3GPP TSG SA WG3 Security — MBMS ad-hoc **S3z030022**
3-4 September 2003
Antwerp, Belgium

Agenda item: MBMS Security

Source: **QUALCOMM Europe**

Title: Updating Encryption Keys For MBMS

Document for: Discussion and Decision

1 Introduction

Security for MBMS relies on a secret key being distributed to many authorized subscribers for the purpose of decrypting MBMS content. As the Mobile Equipment may be insecure, these keys must be updated frequently to outweigh the effectiveness of an attacker deriving keys and distributing them.

This contribution provides estimates of the signalling overhead in delivering keys in a purely point-to-point manner.

2 Discussion

Fundamental to 3GPP2's framework for MBMS security is the notion that a common symmetric key is delivered to the UICC, from which encryption keys are derived using broadcast material. The goal is to make use of the trust in the UICC to provide frequent point-to-multipoint re-keying while making efficient use of radio resources. It is anticipated that keys on the ME must be changed frequently to counter the threat that an attacker may derive keys from an insecure terminal and publish them, thus allowing non-subscribers inexpensive access to broadcast data.

This contribution considers the signalling overhead in the alternative scenario that all the keys are delivered to the ME in a point-to-point manner. In these scenarios it is presumed the UE goes from idle mode to RRC connected mode, performs some upper layer signalling, and returns to idle mode. This is similar to the signalling exchange required to set up and release a PS data call. The aim is to provide conservative estimates which do not even account for the messages required to derive or deliver the keys themselves.

In particular one of the most problematic messages may be the RRC CONNECTION SETUP message sent by UTRAN in the early stages of the procedure. This message is very long (1112 bits) and sent on a common channel (CCCH : FACH : SCCPCH), which is not power controlled. For this reason it requires 5 to 10 times the amount of power that it would require if it was sent on dedicated (power controlled) channels. Moreover, as it is sent in RLC Unacknowledged Mode, this means that UTRAN must repeat it several times to increase the probability that it is received correctly by the UE.

Sending this message often, there is the serious risk of overloading the capacity of the common channels. The problems will be particularly severe when many subscribers must perform point-to-point key management at the same time, such as in a football stadium scenario. Thus frequent point-to-point re-keying for MBMS is untenable. Detailed estimates of the signalling overhead are provided in the Appendix.

3 Conclusion

A two-tiered solution provides the flexibility to change encryption keys with whatever granularity is desired, but keeping the signalling overhead to a minimum. The cost of point-to-point re-keying, in terms of signalling overhead, may be so high that keys cannot be updated sufficiently often to counter attacks. SA3 should adopt a solution whereby frequent re-keying is performed by the UICC based on material which is broadcast.

[1] MBMS Security Framework, S3-030356

[2] Levels of Key Hierarchy for MBMS, S3-030360

4. Appendix: Signaling Overhead in a PS Call

This appendix provides estimates of the signaling overhead in mobile-originated and mobile-terminated packet-switched calls. It is assumed that the mobile has previously registered with the network for packet switched services, and that a 6-digit P-TMSI has been assigned to the mobile. It is assumed that the mobile is in the idle mode, with no RRC connection, before and after the call.

Mobile Originated Calls

Call flow

Step	**Direction**		**RRC Message** **[NAS Source: NAS message]**	**Logical :** **Transport :** **Physical**
	MS	**NW**		
1	→		RRC Connection Request	CCCH : RACH : PRACH
2	←		RRC Connection Setup	CCCH : FACH : SCCPCH
3	→		RRC Connection Setup Complete	DCCH : DCH : DPDCH

4	→	Initial Direct Transfer [GMM: Service Request]	DCCH : DCH : DPDCH
5	←	Downlink Direct Transfer [GMM: Authentication And Ciphering Request]	DCCH : DCH : DPDCH
6	→	Uplink Direct Transfer [GMM: Authentication And Ciphering Response]	DCCH : DCH : DPDCH
7	←	Downlink Direct Transfer [GMM: Service Accept]	DCCH : DCH : DPDCH
8	→	Uplink Direct Transfer [SM: Activate PDP Context Request]	DCCH : DCH : DPDCH
9	←	RB Setup	DCCH : DCH : DPDCH
10	→	RB Setup Complete	DCCH : DCH : DPDCH
11	←	Downlink Direct Transfer [SM: Activate PDP Context Accept]	DCCH : DCH : DPDCH
12	→ ←	UL/DL Data Transfer (user data transfer)	DTCH : DCH : DPDCH
13	→	Uplink Direct Transfer [SM: Deactivate PDP Context Request]	DCCH : DCH : DPDCH
14	←	Downlink Direct Transfer [SM: Deactivate PDP Context Accept]	DCCH : DCH : DPDCH
15	←	Radio Bearer Release	DCCH : DCH : DPDCH
16	→	Radio Bearer Release Complete	DCCH : DCH : DPDCH
17	←	RRC Connection Release	DCCH : DCH : DPDCH
18	→	RRC Connection Release Complete	DCCH : DCH : DPDCH

Steps 1-3 set up the RRC connection for signalling. Steps 4-11 sets up the mobile originated packet data call. Steps 13-16 release the packet data call. Steps 17-18 release the RRC signaling connection.

The radio network may alternatively decide to keep RRC signalling connections for future use. The Security Mode Command may be issued by the UTRAN after step 6 if the security mode control procedure is supported.

