3GPP TSG CN Plenary Meeting #26 **NP-040535**
8th – 10th December 2004 Athens, Greece.

Source: TSG CN WG4

Title: Corrections on MAP Security

Agenda item: 9.3

Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level N4-040	Phase	Subject	Cat	Ver_C
29.002	740	2	1641	Rel-6	SMS Fraud countermeasures	F	6.7.0

3GPP TSG-CN WG4 Meeting #25 ***N4-041641***

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘	**29.002**	**CR**	**740**	⌘**rev**	**2**	⌘	Current version:	**6.7.0**	⌘

*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:	⌘	SMS Fraud countermeasures			
Source:	⌘	CN4			
Work item code:	⌘	TEI6	***Date:***	⌘	18/11/2004
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:	⌘	To address the SMS Fraud scenario identified in S3-040581
Summary of change:	⌘	Introduce a TCAP handshake before transmitting an MT-Short-Message as an operator option
Consequences if not approved:	⌘	The SMS Fraud problem remains unsolved

Clauses affected:	⌘	23.3, figures 23.3/4, 23.3/6, 23.3/10				
		Y	**N**			
Other specs affected:	⌘	X		Other core specifications	⌘	33.200-023
			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.

23.3 The mobile terminated short message transfer procedure

The mobile terminated short message transfer procedure is used for forwarding a short message or several short messages from a Service Centre to a mobile subscriber. The message flow for the mobile terminated short message procedure for a single short message transfer is shown in figure 23.3/1.

