**3GPP TSG SA WG3 #28** **S3-030249**

**6-9 May 2003**

**Berlin, Germany**

**Agenda Item:** 6.21 MBMS

**Source:** Ericsson

**Title:** Key generation and distribution in MBMS

**Document for:** Discussion and decision

# 1. Scope

This paper aims to discuss different proposals on how the traffic encryption key (TEK) generation and distribution to UE can be implemented in the MBMS architecture; and proposes as a conclusion that TEK generation and distribution to UE are performed by the BM-SC. This is the Ericsson preferred solution.

# 2. Introduction

At SA3 #27 it was decided that encryption for MBMS traffic shall take place between the BM-SC and the UE. Encryption for MBMS traffic in the BM-SC is optional. For other services as DRM, when encryption is already provided of the content outside the BM-SC, the operator should be able to switch off encryption in the BM-SC.

In particular three still outstanding issues related to security are how the authentication procedure in MBMS shall be supported in the MBMS architecture; and also traffic encryption key (TEK) generation and distribution for the MBMS needs to be resolved. These three issues are very related but discussed in two different contributions. This contribution discusses the key generation and distribution. For authentication procedure in MBMS, see contribution [3] from Ericsson.

At SA3 #27 Ericsson presented a comparison of five identified security framework scenarios for MBMS [2]. The scenarios are based on Alcatel's MBMS security discussion paper [1]. The main properties of the scenarios are repeated below as well as figure of scenario 1, as an illustration of the architecture. Scenario 1b is a variation of scenario 1, where there is no MBMS specific authentication, but the GPRS authentication is re-used.

**Scenario 1:** all security functions performed by BM-SC

**Scenario 1b:** all security functions performed by BM-SC, except the authentication procedure between the UE and SGSN which is re-used

**Scenario 2:** authentication between UE and SGSN, key distribution is performed by SGSN, key generation and traffic protection done by BM-SC

**Scenario 3:** authentication between UE and SGSN, traffic protection done by RNC, key distribution done by SGSN, key generation done by BM-SC

**Scenario 4:** authentication between UE and SGSN, traffic protection done by RNC, key generation and distribution done by SGSN

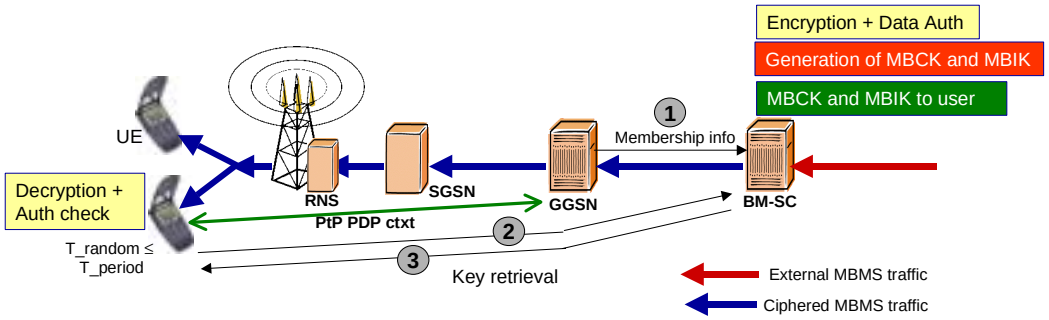


**Figure 1** Scenario 1: all security functions performed by BM-SC [1]

Scenarios 3 and 4 are ruled out according to the decision at SA3 #27 that encryption for MBMS traffic shall take place between the BM-SC and the UE, since these scenarios don't use encryption between the UE and BM-SC.

This contribution discusses which nodes should perform the traffic encryption key (TEK) generation, and distribution of this key to the UE. For completeness this contribution discusses all combinations where the BM-SC or SGSN can take the roles of TEK generator or TEK distributor.

