3GPP TSG SA WG3 Security — S3#31 **S3-030752**

18 - 21 November 2003

Munich, Germany

Title: **DRM usage for MBMS security**

Source: **Nokia**

Document for: **Discussion and decision**

Agenda Item: **6.20**

Work Item: **MBMS**

1 Introduction

SA3 has received liaisons from SA4 on work division between 3GPP and OMA on DRM protected content [S3-030313] and suitable cipher selection [S3-030314]. The response liaison from SA3#30 Porto meeting to SA4, OMA-SEC and OMA-DRM+DL [S3-030650] states *"SA3 is considering solutions for the encryption and integrity protection of MBMS streaming media and it would be advantageous to consider alignment of these solutions (and the associated requirements) with the encryption and integrity protection mechanisms for DRM."*

This paper studies how OMA DRMv2 could be used in the MBMS context. Ericsson has also discussed multicasting DRM content via the MBMS architecture in SA3#28 contribution [S3-030248].

2 Discussion

2.1 OMA DRMv2

Let us first recall that the main idea of MBMS security is to keep unauthorized service listeners out. The basic target of OMA DRM is very similar.

OMA DRM model is not about absolute security but agreeing suitable ciphering method for the content to be pre-protected. The majority of the content is assumed to be off-line content. OMA DRM has support for both standard 3GPP streaming and download. A protected 3GPP SA4 3GP file format is defined for PSS and that is applied for downloadable and streamed content.

The below Figure 1 presents the parts of a Media DRM system according to the OMA DRMv2 view. This figure has been presented in SA4 contribution [S4-030367].

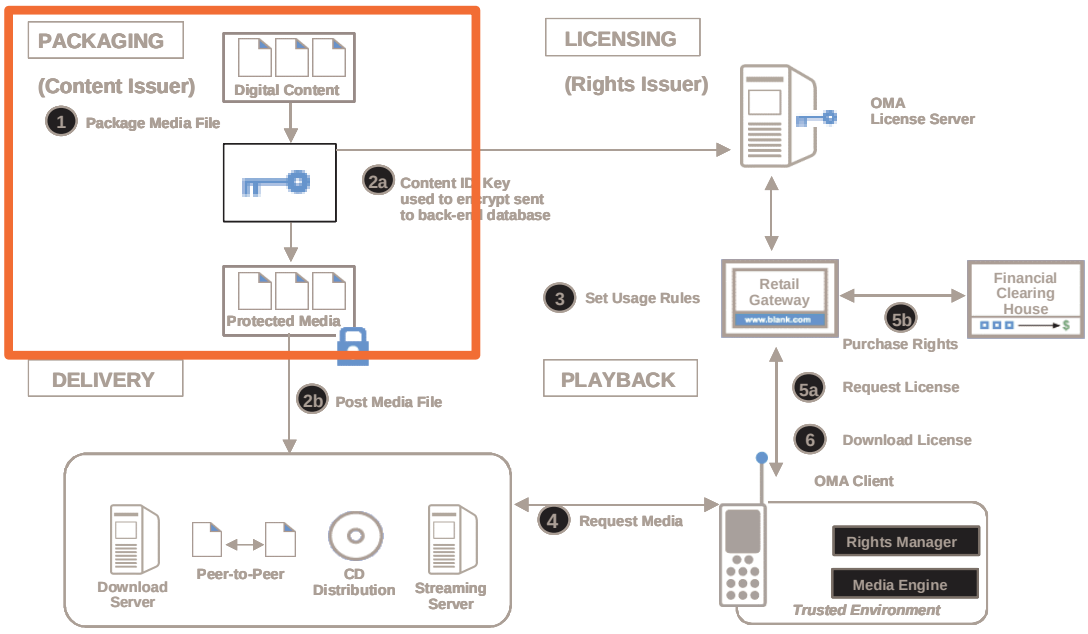

Figure 1 – OMA DRMv2 view

2.2 OMA DRMv2 usage in MBMS

Taking into account the background given in earlier chapter, OMA DRM could be used to support the MBMS service. The OMA DRM model assumes that all rights have to be managed for contents (but it may well be that the same rules apply for every piece of content, and different rules are not needed for every content). One difficulty in aligning DRM model with MBMS is that MBMS does not have a guaranteed delivery for the content, as there is no way of knowing which UEs have received the data. Hence, it may happen that UE has purchased rights for certain content but has not received the content itself.

One potential way of applying DRM model better in MBMS context is described in the following. BM-SC could act in the role of a content owner in cases where the content provider does not support DRM or it wants to delegate the role of the content owner to the BM-SC for some other reason. Now DRM could be used for every content, but we would not have a complete solution for the reason of explained above about the nonguaranteed content delivery. On the other hand, this is an open issue to be solved also for non-DRM protected content. For instance, SRTP as such doesn't have support for the reliable delivery. Anyway, MBMS BM-SC could have certain functionalities of OMA DRMv2 entities, like delivery and packaging, and the 3GPP MBMS needs to define the missing parts. With this approach, i.e.if BM-SC would be DRM compliant entity (i.e. rights issuer combined with packaging and delivery), then we would have the benefit that DRM mechanisms could be fully used for the protection of the content and need for MBMS-specific solutions would be minimized.

The division of functions between the MBMS-specific part and generic OMA DRM-based part would be the following. For MBMS service you have to have a subscription. Subscription management would be MBMS specific and the associated security mechanims, e.g. authentication of the subscriber at the highest level (for joining the service) have to be defined in 3GPP. This would be done by using the UICC. As a byproduct, we obtain shared secrets between BM-SC and UE. However, it is FFS how the DRM mechanisms could then utilize these secrets.

3 Conclusions

Principles were presented by which the SA3 work on MBMS security can be aligned with the ongoing co-operation between OMA DRM group and SA4 group for PSS.

4 References

[S3-030248] Authentication in MBMS, Discussion paper in SA3#28, May 2003, Ericsson

[S3-030313] LS (from SA WG4) on DRM Content Format, SA3#29 San Francisco

[S3-030314] Reply LS (from SA WG4) to “Reply to Liaison Statement on MBMS Codec Requirements”, SA3#29 San Francisco

[S3-030650] Reply LS on cipher suite for DRM-protected streamed media for PSS, SA3#30 Porto

[S4-030367] DRM Content Format, SA4#26, May 2003