bmcoforum
Broadcast_Mobile_Convergence

bmcoforum **Recommendation for Implementation Profile**

OMA BCAST Service and Content Protection: Smartcard Profile

Approved Version 2.0

30 June 2009

Based on OMA BCAST V1.0 Enabler Specification

This document is solely for information and has no binding status for any party, not even the **bmco**forum members.

Note

This document is provided for information purposes only. Unless permitted by law, the document or any part of it may not be reproduced, published, adapted or distributed, in any form and by any means without prior written consent of **bmco**forum.

This document is provided on an "as is" basis. **bmco**forum does not represent or warrant that the information provided in the document is accurate, complete, current or suitable for a specific use. **bmco**forum has not conducted an intellectual property rights review of this document and the information contained herein and makes no representations or warranties regarding third party intellectual property rights or other rights that might be claimed to pertain to the document and the information contained herein. In particular, **bmco**forum disclaims any responsibility for identifying the existence of or for evaluating the applicability of any copyrights, patents, patent applications, trade secrets or other intellectual property rights, licenses and respective restrictions, the extent to which any license under such rights might or might not be available and takes no position on the validity or scope of any such rights. **bmco**forum is not liable for and hereby disclaims any damages or losses arising out of or in connection with the use of this document or the information contained herein.

Content:

Introduction

Scope

The “Broadcast Mobile Convergence Forum” (**bmco**forum) is an international organisation targeting to shape an open market environment (eco-system) for mobile broadcast services. This ranges from support of the various bearer technologies over application architecture to regulatory and business issues.

The Interoperability Work item (WI2) targets on enabling interoperability between back end systems and terminals of different vendors, even before standards are available or complete.

For this purposes and based on commercial requirements from our membership, profiles of the standard specifications are developed. The profiles serve as a prioritization for implementers so that interoperability of the profile features can be maximised. The profiles are prepared as valid subsets of the standard.

The main objective of the recent activity is to facilitate and accelerate the development of OMA BCAST implementations by focussing implementations of **bmco**forum members who wish to launch mobile TV services to a subset of features which has been agreed between operators, system and handset vendors.

As the specifications **bmco**forum are profiling will evolve, the profiles are reviewed and enhanced. Still, the profiles may not include the entire specifications, since **bmco**forum works on the superset of commercial requirements of its members.

Implementers of the profiles may use other features of OMA BCAST, however with the caveat that they may not be supported by other **bmco**forum profile implementers.

This document includes **bmco**forum’s implementation profile recommendation for the Smartcard Profile of the OMA BCAST 1.0 Enabler. It is intended to support industry players in developing interoperable OMA BCAST 1.0 standards-based solutions.

This document is intended to be used as a support and clarification when implementing OMA BCAST 1.0 Smartcard Profile.

The used reference OMA BCAST baseline document has been:
Service and Content Protection for Mobile Broadcast Services, Open Mobile Alliance, [1].

The document contains the following information:

- A list of the OMA BCAST 1.0 Smartcard Profile features which are required by **bmco**forum members who wish to launch mobile TV services.
- Implementation guidelines related to those features (where appropriate).

How to read this document

The chapter numbering in this document matches that of the original OMA BCAST Services specification [8] and OMA BCAST Service and Content Protection specification [1].

Therefore after this introduction the numbering jumps to '5' (to match [8] numbering and then '6' to match [1] numbering). This makes it easier to cross-reference against the original OMA items.

This document profiles a baseline of OMA BCAST features intended to promote interoperability between the service providers, mobile and broadcast operators and terminal vendors involved in a BCAST deployment. The phrases "part of this profile"/"not part of this profile" are used instead of "supported/not supported". This is because implementers may use other features of OMA BCAST, however with the caveat that they may not be supported by other **bmco**forum profile implementers. If a particular feature described in the referred BCAST specification(s) is not explicitly mentioned in this profile, it means that the feature is implicitly "not part of this profile".

Terminology

Content Encryption	The cipher algorithm is applied on the data in a file before packetization for transport or encapsulations occur.
Content Protection	This involves the protection of content (files or streams) during the complete lifetime of the content i.e. it is NOT an access control mechanism as it involves post-acquisition rules. Content protection is enabled for encrypted content through the use of appropriate rules or rights, e.g. using DRM Profile or Smartcard Profile based solution for file and stream distributed content. Content remains protected in the Terminal. Usage rules are enforced at "consumption time" (based on DRM or Smartcard Profile). In addition to subscription and pay-per-view, typically associate with Service Protection, Content Protection enables more fine-grained usage rules, such as for displaying, saving in unencrypted form, printing, processing, re-distributing, etc.
Long-Term Key Message	Collection of keys and possibly, depending on the profile, other information like permissions and/or other attributes that are linked to items of content or services.
MIKEY (Multimedia Internet KEYing)	IETF defined key management protocol to support multimedia security protocols, as defined in [7] and BCAST extension in [12]
Secure	The secure function protects sensitive data such as

