3GPP TSG SA WG3 Security — S3#23 S3-020355

9 - 12 July 2002

Helsinki, Finland

3GPP TSG-SA WG2 meeting #25 **Tdoc S2-022040**

Naantali, Finland, 24th – 28th June 2002

Title:	**Liaison statement on the MBMS security**
Source:	**SA2**
To:	**SA3**
Cc:	**SA1, RAN2**
Response to:	**-**

Contact Person:

Name:	Laurent Thiébaut
E-mail Address:	laurent.thiebaut@alcatel.fr

Attachments: S2-021987, S2-021983.

1. Overall Description:

1. Introduction:

SA2 has been discussing security of MBMS service (while considering many Tdocs among which 2 are attached[1]). SA2 would like to ask SA3's opinion on the issues mentioned in this LS.

2. Discussion

SA2 discussed following (non exhaustive) list of potentials requirements:

- The ciphering key shall be common to all users / many users (e.g. within an SGSN area) receiving the same MBMS service. Ciphering key cannot be particular to a user. Ciphering key cannot be part of user UMTS subscriptions.
- Should The ciphering key used at one moment for a MBMS service be the same for the whole MBMS distribution tree so that a UE is not obliged to get a new ciphering key each time it changes its location within a same MBMS distribution area? (questions about synchronization of keys have been raised) The entities that will use the ciphering key (UE + Network element) shall obtain it from the entity providing the ciphering key. Should the ciphering key change during the session?As the ciphering key can change during a MBMS session (to avoid fraudulent access to the service when users leave the service), access to the key shall be possible at start of the MBMS session and during session duration. Ciphering applied to MBMS content shall cope with compression tools (RoHC) used on the radio interface.

[1] It has to be noted that consensus on this Tdochas not been reached.

- Where should encryption (and - if needed - integrity protection (i.e. traffic protection) be done)?
- Which entity should be responsible for key management?
- Which entity should take care of key distribution to the authorized UEs
- How often should we change the key?
- Which mechanism to use for this key refresh?
- Issue related to Digital Rights Management (DRM)
- Should not event driven key mechanism be provided?
- We also discussed scalability and roaming issues.

.

3. Actions:

Action for SA3:

Therefore, SA2 kindly asks SA3 to provide answer / guidance ASAP to the questions / issues mentioned in section 2 of this LS.

Could you also comment on the attached documents that were used during our discussions.

4. Date of Next SA2 Meetings:

Title	Date	Location
SA2#26	19th August –August 2002	Toronto, Canada

3GPP TSG SA WG2 #24 **S2-02~~1744~~1983**

Naantali, Finland, 24th-28th June 2002

Agenda Item: **9.5 MBMS**

Source: Nortel Networks

Title: MBMS data ciphering key use

Document for: Discussion & approval

1. Introduction

This contributions proposed discussions on MBMS ciphering key use.

2. Constraints for MBMS ciphering key use

The ciphering key management for MBMS faces the following constraints:

- There is a need to change the MBMS ciphering key as some ~~when a~~ UE ~~leaves~~ can leave a MBMS session or ~~when its~~ their subscription to a MBMS service ~~is~~ can be removed in order to forbid them~~it~~ to listen to the MBMS data still distributed for other users.
- The new key have to be provided to the remaining users. It appears not probable that each UE in the entire MBMS distribution tree get the new key at the same instant. So that the key has to be distributed before it is used and the trigger to determine when the key will be used has to be known by the users. Until the new key can be used, the user have to use the old key with which the MBMS data are ciphered.
- To provide the key individually to each ~~right~~ authorized user~~, a dedicated channel has to be used~~. It is seen as reasonable to avoid to ~~get~~ provide simultaneously ~~all the dedicated channel~~the key established for all the users present in a cell at the same time.

3. Proposal of a ciphering key use principle

It is proposed to use an odd & even key principle. With this principle:

- 2 keys will be made available in each UE: the "current key" and the "next key" to be used.
- The change of key for data ciphering will occur and the trigger has to be known by each UEs that activated the service. At each trigger, the "current key" is not more used to encrypt/decrypt the MBMS data and the "next key" becomes the "current key".
- Definition of the trigger is FFS
- Each UE has to get the "next key" before the trigger that un-validate the "current key" occurs
- A smooth distribution of the key is provided as each UE can initiates this key request independently.

