3GPP TSG-SA WG3 Meeting S3#37
Sophia, France, 21-25 February, 2005

Tdoc ⌘S3-050085

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **048** ⌘ **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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Requesting specific MSK
Source:	⌘	Ericsson
Work item code:	⌘	MBMS
Date:	⌘	14/2/2005
Category:	⌘	**B**
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:	⌘	Current TS 33.246 allows the UE to request only the current MSK from the BM-SC. This is done by setting the Key Number part of MSK-ID to zero. However, there are likely to be situations where the UE should be able to ask for other MSK s than the current one. An example of such a situation could be where the UE has downloaded two objects that are protected with different MSKs. If the UE has missed the push key update of the first object, the UE has no means to request the corresponding MSK. Additionally, in order to avoid that many UEs request a specific MSK at the same time and therefore cause congestion, UEs should re-use the "back-off" mechanism that is used within 'Associated delivery procedures' in TS 26.346. Usage of this mechanism should be optional to use but mandatory to implement. This is indicated in the Service Announcement information.
Summary of change:	⌘	UEs are able to request specific MSKs from the BM-SC, i.e. Key Number is set to specific value (other than zero). UEs should use the back-off mechanism specified in TS 26.346 to avoid that many UEs request the MSK at the same time.
Consequences if not approved:	⌘	UEs may not be able to decrypt delivered data.

Clauses affected:	⌘	6.3.2.1, 6.3.2.2.1, 6.3.2.2.2, 6.3.2.3.1			
		Y	**N**		
Other specs	⌘	**Y**		Other core specifications	⌘ TS 26.346 should have back off parameters optionally related to every MSK in the service announcement
Affected:			**N**	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

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

6.3.2.1 MSK identification

Every MSK is uniquely identifiable by its Key Domain ID MSK ID

where

Key Domain ID = MCC || MNC and is 3 bytes long.

MSK ID is 4 bytes long and with byte 0 and 1 containing the Key Group part, and byte 2 and 3 containing the Key Number part. The Key Number part is used to distinguish MSKs that have the same Key Domain ID and Key Group part. Key Group part is used to group keys together in order to allow redundant MSKs to be deleted. The MSK ID is carried in the extension payload of MIKEY extension payload.

NOTE: It needs to be ensured that the Key Group parts are unique within an operator, i.e. two BM-SCs within an operator shall not use the same Key Group value.

If the UE receives an MSK and already contains two other MSKs under the same Key Domain ID and Key Group part, then the UE shall delete the older of these two MSKs.

~~Editor's Note: The handling of MSKs may need some enhancement to cover download services, where the MSK is fetched after the UE has received the encrypted data.~~

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

6.3.2.2.1 Basic MSK retrieval procedure

When a UE detects that it needs the MSK(s) for a specific MBMS User service, the UE should try to get the MSKs that will be used to protect the data transmitted as part of this User Service. In the MSK request the UE shall list the MSK IDs for which the UE needs the MSK(s).

The basic MSK retrieval procedure is a part of different other procedures, e.g.:

- initiation of key management when the UE has joined the MBMS user service;
- retrieval of MSK(s) when the UE has missed a key update procedure e.g. due to being out of coverage.
- BM-SC solicited pull.

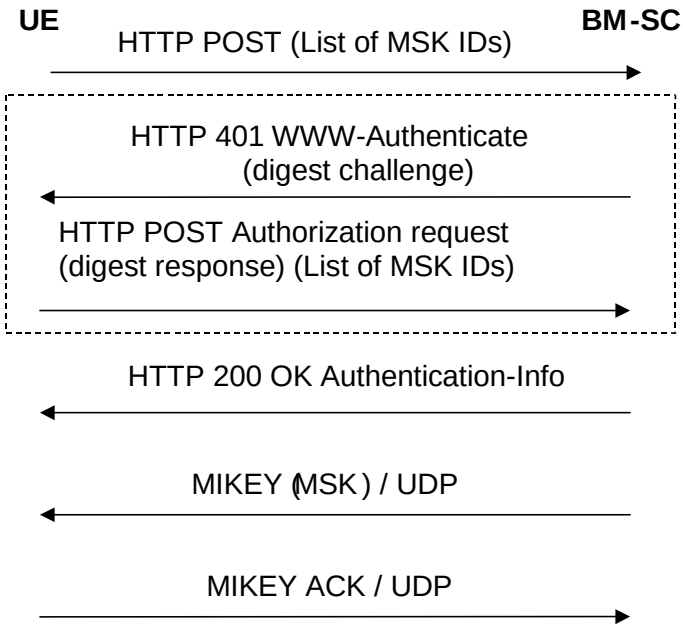

Figure 6.1: Basic MSK retrieval procedure

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 WITH the HTTP POST message. The following information is included in the HTTP message.

- key identification information: a list of MSK IDs.