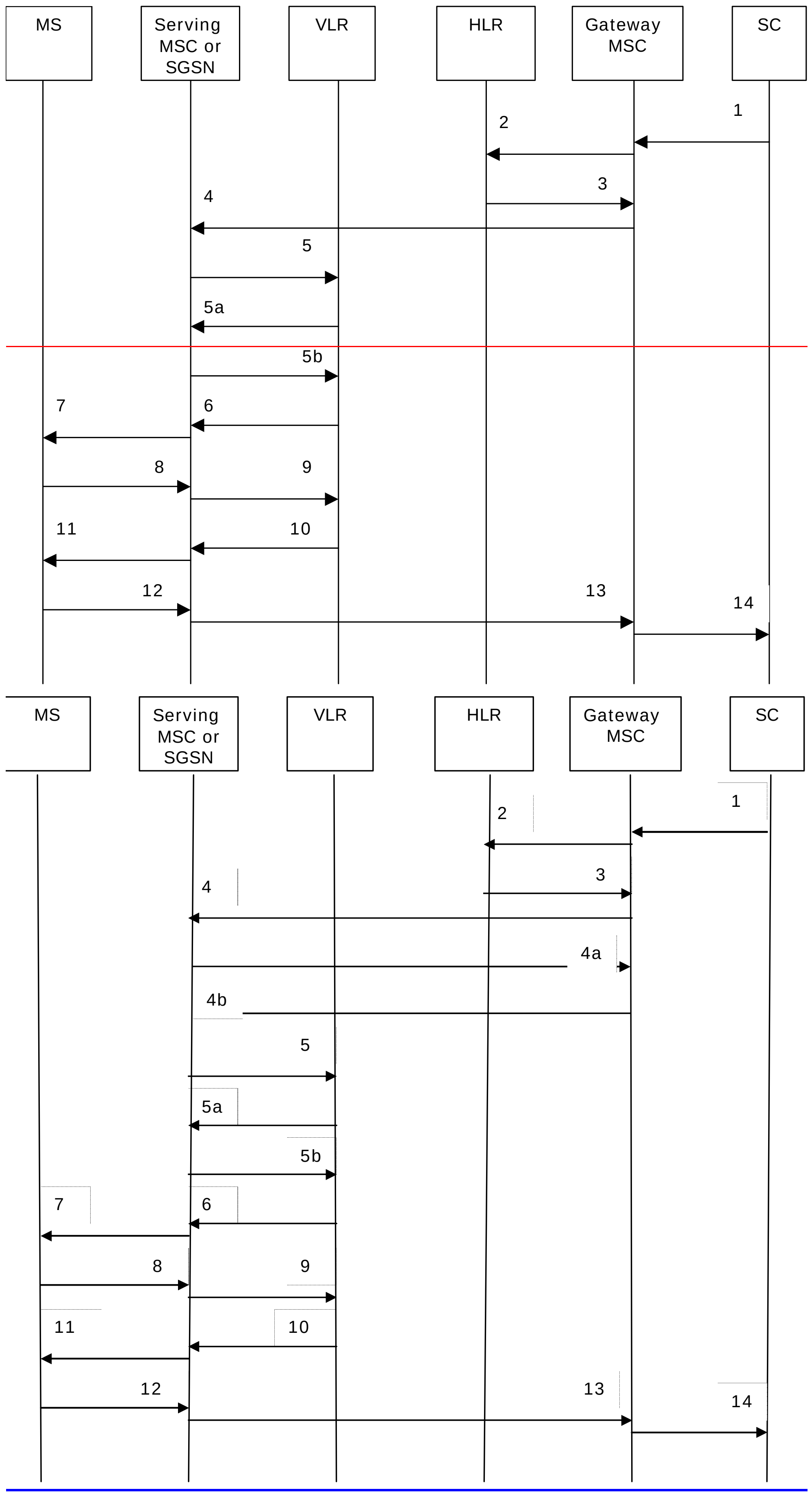


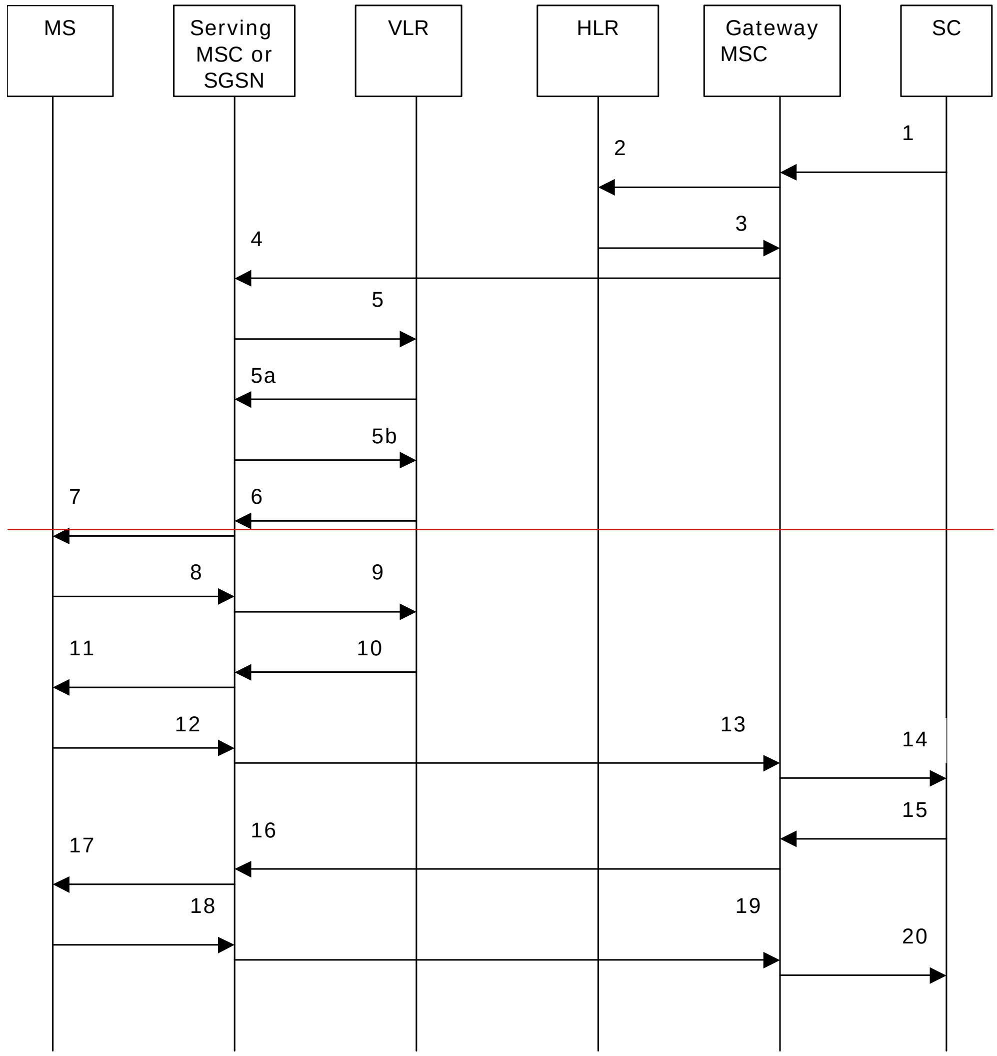
Figure 23.3/1: Mobile terminated short message service procedures

1) Short Message (3GPP TS 23.040).
2) MAP_SEND_ROUTING_INFO_FOR_SM.
3) MAP_SEND_ROUTING_INFO_FOR_SM_ACK.
4) TCAP BEGIN (***)
4a) TCAP CONTINUE (***)
4b) MAP_MT_FORWARD_SHORT_MESSAGE.
5) MAP_SEND_INFO_FOR_MT_SMS (*).
5a) MAP_CONTINUE_CAMEL_SMS_HANDLING (*)(**)
5b) MAP_SEND_INFO_FOR_MT_SMS (*)(**)
6) MAP_PAGE/MAP_SEARCH_FOR_MOBILE_SUBSCRIBER (*).
7) Page (3GPP TS 24.008 [35]).
8) Page response (3GPP TS 24.008 [35]).
9) MAP_PROCESS_ACCESS_REQUEST_ACK and
MAP_SEARCH_FOR_MOBILE_SUBSCRIBER_ACK (*).
10) MAP_SEND_INFO_FOR_MT_SMS_ACK (*).
11) Short Message (3GPP TS 24.011 [37]).
12) Short Message Acknowledgement (3GPP TS 24.011 [37]).
13) MAP_MT_FORWARD_SHORT_MESSAGE_ACK.
14) Short Message Acknowledgement (3GPP TS 23.040).

(*) Messages 5), 5a), 5b), 6), 9), and 10) are not used by the SGSN.
(**) These messages are used only for a subscriber provisioned with MT-SMS-CSI in the VLR.
(***) 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_MT_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 SMS Gateway 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.

The message flow for the mobile terminated short message procedure for multiple short message transfer is shown in figure 23.3/2.


MS
Serving MSC or SGSN
VLR
HLR
Gateway MSC
SC
1
2
3
4
5
5a
5b
7
6
8
9
11
10
12
13
14
15
16
17
18
19
20