The procedure used by the UE to get the "next key" and the entity that provide the key remain FFS.

4. Conclusion

It is proposed to discuss the above constraints and the proposal and to add the agreed statements of section 2 ~~and 3~~ in the MBMS TR 23.846 under Security chapter 5.4.6~~1.2~~ and to add the content of section 3 in a new sub-chapter 5.4.6.1 with the title “Proposal 1 for a ciphering key use principle”.~~.~~

3GPP TSG-SA WG2#25 **Tdoc S2-021987**
Naantali, Finland
24th – 28th June 2002

Agenda items: **Agenda 9.4, MBMS**
Source: Alcatel
Title: MBMS security
Document for: Discussion and Decision

1. Introduction

To prevent unauthorized user access to MBMS data, the MBMS data may be secured. The security functions to be applied may include integrity protection and data confidentiality. Confidentiality is assured by encryption of the data. It’s important to decide at which level as well as where in the MBMS network the security functions shall be applied. In this document we give a high level overview of possible scenarios. We identify the level at which encryption and integrity protection should be done (application level or radio part), the entity that should be responsible for key management and the way membership management and key distribution should be done.

The aim of this paper is to present the different possible scenarios to the SA2 community as well as their architectural implications and to initiate a discussion that can lead to a liaison statement for SA3.

Main questions

Where should encryption (and integrity protection (i.e. traffic protection) be done?
We consider here two possibilities, either traffic protection can be done at RAN level by the RNC as is the case for unicast GPRS, or it can be done at application level by the BM-SC.

Which entity should be responsible for key management?
The function of key management involves generating the secret key material (used for encryption and integrity protection), up-dating this key material regularly if necessary and passing this key material to the entity that is in charge of applying encryption/integrity protection and key distribution down to the UEs (which could be the same as the entity responsible for key generation).

Which entity should take care of group membership management and key distribution to the UEs?
Finally the key and key updates should be delivered to the authorized users. This comprises authentication and authorization of the receivers such that only the authorized receivers obtain valid key material.

The last two functions are often considered together and called “key management”. However for scalability reasons it may sometimes be useful to delegate the latter function (membership management and key distribution) to separate entities.

Assumptions

For point-to-point PDP contexts, integrity protection and ciphering is done in the RAN and stays exactly the way it is specified.
If MBMS data is secured in the RAN then the AKA mechanisms to decide on security algorithms and corresponding keys should be modified such that all group members can share the same security parameters.
If MBMS data is secured at application level (by the BM-SC) then the security features provided for the RAN (e.g. data encryption) should be switched off for MBMS traffic.

2. Overview of different security scenarios

Scenario 1: all security functions performed by BM-SC

In this scenario the BM-SC acts as the source of the data from the UE point of view. The BM-SC chooses the keys and protects (encryption and integrity protection) the data before sending it on the MBMS network. Although the figures focus on encryption, integrity protection may if needed always be provided jointly with ciphering. This is not indicated in the figures in order not to overload them. The UE receives the keys directly from the BM-SC. This is indicated by steps 2 and 3 in Figure 1. We propose that the user fetches a new key over a secure ptp connection to the BM-SC. We propose that the UE initiates this process at a random time within the re-key period to avoid too many simultaneous ptp connections to the BM-SC.

Before the UE receives the keys he is authenticated and authorized by the BM-SC. For this the BM-SC performs two checks: is the UE a valid group member and has the UE activated the right MBMS PDP context. If both checks succeed the UE receives the keys. The first check warrants that the UE paid for the multicast service (i.e. for the content) whereas the second check ensures that the UE will be charged by the operator for the bytes received over the mobile network.
The BM-SC knows about group membership but it might be necessary that it receives the information about PDP context activation in a secure way from the GGSN. The latter information exchange is indicated by step 1 in Figure 1.

