bmcoforum **Recommendation for Implementation Profile**

OMA BCAST Service and Content Protection:

DRM Profile for non-connected devices

Approved Version 2.0

30 June 2009

Based on OMA BCAST V 1.0 Enabler Specification

bmcoforum
Broadcast_Mobile_Convergence

Note:

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 DRM Profile of the OMA BCAST 1.0 Enabler for non-connected devices. 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 the OMA BCAST 1.0 DRM Profile for non-connected devices.

The used reference OMA BCAST baseline documents have been:

Service and Content Protection for Mobile Broadcast Services, Open Mobile Alliance, [1].

OMA DRM v2.0 Extensions for Broadcast Support, Open Mobile Alliance, [2].

The document contains the following information:

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

How to read this document

The document has two main sections, A and B.

The chapter numbering in the section A matches that of the original OMA BCAST Service and Content Protection specification [1]. The chapter numbering in the section B matches that of the original OMA BCAST Extensions for Broadcast Support specification [2].

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

Non-connected device: A device which does not use interactive channel to receive LTKM messages.

Please refer to [1] and [2] for other definitions and abbreviations.

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] OMA DRM v2.0 Extensions for Broadcast Support, Open Mobile Alliance OMA-TS-DRM_XBS-V1_0, available from http://www.openmobilealliance.org

[3] OMA DRM 2.0 Enabler, Open Mobile Alliance™, OMA-ERP-DRM-V2_0, available from http://www.openmobilealliance.org

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

A. Service and Content Protection for Mobile Broadcast Services

A.4 Introduction

The DRM profile for non-connected devices is part of the profile for Service and Content Protection for terminals with or without a cellular radio interface and (U)SIM/R-UIM.

A.4.1.1 Selected technologies

These are the main standards, which are part of the profile. See section 4.1.1 in [1] for more details.

- Advanced Encryption Standard (AES) as specified in [1]
- Secure Internet Protocol (IPsec), as specified in [1]
- ISMACryp v1.1, as specified in [1]
- Traffic Encryption Key (TEK) as specified in [1]
- OMA Digital Rights Management version 2.0 [3] for service and content protection

A.4.1.2 Overview of Operations for Streaming Content

Part of this profile as defined in [1].

A.4.1.3 Overview of Operation for Download of Content

For the DRM Profile the protection of files is part of the profile as defined by the OMA DRM 2.0 specifications [3].

A.4.1.4 Key Management

DRM Profile Key Management as specified in section 4.1.4.1 of [1] is part of this profile.

A.5 DRM Profile

Details about the DRM profile in this profile proposal are listed below.

- The Key provisioning as defined in section 5.2 of [1] is part of the Profile.
- The Layer 1 registration as defined in section 5.3 of [1] for devices that do not support interaction channel is part of the profile. However, OMA DRMv2 Domains and Broadcast Domains are not part of the profile. Further, mixed mode devices and the 'BroadcastRegistration' Trigger according to section 7.3.1 of [2] are not part of the profile.
- Long Term Key Message as specified in 5.4 'Layer 2: Long Term Key Message – LTKM' of [1]

  - Use of Broadcast Rights Objects (BCROs) as specified in 5.4.1 of [1] is part of this profile.
  - The use of OMA DRM v2 extensions for Broadcast Rights Objects is part of this profile. The broadcast delivery of BCROs as defined in 5.2.1 of [2] is part of this profile, as well as the use of the <access> permission (section 8.4.2 of [2]).
  - Use of BCROs in Long Term Key Delivery layer as specified in 5.4.3 of [1] is part of this profile.
- Use of Short Term Key message as specified in the section 5.5 'Layer 3: Short Term Key Message – STKM' of [1] is part of the profile.
- Traffic encryption as defined in section 5.6 'Layer 4: Traffic Encryption' of [1]
  - Use of Layer 4 for Streaming as specified in 5.6.1 of [1] is part of the profile.
  - Use of Layer 4 for File Delivery as specified in 5.6.2 of [1] is part of the profile.
- Recording as defined in section 5.7 of [1] is not part of the profile. SG ignalling as defined in section 5.8 of [1] is part of the profile.
- Usage metering as defined in section 5.9 of [1] is not part of the profile.

More constraints are defined in the **bmco**forum IPDC over DVB-H Adaptation profile document [4].

A.7 Short Term Key Message – Common attributes

This is part of the profile with the exception that Location_based_restriction_descriptor is not part of the profile. Please note that further constraints are specified in the **bmco**forum IPDC over DVB-H Adaptation profile document [4].

Note that in the parental_rating Access Criteria Descriptor, when the rating_type is 0, the rating_value is the minimum age minus 3 (as specified in ETSI EN 300 468). For example, if the minimum allowed age is 18, the rating_value is 0x0F.

A.8 Recording

Not part of the profile.

A.9 Encryption protocols

The technologies for the "Content Layer" in the 4-layer model for Service and Content Protection:

- Use of IPSec is part of the profile as specified in 9.1 of [1].
- Use of ISMACryp v1.1 is part of the profile as specified in section 9.3 of [1], however, authentication as specified in section section 9.3.2 of [1] is not part of the profile. IsmaCryp v2.0 is not part of the profile.

A.10 Signaling

A10.1 Protection Signaling in SDP

Signaling of protection parameters is part of the profile as described in section 10.1 of [1].

