3GPP TSG SA WG3 Security — S3#26
19 - 22 November 2002, Oxford, UK

S3-020613

CR-Form-v7

CHANGE REQUEST

⌘	**33.cde**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	**0.0.2** ⌘

*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 ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	MBMS: Reorganisation of Requirement chapters		
Source:	⌘	Siemens		
Work item code:	⌘	MBMS	***Date:*** ⌘	13/11/2002
Category:	⌘	**D**	***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:	⌘	Separate the key management requirements from data protection requirements as these functions may be realized in separate entities or layers. This improves readability and discussions. Clause 4 will map onto described functions of chapter 5. Some other smaller editorials.
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	4				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

4.1 Security requirements

The following security requirements have been identified for MBMS.

Editor's note: Not all the security requirements in this section have been agreed.

4.1.1 Requirements on security service access

4.1.1.1 Requirements on secure service access

R1a: A valid USIM shall be required to access any 3G service including the MBMS service.

R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS services by masquerading as authorized users.

4.1.1.2 Requirements on secure service provision

R2a: It shall be possible for service providers (i.e. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS services.

R2b: It shall be possible to prevent the use of a particular USIM to access MBMS services.

Editor's Note: It is for FFS to what extent it is required to detect and prevent fraudulent use of MBMS services.

4.1.2 Requirements on integrity protection of MBMS multicast data ~~and security keys~~

R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS multicast data sent to the UE on the radio interface.

Editor's note: Requirement R3a has not been agreed.

R3b: The MBMS multicast data may be integrity protected with a common integrity key, which shall be available to all users that has joined the MBMS service.

R3c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi and Gmb.

Editor's Note: It may be required to integrity protect the multimedia content on the "Content Provider - BM-SC" interface. As this interface shall not be standardized in 3GPP, according to TR 23.846, no such requirement can be defined by 3GPP.

4.1.3 Requirements on confidentiality~~encryption~~ protection of MBMS multicast data ~~and security keys~~

R4a: It shall be possible to protect the confidentiality of MBMS multicast data on the radio interface.

R4b: The MBMS multicast data may be encrypted with a common encryption key, which shall be available to all users that have~~s~~ joined the MBMS service.

~~R4c: The encryption key(s) and the integrity key for the MBMS multicast service shall be encrypted when delivered to the users. In addition, it may be required to protect these keys with a MAC.~~

~~R4d: Only the valid users that has joined a MBMS multicast service shall be able to decrypt the encryption key(s) and the integrity key delivered from the network.~~

~~R4e: Mandate support of re-keying in the UE and BM-SC in order to ensure that users that has joined a MBMS service, but then left, shall not gain MBMS multicast service without being charged.~~

R4c~~g~~: It may be required to encrypt the MBMS multicast data on the “BM-SC - GGSN” interface, i.e. the reference points Gi and Gmb.

~~R4h: User identity should not be exposed to the content provider or linked to the content, in the case the Content Provider is located in the 3GPP operator’s network.~~

Editor’s Note: It may be required to encrypt the multimedia content on the “Content Provider - BM-SC” interface. As this interface shall not be standardized in 3GPP, according to TR 23.846, no such requirement can be defined by 3GPP.

4.1.4 Requirements on MBMS Key Management

R5a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R5b: The transfer of the MBMS keys between the MBMS key generator and the UE may be integrity protected.

R5c: The UE and the MBMS key generator shall support re-keying in order to ensure that users that have joined an MBMS service, but then left, shall not gain MBMS multicast service without being charged.

R5d: Only authorized users that have joined an MBMS multicast service shall be able to receive MBMS keys delivered from the MBMS key generator.

Editor’s Note: The MBMS key generator function is still to be allocated to a network node.

4.1.5 Requirements on Privacy

R6a: The User identity should not be exposed to the content provider or linked to the content in the case the Content Provider is located in the 3GPP operator’s network.