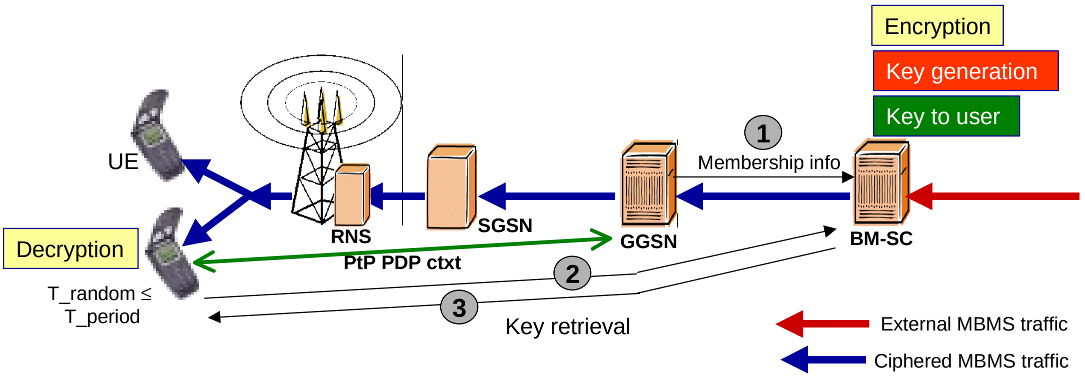

Fig 1. Scenario 1: all security functions performed by BM-SC

If encryption is done end-to-end between the BM-SC and the UE this is most likely to be at IP level or at a higher level (application level) and we recommend it to be at higher level to cope with compression on the radio. In the case that the mobile terminal connects a laptop to the internet this means that decryption will be done on the laptop. The USIM should however always be involved in the authentication and authorization process.

Scenario 2: key distribution is performed by SGSN, key derivation and traffic protection done by BM-SC

In the second scenario illustrated in Figure 2, the function of group membership management and key distribution is delegated to the SGSNs. The BM-SC still derives and periodically updates the keys and performs integrity protection and encryption of the data.

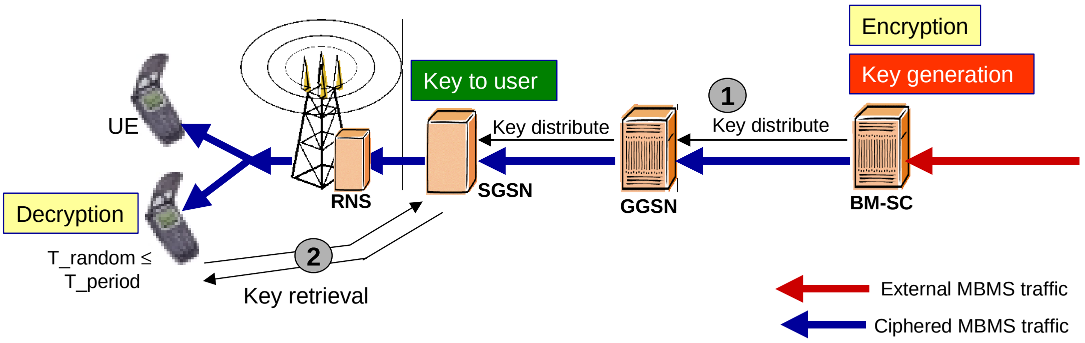

Fig 2. Scenario 2: key distribution done by SGSN, other security functions performed by BM-SC

As for scenario 1, this scenario implies that the UE fetches a new key at random times within the re-key interval but this time from the SGSN.
Note (valid for all scenarios with SGSN distributing the key to the UE): Existing GPRS procedure for key agreement (AKA) cannot be used

- The current PS domain key is specific for an UE while this is not the case for MBMS
- The current PS domain key (i.e. Key used by current PS domain point to point procedures) is not linked with a specific session while this is needed for MBMS
- The messages used to transfer information are linked to attachment of the user, not to the session activation, so cannot be re-used for MBMS

The process of fetching a new key may be combined with a routing area update, relocation etc. The issue behind reusing GMM/PMM procedure to fetch the key is that the period of these procedures may not be compatible with the period required by MBMS key re-fresh procedure.