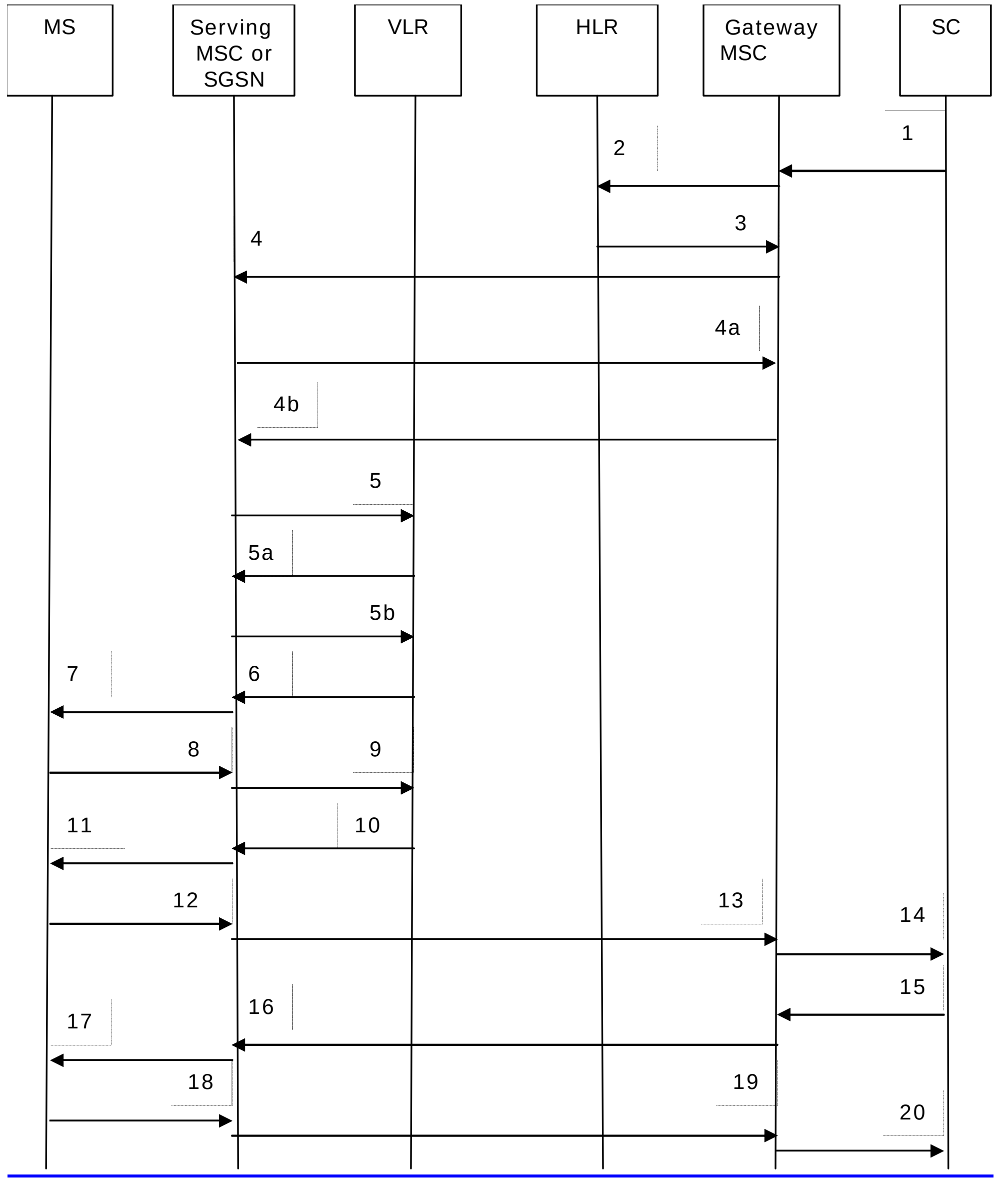


Figure 23.3/2: Mobile terminated short message procedure for multiple short message transfer

1) Short Message (3GPP TS 23.040).
2) MAP_SEND_ROUTING_INFO_FOR_SM.
3) MAP_SEND_ROUTING_INFO_FOR_SM_ACK.
4) TCAP BEGIN (***)
4a TCAP CONTINUE (***)
4b) MAP_MT_FORWARD_SHORT_MESSAGE (note 1).
5) MAP_SEND_INFO_FOR_MT_SMS (*).
5a) MAP_CONTINUE_CAMEL_SMS_HANDLING (*)(**)
5b) MAP_SEND_INFO_FOR_MT_SMS (*)(**)
6) MAP_PAGE/MAP_SEARCH_FOR_MOBILE_SUBSCRIBER (*).
7) Page (*3GPP TS 48.008 [49]*).
8) Page response (3GPP TS 24.008 [35]).
9) MAP_PROCESS_ACCESS_REQUEST_ACK and
MAP_SEARCH_FOR_MOBILE_SUBSCRIBER_ACK (*).
10) MAP_SEND_INFO_FOR_MT_SMS_ACK (*).
11) Short Message (3GPP TS 24.011 [37]).
12) Short Message Acknowledgement (3GPP TS 24.011 [37]).
13) MAP_MT_FORWARD_SHORT_MESSAGE_ACK.
14) Short Message Acknowledgement (3GPP TS 23.040).
15) Short Message (3GPP TS 23.040).
16) MAP_MT_FORWARD_SHORT_MESSAGE (note 2).
17) Short Message (3GPP TS 24.011 [37]).
18) Short Message Acknowledgement (3GPP TS 24.011 [37]).

19) MAP_MT_FORWARD_SHORT_MESSAGE_ACK.
20) Short Message Acknowledgement (3GPP TS 23.040).

(*) Messages 5), 5a), 5b) 6), 9), and 10) are not used by the SGSN.
(**) These messages are used only for a subscriber provisioned with MT-SMS-CSI in the VLR.
(***) 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_MT_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 SMS Gateway 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.

NOTE 1: The “More Messages To Send” flag is TRUE.
NOTE 2: The “More Messages To Send” flag is FALSE.

In the multiple short message transfer the service MAP_MT_FORWARD_SHORT_MESSAGE can be used several times. However, the short message transfer is always acknowledged to the Service Centre before the next short message is sent.

In addition the following MAP services are used:

MAP_PROCESS_ACCESS_REQUEST	(see subclause 8.3); (*)
MAP_PAGE	(see subclause 8.2); (*)
MAP_SEARCH_FOR_MS	(see subclause 8.2); (*)
MAP_AUTHENTICATE	(see subclause 8.5); (*)
MAP_SET_CIPHERING_MODE	(see subclause 8.6); (*)
MAP_CHECK_IMEI	(see subclause 8.7);
MAP_FORWARD_NEW_TMSI	(see subclause 8.9); (*)
MAP_REPORT_SM_DELIVERY_STATUS	(see subclause 12.3);
MAP_INFORM_SERVICE_CENTRE	(see subclause 12.6);
MAP_TRACE_SUBSCRIBER_ACTIVITY	(see subclause 9.1); (*)
MAP_READY_FOR_SM	(see subclause 12.4).

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

****

23.3.1 Procedure in the SMS-GMSC

Any CAMEL-specific handling described in this subclause is omitted if the SMS-GMSC does not support CAMEL. CAMEL-specific handling is invoked only if the SMS-GMSC is integrated with the VMSC.

The process starts when the SMS-GMSC receives an SC_RP_MT_DATA indication from a Service Centre. 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.

Process MT_SM_GMSC sheet 1: If the MAP_SEND_ROUTING_INFO_FOR_SM confirmation included an LMSI, it may be included in the sm-RP-DA information field of the first MAP_MT_FORWARD_SHORT_MESSAGE request sent to the serving MSC. In this case, the IMSI shall be included in the Destination Reference of the MAP_OPEN request. The SMS-GMSC shall not send an LMSI to an SGSN. If the SMS-GMSC does not send an LMSI to the serving node, the sm-RP-DA information field in the first MAP_MT_FORWARD_SHORT_MESSAGE request sent to the serving MSC or SGSN shall contain the IMSI, and the Destination Reference in the MAP_OPEN request shall not be present. The parameter SM_RP_OA shall contain the Service Centre address.

Process MT_SM_GMSC sheet 1: The indication of which number belongs to the SGSN and which to the MSC, received from the HLR in the MAP_SEND_ROUTING_INFO_FOR_SM confirm (see subclause 23.3.2) will enable the SMS-GMSC to map the causes received from one or both serving nodes into the appropriate causes for non GPRS, GPRS or both, and send them to the SC and the HLR.

Process MT_SM_GMSC sheet 2: The SMS-GMSC maps "Unexpected data value" and "System failure" MAP errors from the serving node to a "System failure" RP_ERROR error cause. The mapping between other MAP error causes and the RP_ERROR error cause is given in 3GPP TS 23.040 [26] and 3GPP TS 24.011 [37].

Process MT_SM_GMSC sheet 2: If the SMS-GMSC receives both MSC and SGSN numbers from the HLR as routeing information, it may choose which serving node to use for the first delivery attempt.

