3GPP TSG SA WG3 Security — S3#31 **S3-030703**
18 - 21 November 2003
Munich, Germany

Agenda item:	**MBMS , 6.20**
Title:	**Evaluation of re-keying methods**
Source:	**Huawei Technologies Co., Ltd**
Document for:	**Discussion and Decision**

1 Introduction

In recent meetings, several re-keying methods had been proposed, and those methods have their respective advantages and disadvantages. This contribution reviews those issues and recommends adopting an improved combined re-keying method or the simple PTP re-keying method.

2 Discussion

2.1 Re-keying resource

For simple PTP, one concern is that simple PTP re-keying will require more resources and impact MBMS data transfer. While it is possible for mass amounts of MBMS data, initial MBMS services will be relatively simple and use shorter sessions. Because of this, simple PTP re-keying will have minimal impact on MBMS service.

For the 3GPP2 method and combined method, usage of re-keying resources is included in the data packet. But if the usable space for MBMS data is reduced, then the time for multicasting data will increase. In other words, the more overhead put in data packet, the bigger the impact is for MBMS data. That is, the re-keying resources used are proportional to the amount of MBMS data, not the number of users.

2.2 Security and quality of key and key material in data packet

2.2.1 Security

TEK in data packet is encrypted with BAK, and the SK_RAND in data packet is clear text. There is a potential problem if the integrity protection of the multicast data is unachieved or optional. If the encrypted TEK/SK_RAND are modified in the data

packet, users will not be able to decrypt the MBMS data correctly with received key. While the encrypted TEK/SK_RAND are extremely important, the MBMS data may not be protected with integrity.

2.2.2 Quality

For the encrypted TEK/SK_RAND (i.e. key / key material), the Qos should be high. However, the Qos may be low for the data packets. A few errors with the encrypted TEK/SK_RAND will make users unable to decrypt MBMS data correctly.

It is impossible to define different Qos for MBMS data and key or key material contained in the same data packet. If information is implemented with high Qos, the quality can be ensured, but at the cost of providing high Qos for MBMS data.

There are other methods to ensure the quality, e.g. adding redundance for the key or key material, but additional bandwidth is required for each one.

2.2.3 Security and quality with simple PTP

The security and quality in simple PTP is easy to ensure. Integrity and encryption protection of TEK can be implemented with the IK/CK results of AKA.

TEK transmissions can be assigned a high Qos, so the quality can be ensured easily without requiring additional bandwidth.

2.5 Summary of comparison

Method	Advantage	Disadvantage
Combined method	1 More users will not cause additional burden 2 Re-keying can be frequent 3 Compatible with the old UICC	1 The integrity of key material in data packet is difficult to ensure 2 The Qos of key material in data packet transfer is difficult to ensure 3 The key material reduces space for data in data packet
3GPP2 method	1 More users will not cause additional burden 2 Re-keying can be frequent	1 Requires most changes in UE (new UICC or OTA upgrade) and network 2 The integrity of key

	frequent	material in data packet is difficult to ensure 3 The Qos of key material in data packet transfer is difficult to ensure 4 The key material reduces space for data in data packet
Simple PTP method	1 Simple and easy to implement 2 Requires minimal changes in UE and network 3 Doesn't need to change the USIM 4 The confidentiality and integrity of transfer is good 5 The Qos of key transfer can be ensured 6 Easy to upgrade to new method	1 More users increase the burden (the main fault) 2 Re-keying can't be frequent unless few users

In the above analysis, implementation feasiblility is the first point that should be considered. The next most important criteria is the re-keying resource, followed by the integrity and quality of the key and key material.

The most feasible method is the simple PTP re-keying method followed by the first phase of the combined method. The 3GPP2 method most likely will require changes to the UICC which will be difficult to complete within the current Release-6 schedule.

For the resource perspective, prior analysis [S3-030580] shows that the simple PTP and combined methods are roughly equal with respect to data overhead. The 3GPP2 method was assumed to come between the two. However, the combined and 3GPP2 methods are expected to be more scalable for re-keying because they use PTM re-keying messages.

From standpoint of the integrity and Qos of encrypted key and key material, the simple PTP method can easily guarantee integrity and Qos of the key/material

because they are transferred indepedently. For the combined method, contribution S3-030520 provides a mechanism to increase the Qos of the key/material. Additional signalling could increase the integrity of the key/material but at the expense of using more bandwidth.

3 Conclusion

Based on the analysis summarized in section 2.5, we propose accepting the improved combined re-keying method or the simple PTP re-keying method.

1. If the combined re-keying method is accepted, we propose adopting the improvement described in S3-030520.

2 If the simple PTP re-keying method is accepted, we propose adding the figure and bullets proposed in S3-030521.