**3GPP TSG SA WG3 Security — S3#32** **S3-040080**

**9 - 13 February 2004**

**Edinburgh, UK**

**Title:** **Further updates on DRM usage for MBMS security**

**Source:** **Nokia**

**Document for:** **Discussion and decision**

**Agenda Item:** **6.20**

**Work Item:** **MBMS**

# 1 Introduction

Discussion paper [S3-030752] in SA3#31 presented principles how OMA DRMv2 could be utilized in the MBMS context. This paper provides further details on how this can be achieved.

# 2 Discussion

## 2.1 Broadcast/Multicast of Discrete contents

MBMS can be used to distribute discrete contents (texts, images, video clips, etc) in OMA DRM DCF (Discrete Content Format) [DCF] to users/subscribers. The DCF contains information of the Right Issuer URL, which the DRM agent in the device will use to contact the Right Issuer in order to obtain a Right Object (RO). The DRM agent can retrieve the Content Encryption Key (CEK) from the RO, and thereby decrypt the content for consumption.

MBMS, however, has the undesirable property of un-guaranteed delivery of content. On the other hand, this is an open issue to be solved also for non-DRM protected content, as indicated earlier [S3-030752].

## 2.2 Broadcast/Multicast of Streaming contents

For streaming contents, OMA DRM v2 defines the Packetized DRM Content Format (PDCF) [DCF] for packetizing the content. MBMS can be used to distribute a session descriptor (in the form of an SDP file) in DCF format to users/subscribers. Similar to the discrete content case, the DRM agent in the device can then acquire the RO from the Right Issuer as desired. Streaming sessions can then utilize the SA4 defined protected RTP payload format with OMA DRM key management.. The streaming contents can be distributed to the users/subscribers in PDCF format using MBMS. OMA is currently discussing how to optimize the usage of ROs in case several DCFs link to each other. Streaming is a typical example of this but there are also other cases like receiving several protected video clips from the same event (e.g. football match).

## 2.3 Issues with Right Objects

The OMA concept of issuing rights is based on public key technology. However, it seems in principle to be possible to utilize the idea of right objects also in the case their security is based on shared secrets. It is ffs to find out the details, e.g. it should be studied what kind of MBMS-specific extensions could be introduced on top of OMA right object syntax.

# 3 Conclusions

It is proposed that SA3 would adopt OMA DRMv2 mechanisms for protecting MBMS content. This would apply for both download and streaming. As regards key management, it should be further studied into what extent OMA rights issuing mechanisms may be utilized for MBMS as well.

# References

[S3-030752] DRM usage for MBMS security, SA3#31 November 2003, Nokia

[DCF] DRM Content Format, OMA-DRM-DCF-v2_0-20031103-D