Process MT_SM_GMSC sheet 2: If the SMS-GMSC makes two delivery attempts, it may report the result of each delivery attempt to the HLR according to the conditions described below.

Procedure MT_SM_Delivery_Attempt_GMSC sheet 1: if the macro MT_SM_Transfer_MSC takes the Error exit, the SMS-GMSC maps the MAP User Error to the corresponding SC_RP error, as defined in 3GPP TS 23.040 [26].

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

Procedure MT_SM_Delivery_Attempt_GMSC sheet 1, sheet 2, sheet 4, sheet 5: The SMS-GMSC invokes the macro Report_SM_Delivery_Stat_GMSC if:

- the reason received from the serving node for failure to deliver the message is absent subscriber_SM, unidentified subscriber or SM delivery failure with error cause "MS memory capacity exceeded", and the SC address is not yet included in the MWD set, or

- the reason received from the serving node for failure to deliver the message is absent subscriber_SM, unidentified subscriber or SM delivery failure with error cause MS memory capacity exceeded, and the corresponding flag in the HLR (as indicated in the information received in the MAP_INFORM_SERVICE_CENTRE) is not set, or

- the reason received from the serving node (MSC or SGSN) for failure to deliver the message is absent subscriber_SM and the absent subscriber diagnostic is different from the absent subscriber diagnostic received in the MAP_INFORM_ SERVICE_CENTRE.

Procedure MT_SM_Delivery_Attempt_GMSC sheet 1, sheet 2, sheet 4, sheet 5: If absent subscriber diagnostic information (see 3GPP TS 23.040 [26]) is included with the absent subscriber_SM error indication then the SMS-GMSC relays this information to the HLR using the MAP_REPORT_SM_DELIVERY_STATUS service.

Procedure MT_SM_Delivery_Attempt_GMSC sheet 1, sheet 4: The More Messages To Send flag is set to TRUE or FALSE according to the information received from the Service Centre.

Procedure MT_SM_Delivery_Attempt_GMSC 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_MT_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.

The mobile terminated short message transfer process in the SMS-GMSC is shown in figure 23.3/3. The procedure MT_SM_Delivery_Attempt_GMSC is shown in figure 23.3/4. The macro MT_SM_Transfer_MSC is shown in figure 23.3/7.

****

23.3.3 Procedure in the Serving MSC

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

The process starts when the MSC receives a dialogue opening request with the application context shortMsgMT-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.

The mobile terminated short message transfer process in the serving MSC is shown in figure 23.3/6

Procedure MT_SM_VMSC sheet 1: The decision box "TCAP Handshake required" takes the "yes" or "no" exit depending on agreements between the Serving MSC's operator and the SMS Gateway MSC's operator (see 3GPP TS 33.200 [34a]).

The macro MT_SM_Transfer_MSC may be invoked either in a stand-alone serving MSC or in a serving MSC which is integrated with the SMS-GMSC. It is used to transfer the first MT short message of a possible sequence of messages. The macro invokes macros not defined in this clause; the definitions of these macros can be found as follows:

Check_Confirmation	see subclause 25.2.2.
Page_MSC	see subclause 25.3.1;
Search_for_MS_MSC	see subclause 25.3.2;
Process_Access_Request_MSC	see subclause 25.4.1;
Trace_Subscriber_Activity_MSC	see subclause 25.9.1.

The macro MT_SM_Transfer_MSC is shown in figure 23.3/7. The macro Check_Subscr_Identity_For_MT_SMS is shown in figure 23.3/8.

****

23.3.5 Procedure in the SGSN

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

The process starts when the SGSN receives a dialogue opening request with the application context shortMsgMT-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.

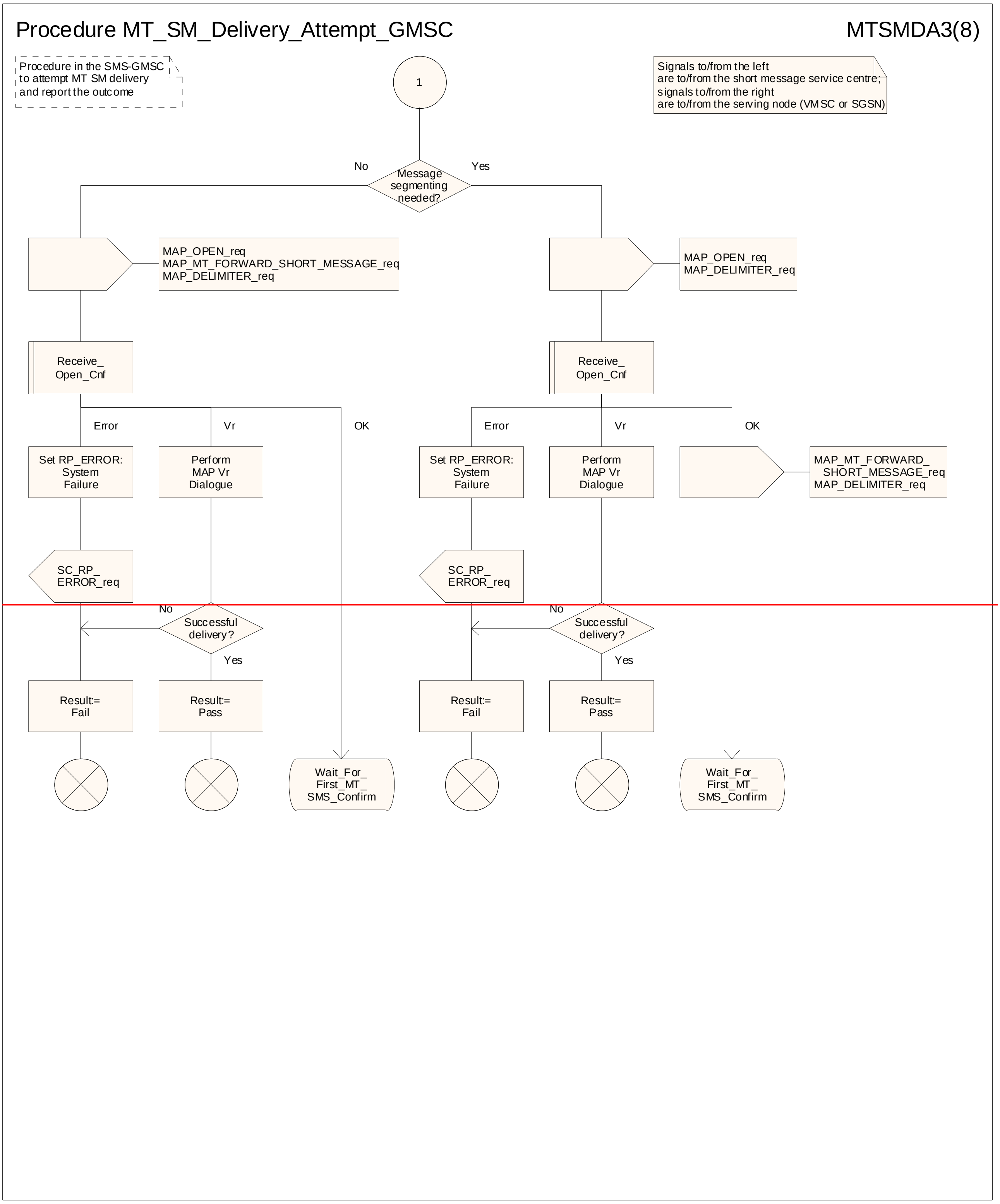
The mobile terminated short message transfer process in the SGSN is shown in figure 23.3/10.

