3GPP TSG SA WG3 Security — S3#31 **S3-030709**
18 - 21 November 2003
Munich, Germany

Agenda item:	6.20
Source:	Samsung Electronics
Title:	Compositive MBMS Key Distribution
Document for:	Discussion and Decision

1. Introduction

There exist several discussion papers during previous meetings [1][2], comparing the 3 different re-keying methods: simple point-to-point model [3], BAK method [4] and the combined re-keying method [5]. It should be noted that the network cannot find out which UE leaks out the keys in deed for all these 3 method. A compositive MBMS key distribution method is then presented, which may help the network to find out the peddler, while trying to combine good aspects of all these methods at the same time to avoid the long pending on the MBMS key distribution method selection.

2. Problems

2.1 operator detection of the keys leakage

It was clarified that all the 3 MBMS key distribution methods -- simple point-to-point method, BAK scheme and the combined methods -- can fulfil general security requirements (all keys are uniquely identifiable, regular change of keys, re-keying etc.). This document shall not make any further analysis about to what extent each method can fulfil these requirements. During previous meeting, several discussion papers have been presented comparing these 3 methods[1][2]. However, it should be noted that one common question for all these 3 methods is that the network cannot find out which UE leaks out the keys in deed. For the simple point-to-point method, if one illegal UE leaks out the common TEK, other UEs may eavesdrop the content free of charging using this common TEK, until the next TEK is widely distributed to all UEs and used instead. As for the BAK scheme and the combined method, if BAK is leaked out, other UEs shall be able to obtain the current TEK encrypted by or generated from this BAK, and thus eavesdrop the content free of charging until the next BAK is widely distributed to all UEs and used instead.

On the other hand, if only the TEKs(SKs) are leaked out, for the BAK scheme, other UEs can be able to eavesdrop the content free of charging, if they can know the correct key mapping relationship between the SK and SK_RAND, which shall be discussed later in section 2.2. As for the combined solution, it is the same problem if the TEKs are leaked out, and the correct key mapping relationship between TEK and TEK_Id is leaked out as well.

While at the same time, for all these methods, it is quite difficult for the operator to find out at last which illegal UE leaks out these keys, because these keys (TEK and BAK) are the same for every joined UE.

2.2 UE collection of the key mapping relationship

On the other hand, even if the keys are kept confidently within the UICC, it should be noted that the UICC-ME interface for TEK distribution or even the ME itself is not believed to be secure enough. Thus, for BAK scheme, the common SK_RAND information is broadcasted to all UEs in-band, in order to lead to the same SK transmitted from the UICC to ME for each UE. In this case, any malicious one of these UEs can collect this mapping relationship between the common SK_RAND information and the actual SK transmitted from the UICC to ME and leak out it to the internet. As for the combined solution, the common TEK identification information is broadcasted to all UEs in-band, in order to lead to the same TEK transmitted from the UICC to ME for each UE, or used within each ME. In this case, any malicious one of these UEs can collect this mapping relationship between the common TEK identification information and the actual TEK transmitted/used and leak out it to the internet. Again, in both cases, it is quite difficult for the network operator to find out at last which illegal UE leaks out this mapping relationship, because it is the also same for every joined UE.

It should be also noted that for each of these 3 methods, BMSC shall assign one unique KEK to each UE for the protection of TEK/BAK transmission.

3. Compositive method

This combined method is designed to combine fast re-keying of BAK scheme and combined solution, applicability to pre-Rel-6 UICCs of combined solution, low cost of introduction of simple point-to-point method, and to increase security level by trying to solve the problems listed above.

3.1 solution 1

It is indicated that multiple different and uniquely identifiable BAKs shall be used for the MBMS service[6]. One of these keys shall be selected at the same time. And this BAK selection/identifier information shall be given by the BMSC to each joined UE. Thus we have the following solution:

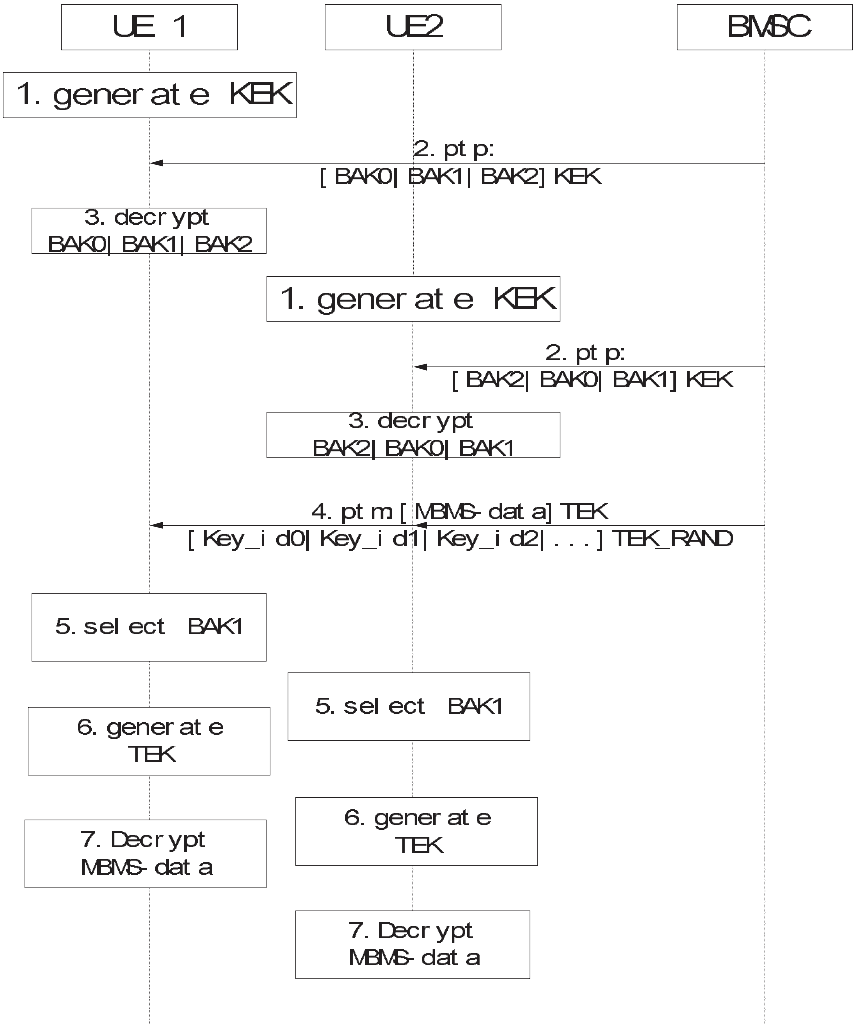
These multiple BAKs shall be transmitted to different UE in different order, based on each UE's identifier assigned by the BMSC, e.g. KEK; this mapping relationship between the transfer order and the UE identifier is kept confidential within the BMSC and unknown by the UEs;

One of these BAKs shall be selected to generate TEK at the same time. And the BAK selection related information is different for different UEs and shall be combined together to be broadcast by the BMSC to each joined UE; the TEK_RAND information shall be broadcast by the BMSC to each joined UE as well;

Based on its own identifier (i.e. KEK in the first step), each joined UE shall find its own corresponding BAK selection related information to obtain which BAK key in its own BAKs list received should be selected;

UE uses the BAK and the broadcasted TEK_RAND information to generate the finial TEK for content data decryption.

The Figure 1 shows this solution 1. It should be noted that for all these 3 solutions, it makes no difference with the case of whether one old UICC or new UICC is used, i.e. it makes no difference whether the BAKs list is kept on the UICC or ME. And it also does not specify how these keys shall be transmitted from the BMSC to the each UE (UICC or UE) in point-to-point mode via OTA or whatever means. This specific method used is not important for the present subject.



1. The UE(UICC or ME) generates a KEK
2. The UE receives an encrypted BAKs list
3. The UE decrypts the BAKs list using its KEK
4. The UE receives encrypted MBMS data, the combined BAK key identification information, and the necessary TEK identification information in the clear text

5. Based on its own identifier, the UE finds out its own corresponding BAK key identification information and select the correct BAK from its own BAKs list

