3GPP TSG SA3 Ad-hoc Meeting **S3z030016**
3 - 4 September 2003
Antwerp, Belgium

Agenda item: 6.3

Source: Samsung

Title: MBMS service activation and Initial TEK distribution

Document for: Discussion and Decision

1. Introduction

MBMS users may activate or deactivate one service long before one session of the service starts. And the initial MBMS traffic encryption key (TEK) for this service should also be distributed from the network to each privileged UE before session starts. This contribution makes some analysis about the MBMS service activation/deactivation procedure and the initial TEK distribution. Then it proposes that the initial TEK shall be distributed from the network to one UE among its joining procedure, and the UE joining operation can only be accepted after the "Joining Availability Time", which is given by the network in the service announcement.

2. Discussion

As defined in current MBMS TS23.246[1],MBMS Service Provision Phases include service announcement, Joining(i.e. MBMS multicast activation by the user), Session Start and so on. And it is a normal case that service announcement for a certain MBMS service may be carried out for as long as a few weeks before session starts (i.e. actual traffic data transmission). From the service provider's point of view, this is especially welcomed for some special MBMS service (e.g. the first match of world cup); since more users may be able to know the existence of this service if service announcement takes a long time before session starts. On the other hand, UE joining(leaving) operation can be carried out by one user at any time at his will after he can receive the service announcement and has enough(no) interest in this service. That is, UE joining(leaving) can occur maybe long before the session start.

As we know, MBMS TEK distribution may include the Initial TEK distribution phase and the latter TEK re-keying. The latter TEK re-keying may require previous some kind of keys which are securely transmitted during the initial TEK distribution phase. The initial TEK distribution shall be done in point-to-point mode. The MBMS multicast service activation procedure registers the user in the network to enable the reception of data from a specific MBMS multicast service. Since this activation signalling procedure is carried out in ptp mode between the UE and the network, usually, the initial MBMS TEK shall be distributed to this UE just after it passes the mutual authentication and authorization during this activation procedure.

As MBMS multicast service activation can occur long before the session start, when the TEK shall be used, this means that the user can obtain the initial MBMS TEK long before these keys are actually used. This shall increase the possibility of these keys to be cracked or leaked out.

On the other hand, MBMS multicast service deactivation can also occur long before the session start depending on the user's own will, and this may bring some problem to the charging issue. If flat rate charging is adopted for this service and this user is charged just from the time when it activates the service, obviously it is not welcomed by this user as he selects to deactivate this service actually long before the service begins. But if charging is done from the time when the MBMS data is coming and the service begins, those users who have deactivated this service before may be able to receive the data free of charging at least for some time, because they have already received the initial TEK for content deciphering.

Actually these problems may by solved by the following methods: 1) setting a Joining availability time; or 2) to define one separate initial TEK distribution procedure; or 3) the combination of the above 2 approaches . These methods shall be discussed in the following sections.

3. Solutions

3.1 Joining availability time

Apart from session start time, we can add one additional parameter in service announcement - "Joining Availability Time", which denotes the starting time after which MBMS users can join an MBMS service and then charging shall be done surely for one user if he activates this service. That is, service announcement occurs before Joining Availability and session start, and Joining availability occurs before session start. Thus, one user can clearly know to join his interested service after this time and charging shall be done once he activates this service. The initial MBMS TEK shall be given to this UE in this activation procedure. UE activation requests before Joining Availability shall be refused by the network with some response to this UE indicating again the Joining availability time.

Period between join availability and session start can be sophisticatedly designed by operators based on statistics or experiences to be just long enough to allow as many as possible users to join the service before session starts.

By this method, no additional initial TEK distribution procedure is needed. This shall reduce some signalling load to some extend. However, this "Joining Availability Time" could give a bad user feel as one user could join the service and another next to him might not just a few seconds ago.

3.2 Separate initial TEK distribution procedure

In this case, the user can join the service at any time after he receives the service announcement. But the initial MBMS TEK shall not be given to this UE during the service activation procedure. The network shall carry out one additional initial TEK distribution procedure separately in ptp mode for each authorized UE some time just before the session starts. Charging to these users shall be carried out once they obtain the initial TEK, no matter whether they deactivate the service after that or not.

This period between the initial TEK distribution and session start can also be sophisticatedly designed by operators based on statistics or experiences to be just long enough to allow the initial TEK distribution can be successfully carried out to each privileged UE before session starts.

In this case, users can join the service at any time after the service announcement, and are treated equally. But additional initial TEK distribution procedure is needed latter, which shall bring some extra signalling load to the system.

3.3 Hybrid Initial TEK distribution

In this case, one predefined Joining Availability Time is also used by the system. If one user activates the service after this time, the initial MBMS TEK shall be given to this UE in this activation procedure. And, charging shall done surely for this user accordingly.

If one user activated the service before the "Joining Availability Time", the initial MBMS TEK shall not be given to this UE during the service activation procedure. Certainly, no charging shall be done for this user at this time. After the Joining Availability Time, the network shall carry out one additional initial TEK distribution procedure separately in ptp mode for this UE. And charging shall be done for this UE from this time.

In this case, users can also join the service at any time after the service announcement, and charging shall be done to these users equally from the "Joining Availability Time". But different UEs may obtain the initial TEK from different procedures. And additional initial TEK distribution procedure may be needed for some privileged UEs, which shall bring some extra signalling load to the system.

4. Conclusion

As a result of the above analysis, we recommendate SA3 to adopt method 1 "Joining availability time" for the initial TEK distribution and reflect this into current TS and agree on the following text proposal:

5.2 Key management and distribution

Like any service, the keys that are used to protect the transmitted data in a Multicast service should be regularly changed to ensure that they are fresh. This is even more necessary in a Multicast service, as the need to changed keys can also be driven by a new user joining the service (to stop them being able to decrypt data sent before they joined the service) or a user leaving the service (to stop them being able to decrypt traffic sent after they left the service).

The network shall indicate the "Joining Availability Time" in the service announcement for one service when distributing the service related information to users. This "Joining Availability Time" denotes the starting time after which MBMS users can join an MBMS service. The initial traffic encryption key shall be distributed from the network to this UE among the joining procedure and charging shall also be accounted for this user if flat rate charging mode is adopted for this service. A join request before "Joining Availability Time" may not be accepted by network.

Editor’s note: It needs to be decided if there is to be a minimum amount of traffic that is to be protected with one key, as this puts a lower limit on the frequency of key changes, e.g. one continuous transmission of data. It could also be possible for several of these minimum amounts to be transmitted with changing the key. It is ffs what this minimum amount should be and whether several of these minimum amounts can be transmitted without changing the key.

Editor’s note: If all users need to request a key update simultaneously then there may need to be some method of ensuring that all the users do not request a key update at the same time. This mechanism is ffs.

Editor’s note: The keys can be distributed to each user receiving the same MBMS service in point-to-point mode when the number of the users is relatively small. And the 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.