3GPP TSG CN Plenary Meeting #27 **NP-050040**
9th – 11th March 2005 Tokyo, JAPAN.

Source: TSG CN WG4

Title: Corrections on MAP security

Agenda item: 9.3

Document for: APPROVAL

Doc-2nd-Level	Spec	CR	Rev	Phase	Subject	Cat	Ver_C
N4-050444	29.002	759	1	Rel-6	Addition of TCAP-Handshake for MO-ForwardSM	C	6.8.0

3GPP TSG-CN WG4 Meeting #26 ***N4-050444***

Sydney, Australia. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.002** **CR** 759 ⌘ **rev** **1** ⌘ Current version: **6.8.0** ⌘

*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:	⌘	Addition of TCAP-Handshake for MO-ForwardSM
Source:	⌘	CN4
Work item code:	⌘	TEI6
Date:	⌘	17/02/2005
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:	⌘	Recent addition of TCAP-Handshake does not protect against spoofed MO SMS
Summary of change:	⌘	Introduce a TCAP handshake before transmitting an MO-Short-Message as an operator option
Consequences if not approved:	⌘	The SMS Fraud problem remains unsolved

Clauses affected:	⌘	23.2, figures 23.2/2, 23.2/4, 23.2/5

Other specs affected: ⌘	Y	N		⌘
	X		Other core specifications	33.200
		X	Test specifications	
		X	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:

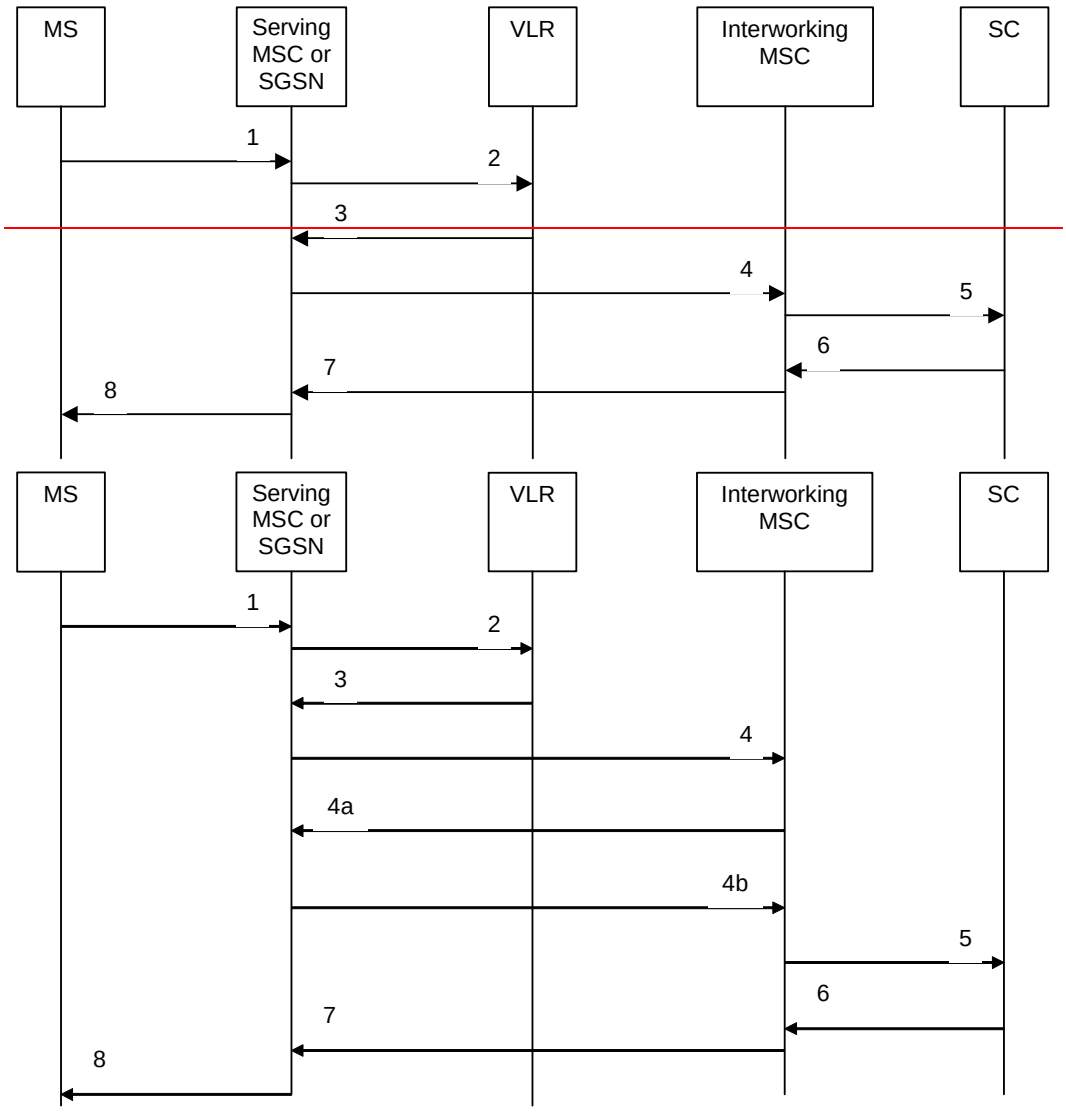
1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

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.

