3GPP TSG-SA WG3 Meeting #37 ***Tdoc ⌘S3-050076***
Sophia Antipolis, France, 21-25 February 2005

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **040** ⌘ **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⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarify Time Stamp verification in MSK Verification Message procedure
Source:	⌘	Gemplus, Axalto
Work item code:	⌘	MBMS
Date:	⌘	10/02/2005
Category:	⌘	**F**
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:	⌘	According to the current MSK Verification Message procedure the UICC verifies that "the Time Stamp MIKEY field corresponds to the previous MSK Update message". This is not clear whether this "previous" Time Stamp is maintained per MUK ID or per UICC. A counter per UICC is not possible since it would introduce some threats. E.g the UICC could sign arbitrary message. So, the UICC shall compare the Time Stamp MIKEY message with the Time Stamp of the last accepted MSK Update procedure of the related MUK ID.
Summary of change:	⌘	Clarify that the Time Stamp MIKEY fied corresponds to the Time Stamp of the last accepted MSK Update procedure of the related MUK ID.
Consequences if not approved:	⌘	The Time Stamp verification in MSK Verification Messasge procedure is ambiguous.

Clauses affected:	⌘	Annex D.2			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

D.2 MSK Verification Message Generation

This procedure is part of the MSK Verification Message as described in clause 6.4.5.2 (MSK Verification message).

The ME constructs the verification message in response to the MSK-transport message when it is required by BM-SC.

The ME shall then give the constructed MIKEY verification message, with an empty MAC field, to the UICC. The ME also includes in this request NAF_Id to identify the stored Ks_int_NAF=MUK to be used in the MSK Verification Message Generation.

The UICC will verify that the Time Stamp MIKEY field correspond to the ~~previous MSK Update procedure~~ Time Stamp of the last accepted MSK Update procedure of the related MUK ID. Then, the UICC shall compute and send the MIKEY packet to the ME (including the calculated MAC field) as defined in clause 6.4.5.2. (MSK Verification message).

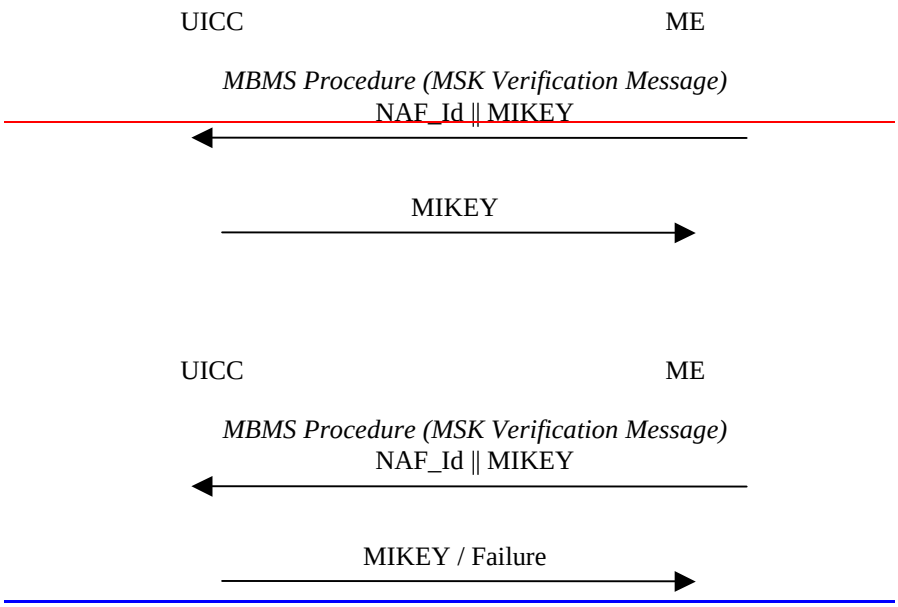

Figure D.2: MSK Verification Message