3GPP TSG SA WG3 (Security) –S3 #32 **S3-040052**
09-13 February 2004
Edinburgh, Scotland, UK

Agenda Item:	**6.20 – Multimedia broadcast/multicast service (MBMS)**
Source:	**TIM, Orange, Oberthur, Gemplus**
Title:	**MBMS key management: follow up from SA#22 meeting**
Attachment:	TD SP-030743
Document for:	**Discussion and Decision**

1. Introduction

The *Draft TS 33.246 version 1.0.0: Security of Multimedia Broadcast/Multicast Service (Rel-6)* was presented to SA, for information, during SA #22 meeting (15th -18th December 2003).

Particularly referring to the MBMS key management mechanism, the attached TD SP-030743 ("*Considerations about supporting ME solution for key management in Rel-6*") was also presented and discussed.
It summarizes pros and cons of each alternative (UICC-based only, ME-based only and, finally, the "combined" method), reports the conclusion reached within SA WG3 and asks comments from SA Group.

According to the SA#22 Draft meeting report:

- *"It was clarified that the use of the UICC-based solution had been discussed in SA WG3 and a UICC-based solution could offer a higher security and low impact on network resource".*
- *"Several operators expressed a preference for the UICC-based only solution". The TSG SA Chairman asked whether any operators would reject the UICC-only proposal on the grounds that a next-generation UICC is required and one Company indicated that they would object".*
- *It was commented that the Options for implementation should be kept to a minimum for ease of implementation and interoperability.* ***Members were asked to contribute to SA WG3 on this and TSG SA requested that SA WG3 also consider their request that the final solution should not include any options****".*

2. Proposal

Following the discussion held within SA#22 meeting, the proposal is to take in the SA comments and particularly the request that the final solution should not include any options.

More in detail, the proposal is to allow only the UICC-based key distribution mechanism.

Technical Specification Group Services and System Aspects TSG SA#22 (03)0743
Meeting #22, Hawaii, USA, 15-18 December 2003

Source: **TIM, Orange**

Title: Considerations about supporting ME solution for key management in Rel-6

Release: Rel-6

Document for: Decision/Discussion

1. Background:

In order to avoid unauthorized access to MBMS contents (e.g. to avoid keys to be leaked and then passed from a legitimate Subscriber to his/her friends), a MBMS key (re)distribution mechanism has to be implemented.

Referring to this, at SA3#31 (Munich, 18th-21st November 2003) the following proposals have been discussed:

- “ME only”-based solution;
- UICC-based solution;
- “combined” (ME and UICC-based) solution, (compromise solution between the previous 2).

Some considerations regarding the different proposals, taking into account the requirement to have an effective protection of the MBMS content, are the following:

- the first solution (ME based), would store the MBMS key on the ME, would not introduce new requirements on the UICCs and it would entail a point-to-point key (re)distribution mechanism anyway a new MBMS-capable handset is required. As the ME has been recognized as a not suitable secure environment to store the MBMS key, in order to have the desired effective MBMS content protection the above mentioned point-to-point key (re)distribution mechanism might occur very often, and then it could be heavy in terms of network resources usage, or even not consistent with the MBMS overall approach;
- the second solution (UICC based) would store the MBMS key on the UICC, where the MBMS key would be generated locally, based on a multicast mechanism. The main drawback of this approach is the lack of backward compatibility: in order to access the MBMS service, some (low performance) pre-Rel6 UICCs should have to be replaced with MBMS-capable ones, whilst the others should have to be upgraded (Over The Air). As the UICC has been recognized as a secure environment to store the MBMS key, this approach would provide a higher security level (reducing fraud detection actions and efforts for the Operator).
- the third solution was presented as a compromise between the two above-mentioned. “Low value” and “High value” MBMS contents would be protected using the first and the second solution, respectively (*“The combined method is designed to combine fast and reliable re-keying of two-tiered and low cost of introduction of simple point-to-point method. Low value MBMS services can allow KEK generation and storage of BAK in the ME, but high value MBMS services can require KEK generation and storage of BAK in the UICC”).* Operator would decide, MBMS content per MBMB content, if it belongs to the “Low value” or “High value” category and then it would behave accordingly.

SA3#31 decided that both UICC-based and “ME only”-based solutions shall be supported for MBMS key (re)distribution mechanism (Rel-6), as reported hereafter (SA3#31 draft meeting report):

“It will be possible to run the whole MBMS security with ME only, but will also be possible to run key management using the UICC. A migratory path between the two solutions is needed and the solutions will be developed to allow this. Deviations between the two solutions would only be made for the benefit of the whole system (this implies the use of a 2-tiered system). The difference between the two solutions for delivering the low level keys would be visible only inside the UE and secondly, the BMSC would know which solution is implemented in the UE side. A Rel-6 compliant UE will support both UICC based and ME based solutions and the Operator will have control over the choice of method used for MBMS services”

At SA3#31 some Companies expressed their reservation to this decision.

This contribution analyzes some of the reasons of these concerns.

2. Analysis:

- Referring to the combined method, for an Operator point of view, the “Low value” MBMS content concept does not really apply: cheaper contents will likely attract a wider Customer Base part. In order to prevent fraudulent accesses to “Low value” MBMS contents, the Operator should perform very frequent key (re)distributions, that would be “point-to-point”. In practice the only MBMS contents that can be considered as belonging to the “Low value” category are the “Free” MBMS contents, that from an Operator perspective might not justify any specific investment on key management.
- ME-based solution does not provide an effective MBMS content protection, so it is not justified in terms of security, but just as a way to balance a possible lower implementation cost with the need to protect alleged “Low value” MBMS contents, that from an Operator perspective might not exist (see above).
- ME-based solution got support within SA3 as it would allow MBMS access to the generic Subscriber that does not have a MBMS-capable UICC, even if, regardless of the chosen approach, he/she would need a new MBMS-capable handset anyway (that will be much more costly than a new UICC);
- The backward compatibility threat raised for the UICC-based solution can be minimized: MBMS is a Rel-6 feature and pre-Rel6 UICCs able to support the Over The Air “MBMS” upgrade are already available.
- The option (UICC- and “ME only”-based, both supported) requires a higher standardization effort for Rel-6.
- The option (UICC- and “ME only”-based, both supported) may lead to possibly difficult migrations;
- Last, but not least, the option (UICC- and “ME only”-based, both supported) leaves the choice to the Operators, i.e. to the market, and this will lead to interoperability problems especially for roaming cases, which have not yet been sufficiently studied.

3. Proposal

It is proposed:

- to consider the above-reported Analysis from an Operator perspective;
- to avoid the introduction of a (possibly harmful) new option in the 3GPP standard;
- to propose SA3 to revise the decision on the MBMS Key (re)distribution mechanism, allowing only the UICC-based solution.