Broadcast Distribution System Adaptation - 3GPP/MBMS

Candidate Version 1.0 – 29 May 2007

Open Mobile Alliance

OMA-TS-BCAST_MBMS_Adaptation-V1_0-20070529-C

Contents

Figures

Tables

1. Scope

This document specifies how the BCAST 1.0 enabler is implemented over a specific BDS(Broadcast Distribution System).

The BCAST 1.0 Enabler supports the global interoperability among different Broadcast Distribution Systems, and can also be adapted according to the characteristics of Broadcast Distribution Systems for BCAST 1.0 enabler implementation over a certain BDS. In this document, two types of adaptation are presented.

The BCAST 1.0 Enabler includes 9 functions and all 9 functions 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 1.0 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 v6] ; “Multimedia Broadcast/Multicast Service (MBMS) user services; Stage 1”, Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project, 3GPP TS 22.246,
URL:http://www.3gpp.org/

[3GPP TS 23.003 v6] "Numbering, Addressing and Identification"; 3rd Generation Partnership Project, 3 GPP TS 23.003,
URL:http://www.3gpp.org/

[3GPP TS 23.246 v7] ”Multimedia Broadcast/Multicast Service (MBMS)”; Architecture and functional description (Release 7), Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project; 3GPP TS 23.246,
URL:http://www.3gpp.org/

[3GPP TS 25.331 v6] “Radio resource control(RRC); Protocol specification”, 3rd Generation Partnership Project, 3GPP TS 25.331,
URL:http://www.3gpp.org/

[3GPP TS 25.346 v6] “Inclusion of the Multimedia Broadcast Multicast Service(MBMS) in the Radio Access Network (RAN); Stage 2”, 3rd Generation Partnership Project, 3GPP 25.346,
URL:http://www.3gpp.org/

[3GPP TS 25.401 v6] “UTRAN overall description (Release 6)”, Technical Specification Group Radio Access Network, 3rd Generation Partnership Project, 3GPP TS 25.401,
URL:http://www.3gpp.org/

[3GPP TS 26.346 v7] “Multimedia Broadcast/Multicast Service (MBMS), Protocols and codecs (Release 7)”, Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project, 3GPP TS 26.346,
URL:http://www.3gpp.org/

[3GPP TS 33.246 v7] “3G Security; Security of Multimedia Broadcast/Multicast Service (Release 7)”, Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project, 3GPP 33.246,
URL:http://www.3gpp.org/

[BCAST10-Distribution] "File and Stream Distribution for Mobile Broadcast Services ", Open Mobile Alliance™, OMA-TS-BCAST_Distribution-V1_0,
URL:http://www.openmobilealliance.org/

[BCAST10-Ser vices] "Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_Services-V1_0,
URL:http://www.openmobilealliance.org/

[BCAST10-ServContProt] "Service and Content Protection for Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_SvcCntProtection-V1_0,
URL:http://www.openmobilealliance.org/

[BCAST10-SG] "Service Guide for Mobile Broadcast Services", Open Mobile Alliance™, OMA-TS-BCAST_ServiceGuide-V1_0,
URL:http://www.openmobilealliance.org/

[DRM20-Broadcast-Extensions] "OMA DRM v2.0 Extensions for Broadcast Support", Open Mobile Alliance™, OMA-TS-DRM-XBS-V1_0,
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

2.2 Informative References

[3GPP TS 23.060 v6] "General Packet Radio Service (GPRS); Service description; Stage 2", 3rd Generation Partnership Project, 3GPP TS 23.060,
URL:http://www.3gpp.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.

3.2 Definitions

Cell_ID	Cell Identifier as defined in [3GPP TS 25.401 v6] chapters 6.1.5
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 v6] (section 5.2.2) and [3GPP TS 25.331 v6] (section 10.2.16h)

3.3 Abbreviations

BCMCS	Broadcast Multicast Service (3GPP2)
DVB-H	Digital Video Broadcasting - Handheld
MBMS	Multimedia Broadcast Multicast Service (3GPP)
MKI	Master Key Identifier
MSK	MBMS Service Key
MTK	MBMS Traffic Key
SG	Service Guide
SRTP	Secure Real-time Transport Protocol

4. Introduction (Informative)

This technical specification specifies how the OMA Mobile Broadcast Services (BCAST) Enabler can be implemented to achieve two modes of adaptation:

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 Broadcast 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 Broadcast 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.

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.

