3GPP TSG SA WG3 Security — S3#29 **S3-030335**
15 - 18 July 2003
San Francisco, USA

Source: **BT Group**

Contact: **Colin Blanchard colin.blanchard@bt.com**

Title: **Hybrid MBMS Key Management Scheme**

Document for: **Discussion and decision**

Agenda Item: **MBMS**

Abstract

This contribution is based on contributions to SA3#27 and SA3#28 on the LKH and BAK schemes [1], [2],[3],[4] on the merits or otherwise of point to multipoint key distribution and key hierarchy for MBMS. It supports the view that efficient use of the radio and network resources is important, and proposes that by making use of the uplink messages, a hybrid scheme may be designed which retains the multipoint principle of the LKH scheme, but is more in line with the hierarchy of the BAK scheme. This hybrid scheme more closely matches the needs of network operators, in terms of complexity, operational efficiency and perhaps most importantly, in minimising potential complaints from users that they have missed the start of a broadcast event that they have paid for, due to keying errors.

1 Introduction

At SA3#28 Samsung Electronics in S3-03286 [1], reemphasised that "*The original intention for the introduction of MBMS was to efficiently use the radio/network resources. … Users receiving the same Multicast service within the same area can also be further combined into one (or several subgroups) to make it possible for keys to be given to all users within one subgroup at a time in point-to-multipoint mode.*

However, a contribution from Qualcomm (S3-03197) [2] proposed "*SA3 should adopt the point-to-point BAK scheme for Release 6, and later consider such enhancements as LKH functionality if there is a requirement for it."*

This contribution supports the Samsung Electronics view that efficient use of the radio and network resources is important, and proposes that by making use of the uplink messages, a hybrid scheme may be designed which retains the multipoint principle of the LKH scheme, but is more in line with the hierarchy of the BAK scheme. This hybrid scheme more closely matches the needs of network operators, in terms of complexity, operational efficiency and perhaps most importantly, in minimising potential complaints from users that they have missed the start of a broadcast event that they have paid for, due to keying errors.

It assumes that multicast radio bearers will be used to provide MBMS but on 25/05/3, Stefan Schröder, T-Mobile Deutschland GmbH wrote on the SA3 list "*The recent GERAN MBMS adhoc found severe problems implementing confirmed acknowledge of multicast radio bearers. They concluded that even if it could be implemented, a plain point-to-point bearer may be more spectrum efficient than point to multipoint"*

It is therefore recognized that there is little point in discussing the efficiency of broadcasting key changes if this is just a small proportion of the user traffic, which for technical reasons has to be delivered point to point anyway. This will need to be resolved before SA3 commit to any further work.

This contribution also shows that while for 3GPP, it would be a new scheme requiring development, there is a complete specification for TETRA based mobile systems [5], and sample messages used to implement the required functionality have been include in an appendix for reference.

