3GPP TSG SA WG3 Security — S3#30 **S3-030521**
06 - 10 October 2003
Povoa de Varzim, Portugal

Agenda item:	**MBMS**
Title:	**Simple PTP method in detail**
Source:	**Huawei Technologies Co., Ltd**
Document for:	**Discussion and Decision**

1 Introduction

This paper analyses the simple PTP re-keying method more in detail and discusses whether the key change indication should be done in-band or out-of-band. If simple PTP is accepted for initial MBMS service, we propose adding an example of simple PTP re-keying to the TS.

2 Discussion

2.1 Simple PTP model

The simple PTP model doesn't require many changes to the UE and network. The most important thing is implementing a policy so that users will request the TEK at different times.The following is an example of re-keying with Simple PTP.

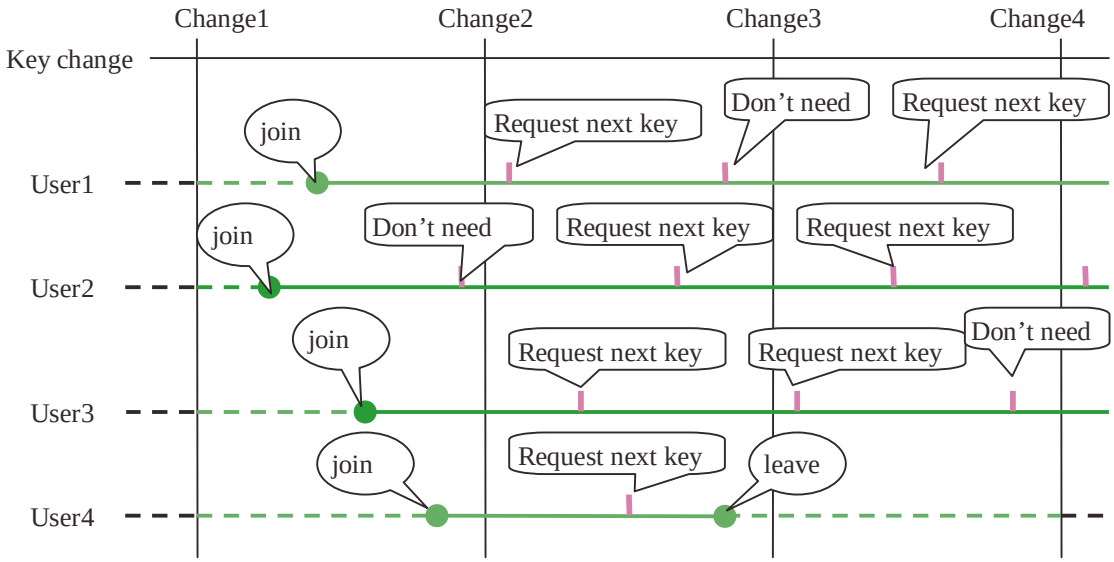

Figure 1 :Example of Simple re-key

2.1.1 User keys

Users have two keys, the current key and the next key. The current key is used to decrypt current traffic data; the next key will become the current key after some period of time.

2.1.2 Key change

The server can control key changing on a regular time interval, by issuing a switching command or by sending the new key ID with the traffic data.

During the ad hoc meeting, it was discussed that the switching command is an out-of-band command, which may cause the user to miss some data when the switching command is not received properly. In these cases, the user must request the new key and avoiding any subsequent delay is difficult.

On the other hand, the key change may be done in-band, i.e. the traffic data contains the key ID. This method doesn’t lead to delays because if the user doesn’t have the key, he can request the new key and save the encrypted data. Then once he obtains the new key, he can decrypt the saved data. However, a related problem should be considerd. If an eavesdroper saves all of the encrypted data and he gains access to the key in the future, then he also can decrypt the traffic data. This problem occurs in both 3GPP2 PTP and combined PTP methods.

So it should be decided which is more important, i.e. security and key delay. This decision will influence which method is preferred, in-band or out-of-band key change indication.

2.1.3 Request next key

When a user joins the service, the server should respond to the initial request and assign a time interval. The user starts his time interval when he receives it and requests the next key based on the time interval. Even if the assigned time intervals are the same, users join at different times, so all users will not request next key simultaneously.

Users' time intervals are shorter than the key changing interval to ensure that the user can obtain next key before key changing. If the user determines that he already has the next key, he should skip the current request.

2.1.4 Join/leave

When a user joins the service, the server should send some keys to the user. In Figure 1, if user1 chooses to receive data as soon as he joins the service, the server should send "current key, next key" to user, and the user should be charged from the "change1" point. If the user wants to avoid additional charging, he may select to receive the data later. Then the server should send "next key" to the user, and the user should be charged from "change2" point.

Charges work similarly if the user wants to leave the service. E.g. In Figure1, if user4 requests the next key between "change2" point and "change3" point and leaves, he should be charged to "change4" point whether or not he receives any data after leaving.

2.2 About simple PTP

The obvious merit of simple PTP is simple and easy to implement. However, if there are many users, the key changing interval may be made relatively long in order to require less resources at the expense of overall security.

From the view of initial service, MBMS service likely will consist of simple and relative short session service. Since most of the time resources will be idle, the frequent re-keying of simple PTP won't impact traffic data resource.

3 Conclusion

1. For the initial MBMS services, if the simple PTP is accepted, we propose adding Figure1 to the TS with the following text and editor note:

1 Users have two keys, the current key and the next key. The current key is used to decrypt current traffic data; the next key will become the current key after some period of time

2 The BM-SC may change the traffic encryption key at some regular time interval

3 Users should complete the next key request according to policy before the key change

4 Users can skip unnecessary key requests (e.g. they already have the next key)

Editor note: Simple PTP re-keying is applicable for initial and simple MBMS services

2. Define key change indication as either in-band or out-of-band.