3GPP TSG SA WG3 Security — S3#30 **S3-030520**
06 - 10 October 2003
Povoa de Varzim, Portugal

Agenda item: **MBMS**

Title: **Improved combined re-keying method**

Source: **Huawei Technologies Co., Ltd**

Document for: **Discussion and Decision**

1 Introduction

The combined re-keying method was presented at ad hoc meeting, and the issue about bandwidths was brought forward. This contribution suggests some approaches to improve the combined re-keying method by reducing re-keying bandwidth.

2 Discussion

2.1 Data packets contain BAK_ID and TEK_ID

With combined re-keying method, the data packets contain encrypted data, an encrypted TEK, and corresponding key indentifier. With this approach, the encrypted TEK requires many bits. However, if the TEK_ID replaces the encrypted TEK, there will more bits for data. Figure 1 shows the improved combined method with the old UICC. Figure 2 shows the improved combined method with the new UICC.

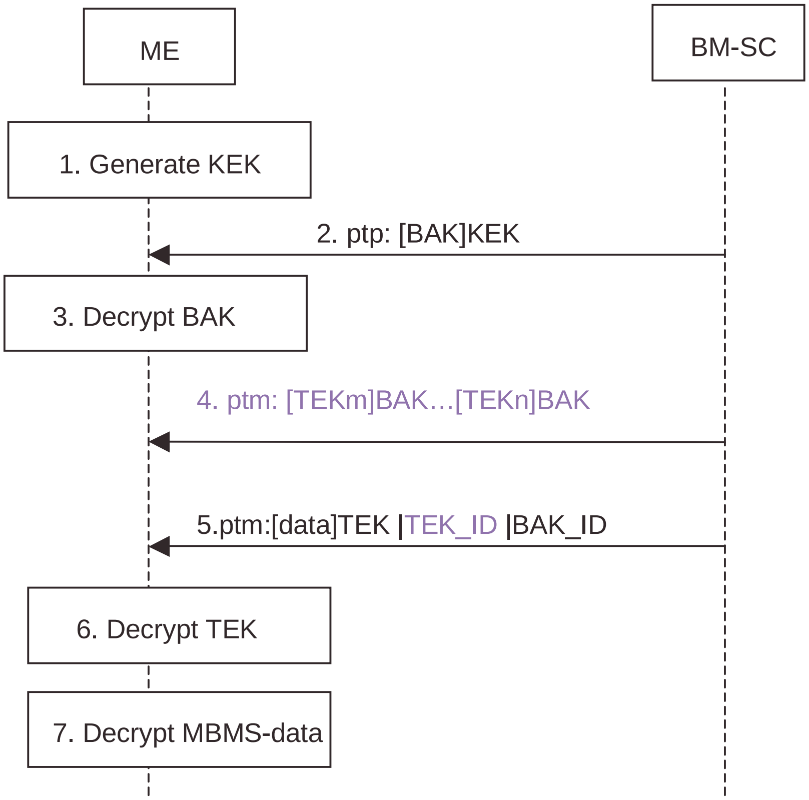

Figure 1: Improved combined method with old UICC (TEK_ID replaces encrypted TEK)

1. The ME generates a KEK
2. The ME receives a new BAK, which is encrypted using the KEK
3. The ME decrypts the BAK using the KEK
4. The ME receives a group of TEKs encrypted with BAK (BAKs may be same or different)
5. The ME receives a MBMS data packet, which contains encrypted MBMS data, TEK_id and BAK_id in clear text
6. If the ME does not have the current TEK then it decrypts the TEK using the BAK
7. The ME decrypts MBMS data using the TEK