Signaling of the LTKM Streams as described in section 10.1.4 of [1] is part of the profile.

A.10.2 SDP Signaling of ISMACryp

The signaling of ISMACryp v1.1 is part of the profile as described in section 10.2 of [1] with the following additions:

- The signaling parameters 'ISMACrypKeyIndicatorLength' and 'ISMACryp-Salt' are used.
- The signaling parameter 'MasterSaltKey' is not used.

A.10.3 Service Guide Signaling

This is part of the profile.

A.11 Common Keys / Sharing Streams for DRM profile and smartcard profile

Common keys are not part of the profile.

A.12 Terminal Binding Key

Terminal Binding Key is not part of the profile.

A.13 Service Side Interfaces and Messages

A.13.1 Interface SP-4

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

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

The ECMG/STKMGSCS interface 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

A.14 Conversion between Time and Date Conventions

The coding of STKM timestamp field, when present, is part of the profile as specified in section 14 of [1].

A.15 Interfaces to Underlying BDSes

Interfacing to the underlying BCMCS BDS as defined in 15.1 of [1] is not part of the profile.

Interfacing to the underlying MBMS BDS as defined in 15.2.of [1] is not part of the profile.

Interfacing to the underlying DVB BDS as defined in 15.3 of [1] is part of the profile for BDS specific adaptation mode as defined in the **bmco**forum IPDC over DVB-H Adaptation profile document [4].

B. OMA DRM v2 Extensions for Broadcast Support

B.5 Four-Layer Key Hierarchy For Service Protection

B.5.1 Registration Layer-Layer 1 Keys (Broadcast Mode)

This is part of the profile.

B.5.2 Long-Term Key Message Layer-Layer 2 Keys

Broadcast delivery of BCROs, as defined in section 5.2.1 of [2] is part of the profile. For addressing modes that are part of this profile, see section 10 below.

Interaction Mode defined in section 5.2.2 of [2] is not part of the profile.

B.5.3 Short-Term Key Message Layer-Layer 3 Keys

This is part of the profile.

B.5.4 Traffic Encryption Layer-Layer 4 Keys

Ipsec and ISMACryp are part of this profile.

B.6 Authentication

Authentication is part of the profile.

B.7 Broadcast Device and Domain Management

B.7.1 General Issues

This is part of the profile.

B.7.2 Broadcast Device Registration

This is part of the profile.

However, the encoding or delivery mechanism of data delivered to the RI is not part of this profile.

B.7.3 On-line Registration

This is not part of the profile.

B.7.4 Offline Notification of Short Device Data for Requests

The encoding or delivery mechanism of data delivered to the RI is not part of this profile. The format of the action request code (ARC) is not part of the profile.

Re-registration (section 7.4.1.1 of [2]) and resend BCRO (section 7.4.1.2 of [2]) are part of this profile.

B.7.5 Inform Registered Device Protocol

Force to Re-Register (section 7.5.2 of [2]), Update RI Certificate (section 7.5.3 of [2]) and Update DRM Time (Section 7.5.4 of [2]) are part of the profile.

Update Contact Number (Section 7.5.5 of [2]) is not part of the profile.

B.7.6 Token Handling

Tokens are not part of this profile.

B.7.7 Domain Management

Domains are not part of this profile.

B.8 Broadcast Rights

B.8.2 Format of the Broadcast Rights Objects

BCRO format as specified in section 8.2 of [2] is part of this profile.

B.8.3 Acquisition of Rights Objects over an Interaction Channel

This is not part of the profile

B.8.4 Save Permission

This is not part of the profile.

However, Access Permission (section 8.4.2 of [2]) is part of the profile.

B.9 Token Management

Tokens are not part of this profile.

B.10 Subscriber Groups

Subscriber groups are part of the profile.

Only the following addressing modes are part of the profile:

- 0x0 Whole Fixed subscriber Group
- 0x1 Subgroup in a Fixed Subscriber Group

- 0x2 A unique device

Other addressing modes are not part of this profile.

B.11 Broadcast Service Support

This is part of the profile.

B.12 Rights Issuer Services

This is part of the profile.

B.13 Adapted File format

This is not part of the profile.

Change history

Version	Date / Status	Description of changes
1.0	20080513-A	Initial version of the Implementation Profile.
1.1	20080709-D	• Alignment of references to latest OMA BCAST specifications. No new functionality added. • Editorial corrections in section A.4 • Clarification that "Location_based_restriction_descriptor" is not part of the profile in sect. A.7. • Clarification that for interface SP-4 theISMACryp encryption protocol is part of the profile (sect. A.13.1).
1.1	20080709-V	
1.1	20080721-A	
1.2	20081111-D	Editorial changes. Updated reference to Final Draft of OMA BCAST specs. Removed unused reference to TS ServiceGuide. Aligned with bug fixes that have been applied to the referenced version of the OMA BCAST specification. No new functionality added. Alignments include: - Signaling of ISMACryp - Profiling-out of mixed mode and Broadcast Registration trigger
1.2	20081128-D	Editorial changes. Updated references to Final Draft OMA BCAST specs and to latest **bmco**forum profile docs.
1.2	20081209-D	Updated references to Final Draft OMA BCAST specs and to latest **bmco**forum profile docs.
1.2	20081211-V	
1.2	20090107-A	
2.0	20090622-V	Reference update to the **bmco**forum profile documents V2.0
2.0	20090630-A	