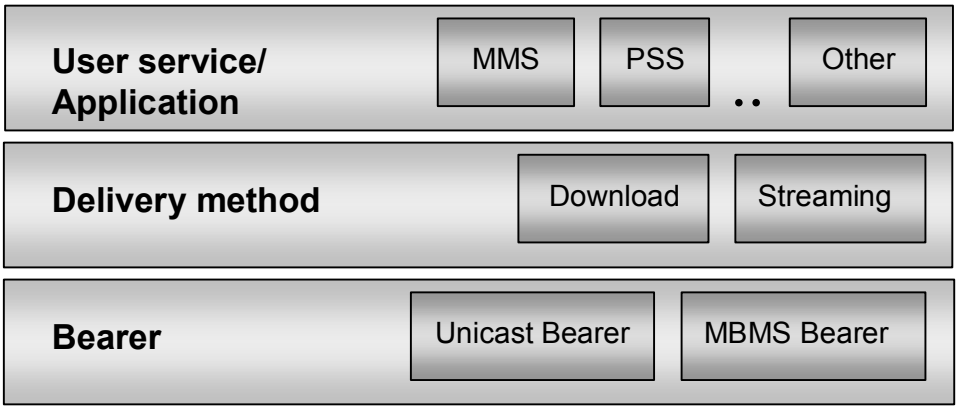

Figure 1: Functional Layers for MBMS User Service

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 v6 and 3GPP TS 22.146 v6 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 v6, 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 6. 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 3 depicts the MBMS network architecture showing MBMS related entities involved in providing MBMS user services.

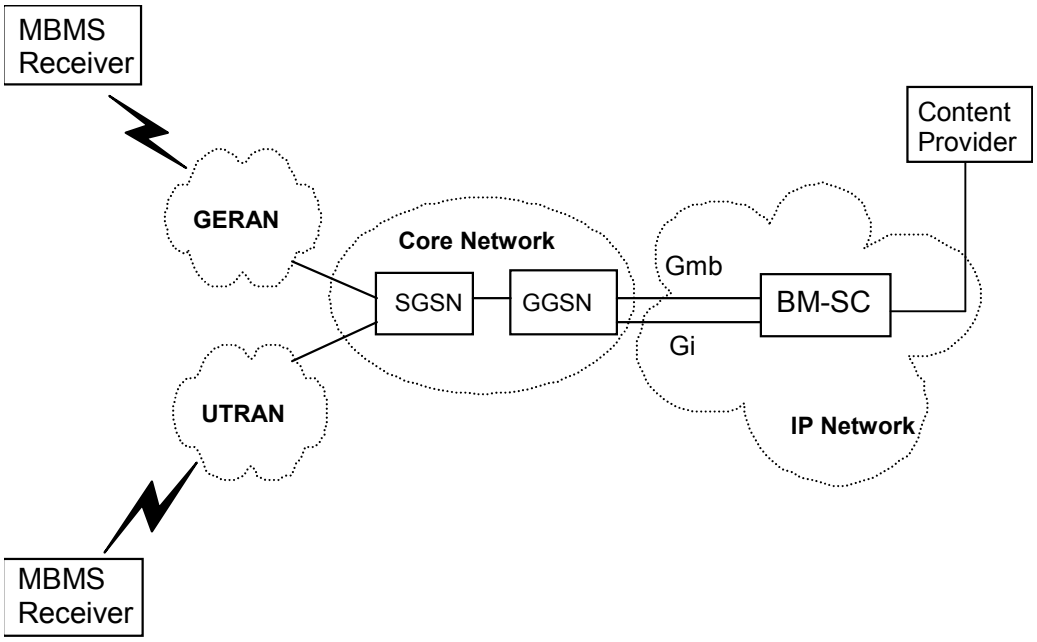

Figure 2: MBMS network architecture model

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.