2 Required Enhancements

2.1 Service Assumptions

1. The use of multicast radio bearers precludes the use of encryption using CK, which is individual to each user and tied to the AKA run e.g. Bearer encryption will be turned off.
2. The use of multicast radio bearers precludes the use of integrity protection using IK, which is individual to each user and tied to the AKA run.
3. As the Traffic Encryption Keys (TEK' s) are not generated or changed by the authentication exchange and there is no explicit binding with an authentication process, a robust key identification and association scheme will be needed.
4. Any delay in commencing the broadcast/multicast while the last member of the group completes an authentication and key agreement process may be unacceptable.
5. There may be a requirement for a user to join after the session set up with the other uses has been completed. For example a "late entry" facility where stream cipher synchronisation and "key in use" information may need to be made available throughout the session.
6. There is a need to change the TEK at regular intervals based on operator policy, which is determined, by the amount of traffic exposed with the key, trust in connected networks, tamper protection in the end user device and trust in the end user.
7. There is a need to change the TEK at any time based on actual or perceived compromise.
8. Key change will not be used to manage users leaving or joining the group, as this is a service subscription issue. A secure key association disassociation mechanism may be needed however.
9. UE's will be switched off, out of coverage or connected to network, which does not participate in the scheme, and so will often be out of step with each other and the network. In the absence of any information to the contrary, each device can only assume that the key it has is the current key.
10. There is a need to distribute keys to all UE's within a group using a single broadcast message.
11. To "catch" as many UE as possible, the message may need to be repeated a number of times around the scheduled key change time.
12. There is a need to allow the operator some flexibility in configuring this key change time e.g. Absolute, Network time, Immediate etc.
13. Each UE must be able to determine which is the current key (as perceived by the network and request a key update if a mismatch is detected.
14. A defined set of rules for deciding if and when a UE acknowledges a key management message is needed, as clearly, if every UE simultaneously acknowledges, by mean of an uplink point-to-point message, the result of a broadcast message, then this will destroy the efficiency that we are aiming for.
15. It must be possible to query the key status of any individual UE at any time for customer support purposes
16. Having stored the keys in the UE, there has to be some means of associating them to different applications on a one to many and many to one basis.
17. The legitimate end user has a motivation to defeat the system and distribute the shared keys that are a necessary feature of any broadcast security scheme. The shared keys while, secure in the UICC are passed over an insecure SIM-ME interface into potentiality insecure ME.

18. It may not be possible to assume effective tamper protection in the end user device and trust in the end user when inserting a UICC into the device in a commercial environment.

19. It may be necessary to implement all key management *and traffic encryption in the UICC* so that the shared key does not need to leave the UICC.

2.2 Identifying the key in use

It is essential to have a means of identifying the status of keys in the system so they may be associated with specific applications. One way of doing this is to define a key set such that:

1. Each TEK shall be a member of a TEK set containing up to a defined number of n keys, and each key shall be identified by its position in the TEK set (TEK number).

2. The TEK number (TEKN), which addresses one of the n TEK's stored in the UE.

3. The TEK Version Number (TEK-VN) shall identify the version of each of the n TEK and should be incremented for each new key identified with the same TEKN.

2.3 How does the UE know which is the "current key" as perceived by the network

A common way of doing this is to provide the necessary information in an appropriate parameter as part of a regular "cell broadcast" message. Since this is only a key identity, and not the actual key, it does not need to be protected by encryption. However, there does need to be protection against forcing the use of an old compromised key.

When scanning a cell prior to registration, a UE shall receive the TEK VN of the TEK in use on that cell in the *"System Information"* broadcast. If the TEK so identified is not known to the UE, the UE shall request the TEK either through its current serving cell or at the new cell using a defined up link command.

2.4 Changing keys

The network can invoke the change of TEK using an appropriate down link command. This shall be performed across the entire network. The network should then notify all UE,s in the cell of the new TEK VN in the *System information* broadcast.

The downlink command shall contain a parameter *"Time Type"* element shall be used to indicate the exact moment of change and may take one of the following forms:

Absolute IV – The network shall activate the new cipher key on the indicated IV.

Network time – The network shall activate the new cipher key on the Network Time.

Immediate - The network shall activate the new cipher key on the first slot in the framing structure

2.4.1 Key overlap scheme

Even with the use of the broadcast key version message and the downlink key change command, only a proportion of UE's will get re- keyed at the same time. By the time they catch up, it is possible that other members of the group will have received new keys and any attempt by the network to broadcast with what it thinks is the current key will fail.

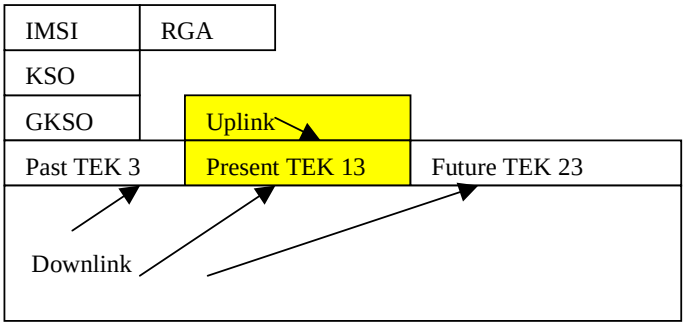
To overcome this problem, a key overlap scheme must be designed such that all users can still communicate when some members of the group have received new keys and the others have not.

