7.2.1	O	BCAST-MBMS-C-004 AND BCAST-MBMS-C-005
BCAST-MBMS-C-004	Support HTTP, TCP, UDP, IP	TS MBMS Adaptation 6.2.1 and 7.2.1	O	BCAST-SERVICES-C-013
BCAST-MBMS-C-005	Support access dependant mechanism	TS MBMS Adaptation 6.2.1 and 7.2.1	O	
BCAST-MBMS-C-006	Support Service Provisioning Function	TS MBMS Adaptation 6.2.2 and 7.2.2	O	BCAST-SERVICES-C-006
BCAST-MBMS-C-007	Support Terminal Provisioning Function	TS MBMS Adaptation 6.2.3 and 7.2.3	O	BCAST-SERVICES-C-011
BCAST-MBMS-C-008	Support Notification Function	TS MBMS Adaptation 6.2.4 and 7.2.4	O	
BCAST-MBMS-C-009	Support the Specific adaptation of Service Guide Function for 3GPP MBMS Network	TS-MBMS-Adaptation section 6.3 and 7.3	O	BCAST-MBMS-C-010 AND BCAST-MBMS-C-011 AND BCAST-MBMS-C-012 AND BCAST-MBMS-C-013 AND BCAST-MBMS-C-014
BCAST-MBMS-C-010	Support Service Guide Delivery over Interaction Channel	TS-MBMS-Adaptation section 6.3.2 and 7.3.2	O	BCAST-SG-C-012
BCAST-MBMS-C-011	Support FLUTE	TS-MBMS-Adaptation section 6.3.1 and 7.3.1	O	

Item	Function	Reference	Status	Requirement
BCAST-MBMS-C-012	Support Session Description	TS-MBMS-Adaptation section 6.3.4 and 7.3.4	O	
BCAST-MBMS-C-013	Support Service Guide Bootstrap over broadcast channel	TS-MBMS-Adaptation section 6.3.6 and 7.3.6	O	
BCAST-MBMS-C-014	Support Service Guide Bootstrap over interaction channel	TS-MBMS-Adaptation section 6.3.7 and 7.3.6	O	
BCAST-MBMS-C-015	Support File Distribution Function	TS-MBMS-Adaptation section 6.5.1 and 7.5.1	O	BCAST-MBMS-C-016 AND BCAST-MBMS-C-017
BCAST-MBMS-C-016	Support FEC RAPTOR	TS-MBMS-Adaptation section 6.5.1 and 7.5.1	O	BCAST-FD-C-009
BCAST-MBMS-C-017	Support Associated Delivery Procedure	TS-MBMS-Adaptation section 6.5.2 and 7.5.2	O	BCAST-FD-C-015
BCAST-MBMS-C-018	Access to IP layer	TS-MBMS-Adaptation section 6.1 and 7.1	O	
BCAST-MBMS-C-019	Support BCAST Service Protection Function	TS-MBMS-Adaptation 6.4 and 7.4	O	BCAST-MBMS-C-020 AND BCAST-MBMS-C-021
BCAST-MBMS-C-020	Support Smartcard profile for Service Protection	TS-MBMS-Adaptation 6.4.2 and 7.4.2.3	O	BCAST-TerminalCapability-C-001
BCAST-MBMS-C-021	Support Encryption Protocol	TS-MBMS-Adaptation section 7.4.1	O	BCAST-MBMS-C-022
BCAST-MBMS-C-022	Support SRTP	TS-MBMS-Adaptation section 7.4.1	O	
BCAST-MBMS-C-023	Support IPSEC	TS-MBMS-Adaptation section 7.4.1	O	
BCAST-MBMS-C-024	Support ISMACrypt	TS-MBMS-Adaptation section 7.4.1	O	