23.2 The mobile originated short message transfer procedure

The mobile originated short message service procedure is used to forward a short message from a mobile subscriber to a Service Centre. The message flow for the mobile originated short message service procedure is shown in figure 23.2/1.



1) Short Message (3GPP TS 24.011 [37]).
2) MAP_SEND_INFO_FOR_MO_SMS (*).
3) MAP_SEND_INFO_FOR_MO_SMS_ACK (*).
4) TCAP BEGIN (**)
4a) TCAP CONTINUE (**)
4b) MAP_MO_FORWARD_SHORT_MESSAGE.
5) Short message (3GPP TS 23.040).
6) Short message Acknowledgement (3GPP TS 23.040).
7) MAP_MO_FORWARD_SHORT_MESSAGE_ACK.
8) Short Message Acknowledgement (3GPP TS 24.011 [37]).
(*) Messages 2) and 3) are not used by the SGSN.
(**) If
a) the capacity of a message signal unit in the lower layers of the protocol is enough to carry the

content of the MAP_OPEN request and the content of the MAP_MO_FORWARD_SHORT_MESSAGE request in a single TC message

and

b1) the MAP signalling for short message transfer is protected by means of MAPsec

or

b2) the Interworking MSC operator and the serving node (MSC or SGSN) operator agreed not to use the TCAP handshake countermeasure against SMS fraud for messages exchanged between their networks (see 3GPP TS 33.200 [34a])

then

the TCAP handshake may be omitted.

Figure 23.2/1: Mobile originated short message transfer

In addition the following MAP services are used:

MAP_PROCESS_ACCESS_REQUEST	(see subclause 8.3); (*)
MAP_AUTHENTICATE	(see subclause 8.5); (*)
MAP_SET_CIPHERING_MODE	(see subclause 8.6); (*)
MAP_PROVIDE_IMSI	(see subclause 8.9); (*)
MAP_CHECK_IMEI	(see subclause 8.7);
MAP_FORWARD_NEW_TMSI	(see subclause 8.9); (*)
MAP_TRACE_SUBSCRIBER_ACTIVITY	(see subclause 9.1); (*)
MAP_READY_FOR_SM	(see subclause 12.4).

(*) These services are not used by the SGSN.

23.2.1 Procedure in the serving MSC

Any CAMEL-specific handling defined in this subclause is omitted if the MSC does not support CAMEL control of MO SMS, or if the subscriber does not have a subscription for CAMEL control of MO SMS.

The process starts when the MSC receives a short message from the MS. The process invokes macros not defined in this clause; the definitions of these macros can be found as follows:

Receive_Open_Cnf	see subclause 25.1.2;
Check_Indication	see subclause 25.2.1;
Check_Confirmation	see subclause 25.2.2.

Sheet 1: If the MSC is integrated with the SMS-IWMSC, it communicates directly with the Short Message Service Centre (SMSC) using one of the protocols described in 3GPP TS 23.039 [25a]; otherwise it communicates with the SMS-IWMSC using MAP.

Sheet 3: If the capacity of a message signal unit in the lower layers of the protocol is enough to carry the content of the MAP_OPEN request and the content of the MAP_MO_FORWARD_SHORT_MESSAGE request in a single TC message, the test "Message segmentation needed" takes the "No" exit; otherwise the test takes the "Yes" exit.

Sheet 3:The decision box "TCAP Handshake required" takes the "yes" or "no" exit depending on agreements between the serving MSC's operator and the SMS-IWMSC's operator (see 3GPP TS 33.200 [34a]).

The mobile originated short message service process in the MSC is shown in figure 23.2/2.

****

23.2.3 Procedure in the SGSN

Any CAMEL-specific handling defined in this subclause is omitted if the SGSN does not support CAMEL control of MO SMS, or if the subscriber does not have a subscription for CAMEL control of MO SMS.

The process starts when the SGSN receives a short message received from the MS over the Gb interface. The MAP process invokes macros not defined in this clause; the definitions of these macros can be found as follows:

Receive_Open_Cnf	see subclause 25.1.2;
Check_Confirmation	see subclause 25.2.2.

Sheet 2: If the capacity of a message signal unit in the lower layers of the protocol is enough to carry the content of the MAP_OPEN request and the content of the MAP_MO_FORWARD_SHORT_MESSAGE request in a single TC message, the test "Message segmentation needed" takes the "No" exit; otherwise the test takes the "Yes" exit.

Sheet 2:The decision box "TCAP Handshake required" takes the "yes" or "no" exit depending on agreements between the serving SGSN's operator and the SMS-IWMSC's operator (see 3GPP TS 33.200 [34a]).

The mobile originated short message service process in the SGSN is shown in figure 23.2/4.

23.2.4 Procedure in the SMS Interworking MSC (SMS-IWMSC)

This procedure applies only when the SMS-IWMSC is not integrated with the serving MSC or SGSN.

