3GPP TSG-SA-WG3 Meeting #33
10th – 14th May 2004, Beijing, China

Tdoc ⌘S3-040238

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.246 CR CRNum** ⌘ **rev** ⌘ Current version: 1.1.0 ⌘

*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:	⌘	Authenticating user in MBMS with HTTP digest
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	05/04/2004
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:	⌘	MBMS user authentication has not been specified. S3-040058 in SA3#32 proposed to use HTTP digest for user authentication in MBMS. This pseudo CR proposes the same and provides text to TS 33.246.
Summary of change:	⌘	HTTP digest is used to authenticate the user.
Consequences if not approved:	⌘	

Clauses affected:	⌘	2, 6.1

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

⌘

Other comments: ⌘

********BEGIN CHANGE**********

2 References

The following documents contain provisions, which, through reference in this text, constitute provisions of the present document.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.146: "Multimedia Broadcast/Multicast Service; Stage 1".

[3] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and Functional Description".

[4] 3GPP TS 33.102: "3G Security; Security Architecture".

[5] 3GPP TS 22.246 "MBMS User Services"

[6] IETF RFC 2617 "HTTP Digest Authentication"

[7] 3GPP TS 33.220 "Generic Bootstrapping Architecture (GBA)"

********END CHANGE**********

********BEGIN CHANGE**********

6 Security mechanisms

6.1 Authentication and authorisation of a user

Editor's note: this section will contain the details of how a user joins a particular Multicast Service

When the user wants to join MBMS user service, it shall use HTTP digest authentication [6] 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 [7]. The BM-SC is used as NAF.

The following adaptations apply to HTTP digest:

- The transaction identifier as specified in [7] is used as username
- MRK (MBMS service Request Key) is used as password. If GBA_ME has been run, the ME and BM-SC derive MRK from Ks_NAF. If GBA_U has been run, the ME and BM-SC derive the MRK from Ks_ext_NAF.
- 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.

********END CHANGE**********