B.2 SCR for BCAST MBMS BSM

Item	Function	Reference	Status	Requirement
BCAST-MBMSBSM-S-001	Support BCAST Adaptation on 3GPP MBMS Network		O	
BCAST-MBMSBSM-S-002	Support 3GPP MBMS Generic Adaptation	TS-MBMS-Adaptation 6	O	
BCAST-MBMSBSM-S-003	Support BCAST Service Protection Function	TS-MBMS-Adaptation 6.4	O	BCAST-BSM-S-004
BCAST-MBMSBSM-S-004	Support Smartcard profile for Service Protection	TS-MBMS-Adaptation 6.4.2	O	
BCAST-MBMSBSM-S-005	Support DRM profile for Service Protection	TS-MBMS-Adaptation 6.4.1	O	
BCAST-MBMSBSM-S-006	Support DRM extension for Service Protection	TS-MBMS-Adaptation 6.4.1	O	
BCAST-MBMSBSM-S-007	Support BCAST Content Protection Function	TS-MBMS-Adaptation 6.4	O	
BCAST-MBMSBSM-S-008	Support DRM profile for Content Protection	TS-MBMS-Adaptation 6.4.1	O	
BCAST-MBMSBSM-S-009	Support Smartcard profile for Content Protection	TS-MBMS-Adaptation 6.4.2	O	
BCAST-MBMSBSM-S-010	Support DRM extension for Content Protection	TS-MBMS-Adaptation 6.4.1	O	
BCAST-MBMSBSM-S-011	Support 3GPP MBMS Specific Adaptation	TS-MBMS-Adaptation 7	O	BCAST-MBMSBSM-S-012 AND BCAST-MBMSBSM-S-013 AND BCAST-MBMSBSM-S-014 AND BCAST-MBMSBSM-S-015
BCAST-MBMSBSM-S-012	Support Interactive communication between BSM and Terminal	TS-MBMS-Adaptation 7.2.1	O	
BCAST-MBMSBSM-S-013	Support Service Provisioning between BSM and Terminal	TS-MBMS-Adaptation 7.2.2	O	BCAST-SERVICES-BSM-001
BCAST-MBMSBSM-S-014	Support Terminal Provisioning between BSM and Terminal	TS-MBMS-Adaptation 7.2.3	O	BCAST-SERVICES-BSM-006
BCAST-MBMSBSM-S-015	Support Notification between BSM and Terminal	TS-MBMS-Adaptation 7.2.4	O	
BCAST-MBMSBSM-S-016	Support BCAST Service Protection Function	TS-MBMS-Adaptation 7.4	O	
BCAST-MBMSBSM-S-017	Support Smartcard profile for Service Protection	TS-MBMS-Adaptation 7.4.2	O	

Item	Function	Reference	Status	Requirement
BCAST-MBMSBSM-S-018	Support DRM profile for Service Protection	TS-MBMS-Adaptation 7.4.2.2	O	
BCAST-MBMSBSM-S-019	Support DRM extension for Service Protection	TS-MBMS-Adaptation 7.4.2.2	O	
BCAST-MBMSBSM-S-020	Support BCAST Content Protection Function	TS-MBMS-Adaptation 7.4	O	
BCAST-MBMSBSM-S-021	Support DRM profile for Content Protection	TS-MBMS-Adaptation 7.4.2.2	O	
BCAST-MBMSBSM-S-022	Support Smartcard profile for Content Protection	TS-MBMS-Adaptation 7.4.2	O	
BCAST-MBMSBSM-S-023	Support DRM extension for Content Protection	TS-MBMS-Adaptation 7.4.2.2	O	

B.3 SCR for BCAST MBMS BSDA

Item	Function	Reference	Status	Requirement
BCAST-MBMSBSDA-S-001	Support BCAST Adaptation on 3GPP MBMS Network		O	BCAST-MBMSBSDA-S-002
BCAST-MBMSBSDA-S-002	Support IP bearer	TS 3GPP MBMS Section 6.1 and 7.1	O	
BCAST-MBMSBSDA-S-003	Support 3GPP MBMS Generic Adaptation	TS-MBMS-Adaptation section 6	O	BCAST-MBMSBSDA-S-004 AND BCAST-MBMSBSDA-S-007 AND BCAST-MBMSBSDA-S-008 AND BCAST-MBMSBSDA-S-009
BCAST-MBMSBSDA-S-004	Support the generic adaptation of Service Guide Function for 3GPP MBMS Network	TS-MBMS-Adaptation section 6.3	O	BCAST-MBMSBSDA-S-005 AND BCAST-MBMSBSDA-S-006
BCAST-MBMSBSDA-S-005	Support Service Guide Bootstrap over broadcast channel	TS-MBMS-Adaptation section 6.3.6	O	
BCAST-MBMSBSDA-S-006	Support Service Guide Bootstrap over interaction channel	TS-MBMS-Adaptation section 6.3.7	O	
BCAST-MBMSBSDA-S-007	Support File Distribution	TS-MBMS-Adaptation section 6.5.1	O	
BCAST-MBMSBSDA-S-008	Support Stream Distribution	TS-MBMS-Adaptation section 6.5.3	O	
BCAST-MBMSBSDA-S-009	Support FEC RAPTOR	TS-MBMS-Adaptation section 6.5.1.and 6.5.3	O	

