3GPP TSG SA WG3 Security — S3#35 **S3-040795**
5 - 8 October 2004
Malta

Source: **Ericsson**

Title: **MBMS download MTK transport**

Document for: **Discussion and decision**

Agenda Item: **MBMS**

1 Introduction

The download case may differ from the streaming case when it comes to the delivery of the MTK. This paper discusses the possibilities that are at hand (they were discussed during the joint SA3/SA4 meeting in August 2004).

2 MTK delivery for download

No matter which type of protection is chosen for download, the three level key hierarchy (MUK, MSK and MTK) can still be used both for streaming and for download. However, while the mechanism for delivering the MTK in streaming may also be used to deliver the MTK in download, there are some possibilities how the MIKEY [1] message should be carried to the UE.

2.1 MTK sent as in streaming

In this approach the MIKEY message containing the MTK is sent over the same transport service as the downloaded object, but to a different port. This requires a daemon listening for MIKEY messages on the specific port, but the processing of the message would be exactly the same as in the streaming case.

The major drawback with this is that there is no reliability in the delivery of the MTK, and the UE would have to request it from the BM-SC if it is lost (UDP (which is unreliable) is assumed here, since TCP is not possible over multicast transport). We would in this case need to specify a mechanism for requesting MTKs from the BM-SC, which is not in place today.

2.2 MTK sent over FLUTE

Another idea is to interleave the MIKEY message with the FLUTE blocks on the transport service. This has the advantage that more reliable delivery of the MTK can be assured. Furthermore, if the delivery still fails, it is possible to request the MIKEY message from the repair server as a post delivery procedure.

For this to work the MIKEY message must be assigned a TOI in the FDT, which should be fairly straightforward. This means that the MIKEY message has the same status as the actual downloaded object from the FLUTE implementation’s point of view.

3 Conclusion and proposal

There are essentially two ways to distribute the MTK in the download case, and these have been discussed above. We propose that the accompanying CR [3] that specifies how the MTK is delivered over FLUTE as a separate object is implemented.

4 References

[1] Arkko et. al., ”Multmedia Internet KEYing (MIKEY)”, RFC3830, IETF
[2] Paila et.al., ”FLUTE - File Delivery over Unidirectional Transport”, draft-ietf-rmt-flute-08.txt, IETF, work in progress
[3] Ericsson, “MBMS Download MTK transport”, S3-040xxx