Function	cryptographic keys introduced by either the DRM Profile or the Smartcard Profile. Only an authorized agent is allowed to access the sensitive data. To ensure that the sensitive data is not manipulated fraudulently, it is integrity protected. The sensitive data are also cryptographically protected to guarantee its confidentiality. The secure function can be implemented on either the smartcard i.e. USIM, or on the terminal.
Service Protection	This involves protection of content (files or streams) during its delivery i.e. it is an access control mechanism only. Content is freely available (thus unencrypted) once it is securely delivered. For the benefit of allowing Content Protection to be provided for the same service, Service Protection is limited to immediate consumption / rendering only.
Short-Term Key Message	Message delivered alongside a protected service, carrying key material to decrypt and optionally authenticate the service, and access rights to delivered content.
Smartcard Profile	The Smartcard Profile uses the Service and Content Protection solution for BCAST receivers in which the long term key management and registration is based on GBA and USIM (for 3GPP MBMS) or a pre-provisioned shared secret key and R-UIM (for 3GPP2 BCMCS).
UICC	A Universal Integrated Circuit Card, an ICC (or 'smart card') is a physically removable secured device as defined in [3] for communication purposes not restricted to mobile convenience only. It is a platform to all the resident applications (e.g. USIM)
USIM	A Universal Subscriber Identity Module is an application defined in [4] residing in the memory of the UICC to register services provided by 3GPP mobile networks with the appropriate security.

Abbreviations

ECMG	Entitlement Control Message Generator
LTKM	Long Term Key Message
MIKEY	Multimedia Internet KEYing
OMA	Open Mobile Alliance
PEK	Program Encryption Key
SCS	SimulCrypt Synchroniser

SEK	Service Encryption Key
SMK	Subscriber Management Key
STKM	Short Term Key Message
TEK	Traffic Encryption Key

References

[1] Service and Content Protection for Mobile Broadcast Services, Open Mobile Alliance, OMA-TS-BCAST_SvcCntProtection-V1_0, available from http://www.openmobilealliance.org

[2] Broadcast Distribution System Adaptation - IPDC over DVB-H, OMA-TS-BCAST_DVB_Adaptation-V1_0, available from http://www.openmobilealliance.org

[3] UICC-terminal interface; Physical and logical characteristics, 3rd Generation Partnership Project, Technical Specification 3GPP TS 31.101, http://www.3gpp.org/

[4] Characteristics of the Universal Subscriber Identity Module (USIM) application, 3rd Generation Partnership Project, Technical Specification 3GPP TS 31.102, http://www.3gpp.org/

[5] Generic Authentication Architecture, Generic Bootstrapping Architecture, 3rd Generation Partnership Project, Technical Specification 3GPP TS 33.220, http://www.3gpp.org/

[6] Security of Multimedia Broadcast/Multicast Service, 3rd Generation Partnership Project, Technical Specification 3GPP TS 33.246, http://www.3gpp.org/

[7] MIKEY: Multimedia Internet KEYing, J. Arkko, E. Carrara, F. Lindholm, M. Naslund, K. Norrman, RFC 3830 August 2004, http://www.ietf.org/rfc/rfc3830.txt

[8] Mobile Broadcast Services, OMA-TS-BCAST_Services-V1_0, available from http://www.openmobilealliance.org

[9] ISMA 1.0 Encryption and Authentication, Version 1.1, release version, http://www.isma.tv

[10] OMA BCAST System Adaptation: IPDC over DVB-H, **bmco**forum Recommendation for Implementation Profile, V2.0 20090630-A

[11] OMA BCAST Services: **bmco**forum Recommendation for Implementation Profile, Launch Profile, V2.0 20090630-A

[12] Multimedia Internet KEYing (MIKEY) General Extension Payload for Open Mobile Alliance BCAST 1.0, A. Jerichow, L. Piron, RFC 5410 January 2009, http://tools.ietf.org/html/rfc5410

[13] The Key ID Information Type for the General Extension Payload inMultimedia Internet KEYing (MIKEY), E. Carrara, V. Lehtovirta, K. Norrman, RFC 4563 June 2006, http://www.ietf.org/rfc/rfc4563.txt

Overview

The OMA BCAST Smartcard Profile defines service protection and content protection mechanisms which provide secure access to a broadcast channel distributing video and audio content. Access control is required to distinguish between subscribed and non-subscribed users. The Smartcard Profile uses a 4-level key hierarchy and is based on GBA [5] and MBMS security [6] features as well as USIM security as specified by 3GPP. Readers of this document are expected to be familiar with the OMA BCAST Smartcard Profile.

Selected Features (Clients)

The following table summarises the features covered by the **bmco**forum profile on the client side. Further details of each feature are given in later sections.

Note that smartcards and terminals which only support MBMS Security are not capable of supporting this profile without extensions. The profile therefore applies to OMA BCAST smartcards and terminals.

