3GPP TSG SA WG3 Security — S3#23 **S3-020363**
9 - 12 July 2002
Helsinki, Finland

3GPP TSG-SA WG3#24 **S3-02xxxx**
Helsinki, Finland
9-12 July 2002

Agenda item: **Agenda 7.19, 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 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.

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 (the Broadcast/Multicast ciphering key (BMCK) and the Broadcast/Multicast integrity key (BMIK)), 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 to the entity in charge of key distribution down to the UE's (the latter 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 keys 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 two functions above 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.

Should it be possible to re-fresh the encryption and data authentication keys during a session?
From a security point of view it can be necessary to regularly re-fresh the keying material. If the charging for multicast traffic has a finer granularity than an entire session then updating the encryption key will additionally be necessary to avoid that users that have left the service (and stopped paying for it) would continue to receive the MBMS data. The issue of key updates exists for each of the scenarios that are discussed below. The following three issues are related to this topic of key updates.

First, with what frequency should the encryption and authentication keys be updated? Considerations related to the frequency of key updates can differ in the different scenarios.

Secondly, if the keys can change during the session then there must be a mechanism to communicate the key updates to the UE during the session. This mechanism will differ in the different scenarios depending on which entities in the network are responsible for key generation and key distribution to the UE.

Finally it should be considered whether the key updates are network initiated or UE initiated.

Should the ciphering and authentication keys used at a particular moment for a particular session be the same for the whole MBMS distribution tree?
Having the same ciphering and data authentication keys for the whole MBMS tree has the advantage that the UE is not obliged to get new keys when it changes location during an MBMS session. On the other hand, this requires distributing a new key material to all UE's every time one UE joins or leaves the MBMS service. Managing different key material more closely to the UE's would enable to update the key material only for the impacted group of UE's.

Scalability and roaming issues
The scalability and the possible implications of roaming should be carefully considered for each proposed solution. One particular aspect of scalability is related to the question above, since the ability to change the key material when UE's join/leave the MBMS service clearly has an impact on the scalability of a solution.

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 (i.e. data encryption and authentication performed by the RNC) should be switched off for MBMS traffic.

2. Overview of different security scenarios

In this section we present four different scenarios. Each scenario corresponds to a different choice of entities that are responsible for key generation and updates, encryption / data authentication and UE authentication and key distribution to the UE. For each scenario we discuss the implications to the main questions that were listed above.

Scenario 1: all security functions performed by BM-SC

In this scenario the BM-SC performs all security functions and acts as the source of the data from the UE point of view. The BM-SC chooses the keys and key updates (BMCK and BMIK), protects (encryption and integrity protection) the data before sending it on the MBMS network and is responsible for user authentication and key distribution to the UE. In this scenario the entire MBMS tree uses the same keys which facilitates mobility. We propose that the user fetches a new key over a secure ptp connection to the BM-SC. We further propose that the UE initiates this process at a random time within a pre-determined re-key period to avoid too many simultaneous ptp connections to the BM-SC. This is indicated by steps 2 and 3 in Figure 1.
Before the UE receives the keys it 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.

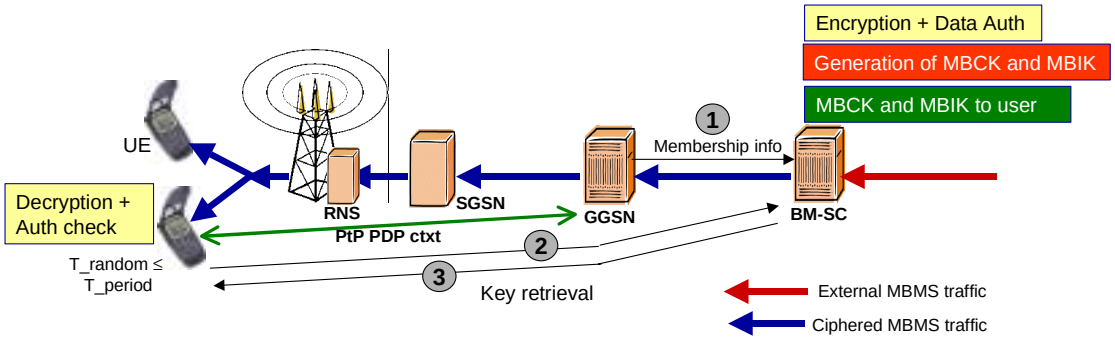

Fig 1. Scenario 1: all security functions performed by BM-SC

Instead of one BM-SC, the central BM-SC could have a number of delegates that perform user authentication and key distribution in a smaller domain to make the solution more scalable. These delegates must of course posssess the right UE information and the last key updates.
This scenario has no special issues for roaming users.
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.