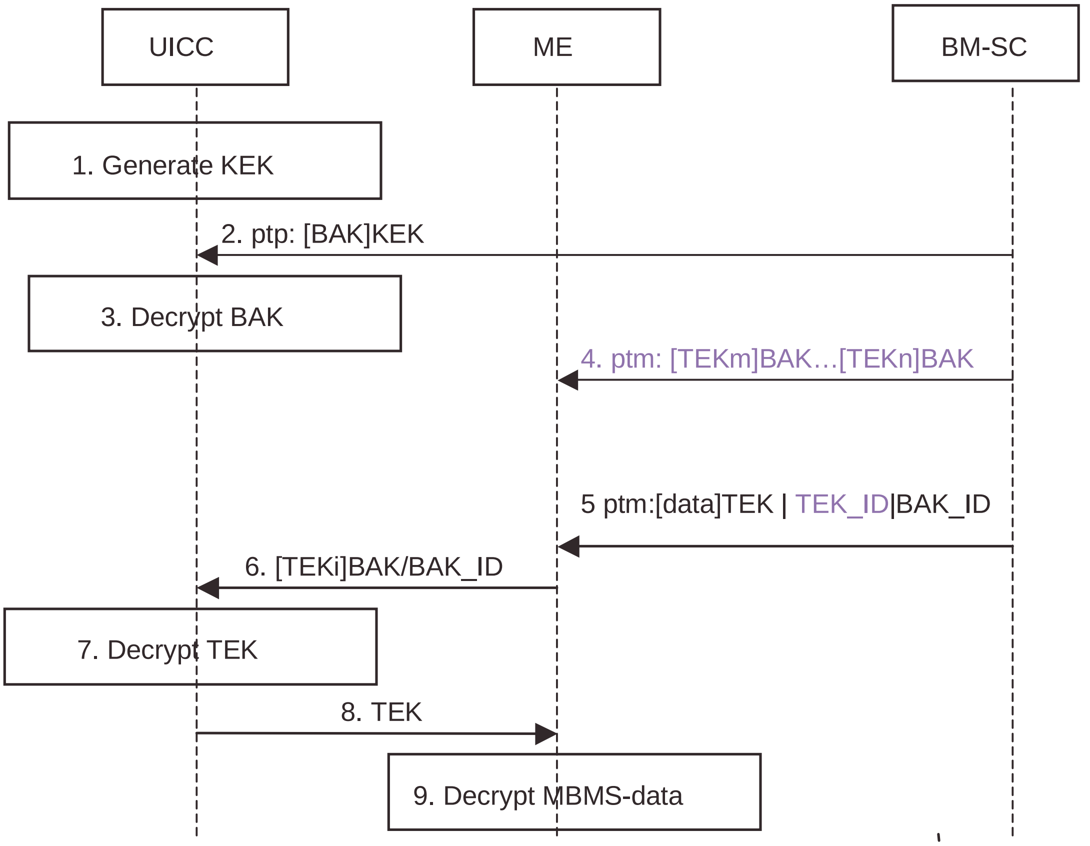

Figure 2: Improved combined method with new UICC (TEK_ID replaces encrypted TEK)

1. The UICC generates a KEK
2. The UICC receives a new BAK, which is encrypted using the KEK
3. The UICC decrypts the BAK using the KEK
4. The ME receives a group of TEKs encrypted with BAK (BAKs may be same or different)
5. The ME receives a MBMS data packet, which contains encrypted MBMS data, TEK_id and BAK_id in clear text
6. If the ME does not have the current TEK then it sends a request to the UICC
7. The UICC decrypts the new TEK
8. The ME receives the new TEK
9. The ME decrypts MBMS data using the TEK

2.2 Data packets contain BAK_ID and RAND_ID

This approach is similar to subclause 2.1, but replaces TEK_ID with RAND_ID in the data packets and the group of encrypted TEKs with a group of RANDs.

Figure 3 shows the improved combined method with the old UICC. Figure 4 shows the improved combined method with the new UICC.

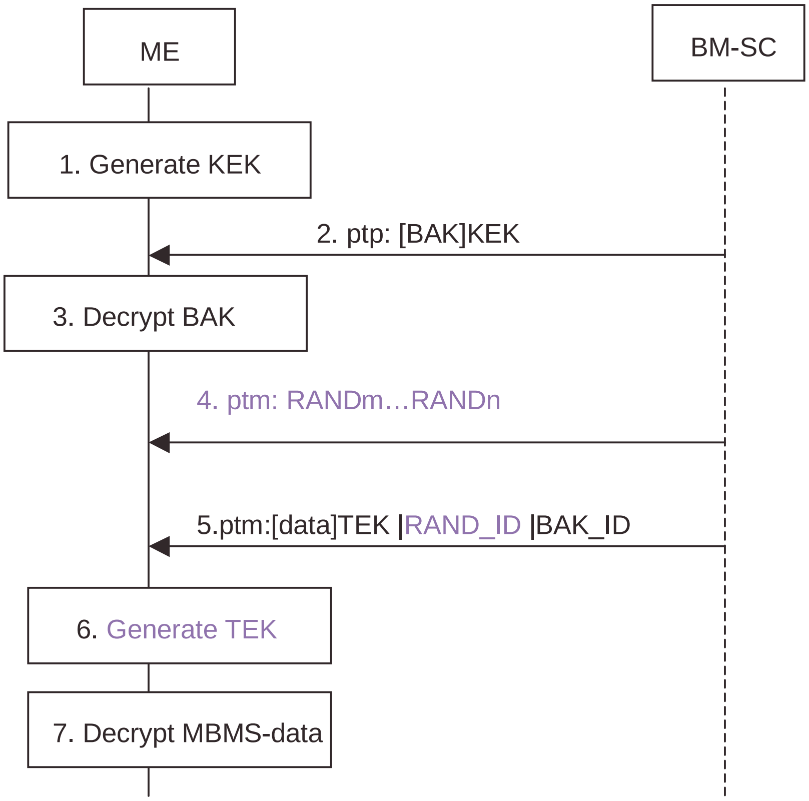

Figure 3: Improved combined method with old UICC (RAND_ID replaces encrypted TEK)

