3GPP TSG-SA3 Meeting #37
Sophia Antipolis, France, 21.-25.02.2005

Tdoc ⌘S3-050051

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.200** **CR** **026** ⌘**rev** **-** ⌘ Current version: **6.0.0** ⌘

*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 **X**

Title:	⌘	Improving the robustness of the TCAP handshake mechanism
Source:	⌘	Vodafone, T-Mobile
Work item code:	⌘	SEC1-MAP
Date:	⌘	08/02/2005
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:	⌘	The current wording of MEAS-2 is vague and doesn't require a secure allocation of TCAP transaction-ids. It cannot be used for checking the compliance of network elements. Therefore the wording of MEAS-2 is enhanced to ensure that a robust TCAP handshake solution can be realised. An alternative measure to TCAP unpredictability measure is also introduced.
Summary of change:	⌘	The unpredictability of the TCAP transaction-id is expressed more precisely. In particular, two options are described of which one is mandatory for implementation: 1) it is specified that the TCAP transaction-id in the third message is predictable with a probability of less than 1/1000. This figure was selected to ensure that the overhead for an attacker to mount a successful attack is sufficiently large (i.e. he would have to send 100 Million TCAP messages in order to deliver 100.000 fraudulent SMSs), whilst ensuring that a relatively simply allocation scheme could be used for the 32 bit transaction-id. It is also specified that that attacker is assumed to know all previous TCAP transaction ids. This is done because a less stringent but more realistic assumption would be very complicated to specify. Furthermore, it should be relatively easy to address the 1/1000 unpredictability requirement even in the unlikely event that the attacker does know the sequence of all previous TCAP transaction ids that were issued by the node. 2) It is specified that the receiving node has to wait n seconds after sendig the second message before processing the third message. During this timeframe the network which (spoofed) address is used in the first message has the chance to abort the transaction (as a reaction of receiving the unexpected

		second message.
Consequences if not approved:	⌘	May lead to insecure implementations if the robustness of the TCAP handshake is not improved.

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

Annex C (normative): Using TCAP handshake for Mobile Terminated SMS transfer

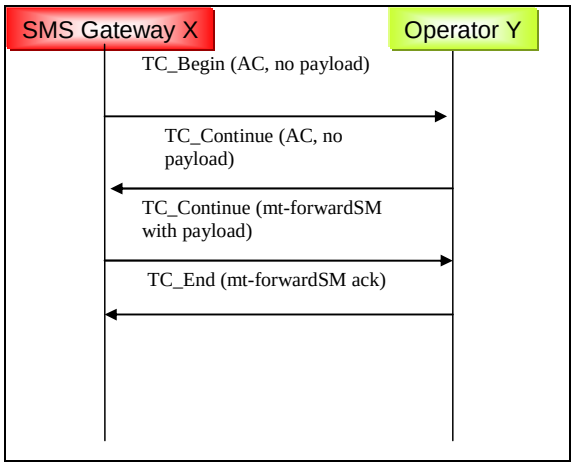

Figure B.1: MAP mt-Forward-SM messages using a TCAP Handshakes

The SMS Gateway operator and the serving node (MSC or SGSN) operator may agree to use the TCAP handshake as a countermeasure against SMS fraud for messages exchanged between their networks (for detailed message flows see TS 29.002 [4]). A limited level of authenticity is provided by the following mechanism: If the serving network receives an mt-forward-SM MAP message which uses the TC_Continue to transfer the MAP payload then it is guaranteed that the SCCP calling party address of the (empty) TC_Begin message is authentic, otherwise the first TC-continue message would be sent to the falsified address. The correct message flow is guaranteed by the TCAP transaction capabilities (use of Transaction ID).

Unfortunately there are some ways in which a fraudulent SMS Gateway operator (called the originator in bullets (a) and (b)) may try to circumvent the implicit SCCP address authentication provided by the TCAP handshake.

(a) The originator includes a falsified SMS-GMSC address within the mt-forward-SM payload carried by the TC-continue (third message in figure B.1)

(b) The originator tries to predict the TCAP transaction ID assigned by the serving node, which is to be used within the third message, and spoofs the third message without waiting for the second message. This attack has to be carried out within the right time window.

If TCAP handshake is to be used, the following measure shall be taken within the network of the serving node in order to counteract the spoofing possibilities of a malicious mt-Forward-SM originator.

MEAS-1: The receiving network shall verify if the received SMS-GMSC address (in the third message) may be used from the originating SCCP-address. Some operators use a single SMS-GMSC address for a range of originating SCCP addresses and this will need to be taken into consideration.

If TCAP handshake is to be used, at least one of ~~t~~The following measures ~~may~~ shall be taken within the network of the serving node in order to counteract the spoofing possibilities of a malicious mt-Forward-SM originator.

MEAS-2a: The receiving node ~~may~~shall use mechanisms to ensure that the destination TCAP transaction ID which needs to be used within the third message is predictable with a probability of less than 1/1000 for a third party knowing all previous TCAP transaction ID ~~tid~~ values.

MEAS-2b: The receiving network shall wait n seconds before it processes the third message (TC-continue(mt-forwardSM with payload)). This should ensure that the TC abort from the spoofed network is processed at the destination node earlier than a TC continue including a successfully guessed TCAP Transaction ID value.

~~The receiving node may use mechanisms to further enhance the unpredictability of the destination TCAP transaction ID which need to be used within the third message.~~

~~NOTE: The combined check (MEAS 1) on SCCP calling party address / SMS-GMSC address and destination TCAP Transaction ID makes spoofing of the second TC_CONTINUE (with payload) practically difficult. MEAS 2 is an optional enhancement that could be used to further enhance the resistance these attacks.~~

The following grouping method may be used for an operator to gradually introduce the TCAP handshake for mt-Forward-SM messages. Define an ‘operator group-1’ as a trusted operator group and ‘operator group-2’ as an un-trusted operator group. Agree that group-1 uses the TCAP handshake, while group-2 does not use the TCAP handshake. As specified by TS 29.002 [4] this requires that the SMS Gateway operators belonging to group-1 shall either use application context2 or 3 for mt-Forward-SM. The management of the two groups requires that the serving network shall implement a policy table of originating SCCP-addresses for which a TCAP handshake is required.

If the above described grouping method is used then the following measure shall be taken at the serving network in order to counteract the spoofing possibilities of a malicious mt-Forward-SM originator that tries to circumvent the policy table checks.

MEAS-3: The serving network shall verify that the originating SCCP address of a first message with a payload (i.e. not using the TCAP handshake) is not from an SMS-GMSC-address that shall use the TCAP handshake.

The benefit gained for operators that belong to group-1 is that spoofing of their SMS-GMSC-addresses ~~cannot be spoofed~~is practically difficult if the policy table has been administrated accurately.