3GPP TSG SA WG3 Security — S3#33 **S3-040240**
10 - 14 May 2004
Beijing, China

Agenda item: MBMS

Title: MSK update rules

Source: Huawei

Document for: Discussion and Decision

1 Introduction

In the last SA3 meeting, it was agreed: if an optional message “new key available” is send to all UEs, then the BM-SC should provide the rules to the UE for subsequent request for the new MSK when a UE joins a multicast service, to avoid simultaneous requesting from all the UEs. In the editor’s note, there provide some possible methods for example. This document analyze those methods and suggest add an example to the protocol text.

2 Discussion

The editor’s note shows“*A possible method for achieving the above is for the BM-SC to allocates different “request delay time” to different UEs; such that when the UEs receive the new key available message, they shall send the request key message after the delay requested by the BM-SC. Alternatively it is possible to use the key lifetime methods suggested in S3-040059.*”

delay time method:

The BM-SC allocate different delay time to different UEs, then the UE just respond to the “new key available” message after the requested delay time passed, thus the all UEs request new key at the same time can be avoided.

The delay time may be same to a subgroup of UEs or different to each UE. If the delay time is same to a subgroup , the subgroup should be in a limit number of UEs to avoid the network congestion. The ideal case is that the delay values are different for each UE. To achieve this , the BM-SC can, for example, spread the delay value randomly over a acceptable maximal delay interval. BM-SC can provide the setting rules and change these flexible, e.g. BM-SC can change the rules at any point to point communication with UE.

The advantage of delay time method: Network control and complete the main work , UE keep simple without the computing resource and mechanisms for the congestion avoiding..

lifetime method:

The suggested method in S3-040059 is “*the key lifetime shall be communicated to the UE with the associated key. The UEs can for example spread the key requests randomly over the lifetime of the key*”

This method looks like also reasonable, but there are some problems should be considered:

1The UE requests the new key randomly over the lifetime, but if the new key is unavailable in BM-SC at this time, the UE should have the capability to request new key again and avoid the network congestion.

2 If the UE request the new key after receiving the new key available message, the UE need to determine the relation between key available message and the lifetime, and compute a random time for the request..

3 The UE should have the capability to generate the random requesting time, e.g. a proper algorithm is necessary..

4. Since the random time is computed by different UEs, it can not reliably avoid the congestion. Advanced algorithm may help mitigate the problem, but need more complexity and more computing in the UE.

3 Conclusion

The lifetime method introduces more requirements in the UE and is less reliable than delay time method. So we suggest include only the simple delay time method as example in the protocol text.

4 Proposal

1 delete the editor's note "*A possible method for achieving the above is for the BM-SC to allocates different "request delay time" to different UEs; such that when the UEs receive the new key available message, they shall send the request key message after the delay requested by the BM-SC. Alternatively it is possible to use the key lifetime methods suggested in S3-040059.*" in section 6.2

2 delete the 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*" in section 5.2

3 include the delay time method as an example in section 6.2

********************************Begin of changes***************************

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 ensures that only legitimate users can get access to the data in the MBMS service. In particular frequent re-keying acts as a deterrent for an attacker to pass the MBMS keys to others users to allow those other users to access the data in an MBMS service.

The BM-SC is responsible for the generation and distribution of the MBMS keys to the UE. A UE has the ability to request a key when it does not have the relevant key to decrypt the data. This request may also be initiated by a message from the BM-SC to indicate that a new key is available.

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.

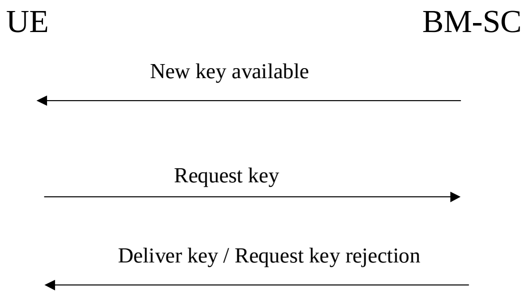
**************************End of changes***

********************************Begin of changes**************************

6.2 Key update procedure

Once a UE has joined a multicast service, the UE should try to get the MSK that will be used to 'protect' the data transmitted as part of this multicast service. If the UE fails to get hold of the MSK or receives confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still-valid, older MSK, the UE shall leave the MBMS user service. The UE tries to get the MSK using the second message in the below flow.

The BM-SC controls when the MSKs used in a multicast service are to be changed. The below flow describes how MSK changes are performed.



The first message is sent out by the BM-SC to indicate that new MSKs are available. It is an optional message in the flow. If it is sent to all UEs, then the BM-SC should provide the rules to the UE for subsequent request for the new

MSK when a UE joins a multicast service, to avoid simultaneous requesting from all the UEs. For example, the BM-SC allocates different “request delay time” to different UEs; when the UEs receive the new key available message, they shall send the request key message after the delay time requested by the BM-SC;

~~Editor’s note: A possible method for achieving the above is for the BM-SC to allocates different “request delay time” to different UEs; such that when the UEs receive the new key available message, they shall send the request key message after the delay requested by the BM-SC. Alternatively it is possible to use the key lifetime methods suggested in S3-040059.~~

The second message is used to request an MSK. This is sent by the UE when it either receives the first message in the flow and does not have the new MSK, or has just joined a multicasts service and does not have an MSK for that service or has received some protected content and does not have the MSK that was used to protect the content. If the UE fails to get hold of the updated MSK or receive confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still valid older MSK, the UE shall leave the MBMS service.

After receiving the second message the BM-SC should send out the appropriate MSK to the UE protected by the relevant means, or reject the UE’s key request with an indication of the cause. Upon successfully receiving the new MSK, the UE should store this key for later use.

Editor’s note: If OTA is used to carry MSKs to the UICC, the following recommendations shall be followed:

- OTA should not use DES in CBC mode,
- The keys used for the ptp transporting of MSK to the UICC shall not be shared among subscribers,
- OTA shall not rely on the same keys for transporting MBMS data and other application data towards the UICC.

Editor’s note: MIKEY is being considered as the method for carrying keys. Possible optimisations were proposed at the ad-hoc in Antwerp (S3z030010). One identified issue was the possible need to terminate MIKEY in the UICC and/or terminal in the combined method. The use of MIKEY relates to the PTP delivery of a key

**************************End of changes***