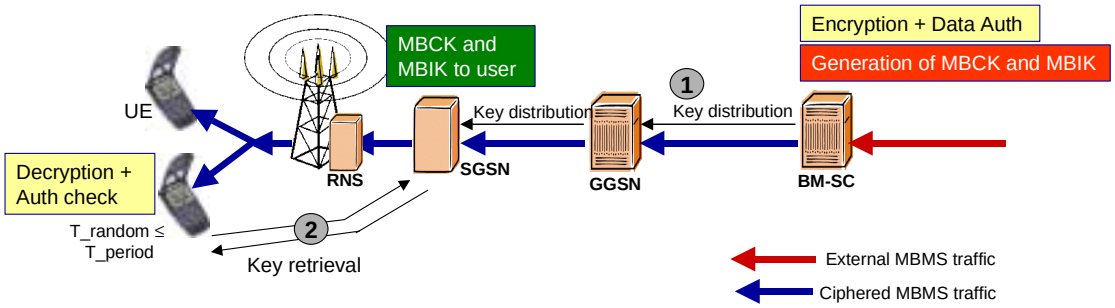

Fig 2. Scenario 2: key distribution done by SGSN, other security functions performed by BM-SC

As in Scenario 1, we propose 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 keys are specific for a UE while this is not the case for MBMS
- The current PS domain keys (i.e. the ciphering and integrity keys used by the current PS domain point to point procedures) are 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. However reusing GMM/PMM procedure to fetch the keys is not always possible e.g. because 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 it must receive the group membership information from the HLR or from the BM-SC. Existing protocols can partially be used for the UE to authenticate to the SGSN although some modifications will be necessary.
A new protocol is required between the BM-SC and the SGSN for key distribution, possibly with an intermediate role for the GGSN.
In this scenario, just as in the first one, the same keys are used in the entire MBMS tree. This facilitates user mobility. Since an SGSN covers a much smaller region than a BM-SC this scenario has no special scalability problems.
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.

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 keys 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 Scenario 2. We propose that the UE fetches the key updates from the SGSN at random times within a pre-defined re-key period. 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.

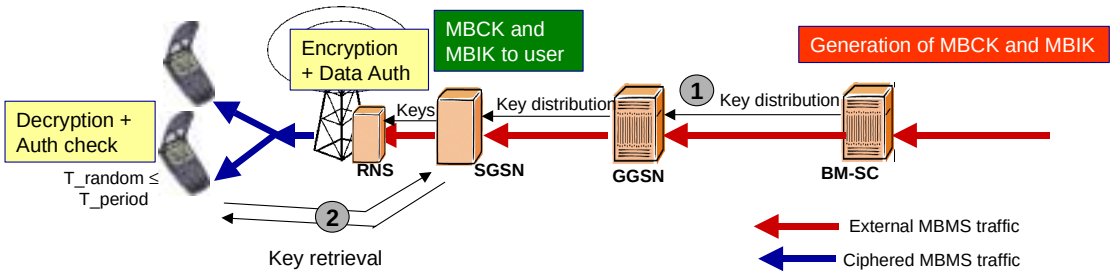

Fig 3. Scenario 3: traffic protection done by RNC, key distribution done by SGSN, key generation done by BM-SC

Again there are no special scalability problems since the number of UEs under one SGSN (and which hence can contact the SGSN for authentication and key updates) is not particularly large.
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.

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.

