3GPP TSG SA WG3 Security — SA3#35 **S3-040704**
October 5-8, 2004
St Paul's Bay, Malta

3GPP TSG-CN WG4 Meeting #24 **N4-041193**
Sophia Antipolis, France. 16th to 20th August 2004.

Title: **LS on SMS Fraud countermeasures**
Response to: **LS (S3-040642) from SA3**
Release: **Rel-6**
Work Item: **-**

Source: **CN4**
To: **SA3**
Cc: **T2**

Contact Person:
Name: Ulrich Wiehe
Tel. Number: +496621169139
E-mail Address: ulrich.wiehe@gksag.de

Attachments: CR 29.002 740 on SMS Fraud countermeasures (N4-040959)

---

1. Overall Description:

CN4 thank SA3 for their LS on SMS Fraud Countermeasures (S3-040642 aka N4-040914).

CN4 has assessed the proposal outlined in S3-040581. The proposal provides some level of authenticity of the SMSC address by introducing a TCAP handshake mechanism. The mechanism is already implemented in application context versions 2 and 3 for Short Message Transfer for cases where the length of the SM payload exceeds a certain limit, and it can easily be extended to be applied also for Short Messages with a shorter payload. A CR to 3GPP TS 29.002 (see attachment) would be needed to mandate the handshake mechaninsm also for short payloads at the SMS-GMSC and to reject transfer of short messages at the MSC/SGSN when Short Messages are received without handshake. A CR to 3GPP TS 23.040 is not required, however, a linked CR to 3GPP TS 33.200 is believed to be appropriate.
It must be noted that the handshake mechanism doubles the signalling load on the interfaces between SMS-GMSC and MSC / SGSN for MT short message transfer. Furthermore the mechanism requires support of application context version 2 or 3, i.e. it cannot be used with version 1.

The discussion on this was not conclusive and there was reluctance to mandate this.

2. Actions:

SA3 are asked to consider the attached CR 29.002 740 and to provide opinion on whether the solution proposed addresses the problem described in the LS S3-040642. In particular to provide guidance as to whether the proposal should be mandated or optional.

3. Date of Next CN4 Meetings:

CN4#25	15th - 19th November 2004	Seoul, KOREA

3GPP TSG-CN WG4 Meeting #24 ***N4-040959***

Sophia Antipolis, France. 16th to 20th August 2004.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.002** **CR** **740** ⌘ **rev** **-** ⌘ Current version: **6.6.0** ⌘

*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:	⌘	Siemens
Work item code:	⌘	TEI6
Date:	⌘	29/07/2004
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:	⌘	To address the SMS Fraud scenario identified in S3-040581
Summary of change:	⌘	Mandate a TCAP handshake before transmitting an MT-Short-Message
Consequences if not approved:	⌘	The SMS Fraud problem remains unsolved

Clauses affected:	⌘	23.3, figures 23.3/4, 23.3/6, 23.3/10			
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.

23.3 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.