1. TEK's may be grouped into one or more subsets to facilitate the key management process. Keys in different subsets associated with the same Re-keying Group Address (RGA) are referred to by the term Key Association Group (KAG).

2. The UE shall consider one TEK of the KAG as current and shall use this TEK as the key for any uplink transmission.

3. Any TEK of the KAG may be used to decrypt downlink messages.

EXAMPLE: If TEKN#3, TEKN#13, TEK23 are members of the same KAG and an UE transmits on the uplink using TEKN#13 then it shall also be prepared to receive downlink message using TEKN3, TERKN#13, TEKN#23.



2.5 Efficiency of key distribution

In normal operation, there will be a smaller number of deliveries of keys, as a result of individual request for key sets from UE's which have missed a key change, then deliveries of scheduled new keys to the whole population of UE's. Hence, delivery of keys, as a result of individual requests, can be made using point-to-point messages. The delivery has to be protected. There are two options:

1. A specific Session Key for OTAR (KSO) may be used to protect the TEK. KSO is individual to each UE and can be derived via an appropriate crypto algorithm from a UE's authentication key (K) and a random seed RSO.

2. As this is individual key, it can be derived from a previous AKA run from CK or IK

However, the regular scheduled key changes based on policy, will cause the bulk of the load on the Key Management system, and it is important that this mechanism is designed to be as efficient as possible, in terms of load on the scarce radio resources. This is achieved by distributing TEK's to groups of UE's, as identified by the Re-keying Group Address (RGA) using a single downlink message.

In the multicast case, the protection of the TEK's cannot be based on K, as in the two options above, as K is specific to each UE and the "unwrapping" process would destroy the efficiency that we are trying to achieve by using a single broadcast message.

Hence, a Group Sealing Key for OTAR (GSKO) shall replace KSO to provide the necessary protection.

GSKO itself is distributed to each UE by OTAR using point-to-point signalling protected by KSO. The assumption is that GSK0 has a much longer life than TEK, and the load on the system would be minimal. In addition, all UE's in the same Re-keying Group Address (RGA) will have the same GSKO.

Note that the RGA and GSKO do not necessary have to correspond to the group structure that is required by the broadcast multicast content.

In summary:

1. The Network broadcasts key download message every few minutes around the key change period. The Re-keying Group Address (RGA) is used as the broadcast download address.

2. UE's that miss these broadcasts, that *do not have the current key*, request it automatically from the network. It is then delivered by the network on a point-to-point basis.

3. UE's that have the current key (VN match), ignore the broadcast.

2.6 Rules for UE response to group key distribution

Key requests by the UE and delivery from the network on a point-to-point basis can follow *Uplink Demand* and *Uplink Result*, type protocol, without much impact on network loading. Clearly, if every UE simultaneously acknowledges, by means of an uplink point-to-point message, the result of every broadcast message, then again, this will destroy the efficiency that we are aiming for.

Since many UE's will already have the key (picked up from the previous broadcast) or will automatically request it when the VN in the "system information" broadcast mismatches the one stored in the UE, we have some flexibility in configuring how the UE responds, if at all.

Hence, when a key is provided to the UE using a group addressed transmission, and using the GSKO for key encryption, the UE shall determine whether to respond to the group addressed OTAR distribution as follows:

1. If the transmission explicitly requires UE to respond, each UE shall respond to inform the Network of the success (or failure) of the transaction following expiry of timer T that is set to a random value on receipt of the OTAR provision.

2. If the transmission does not explicitly require UE to respond, a UE shall respond following the expiry of T on receipt of the OTAR provision, only if the transmission provides that UE with a key or a version of a key that the UE does not have stored.

3. If the transmission does not explicitly require UE to respond, and the transmission does not provide a UE with a key, or a version of a key, that the UE does not have stored, that UE shall not respond.

