3GPP TSG SA WG3 ad hoc **Tdoc S3z030002**
Antwerp, Belgium
3-4 September 2003

Source: **BT**

Title: **Key management requirements (results of AP 29/11)**

Agenda item: **6.2**

Document for: **Discussion**

Email Discussion Summary

Ref	Contributor	Summary
SA3.1	Colin Blanchard BT 27/07 Marc Blommaert Siemens 08/08 Colin Blanchard BT 12/08	Bearer encryption shall be turned off for point to point and for point to multipoint MBMS sessions. SA3#29 decision (See report: TD S3 030328 Response (from RAN WG2) to LS on double ciphering for MBMS multicast data. This was introduced by Siemens and was provided to SA WG3 for information. It was agreed that there was no need to consider the issue of avoidance of double ciphering any further in SA WG3. The LS was noted. The RAN2 response in S3 030328 seems to make a distinction between PTP and PTM and states "In case of ptm MBMS data transmissions it is RAN2's assumption that NO radio interface ciphering would be applied" I expect that this is because it would be impossible, as SA3 designed the ciphering mechanism for point to point only, using a user specific CK and IK. We need to understand the implications of this. I believe there was a contribution in SA3-S3-030293 "Draft LS on DRM content multicasted via MBMS" which suggested that if the content was already protected by an "OMA DRM" mechanism then MBMS ciphering would not be applied. "When the DRM content is distributed to the UE via MBMS, then the DRM content is already encrypted, when reaching the BM-SC. It's unclear whether an additional encryption shall take place in the BM-SC of the DRM content. This could be an operator choice" However, we also need to consider the case, as described by RAN, when no radio interface ciphering is applied and if our MBMS solution is a full substitute. SA3 have always stressed that one of the reasons for ciphering was to protect the currency of the authentication and prevent MITM attacks I expect that it will be argued that we have mandatory integrity protection of signalling with IK, but do we have this protection for "group addressed signalling" on a PTM connection ? Is there such a thing as group addressed signalling ? what IK do we use ? Perhaps SA3 is OK on all this ?
Ref	**Contributor**	**Summary**
SA3.2	Colin	Bearer integrity protection shall be turned off for point to point

	Blanchard BT 27/07 Marc Blommaert Siemens 08/08	and for point to multipoint MBMS sessions. Notes: SA3#29 decision (See report: TD S3-030328 Response (from RAN WG2) to LS on double ciphering for MBMS multicast data. This was introduced by Siemens and was provided to SA WG3 for information. It was agreed that there was no need to consider the issue of avoidance of double ciphering any further in SA WG3. The LS was noted.
SA3.3	Colin Blanchard BT 27/07 Marc Blommaert Siemens 08/08	All keys used for the MBMS service shall be uniquely identified with a key id number and a version number for that key All keys used for the MBMS service shall be uniquely identifyable~~ied with a key id number and a version number for that key~~. Notes: 'with a key id number and a version number' → this is stage 3 solution dependent. Some solutions may only rely on a number. I propose to remove that text.
SA3.4	Colin Blanchard BT 27/07 Marc Blommaert Siemens 08/08	There shall be a means for MBMS service provider to schedule regular changes of keys using both point to point and point to multipoint Over the Air Re-keying Process (OTAR) Notes: The use of TETRA specific terminology shall be avoided (I.e OTAR). The debate on ptp versus Ptm rekeying is a major topic for decision at next SA3. So the proposed requirement is not agreeable at the moment
SA3.5	Colin Blanchard BT27/07 Marc Blommaert Siemens 08/08 Jim Semple QUALCOMM Europe 01/08	It shall be possible for the MBMS service provider to change keys in any (or ?? subset ???) all UE on a command from a key management centre Notes: Administration requirements are outside SA3's scope. The key management centre is not defined within SA3 specs. With some reformulation this looks more like SA1-requirement. I am not sure you want 'any all'
SA3.6	Colin Blanchard BT 27/07 Marc Blommaert Siemens 08/08	The key management scheme shall be resilient to errors caused by UE's which are switched off, out of coverage or connected to network, which does not participate in the scheme. Notes: This relates to the necessity of a key identification scheme (SA3.3), and the availability of a mechanism which can be used by the UE to retrieve the actual key (based on identity match, and mismatch recognition) when the an update was missed or was erroneous/incomplete. So it may be better to reformulate the requirement in that sense. But this then resemble SA1.3
SA3.7	Colin Blanchard BT 27/07 Marc Blommaert Siemens 08/08	The key change messages shall be repeated a number of times around the scheduled key change time. The ptm rekeying ~~key change messages~~ may ~~shall~~ be repeated a number of times around the scheduled rekeying~~key change~~ time. Notes: This requirement would only make sense for Ptm rekeying. Ptp rekeying is assumed to be reliable
SA3.8	Colin Blanchard	The key management scheme shall take account of the fact that the legitimate end user has a motivation to defeat the system and