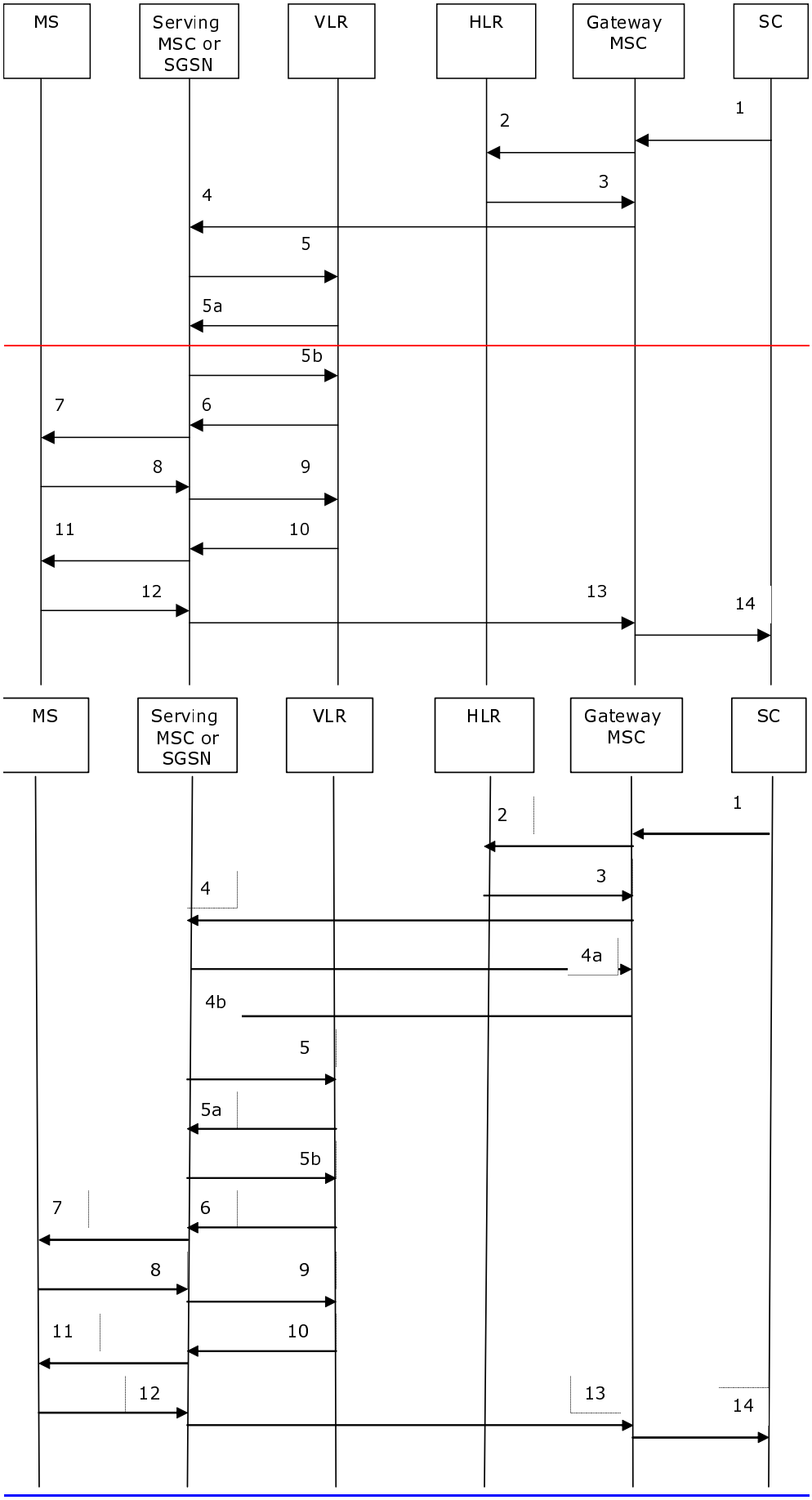