# 3. Discussions

In principle, either BM-SC or SGSN may perform the TEK generation and/or distribution. This gives us four different alternatives, which are discussed below:

- Alt 1: TEK generation: BM-SC, TEK distribution: BM-SC
- Alt 2: TEK generation: BM-SC, TEK distribution: SGSN
- Alt 3: TEK generation: SGSN, TEK distribution: SGSN
- Alt 4: TEK generation: SGSN, TEK distribution: BM-SC

## 3.1 Why SGSN is not a good alternative for key generation

In general it may be beneficial to re-use some existing functionality in a node for new services and applications. For example GPRS authentication between UE and SGSN might be re-used for MBMS service. This is discussed in another paper from Ericsson [3]. However, introducing MBMS TEK generation to SGSN is *not* a case of re-using existing functionality. There are several reasons why SGSN is not a good alternative for key generation:

- Efficiency
  SGSNs have not been designed for generating encryption keys. Introducing key generation function to SGSN means that an existing SGSN platform, that has been designed and optimized for other functionality, needs to be upgraded with totally new functionality. These kind of changes can be very complex to implement. Thus it is most probable more efficient to place the TEK generation function in BM-SC that can be designed and optimized for that purpose from the beginning .
- Easier migration
  Migration to MBMS service is easier for operators if SGSN does not generate the TEK, since instead of introducing key generation function to each SGSN, it can be implemented in one central node, i.e. BM-SC.
- Complexity
  As the traffic encryption is done in BM-SC it is logical that also the TEK is generated in BM-SC. Since if the TEK generation is made in SGSN, the TEK needs to be transferred to the BM-SC and, furthermore, different encryption keys will be generated in different SGSNs and the BM-SC needs to encrypt the same MBMS traffic with different keys.

Moreover, there is the following requirement in [4]:

*R4b: The MBMS multicast data may be encrypted with a common encryption key, which shall be available to all users that have joined the MBMS service.*

This requirement implies that it shall be possible to encrypt the same MBMS multicast data with one common encryption key, which would be difficult to fulfill, if each SGSN generated one individual MBMS encryption key.

Thus alternatives 3 and 4 are discarded.

## 3.2 Alt 1: TEK generation: BM-SC, TEK distribution: BM-SC

In this alternative the BM-SC generates the TEK and also distributes it to the UE.

This alternative is the only one that can be considered access independent from security point of view, since TEK generation and distribution are performed between UE and BM-SC. This allows easier introduction and interoperability of MBMS services with other access technologies such as WLAN. Other alternatives are more or less 3GPP specific, since one or more security functions have been moved to 3GPP specific nodes.

When the BM-SC is the key generator, the TEK is generated in the same node where the traffic encryption takes place and extra key transports between network nodes are avoided.

In case of roaming, the home network has control of key generation and key distribution. I.e. there are no trust issues to the visited network.

If the user authentication for MBMS service is done at between UE and BM-SC, the TEK distribution from the home network to the UE can be incorporated in the authentication procedure (see contribution [3]) between UE and BM-SC. This has been presented also in [5]. Also, when there is a need to perform re-keying, the BM-SC is able to re-authenticate the UE during the re-keying procedure, if needed.

## 3.3 Alt 2: TEK generation: BM-SC, TEK distribution: SGSN

In this alternative the BM-SC generates the TEK but the SGSN distributes it to the UE.

In this alternative synchronization problems become likely when, during an MBMS data transfer, a fresh traffic encryption key (TEK) has to be transferred (due to re-keying) from the BM-SC to the SGSN before distribution to the UE. Also, distribution of keys between nodes adds on the overall complexity of the participating nodes and increases the standardisation effort in 3GPP.

In roaming case the home network has to forward the keys to the visited network and the home network has no control of the key distribution in the visited network. For roaming users to be able to receive MBMS services from their home network there must be an agreement between the two operators such that the BM-SC of the home operator can instruct the SGSN in the visited network.

If the SGSN distributes the keys to the UE in GMM/SM layer, modifications or additions to GMM procedures are needed.

In addition, there will be layering issues in the terminals as encryption key distribution is performed in one layer and decryption of the MBMS traffic is performed in another layer.

# 4. Proposal

Based on the working assumption to have encryption of MBMS traffic between UE and BM-SC and based on the analysis presented, it is proposed that the BM-SC node takes care of the TEK generation and distribution.

Combined this with application level authentication it is proposed that the whole security framework for MBMS is implemented between the UE and BM-SC.

# 5. References

[1] Tdoc S3-020363 MBMS security, Alcatel

[2] Tdoc S3-030061 Comparison of MBMS security scenarios, Ericsson

[3] Tdoc Authentication in MBMS, Ericsson

[4] TS 33.246 v 0.1.0 Security of Multimedia Broadcast / Multicast Service

[5] Tdoc S3-030063 Key distribution at application layer for MBMS, Ericsson