3GPP TSG SA WG3 Security — S3#33 **S3-040227**

10 - 14 May 2004

Beijing, China

Title: **Applying DRM in to MBMS security**

Source: **Nokia**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

Discussion paper [S3-030752] presents principles on how OMA DRMv2 could be utilized in the MBMS context. [S3-040080] elaborates that the OMA DRMv2 message formats can be re-used in MBMS. This paper discusses further issues regarding usage of DRM in MBMS.

2 Discussion

2.1 Applying DRM to MBMS

In [S3-040080], it has been discussed that OMA DRM DCF (Discrete Content Format) and PDCF (Packetized DRM Content Format) can be used for MBMS discrete contents and streaming contents respectively. It has also been mentioned that OMA concept of issuing rights is based on public key technology. Within MBMS, GBA can be used to establish shared secret between ME and BM-SC, and MIKEY is used for transporting the key material towards the UE. There are two proposals of how to apply OMA DRM to MBMS:

Proposal 1: Integration of MBMS and DRM

It should be noted that in OMA DRM, the Right Object (RO) is actually (partially) encrypted using a RO Encryption Key (REK) with *symmetric* encryption (See 8.3 of [DRM]). It is the distribution of the REK that makes use of PKI (See 6.4.2 of [DRM]). Therefore, one way of applying OMA DRM RO is:

1. Each piece of MBMS content is encrypted using a distinct operator-chosen content encryption key (CEK).

2. Each piece of content is associated with a RO, which contains the CEK, as well as usage rules (as specified in [DRM]).

3. MBMS key exchange/transport mechanism will establish the MTK, originally used for decrypting MBMS data on the ME.

4. This MTK will be used as REK, i.e. RO will be encrypted using MTK.

5. When ME received content and associated RO, it will decrypt the RO with the MTK to retrieve the CEK, which further decrypts the MBMS contents.

6. To simplify delivery of ROs, MBMS content and associated RO can be delivered together (See 6.6.2.1.3 of [DRM]). For streaming data, MBMS has to deliver RO beforehand.

This proposal is better than the “normal” MBMS in the sense that content usage rights can be specified in the associated RO, whereas in 'normal' MBMS, no digital rights are specified. So, either a user can play (decrypt) the contents, or not (when the user doesn't have the key). With the existence of RO, operator can specify rights for the MBMS contents, usage rules such as “play once”, “play within this week” can be specified. These usage rules are enforced by the DRM agent embedded in the client.

One drawback of the proposal is that by using the MTK to encrypt REK, the ME has to store the MTK with the same lifetime as the RO. Moreover, many MTKs will need to be stored. A solution would be for the local DRM agent to re-encrypt the ROs using keys that have a longer lifetime, e.g. subscribers PKI-key. The resulting ROs will then be stored in the ME.

The use of Group-ID [GID] or simplified Group-ID [SGID] can be used to simplify the provisioning of subscription-based MBMS service, in that all contents belonging to a particular service are associated with a single Group RO. For MBMS re-keying, using Group-ID is not a problem, since all contents are encrypted using their own CEKs anyway. But for the simplified Group-ID proposal, all contents belonging to the group are encrypted using the same CEK. Therefore when MBMS performs re-keying, the Group-CEK will need to be changed also.

Proposal 2 – Selective Use of DRM Features in MBMS

We recall that the DRM provides content level protection and DRM extends beyond the physical delivery of the content into managing the content lifecycles. For example, a DRM agent that downloads DRM protected content from a content provider can forward the protected content to other DRM agents. The other DRM agents then buy the rights for the content from the right issuer to decrypt the content. However, there are certain applications (streaming), where the content is immediately rendered and not stored in the device.

The MBMS provides protection during transit or distribution from the BM-SC to the users.

There is an issue of “double ciphering” when DRM is used in the MBMS context. The data is encrypted at both the creation (content level) and the distribution (MBMS) time using different keys. The situation can be handled in following way depending on the applications:

1. Since for streaming applications, the streamed data is available for immediate rendering and is not stored in the device, there is no need to provide encryption at content level. It is also important from the performance point of view.

2. For download type of applications content level encryption is needed since the download data can be further distributed to other DRM agents. The MBMS distribution level encryption can be made optional. MBMS distribution level encryption provides added security at the cost of ”double ciphering”. As such performance is not an issue here since data is not rendered in real-time. Alternatively, operator can optionally disable the data encryption altogether at MBMS level for download type applications. However, we will still need MBMS security mechanisms to distribute ROs in a secured manner.

3 Conclusions

This paper further discusses how OMA DRMv2 mechanisms can be adopted for protecting MBMS content. In particular, two proposals are given whereby OMA DRMv2 concept can be used together with MBMS key hierarchy. Proposal 1 is an integration of MBMS and DRM. It uses MTK to encrypt the Right Object (instead of the content), which contains the actual CEK that encrypts the content. Proposal 2 is to allow double ciphering for download type applications, one using CEK at content level, and another using MTK at MBMS distribution level.

Preference is given to Proposal 2, as Proposal 1 may lead to some complications, e.g. having to keep MTKs with the same lifetime as RO, and requires further studies.

There are issues regarding DRM agent authentication and its relationship with MBMS level authentication. UE is authenticated and authorized in two steps when participating in the MBMS service. Firstly, when the

UE establishes a bearer to receive MBMS service and secondly when the UE requests and receives keys for the MBMS service. OMA DRMv2 model uses ROAP (PKI based Right Object Acquisition Protocol) for mutual authentication between Rights Issuers and DRM agents. We need to investigate further whether we need to differentiate between MBMS service level authentication and DRM agent authentication. We assume that both are needed. These topics are ffs.

References

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

[S3-040080] Further updates on DRM usage for MBMS security, SA3#32 February 2004, Nokia

[DRM] OMA DRM Specification V 2.0, www.openmobilealliance.org

[GID] Group ID Proposal, Input contribution, OMA BAC Download+DRM, DLDRM-2003-0286R02

[SGID] Simplified Group ID Proposal, Input contribution, OMA BAC Download+DRM, DLDRM-2004-0013