Category	**Feature**	**Sections in [1]**	**SCR Reference in [1]**
Service Provisioning	Web Portal initiated purchasing (enabling features, e.g. BSM solicited pull message)	6.10.3. Also see 5.1.9 in [8]	---. See BCAST-SERVICES-C-010 in [8]
Service Provisioning	Message-based service provisioning (selected messages described below)	6.6. Also see 5.1.6 in [8]	---. See BCAST-SERVICES-C-008 in [8]
Content Encryption	ISMACryp 1.1 with no authentication	6.8.1.1, 9.3, 9.3.1, 9.3.3. Also see [9]	BCAST-ContentLayer-C-001
STKM	STKM processing for the selected features	6.7, 6.7.2, 6.7.3.1-2	BCAST-STKM_SC-C-02
LTKM	LTKM processing including EXT BCAST for LTKM, security policy extension values 0x04 and 0x0A and other selected features.	6.6, 6.6.4, 6.6.4.1-2, 6.6.6.1, 6.6.7.1, 6.6.7.7, 6.6.7.14	BCAST-LTKM_SC-C-03

LTKM Delivery	LTKM push delivery over UDP	6.6	BCAST-LTKM_SC-C-04
LTKM Delivery	LTKM Request delivery	6.6	BCAST-LTKM_SC-C-05
LTKM Delivery	LTKM verification messages	6.6.6,6.6.6.1, 6.6.7.7	BCAST-LTKM_SC-C-06
LTKM Delivery	BSM-solicited pull procedure initiation over SMS bearer	6.6.2-3	BCAST-LTKM_SC-C-07
LTKM Delivery	LTKM delivery over HTTP	5.1.6.7.3, 5.1.6.8.1, 5.1.6.9.1, 5.1.6.10.3 in [8]	---
LTKM Delivery	Signaling of supported delivery methods	5.1.6.7.1, 5.1.6.7.2 , 5.1.6.10.1	---
LTKM Delivery	LTKM Controlled SEK/PEK and SPE Deletion	6.6.7.5	BCAST-LTKM_SC-C-08
Registration	MBMS User Registration and Deregistration behaviour, including extensions, as defined in BCAST	See sections 5.1.6.7 and 5.1.6.9 in [8]	BCAST-LTKM_SC-C-09
Registration	BSM Solicited Pull Procedure to initiate the Registration procedure	6.6.3	BCAST-LTKM_SC-C-010
Parental Control Message delivery	Parental control message delivery over HTTP	5.1.6.7.2, 5.1.6.11.2 in [8]	---
Parental Control Message Delivery	Signaling of supported delivery methods for parental control messages	5.1.6.7.1, 5.1.6.11.1 in [8]	---
Subscriber Key establishment	GBA-U	6.5.1	---
SDP Signalling	SDP Signalling of STKM including srvKeyList	10.1	---

SDP Signalling	SDP Signalling of ISMACryp	10.2	BCAST-SDP-C-011. Also see section 8 of [9]
BDS Adaptation	DVB-H generic adaptation mode	See [2] and [10]	---
Authenticate command	Parameters required for **bmco**forum profile features, e.g. parental control	Appendix E.2.1.1-2, E.2.2	BCAST-SCCommands-C-035, BCAST-SCCommands-C-036
Support of OMA BCAST Command: SPE Audit Mode	Retrieves information about keys and SPEs on the smartcard.	Appendix E.3.1, E.3.2	BCAST-SCCommands-C-012
Event signalling mode	Signals to the Smartcard that a specific event occurred	Appendix E.3.1, E.3.5	---

Table 1: Client Features

Selected Features (Smartcard)

The following table summarises the smartcard features covered by the **bmco**forum profile.

Category	**Feature**	**Sections in [1]**	**SCR Reference in [1]**
STKM	STKM processing for the selected features	6.7, 6.7.2, 6.7.3.1, 6.7.3.5-9, 6.7.3.11.1, 7.1, 7.1.1, 7.2, 7.3	BCAST-SCSPCP-C-001
LTKM	LTKM processing including EXT BCAST for LTKM, security policy extension values 0x04 and 0x0A and other selected features.	6.6, 6.6.4, 6.6.4.1-2, 6.6.7.2-7, 6.6.7.13-14	BCAST-SCSPCP-C-002, BCAST-SCSPCP-C-03, BCAST-SCSPCP-C-04
LTKM Delivery	LTKM verification messages	6.6.6, 6.6.6.1, 6.6.7.7	BCAST-SCSPCP-C-05

LTKM	LTKM Controlled SEK/PEK and SPE Deletion	6.6.7.5	---
Parental Control	Parental rating enforcement by the smartcard	6.6.5, 6.6.5.1-2, 6.7.3.11.1, 7.1, 7.1.1	BCAST-SCSPCP-C-06, BCAST-SCSPCP-C-07
Subscriber Key establishment	GBA-U	6.5.1	---
Authenticate command	Parameters required for **bmco**forum profile features, e.g. parental control	Appendix E.2.1.1-2, E.2.2	BCAST-SCSPCP-C-08, BCAST-SCSPCP-C-029
SPE Audit Mode	Retrieves information about keys and SPEs on the smartcard.	Appendix E.3.1, E.3.2	BCAST-SCSPCP-C-09
Event signalling mode	Signals to the Smartcard that a specific event occurred	Appendix E.3.1, E.3.5	---

Table 2: Smartcard Features

Selected Features (BSM and BSD/A)

The following table summarises the features covered by the **bmco**forum profile on the server side. Further details of each feature are given in later sections.