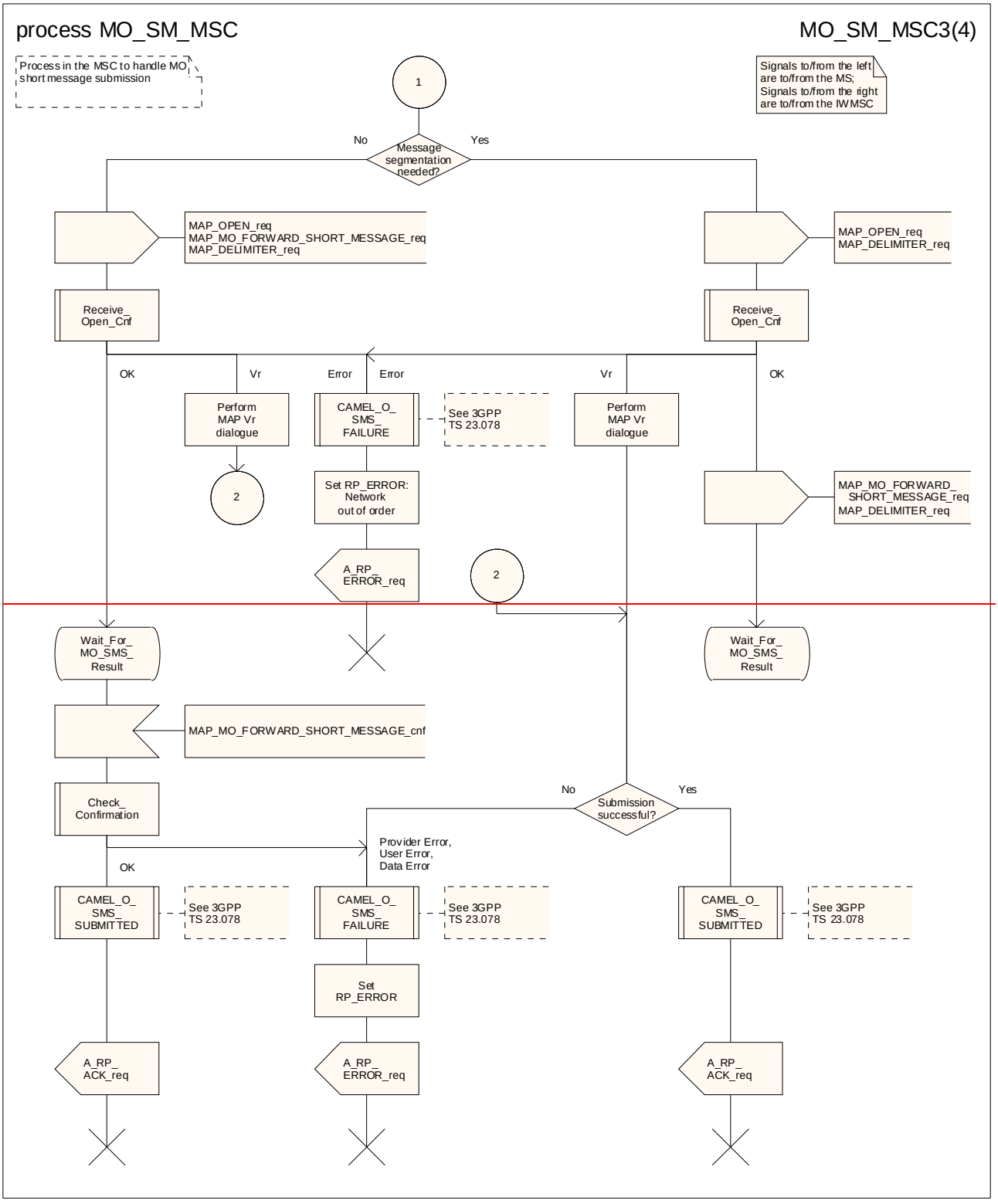
The process starts when the SMS-IWMSC receives a dialogue opening request with the application context shortMsgMO-RelayContext. The MAP process invokes macros not defined in this clause; the definitions of these macros can be found as follows:

Receive_Open_Ind	see subclause 25.1.1;
Check_Indication	see subclause 25.2.1.

Sheet 1:The decision box "TCAP Handshake required" takes the "yes" or "no" exit depending on agreements between the SMS-IWMSC's operator and the serving node's operator (see 3GPP TS 33.200 [34a]).

The mobile originated short message service transfer process in the SMS-IWMSC is shown in figure 23.2/5.

****


process MO_SM_MSC
MO_SM_MSC3(4)
Process in the MSC to handle MO short message submission
1
Signals to/from the left are to/from the MS; Signals to/from the right are to/from the IWMSC
No
Message segmentation needed?
Yes
MAP_OPEN_req
MAP_MO_FORWARD_SHORT_MESSAGE_req
MAP_DELIMITER_req
MAP_OPEN_req
MAP_DELIMITER_req
Receive_ Open_Cnf
Receive_ Open_Cnf
OK
Vr
Error
Error
Vr
OK
Perform MAP Vr dialogue
CAMEL_O_ SMS_ FAILURE
See 3GPP TS 23.078
Perform MAP Vr dialogue
2
Set RP_ERROR: Network out of order
MAP_MO_FORWARD_ SHORT_MESSAGE_req
MAP_DELIMITER_req
A_RP_ ERROR_req
2
Wait_For_ MO_SMS_ Result
Wait_For_ MO_SMS_ Result
MAP_MO_FORWARD_SHORT_MESSAGE_cnf
Check_ Confirmation
No
Submission successful?
Yes
Provider Error, User Error, Data Error
OK
CAMEL_O_ SMS_ SUBMITTED
See 3GPP TS 23.078
CAMEL_O_ SMS_ FAILURE
See 3GPP TS 23.078
CAMEL_O_ SMS_ SUBMITTED
See 3GPP TS 23.078
Set RP_ERROR
A_RP_ ACK_req
A_RP_ ERROR_req
A_RP_ ACK_req

