3GPP TSG SA WG3 Security — S3#30 **S3-030519**
06 - 10 October 2003
Povoa de Varzim, Portugal

Agenda item:	**MBMS**
Title:	**Re-keying resource , security and quality**
Source:	**Huawei Technologies Co., Ltd**
Document for:	**Discussion**

1 Introduction

This contribution discusses re-keying resource, security of key and key material, and quality of key and key material and compares these attributes for each re-keying method. Re-keying resource is the most important point to be considered, but integrity and quality of the key and key material are also important, so they should be studied at the same time.

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 data. Plus, if number of users is small, there will be almost no impact on MBMS data.

For the 3GPP 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. Furthermore, even if the number of users is small, the impact on MBMS data can’t be reduced.

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 more bandwidth is required for each one.

2.4 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.

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

2.5 Summary of comparison

	Combined method	3gpp method	Simple method
Re-key Resource 1) mass MBMS data	Increases more	Increases	No change
Re-key Resource 2) more users	No change	No change	Increases with amount of users

Re-key Resource 3) less users	No change	No change	Decreases with amount of users (if users are a few, it can be ignored)
Integrity protection of key and key material	Requires integrity protection in MBMS data packet	Requires integrity protection in MBMS data packet	Can be implemented with point to point
Quality of key and key material	Requires additional solving	Requires additional solving	Doesn't need additional solving

In the above analysis, the re-keying resource is one main point we should consider, but integrity and quality of the key and key material are important too, so they should be studied at the same time.

3 References

[1] TD S3z030020 MBMS – Combined Re-keying Method, NOKIA

[2] TD S3z030007 MBMS Security Architecture, QUALCOMM

[3] TD S3xxxxxxx MBMS_Simple_PTP_in_detail, HUAWEI