Category	**Feature**	**Sections in [1]**	**SCR Reference in [1]**
Service Provisioning	Web Portal initiated purchasing (enabling features, e.g. e.g. BSM solicited pull message)	6.10.3. Also see 5.1.9 in [8]	---. See BCAST-SERVICES-C-010 in [8]
Service Provisioning	Message-based service provisioning (selected messages are listed below)	6.6. Also see 5.1.6 [8]	---. See BCAST-SERVICES-C-008 in [8]
Server-side interfaces	Support SP-4 by the adaptation of DVB Simulcrypt Head-end interfaces	13.1.1	BCAST-BSMSPCP-S-003

Content Encryption	ISMACryp 1.1 with no authentication	6.8.1.1, 9.3, 9.3.1, 9.3.3. Also see [9]	BCAST-BSDASPCP-S-030
STKM	STKM formatting and delivery for the selected features	6.7, 6.7.2 6.6.7.14, 7.1, 7.1.1, 7.2, 7.3	BCAST-BSMSPCP-S-034, BCAST-BSMSPCP-S-035, BCAST-BSMSPCP-S-039
LTKM	LTKM generation including EXT BCAST for LTKM, security policy extension values 0x04 and 0x0A and other selected features.	6.6, 6.6.2, 6.6.3, 6.6.4, 6.6.6.1, 6.6.4.1-2, 6.6.7.13-14	BCAST-BSMSPCP-S-013, BCAST-BSMSPCP-S-018, BCAST-BSMSPCP-S-019, BCAST-BSMSPCP-S-028
LTKM	LTKM verification messages	6.6.6, 6.6.6.1	BCAST-BSMSPCP-S-032
LTKM Delivery	LTKM Push delivery over UDP	6.6	BCAST-BSMSPCP-S-014
LTKM Delivery	LTKM Request delivery	6.6	BCAST-BSMSPCP-S-015
LTKM Delivery	LTKM delivery over HTTP	5.1.6.7.3, 5.1.6.8.1, 5.1.6.9.1, 5.1.6.10.3 in [8]	---
LTKM Delivery	Signaling of supported delivery methods	5.1.6.7.1, 5.1.6.7.2 , 5.1.6.10.1 in [8]	---
LTKM Delivery	BSM-solicited pull procedure initiation over SMS bearer	6.6.2-3	BCAST-BSMSPCP-S-016
LTKM Delivery	LTKM Controlled SEK/PEK and SPE Deletion	6.6.7.5	---

Registration	Registration and deregistration procedure: MBMS User Registration/DeRegistration including extensions	See sections 5.1.6.7 and 5.1.6.9 in [8]	BCAST-BSMSPCP-S-01
Registration	BSM Solicited Pull Procedure to initiate the Registration procedure	6.6.3	BCAST-BSMSPCP-S-017
Subscriber Key establishment	Subscriber Key Establishment: GBA-U	6.5.1	BCAST-BSMSPCP-S-012
Parental Control	Parental rating enforcement by the smartcard	6.6.5, 6.6.5.1-2	BCAST-BSMSPCP-S-031, BCAST-BSMSPCP-S-036
Parental Control Message delivery	Parental control message delivery over HTTP	5.1.6.7.2, 5.1.6.11.2 in [8]	---
Parental Control Message Delivery	Signaling of supported delivery methods for parental control messages	5.1.6.7.1, 5.1.6.11.1 in [8]	---
SDP Signalling	Signalling of STKM streams (including srvKEYList) in SDP	10.1	BCAST-BSDASPCP-S-035
SDP Signalling	SDP Signalling of ISMACryp	10.2	BCAST-BSDASPCP-S-036
BSD Adaptation	DVB-H generic adaptation mode	See [2] and [10]	

Table 3: BSM and BSD/A Features

OMA BCAST Mobile Broadcast Services Sections

The **bmco**forum Smartcard Profile only includes features which must be available in Smartcard Profile implementations to enable the service provisioning methods defined in [8]. Both the service provisioning message and web portal based provisioning methods are enabled. The full set of service provisioning features required for launch is defined in the **bmco**forum Services launch profile [11]. The section numbers below correspond to the section numbers in [8].

5.1.3 Message Authentication

GBA session information must be available to the Services implementation so that authentication can be supported in web-portal and message-based provisioning. This can be enabled via an authentication proxy or some mechanism of passing GBA session information between the Smartcard Profile and Services implementations. The exact mechanism to be used is outside thescope of this profile.

5.1.6 Smartcard Profile service Provisioning Messages

The selected messages (see subsections below) from smartcard profile service provisioning are part of the profile.

5.1.6.3 LTKM Renewal, Response and Completion Messages

LTKM renewal and verification as described by 5.1.6.3 of [8] is part of the profile.

5.1.6.7 Registration Procedure

The registration procedure as defined by 5.1.6.7 of [8] is part of the profile.

5.1.6.7.1 RegistrationRequestExtension

The RegistrationRequestExtension defined in 5.1.6.7.1 of [8] is part of the profile

5.1.6.7.2 RegistrationResponseExtension

The RegistrationRequestExtension defined in 5.1.6.7.2 of [8] is part of the profile. Note that this extension also enables parental control message delivery over HTTP.

