3GPP TSG-SA WG3 Meeting #37
Sophia Antipolis, France, February 21-25, 2005

Tdoc ⌘S3-050124

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **056** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*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:	⌘	Protection of MBMS Service Announcement sent over MBMS bearer
Source:	⌘	MBMS drafting group
Work item code:	⌘	MBMS
Date:	⌘	22/02/2005
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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change:	⌘	It is considered not practical to protect service announcements in case they are sent over MBMS Bearer.
Summary of change:	⌘	The service announcements are not protected.
Consequences if not approved:	⌘	It is not specified whether MBMS service announcements are protected.

Clauses affected:	⌘	6.3.2.2.2, B.1

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

Other comments: ⌘

===== **BEGIN CHANGE** =====

6.3.2.2.2 Initiation of key management

When a UE has received User Service information via User Service Discovery / Announcement procedures describing a MBMS User Service and the user has triggered the activation of that User Service, the UE should try to get the MSK(s) that will be used to protect the data transmitted as part of this User Service.

NOTE1: The User Service Discovery / Announcement procedures are specified in TS 26.346 [13]. It is out of the scope of the present specification how the UE receives the User Service information and how the User Service is triggered in the UE.

NOTE2: The user service announcements are not protected when sent over MBMS bearer.

The UE shall receive the following information via the User Service Discovery / Announcement procedures:

- Fully qualified domain name of the key management server (i.e. the BM-SC). This for the UE to know to which IP address to send the MSK request.
- Confidentiality protection: on / off.
- Integrity protection: on / off.
- UICC key management required: yes/ no.
- Identifiers of the MSKs needed for the User Service.

  The Key Number part of the MSK ID(s) shall be set to 0x0 to denote the current MSK. Specific Key Number values are not used since they may change over time and Key Group part of MSK ID is sufficient to identify the MSKs, see clause 6.3.2.1.
- Mapping information how the MSKs are used to protect the different User Service Sessions.

Editors' Note: The exact syntax of the service announcement information including security parameters, e.g. possible XML schema of the parameters and its MIME type are to be specified in SA4.

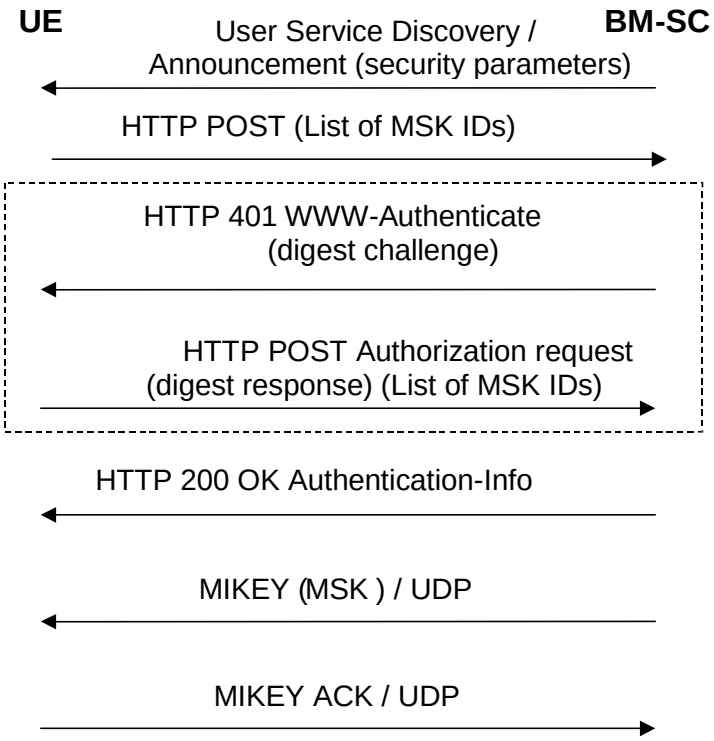

Figure 6.2a: MSK retrieval procedure

In case the UICC key management is required, the UE should only try to access the MBMS user service if the used UICC application is capable of MBMS key management.

The communication between the UE and the BM-SC is authenticated and integrity protected with HTTP Digest as described in clause 6.2.1 of this specification.

The UE requests for the MSKs using with the HTTP POST message.

The rest of the procedure is the same as in clause 6.3.2.3.1.

===== **NEXT CHANGE** =====

Annex B (informative): Security threats

B.1 Threats associated with attacks on the radio interface

The threats associated with attacks on the radio interface are split into the following categories, which are described in the following clauses:

- unauthorized access to multicast data;
- threats to integrity;
- denial of service;
- unauthorized access to MBMS services;
- privacy violation.

The attacks on the MBMS service announcements to the users on the radio interface are not discussed here~~,~~ because in case~~as~~ these are~~will most likely be~~ transferred on a point-to-point connection (e.g. PS signaling connection) they are~~, which is~~ already secured ~~today~~. In case the service announcement is transferred over HTTP, it is protected by HTTP Digest as defined in the current specification and/or it may be ~~(~~integrity protected and optionally encrypted at the RAN level~~)~~. In case the service announcements are sent over MBMS bearer, it is impractical to protect them.

===== **END CHANGE** =====