3GPP TSG SA WG3 Security — S3#32 **S3-040039**
9 - 13 February 2004
Edinburgh, UK

Title: **Usage of GBA in MBMS**

Source: **Nokia**

Document for: **Discussion and decision**

Agenda Item: **6.20**

Work item: **MBMS**

1. INTRODUCTION

SA3#31 November meeting reached the following working assumption on MBMS security as indicated in the draft meeting report:

> *"For the ME part, GBA and MIKEY (with possible 3GPP-specific enhancements, e.g. for the support of encrypted keys) will be used as a basis for the standardised solution."*

In Nokia contribution *Further updates on Combined model for MBMS security* [S3-030751] GBA usage for MBMS authentication was described in high-level. The result of bootstrapping is a security association in the UE and in the bootstrapping server function (BSF). This security association will then be used to mutually authenticate the UE and a network application function (NAF), i.e. BM-SC, which BSF trusts. At the same time sufficient amount of key material is provided to BM-SC and UE. This may be directly used as KEK or at least for KEK generation.

2. DISCUSSION

2.1 MBMS Multicast Service Activation with GBA based UE authentication

Like specified in [TS23246], the MBMS multicast service activation procedure registers the user in the network to enable the reception of data from a specific multicast MBMS bearer service. The activation is a signalling procedure between the UE and the network. The procedure establishes MBMS UE contexts in UE, SGSN and GGSN and BSC/RNC for each activated multicast MBMS bearer service comparable to regular PDP contexts. Figure 1 below is based on Figure 7 in section 8.2 of [TS23246].

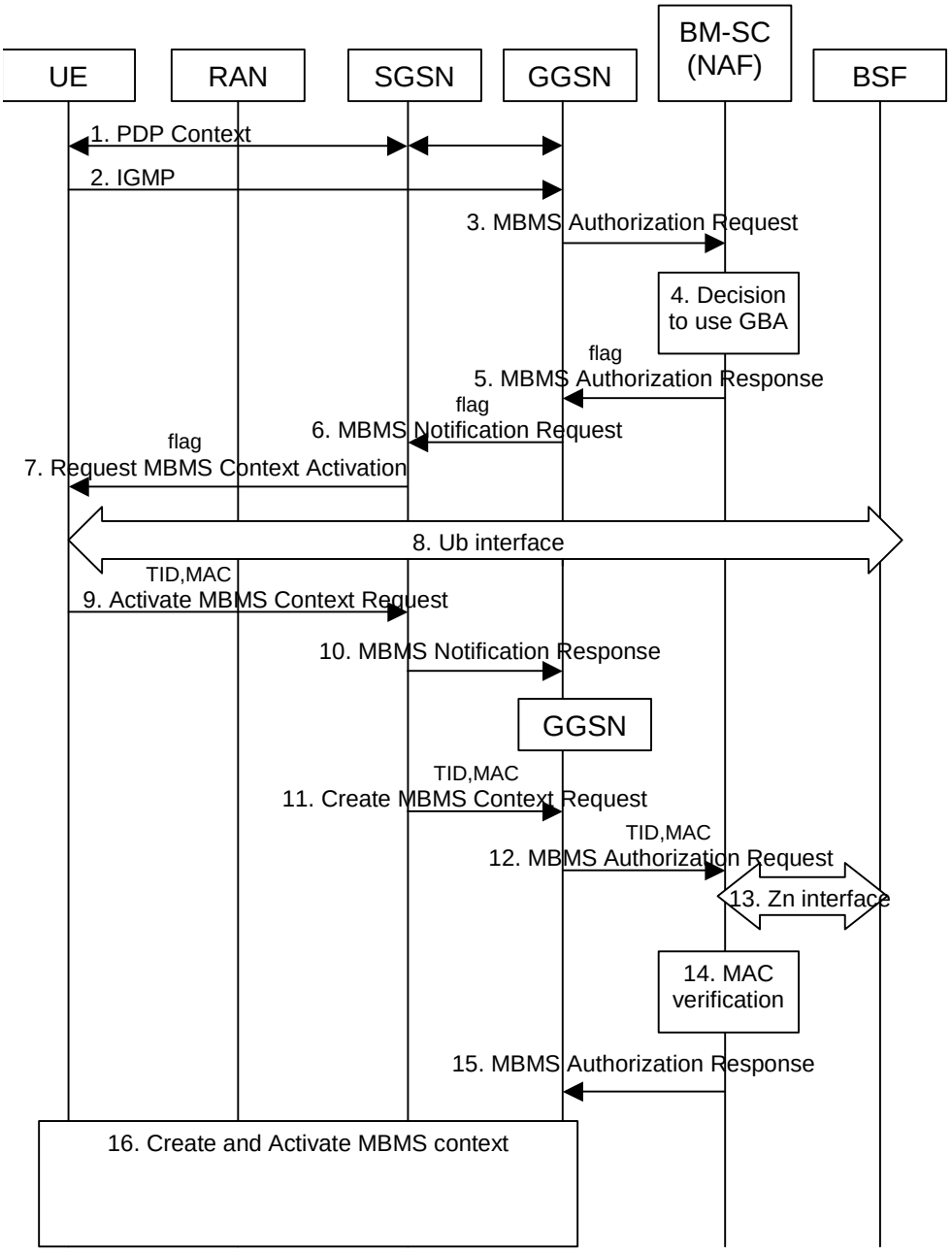

Figure 1: The activation of an MBMS multicast service with GBA based authentication.

The basic steps in figure 1 follow the steps described in section 8.2 of [TS23246]. In addition, the figure and steps describes how GBA based authentication can be used in MBMS service activation procedure.

The actual changes are the following. When BM-SC has decided to use GBA authentication after message 3, BM-SC indicates to the UE that bootstrapping is required by using a “flag” which is transported from BM-SC to UE via messages 5-7. In step 8, UE bootstraps and calculates an authentication value (e.g., a MAC of the parameters in message 7 calculated with a NAF specific key), sends this authentication value and the TID to BM-SC via messages 9, 11, and 12. BM-SC fetches the NAF specific key (Ks_NAF) from BSF using the TID via Zn interface in step 13. If authentication succeeds (i.e. BM-SC verifies the authentication value with a positive result), a successful MBMS authorization response is sent to GGSN in step 15, and rest of the creation and activation procedures (step 16) follow the messages described in section 8.2 of [TS23246]. If authentication fails, a failure is indicated to the GGSN using message 15.

2.1.1 Authentication value

The details about how to define the authentication value are ffs. If the MAC approach is chosen, it has to be defined, e.g.:

- which MAC algorithm is used,
- how to derive the key for MAC calculation from Ks_NAF,
- which parameters from message 7 are included in the MAC calculation.

Note that the key used for MAC calculation should be different from KEK but both keys can be derived from the same key material Ks_NAF.

3. CONCLUSION

The above described GBA usage for MBMS authentication is according to the working assumption reached in SA3#31. It is proposed that SA3 includes the GBA authentication related steps presented in the chapter 2.1 to the TS 33.246.

REFERENCES

[TS23246] 3GPP TS 23.246: “Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description”, Rel-6.

[S3-030751] Further updates on Combined model for MBMS security, SA3#31 November, Nokia