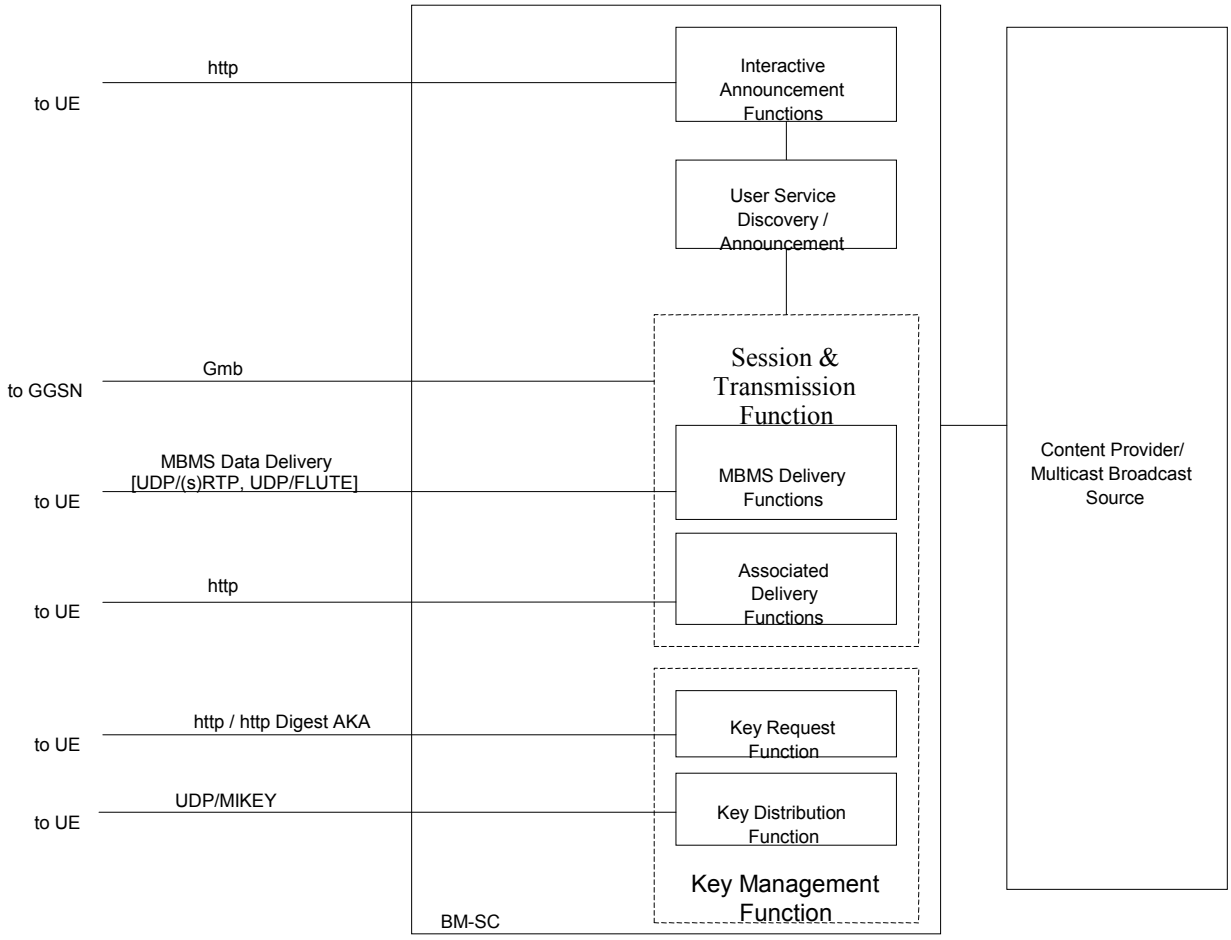

Figure 3: BM-SC sub-functional structure

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.

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 [BCAST10-Services], [BCAST10-SG], [BCAST10-ServContProt], [BCAST10-Distribution] and [DRM20-XBS]) 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 [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 [BCAST10-Services].

The Terminal SHOULD support SMS for service interaction.

6.2.2 Service Provisioning

As defined by [BCAST10-Services].

6.2.3 Terminal Provisioning

As defined by [BCAST10-Services].

Note: SG bootstrap information is provisioned using Terminal Provisioning.

6.2.4 Notification

The specification in section 5.14 of [BCAST10-Services] SHALL apply.

When using 3GPP MBMS as the underlying Broadcast Distribution System the Notification functionality is enabled as specified in [BCAST10-Services].

6.3 MBMS adaptation related to OMA-TS-BCAST_ServiceGuide

6.3.1 Service Guide Delivery over Broadcast Channel

As defined by [BCAST10-SG].

6.3.2 Service Guide Delivery over Interaction Channel

As defined by [BCAST10-SG].

6.3.3 Service Guide Encoding

As defined by [BCAST10-SG].

6.3.4 Session Description

As defined by [BCAST10-SG].

6.3.5 Service Guide Data Model

As defined by [BCAST10-SG].

6.3.5.1 CellTargetArea in MBMS

See section 7.3.5.1.

6.3.6 Service Guide Bootstrap for SG Delivery over Broadcast Channel

The entry point information according to [BCAST10-SG] section 6.1.1 SHALL be provisioned to the terminal using OMA DM as specified in [BCAST10-Services] and using the BCAST MO specified in [BCAST10-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 [BCAST10-Services] and using the BCAST MO specified in [BCAST10-Services].

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

As defined by [BCAST10-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 [BCAST10-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 [BCAST10-ServContProt] section 4.5 and 6.

The Terminal MAY support content protection using the Smartcard Profile as defined in [BCAST10-ServContProt].

6.5 MBMS adaptation related to OMA-TS-BCAST_Distribution

6.5.1 File Distribution

As defined by [BCAST10-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 [BCAST10-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 [BCAST10-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 [BCAST10-Distribution].

6.5.3 Stream Distribution

As defined by [BCAST10-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).

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 9 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 [BCAST10-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 [BCAST10-Services].

The Terminal SHOULD support SMS for service interaction.