Procedure MT_SM_SGSN sheet 1: The decision box "TCAP Handshake required" takes the "yes" or "no" exit depending on agreements between the Serving SGSN's operator and the SMS Gateway MSC's operator (see 3GPP TS 33.200 [34a]).

The macro MT_SM_Transfer_SGSN is used to transfer the first MT short message of a possible sequence of messages. It is shown in figure 23.3/11.

The macro Check_Subscr_Identity_For_MT_SMS is shown in figure 23.3/8. The page and search procedures are shown in figures 23.3/12 and 23.3/13.

****


Procedure MT_SM_Delivery_Attempt_GMSC
MTSMDA3(8)
Procedure in the SMS-GMSC to attempt MT SM delivery and report the outcome
Signals to/from the left are to/from the short message service centre; signals to/from the right are to/from the serving node (VMSC or SGSN)
1
Message segmenting needed?
No
Yes
MAP_OPEN_req
MAP_MT_FORWARD_SHORT_MESSAGE_req
MAP_DELIMITER_req
MAP_OPEN_req
MAP_DELIMITER_req
Receive_ Open_Cnf
Receive_ Open_Cnf
Error
Vr
OK
Error
Vr
OK
Set RP_ERROR: System Failure
Perform MAP Vr Dialogue
Set RP_ERROR: System Failure
Perform MAP Vr Dialogue
MAP_MT_FORWARD_ SHORT_MESSAGE_req
MAP_DELIMITER_req
SC_RP_ ERROR_req
SC_RP_ ERROR_req
Successful delivery?
No
Yes
Successful delivery?
No
Yes
Result:= Fail
Result:= Pass
Result:= Fail
Result:= Pass
Wait_For_ First_MT_ SMS_Confirm
Wait_For_ First_MT_ SMS_Confirm