6. UE uses the BAK and the TEK_RAND to generate the TEK

7. The UE decrypts MBMS data using the TEK

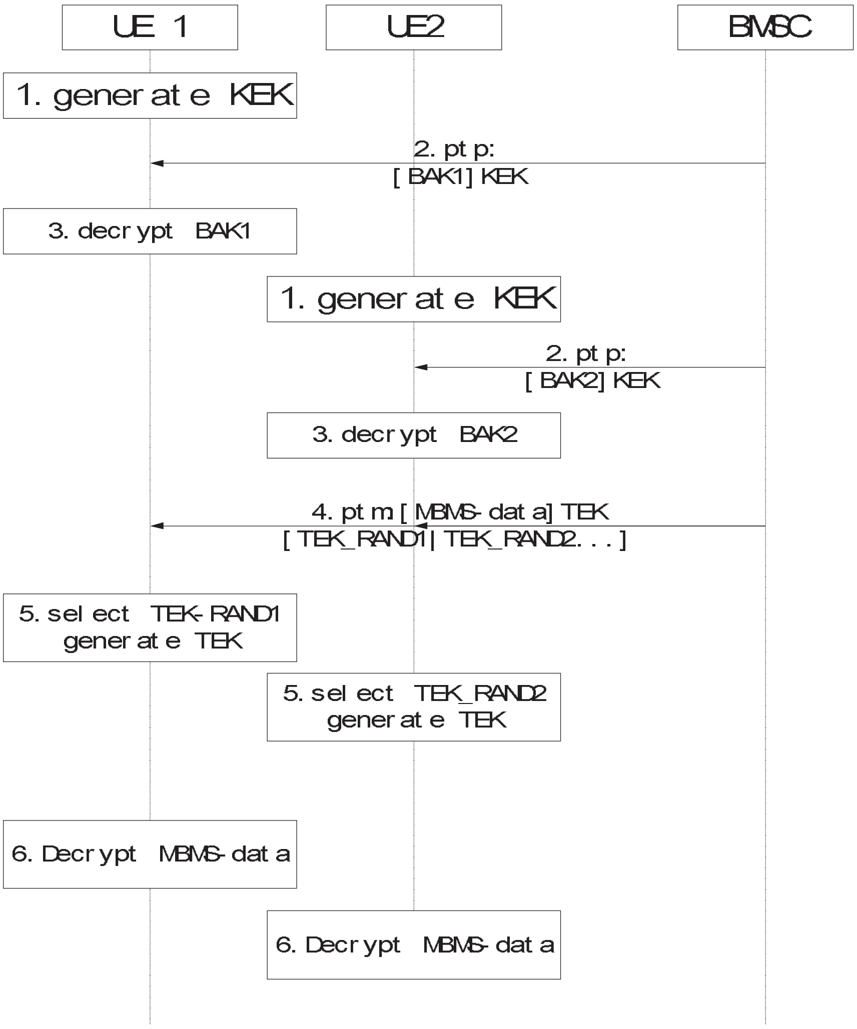
3.2 solution 2

In solution 2, different BAKs shall be transmitted to different UE, based on each UE's identifier assigned by the BMSC, e.g. KEK; the relationship between the BAK and the UE's identifier is kept confidential within the BMSC and unknown by the UEs;

One TEK shall be used for content data protection at the same time. And the TEK_RAND information used to generate this TEK is different for each different BAK; these different TEK_RAND information is combined together to be broadcast by the BMSC to each joined UE;

Based on its own identifier (i.e. KEK in the first step), each joined UE shall find its own corresponding TEK_RAND information and use this TEK_RAND and its own BAK to generate the finial TEK for content data decryption.

The Figure 2 shows this solution 2.



1. The UE(UICC or ME) generates a KEK

2. The UE receives an encrypted BAK

3. The UE decrypts the BAK using its KEK

4. The UE receives encrypted MBMS data, the combined TEK_RAND identification information in the clear text

5. Based on its own identifier, the UE finds out its own corresponding TEK_RAND identification information and use this TEK_RAND and its own BAK to generate the correct TEK