7.2.2 Service Provisioning

As defined in [BCAST10-Services].

7.2.3 Terminal Provisioning

As defined in [BCAST10-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 [BCAST10-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 [BCAST10-SG].

7.3.3 Service Guide Encoding

As defined by [BCAST10-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 the session description as defined by MBMS user service bundle description (MBMS-USBD) as specified in [3GPP 26.346] section 5.2. MBMS-USBD refers to one or several SDP description(s), formatted according to [BCAST10-SG] section 5.1.2.5 and [BCAST10-SPCP] 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 [BCAST10-SG].

7.3.5.1 CellTargetArea in MBMS

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

OMA BCAST Service Guide allows describing the target area for Service and Content in terms of BDS-specific cell identification. In the case of MBMS, ,the value of "CellTargetArea" element of "TargetArea" element is expressed as defned in [BCAST10-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 [BCAST10-ServContProt] sections 4.5, 6 and 13.

The Terminal MAY support service protection using the DRM Profile as defined in [BCAST10-ServConProt].

As defined by Section 9 Encryption Protocols of [BCAST10-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 [BCAST10-ServContProt] with the constraints indicated below in Section 0 SHALL apply.

SRTP is the common content encryption method included in [3GPP TS 33.246] and [BCAST10-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 [BCAST10-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 between BCAST and 3GPP- MBMS terminals

This subsection describes how a number of Broadcast service providers can share the same SRTP protected stream(s) while maintaining compatibility with the 3GPP MBMS specifications. This solution also allows MBMS only terminals to share the same protected media stream with BCAST terminals1. The use of SRTP is mandatory with respect to 3GPP MBMS [3GPP TS 33.246]. This does not exclude the use of IPSec or ISMACryp with BCAST terminals, but this means the protected streams can not be shared with MBMS terminals.

The Master Key Identifier (MKI) value introduced by SRTP protocol cf. [RFC 3711] enables the retrieval of the correct BCAST TEK (which is functional equivalent to the MBMS Traffic Key, MTK) in order to decrypt the protected media stream. The MKI SHALL be used as defined in [RFC 3711]

The value of MKI SHALL be unique to enable access to the corresponding shared protected stream among different broadcast service providers.

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

MKI = BCAST TEK ID = (MSK ID || MTK ID)

MSK ID (4 bytes) and MTK ID (2 bytes) are carried by the MIKEY short term key message extension payload, where:

- MSK ID(4 bytes): is split into 2 sub parameters: the key group part and the key number part.
  - Key group part (2 bytes): enables to group keys within a group, so that redundant MSKs are deleted. The key group part enables the terminal to know which MSK has to be updated upon reception of a new MSK.

[1] It is noted that the MBMS terminals and BCAST terminals are likely to be receiving the media stream over different bearers in which cases their would be no bandwidth efficiency savings but there are still potentially valid use cases, e.g. an Broadcast service provider chooses to broadcast protected media over MBMS or another bearer dependent location to dual mode terminals.

        - Key number part (2 bytes): to distinguish MSKs that have the same key domain ID and Key group part.
    - MTK ID(2 bytes): used to distinguish MTKs that have the same MSK ID and Key domain ID. This parameter is increased for each MTK update.

Considering several broadcast service providers sharing the same SRTP protected stream distributed by a single BSDA provider (BSDA), the MKI value MUST be shared.

Following the MKI definition in [TS 3GPP 33.246], requiring the MKI to be shared between Broadcast service providers has an impact on the management of MSK and MTK ID values used by the 3GPP MBMS variant of the Smartcard Profile. There is also a resulting impact on the update periods of the MSK and MTK IDs and key material. The following rules apply to the MKI parameters definition:

- **MSK ID (4 bytes)**
    - Key group part (2 bytes):

      If the UE receives a MSK with the same key domain ID and the same key group part, but different key number part, then the existing MSK SHALL be discarded and replaced by the new MSK.

      The MSK key group part value MUST be configured to be the same by the participating broadcast service providers. Then the terminal will be able to distinguish the MSKs of the different protected streams based on the key group part of the MSK ID parameter.

      Sharing a single key group part value between broadcast service providers does not enable to share several protected streams as the MSKs updates may overlap. It is necessary to use a dedicated key group value for each protected stream.
    - Key number part (2 bytes):

      The key number part MUST also be synchronised among broadcast service providers.
- **MTK ID (2 bytes)** is synchronised *implicitly* as it increments for each MTK update.

Broadcast service providers must use the same traffic key material. A shared protected media stream is encrypted using a single set of traffic keys. All broadcast service providers wishing to share the same encrypted media stream must provide the used traffic key material and traffic key IDs to their users via the STKM. The BSDA provider (BSDA), in charge of broadcasting the encrypted media stream, SHALL generate TEK key material and identifier.