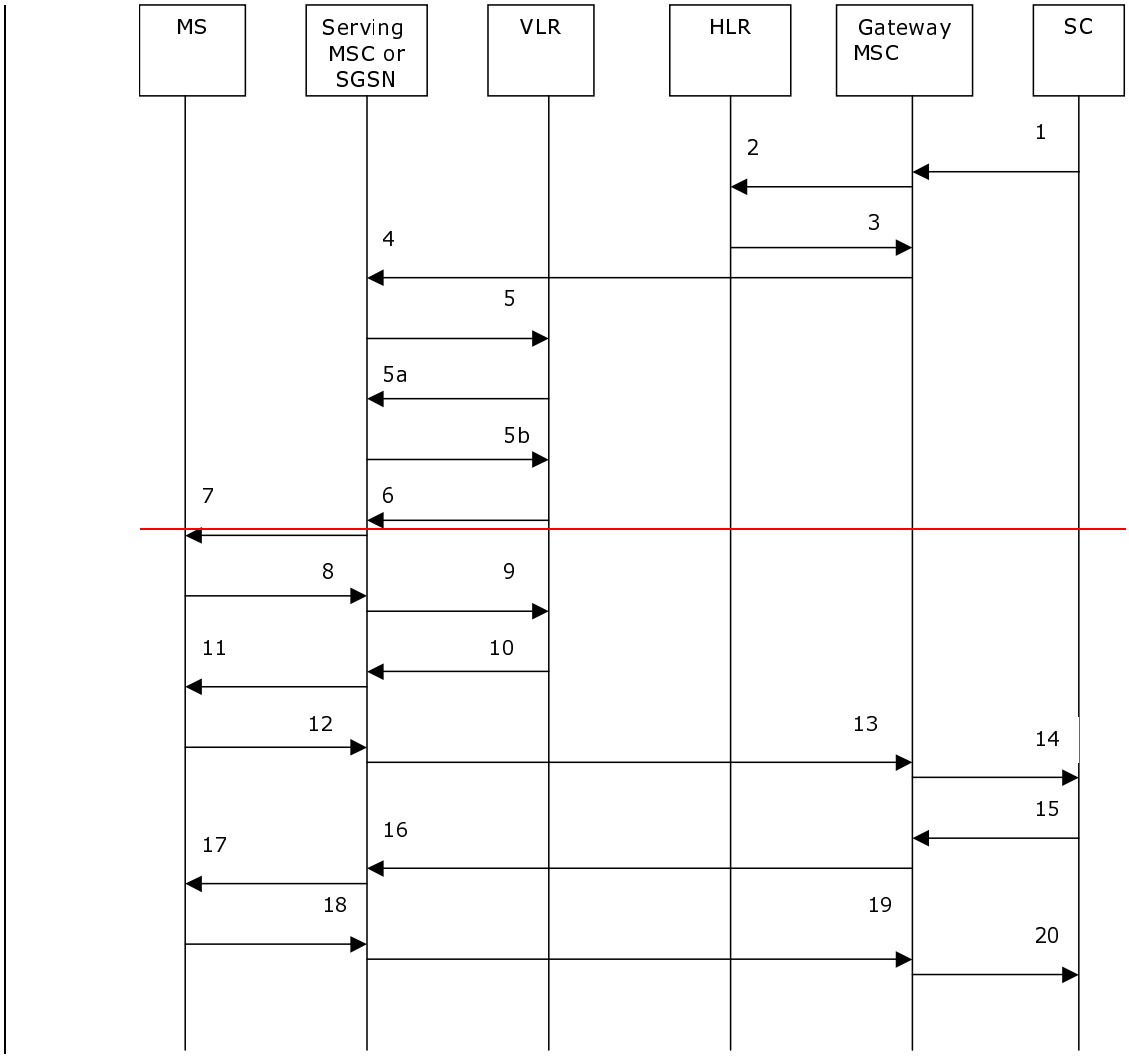


