3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040535

CR-Form-v7

CHANGE REQUEST

⌘	**33.246**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**1.2.1**	⌘

*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: ⌘	User authentication in MBMS		
Source: ⌘	Ericsson, Nokia		
Work item code: ⌘	MBMS	***Date:*** ⌘	30/06/2004
Category: ⌘	**C**	***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: ⌘ The authentication of the user is incompletely defined in the specification. User authentication is needed in several situations in MBMS. The present TS should be clear what these situations are and how the user authentication is performed.

Summary of change: ⌘ It is clarified in which cases UE is autenticated in MBMS. The following situations are identified:
- When user requests for keys for MBMS user service
- When user requests MBMS bearer establishment or release
- When user joins or leaves MBMS user service (This is dependent on work of SA4)
- When the user performs post delivery procedures (This is dependent on work of SA4)

Consequences if not approved: ⌘ Authentication of the UE remains unclear.

Clauses affected: ⌘ 5.1, 6.2

Other specs affected: ⌘

Y	N		
X		Other core specifications ⌘	TS 24.109
	X	Test specifications	
	X	O&M Specifications	

Other comments: ⌘

*********************************** *** NEXT CHANGE **********************************

5 MBMS security functions

5.1 Authenticating and authorizing the user

A UE is authenticated and authorised in ~~two~~ following situations ~~parts~~ when participating in an MBMS User Service. That is: ~~Firstly~~

- when the UE performs User Service joining (or leaving) on the application level

Editor's Note: The final decision on application level join procedures relies of work in SA4.

- when the UE establishes (or releases) the MBMS bearer(s) to receive an MBMS User Service. ~~and secondly when the UE requests and receives MSKs for the MBMS User Service. The MBMS bearer establishment requires a point to point connection with the network on which authentication is performed using network security described in TS 33.102 [4]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish the MBMS bearer(s) corresponding to an MBMS User Service (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the MBMS bearer(s) related to a UE that is no longer authorised to access an MBMS User Service.~~

- when the UE requests and receives MSKs for the MBMS User Service

- when the UE performs post delivery procedures (e.g. point to point repair service)

Editor's Note: The final decision on post delivery procedures relies of work in SA4.

NOTE: The list above does not reflect the order of authentications.

Editor's Note: It was agreed that the GBA method will be used for MBMS Security (GBA-U + GBA-ME + MIKEY). It was agreed that the work would continue under the assumption of there being both the UICC-based solution and ME-based solution. If a Terminal is to support MBMS, then it will need to support GBA-U.

~~Editor's Note: Authentication may also be needed for application layer joining and leaving. The final decision relies of work in SA4.~~

************************************** NEXT CHANGE **********************************

6.2 Authentication and authorisation of a user

Editor's note: this section will contain the details on authentication and authorization of an MBMS user

Editor's Note: The exact details on how to derive the keys MRK and MUK from the GBA keys are for ffs.

6.2.1 Authentication and authorisation in application level joining

When the user wants to join (or leave) an MBMS user service, it shall use HTTP digest authentication [~~6~~8] for authentication. HTTP digest is run between BM-SC and ME. The MBMS authentication procedure is based on the general user authentication procedure over Ua interface that is specified in chapter "Procedures using the bootstrapped Security Association" in [6]. The BM-SC will act as a NAF according to [6].

The following adaptations apply to HTTP digest:

- The transaction identifier as specified in [~~8~~6] is used as username
- MRK (MBMS Request Key) is used as password.
- The joined MBMS user service is specified in client payload of HTTP Digest message.

Editor's Note: The contents of the client payload are FFS and may require input from TSG SA WG4.

Editor's Note: The final decision on application level join and leave procedures relies of work in SA4.

6.2.2 Authentication and authorisation in MBMS bearer establishment

The authentication of the UE during MBMS bearer establishment relies on the authenticated point~~-~~-to-point connection with the network, which was set up using network security described in TS 33.102 [4]. Authorisation for the MBMS bearer establishment happens by the network making an authorisation request to the BM-SC to ensure that the UE is allowed to establish the MBMS bearer(s) corresponding to an MBMS User Service (see TS 23.246 [3] for the details). As MBMS bearer establishment authorisation lies outside the control of the MBMS bearer network (i.e. it is controlled by the BM-SC), there is an additional procedure to remove the MBMS bearer(s) related to a UE that is no longer authorised to access an MBMS User Service.

6.2.3 Authentication and authorisation in MSK request

When the UE requests MSK(s), the UE shall be authenticated with HTTP digest as in chapter 6.2.1.

6.2.4 Authentication and authorisation in post delivery procedures

When the UE requests post delivery procedures, the UE shall be authenticated with HTTP digest as in chapter 6.2.1.

Editor's Note: The final decision on post delivery procedures relies of work in SA4.

~~Editor's Note: The use of bootstrapped keys for leaving an MBMS user service, for an MSK key request and request to a download repair server is for ffs.~~

Editor's Note: According to S3-040212, SA4 has a working assumption to use HTTP as the transport protocol but this is only agreed for the download repair service.