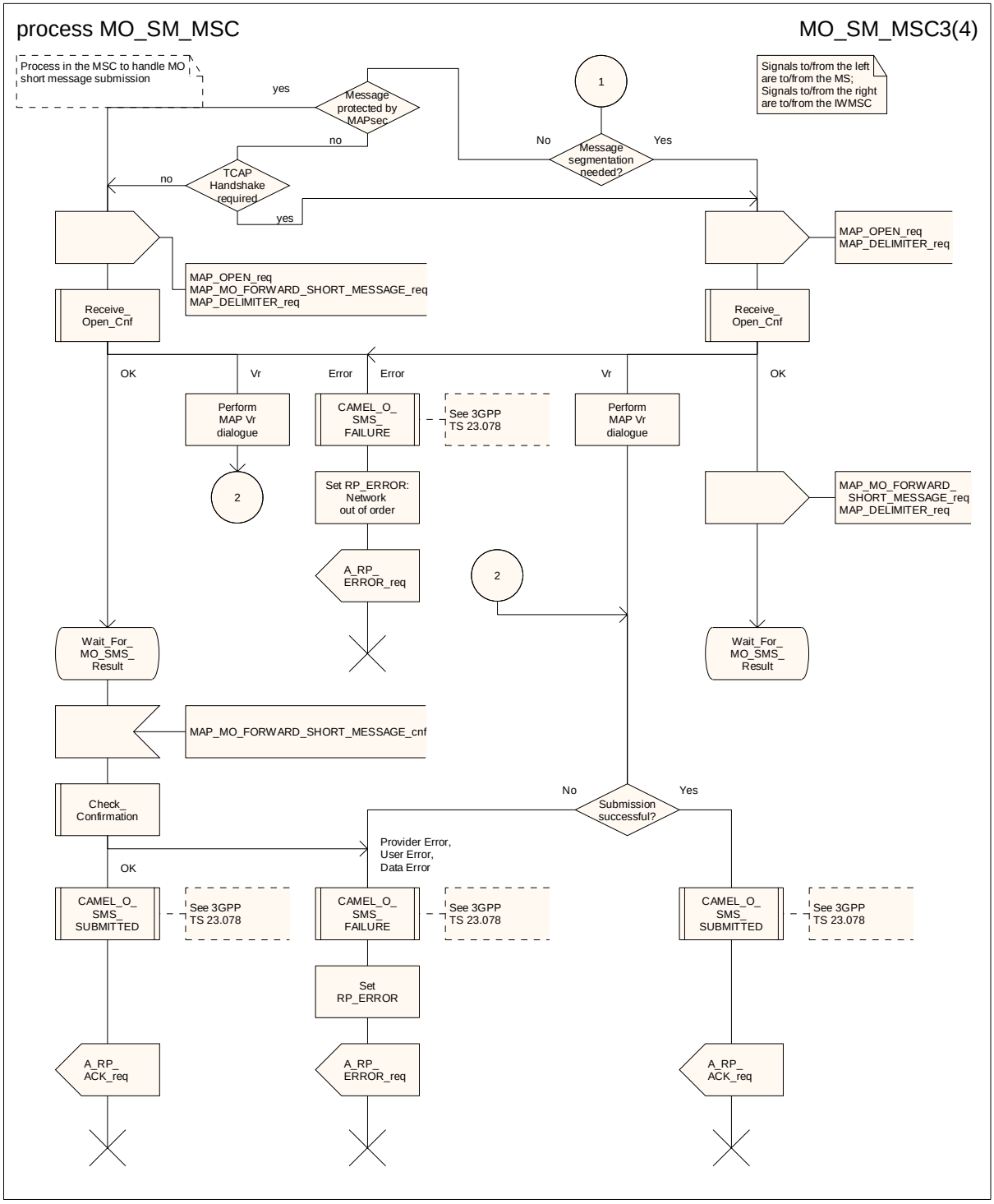
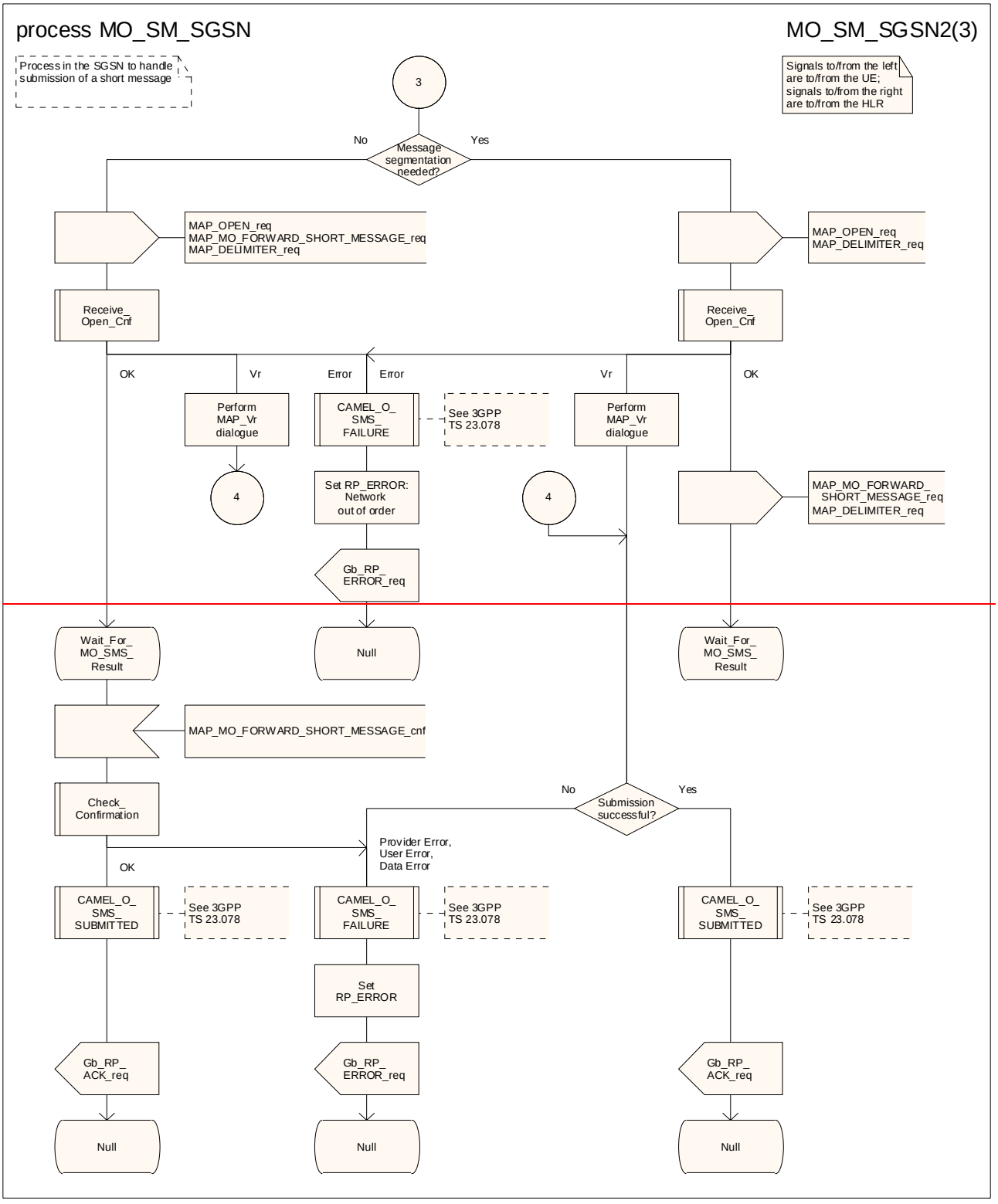