Figure 23.3/1: Mobile terminated short message service procedures

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 both,
- 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
- the MAP signalling for short message transfer is protected by means of MAPsec, 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
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

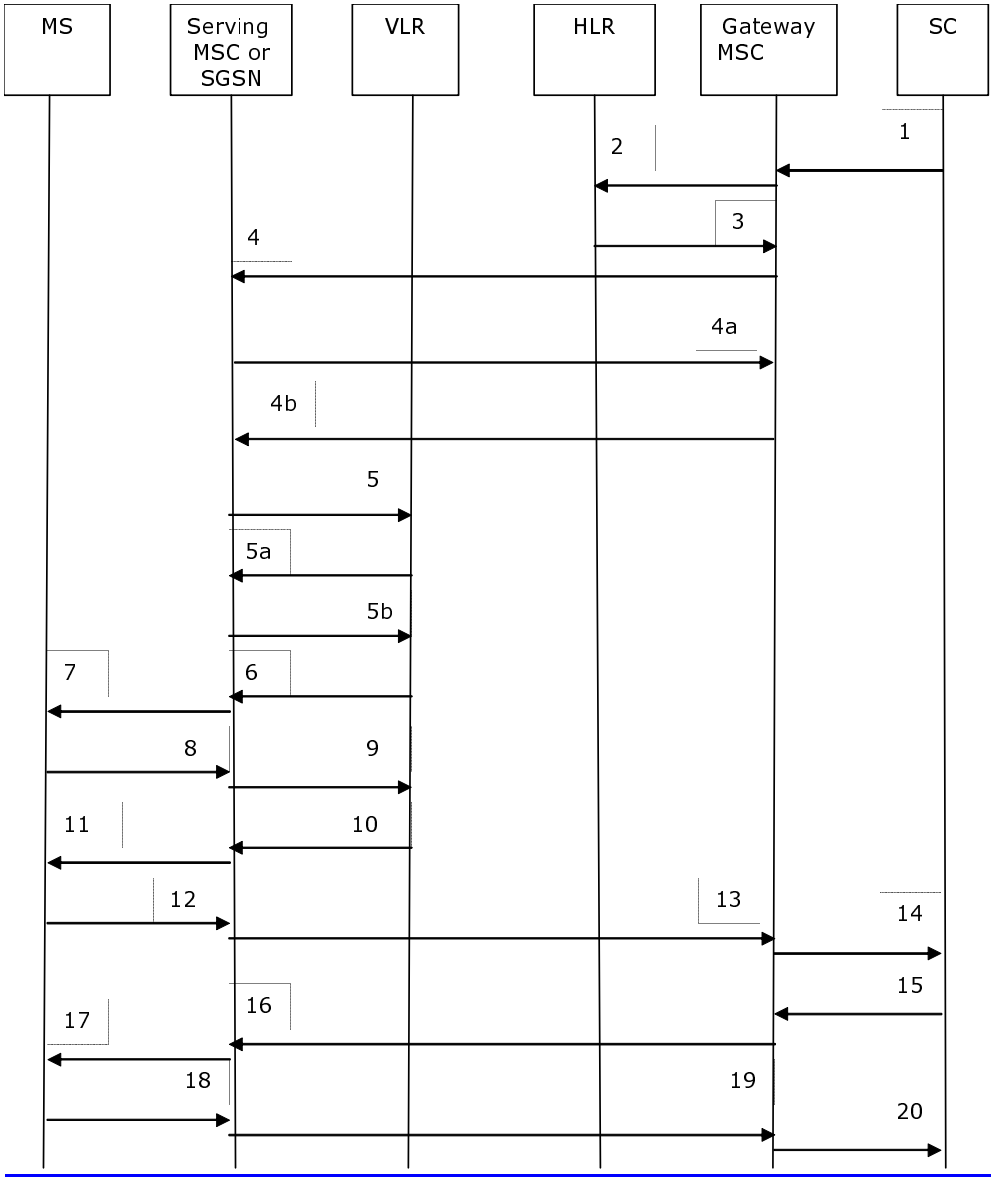


Figure 23.3/2: Mobile terminated short message procedure for multiple short message transfer

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 both,
- 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
- the MAP signalling for short message transfer is protected by means of MAPsec, 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.