~~NOTE:~~ UEs may request specific MSKs by setting the Key Number part of the MSK ID to the requested value. When the Key Number part of the MSK ID is set to 0x0, this means the current MSK, see clause 6.3.2.1.

Editors' Note: The exact syntax of the HTTP request message, e.g. possible XML schema of the request parameters in the client payload and its MIME type are to be specified in stage 3.

The BM-SC authenticates the UE with HTTP Digest using the keys received from GBA as described in clause 6.2.1 and verifies that the subscriber is authorized to receive the MSKs for this service.

If the authentication is successful then the BM-SC sends a HTTP 200 OK message with Authentication-Info header. If the authentication fails then the BM-SC resends HTTP 401 Authorization required message with the WWW-Authenticate header.

Editors' Note: The exact syntax of the HTTP response message, e.g. possible XML schema of the success or failure parameters in the client payload and its MIME type are to be specified in stage 3.

The UE checks the validity of the HTTP response message. If the message indicated failure, the UE may retry or leave the User Service.

If the HTTP procedure above resulted to success, the BM-SC initiates MIKEY message procedures over UDP transporting the requested MSKs to the UE.

If it was requested by the BM-SC, the UE sends a MIKEY acknowledgement message to the BM-SC.

If the UE fails to get hold of the MSK or receives no confirmation that no updated MSK is necessary or available at this time, then, unless the UE has a still-valid, older MSK, the UE shall leave the MBMS user service

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.

NOTE: 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.

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.
- Back off mode parameters, as defined in [13], may be specified in association with each MSK ID if wanted by the service provider. Back off mode is used to avoid congestion in MSK requests and it is mandatory to implement but optional to use.

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.

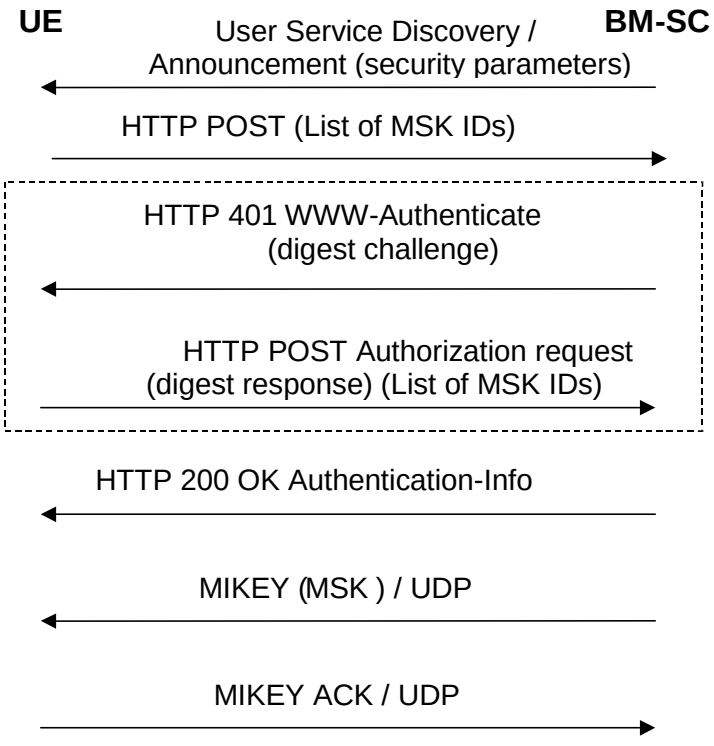

Figure 6.2a: MSK retrieval procedure

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 *****

6.3.2.3.1 Pushing the MSKs to the UE

The BM-SC controls when the MSKs used in a multicast service are to be changed. The below flow describes how MSK changes are performed.

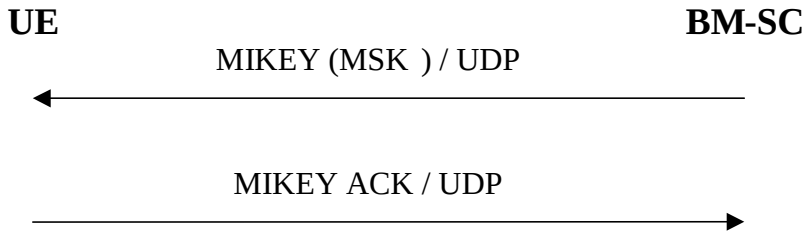

Figure 6.3: Pushing the MSKs to the UE

When the BM-SC decides that it is time to update the MSK, the BM-SC sends MIKEY message over UDP transporting the requested MSKs to the UE.

The BM-SC may also refrain from sending the MSK update message to the UE and let the UE request for the MSK. This may be needed in some download services where the UE fetches the MSK after receiving encrypted download object. In this case the back-off mode as described in 6.3.2.2.2 should be used.

If requested by the BM-SC, the UE sends a MIKEY acknowledgement message to the BM-SC.