Figure 23.2/2 (sheet 3 of 4): Process MO_SM_MSC

****


process MO_SM_SGSN
MO_SM_SGSN2(3)
Process in the SGSN to handle submission of a short message
Signals to/from the left are to/from the UE; signals to/from the right are to/from the HLR
3
No
Message segmentation needed?
Yes
MAP_OPEN_req
MAP_MO_FORWARD_SHORT_MESSAGE_req
MAP_DELIMITER_req
MAP_OPEN_req
MAP_DELIMITER_req
Receive_ Open_Cnf
Receive_ Open_Cnf
OK
Vr
Error
Error
Vr
OK
Perform MAP_Vr dialogue
CAMEL_O_ SMS_ FAILURE
See 3GPP TS 23.078
Perform MAP_Vr dialogue
4
Set RP_ERROR: Network out of order
4
MAP_MO_FORWARD_ SHORT_MESSAGE_req
MAP_DELIMITER_req
Gb_RP_ ERROR_req
Wait_For_ MO_SMS_ Result
Null
Wait_For_ MO_SMS_ Result
MAP_MO_FORWARD_SHORT_MESSAGE_cnf
Check_ Confirmation
No
Submission successful?
Yes
Provider Error, User Error, Data Error
OK
CAMEL_O_ SMS_ SUBMITTED
See 3GPP TS 23.078
CAMEL_O_ SMS_ FAILURE
See 3GPP TS 23.078
CAMEL_O_ SMS_ SUBMITTED
See 3GPP TS 23.078
Set RP_ERROR
Gb_RP_ ACK_req
Gb_RP_ ERROR_req
Gb_RP_ ACK_req
Null
Null
Null