Message sizes

RRC Message [NAS Source: NAS message]	RLC size (bits)	RRC size (bits)	NAS size (bits)	Total size (bits)
RRC Connection Request	0	80	0	80
RRC Connection Setup	80	1032	0	1112
RRC Connection Setup Complete	56	152	0	208
Initial Direct Transfer [GMM: Service Request]	=16*2+24	88	=9*8	216
Downlink Direct Transfer [GMM: Authentication And Ciphering Request]	=16*3+24	32	=40*8	424
Uplink Direct Transfer [GMM: Authentication And Ciphering Response]	=16*2+24	80	80	216
Downlink Direct Transfer [GMM: Service Accept]	40	32	16	88
Uplink Direct Transfer [SM: Activate PDP Context Request]	=16*5+24	80	=61*8	672
RB Setup	=16*6+24	720	0	840
RB Setup Complete	40	16	0	56
Downlink Direct Transfer [SM: Activate PDP Context Accept]	=16*2+24	32	=20*8	248
UL/DL Data Transfer (user data transfer)	0	0	0	0
Uplink Direct Transfer [SM: Deactivate PDP Context Request]	40	80	24	144

Downlink Direct Transfer [SM: Deactivate PDP Context Accept]	40	32	16	88
Radio Bearer Release	=16*5+24	624	0	728
Radio Bearer Release Complete	40	16	0	56
RRC Connection Release	8	16	0	24
RRC Connection Release Complete	8	8	0	16
Total size (bits)	**920**	**3120**	**1176**	**5216**

Mobile Terminated Calls

Call flow

This procedure sets up a mobile terminated packet switched data call, and then releases it.

Step	**Direction**		**RRC Message** **[NAS Source: NAS message]**	**Logical :** **Transport :** **Physical**
	MS	**NW**		
1	←		Paging Type 1	PCCH : PCH : SCCPCH
2	→		RRC Connection Request	CCCH : RACH : PRACH
3	←		RRC Connection Setup	CCCH : FACH : SCCPCH
4	→		RRC Connection Setup Complete	DCCH : DCH : DPDCH
5	→		Initial Direct Transfer [GMM: Service Request]	DCCH : DCH
6	←		Downlink Direct Transfer [GMM: Authentication And Ciphering Request]	DCCH : DCH

7	→	Uplink Direct Transfer [GMM: Authentication And Ciphering Response]	DCCH : DCH
8	←	Downlink Direct Transfer [GMM: Service Accept]	DCCH : DCH
9	←	Downlink Direct Transfer [SM: Request PDP Context Activation]	DCCH : DCH
10	→	Uplink Direct Transfer [SM: Activate PDP Context Request]	DCCH : DCH
11	←	RB Setup	DCCH : DCH
12	→	RB Setup Complete	DCCH : DCH
13	←	Downlink Direct Transfer [SM: Activate PDP Context Accept]	DCCH : DCH
14	→ ←	UL/DL Data Transfer	DTCH : DCH
15	←	Downlink Direct Transfer [SM: Deactivate PDP Context Request]	DCCH : DCH
16	→	Uplink Direct Transfer [SM: Deactivate PDP Context Accept]	DCCH : DCH
17	←	Radio Bearer Release	DCCH : DCH
18	→	Radio Bearer Release Complete	DCCH : DCH
19	←	RRC Connection Release	DCCH : DCH
20	→	RRC Connection Release Complete	DCCH : DCH

Step 1 pages the mobile for the mobile terminated packet data call. Steps 2-4 set up the RRC connection for signalling. Steps 5-13 sets up the mobile terminated packet data call. Steps 15-18 release the packet data call. Steps 19-20 release the RRC signalling connection. The radio network may alternatively decide to keep RRC signalling connections for future use.

Security Mode Command may be issued by the UTRAN after step 6 if the security mode control procedure is supported.

Message sizes

RRC Message **[NAS Source: NAS message]**	**RLC size** **(bits)**	**RRC size** **(bits)**	**NAS size** **(bits)**	**Total size** **(bits)**
Paging Type 1	0	72	0	72
RRC Connection Request	0	80	0	80
RRC Connection Setup	80	1032	0	1112
RRC Connection Setup Complete	56	152	0	208
Initial Direct Transfer [GMM: Service Request]	=16*2+24	88	=9*8	216
Downlink Direct Transfer [GMM: Authentication And Ciphering Request]	=16*3+24	32	=40*8	424
Uplink Direct Transfer [GMM: Authentication And Ciphering Response]	=16*2+24	80	=10*8	216
Downlink Direct Transfer [GMM: Service Accept]	40	32	=2*8	88
Downlink Direct Transfer [SM: Request PDP Context Activation]	=16*2+24	32	=17*8	224
Uplink Direct Transfer [SM: Activate PDP Context Request]	=16*5+24	80	=61*8	672
RB Setup	=16*6+24	720	0	840
RB Setup Complete	40	16	0	56
Downlink Direct Transfer [SM: Activate PDP Context Accept]	=16*2+24	32	=20*8	248
UL/DL Data Transfer	0	0	0	0

Downlink Direct Transfer [SM: Deactivate PDP Context Request]	40	32	=3*8	96
Uplink Direct Transfer [SM: Deactivate PDP Context Accept]	40	80	=2*8	136
Radio Bearer Release	=16*5+24	624	0	728
Radio Bearer Release Complete	40	16	0	56
RRC Connection Release	8	16	0	24
RRC Connection Release Complete	8	8	0	16
Total Size (bits)	**976**	**3224**	**1312**	**5512**