As the MKI value for a shared protected media stream has to be both unique and shared, Broadcast service providers must synchronise the MSK and MTK IDs, implying a synchronisation regarding the frequency of the update of MSKs and MTKs2.

In summary:

- Broadcast service providers must use the same MKI for the shared SRTP stream as it is used to identify the traffic key (MTK) that is used to decrypt the broadcasted protected media content
- The MKI must be constructed as follows: MKI = (MSK ID || MTK ID) (6 bytes)
- Broadcast service providers must share the same traffic key material (MTK)
- Broadcast service providers don't have to share the same service key material (MSK)
- Broadcast service providers must synchronise the update of MSK key material, and MTK key material. Indeed the renewal of the MSK key material (MSK ID changes) implies a reset of the MTK ID [TS 3GPP 33.246].

This is illustrated in the table below.

[2] The constraint related to the synchronisation of the identifiers, and the frequency of the update of the keys is heavy, but it was the best alternative to suit 3GPP specifications as the key identifier is related to MSK and MTK IDs and as the update of the MSK key material, and then of the MSK ID implies a reset of the MTK ID.

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

However, it should be noted that Broadcast service providers implementing the 3GPP MBMS variant of the Smartcard Profile can define their own key validity period as the key validity period of a given MSK can be updated without updating the MSK key material, cf. section 6.5.3 [TS 3GPP 33.246].

The following can then be considered:

1. A subscriber from Broadcast service provider A has access to media streams 1, 2 and 3, using MSK_Id=MSK_ID, key material = MSK1, and has a key validity period = 1 week. MSK1 is transmitted by Broadcast service provider A.

2. A subscriber from Broadcast service provider B has access to media streams 1, 2 and 4, using MSK_Id=MSK_ID, key material = MSK2, and has a key validity period = 1 month. MSK2 is transmitted by Broadcast service provider B.

The value of the MSK_ID is shared, but key material is different and can be mapped to customized key validity period according to the definition of the service offering for a given broadcast service provider.

It is possible to adapt the key validity period of an MSK depending on the properties of the service/program of the Broadcast service provider's offering, without implying necessarily an update of the MSK key material. The delivery of a new MSK key material implies necessarily a new value for the MSK ID.

Media streams 1 and 2 are shared between Broadcast service providers A and B, media streams 3 and 4 are not shared. The Broadcast service providers can define their own service offering, composed with shared media streams and non shared media streams, as the key material is not shared among broadcast service providers.

Broadcast service providers A and B have to update the MSK key material, which can be different for each Broadcast service provider, at the same time and must use the same identifier (MSK_ID) for the new MSKs. Different key validity periods for the MSKs can be configured, and updated at any time and by each Broadcast service provider independently..

With the above solution, different use cases are possible, depending on the number of BSDA providers (BSDA) and on the 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.

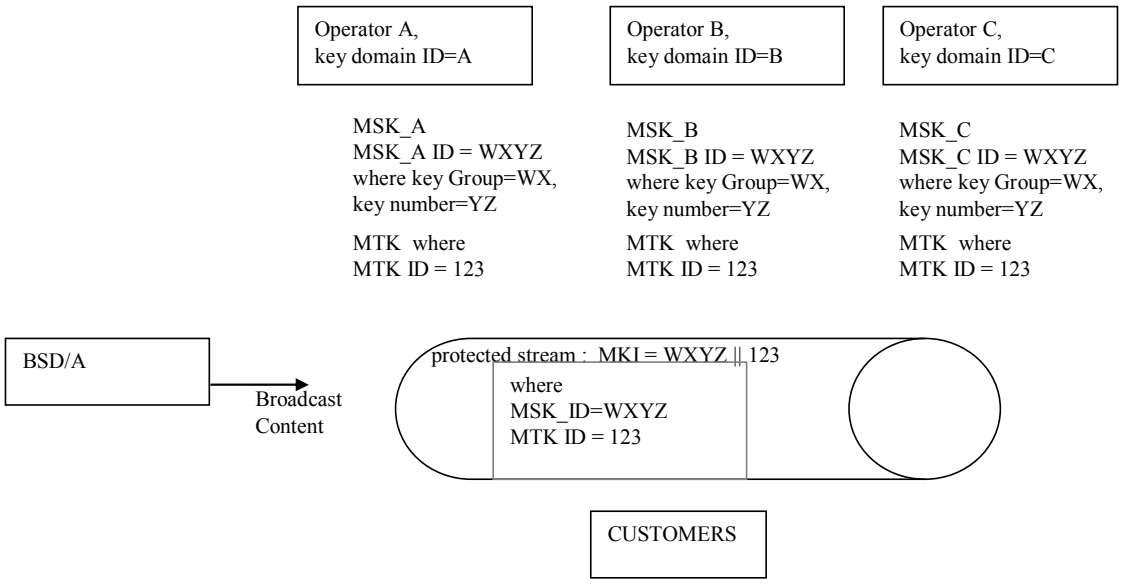

Figure 4: Sharing a single SRTP stream between three broadcast service providers implementing the Smartcard Profile for key management

