3GPP TSG SA WG3 Security — SA3#35 **S3-040753**

October 5-8, 2004

St Paul's Bay, Malta

Source: Samsung Electronics

Title: **MKI field transmission method for SRTP packet in MBMS**

Agenda item: MBMS

Document for: Discussion/Approval

1 Introduction

During the August SA3-SA4 MBMS security joint meeting, it was noted that since the MKI (the Master Key Identifier field in SRTP) field shall be included in all SRTP packets to indicate which MTK is used currently for MBMS, more study was needed to look if the MKI field (9 bytes currently) can be omitted. In this contribution, we show one solution to this need of reducing the length of MKI field used while not impacting other aspects.

2 Proposed solution

The proposed MKI field structure is illustrated in Figure 1. This MKI field is composed of 3 parts: Indicator of one bit, optional Content of variable length, and MTK ID of 2 bytes (*FFS*). The one bit Indicator indicates whether this MKI field is compressed or uncompressed.

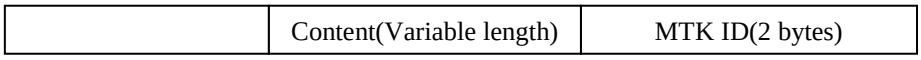

Figure 1: MKI field structure

Referring to Figure 2, for the uncompressed case, the indicator shall be "1", and the Content shall be a concatenation of Network ID, Key Group ID, MSK ID, i.e. Content = (Network ID || Key Group ID || MSK ID).

Figure 2. Uncompressed MKI field

Referring to Figure 3, for the compressed case, the indicator shall be "0" and the optional Content part shall be one MAC(Message Authentication Code). BMSC shall carry out one HASH operation to the Network ID, Key Group ID and MSK ID to obtain this MAC, i.e. Content = HASH(Network ID || Key Group ID || MSK ID). The length of MAC may be 7 bits for example. If the BMSC decides not to take use of this MAC, the length of this MAC shall be 0.

Figure 3. Compressed MKI field

The principal MKI transmission method is illustrated in figure 4. During normal operation a flow of compressed MKI field is transmitted. When one new Network ID, Key Group ID or MSK ID is used instead, or BMSC believes there exists data loss during previous transmission, the transmission of uncompressed MKI field is used instead, cf. packet#2 in figure 4. BMSC controls when to give out these uncompressed MKI fields transmission.

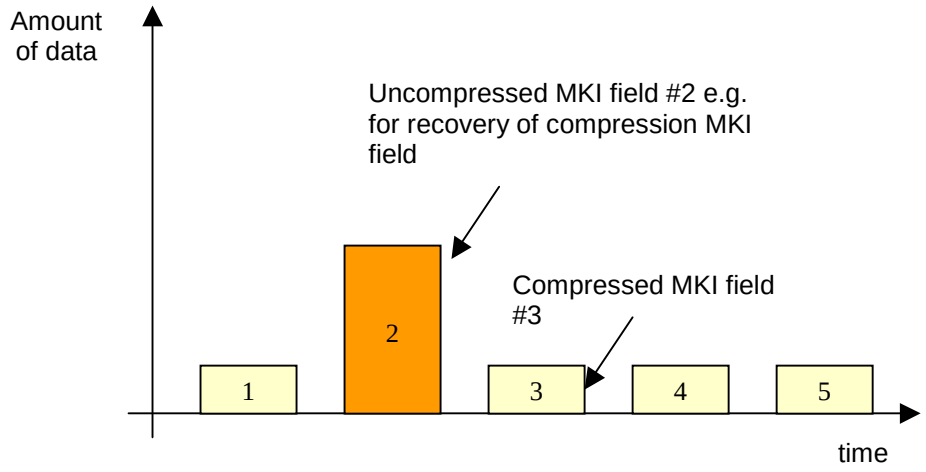

Figure 4: Compressed MKI field transmission together with uncompressed MKI field

For the UE receiving, when the UE obtains the MKI field, it shall check the Indicator at first. For "1", which means the uncompressed MKI field, it shall save and use the Network ID, Key Group ID and MSK ID obtained from the Content part. For "0", which means the compressed MKI field, UE shall carry out the same HASH operation as BMSC does to the Network ID, Key Group ID and MSK ID that it currently uses to obtain one expected MAC, and compare it with the MAC received in the Content part from the BMSC. When the comparison result is the same, UE shall continue to use current Network ID, Key Group ID and MSK ID; otherwise, it shall request BMSC to re-transmit these parameters together with the actual MSK individually for this UE. This can be done by the MSK updating procedure stated in TS33.246 section 6.3 This kind of comparison result inconsistency may occur when the UE runs into data loss for uncompressed MKI field transmission. In this case, UE may own the keys with the correct Network ID, Key Group ID and MSK ID, but it does not know change to use them and continues to use old ones. This kind of comparison result inconsistency may also occur when UE missed the key updating procedure at all. In this case, the UE does not own the keys with the correct Network ID, Key Group ID and MSK ID.

By this method, the length of MKI field shall be 3 bytes when compressed (in case the length of MAC is 7 bits), and kept 9 bytes when uncompressed, while not affecting other aspects, such as key transmission/updating procedure and key identifier composing.

3 Conclusions

We propose that SA3 considers the method introduced for MKI field transmission that does not lead to further modification to other aspects.