5.1.6.7.3 RegistrationResponseServiceExtension

The RegistrationReponseServiceExtension as defined in 5.1.6.7.3 of [8] is part of the profile. Note that this extension also enables LTKM delivery over HTTP.

5.1.6.8 LTKM Request Procedure

The LTKM request procedure as specified by 5.1.6.8 of [8] is part of the profile.

5.1.6.8.1 LTKMResponseMSKExtension

The LTKMResponseMSKExtension, which enables LTKM delivery over HTTP, as defined in 5.1.6.8.1 of [8] is part of the profile.

5.1.6.9 Deregistration Procedure

The de-registration procedure as defined by 5.1.6.9 of [8] is part of the profile.

5.1.6.9.1 Deregistration Response Service Extension

The DeregistrationResponseServiceExtension as defined in 5.1.6.9.1 of [8] is part of the profile. Note that this extension also enables LTKM delivery over HTTP.

5.1.6.10 LTKM Delivery Mechanisms

LTKM Delivery over UDP and HTTP as well as trigger delivery over UDP and SMS bearers is part of the profile.

5.1.6.10.1 Signaling of supported delivery mechanisms for triggers and LTKMs

The signalling of LTKM delivery methods as referenced in 5.1.6.10.1 and defined in section 5.1.6.7.1 and 5.1.6.7.2 of [8] is part of the profile.

5.1.6.10.2 LTKM delivery over SMS

The BSM solicited pull procedure and the BSM Solicited Pull Procedure to initiate registration as referenced in section 5.1.6.10.2 of [8] and defined in section 6.6.1 and 6.6.2 of [1] is part of the profile.

5.1.6.10.3 LTKM delivery over HTTP

HTTP delivery of LTKMs as referenced in 5.1.6.10.3 of [8] and defined in 5.1.6.7.3 (RegistrationResponseServiceExtension), 5.1.6.8.1 (LTKM Response), 5.1.6.9.1 (Deregistration response) of [8] are part of the profile.

5.1.6.10.4 LTKM General Processing

The LTKM general processing guidelines, and in particular the text on how to address LTKM verification messages (IP address and ports), in this section is part of the profile.

5.1.6.11 Parental control messages delivery mechanisms

Parental control message delivery over UDP and HTTP is part of the profile.

5.1.6.11.1 Signaling of supported Parental Control Message delivery mechanisms

Signaling of supported parental control messages delivery mechanisms as referenced in 5.1.6.11.1 and defined in 5.1.6.10.1 of [8] is part of the profile.

5.1.6.11.2 Parental Control Message delivery over HTTP

Parental Control Message delivery over HTTP as referenced in 5.1.6.11.2 and defined in 5.1.6.7.2 of [8] is part of the profile.

5.1.6.11.3 Parental Control Message general processing

The parental control message processing guidelines as referenced in 5.1.6.11.3 and defined in 5.1.6.10.4 of [8] is part of the profile.

5.1.6.12 PDP context handling

The PDP context handling rules defined in 5.1.6.12 are part of the profile.

5.1.9 Web-based Service Provisioning

The guidelines on usage of web-based provisioning for the smartcard profile, e.g. usage of BSM solicited pull message, are part of the profile.

OMA BCAST Service and Content Protection Sections

Each of the following sections uses the same chapter numbering as the corresponding features in [1]. The text below defines features from those sections which are part of the profile and any implementation options which should be used.

All specification text from [1] should be followed in line with the implementation options required below. Any chapter from [1] not mentioned below is not part of the **bmco**forum profile

6.4 Use of Pre-provisioned Keys

The Smartcard Profile uses a pre-provisioned "Smartcard Key" (SCK) stored on the smartcard to establish the shared layer 1 key(s) between the BSM and the smartcard. The methods used to provision the SCK are outside the scope of the **bmco**forum profile.

6.5 Layer 1: Subscriber Key Establishment

Establishment of a Subscriber Management Key (SMK) using a (U)SIM is part of the profile. Establishment of an SMK using an IUIM/CSIM is not part of the profile.

Note that the Ua protocol used for this GBA procedure is the Ua protocol defined for MBMS, i.e. The Ua protocol value is 0x01 0x00 0x00 0x00 0x01.

6.5.1 Subscriber Key Establishment using a (U)SIM

GBA-U is part of the profile and is used for the establishment of shared keys between the BSM and the smartcard. GBA-ME is not part of this profile.

The GBA procedure is initiated as defined in Section 6.1 of [6].

6.6 Layer 2: Service Provisioning and LTKM Delivery

The MIKEY Message Format [7] is used to deliver LTKMs. It corresponds to the MIKEY format defined by [6] and [13] together with a BCAST extension payload [section 6.6.4 in [1] and [12]] known as the EXT BCAST for LTKM.

The CSB ID (Crypto session bundle ID) in [12] in LTKM MIKEY messages is created at random for every LTKM MIKEY message. The CS ID map type subfield SHALL be set to value "1' (empty map) as defined in [13] regardless of whether SRTP authentication is used or not. The number of crypto sessions (#CS), defined in the MIKEY header, is set to 0. SP is not present since it is only used when the LTKM addresses a streaming service which uses SRTP.

The HTTP DIGEST authentication directives defined in this section and used in the LTKM Request, Registration and Deregistration procedures are part of the profile.