Figure 4 illustrates how a single broadcast content distributed by the BSDA Provider (BSDA) is 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 MSK key material, MSK_A, MSK_B and MSK_C respectively, which are all different. The frequency of the update of MSK_A, MSK_B and MSK_C is synchronised amongst Broadcast service providers. The identifiers of MSKs are synchronised between the broadcast service providers so that the same MSK_ID (WXYZ) and MTK ID (123) are used. The common MTK is broadcast on the broadcast bearer.

The BSDA provider (BSDA) can then broadcast the content encrypted with this common MTK. Upon reception the terminal retrieves the MTK based on the MKI, generated from the MSK ID and the MTK ID:

MKI = WXYZ||123.

Each terminal can use the MKI value to retrieve the MTK required to decrypt the shared protected media stream.

7.4.1.2.2 Two SRTP streams, provided by two different BSDA providers (BSDA) and shared by three broadcast service providers using the Smartcard Profile

The second use case illustrates how two SRTP protected media streams, provided by different BSDA providers (BSDA1 and BSDA2), can be shared between three Broadcast service providers implementing the Smartcard Profile. Figure 5 outlines this use case.

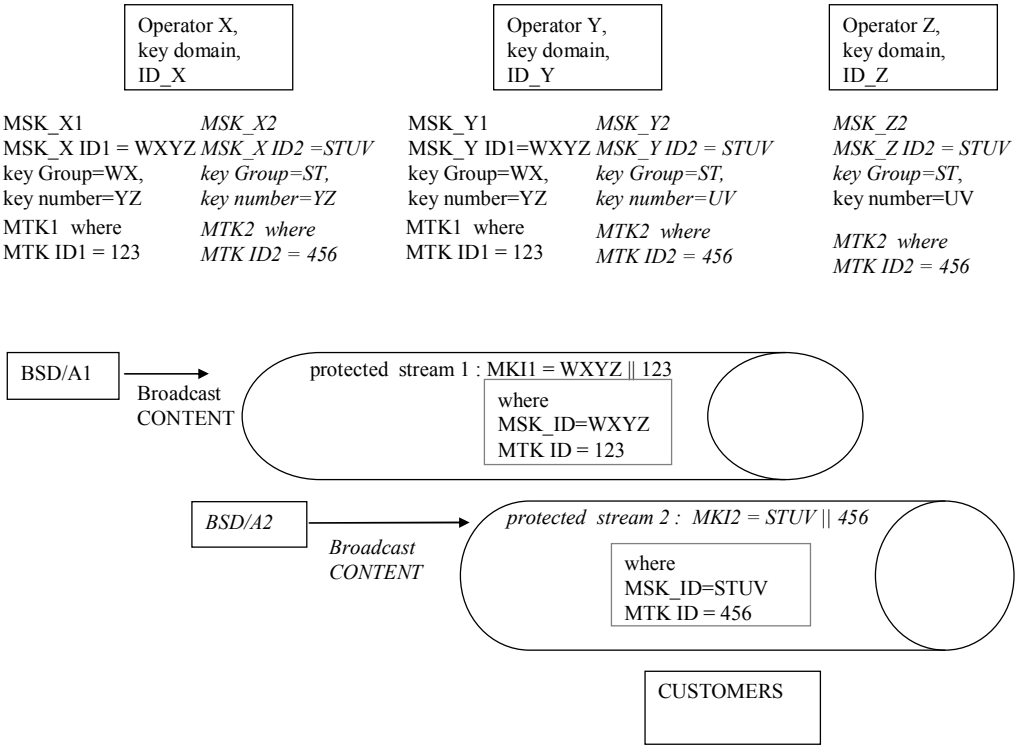

Figure 5: Sharing two SRTP streams between three broadcast service providers using the Smartcard Profile for key management

Figure 5 illustrates how two SRTP protected streams provided by BSDA provider 1 (BSDA1) and BSDA provider 2 (BSDA2) can be shared between three broadcast service providers: X and Y for content broadcast by BSDA provider 1 and X,Y and Z for content broadcast by BSDA provider 2. Broadcast service providers X, Y and Z all implement the Smartcard profile for key management.

Broadcast service providers X, Y and Z generate their own MSKs; MSK_X1/MSK_X2, MSK_Y1/MSK_Y2 and MSK_Z2 respectively for the protected content of content provider 1 and 2. The key materials for MSK_X1/MSK_X2, MSK_Y1/MSK_Y2 and MSK_Z2 are all different.

