3GPP TSG SA WG3 Security — S3#32 **S3-040127**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda item: 6.20 MBMS

Title: high level key update

Source: Huawei Technologies Co., Ltd.

Document for: Discussion and Decision

1 Introduction

The BM-SC controls when the high level keys used in a multicast service are to be changed, and BM-SC will send a "new key available" message to the UE, if this message is send to all UEs, then all UEs may request the new key at the same time. This contribution suggests a UE requests a new key base on some rules in order to avoid a high number of simultaneous requests.

2 Discussion

At the last SA3 meeting ,it was clarified that there are two keys for each multicast services. When the high level keys used in a multicast service are to be changed, the BM-SC send a "new key available" message to UE. If all UEs receive the "new key available" message and determine that they don't have the new key, the UEs will request the new key from BM-SC. If all UEs request the new key simultaneously, the burden of network is huge. The follow suggestion can solve this problem .

When the UE join the multicast service , the BM-SC provides some rules to the UE such that subsequent requests for a new key are made according to the rules.

For example~~E.g~~. the BM-SC assign a time interval to the UE, and at the end of each time interval, the UE checks whether it needs to request the new key. If the UE receives a "new key available" message and the time reaches the end of the time interval, the UE requests the new key. The time interval may be same to each UE but because the time that each UE joins is different, the start point of the interval is different , so the simultaneous requests are avoided. To avoid the complexity in UE, the BM-SC can allocate different delay value to different UE, then the UE just respond to the "new key available" message after the requested delay time passed.

If it leaves for the UE to determine some ways to avoid the simultaneous Key update, it will not be reliable and add lots of complexity to the UE, for example install a randomizer for each UE, it will consume storage and computing resource,

3 Conclusion and proposal:

The basic rule for avoiding the congestion of network in this case is that the BM-SC determine the response rule of the UEs. When a UE joins the multicast service, the BM-SC gives ~~some~~ the rules to UE. The UEs shall request~~s~~ the new high level key base on those rules to avoid network congestion~~ when it needs the new high level key~~.

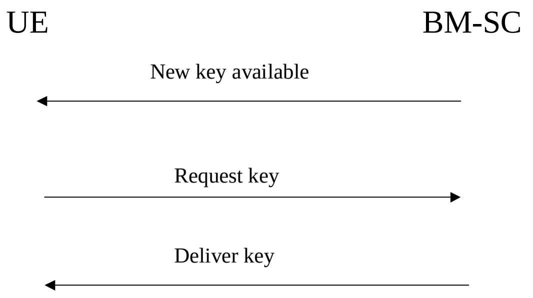
Include the following changes in the TS.

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

6.2 Key update procedure

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

The BM-SC controls when the high level keys used in a multicast service are to be changed. The below flow describes how the high-level key changes are performed.



The first message is sent out by the BM-SC to indicate that new keys are available. It is an optional message in the flow. If it is sent to all UEs~~, then it needs to be ensured that all the UEs do not request the new key simultaneously.~~, then the BM-SC should provide the rules to the UE for subsequent request for the new key 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 requested by the BM-SC;

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

After receiving the second message the BM-SC should send out the appropriate key to the UE protected by the relevant means. Upon successfully receiving the new key, the UE should store this key for later use.

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**

CR-Form-v7

CHANGE REQUEST

⌘	**TS 33.246**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**V 1.0.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network □

Title:	⌘	High level key update		
Source:	⌘	Huawei		
Work item code:	⌘	MBMS	***Date:*** ⌘	09-02-2004
Category:	⌘	**C**	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The section 6.2 key update procedure of TS 33.246-: If BM-SC send "New key available" message to all UEs, and the UE determine the key request message is necessary, the UEs will request the new high level key simultaneously. In this case, it is necessary to define the principle and method to ensure that all the users do not request a key update at the same time.
Summary of change:	⌘	BM-SC should provide the rules to UE for subsequent request for the new key when a UE joins a multicast service, to avoid simultaneous requesting from all the UEs.
Consequences if not approved:	⌘	Network congestion when users request new key simultaneously.

Clauses affected:	⌘	6.2				
		Y	**N**			
Other specs Affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

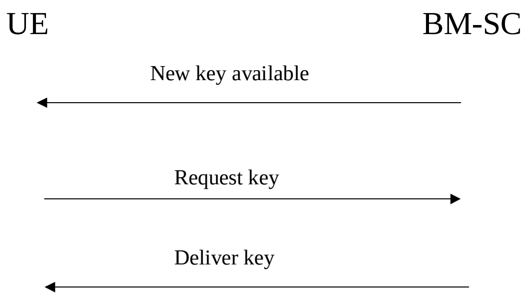
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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

6.2 Key update procedure

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

The BM-SC controls when the high level keys used in a multicast service are to be changed. The below flow describes how the high-level key changes are performed.



The first message is sent out by the BM-SC to indicate that new keys are available. It is an optional message in the flow. If it is sent to all UEs~~, then it needs to be ensured that all the UEs do not request the new key simultaneously.~~, then the BM-SC should provide the rules to the UE for subsequent request for the new key 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 requested by the BM-SC;

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

After receiving the second message the BM-SC should send out the appropriate key to the UE protected by the relevant means. Upon successfully receiving the new key, the UE should store this key for later use.

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**