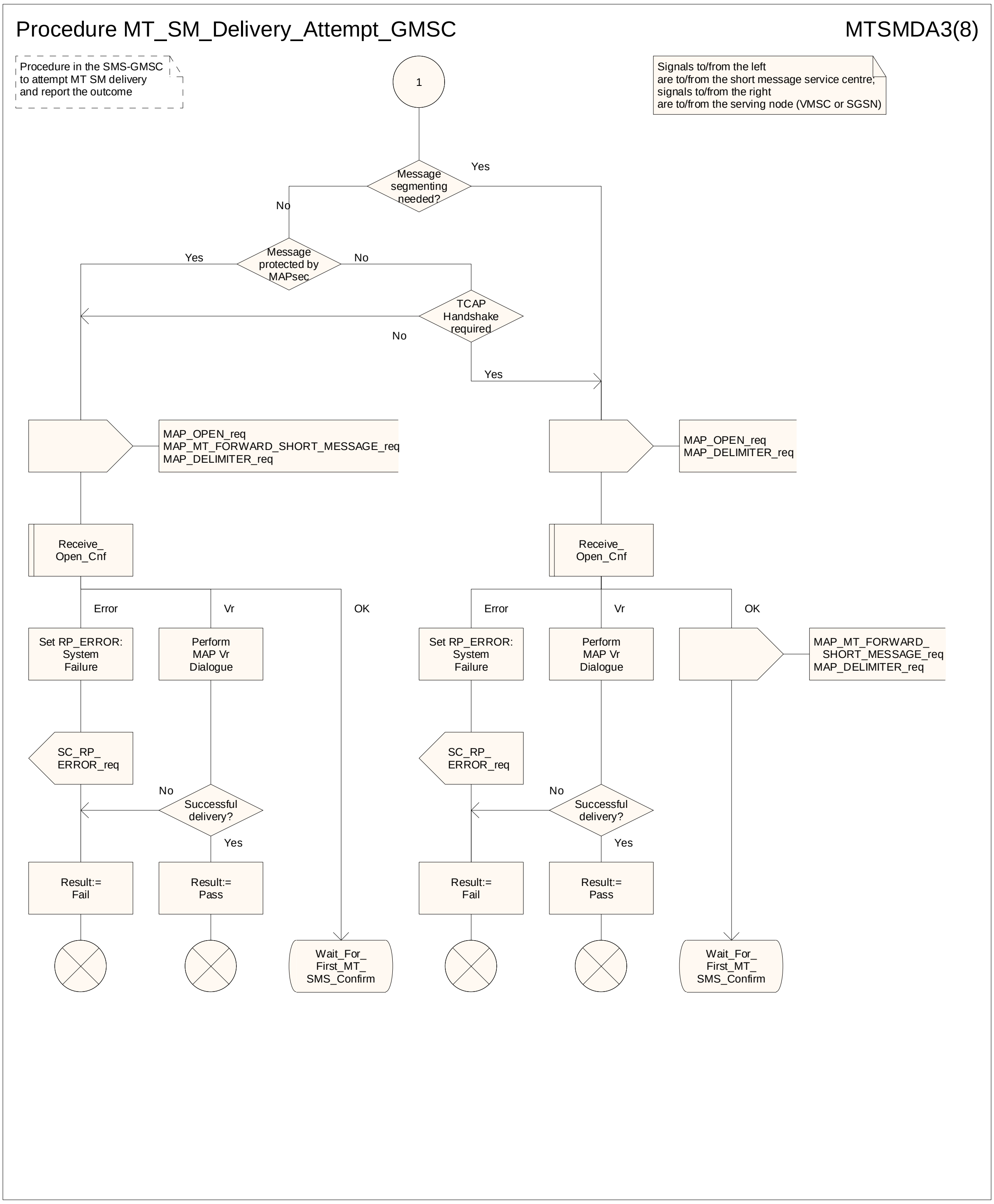
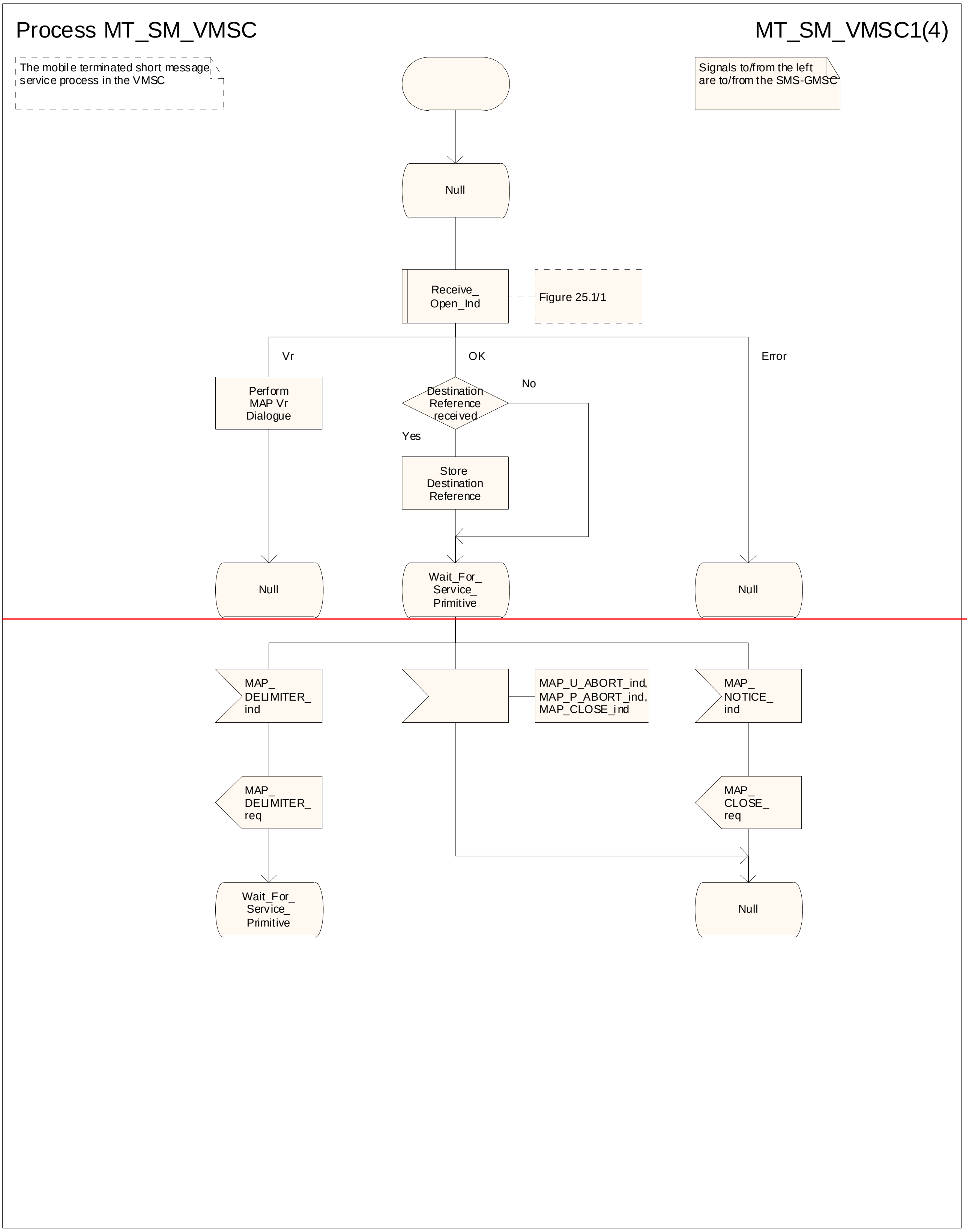

Procedure MT_SM_Delivery_Attempt_GMSC
MTSMDA3(8)
Procedure in the SMS-GMSC to attempt MT SM delivery and report the outcome
Signals to/from the left are to/from the short message service centre; signals to/from the right are to/from the serving node (VMSC or SGSN)
1
Message segmenting needed?
Yes
No
Message protected by MAPsec
Yes
No
TCAP Handshake required
No
Yes
MAP_OPEN_req
MAP_MT_FORWARD_SHORT_MESSAGE_req
MAP_DELIMITER_req
MAP_OPEN_req
MAP_DELIMITER_req
Receive_ Open_Cnf
Receive_ Open_Cnf
Error
Vr
OK
Error
Vr
OK
Set RP_ERROR: System Failure
Perform MAP Vr Dialogue
Set RP_ERROR: System Failure
Perform MAP Vr Dialogue
MAP_MT_FORWARD_ SHORT_MESSAGE_req
MAP_DELIMITER_req
SC_RP_ ERROR_req
SC_RP_ ERROR_req
No
Successful delivery?
Yes
No
Successful delivery?
Yes
Result:= Fail
Result:= Pass
Result:= Fail
Result:= Pass
Wait_For_ First_MT_ SMS_Confirm
Wait_For_ First_MT_ SMS_Confirm

Figure 23.3/4 (sheet 3 of 8): Procedure MT_SM_Delivery_Attempt_GMSC

****


Process MT_SM_VMSC
MT_SM_VMSC1(4)
The mobile terminated short message service process in the VMSC
Signals to/from the left are to/from the SMS-GMSC
Null
Receive_ Open_Ind
Figure 25.1/1
Vr
OK
Error
Perform MAP Vr Dialogue
Destination Reference received
No
Yes
Store Destination Reference
Null
Wait_For_ Service_ Primitive
Null
MAP_ DELIMITER_ ind
MAP_U_ABORT_ind, MAP_P_ABORT_ind, MAP_CLOSE_ind
MAP_ NOTICE_ ind
MAP_ DELIMITER_ req
MAP_ CLOSE_ req
Wait_For_ Service_ Primitive
Null

