3GPP TSG SA WG3 Security — adhoc **S3z030006**
3 - 4 Sept 2003
Antwerp, Belgium

Agenda item: MBMS 6.3

Source: Huawei Technologies Co., Ltd.

Title: Using CK with switching command

Document for: Discussion and Decision

1 Introduction

At the SA3#29 San Francisco meeting, it was agreed that there is a problem on how to indicate when to switch to a new Ciphering key. This contribution provides a method to inform all users to switch to the new Ciphering key and suggests some mechanisms to ensure that users can always get the new ciphering key.

2 Discussion

In TD S3-030349 MBMS re-keying: PTP with periodic re-keying, a method for indicating a new cipher key was described. That is, the server can send a switching command to inform all users to switch to the new ciphering key. The switching command may be a broadcast message. After a user receives the switching command, he can start using the new ciphering key. The broadcast switching command can be repeated several times to reduce the chance that users don't receive it. The switching command is critical because if users don't receive it, they will not receive subsequence traffic data normally. The following section analyses several possible cases and their corresponding solutions.

2.1 Analyze

- **Case1: User powers off**

  If the user powers off, there is no problem. When user powers on, authentication and authorization will be executed, then the BMSC relevant information will be sent to user, and the user will know which key should be used.

- **Case2: User is out of service**

  If a user is out of service and then returns soon, he may miss the first broadcast switching command and catch the repeated broadcast switching command. If a user is out of service for a long time, he maybe miss the first and the repeated broadcast switching commands, then he can't receive the traffic data normally once he returns. To avoid this failure, the user may

inquire about whether he missed some broadcast switching commands or inquire about the current ciphering key ID. If a user determines he is out of service, when he returns he can send such an inquiry to the server.

Some inquiries may be unnecessary, so there can be some limiting conditions. If a user returns from out of service and meets the limiting conditions, he can send an inquiry to the server. The limiting conditions may include a minimum time length, i.e. if the user is out of service for less than a certain time length, he can't send an inquiry to server. E.g. the limited time length may be a sum of the number of repeated switching commands times the repeated interval.

The inquiry may not only apply for inquiring about the current key ID, but also may apply for inquiring about other missed broadcast signal messages.

- **Case3: The cause is unclear**

  It may be possible that a user doesn't receive the first and all subsequence repeated switching commands, and neither of the above two cases apply. However, this case should occur seldom. If it does occur, we may have to treat it as case1, i.e. power off and then power on. Perhaps, there are other methods that can handle these unusual cases. It is FFS.

3 Conclusion

Proposal 1: For the user to know when he should use the new ciphering key, we propose that the server broadcasts a switching command to inform all users to switch to the new ciphering key.

Proposal 2: If user is out of service when one or more switching commands are issued, when he returns, he can send an inquiry to the server according to some limiting conditions such as time.