3GPP TSG-SA3 #29
San Fransisco, USA, 15-18 July, 2003

Tdoc ⌘S3-030366

CR-Form-v7

CHANGE REQUEST

⌘	**33.246**	**CR**		⌘ **rev**	**-**	⌘	Current version:	**0.2.0** ⌘

*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 ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Confidentiality protection of MBMS multicast data		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	2003-07-04
Category:	⌘	**D** *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.	***Release:*** ⌘	Rel-6 *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:	⌘	Ericsson proposes to add two new security requirements regarding man-in-the-middle attacks on encrypted MBMS multicast data between BM-SC and UE.
Summary of change:	⌘	The following security requirements are added: - It shall be infeasible for an attacker to act as a man-in-the-middle to degrade the security protection offered to an MBMS multicast session from the BM-SC to the UE. - It shall be infeasible for a man-in-the-middle to break the confidentiality of the MBMS multicast session when it is encrypted.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.1.3				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

4 MBMS security architecture

MBMS introduces the concept of a point-to-multipoint service into a 3G network. A requirement of a multicast service is to be able to securely transmit data to a given set of users. In order to achieve this, there needs to be a method of authentication, key distribution and data protection for a multicast service. The point-to-point services in a 3G network use the AKA protocol (see TS 33.102 [4]) to both authenticate a user and agree on keys to be used between that user and the network. These keys are subsequently used to provide integrity protection of signalling traffic and optional confidentiality protection of both signalling and user data between the RNC and the UE.

MBMS could possibly use the AKA procedure to authenticate the user. It requires its own key management/distribution process, as the same key(s) needs to be sent to a group of users. The key distribution method could rely on the point-to-point confidentiality to protect the transfer of MBMS keys. The protection of the data may also require a special mechanism.

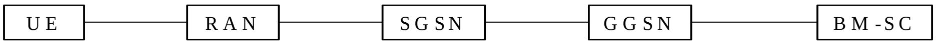

Figure 1: MBMS security architecture

Figure 1 gives an overview of the network elements involved in MBMS from a security perspective. The Broadcast Multicast – Service Centre (BM-SC) is a source for MBMS data. It could also be responsible for scheduling data and receiving data from third parties (this is beyond the scope of the standardisation work) for transmission.

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. Most of the requirements are for the multicast service only.

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 the network service providers (i.e.g. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS services.

Editor’s note: Authentication during service is ffs.

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

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. The use of integrity shall be optional.

Editor's note: It may be possible to detect the deletion of MBMS data packets, but it is impossible to prevent the deletion. Packets may be lost because of bad radio conditions, providing integrity protection will not help to detect or recover from this situation.

Note: the use of shared keys (integrity and confidentiality) to a group of untrusted users only prevents attacks of lower levels of sophistication, such as preventing eavesdroppers from simply listening in

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

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

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 protection of MBMS multicast data

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 joined the MBMS service.

R4c: It may be required to encrypt the MBMS multicast data on the "BM-SC - GGSN" interface, i.e. the reference points Gi.

R4d: It shall be infeasible for an attacker to act as a man-in-the-middle to degrade the security protection offered to an MBMS multicast session from the BM-SC to the UE.

R4e: It shall be infeasible for a man-in-the-middle to break the confidentiality of the MBMS multicast session when it is encrypted.

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.