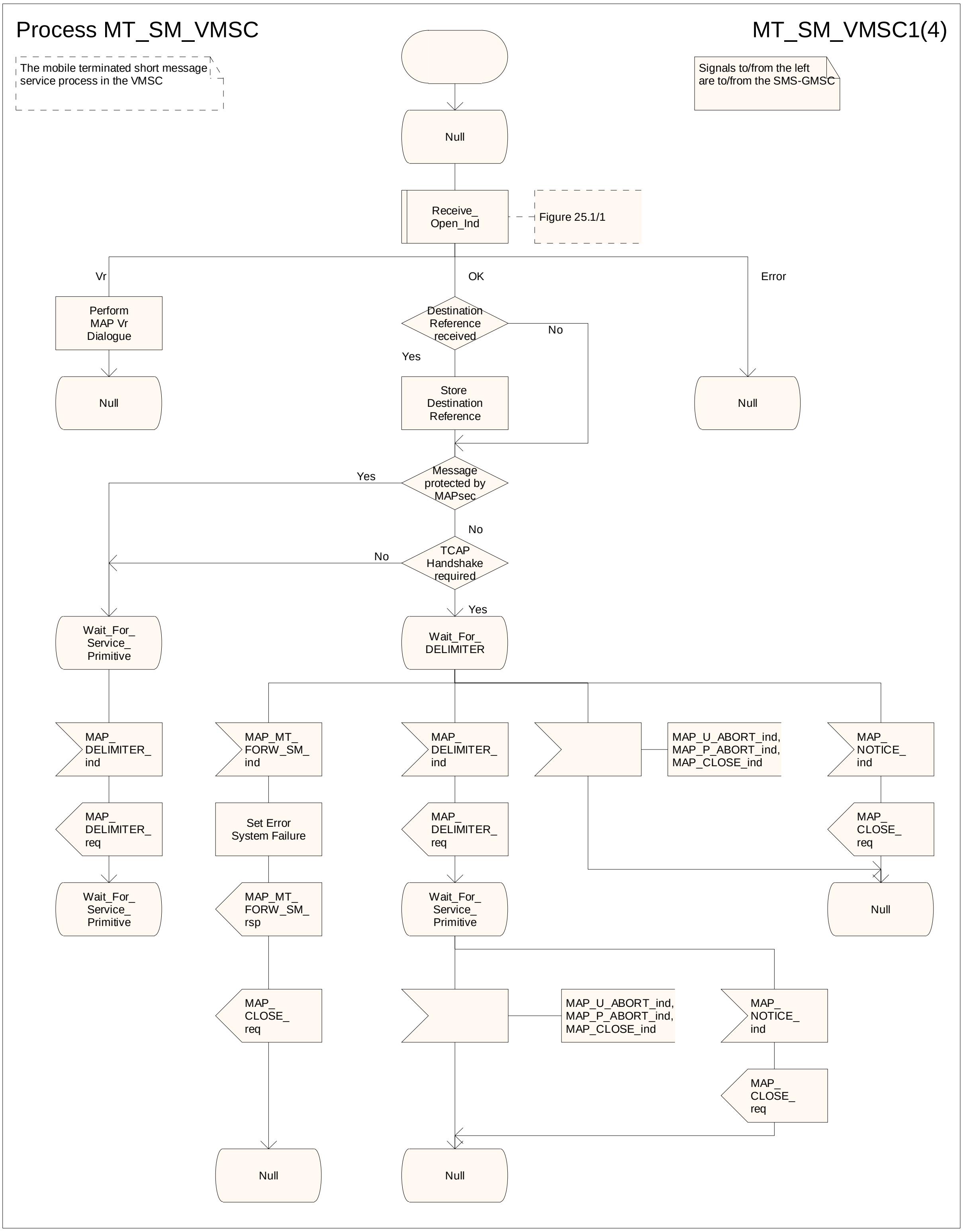
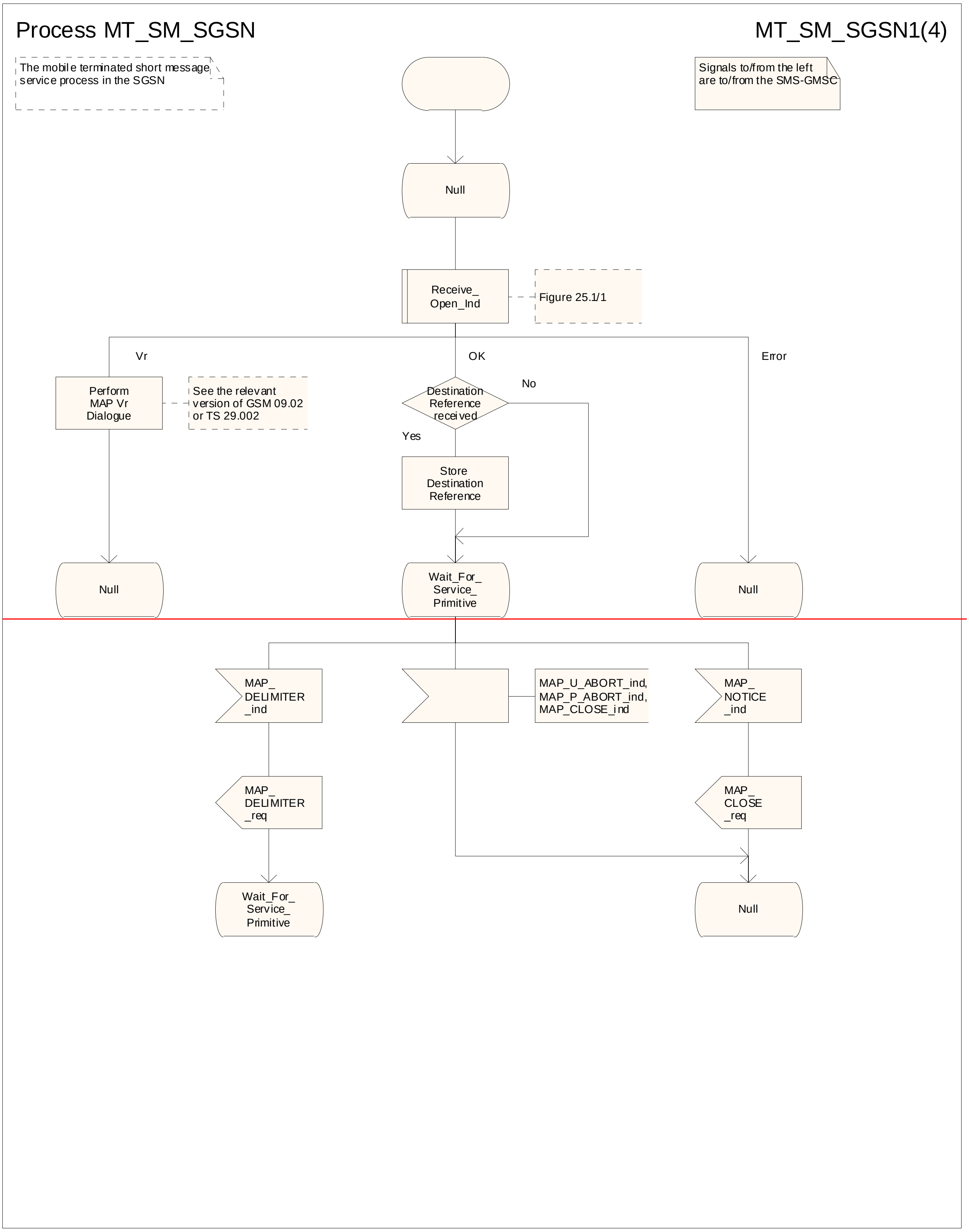