Item	Function	Reference	Status	Requirement
BCAST-MBMSBSDA-S-010	Support MBMS Specific Adaptation	TS-MBMS-Adaptation section 7	O	BCAST-MBMSBSDA-S-011 AND BCAST-MBMSBSDA-S-028 AND BCAST-MBMSBSDA-S-029 AND BCAST-MBMSBSDA-S-030
BCAST-MBMSBSDA-S-011	Support the Specific adaptation of Service Guide Function for 3GPP MBMS Network	TS-MBMS-Adaptation section 7.3	O	BCAST-MBMSBSDA-C-018 AND BCAST-MBMSBSDA-C-019
BCAST-MBMSBSDA-S-012	Support Service Guide Delivery over Broadcast Channel	TS-MBMS-Adaptation section 7.3.1	O	BCAST-SGGAD-S-019
BCAST-MBMSBSDA-S-013	Support FLUTE	TS-MBMS-Adaptation section 7.3.1	O	
BCAST-MBMSBSDA-S-014	Support Service Guide Encoding	TS-MBMS-Adaptation section 7.3.2	O	BCAST-SGGAD-S-017
BCAST-MBMSBSDA-S-015	Support Session Description	TS-MBMS-Adaptation section 7.3.3	O	
BCAST-MBMSBSDA-S-016	Support Restrictions on use of elements and attributes on SGDD	TS-MBMS-Adaptation section 7.3.4	O	
BCAST-MBMSBSDA-S-017	Support Service Guide Data Model	TS-MBMS-Adaptation section 7.3.4	O	BCAST-SGGAD-S-005
BCAST-MBMSBSDA-S-018	Support Service Guide Bootstrap over broadcast channel	TS-MBMS-Adaptation section 7.3.6	O	
BCAST-MBMSBSDA-S-019	Support Service Guide Bootstrap over interaction channel	TS-MBMS-Adaptation section 7.3.6	O	
BCAST-MBMSBSDA-S-020	Support the specific adaptation of Service Protection Function and Content Protection Function	TS-MBMS-Adaptation section 7.4	O	BCAST-MBMSBSDA-S-021 AND BCAST-MBMSBSDA-S-025
BCAST-MBMSBSDA-S-021	Support Encryption Protocol	TS-MBMS-Adaptation section 7.4.1	O	
BCAST-MBMSBSDA-S-022	Support SRTP	TS-MBMS-Adaptation section 7.4.1	O	
BCAST-MBMSBSDA-S-023	Support IPSEC	TS-MBMS-Adaptation section 7.4.1	O	
BCAST-MBMSBSDA-S-024	Support ISMACrypt	TS-MBMS-Adaptation section 7.4.1	O	

Item	Function	Reference	Status	Requirement
BCAST-MBMSBSDA-S-025	Support Key management	TS-MBMS-Adaptation section 7.4.2	O	
BCAST-MBMSBSDA-S-026	Support DRM Profile Key management	TS-MBMS-Adaptation section 7.4.2.2	O	
BCAST-MBMSBSDA-S-027	Support Smartcard Profile Key management	TS-MBMS-Adaptation section 7.4.2.3	O	
BCAST-MBMSBSDA-S-028	Support File Distribution	TS-MBMS-Adaptation section 7.5.1	O	
BCAST-MBMSBSDA-S-029	Support Associated Delivery Procedure	TS-MBMS-Adaptation section 7.5.2	O	
BCAST-MBMSBSDA-S-030	Support Stream Distribution	TS-MBMS-Adaptation section 7.5.3	O	

B.4 SCR for BCAST MBMS BSA

Item	Function	Reference	Status	Requirement
BCAST-MBMSBSA-S-001	Support for 3GPP MBMS		O	BCAST-MBMSBSA-S-002
BCAST-MBMSBSA-S-002	Support BCAST Adaptation on 3GPP MBMS Network		O	
BCAST-MBMSBSA-S-003	Support 3GPP MBMS Generic Adaptation	TS MBMS Adaptation 6	O	BCAST-MBMSBSA-S-004 AND BCAST-MBMSBSA-S-005
BCAST-MBMSBSA-S-004	Support CODECS for 3GPP MBMS	TS MBMS Adaptation 6.5.4	O	
BCAST-MBMSBSA-S-005	Support the interactive communication between BSA and Terminal	TS MBMS Adaptation 6.2.1	O	BCAST-SERVICES-BSA-001
BCAST-MBMSBSA-S-006	Support 3GPP MBMS Specific Adaptation	TS MBMS Adaptation 7	O	BCAST-MBMSBSA-S-007 AND BCAST-MBMSBSA-S-008
BCAST-MBMSBSA-S-007	Support CODECS for 3GPP MBMS	TS MBMS Adaptation 7.5.4	O	
BCAST-MBMSBSA-S-008	Support the interactive communication between BSA and Terminal	TS MBMS Adaptation 7.2.1	O	BCAST-SERVICES-BSA-001