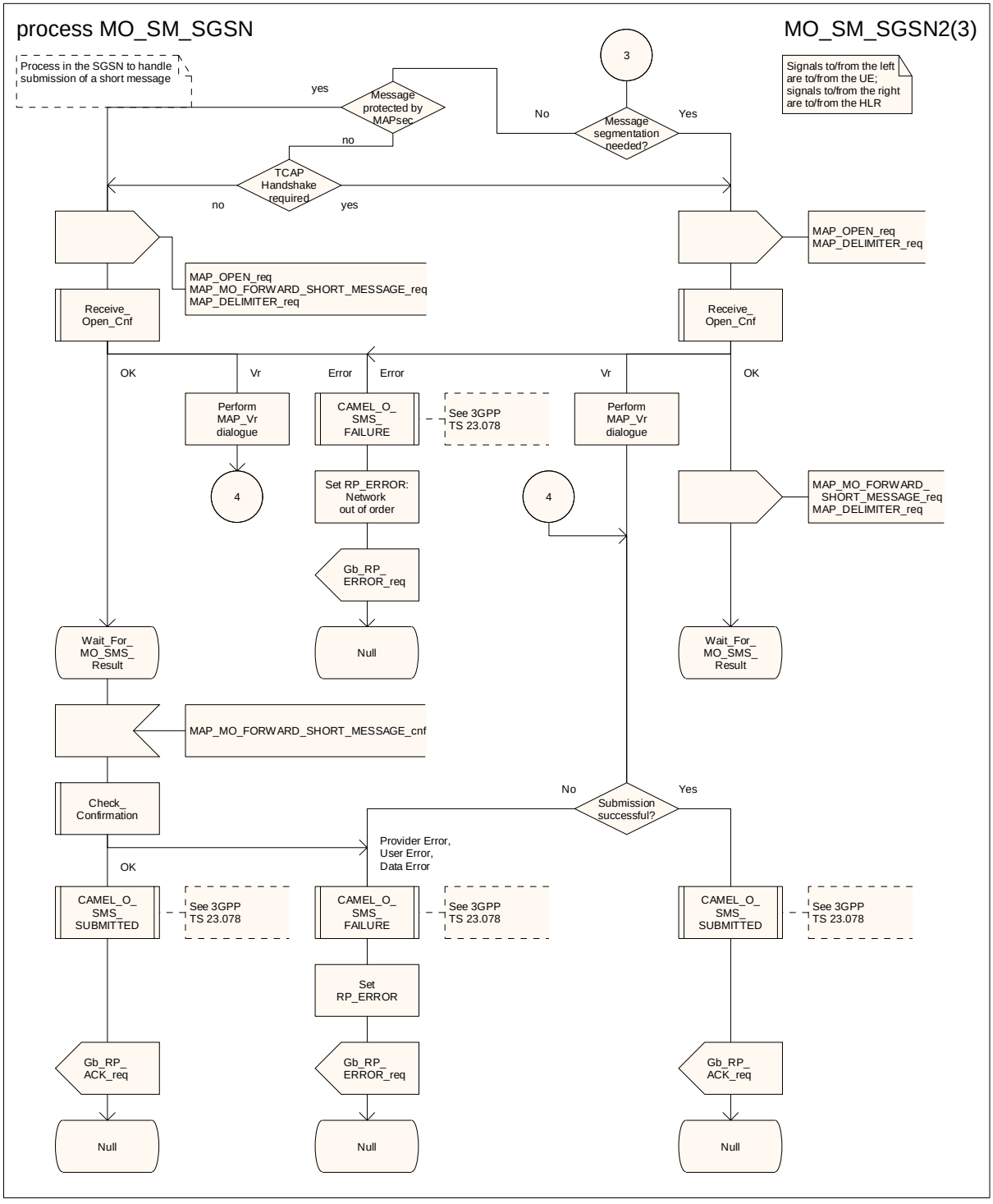
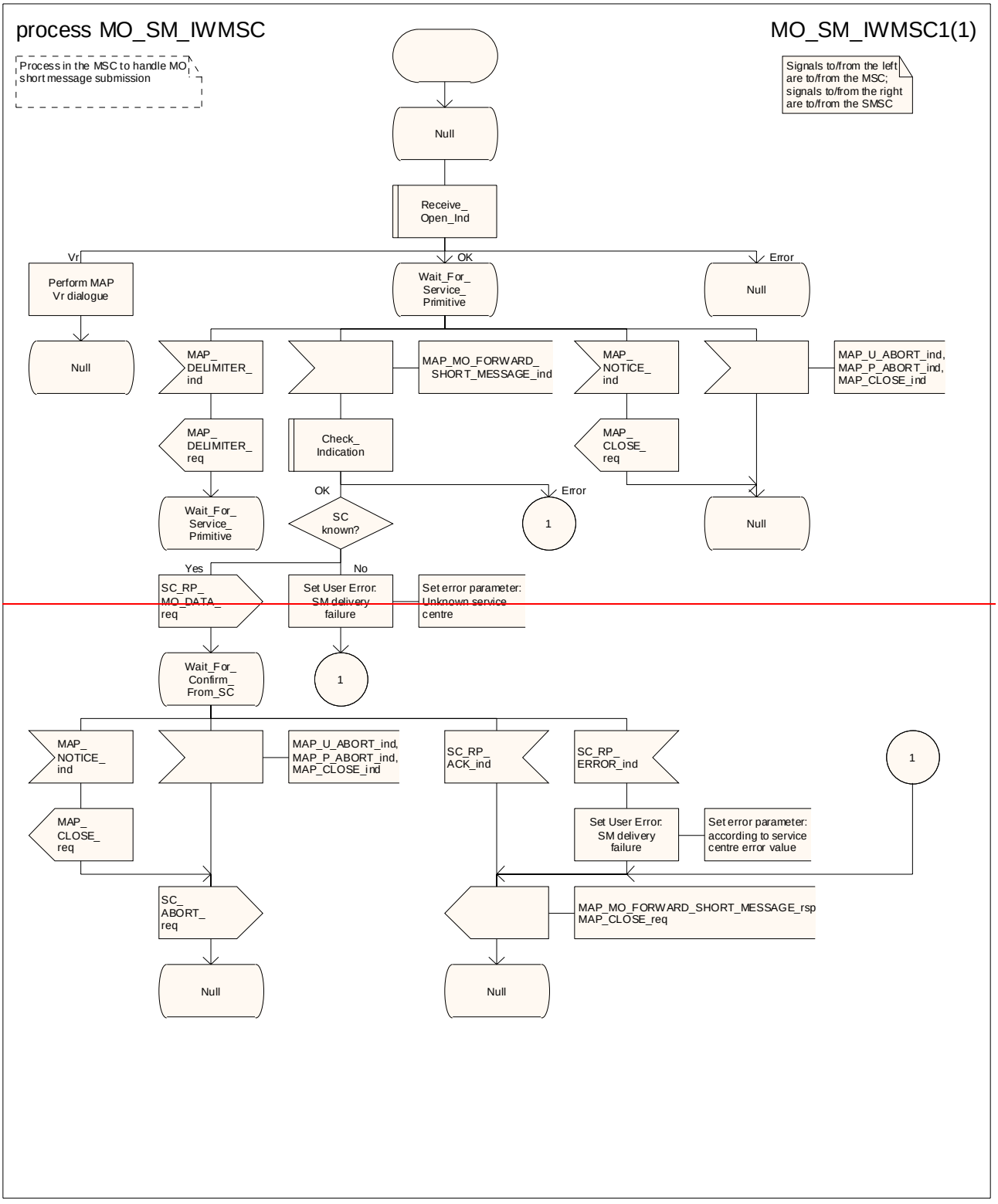


