3GPP TSG SA WG3 Security — S3#32 **S3-040040**

9 - 13 February 2004

Edinburgh, UK

Title:	**MBMS key management approach**
Source:	**Nokia, Siemens, Ericsson**
Document for:	**Discussion and decision**
Agenda Item:	**6.20**
Work Item:	**MBMS**

1 Introduction

The purpose of this contribution is to elaborate more why the current SA3 MBMS key management approach, i.e. both ME- and UICC-based solutions developed for Rel6, is feasible. The SA3#31 draft meeting report states the following about the conclusion reached regarding MBMS key model:

> *"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."*

Like stated above, the use of a 2-tiered system is implied by the achieved SA3 working assumption. Such a two-tiered model, whether it is the Combined model [S3-030751] with TEK delivered as encrypted or the MIKEY model [S3-030723] with TEK generated from a random value, can be implemented as an ME-based solution or a UICC-based solution. The difference in key flows is indeed visible only inside the UE. Contributions [S3-030751] and [S3-030723] have shown that for such models migration from a ME-based solution to a UICC-based solution is possible.

2 Analysis

2.1 SA#22 advise

According to draft SA meeting #22 report on MBMS security *"It was commented that the Options for implementation should be kept to a minimum for ease of implementation and interoperability."* It is fully agreed that this reasonable principle about limiting implementation options should be adhered in the choice of MBMS key model also. Actually no two solutions for exactly to the same thing was even intended to be developed, but other constraints are forcing SA3 to develop ME-based solution and also a more far reaching UICC-based solution. Although also UICC-based solution is planned to be developed in Rel6 standard specifications the deployment of needed network functionality will take some time and the support will not be available at the same time in the field as for ME-based solution.

2.1.1 Considerations presented in SA#22

In SA#22 there was a contribution [SP-030743] *Considerations about supporting ME solution for key management in Rel-6* tabled, which had the below analysis concerning the Combined model.

> *"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."*

This is not fully correct as in a two-tiered keying model with ME-based solution the more frequent lowest level key (re)distributions are done point-to-multipoint and not point-to-point, similar as with a two-tiered keying model with UICC-based solution. Thus frequent re-keying of lowest level key would not be heavy in terms of radio resource usage. This was also shown in *MBMS – Overhead of the Re-keying paper* [S3-030580] presented in SA3#30.

[SP-030743] additionally claims the following:

> *"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)."*

Related to [S3-030700] *MBMS (re-)keying models* discussion paper by Siemens in SA#31 one of the agreed working assumptions as in SA3#31 draft meeting report:

> *"If a UICC-based solution will be developed then the design of a UICC-based solution shall take care that the security is as high as possible but the solution shall at the same time be cost-efficient. In particular there has to be a way to recover from the situation where secrets from within one single UICC are revealed by an attacker."*

This working assumption was reached concerning UICC-based solutions, but a direct implication is that cost-efficiency needs to be taken into account also in ME-based solution. Thus it indeed is found to be reasonable to offer differentiation to "Low value" and "High value" content as is possible in variant implementation of a two tiered key model. This is done between lower value content that can be decrypted also in case subscriber has a BAK in the ME and a higher value content that requires BAK in UICC. Furthermore, the cost of an attack against the ME-based solution should be considered. An attacker needs a custom application to extract BAKs and a method to send them to other malicious users. Additionally malicious users for their part need a specific application to use the leaked BAKs.

3 Conclusions

Based on the above analysis and considerations it is concluded that while the reasons that were brought forward by SP-030743 seem to be unjustified, there seems currently no reason to change the SA3#31 working assumption Thus it is proposed that the earlier SA3 working assumption about developing both ME- and UICC-based solutions for MBMS Rel6 key management is kept. Furthermore, it is proposed that this discussion paper is used as a basis when providing justification of this SA3 approach to SA#23.

4 References

[S3-030580] MBMS – Overhead of the Re-keying, SA3#30 October, Nokia

[S3-030700] MBMS (re-)keying models, SA3#31 November, Siemens

[SP-030723] Migration of MIKEY in MBMS key management, SA3#31 November, Ericsson

[S3-030751] Further updates on Combined model for MBMS security, SA3#31 November, Nokia

[SP-030743] Considerations about supporting ME solution for key management in Rel-6, SA#22 December, TIM and Orange