3GPP TSG SA WG3 Security — S3#34   **S3-040598**

July 6 - 9, 2004

Acapulco, Mexico

TSG-SA WG1 #25   **S1-040729**
Montreal, Canada, 28 June- - 02 July 2004   **Agenda Item: 6.1.2**

Title:	**LS on MBMS key Management**
Response to:	LS to SA1/SA4/T3 on **LS on MBMS key Management**
Release:	Release 6
Work Item:	Rel-6 MBMS

Source:	SA1
To:	SA3
Cc:	SA4, T3

Contact Person:
    Name: John Watson
    Tel. Number: +44 1635 682178
    E-mail Address: John.Watson@Vodafone.com

Attachments: S1-040720 "Key management priority for MBMS services"

SA1 would like to thank SA3 for their liaison in document S1-040564 [S3-040445].

1. Overall Description:

SA1 has taken into account the considerations within the S3 LS and agree that the assumptions in point 3 are in line with current 3GPP service requirements on MBMS.

SA1 would like to add that it has no view on the actual S3 implementation as long as the security requirements are met, SA1 can not comment on the solution itself.
SA1 does understood that allowing launch of MBMS services without requiring an updated UICC will allow for a more cost effective and early launch of MBMS which would stimulate the mass market MBMS requires, further to this SA1 believes that speed to market is important and if the use of ME as well as the UICC solution allows a faster deployment and better evolution path for operators then SA1 agrees with SA3 that the combined ME/UICC solution is the best way forward.

In addition to the above SA1 has agreed that the UICC solution is to have priority and that the ME based solution is to be optional. SA1 have agreed a CR to TS 22.146 to reflect this decision which is attached to this LS for information.

2. Actions:

None.

3. Date of next SA1 Meetings:

SA1 SWGs   23rd – 27th August 2004   Vienna, Austria

SA1#26   11 – 15 October 2004   Sophia Antipolis, FR

CR-Form-v7

CHANGE REQUEST

· **22.146** CR **045** · rev **-** · Current version: **6.5.0** ·

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 [X] Radio Access Network [ ] Core Network [ ]

Title:	· Key management priority for MBMS services

Source:	· SA1

Work item code:	· MBMS	Date: · 28/06/2004

Category:	· **F**	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: ·	Presently it is unclear if key management for MBMS services is required on ME.

Summary of change: ·	Explicit requirement about key management is added, indicating clearly the priority of the mechanisms.

Consequences if not approved: ·	Unclear requirement and non homogeneous implementation of the MBMS key management

Clauses affected: ·	6

	Y	N		
Other specs affected: ·	X		Other core specifications ·	33.220
		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.

**************** first modified section***

6 Security

In multicast mode it shall be possible to ensure that only those users who are entitled to receive a specific multicast service may do so. It should be possible to choose whether a given multicast service is to be delivered with or without ensured group privacy.

If a terminal supports MBMS, then it shall support UICC based key management and all the function and interfaces required for it. ME key management can be optionally supported. If the UICC is capable of MBMS key management, ME key management shall not be activated.