3GPP TSG SA WG3 (Security) –S3 #33 **S3-040232**
10-14 May 2004
Beijing, CN

Agenda Item:	**6.20 – Multimedia broadcast/multicast service (MBMS)**
Source:	**Telecom Italia**
Title:	**MBMS key management: *OTA*- versus *GBA-based* Point-to-Point key distribution**
Document for:	**Discussion and Decision**

1. Introduction

During SA WG3#32 meeting (Edinburgh, 9th-13th February 2004) a long discussion took place about the MBMS key distribution mechanism.

In particular, it was also discussed how to (re)distribute, in a Point-to-Point way, the MSK[1] key(s) to the entitled UEs.

Referring to this specific aspect, n.2 different proposals were presented (*OTA-based* and *GBA-based* distribution) and this paper aims to clarify the view from an Operator's perspective.

2. *OTA versus GBA* discussion

Regardless of the chosen MBMS key distribution mechanism (*UICC-based only* or *combined* method), the MSK keys have to be (re)distributed to the entitled UEs in a Point-to-Point way.

During SA WG3#32 meeting the *OTA*- (TD S3-040050) and the *GBA-based* (TD S3-040058) approaches were discussed.

Considering that:

- OTA was designed to allow the network to directly interact with the UICCs.
- OTA is an established and proven technology.
- The *OTA-based* solution appears simpler than the *GBA-based* one. Moreover, as the information to update is stored in the UICC, the *OTA-based* solution also appears as a logical one.
- OTA allow the Operator to easily control the information stored in the UICC, that is to update the keys, but also to delete them and to perform other administrative procedures.
- Most Operators already have an OTA platform. Moreover, as MBMS is a quite "advanced" service, likely Operators that do not have an OTA platform will not be interested to offer MBMS.

[1] the *long lasting* keys

- According to the *UICC-based only* key distribution mechanism, the MBMS MSK key(s) will be stored in a secure environment, the UICC. So, in normal operations *OTA-based* MSK key (re)distributions may be scheduled and performed in advance by the network. Moreover, in normal operations the above-mentioned *OTA-based* key (re)distributions will be performed by the network in a “push” way and then problems related to massive and possible “simultaneous” key update requests will not occur (and will not have to be solved).
- GBA is part of the **Generic** Authentication Architecture (GAA) and it is **one** possible authentication mechanism. GAA is an independent Work Item and it is not mandatory. Using GBA as the way to distribute the MBMS MSK keys makes GAA/GBA implicitly mandatory, at least for those Operators interested in MBMS.
- In normal operations, *GBA-based* MSK key (re)distributions would be performed by the network in a “pull” way and then problems related to massive and possible “simultaneous” key update requests would occur (and would have to be solved).
- GAA/GBA is a new Work Item, like MBMS is. According to this, considering GBA as “stable” technology may be premature and Operators cannot take on the risk that possible GBA-related threats jeopardize the success of the MBMS service,

the proposal is:

To choose OTA as Point-to-Point way to (re)distribute the expected MBMS MSK key(s).