	BT 27/07 Jim Semple QUALCOMM Europe 01/08	distribute the shared keys that are a necessary feature of any broadcast security scheme. E.g. The shared keys while, secure in the UICC are passed over an insecure SIM-ME interface I suppose it is not certain that shared keys will be passed over the interface, but we need to add the assumption that we cannot assume all terminals to be secure and, no matter how the shared encryption keys are delivered to the terminal, we have to assume they can be derived in an attack
SA3.10	Colin Blanchard BT 27/07 Marc Blommaert Siemens 08/08	The MBMS security design shall not preclude the use of UICC designs where the content decryption is carried out on the UICC instead of in the ME Questions: What would be the cost of such a UICC: the interface between the UICC and the UE needs to be able transfer/process the whole stream in real-time ! What current state-of the art smartcard can already provide this? Therefore it seems only be worth considering the requirement if the above questions can be answered (it needs to be feasible in future and need some standardisation too). And at the same time: The MBMS security design shall not preclude the use of Pre Rel-6 UICC's.'

Ref	**Contributor**	**Summary**
General	Marc Blommaert Siemens 08/08	I feel unsure about discussing this in SA3 and then liasing it to SA1. In my feeling it may be better to discuss this directly within SA1 (MBMS adhoc this month), so I did not check SA1 requirements in full detail.
SA1.1	Colin Blanchard BT 27/07	It shall be possible for a user to receive content within X1 (? Where does this refer to) of subscribing to the service without any user interaction required
SA1.2	Colin Blanchard BT 27/07 Marc Blommaert Siemens 08/08 Colin Blanchard BT 12/08	It shall be possible for a user to receive content within X2 of subscribing to the service without any user interaction required Note: I do not understand this proposed text. Sorry for not making this clearer, but the problem seems to be is that when we developed the R99 security architecture, we all knew what to expect when subscribing to mobile phone voice services e.g. compare tariffs/coverage/phone models, find a retailer, hand over some money, take home, charge battery, switch on phone, make call to auto help desk to enable prepay voucher (softkey) and the phone is ready to recieve/make calls. If I go into the same shop and buy an MBMS service and are told that I will have to wait until the end of the month, before I can use the service, I might be a bit annoyed, but I don't know this for sure, because I don't know what an MBMS service is and if a rival provider, not working to 3G specifications can do any better. However, there must be some generic service performance requirements that constrain our security solution. Hence "X2" in the above requirement was intended to represent a number e.g. 1

		hour, 1 day, 7 days which will meet customer expectations for the service. The service provider would configure the phone via SMS say, ie "without any user interaction required". The last time configured a WAP phone I had to do it manually as the SMS sender was "down" ! not easy and I am supposed to know about these things I assume that MBMS will be more complex. Otherwise, I agree with your comments, but we need to translate this discussion into a CR for TS 33.246 and draft an LS to SA1 if we are to move forward.
SA1.3	Colin Blanchard BT 27/07 Marc Blommaert Siemens 08/08	It shall be possible for a user to receive content within X3 of subscribing to the service without any user interaction required Note: I do not understand this proposed text. (Same as above)
SA1.4	Colin Blanchard BT 27/07 Marc Blommaert Siemens 08/08 Jim Semple QUALCOMM Europe 01/08	A provide, transfer and cease subscription service shall be provided which is independent of the key management provide, associate and delete service Note: Terminology – associate service in SA1/SA3 specs ? I am not sure what this means? (By the way, we were thinking it might be an idea to have a 'delete BAK' function as part of the MBMS key management to the USIM, so you could un-subscribe a particular user optionally. It may not be perfectly resilient against replay attacks but for example there might be a trade-off between unsubscribing users one day and refreshing all the BAKs the next, rather than refreshing BAK every day, or something like that.