4. The network provides the maximum value to which the timer T may be set by the UE

5. If a UE is required to respond for one of the reasons given above, but needs to leave the Network by sending "detach" signalling before the expiry of T, the UE shall consider T to have expired at this point, and shall send the response to the OTAR signalling before detaching from the Network.

6. If the UE was unable to send the response, it should store the need to respond, until it next attaches to the network, even if is switched off and on again in the meantime.

3 Conclusion

1. SA3 needs to confirm the service assumptions listed in section 2.1 with SA1 and SA2 and RAN.

2. SA3 needs to check if a suitable system information " cell broadcast " field is available to carry the TEKN and TEK VN information.

3. If confirmed, then SA3, should consider incorporating this mechanism into the TS 33.246 after further elaboration.

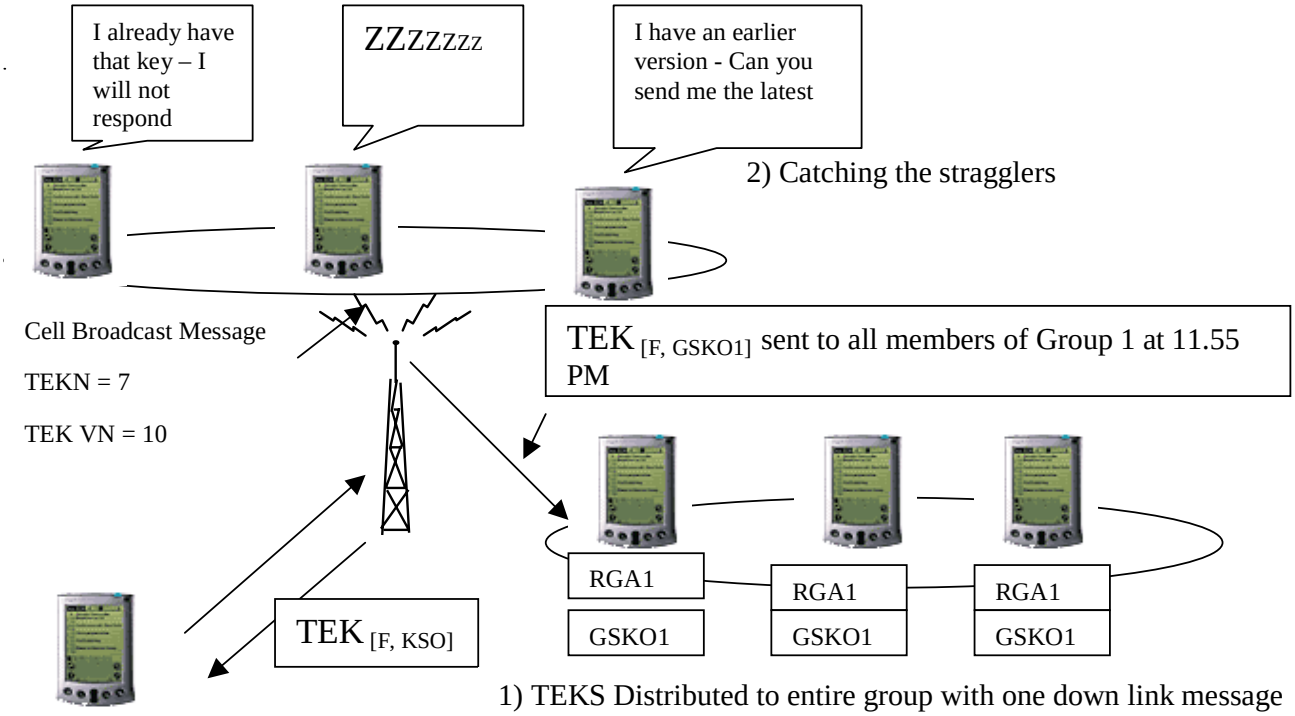
4 References

[1] S3-03286 Further consideration of LKH for MBMS re-keying, Samsung Electronics
[2] S3-03197 MBMS re-keying: point-to-point and LKH, QUALCOMM Europe
[3] S3-030054 Text proposal for MBMS re-keying based on LKH principles. Samsung Electronics
[4] S3-030040 MBMS Security Framework and Pseudo-CR to 33.246. Qualcomm
[5] TETRA Specification ETSI EN 300 392-7 V2.1.19 (2003-05)
(Status submitted to EPT in June 03 for EPT approval prior to submission to Public Enquiry)