The MSK IDs have been coordinated between broadcast service providers so that the same MSK_ID = "WXYZ" for stream 1 and "STUV" for stream 2 is used. The frequency of the update of MSK_X1/MSK_X2, MSK_Y1/MSK_Y2 and MSK_Z2 is synchronised among Broadcast service providers. Furthermore, a common MTK MUST be used, e.g. set to "123 "for stream 1 and "456" for stream 2. The common MTKs (MTK1 and MTK2) are broadcast on the broadcast bearer.

The BSDA providers (BSDA1 and BSDA2) can then broadcast the content encrypted with the corresponding MTK: MTK1 for protected stream 1 and MTK2 for stream 2. Upon reception the terminal retrieves the MTK based on the MKI, generated from MSK ID and MTK ID:

MKI 1 = WXYZ||123 for the stream 1

MKI 2 = STUV||456 for the stream 2

Each terminal can use the MKI value to retrieve the MTK required to decrypt the shared protected media stream.

7.4.1.2.3 A single SRTP stream shared by broadcast service providers using DRM profile and Smartcard profile

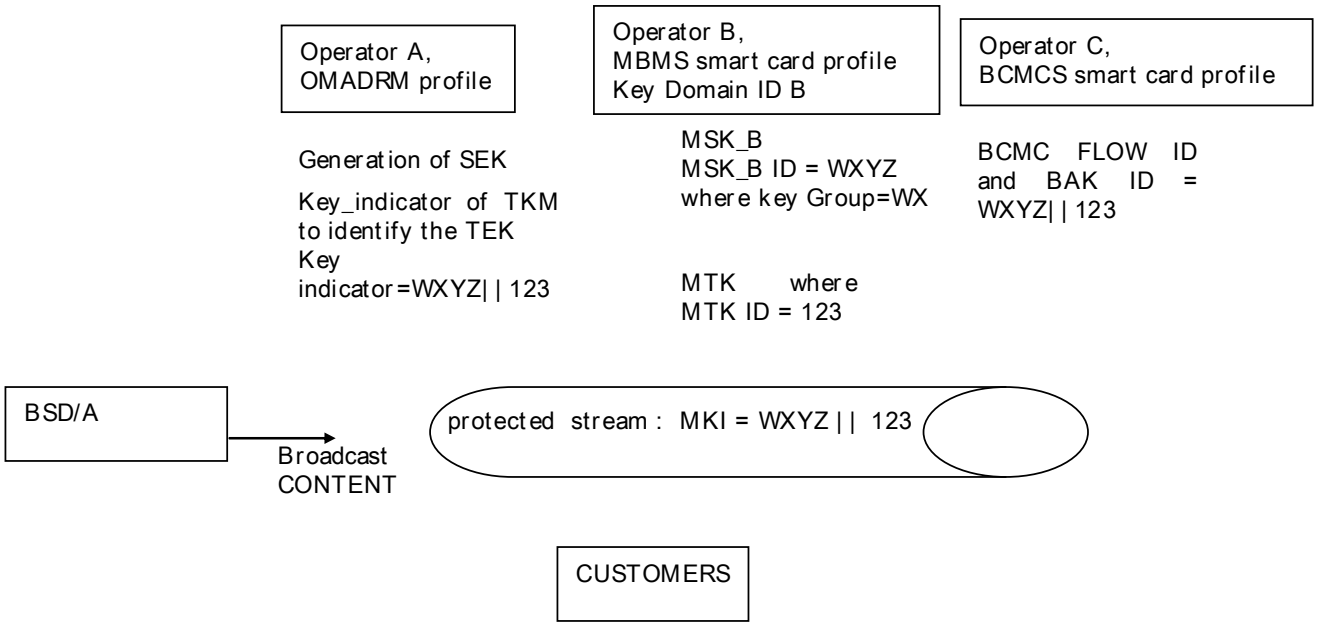

Figure 6: sharing a single SRTP stream between several Broadcast service providers, using the Smartcard profile and the DRM Profile for key management

This 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 for key management. Figure 6 illustrates this use case.

For key management Broadcast service providers A implements the DRM Profile, Broadcast service provider B implements the Smartcard Profile. Synchronisation is necessary to allow a unique value of the key identifier to be used for the traffic key material retrieval used by the terminal.

Broadcast service providers A and B generate their own service keys. A common traffic key is considered independently of the key management profile implemented by the broadcast service provider. The MKI that allows the traffic key material to be retrieved on the terminal side SHALL be unique and common between broadcast service providers.

The value of the MKI " WXYZ || 123" has to be synchronised between:

- the Broadcast service provider implementing OMA DRM key management for the key indicator parameter identifying the TEK.
- the Broadcast service provider implementing the 3GPP MBMS key management for the MSK ID and the MTK ID values.