Figure 23.2/4 (sheet 2 of 3): Process MO_SM_SGSN

****


process MO_SM_IWMSC
MO_SM_IWMSC1(1)
Process in the MSC to handle MO short message submission
Signals to/from the left are to/from the MSC; signals to/from the right are to/from the SMSC
Null
Receive_ Open_Ind
Vr
OK
Error
Perform MAP Vr dialogue
Wait_For_ Service_ Primitive
Null
Null
MAP_ DELIMITER_ ind
MAP_MO_FORWARD_ SHORT_MESSAGE_ind
MAP_ NOTICE_ ind
MAP_U_ABORT_ind, MAP_P_ABORT_ind, MAP_CLOSE_ind
MAP_ DELIMITER_ req
Check_ Indication
MAP_ CLOSE_ req
OK
Error
Wait_For_ Service_ Primitive
SC known?
1
Null
Yes
No
SC_RP_ MO_DATA_ req
Set User Error: SM delivery failure
Set error parameter: Unknown service centre
Wait_For_ Confirm_ From_SC
1
MAP_ NOTICE_ ind
MAP_U_ABORT_ind, MAP_P_ABORT_ind, MAP_CLOSE_ind
SC_RP_ ACK_ind
SC_RP_ ERROR_ind
1
MAP_ CLOSE_ req
Set User Error: SM delivery failure
Set error parameter: according to service centre error value
SC_ ABORT_ req
MAP_MO_FORWARD_SHORT_MESSAGE_rsp MAP_CLOSE_req
Null
Null