6. The UE decrypts MBMS data using TEK

3.3 solution 3

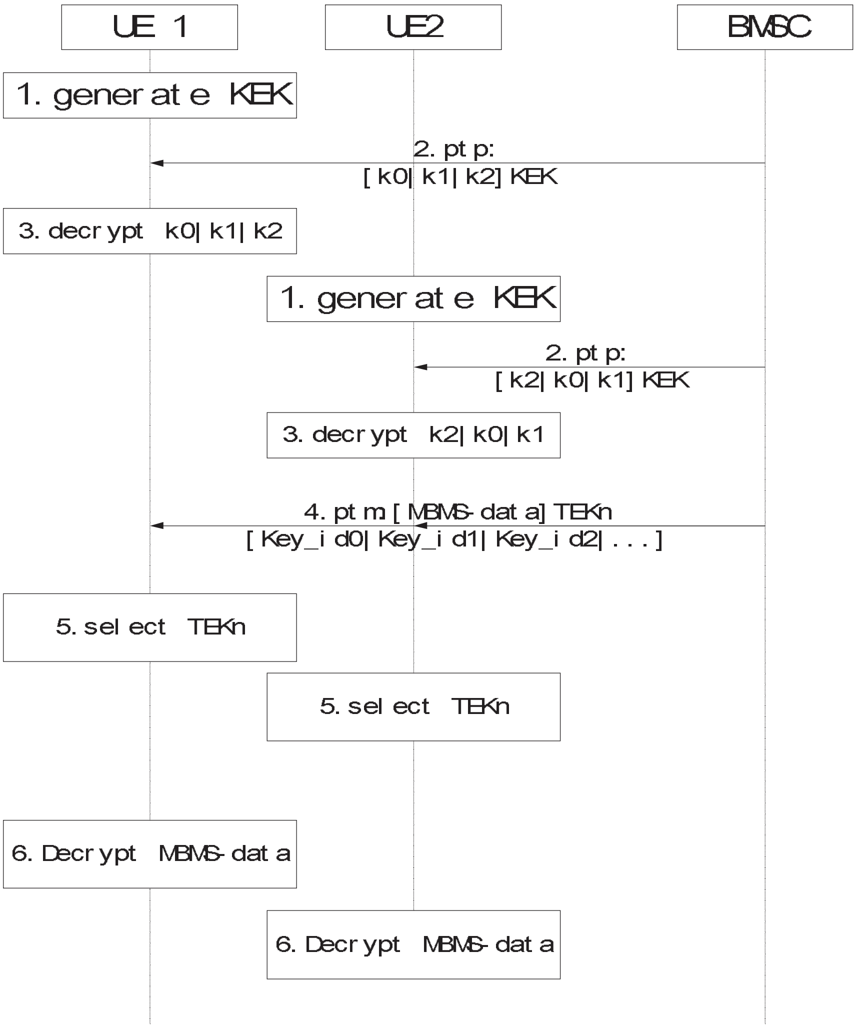
It is indicated that multiple different and uniquely identifiable TEKs shall be used for the MBMS service[6]. One of these keys shall be selected at the same time. And this TEK selection/identifier information shall be given by the BMSC to each joined UE. Thus we have the following solution:

These multiple TEKs shall be transmitted to different UE in different order, based on each UE's identifier assigned by the BMSC, e.g. KEK; this mapping relationship between the transfer order and the UE identifier is kept confidential within the BMSC and unknown by the UEs;

One of these TEKs shall be selected at the same time. And the TEK selection related information is different for different UE and shall be combined together to be broadcast by the BMSC to each joined UE;

Based on its own identifier (i.e. KEK in the first step), each joined UE shall find its own corresponding TEK selection related information to obtain which key in its own TEKs list received should be selected and used for data decryption.

The Figure 3 shows this solution 3.



1. The UE(UICC or ME) generates a KEK

2. The UE receives an encrypted TEKs list

3. The UE decrypts the TEKs list using the KEK

4. The UE receives encrypted MBMS data, necessary key identifier information in the clear text

5. Based on its own identifier, UE finds out its own corresponding key identifier information

6. The UE selects the correct TEK from its own TEKs list

7. The UE decrypts MBMS data using the TEK

3.4 Analysis and comparison

Based on their own decision, operators may select the suitable method for the BMSC to generate one identifier for each joined UE. One possible example for the BMSC to generate the identifier for each UE can be KEK mod operation. For example, for solution 3, in the case where 8 TEKs can be used, there shall be 8!=40320 kinds of different keys transmission order. All joined UEs for this service can be divided into these 40320 groups by KEK mod 40320. Users within the same group can share the same TEKs list. This means that one UE shall 1/40320 chance to select to use the correct TEKs list among all possible TEKs transmission permutations and combinations, even the UE can know which TEKs are used ! In this case, the illegal UE which attempts to leak out the keys has to leak out the TEK list it receives as well as its group identifier, since the broadcasted key selection related information for each group is related to the group identifier. Thus, this can help the network to find out which group of illegal UEs may try to leak out the keys.

Further analysis about these 3 solutions is listed in the following table:

	Solution 1	Solution 2	Solution 3
1.Can the operator be able to find out which UE leaks out these keys, if the UE only leaks out the BAKs(TEKs) received by itself ?	Yes, if there's only one UE in one group. The illegal UE has to leak out the its own BAKs list and its own group identifier information, and it cannot know the mapping relationship between the BAKs list and the group identifier, because this relationship is kept secret within the BMSC.	Yes, if there's only one UE in one group. The illegal UE has to leak out the its own BAK, and it cannot know other UE's BAK, because the BAK is different for different group of UEs and its transmission is encrypted by KEK.	Yes, if there's only one UE in one group. The illegal UE has to leak out the its own TEKs list and its own group identifier information, and it cannot know the mapping relationship between the TEKs list and the group identifier, because this relationship is kept secret within the BMSC.
Conclusion: all these 3 methods are helpful for the operator to find out the illegal UE which only leaks out the keys it receives.			

