**OMA-DLDRM-2005-0044-Answer-LS-3GPP-SA3-on-DCF**
**Liaison Statement**

# LIAISON STATEMENT

| | |
|---|---|
| Title: | Answer to LS on Adapting OMA DRM v2.0 DCF for MBMS download protection ☒ Public ☐ Confidential LS[1] |
| Date: | 17 feb 2005 |
| To: | 3GPP SA3<br>contact: Tiina Koskinen, tiina.s.koskinen@nokia.com |
| Response to: | LS on Adapting OMA DRM v2.0 DCF for MBMS download protection (S3-041129) |
| Source: | BAC Download Digital Rights Management SWG of the Open Mobile Alliance |
| Send Replies to: | BAC Download Digital Rights Management SWG of Open Mobile Alliance<br>OMA-LIAISON@mail.openmobilealliance.org |
| Contact(s): | Frank Hartung, Ericsson Research, frank.hartung@ericsson.com<br>Oliver Bremer, Nokia, oliver.bremer@nokia.com<br>Robert Lukassen, Philips, robert.lukassen@philips.com |
| Attachments: | <list of attachments> or n/a |

## 1 Overview

This Liaison Statement is in answer to the S3-041129 Liaison Statement from 3GPP TSG WG3 Security – S3#36 in which extensions and deviations to OMA DRM v2.0 DCF for MBMS download protection have been proposed to OMA BAC DLDRM.

The proposals and extensions have been reviewed by the OMA BAC DLDRM sub working group.

## 2 Proposal

With the understanding that 3GPP MBMS DCF content files are used in a transient manner, and will not be exported from receiving devices in their received format, OMA BAC DLDRM does not have objections to the proposed extensions and adaptations as specified by the S3-041129 Liaison Statement.

Specifically:

- OMA BAC DLDRM proposes to define the required new semantics of the extensions and adaptations in the scope of a new minor version of the DCF structure specification. The value of this new minor version will be 0x00000003.
- OMA BAC DLDRM does not see any problem in adding the MBMSSignature Box in the Free Space Box of the OMA DRM v2.0 DCF structure.

  However, because of the generic nature of this feature, OMA BAC DLDRM proposes to change the name:

[1] If the "Confidential LS" box is selected, this liaison statement is intended to be Confidential per agreement by OMA and the addressed organization. Neither side should make this communication available to non-members.

```
aligned(8) class OMADRMSignature extends FullBox('odfs', version, flags)
{
unsigned int(0)   SignatureMethod;  // Signature Method
char              Signature[];      // Actual Signature
}
SignatureMethod field:
NULL        0x00
HMAC-SHA1   0x01
```

This box will be optional, and will appear inside the optional Mutable DRM information box ('mdri').

- OMA BAC DLDRM does not regard global uniqueness of ContentID as critical for DCF files used in the MBMS transport layer. However, if the ContentID is to propagate above the MBMS transport layer, OMA BAC DLDRM does recommend 3GPP SA3 to reconsider and define a method to ensure globally unique ContentIDs.
- OMA BAC DLDRM will define the 'mbms-key://<key_id>' mechanism as the URL scheme to use to interpret the value of the RightsIssuerURL field in case the DCF is used in the MBMS context.
- OMA BAC DLDRM feels that the new minor version number along with the structure of the value of the RightsIssuerURL field should be enough information to prevent misunderstanding of a MBMS DCF in a general OMA DRM context, or vice versa. Hence the definition of the special value 1 of the flags field in the CommonHeaders box is unnecessary.

## 3 Requested Action(s)

OMA BAC DLDRM requests 3GPP SA3 to review this answer and in particular see whether the changes proposed by this liaison statement are acceptable to 3GPP SA3. This refers in particular to the proposed name of the signature box and its positioning in the Mutable DRM information box, and the proposed use of the minor version number 0x00000003 instead of using the 'flags=1' indicator.

The extensions and adaptations as presented by this document will be incorporated into the specifications that are now work-in-progress. As soon as the references to the final specifications containing these extensions and adaptations are known, OMA BAC DLDRM will make these references known to 3GPP SA3. According to the current work schedule, this may be expected in August 2005.

## 4 Conclusion

Open Mobile Alliance, through its active sub-working group BAC-DLDRM, wishes to express its gratitude to 3GPP for considering this liaison statement.