3GPP TSG SA WG3 (Security) –S3 #33 **S3-040233**
10-14 May 2004
Beijing, CN

Agenda Item:	**6.20 – Multimedia broadcast/multicast service (MBMS)**
Source:	**Telecom Italia**
Title:	**MBMS key management: *UICC-based only* solution versus *combined* method.**
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 to choose (*UICC-based only* solution versus *combined* method).

As it was commented that the decision is more a “business” matter than a technical issue, this paper aims to clarify the view from an Operator’s perspective.

2. ”*UICC-based only* versus *combined* method” discussion

The *combined* method (TD S3-030751) would leave each Operator to choose (between *UICC-* and *ME-based*) the MBMS key distribution mechanism to use. As each Operator would be allowed to make its own choice,

- **the *combined* method introduces an option in the 3GPP standard.**

As some Operators may choose the *UICC-based* solution, the *combined* method specification has to fully specify it, from both the network and the UE sides.

As some Operators may choose the *ME-based* solution, the *combined* method specification has to fully specify it, from both the network and the UE sides.

Moreover, in order to allow full interoperability (e.g. in case of roaming[1]), the *combined* method implies that also the interworking between the *UICC-based* and the *ME-based* solutions has to be carefully specified, from both the network and the UE sides. According to this,

- **the *combined* method introduces complexity and may lead to possible interoperability threats.**

By definition MBMS is a service designed to be able to target a wide customer base. In order to avoid complaints from the end-users, the MBMS service has to work, as a general rule, in the HPLMN and in whatever VPLMN roaming partner, according to the end-user’s subscription. Even while roaming abroad, the end-user has to feel the MBMS as a service “available” and “stable”, like the speech call is.

According to this,

- **from an Operator’s perspective, whatever interoperability threat that may prevent, limit or modify the access to the service has to be avoided**.

[1] as TS 22.246 v.6.0.0 says that *an MBMS user service may be provided to the operator’s own subscribers and/or to inbound roaming subscribers from other operators*

Moreover, as MBMS is a service designed to target a wide customer base, possible frauds aiming to get (or to allow) free access to the (even cheap) contents have to be seriously taken into account, regardless of the MBMS content cost. According to this,

- **from an Operator's perspective, MBMS-related frauds have to be prevented.**

Considering that:

- It is generally acknowledged that handsets are not tamper-resistant devices and then that the *UICC-based* solution provides a higher security level than the *ME-based* one.
- Assuming the *combined* method as the way forward, the "included" *ME-based* solution option would open the Operators to higher risks of MBMS-related frauds, to detect and to counteract. In fact, the MBMS is designed to target a wide customer base and the *ME-based* solution implies that the MSK key[2] has to be stored in the ME. As MEs cannot be considered as tamper-resistant devices, the stored MSK key may be retrieved (e.g. by a legitimate subscriber) and then distributed to non entitled UEs (e.g. his/her friends) or even made public (e.g. through internet). According to this, the *ME-based* solution does not provide an effective MBMS content protection. Moreover, as the IMEI can be modified, Operators might be unable to stop possible MBMS-tampered handsets. According to this, there are no reasons to believe that most Operators would really use the *ME-based* solution option offered by the *combined* method.
- According to TS 22.246 v6.0.0, MBMS shall also support usage-based charging "*based on keys that allow the user access to the data*". According to this, in order to avoid possible frauds from legitimate UEs providing the Operator with false MBMS usage-related data[3], the latter have to be stored in a tamper-resistant device, the UICC. Moreover the ME has to be unable to modify/forge them.
- As shortly described above, the *combined* method introduces more complexity that in this case is perceived as unnecessary and even potentially dangerous for the service itself.
- Even if the *UICC-based* solution provides only a partial backward compatibility, most pre-Rel6 UICCs may be made "MBMS-capable" Over The Air.
- During TSG SA#22 meeting (15th -18th December 2003) most Operators expressed a preference for the *UICC-based only* solution even on the grounds that a next-generation UICC is required.
- T WG3 confirm that the *UICC-based only* solution can be implemented on the USIM for release 6 (TD S3-040171),

the proposal is:

to choose the *UICC-based only* solution as MBMS key distribution mechanism.

[2] the "high level" or "long lasting" one

[3] e.g. a lower number of received keys