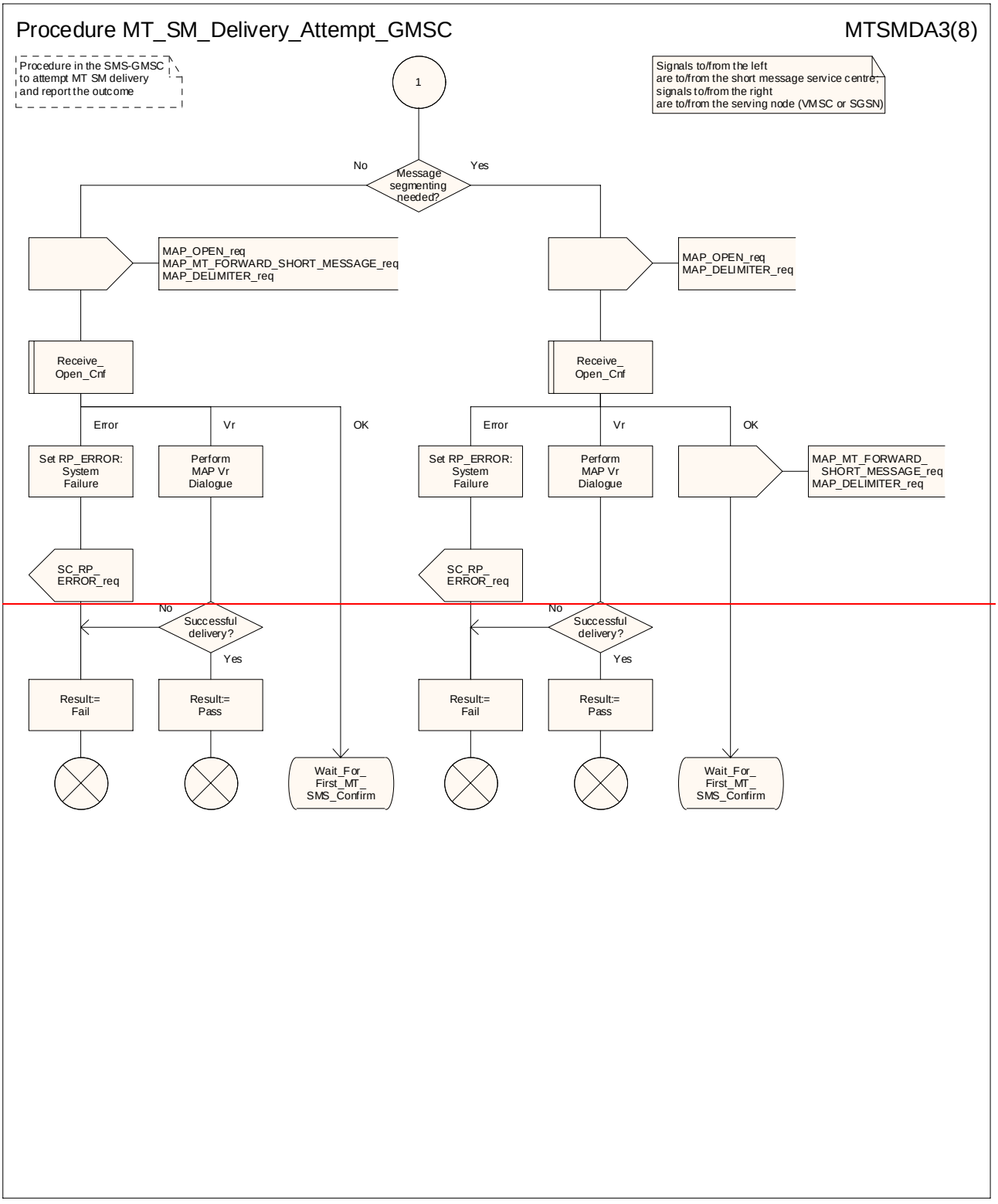
In the multiple short message transfer the service MAP_MT_FORWARD_SHORT_MESSAGE can be used several times. However, the short message transfer is always acknowledged to the Service Centre before the next short message is sent.

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.

