3GPP TSG-SA WG3 (Security) meeting #29 ***Tdoc S3-030401***
15-18 July 2003
San Francisco, USA

Agenda Item: **7.20 MBMS**

Source: **Nortel Networks**

Title: **MBMS Security Requirements Clarification**

Document for: **Discussion and Decision**

1. Introduction

SA3 is considering various security mechanisms for MBMS service. This document discusses Nortel's understanding of the MBMS Service requirements in TS 22.146. The accompanying pseudo-CR proposes the required changes to reflect these clarifications in the SA3 TS 33.246 in order to aid SA3 to further progress the MBMS work item.

2. Discussion

2.1 Split between MBMS Bearer Capability and MBMS Application

The 3GPP specification of MBMS involves two distinct aspects. The first part is the specification of enhancements to the GPRS network to provide for multicast and broadcast data distribution as a bearer capability. The second part is the specification of MBMS applications which will use the MBMS bearer capabilities to meet the service requirements as identified by each such MBMS application. The table below (reproduced from TS 22.146, Annex A) lists some of the possible applications and their bit-rates using the MBMS bearer service:

Application	**Media type(s)**	**[1]Typical Bit rate**
Traffic telematics	Text, audio, pictograms, video	8kb/s ~ 64kb/s
Weather	Text, video, pictograms	8kb/s ~ 64kb/s
Advertising	Text, video, pictograms	8kb/s ~64kb/s
News broadcast	Audio, video	8kb/s ~ 256kb/s
Music streaming, (Web radio)	Audio	8kb/s ~ 64kb/s
Video concert	Audio/Video	32kb/s ~ 256kb/s
Sports replay	Video	32kb/s ~ 256kb/s
File sharing	Binary data	8kb/s ~ 256kb/s

1. Actual bit rates are dependent on radio access technology and terminal capabilities

The TS 22.146 (MBMS Stage 1) further states that for Broadcast mode (Section 5.1.1):

"- Types of data services

MBMS in The broadcast mode shall be transparent for the transferred data packets independent of the type of service being transmitted, will support a number of services, and permit support of and therefore transfer all data types e.g. Audio, Data, Video or combinations thereof. A minimum number of data types may need to be identified to enable interoperability.

For Multicast mode (Section 5.2.1):

"- Types of services

The multicast mode shall be independent of the type of service being transmitted, will support a number of services, and permit support of all data types e.g. Audio, Data, Video or combinations thereof. A minimum number of data types may need to be identified to enable interoperability"

Figure 1 further illustrates these two distinct aspects.

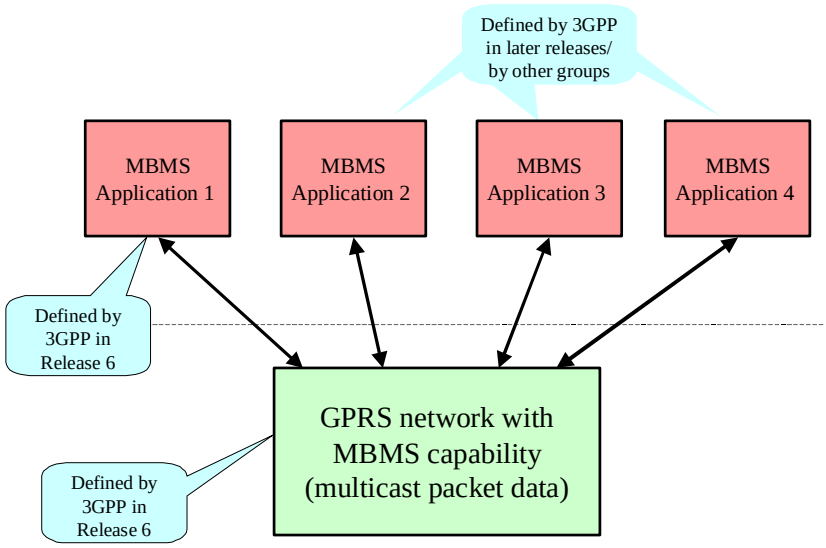

Figure 1 Split between MBMS Bearer capability and MBMS applications

In SA plenary #20, a Work Item Description to specify "MBMS Codecs and Protocols" was approved. This new work item requires work in SA1 in drafting of a new "MBMS Teleservice" stage 1 specification. SA1 is currently studying the service requirements and uses cases for the MBMS Teleservice. Based on the MBMS Teleservice requirements, SA4 is primed to specify "set of media codecs, formats and transport/application protocols for MBMS" to meet such service requirements identified by SA1.

Any security architecture that is developed by SA3 for such MBMS Teleservice would have to take into account the progress of this work item in other groups.

<u>Conclusion 1:</u> It is clear that the intention of 3GPP is to define MBMS as a GPRS network bearer service and standardize (potentially limited) set of MBMS applications utilizing the basic MBMS bearer capability.

2.2 Implications for SA3 work

The split of MBMS as a bearer service and MBMS application has a direct impact on the on-going SA3 work on MBMS Security. Two major implications of the MBMS work split are:

1) Any security mechanism specified for MBMS bearer service by SA3 has to be general (i.e., all MBMS services should be able to use the security mechanisms specified by SA3). Such general purpose security tools/mechanisms may include key generation and/or distribution, especially on the UICC in order to ensure interoperability of MBMS applications.
2) Different MBMS applications may potentially use different protocols (based on the outcome of the SA4 work). This has implications on the nature of the security protections (e.g., confidentiality/integrity protection) that is appropriate for the selected media formats and/or protocols for that particular MBMS application. For example, the protocols and/or security mechanisms that are appropriate for file download may be quite different from the media streaming application requirements.

<u>Conclusion 2</u>: At this time, only the security mechanisms/requirements that apply to MBMS bearer capability needs to be specified by SA3. Any MBMS application specific security mechanisms/requirements, if needed, needs to be specified by SA3 when such application service requirements and codec/protocol work stabilizes in other 3GPP working groups.

3. Proposal

1) It is proposed that the conclusions 1 & 2 presented in this paper be agreed as a working assumption for further MBMS work in SA3.
2) It is also further proposed that attached pseudo-CR clarifying these MBMS requirements be approved and incorporated in to the TS 33.246

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

Tdoc ⌘S3-030xxx

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** ⌘ **rev** **-** ⌘ Current version: **0.1.0** ⌘

*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:	⌘	Security requirements clarification for MBMS
Source:	⌘	Nortel Networks
Work item code:	⌘	MBMS
Date:	⌘	2003-07-08
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:	⌘	MBMS security requirements are more clearly stated to differentiate between MBMS bearer service and MBMS applications.
Summary of change:	⌘	The following MBMS security requirements are added: - MBMS is considered to be a GPRS network bearer service. Therefore, any MBMS security mechanisms specified in this specification shall be MBMS bearer-service specific, so that any MBMS application that is developed using the MBMS bearer service could utilize the security mechanisms. - Any MBMS application specific security requirements shall be specified as part of the MBMS application specification development
Consequences if not approved:	⌘	The security requirements specified in the TS does not take into consideration the MBMS requirements specified in TS 22.146

Clauses affected:	⌘	4.1

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			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.

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

MBMS is considered to be a GPRS network bearer service. Therefore, any MBMS security mechanisms specified in this specification shall be MBMS bearer-service specific, so that any MBMS application that is developed using the MBMS bearer capability could utilize the security mechanisms/or tools specified in this specification. Any MBMS application specific security requirements shall be specified as part of the MBMS application-specific security specification development

The following security requirements have been identified for MBMS bearer service.

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.