The BSDA provider (BSDA) can then broadcast the content encrypted with a given (common) traffic key.

Upon reception the terminal retrieves the traffic key based on the MKI set equal to WXYZ||123. Each terminal independently of the broadcast service provider they have subscribed to can retrieve the MTK to decrypt the protected stream using key management specific mechanisms.

SUMMARY

When the broadcast media is protected using SRTP, the MKI value is constructed as follows:

MKI = (MSK ID || MTK ID)

where MSK ID is 4 bytes long and MTK ID is 2 bytes long. Hence the MKI length is 6 bytes.

7.4.2 Key Management

As defined by [BCAST10-ServContProt].

7.4.2.1 SDP Signaling of Key Management Information

As defined by [BCAST10-SG] and [BCAST10-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 [BCAST10-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 [BCAST10-ServContProt] section 4.5 and 6.

The Terminal MAY support content protection using the Smartcard profile as defined in [BCAST10-ServContProt].

7.4.3 File Protection

As defined by [BCAST10-ServContProt].

7.5 MBMS adaptation related to OMA-TS-BCAST_Distribution

7.5.1 File Distribution

As defined by [BCAST10-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 [BCAST10-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 [BCAST10-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 [BCAST10-Distribution].

The Terminal and the BSDA SHALL implement file repair and reception reporting mechanisms as specified in [BCAST10-Distribution].

7.5.3 Stream Distribution

As defined by [BCAST10-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).

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
n/a	n/a	No prior version –or- No previous version within OMA
OMA-xxyyz-V1_0-20021001-A	01 Oct 2002	Initial document to address the basic starting point Ref TP Doc# OMA-TP-2002-1234-xxyyzForApproval
OMA-xxyyz-V1_1-20030405-A	05 Apr 2003	description of changed Ref TP Doc# OMA-TP-2003-0321-xxyyzV1_1forApproval

A.2 Draft/Candidate Version 1_0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS_BCAST-MBMS-Adaptation_V1_0	15 Dec 2004		Initial Document Template approved
	21 Nov 2005		Created from: OMA-BCAST-2005-0612-Cell-ID-based-broadcast-for-MBMS-adaptation-specification OMA-BCAST-2005-0618R01-MBMS-adaptation-spec
	04 Jan 2006		Created from: OMA-BCAST-2005-0732-CR-MBMS_Interaction OMA-BCAST-2005-0670R02-CR-MBMS-bearer-independence
	15 Mar 2006		Created from: OMA-BCAST-2006-0225R01-CR-harmonized-BCAST-crossreferences OMA-BCAST-2006-0251-CR-MBMS-adaptation-of-initial-buffering
	24 Mar 2006		Created from OMA-BCAST-2005-0722R05-Sharing_Single_protected_Stream Adding SCR tables in the Appendix B.
	19 Apr 2006		Update of 2006 Copyright and comments boxes/empty Appendix C from template deleted
	26 Dec 2006		Created from OMA-BCAST-2006-271 OMA-BCAST-2006-390R01 OMA-BCAST-2006-341R01 OMA-BCAST-2006-960R01 OMA-BCAST-2006-729R01 OMA-BCAST-2006-971R01 OMA-BCAST-2006-779
	11 Jan 2007		Update of OMA-TS-BCAST_MBMS_Adaptation-V1_0-20061226 as modifying the editorial errors.
	23 Jan 2007		Update of OMA-TS-BCAST_MBMS_Adaptation-V1_0-20070111 as modifying the editorial errors.
	16 Mar 2007		Created from OMA-BCAST-2007-255R01 OMA-BCAST-2007-256 OMA-BCAST-2007-370 OMA-BCAST-2007-400 OMA-BCAST-2007-405R02
	28 Mar 2007	All	Cleanup in preparation for Approval as Candidate
	4 Apr 2007	6.2.4	Editorial changes for a reference
Candidate Version OMA-TS_BCAST-MBMS-Adaptation_V1_0	29 May 2007	n/a	Status changed to Candidate by TP TP ref# OMA-TP-2007-0129R01-INP_BCAST_V1_0_ERP_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 (Broadcast Distribution System), may overrule or adapt requirements from this SCR or provide additional requirements.

a. 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. 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	
BCAST-MBMSBSM-	Support DRM profile for	TS-MBMS-Adaptation	O	

Item	Function	Reference	Status	Requirement
S-018	Service Protection	7.4.2.2		
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	

c. 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	O	

Item	Function	Reference	Status	Requirement
		6.5.1.and 6.5.3		
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	

Item	Function	Reference	Status	Requirement
BCAST-MBMSBSDA-S-024	Support ISMACrypt	TS-MBMS-Adaptation section 7.4.1	O	
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	

d. 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