**3GPP TSG SA WG3 Security — S3#36** **S3-041057**
**Shenzhen, China, November 23-26, 2004**

| | |
|---|---|
| **Title:** | [DRAFT] LS on Adapting OMA DRM v2.0 DCF for MBMS download protection |
| **Response to:** | |
| **Release:** | Rel-6 |
| **Work Item:** | MBMS |
| | |
| **Source:** | 3GPP SA3 |
| **To:** | OMA BAC DLDRM |
| **Cc:** | |

**Contact Person:**

| | |
|---|---|
| **Name:** | Tiina Koskinen |
| **Tel. Number:** | +358 50 482 1347 |
| **E-mail Address:** | tiina.s.koskinen@nokia.com |

| | |
|---|---|
| **Attachments:** | S3-040903 (CR), TS 33.246 |

---

### 1. Overall Description:

3GPP SA3 would like to inform OMA BAC DLDRM that SA3 has decided to re-use the DCF format from OMA DRM v2.0 as a basis for MBMS download protection. SA3 has identified the following extensions and deviations to OMA DRM v2.0 DCF when adapting it for MBMS purposes:

- To distinguish an MBMS protected DCF content from ordinary OMA DRM v2.0 DCF content, SA3 proposes to define a 3GPP MBMS flag in the Common Headers Box.

```
3GPP-MBMS-DCF = 0x000001 // or any other value assigned by OMA
```

The flag indicates to an MBMS conforming parser the following new usage of DCF format:

- Right Objects are not used in MBMS download protection. Instead the RightsIssuerURL in the Common Headers Box will be used to carry MBMS KEY_ID information.. To transport the MBMS Key_ID information, a new URL scheme has to be defined for MBMS, e.g. mbms-key. The RightsIssuerURL may then contain:

```
mbms-key://key_id
```

where key_id is defined as the base64 encoded Key_ID string

- As RO is not used in MBMS download protection, SA3 proposes to define the following extended box to include a signature to the proposed MBMS usage of DCF format:

```
aligned(8) class MBMSSignature extends Fullbox(‘sign’, version, flags)
{
Unsigned int(8)         SignatureMethod;  // Signature Method
Char                                      Signature[];
      // Actual Signature
}
SignatureMethod Field:
NULL                    0x00
HMAC-SHA1   0x01
```

SA3 intends to add the MBMSSignature Box in the Free Space Box of the OMA DRM v2.0 DCF structure. SA3 asks OMA DRM to comment if they see any problems with this approach.

- For MBMS use, the requirement of globally unique ContentID is unnecessary and creates a burden on the issuer (i.e. the BM-SC). SA3 would like to ask if it is acceptable for OMA to deviate from the OMA requirement in case of MBMS use.

SA3 has the understanding that these extensions and deviations are best specified in OMA DRM v2.0 DCF specification. SA3 would like to ask guidance from OMA BAC DLDRM whether it is possible to include these extensions and deviations to OMA DRM v2.0 DCF specification or if OMA BAC DLDRM sees another way of handling them within OMA.

SA3 would also like to ask OMA BAC DLDRM to consider if any explanatory text needs to be added to the OMA-DRM-DCF, OMA-DRM-DRM or OMA-DRM-ARCH specifications about the use of OMA DCF extensions for MBMS.

## 2. Actions:

**To OMA BAC DLDRM group.**

**ACTION:**

- SA3 has the understanding that these extensions and deviations are best specified in OMA DRM v2.0 DCF specification. SA3 would like to ask guidance from OMA BAC DLDRM whether it is possible to include these extensions and deviations to OMA DRM v2.0 DCF specification or if OMA BAC DLDRM sees another way of handling them within OMA.
- SA3 would also like to ask OMA BAC DLDRM to consider if any explanatory text needs to be added to the OMA-DRM-DCF, OMA-DRM-DRM or OMA-DRM-ARCH specifications about the use of OMA DCF extensions for MBMS.

## 3. Date of Next SA3 Meetings:

| | | |
|---|---|---|
| SA3#37 | 21-25 February 2005 | Sophia Antipolis |
| SA3#38 | 25 - 29 April 2005 | Switzerland (TBC) |