

CHANGE REQUEST

33.246 CR 041
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: | Clarify the usage of the MUK in the BM-SC solicited pull procedure | | |
| Source: | Gemplus, Axalto | | |
| Work item code: | MBMS | Date: | 10/02/2005 |
| Category: | F | Release: | Rel-6 |
| | <p>Use <u>one</u> of the following categories:</p> <p>F (correction)</p> <p>A (corresponds to a correction in an earlier release)</p> <p>B (addition of feature),</p> <p>C (functional modification of feature)</p> <p>D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p> | | <p>Use <u>one</u> of the following releases:</p> <p>Ph2 (GSM Phase 2)</p> <p>R96 (Release 1996)</p> <p>R97 (Release 1997)</p> <p>R98 (Release 1998)</p> <p>R99 (Release 1999)</p> <p>Rel-4 (Release 4)</p> <p>Rel-5 (Release 5)</p> <p>Rel-6 (Release 6)</p> <p>Rel-7 (Release 7)</p> |

| | |
|--------------------------------------|---|
| Reason for change: | It may happen that the UE has generated a MUK/MRK pair but the BM -SC was not informed. The UE shall store the last MUK successfully used by the BM-SC in case that the BM-SC does not use the last generated MUK for protecting the BM-SC solicited pull MIKEY message. Consequently, only one MUK can exist for the BM-SC (the last generated MUK) and two MUKs can exist for the UE: the last generated MUK and the MUK that was last successfully used by the BM-SC. In the current description of the BM-SC solicited pull procedure the terms "last MUK" or "last used MUK" or "last known MUK" are equally used, some clarification on the usage of the MUK is required. |
| Summary of change: | Clarify the usage of the MUK in the BM-SC solicited pull procedure. |
| Consequences if not approved: | Terms used to refer to the MUK in the BM-SC solicited pull procedure are misleading. |

| | | | | | | | |
|------------------------------|--|---------------------|---|--------------------------|-------------------------------------|---------------------------|--|
| Clauses affected: | 6.3.2.2.4 | | | | | | |
| Other specs affected: | <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;">Y</td> <td style="text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> | Y | N | <input type="checkbox"/> | <input checked="" type="checkbox"/> | Other core specifications | |
| Y | N | | | | | | |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | | | | | | |
| | <input checked="" type="checkbox"/> | Test specifications | | | | | |
| | <input checked="" type="checkbox"/> | 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.

6.3.2.2.4 BM-SC solicited pull

While the push is the regular way of updating the MSK to the UE, there may be situations where the BM-SC solicits the UE to contact the BM-SC and request for new MSK. An example of such a situation is when the BM-SC wants the UE to trigger a UE that it needs to update the MSK.

