bmcoforum **Recommendation for Implementation Profile**

OMA BCAST Service and Content Protection:

DRM Profile for connected devices

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.

Broadcast_Mobile_Convergence

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.

Broadcast_Mobile_Convergence

Content:

Broadcast_Mobile_Convergence

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 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 connected devices.

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 DRM Profile for connected devices features which are required by **bmco**forum members who wish to launch mobile TV.
- Implementation guidelines related to those features (where appropriate).

Broadcast_Mobile_Convergence

How to read this document

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

Therefore after this introduction the numbering jumps to '4'. 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

Please refer to [1] for 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, OMA-TS-DRM_XBS_V1_0, available from http://www.openmobilealliance.org

[3] OMA DRM2.0 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

[5] OMA BCAST System Adaptation: 3GPP/MBMS, **bmco**forum Recommendation for Implementation Profile, V2.0 20090630-A

4 Introduction

The DRM profile for connected devices is part of the profile for Service and Content Protection for terminals with a cellular radio interface and (U)SIM/R-UIM.

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

4.1.2 Overview of Operations for Streaming Content

Part of this profile as defined in [1]

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].

4.1.4 Key Management

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

5 DRM Profile

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

- The Key provisioning as defined in section 5.2 is part of the Profile.
- The Layer 1 registration as defined in section 5.3 of [1] 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'
    - Use of Ros as specified in 5.4.1 of [1] is part of this profile.

    - The use of OMA DRMv2 extensions for Broadcast Rights Objects is not part of this profile. However, the interactive delivery of Rights Objects as defined in 5.2.2 and 8.3 of [2] is part of this profile, as well as the use of the <access> permission (section 8.4.2 of [2])
    - Use of Ros 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'
    - 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 signaling as defined in section 5.8 of [1] is part of the profile.
- Usage metering as defined in section 5.9 is not part of the profile

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

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.

8 Recording

Not part of the profile

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.

10 Signaling

10.1 Protection Signaling in SDP

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

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.

10.3 Service Guide Signaling

This is part of the profile.

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

Common keys are not part of the profile.

12 Terminal Binding Key

Terminal Binding Key is not part of the profile.

13 Server Side Interfaces and Messages

For SP-4, when ISMACryp is used, 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/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

Broadcast_Mobile_Convergence

- Send the STKMs from the BSM to the SCS

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].

15 Interfaces to Underlying BDS-es

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 part of the profile for BDS specific adaptation mode as defined in the **bmco**forum IPDC over MBMS Adaptation profile document [5]. 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].

Broadcast_Mobile_Convergence

Change history

Version	Date / Status	Description of changes
1.0	20070930-A	Initial version of 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. Modifications: - Editorial corrections in section A.4 - Clarification that "Location_based_restriction_descriptor" is not part of the profile in sect. 7. - Correction to SDP format in sect. 10.1. - Section 13.1.1 added in alignment with the OMA DRM for non-connected devices profile and Smartcard profile. - Clarification that for interface SP-4 the ISMACryp encryption protocol is part of the profile (sect. 13.1). - Reference to MBMS Adaptation profile added in sect. 15.
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: - ISMACryp signaling - 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 latest **bmco**forum profile docs.
1.2	20081211-V	

Broadcast_Mobile_Convergence

1.2	20090107-A	
2.0	20090622-V	Reference update to the **bmco**forum profile documents V2.0
2.0	20090630-A	