**3GPP TSG SA WG3 Security — S3#31** **S3-030751**

**18 - 21 November 2003**

**Munich, Germany**

**Title:** **Further updates on Combined model for MBMS security**

**Source:** **Nokia**

**Document for:** **Discussion and decision**

**Agenda Item:** **6.20**

**Work Item:** **MBMS**

# 1 Introduction

This discussion paper provides further updates on the combined model presented first time in SA3 Antwerp ad hoc [S3z030020]. It also discusses the model for different aspects and summarizes comparison with other proposed models in some relevant aspects.

# 2 Discussion

The Combined method is designed to combine fast and reliable re-keying of Two-tiered method and low cost of introduction of Simple point-to-point method.

Low value MBMS services can allow KEK generation and storage of BAK in the ME, but high value MBMS services can require KEK generation and storage of BAK in the UICC.

This requires that BAK for low value services (BAK_low) is different from the BAK for high value services (BAK_high). Therefore, we have the following cases:

1. For ME with an old UICC only low value services can be accessed; ME contains BAK_low.
2. For ME with a new UICC, all services may be accessed; UICC contains BAK_high and ME (or UICC) contains BAK_low.

## 2.1 ME-based method

The ME-based method presented in the following is updated to include also the reply messages. The Figure 1 shows Combined method with an old UICC:

1. Mutual authentication
2. The ME and BM-SC generate a KEK
3. The ME receives a new BAK, which is encrypted using the KEK
4. The ME decrypts the BAK
5. The ME sends a response to the key update request message

6. The ME receives a MBMS data packet, which contains encrypted MBMS data, necessary key identification information in clear text. The packet may contain a new TEK in encrypted form.

7. If the ME has not the current TEK and the packet contained a new TEK then it decrypts the TEK using the BAK

8. The ME decrypts MBMS data using the TEK

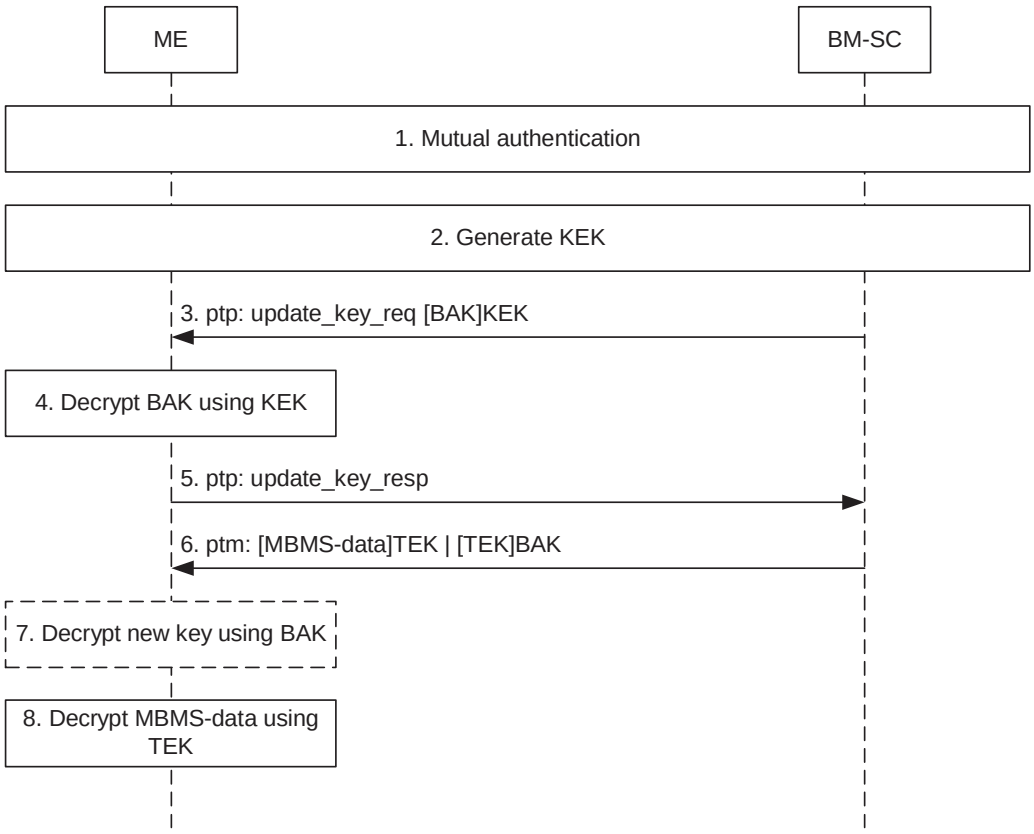


**Figure 1 - The Combined model with an old UICC**

## 2.2 UICC-based method

The UICC-based method presented in the following is updated to include also the reply messages. The Figure 2 shows Combined method with a new UICC:

1. Mutual authentication

2. The UICC and BM-SC generate a KEK

3. The ME receives an encrypted BAK

4. The ME request a BAK update from the UICC

5. The UICC decrypts the BAK using the KEK

6. The UICC sends a BAK response to the ME

7. The ME sends a update key response to the BM-SC

8. The ME receives encrypted MBMS data and necessary key identification information in the clear text. The packet may contain a new TEK in encrypted form.

9. If the ME has not the current TEK and the packet contained a new TEK then it sends a request to the UICC

10. The UICC decrypts the TEK using BAK

11. The UICC sends the TEK to the ME

12. The ME decrypts MBMS data using the TEK

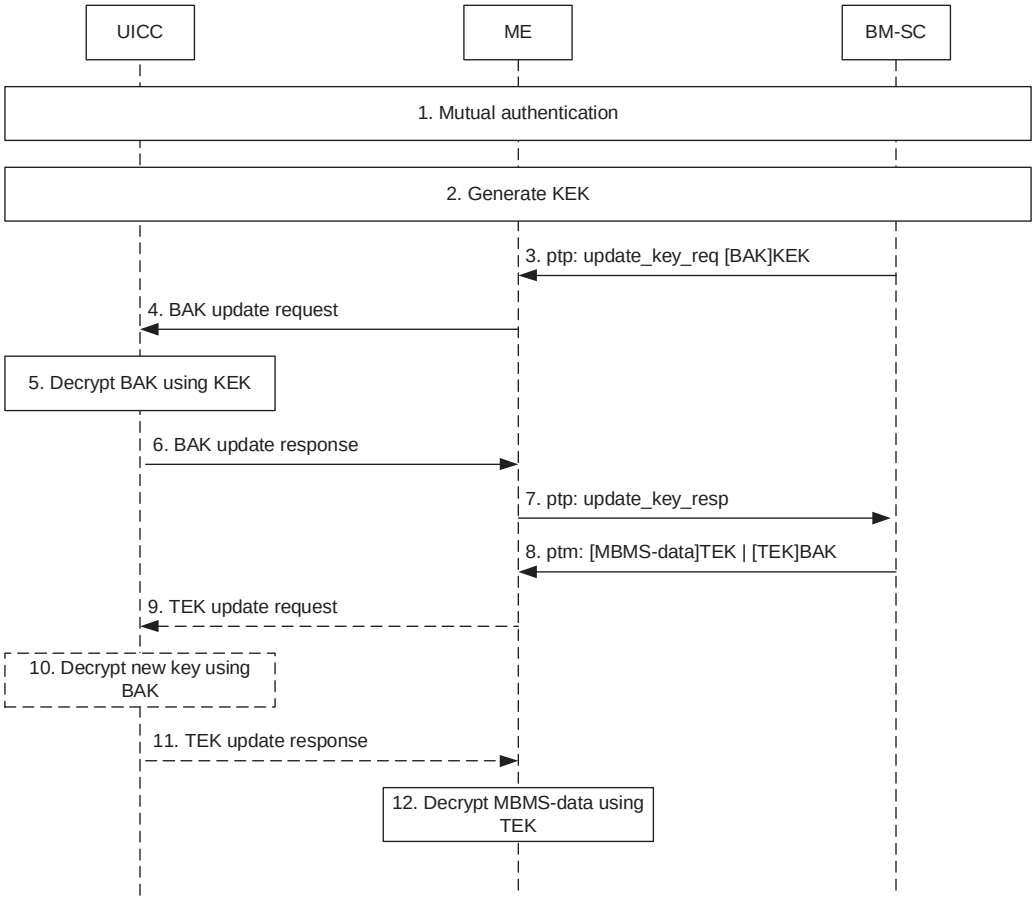


**Figure 2 - The Combined model with a new UICC**

## 2.3 KEK Generation

If GBA is used for mutual authentication (see Chapter 2.4), sufficient amount of key material is already available in both UE and BM-SC. If GBA is not used, then the KEK generation may be based on the use of pseudo random function (prf). This method is used in several key generation schemes (e.g. IKEv1 and EAP/AKA).