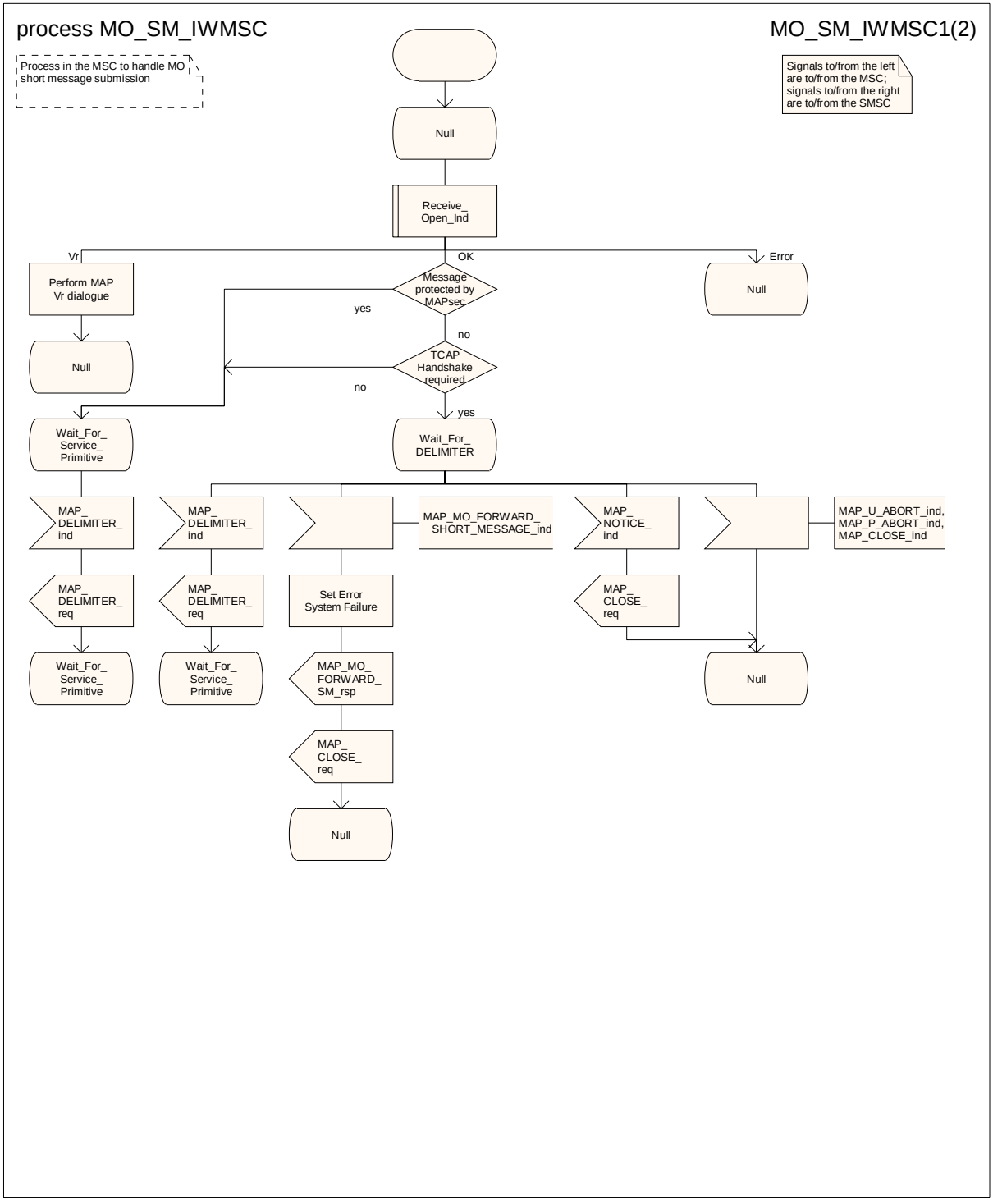


Figure 23.2/5 (sheet 1 of 2): Process MO_SM_IWMSC

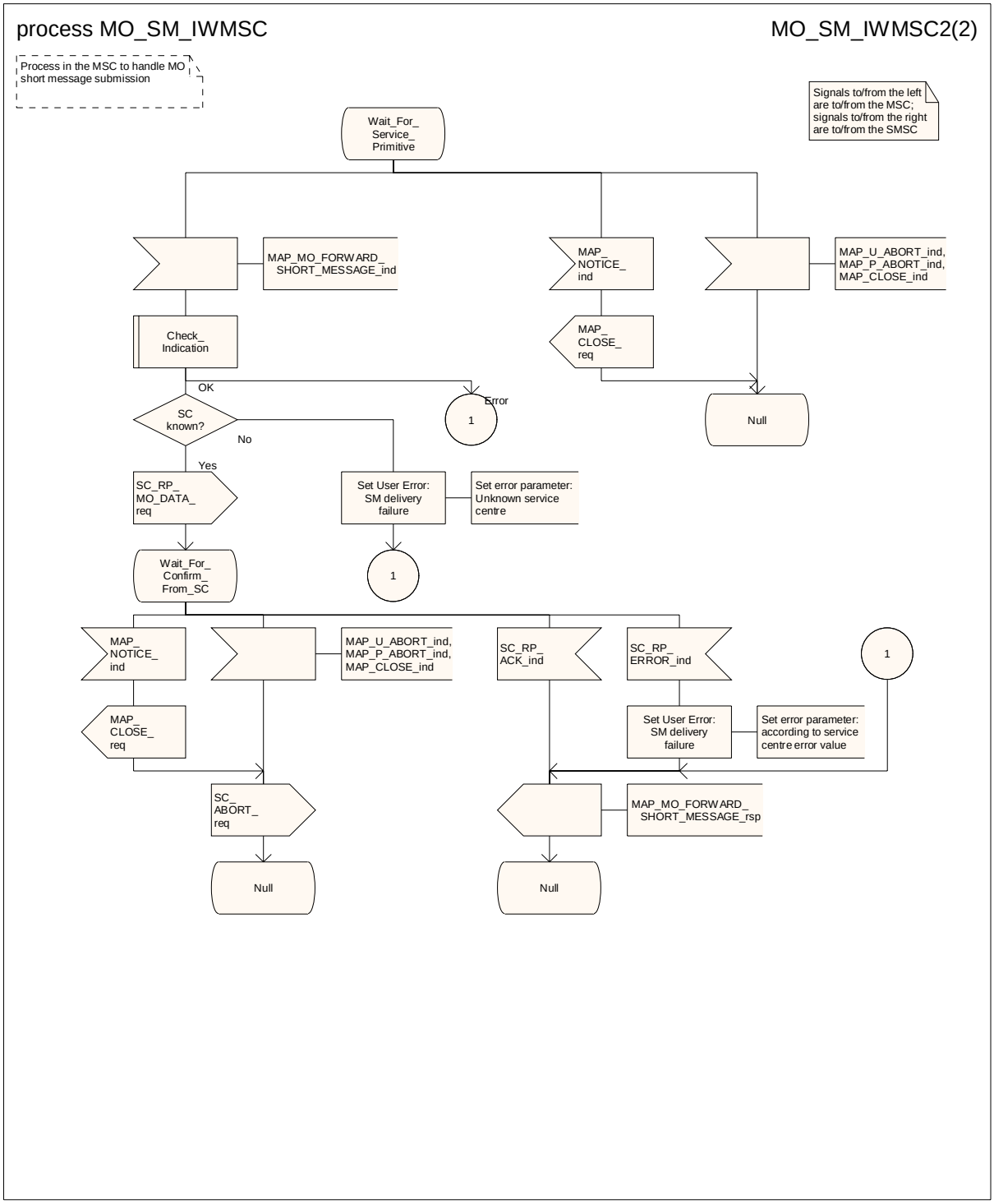


Figure 23.2/5 (sheet 2 of 2): Process MO_SM_IWMSC