Agenda item:	MBMS
Source:	Samsung
Title:	Bearer level joining and application level joining for MBMS security
Document for:	Discussion and decision

1. Introduction

During last SA3#32 meeting, there was some discussion about the MBMS bearer level joining and the application level joining. This contribution tried to make a separation between this 2 levels of joining from MBMS security point of view and proposed to agree on this understanding within SA3.

2. Bearer level joining

Currently within SA2, joining (i.e. MBMS multicast activation by the user) procedure is defined as"the process by

which a subscriber joins (becomes a member of) a multicast group, i.e. the user indicates to the network that he/she is willing to receive Multicast mode data of a specific service." Actually, from MBMS security point of view, this kind of joining can be regarded as the bearer level joining, which means the UE can be informed about the transmission bearer information and receive the traffic data once it finished this bearer level joining. This bearer level joining any occur at any time after the service announcement at the UE's own will. During this bearer level joining, the MUK (MBMS user key) can be generated and shared by the BMSC and the UE.

From the operator's viewpoint, the operator may always prefer one point-to-multipoint transmission bearer for one service with the consideration of saving resources, because once it is established, the same point-to-multipoint transmission bearer can be used no matter exactly how many more UEs joined the service. Thus, it is good if as many UEs as possible can perform this bearer level joining, maybe without any actual limitation such as charging, security.

It may seems simple if the user can implicitly carry out the bearer level joining when he subscribes to one service. However, from the user's point of view, he must need to explicitly perform the bearer level joining separately, because receiving the MBMS transmission bearer may consume some UE resources (e.g. power, storage), and this user must explicitly express his will for consuming these UE resources.

3. Application level joining

For security reasons, the MBMS MSK can be regularly during the service to ensure that it is fresh. However, the data transmission bearer may keep the same when this MSK is changed. During discussions hold in previous SA3 meetings, it was pointed out that the MBMS flat rate charging can be based on the usage of the MSK (MBMS service key). That

is, if one UE requests for one MSK, this UE shall be charged for the lifetime of this MSK. In this means, this kind of MSK request may be regarded as application level joining procedure from security point of view. During this application level joining procedure, the MSK is generated and shared by the BMSC and UE. This kind of flat rate charging can be adopted for MBMS streaming service as well as download service.

From operator's view point, without the consideration of security, it shall save the resource if the UE can obtain the initial MSK during its bearer level joining procedure without setting up additional ptp bearer for MSK distribution. That is, it is beneficial to join the first application level joining procedure together with the bearer level joining procedure. And it may be even more simple if there is only one MSK for one service, which means the application level joining an be implicitly the same with the bearer level joining. One UE may obtain this only MSK once it carries out the bearer level joining.

From user's point of view, without the consideration of charging, it also may be simple if there is only one MSK for one service, which means the application level joining can be implicitly the same with the bearer level joining. One UE may obtain this only MSK once it carries out the bearer level joining. However, note that one UE may temporarily move out of the service area and back after some period, or the user may not be interested in the service for some period, in this case, multiple MSK for one service and associated MSK request (i.e. application level joining procedures) from the UE can give the user a fare charging.

4. Conclusion

It is proposed to agree on the above understanding about bearer level joining and security level joining from security point of view, and LS to other related WGs about SA3's understanding if it is needed .