The LTKM delivery procedures which are part of the profile are fully specified elsewhere in this document but they include

- Push delivery of LTKMs via UDP.
- Delivery of LTKMs over HTTP.
- BSM solicited pull procedure initiation over UDP and SMS bearers.
- The BSM solicited pull procedure to initiate the registration procedure over UDP or SMS bearers.

6.6.2 BSM Solicited Pull Procedure Initiation over SMS Bearer

BSM Solicited Pull Procedure Initiation over SMS Bearer is part of the profile.

6.6.3 BSM Solicited Pull Procedure to initiate the Registration Procedure

BSM Solicited Pull Procedure to initiate registration bearer is part of the profile. Both UDP and SMS delivery methods will be supported.

6.6.4 EXT BCAST for LTKM

The EXT BCAST for LTKM including the following parameters is part of the profile. These parameters are further described in Section 6.6.4.2 of [1].

Parameter	Value
protocol_version	0x0
security_policy_ext_flag	LTK_FLAG_TRUE if a security_policy_extension is carried, LTK_FLAG_FALSE otherwise.
security_policy_extension	SPE values 0x04 or 0x0A are part of the profile

Table 4: EXT BCAST fields and values

6.6.4.1 Constant Values

The constants in this section are part of the profile.

6.6.4.2 Coding and semantics of attributes

The coding and semantics of the parameters in Table of this profile document above (according to the rules defined in Section 6.6.4.2 [1]) is part of the profile.

6.6.5 Parental Control Message Structure and Processing

The MIKEY message for parental control is part of the profile.

6.6.5.1 EXT BCAST Parental Control

The EXT BCAST parental control data payload is part of the profile. Rating_type value 0 (as defined by OMNA) is part of the profile.

6.6.5.2 Parental Control Message Processing

This profile assumes that the secure function is located in the smartcard. The processing described in this section relevant to a secure function on the smartcard is part of the profile.

6.6.6 LTKM Verification Message and Reporting Message Structure

The LTKM verification message sent to confirm successful reception of an LTKM is part of the profile. The LTKM Reporting Message is *not* part of the profile.

6.6.6.1 LTKM Verification Message

The format of the LTKM verification message as defined in section 6.4.5.2 of [6] is part of the profile.

6.6.7 OMA BCAST LTKM Processing

The LTKM processing described in the selected subsections below is part of the profile for the smartcard.

6.6.7.1 LTKM Terminal Processing

The terminal processing of LTKMs described in this section is part of the profile.

6.6.7.2 Initial LTKM Processing in the Smartcard

The smartcard processing of LTKMs described in this section is part of the profile.

6.6.7.3 LTKM Message Validation

The message validation processing described in this section is part of the profile.

6.6.7.4 LTKM Replay Detection in the Secure Function

The LTKM replay detection check performed by the smartcard and described in this section is part of the profile.

6.6.7.5 LTKM Controlled SEK/PEK and SPE Deletion

LTKM controlled SEK and SPE deletion as described in this section is part of the profile.

Note that for the BSM, SPE deletion of a single SPE with a given key validity (2nd bullet in this section) is *not* part of the profile.

6.6.7.6 LTKM Processing based on security_policy_extension (SPE)

The processing of SPE values 0x04 (subscription to live content) and 0x0A (key deletion) as described in this section is part of the profile.

6.6.7.7 LTKM Verification Message Request

The creation of LTKM verification messages when a V-bit is detected in the incoming LTKM is part of the profile.

6.6.7.13 Association between Parameters and IDs Stored in Secure Function

The associations defined in this section are part of the profile.

6.6.7.14 Implementation Notes

The implementation notes in this section relevant to the other features supported in the **bmco**forum smartcard profile are part of the profile.

6.7 Short Term Key Message – STKM

The MIKEY Message Format [7][12] used to deliver smartcard profile STKMs is part of the profile.

The CSB ID is newly created by random for every MIKEY message. The number of crypto sessions (#CS), defined in the MIKEY header, is set to 0. The TEK is included in the message's key data payload. The key data is always of type 2 (TEK without salt).

6.7.2 EXT BCAST for STKM

The EXT BCAST for STKM is part of the profile. The following parameters in the payload, many of which are more completely specified in section 7 of [1], are part of the profile.

Parameter	Value
protocol_version	0x0 (i.e. the original format)
protection_after_reception	0x03 (service protection)

access_criteria_flag	TKM_FLAG_TRUE if parental control access criteria are included. Otherwise TKM_FLAG_FALSE
traffic_protection_protocol	TKM_ALGO_ISMACRYP
traffic_authentication_flag	TKM_FLAG_FALSE. Authentication is not supported in the **bmco**forum profile
number_of_access_criteria_descriptors	Number of access_criteria_descriptors present in the STKM
access_criteria_descriptor_loop	May contain a parental_rating access control descriptor. All parameters within the parental_rating_descriptor access criteria descriptor are part of the profile except for country_code as country_code_flag SHALL always be set to LTK_FLAG_FALSE
secure_channel_flag	TKM_FLAG_FALSE indicates that a secure channel is not required; TKM_FLAG_TRUE indicates that a secure channel is required.