<table>
<tr><td>2.Can the UE know the BAKs(TEKs) received by UE in another group ?</td><td>Yes.
The BAKs are the same for all UEs, but transmitted in different order for different group of UEs.</td><td>No.
Different group of UEs shall be able to own different BAKs.</td><td>Yes.
The TEKs are the same for all UEs, but transmitted in different order for different group of UEs.</td></tr>
<tr><td>3. If yes for the above question 2, can the UE know BAKs(TEKs) transmission order of another group of UE ?</td><td>No.
BAKs shall be transmitted in different order for different group of UEs. And this order assignment is carried out internally within BMSC.</td><td>X</td><td>No.
TEKs shall be transmitted in different order for different groups of UEs. And this order assignment is also carried out internally within BMSC.</td></tr>
<tr><td colspan="4">Conclusion: all these 3 methods makes it difficult for one UE to know the correct key (keys list) received by another group of UEs.</td></tr>
<tr><td>4. Can the UE collect the key mapping relationship ?</td><td>Yes, if the same TEK is generated and used for several times, which leads to the same combined BAK identification information broadcasted from the BMSC;
No, if one TEK is generated and used for only one time.</td><td>Yes, if the same TEK is generated and used for several times, which leads to the same combined BAK identification information broadcasted from the BMSC;
No, if one TEK is generated and used for only one time.</td><td>Yes, if the same TEK is used for several times, which leads to the same combined TEK identification information broadcasted from the BMSC;
No, if one TEK is used for only one time.</td></tr>
<tr><td>5. If possible for question 4, is it difficult that one TEK shall never be used for again ?</td><td>No. The TEK_RAND can be changed very quickly without sameness.</td><td>No. The TEK_RANDs for each UE can be changed very quickly without sameness.</td><td>Yes. The number of TEKs saved by the UE is limited.</td></tr>
<tr><td colspan="4">Conclusion: The leakage problem of key mapping relationship can be avoided if one TEK is used for at most one time, which can be easily supported by the solution 1 and solution 2.</td></tr>
<tr><td>6. Is the transmission of the keys from the BMSC to UE one big</td><td>Depending on the number of groups, each group of UEs</td><td>Each group of UEs shall need to receive its own BAK for this</td><td>Depending on the number of groups, each group of UEs</td></tr>
</table>

load for the system ?	shall need to receive its own BAKs list.	group.	shall need to receive its own TEKs list.
7. Is the broadcasted overhead(i.e. key identification information) one big load for the system ?	Depending on the number of groups, the overhead consists of information for each group of UEs.	Depending on the number of groups, the overhead consists of information for each group of UEs.	Depending on the number of groups, the overhead consists of information for each group of UEs.
Conclusion: Compared to solution 1 and solution 3, solution 2 means less load for the keys transmission from BMSC to UE. But all these 3 methods need one big overhead for the broadcasted key identification information, which is related to the number of group of UEs.			

From the above analysis, we can see that it is one contradiction between the security and the system load. In case the number of UEs within one group is small, it is more helpful for the operator to find out which UE leaks out the keys indeed; while at the same time, it brings longer overhead and more load to the system accordingly. Thus, the operator has to make a colligated decision about how many groups the joined UEs shall be divided into and how many UEs shall be allocated into one group.

On the other hand, we can see that solution 2 can help to solve the mentioned “operator detection of keys leakage” problem and the “UE collection of the key mapping relationship” problem, while bring less overhead to the system.

4. Conclusion

As a result of the above analysis, we propose SA3 to adopt this compositive method for MBMS key distribution, and especially, to select the proposed solution 2 for MBMS key distribution.

5. Reference

[1] Tdoc S3-030539, Key management considerations for MBMS, Ericsson

[2] Tdoc S3-030580, MBMS – Overhead of the Re-keying, Nokia

[3] Tdoc S3-030368, Introducing SRTP and MIKEY in TS 33.246, Ericsson

[4] Tdoc S3-030360, Levels of Key Hierarchy for MBMS, Qualcomm

[5] Tdoc S3z030020, MBMS – Combined Re-keying Method, Nokia

[6] Tdoc S3-030641, TS33246 MBMS Security Requirements CR, BT