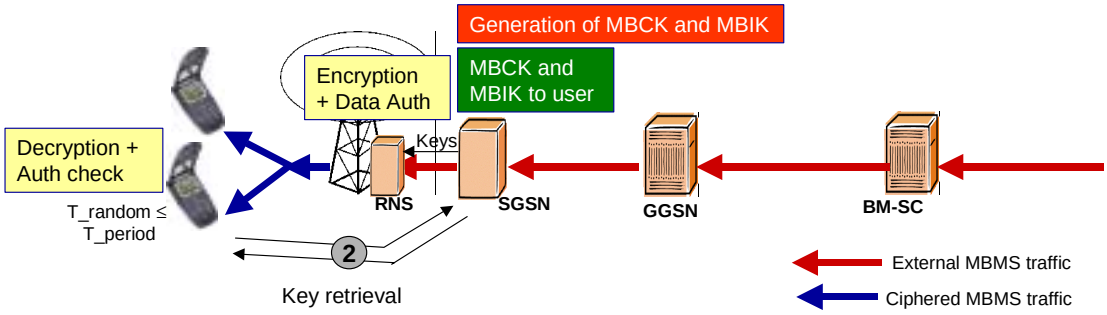

Fig 4. Scenario 4: traffic protection done by RNC, key derivation and distribution done by SGSN

The SGSN must now generate and periodically refresh the keys as well as authenticate and authorize the UEs and distribute the keys to the UE's. The RNC performs integrity protection and data encryption. Hence, the same modifications to the SGSN-RNC protocol are required as in Scenario 3 to deliver the correct keys from the SGSN to the RNC.
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 to Scenario 2.
In this Scenario 4, mobility problems may arise as Iur interface may be used. Users of the same service may then receive the same content encrypted and integrity protected with different keys in the same cell. Alternatively, users that change SGSN while moving from one region to another will have to switch over to new decryption and data authentication keys and this must be synchronized with the data streams.
This scenario has also extra issues for roaming users. If users want to receive an MBMS session from their home network then the foreign SGSN must deal with the security of this traffic independent of the network of origin.

3. Discussion

In the table below we summarize the arguments in favour and against the different scenarios. The properties in red and italic are negative whereas the properties in green which are not italic are the positive characteristics.

	BM-SC	SGSN	RNC
Key to User	*Scalability issue* Group membership maintained in BM-SC (one place) ❶	*SGSN must know group subscriptions* *Roaming issue in* ❷, ❸ Scalability Secure protocol UE-SGSN largely exists but need changes as current AKA procedure cannot be re-used ❷, ❸, ❹	
Ciphering and Integrity protection	Encryption done only once BM-SC to RNC also protected (Iu, Gn, Gi) ❶, ❷		*Need to refresh the key on RNC implies a RANAP modification* *Roaming issue* Encryption technology already exists ❸, ❹
Key Derivation	❶, ❷, ❸	*Mobility problems* ❹	

A scenario where the individual UEs fetch the keys directly from the BM-SC can lead to scalability problems (Scenario 1). Optionally the UE authentication and key distribution can be delegated by the central BM-SC to several delegate BM-SCs spread over the network. This should be further studied for Scenario 1. If the scalability issue can be solved for Scenario 1 then Scenario 1 has certainly the most favorable arguments and is therefore our preferred solution.

If the SGSN distributes keys that are derived by the BM-SC then the BM-SC must be able to instruct the SGSN (Scenarii 2 and 3). This might be an issue for roaming users where the SGSN is in a different PLMN than the BM-SC. The same issue exists in the case where the BM-SC derives the keys and the RNC, possibly in a different PLMN, is in charge of traffic protection.

A disadvantage that implies a serious overhead is the mobility issue in the case that the SGSN is in charge of key generation (Scenario 4). The fact that the SGSN chooses the keys implies that when a UE moves from a region covered by one SGSN to a region covered by another SGSN this UE should fetch and switch over to the new keys in synchronization with changing SGSN. This is an overhead which does not appear at all in the other scenario. We would therefore reject Scenario 4.

Further Issues

For the BM-SC to perform traffic protection (encryption and integrity protection), all MBMS data has to pass via the BM-SC also if the data would come from a third party content provider. This can also be tackled if there is coordination amongst the set of BM-SC's.

Digital Rights Management (DRM) can also come into the picture when MBMS data is stored on the user's device. This issue is however not typical for MBMS but exists also for unicast and in the fixed world.

4. Proposal

The proposal gives an overview of 4 different security scenarios that differ based on the entity that performs the following security functions: key derivation, data integrity and encryption and key distribution to the UE. Based on a comparison between pros and contras of the different scenarios, preference goes to the scenarios where at least key derivation is performed by the BM-SC. If the scalability issue of the first Scenario can be solved e.g. by using a number of delegate BM-SCs then it is suggested to adopt Scenario 1 as the preferred solution.