Table 5: STKM EXT BCAST fields and values

6.7.3 OMA BCAST STKM Processing

The secure function on the smartcard supports the STKM processing of the parameters defined in Table of this profile document above and all related STKM features included in this profile.

6.7.3.1 Event Information sent by the Terminal

The use of Event signalling mode to inform the Smartcard of an event that can impact the parental control decision process is part of the profile.

6.7.3.2 STKM Resending Check in the Terminal

The resending check in the terminal is part of the profile.

6.7.3.5 STKM Message Validation in the Secure Function

Message validation is part of the profile.

6.7.3.6 STKM Replay Detection in the Secure Function

The performance of the STKM replay detection check is part of the profile.

6.7.3.7 Choice of the Security Policy Extension (SPE) for Processing the STKM

The smartcard choice of the SPE, where relevant to SPE values 0x04 and 0x0A, is part of the profile.

6.7.3.8 STKM Processing based on the LTKM security_policy_extension (SPE)

STKM processing for SPE values 0x04 and 0x0A is part of the profile.

6.7.3.9 Deletion of Expired LIVE Security Policy Extensions and SEK/PEK

The mechanism for deletion of expired LIVE SPE and SEK/PEK described in this section is part of the profile.

The mechanism described in section 6.7.3.9 only applies to expired SEKs and SPEs for which STKMs have been processed after expiry. If the smartcard manufacturer considers that this and the server-side key deletion mechanisms described in this profile are not sufficient to prevent the card from filling up with expired live SEKs, SPEs and related data, the manufacturer is free to implement supplementary proprietary deletion mechanisms in the smartcard. The exact mechanisms used are at the discretion of the smartcard manufacturer but should not require BSM or terminal involvement.

6.7.3.11 Access Criteria

Parental control access criteria are part of the profile. Location-based access criteria are not part of the profile.

6.7.3.11.1 Parental Control

Enforcement of parental control by the smartcard, including PINCODE management, is part of the profile.

Rating type 0 is part of the profile. Processing of other rating types is not part of the profile.

6.7.4 STKMs and Traffic Encryption Protocols

The Smartcard Profile STKM as used for ISMAcryp is part of the profile. Note that the CS ID map type subfield in STKM message SHALL be set to val‘e”1' (empty map) regardless of SRTP authentication is used or not.

6.8 Layer 4: Traffic Encryption

Service protection of streams is part of the profile. Content protection of streams is not part of the profile. File delivery is not part of the profile.

6.8.1 Streaming Delivery

Service Protection of streams is part of the profile.

6.8.1.1 Service Protection of Streams

Service protection of ISMACryp streams is part of the profile.

6.10.3 Web portal used as an entry point

Web-based provisioning for the smartcard profile, e.g. usage of BSM solicited pull message, is part of the profile.

6.12.1 Use of the secure channel between the smartcard and the terminal

Support for the secure channel is *not* part of the profile.

However, the processing of the secure_channel flag in the STKM is part of theprofile.

7. Short Term key Message – Common Attributes

The common attributes which are part of the profile are listed in section 6.7.2 above.

7.1 Descriptors for access_criteria_descriptor_loop

The parental rating descriptor is part of the profile. The location based descriptor is not part of the profile.

7.1.1 Parental_rating_descriptor

The parental rating descriptor is part of the profile.

7.2 Coding and Semantics of Attributes

The constant values defined in this section are part of the profile.

7.3 Coding and Semantics of Attributes

The common attributes which are part of the profile are listed in section 6.7.2 above. Section 7.3 of [1] elaborates on the meaning of each attribute.

9.3 ISMACryp

ISMACryp 1.1 [9] (used in line with section 9.3 of [1]) is part of the profile with the following exceptions:

- Authentication as defined in section 9.3.2 of [1] is not part of the profile.

9.3.1 Encryption Algorithm

Encryption as defined in this section and IsmaCryp 1.1 [9] is part of the profile.

9.3.3 RTP Transport of Encrypted AUs (ISMACryp)

IsmaCryp 1.1 is part of the profile. The codecs defined in the Section 6.5.4 of [10] are part of this profile.

Ismacryp 2.0 is not part of the profile.

10.1 Protection Signalling in SDP

The signalling of STKM streams is part of the profile.

10.1.2 Short-Term Key Message Streams (STKM)

The parameters is supported for signalling STKM streams in the SDP.

Parameter	**Description**
stream id	Unique positive integer identifying a particular key stream. Numbers are unique within a particular SDP session i.e. no global numbering is required. Used to indicate which media stream is protected by the actual STKM stream.
kmstype	Identifies the Key Management system (KMS) used.
serviceproviders	Identifies the service providers using the key stream, by referencing one or more BSMSelectors as declared in the SGDD in the SG [BCAST10_SG] or by referencing one or more <X>/ServiceProviders/<X>/ID nodes as specified in [BCAST10-Services].
srvKEYList	A list of so-called srvKEY values. Each srvKEY value is a concatenation of the Key Domain ID with the Key Group part of a SEK/PEK associated to the

	related STKM stream. Allows multiple STKM streams to be associated with the same streaming content.