Possible SA3 Security Requirements from 27/07

Ref	Original Assumption from S3-030335	Suggested Requirement
SA3.1	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 (1)	Bearer encryption shall be turned off for point to point and for point to multipoint MBMS sessions
SA3.2	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. (2)	Bearer integrity protection shall be turned off for point to point and for point to multipoint MBMS sessions
SA3.3	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. (3)	All keys used for the MBMS service shall be uniquely identified with a key id number and a version number for that key
SA3.4	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	There shall be a means for MBMS service provider to schedule regular changes of keys using both point to point and point to multipoint Over the Air Re-keying Process

	connected networks, tamper protection in the end user device and trust in the end user. (6)	(OTAR)
SA3.5	There is a need to change the TEK at any time based on actual or perceived compromise. (7)	It shall be possible for the MBMS service provider to change keys in any all UE on a command from a key management centre
SA3.6	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 (9)	The key management scheme shall be resilient to errors caused by UE's which are switched off, out of coverage or connected to network, which does not participate in the scheme,
SA3.7	To "catch" as many UE as possible, the message may need to be repeated a number of times around the scheduled key change time (11)	The key change messages shall be repeated a number of times around the scheduled key change time
SA3.8	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. (17)	The key management scheme shall take account of the fact that 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. E.g. The shared keys while, secure in the UICC are passed over an insecure SIM-ME interface
SA3.9	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 (18)	No requirements shall be placed on the UE which requires UE to be customised to a particular customer prior to the point of sale
SA3.10	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. (19)	The MBMS security design shall not preclude the use of UICC designs where the content decryption is carried out on the UICC instead of in the ME

Possible SA1 Service Requirements from 27/07

Ref	Original Assumption from S3-030335	Suggested Requirement
SA1.1	Any delay in commencing the broadcast/multicast while the last member of the group completes an authentication and key agreement process may be unacceptable. (4)	It shall be possible for a user to receive content within X1 of subscribing to the service without any user interaction required
SA1.2	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 (5)	It shall be possible for a user to receive content within X2 of subscribing to the service without any user interaction required
SA1.3	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. (13)	It shall be possible for a user to receive content within X3 of subscribing to the service without any user interaction required
SA1.4	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 (8)	A provide, transfer and cease subscription service shall be provided which is independent of the key management provide, associate and delete service
SA1.5	There is a need to distribute keys to all UE's within a group using a single broadcast message. (10)	The key management scheme shall be designed to keep the load on the radio access network to the minimum while ensuring maximum security for the service
SA1.6	~~12.~~There is a need to allow the operator some flexibility in configuring this key change time e.g. Absolute, Network time, Immediate etc. (12)	The scheme shall be designed to allow the MBMS service provider to control the load on the MBMS nodes by configuring the key change time e.g. Absolute, Network time, Immediate etc.
SA1.7	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. (14)	It shall be possible for the MBMS service provider to request acknowledgements from specific UE or groups of UE but the scheme shall be designed to keep the load on the radio access network to the minimum while ensuring maximum security for the service
SA1.8	It must be possible to query the key status of any individual UE at any time for customer support purposes (15)	It shall be possible to query the key status of any individual UE at any time for customer support purposes
SA1.9	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 (16)	There may be more than one service provided a MBMS service provider and more than one MBMS service provider. a) There shall be a means of associating Security associations to different applications on a one to many and many to one basis b) The bits allocated in the key Id field shall be sufficient for X4 services per service provider and X5 service providers.