3GPP TSG SA WG3 Security — S3#36 **S3-040910**

23 - 26 November 2004

Shenzhen, China

Title:	**Required Changes in OMA DRM specifications for using the DCF for MBMS Download protection**
Source:	**Ericsson**
Document for:	**Discussion/Decision**
Agenda Item:	**MBMS**
Work Item:	

1. Introduction

In [1] and [2] it has been proposed to use the OMA DRM DCF for download protection in MBMS. In the proposals and the discussion, the impression is given that this is possible without modifications to the existing DRM specifications. In fact, the existing OMA DRM specifications do explicitly not allow the use of the DCF as proposed. Should SA3 decide to follow the DCF proposal, some changes to the OMA DRM specifications are necessary; some other changes are not necessary, but deemed useful to explain this use of the DCF in the DRM specs.

We believe 3GPP and OMA should cooperate in a way satisfying both sides. 3GPP SA3 should not re-define parts of OMA specifications and contained semantics, without properly consulting and cooperating with OMA.

2. DRM specification changes

The following changes are necessary:

- In the Rights Expression Language [3] specification one basic assumption is that the content in a DCF may be accessed only according to permissions contained in Rights Objects, section 5.4 of [3]:"*The DRM Agent MUST NOT grant alternative, not explicitly specified rights to access Content […].*"). Thus, for the MBMS case, such rights have to be defined, since no RO is used.

- In the DCF specification [4] section 5.2.1.8: The use of ContentID should be redefined. Currently, the specification specifies "*The ContentID field MUST contain a globally unique identifier for this Content Object. The value MUST be encoded using US-ASCII encoding. The value MUST be a unique URI according to [RFC2396]. The use of globally unique ContentID's is required for OMA DRM and it is the responsibility of the content author to guarantee the uniqueness of the ContentID within their own namespace*." For MBMS use, the requirement of globally unique identifiers is unnecessary and creates a burden on the ContentID issuer (e.g., the BM-SC).

- In the DCF specification [4] section 5.2.1.9: It is proposed that the RightsIssuerURL is used to carry MBMS Key_ID information. Thus, a new URI scheme for the RightsIssuerURL has to be defined for MBMS. Currently [4] says "*The RightsIssuerURL field defines the Rights Issuer URL. The Rights Issuer URL MAY be used by the consuming Device to obtain Rights for this DRM Content. […] The value of the RightsIssuerURL MUST be a URL according to [RFC2396]"* (Note not a general URI as proposed for MBMS)

- In the DCF specification [4] section 6.3.1: define the proposed new flag that enables a DRM agent to distinguish between DCFs used for DRM and for MBMS download, including its meaning (use of the MTK). Currently no flag is defined, and the DCF specification [4] section 6.2.1 states "*The flags field MAY be used to include additional information, but SHOULD normally be set to 0, unless otherwise specified."*

    - Note: This needs to be specified in the DCF specification [4]. It is not possible to define this flag outside the DCF specification. The existing possible values of all fields and flags are defined within the DCF specification, (for example sections 5.2.1.2, 5.2.1.3, 6.2.2, 6.3.2.3. first paragraph, 7.1.1, 7.1.4 Table 15, Appendix A Table 17/18), and the OMA naming authority (OMNA) does not administer any values, flags or fields used in the DCF specifications (see OMNA page [7]).

- In the DCF specification [4]: For the proposed new "MBMS signature" for the MBMS DCF (e.g. using HMAC-SHA1), the following extended box needs to be defined in 5.2.4 where also Rights Object box and Transaction Tracking box are defined:

    - ```
      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
      ```

The following changes seem sensible:

- In the DCF specification [4] section 4: Explanatory text needs to be added about the use for MBMS. Currently, a DCF is not a general-purpose file container, but bound to DRM: "*The DCF can be delivered separately from an associated Rights Object, which contains the encryption key used to encrypt the Media Object*."

- In the DCF specification [4] section 5.2.2: to make an MBMS DCF parser simpler, it might be useful to disallow use of any Textual Headers. Some of the Textual Headers are anyway not usable for MBMS (Silent Header, Preview Header). In general, it should be specified which features of the DCF may or may not be used for MBMS use (e.g., Transaction Tracking Box, User Data).

- Explanatory text should be added to the DRM [5] and ARCH (architecture) specifications [6], to explain that the OMA DRM DCF is used outside its usage area expressed in the specification, namely DRM protection.

3. Conclusions

The DCF proposal described in [1] and [2] requires modifications to OMA DRM specifications although the opposite is claimed. This contribution has shown the modifications that are required to OMA DRM specifications if the DCF proposal described in [1] and [2] is adopted.
      ```

4. References

[1] Nokia, “Extensions to OMA DRM V2.0 DCF for MBMS Download Protection”, S3-040781

[2] Nokia, “An Update to Using OMA DRM V2.0 DCF for MBMS Download Protection”, S3-040901

[3] OMA DRM 2.0 Rights Expression Language, OMA-DRM-REL-V2_0-20040716-C

[4] OMA DRM 2.0 Content Format, OMA-DRM-DCF-V2_0-20040715-C

[5] OMA DRM 2.0, OMA-DRM-DRM-V2_0-20040716-C

[6] OMA DRM 2.0 Architecture, OMA-DRM-ARCH-V2_0-20040715-C

[7] OMNA page for a list of administered numbers,
http://www.openmobilealliance.org/tech/omna/index.htm