Key generation function:

key_material = prf(CK|IK)

The part of key_material (e.g. 128 bits for AES) may be used for the KEK and the other part of key_material may be used for the optional integrity key. The latter may be used for verifying the TEK integrity.

The algorithm specified in [FIPS 186-2] in appendix 3.1 may be used as a prf. It is based on SHA-1.

## 2.4 GBA usage for MBMS authentication

Alcatel contributed to SA3#29 San Francisco the idea to use generic bootstrapping application security mechanism for authentication between the UE and the BM-SC for MBMS [S3-030393]. Nokia sees that the authentication of the user towards BM-SC could indeed be done based on GBA [S3-030662], independently of which encryption and integrity protection mechanisms are chosen to protect the content delivery. This approach simplifies the overall security solution and it decreases the need of direct link between BM-SC and the bearer network.

The result of bootstrapping is a security association in the UE and in the bootstrapping server function (BSF). This security association can then be used to mutually authenticate the UE and a network application function (NAF) which BSF trusts.

The GBA uses existing 3GPP security mechanisms, in particular authentication and key agreement mechanism, to bootstrap a shared secret, which can further used to provide authentication services to BM-SC directly (BM-SC would be a normal NAF). At the same time key material is provided to BM-SC and UE. This may be directly used as KEK or at least for KEK generation.

The choice of Ua protocol (between UE and NAF) is dependent on non-security features also, i.e. joining procedure issues. Therefore the choice can't be done yet.

## 2.5 Comparison to 3GPP2 model

One difference between Combined and 3GPP2 model is that in the former model TEK is encrypted by BAK and not generated by a one-way function as is the case in the latter model. Therefore, it is possible to use in Combined model different BAKs in UICC and terminal, but still use the same TEK for same content (this is not possible in the 3GPP2 model). The benefit achieved with this is the following. For each (piece of) content, one TEK is enough to protect it. But it is still possible to decide independently whether the content can only be decrypted in case the MBMS subscriber has a BAK in the UICC. (To realize this, the TEK would only be sent downlink encrypted by "BAK_high", and not encrypted by "BAK_low"). This is a useful property if a differentiation 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.

## 2.6 Scalability

Nokia presented in SA3#30 Porto meeting MBMS – Overhead of the Re-keying paper [S3-030580], which estimated overhead in data amount in Combined and Simple point-to-point re-keying methods. The overhead was considered from the point of view of UE, radio resources and BM-SC. The calculations were rough estimations and were based on typical RTP traffic and educated guesses. According to the calculations the Combined method is more scalable compared to Simple model as re-keying is performed using point-to-multipoint messages.

The essence of calculation was to compare keys that are in the same level, i.e. Simple PTP TEK and Combined PTM TEK are in the same level and updated in same time intervals. In Simple model there are only one level of keys, but if there are derived keys for some other protocol, they are independent of this.

# 3 Conclusions

This paper has presented further updates on the Combined model for key management including e.g. the response messages. Additionally other relevant considerations on KEK generation, GBA usage, scalability and comparison to 3GPP2 model were provided.

Nokia proposes that the following are adopted as working assumptions in SA3.

1) Combined model adopted as a compromise between Simple and Two-tiered model

2) ME based solution chosen as a solution for Rel6

3) GBA [1] usage considered as a basis for authentication between UE and BM-SC

4) In later releases, BM-SC shall be able to distinguish between different solutions used by the UE

# 4 References


[S3z030020] MBMS – Combined Re-keying Method, SA3 ad hoc September, Nokia

[S3-030393] Discussion paper on Authentication in MBMS, SA3#29 San Francisco, Alcatel

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

[S3-030662] TS 33.220 V0.1.1: Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (Rel-6), SA3#31 November

[FIPS 186-2] Digital Signature Standard (DSS)", Federal Information Processing Standards Publication (FIPS PUB) 186-2, January 2000