1. The ME generates a KEK
2. The ME receives a new BAK, which is encrypted using the KEK
3. The ME decrypts the BAK using the KEK
4. The ME receives a group of RANDs in clear text.
5. The ME receives a MBMS data packet, which contains encrypted MBMS data, RAND_id and BAK_id in clear text
6. If the ME does not have the current TEK then it generate TEK using the BAK and RAND
7. The ME decrypts MBMS data using the TEK

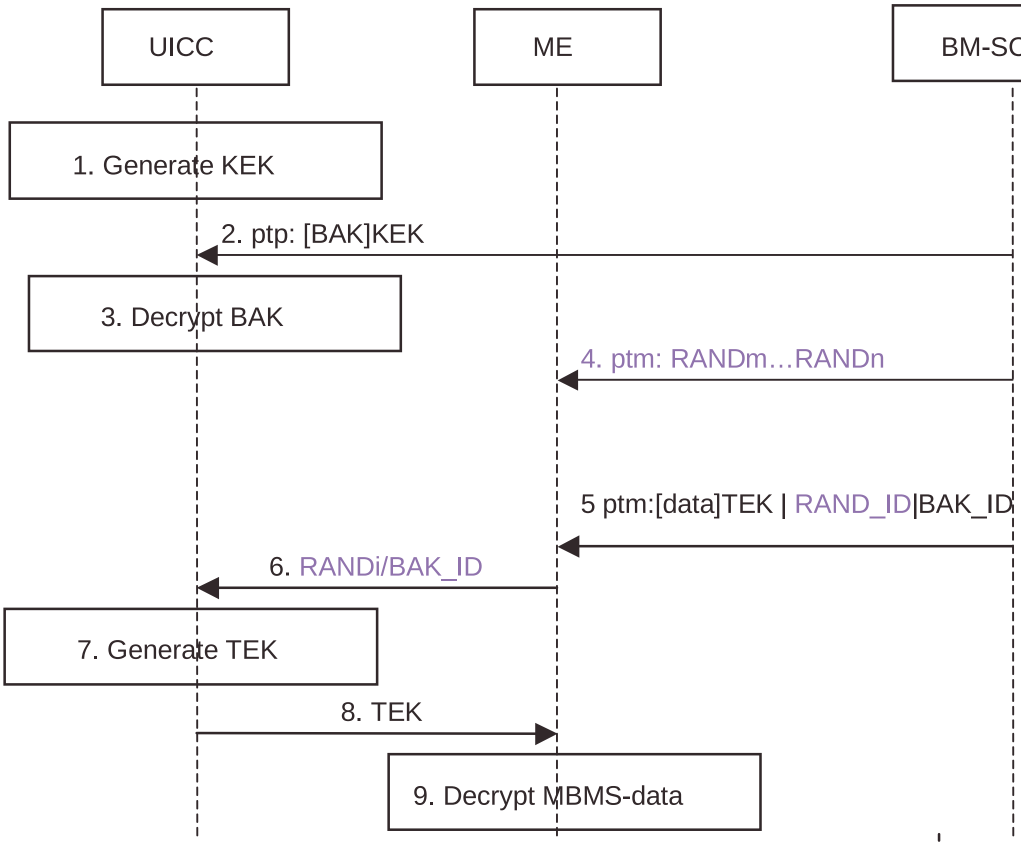

Figure 4: Improved combined method with new UICC (RAND_ID replaces encrypted TEK)

1. The UICC generates a KEK
2. The UICC receives a new BAK, which is encrypted using the KEK
3. The UICC decrypts the BAK using the KEK
4. The ME receive a group of RANDs in clear text
5. The ME receives a MBMS data packet, which contains encrypted MBMS data, RAND_id and BAK_id in clear text
6. If the ME does not have the current TEK then it sends a request to the UICC
7. The UICC generate the new TEK using BAK and RAND
8. The ME receives the new TEK
9. The ME decrypts MBMS data using the TEK

3 Conclusion

Subclauses 2.1 and 2.2 provide two methods to improve combined re-keying. Both methods decrease re-keying bandwidths (since only the key id or similar information is indicated). The main difference is that one uses the encryped TEK group and the other uses the RAND group in clear text. However, since the encrypted TEK group using BAK occurs frequently, the security of BAK is less.

If combined re-keying method is accepted, we propose selecting either subclause 2.1 or subclause 2.2 to enhance the combined re-keying performance.