5 Glossary

BAK	Broadcast Access key
F	Cryptographic Function used to protect TEK with either KSO or GSKO as the key
GSKO	Group Sealing Key for OTAR
KAG	Key Association Group (KAG).
KSO	Session Key for OTAR
LKH	Logical Key Hierarchy
MBMS	Multimedia Broadcast Multicast Service
OTAR	Over The Air Re-keying
RGA	Re-keying Group Address
TEK	Traffic Encryption Key
TEKN	Traffic Encryption Key Number (in set of TEK's - KAG)
TEK VN	Traffic Encryption Key Version Number
T	UE Response timer

Figure 1 Hybrid MBMS Key Management Scheme



Appendix Extracts from TETRA Specification ETSI EN 300 392-7 V2.1.19 (2003-05)

Function	Clause	Uplink (U) and Downlink (D) Commands
How does the UE know which is the "current key" as perceived by the network	4.5.5.4	The SwMI may administer the change of SCK using the D-CK CHANGE DEMAND PDU. This shall be performed across the entire network. The SwMI MM shall notify all MSs in the cell of the new SCK-VN in the SYSINFO broadcast and in the header of the MAC–RESOURCE PDU described in clause 6.5.1
Changing keys	4.5.5.6	When the D-CK CHANGE DEMAND PDU is used to indicate a change of cipher key or security class of the LA, the "Time Type" element shall be used to indicate the exact moment of change and may take one of the following forms…….
Key overlap scheme	4.2.4.1.1	Key Association Group (KAG). The MS shall consider one SCK of the KAG as current and shall use this SCK as the key for transmission. Any SCK of the KAG may be used for reception.
Requesting missing keys	4.5.2.1	This scenario shows the case where the MS requests provision of one or more SCKs in use on a system. The MS may initiate this procedure at any time using U-OTAR SCK Demand PDU
Keys are given to all users within one subgroup at a time in point-to-multipoint mode.	4.2.5	In some cases keys may need to be distributed to groups as identified by GTSI. In order to allow the sealing mechanisms described in clauses 4.2.2 and 4.2.4 to operate KSO shall be replaced by an Extended Group Session Key for OTAR (EGSKO) derived using algorithm TB7 from the Group Sealing Key for OTAR (GSKO). When distributing GSKO by an OTAR mechanism (algorithms TA91 and TA92) a session key for OTAR (KSO) shall be used to protect the GSKO. KSO shall be individual to each MS and shall be derived from an MS's authentication key (K) and a random seed RSO with algorithm TA41 as for distribution of SCK and GCK. The GSKO has an associated version number, GSKO-VN which can be used for replay protection
Rules for MS response to group key distribution	4.2.5.3	Where a key is provided to the MS using a group addressed transmission, and using the GSKO for key encryption, the MS shall determine whether to respond to the group addressed OTAR distribution as follows:….
Key Association to applications	4.5.4.1	The OTAR KEY ASSOCIATE protocol exchange allows the SwMI to make links between keys and group addresses. The SwMI may request that the MS associates a particular SCK (identified by SCKN) with up to 30 groups (identified by the 'Number of groups' element of the PDU) for which the GSSI of each is listed, or for a range of groups identified by the first and last GSSIs in the range. In this case the key-type element of the D-OTAR KEY ASSOCIATE DEMAND shall be set to SCK. The SwMI may request that the MS associates more than one SCK to one or more groups, where the SCKs are members of the same KAG in different SCK subsets. In this case, it will also identify the structure of the subsets and the member SCK to be associated.