Figure 23.3/6 (sheet 1 of 4): Procedure MT_SM_VMSC

****


Process MT_SM_SGSN
MT_SM_SGSN1(4)
The mobile terminated short message service process in the SGSN
Signals to/from the left are to/from the SMS-GMSC
Null
Receive_ Open_Ind
Figure 25.1/1
Vr
OK
Error
Perform MAP Vr Dialogue
See the relevant version of GSM 09.02 or TS 29.002
Destination Reference received
No
Yes
Store Destination Reference
Null
Wait_For_ Service_ Primitive
Null
MAP_ DELIMITER _ind
MAP_U_ABORT_ind, MAP_P_ABORT_ind, MAP_CLOSE_ind
MAP_ NOTICE _ind
MAP_ DELIMITER _req
MAP_ CLOSE _req
Wait_For_ Service_ Primitive
Null

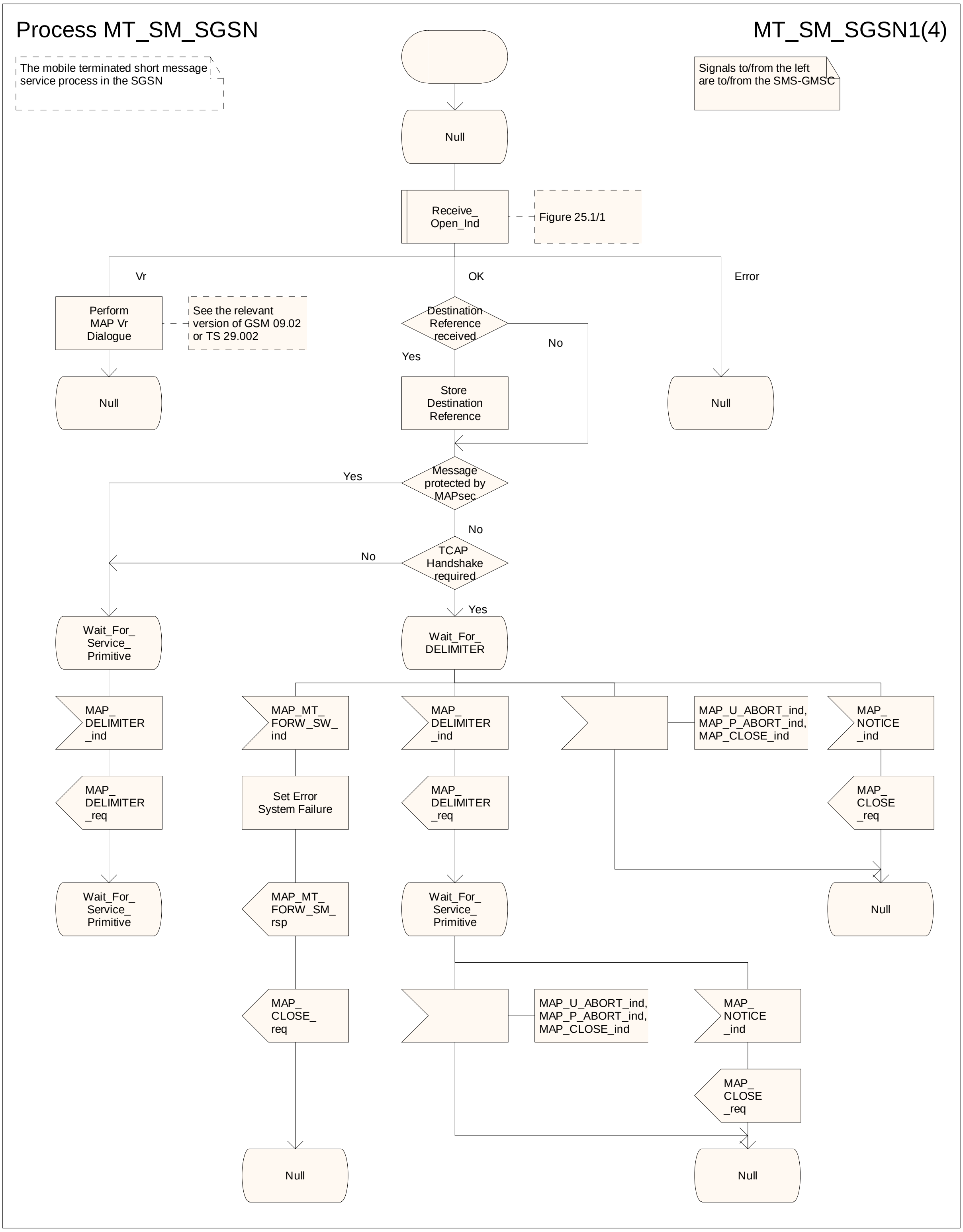

Process MT_SM_SGSN
MT_SM_SGSN1(4)
The mobile terminated short message service process in the SGSN
Signals to/from the left are to/from the SMS-GMSC
Null
Receive_ Open_Ind
Figure 25.1/1
Vr
OK
Error
Perform MAP Vr Dialogue
See the relevant version of GSM 09.02 or TS 29.002
Destination Reference received
No
Yes
Null
Store Destination Reference
Null
Message protected by MAPsec
Yes
No
TCAP Handshake required
No
Yes
Wait_For_ Service_ Primitive
Wait_For_ DELIMITER
MAP_ DELIMITER _ind
MAP_MT_ FORW_SW_ ind
MAP_ DELIMITER _ind
MAP_U_ABORT_ind, MAP_P_ABORT_ind, MAP_CLOSE_ind
MAP_ NOTICE _ind
MAP_ DELIMITER _req
Set Error System Failure
MAP_ DELIMITER _req
MAP_ CLOSE _req
Wait_For_ Service_ Primitive
MAP_MT_ FORW_SM_ rsp
Wait_For_ Service_ Primitive
Null
MAP_ CLOSE_ req
MAP_U_ABORT_ind, MAP_P_ABORT_ind, MAP_CLOSE_ind
MAP_ NOTICE _ind
MAP_ CLOSE _req
Null
Null

Figure 23.3/10 (sheet 1 of 4): Process MT_SM_SGSN