Table 4: Protection signalling parameters for STKM streams

10.2 SDP Signalling of ISMACryp

Support for SDP signaling of ISMAcryp is part of the profile. The following SDP parameters as defined in section 8 of [9] are part of the profile.

- The IV length (ISMACrypIVLength)
- Key indicator length (ISMACrypKeyIndicatorLength)
- Selective encryption (ISMACrypSelectiveEncryption) set to FALSE.
- Salt key (ISMACrypSalt)

13.1 Interface SP-4

For SP-4, the DVB Simulcrypt interface is part of the profile.

13.1.1 Interface SP-4: Adaptation of DVB Simulcrypt Head-End Interfaces to the OMA BCAST Environment

The ECMG/STKMG⇔SCS interface described in section 13.1.1.3.1 is part of the profile in order to:

- Send TEK from the SCS to the ECMG/STKMG to enable the BSM to create the STKM
- Send the STKMs from the BSM to the SCS

The EMMG-LTMKG to Multiplex interface described in section 13.1.1.3.4 of [1] is not part of the profile.

15.3 IPDC over DVB-H adaptation

The “generic adaptation” of IPDC over DVB-H adaptation as specified in [2] and [10] is part of the profile.

Appendix E.1 Terminal-BCAST Smartcard Interface in the Smartcard Profile (Normative)

The following elements of the terminal-smartcard interface are part of the profile:

- MTK generation mode (BCAST management_data operation and parental control operation)
- MSK update mode (BCAST management_data operation)
- SPE audit mode
- Event Signalling mode

Appendix E.2 Extension of the MBMS Security Context

The parameters of the Authenticate command response for the MBMS security Context Mode (extended for BCAST) are part of the profile.

E.2.1 MTK Generation Mode

The response parameters defined for the processing of MTK Generation Mode and required by the BCAST management_data operation and the parental control operation are part of the profile.

E.2.1.1 OMA BCAST Operation Response: BCAST management_data Operation

The coding of the OMA BCAST Operation Response as defined in this section for MTK generation mode (BCAST management_data operation) is part of the profile.

E.2.1.2 OMA BCAST Operation Response: Parental Control Operation

The coding of the OMA BCAST Operation Response as defined in this section for the parental control operation is part of the profile.

E.2.2 MSK Update Mode

The response parameters defined for the processing of MSK Update Mode (BCAST management_data operation) are part of the profile.

E.2.2.1 OMA BCAST Operation Response: BCAST management_data Operation

In the processing of MSK Update Mode (in particular for processing of the parental control message), the response parameters and data defined in this section for the response of the Authenticate Command is part of the profile.

Appendix E.3 OMA BCAST Command

The OMA BCAST command in SPE audit mode and event signalling mode is part of the profile.

Record Signalling mode is *not* part of the profile.

E.3.1 Description of the command

The OMA BCAST command format is part of the profile.

E.3.2 SPE Audit Mode

SPE Audit mode (as required to enable the usage of srvKeylist in SDP signalling – see section 10.1.2) is part of the profile.

E.3.5 Event Signalling Mode

Event signalling mode (as required to enable the usage of parental control on the smartcard) is part of the profile.

Change history

Version	Date / Status	Description of changes
1.0	n/a	Initial version of the Implementation Profile.
1.1	20080708-D	Aligned with bug fixes that have been applied to the referenced versions of the OMA BCAST specifications. No new functionality added. Alignments include: - Updates to Tables 1, 2 and 3 (Features deleted) SCR references where changes - Updates to all section numbers which have changed. - Clarifications of usage of MBMS registration/deregistration - Clarifications of usage of CS ID map type subfield
1.1	20080902-V	Aligned with bug fixes that have been applied in the Aug 26th SPCP specification and Aug 7 services specifications. Alignments include: – Updates to SCR tables – Bug-fixes on parental control and SPE deletion features – Removal of the smartcard profile trigger
1.2	20081209-D	Aligned with bug fixes that have been applied since **bmco**forum profile 1.1 up to and including the Nov 20th SPCP specification and Nov 21 Services specifications. Alignments include ▪ IsmaCryp 2.0 reference update ▪ Clerical BSM SCR updates ▪ Deletion of a single SPE ▪ Removal of smartcard profile trigger ▪ LTKM port clarifications for verification messages. ▪ Reworked services text since all services sections relevant to smartcard profile are now referred to only in the smartcard profile document.

		▪ Various clerical changes to clarify the supported features and clean up inconsistencies. ▪ Removed 6.7.3.4 to indicate that MBMS replay check on the terminal is not part of the profile and also references to service No. 75 (see CR 345R05). ▪ Added text to clarify implicitly excluded features
1.2	20081211-V	
1.2	20090107-A	
2.0	200906016-D	Updated the specification references and added the following features: ▪ Extensions to MBMS Registration including RegistrationRequestExtension, RegistrationResponseExtension, RegistrationResponseServiceExtension, DeregistrationServiceExtension ▪ LTKM delivery over HTTP via LTKMResponse. ▪ srvKEYList in SDP for STKM streams. ▪ Secure channel flag ▪ SPE audit mode ▪ Event signalling mode
2.0	20090622-V	Reference update to the **bmco**forum profile documents V2.0
2.0	20090630-A	