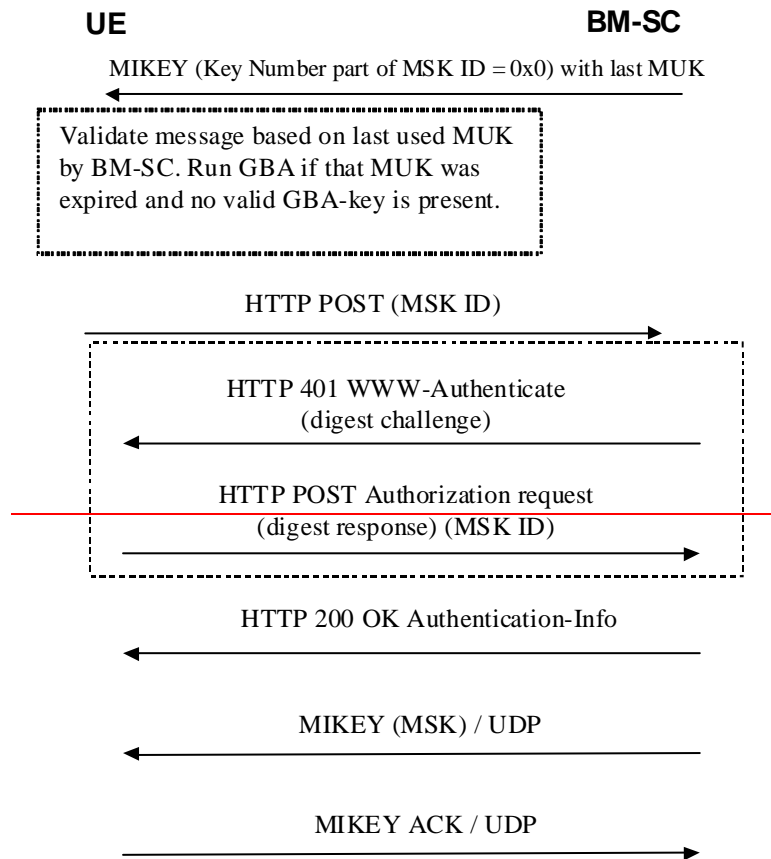


Figure 6.2b: BM-SC solicited pull

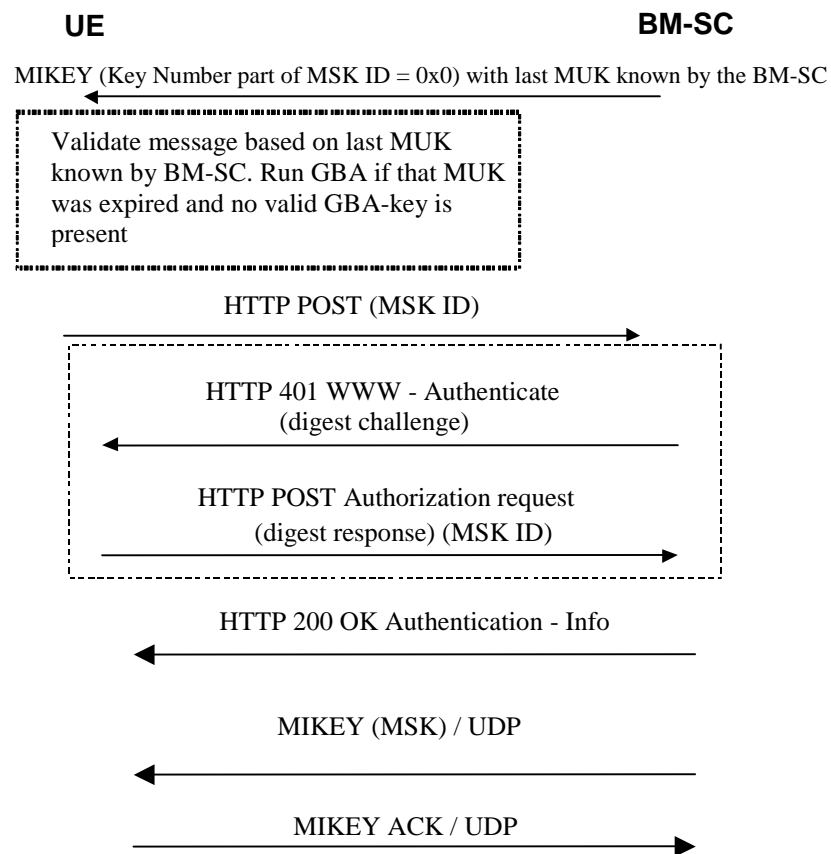


Figure 6.2b: BM-SC solicited pull

The BM-SC sends a MIKEY message over UDP to the UE. The MIKEY message shall be protected by the **most recent last** MUK known by the BM-SC. The Key Number part of the MSK ID in the extension payload of the MIKEY message shall be set to 0x0 to indicate that the UE should request for current MSK from the BM-SC.

If the last MUK known by the BM-SC does not correspond to the last MUK known by the UE, then the UE checks the solicited pull MIKEY message with the last MUK successfully used by the BM-SC.

NOTE 1: A MUK may be used by the BM-SC beyond the GBA key lifetime of the corresponding Ks_xx_NAF for the purpose of using the MUK within the first MIKEY message of a push solicited pull procedure.

NOTE 2: Since the integrity of the MIKEY message still needs to be assured, a KEMAC payload shall be included in the MIKEY message from the BM-SC. There is however no key present in the message. Thus by setting the Encr data len field to zero, only the MAC of the message will be included.

When receiving the message, the UE shall request for the current MSK for the specified Key Group. The BM-SC may trigger re-authentication of the UE or even re-run of GBA procedure to update the MUK as is described in TS 33.220 [6].

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