The SGSN needs to authenticate and authorize the UE. The SGSN has the right PDP context information but he must receive the group membership information from the HLR or from the BM-SC. Existing protocols can be used for the UE to authenticate to the SGSN.
A new protocol is required between the BM-SC and the SGSN for key distribution, possibly with an intermediate role for the GGSN.

Scenario 3: traffic protection done by RNC, key distribution done by SGSN, key derivation done by BM-SC

This scenario is illustrated in Figure 3. The BM-SC still generates the key and key updates. Key distribution to the UE and authentication and authorization of the UE is delegated to the SGSN and happens in exactly the same way as in the previous scenario 2. This means that also in this scenario a new protocol is required between the BM-SC and the SGSN for key distribution, possibly with an intermediate role for the GGSN.
Additionally also encryption and integrity protection is now delegated, to the RNC. This means that the RAN must be informed of the appropriate key material and instructed to protect the data before forwarding it. This requires modifications to the protocol between the SGSN and the RNC.

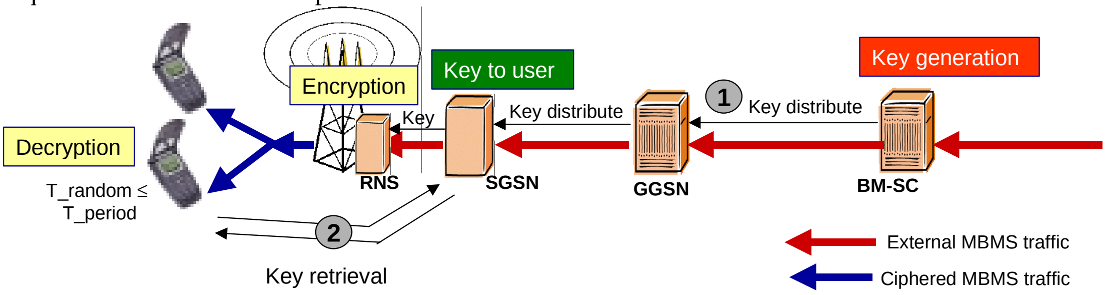

Fig 3. Scenario 3: traffic protection done by RNC, key derivation done by SGSN, key generation done by BM-SC

Scenario 4: traffic protection done by RNC, key derivation and distribution done by SGSN

In the final scenario the BM-SC is not involved at all in the MBMS security. It is illustrated in Figure 4.

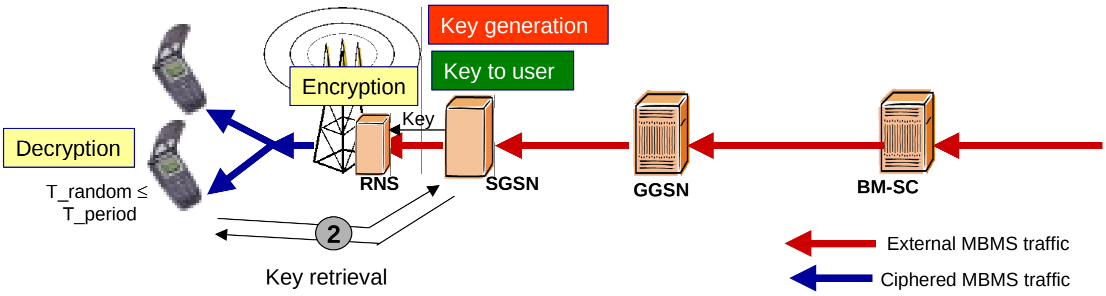

Fig 4. Scenario 4: traffic protection done by RNC, key derivation and distribution done by SGSN

The SGSN must now generate and periodically refresh the keys. The RNC performs integrity protection and data encryption and hence the same modifications to the SGSN-RNC protocol are required as in scenario 3.
To be able to do the necessary UE authorization the SGSN must receive group membership information from the HLR or from the BM-SC. This is identical as in scenario 2.
With scenario 4, mobility problems may arise as Iur interface may be used. Users of the same service may then receive the same content encrypted with different key in the same cell.