3GPP TSG SA3 Ad-hoc Meeting **S3z030015**
3 - 4 September 2003
Antwerp, Belgium

Agenda item: 6.3

Source: Samsung

Title: User grouping for MBMS key distribution

Document for: Discussion and Decision

1. Introduction

This contribution focuses on user grouping for MBMS key distribution. It is pointed out that the key distribution for multiple services is something similar to the key distribution for LKH, and hierarchical TMGI composing is proposed based on this similarity. As this hierarchical TMGI can be easily implemented to support LKH based re-keying according to operator's decision, it is proposed to be adopted by SA3 for MBMS key distribution.

2. Discussion

2.1. Key distribution for multiple services

As we know, depending on its capability, the network may be able to support multiple different MBMS services at the same time. Thus, multiple MBMS services may exist at the same time within one user's home network, which may be interesting for this user. So, depending on UE's capability, this user may select to join multiple services and receive them at the same time. For example, one user may wish to read some real-time news provided by BBC while listening to one living concert provider by Berlin Philharmonic. Different TEKs shall be likely used for these different services, and different Key Encryption Key (KEK) may be used for the protection of these TEKs distribution. Thus, this UE should store all these keys and know which key is for which service. As each MBMS service is uniquely identified by its service Identifier, this means that each TEK and KEK shall be associated with one service_Id, and latter key updating for each service shall also be done based on these service_Ids.

Currently within SA2 [1], "Temporary Mobile Group Identity (TMGI) is used for group notification purpose. The BM-SC will allocate a TMGI per service that is unique within HPLMN. For Multicast Service the TMGI will be transmitted to UE via service activation procedure." As there is one one-to-one mapping relationship between the service_Id and the TMGI, in this means, each TEK and KEK shall be associated with one TMGI – one identifier for a group of MBMS users. Latter key updating for one specific service shall be indicated by the TMGI for this service.

Actually this usage scenario is quite similar to the intermediate keys usage scenario used in LKH based re-keying, which shall be illustrated in detail in the following section.

2.2. Key distribution for LKH

For LKH based TEK re-keying[2], “users receiving the same Multicast service within the same area can also be further combined into one to several subgroups to make it possible that the keys can be given to all users within one subgroup at a time in point-to-multipoint mode.” Thus, each user may keep multiple intermediate keys. And users belonging to the same subgroup shall share one common intermediate key (also one kind of KEK) for this subgroup. That is, every intermediate key is associated with one subgroup identifier – one identifier for a subgroup of MBMS users. Latter key updating for users within one specific subgroup shall be indicated by the subgroup identifier for this subgroup.

Comparing the key distribution for multiple service and the key distribution for LKH, it is obvious that if multiple TMGIs can be assigned for one service, and each TMGI is used to identify one specific subgroup, there shall be no significant difference between re-keying for multiple service and re-keying for LKH. Latter re-keying in both cases shall be indicated only by the TMGI.

3. Hierarchical TMGI

The hierarchical composing of TMGI can described in the figure below.

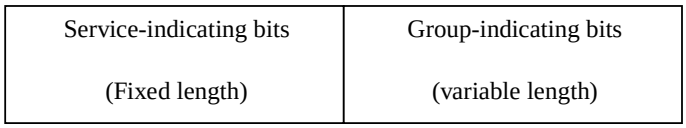

Figure 1. Hierarchical composing of TMGI

TMGI is composed of service-indicating bits and group-indicating bits. The fixed-length service-indicating bits are used to distinguish different MBMS services, and the group-indicating bits are used to distinguish different groups of users for one specific service. Users who join the same service but are assigned into different groups shall share the same service-indicating bits but different group-indicating bits.

Upon activation, one UE shall be assigned into one group and obtains its TMGI. This group assignment operation may be based on this UE’s IMSI for example. This shall be discussed in more detail later in section 4. The initial intermediate group key for this group is distributed to this UE in ptp mode during this activation procedure. The initial TEK can also be distributed to this UE during this activation procedure.

Then for later re-keying, if there’s no UE leaving occur within this group, the updated TEK shall be able to distributed to all UEs within this group indicated by the TMGI for this group and encrypted by this initial intermediate group key. Otherwise, if there’s UE leaving or joining occur within in group, the updated TEK and the updated intermediate key for this group shall be distributed to each of the privileged UEs within this group in ptp mode, which is in the same way as the initial key distribution.

Specially, in order to provide common and simple indication to all groups of users for one service, one pre-defined combining of the “group-indicating” bits, e.g. all “0” , may be used to indicating information for all groups of users for this service.

Actually, depending the number of users for one specific service, it is only up to the operator to decide whether or how many TMGIs should be used for one specific service indeed. If there are quite a lot of users for one specific service, the operator may separate them into more groups with more group-indicating bits. If the length of the group-indicating bits is 0, i.e, no group-indicating bits, this kind of LKH based re-keying becomes the ptp based re-keying exactly.

Because UE may own the capability to support multiple services coexistence case, this means that this UE also can be updated to support LKH based re-keying with very minimal modification.

4. User grouping mechanism

After one user activates one specific service, the TMGI (i.e. group-indicating bits) assigned to him may be fixed or flexible. Fixed TMGI has the benefit that it doesn’t need to be updated latter. One feasible generation mechanism of the group-indicating bits can be based on IMSI mod operation. For example, if operator decides to assign all users for one service into 12 groups, then the group-id for one specific user is group-id = IMSI mod 12. Flexible TMGI means that the operator may change the TMGI assigned to one user latter. For example, operator may want to assign the users into more groups and use longer TMGI when more users activates the service. Anyway, this user grouping mechanism is quite one implementation issue for the operator.

5. Conclusion

From the analysis above, we can see that UEs may own the capability to support multiple services coexistence case themselves and can be updated to support LKH based re-keying with very minimal modification by means of the proposed hierarchical TMGI. And, the proposed hierarchical TMGI composing provides the option for the operator to decide whether or how many groups of users shall be assigned for one specific service. As, it can be easily implemented to support LKH based re-keying according to operator’s decision, this hierarchical TMGI is proposed to be adopted by SA3 for MBMS key distribution and reflected in current TS33.246.

6. Reference

[1] 3GPP TS 23.246 V.1.2.1 (2003-08) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description (Release 6)

[2] S3-030054, “Text proposal for MBMS re-keying based on LKH principles” from Samsung in SA3#27