****


Procedure MT_SM_Delivery_Attempt_GMSC
MTSMDA3(8)
Procedure in the SMS-GMSC to attempt MT SM delivery and report the outcome
1
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)
No
Message segmenting needed?
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?
No
Successful delivery?
Yes
Yes
Result= Fail
Result= Pass
Result= Fail
Result= Pass
Wait_For_ First_MT_ SMS_Confirm
Wait_For_ First_MT_ SMS_Confirm

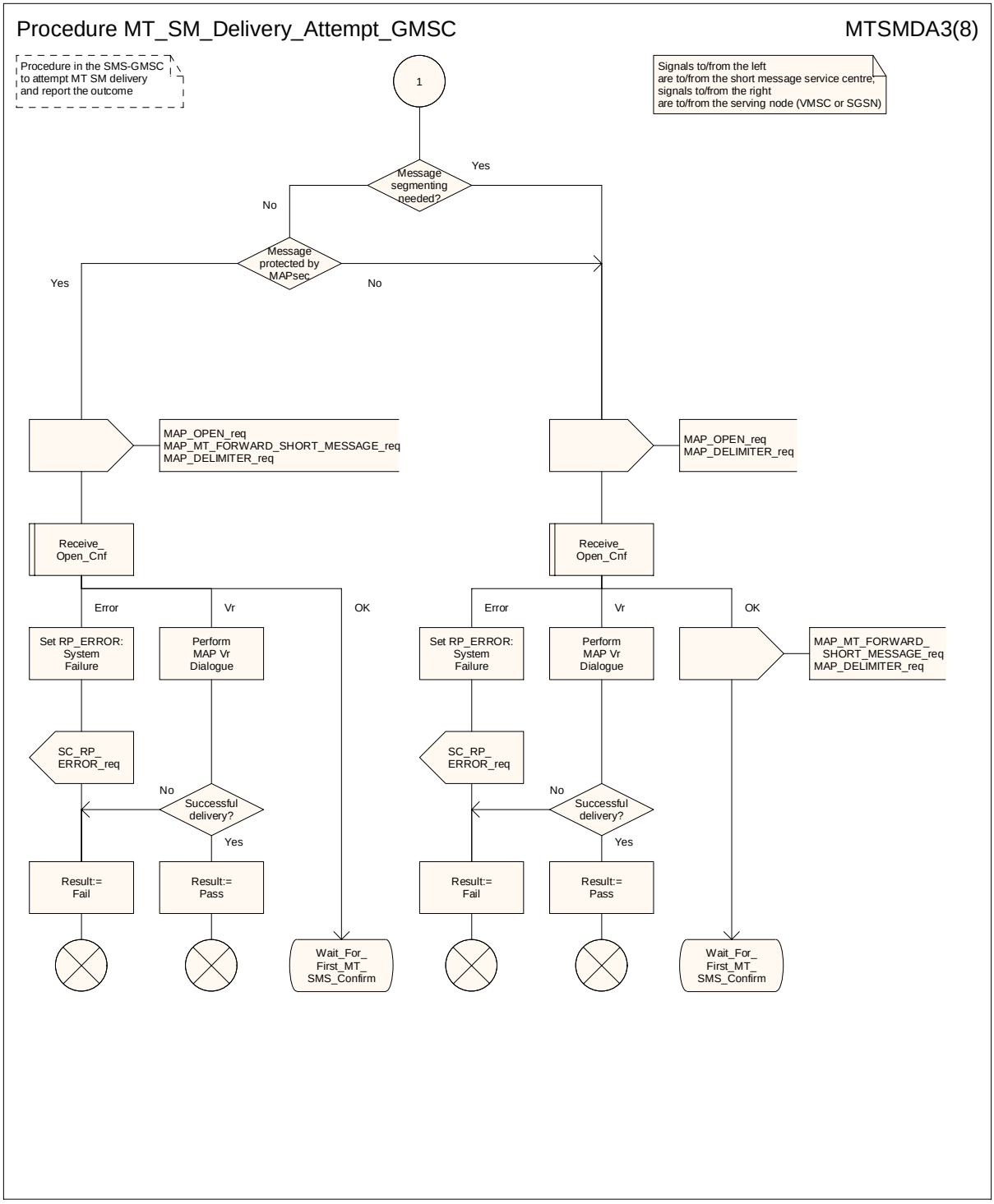
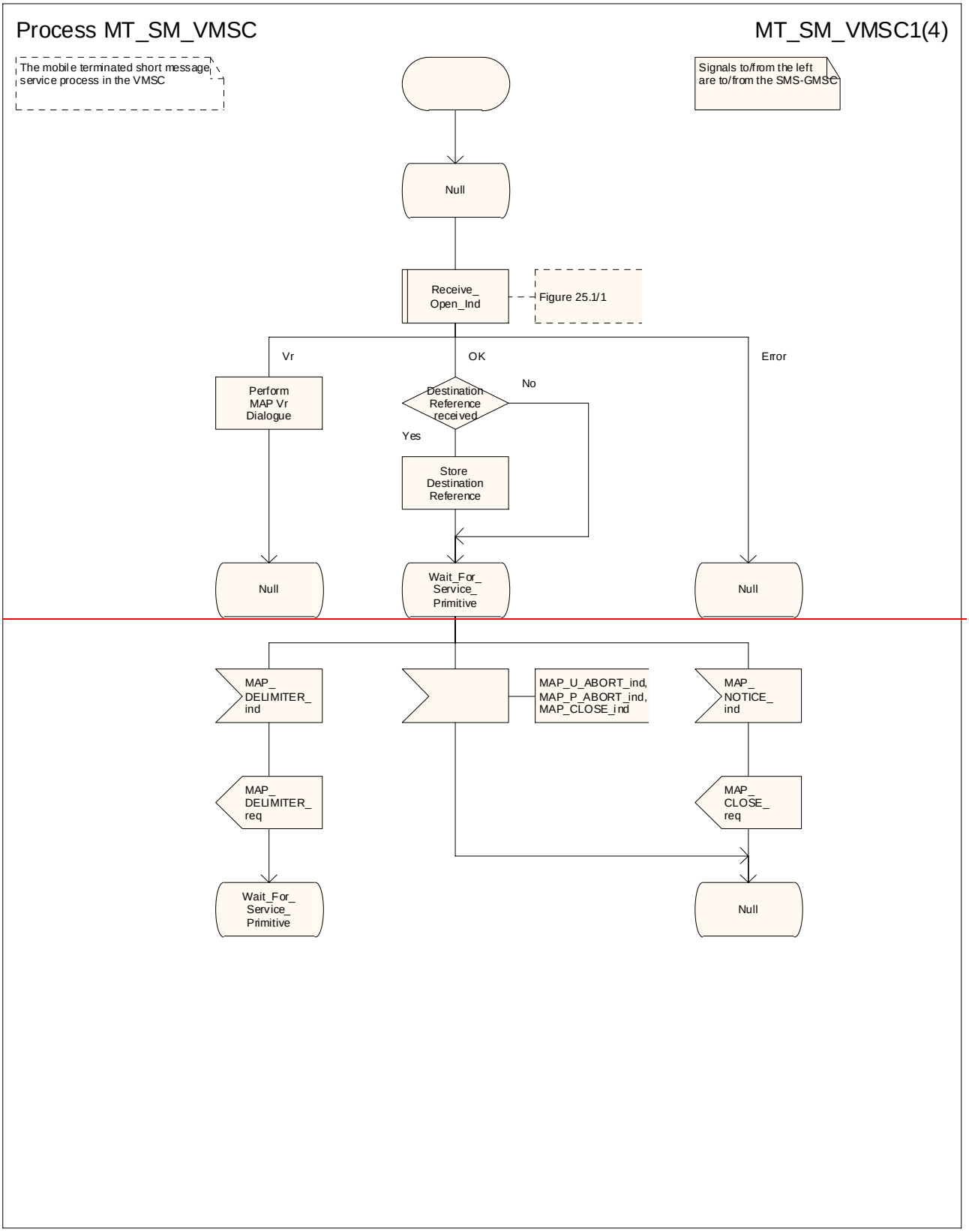


Figure 23.3/4 (sheet 3 of 8): Procedure MT_SM_Delivery_Attempt_GMSC

****


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

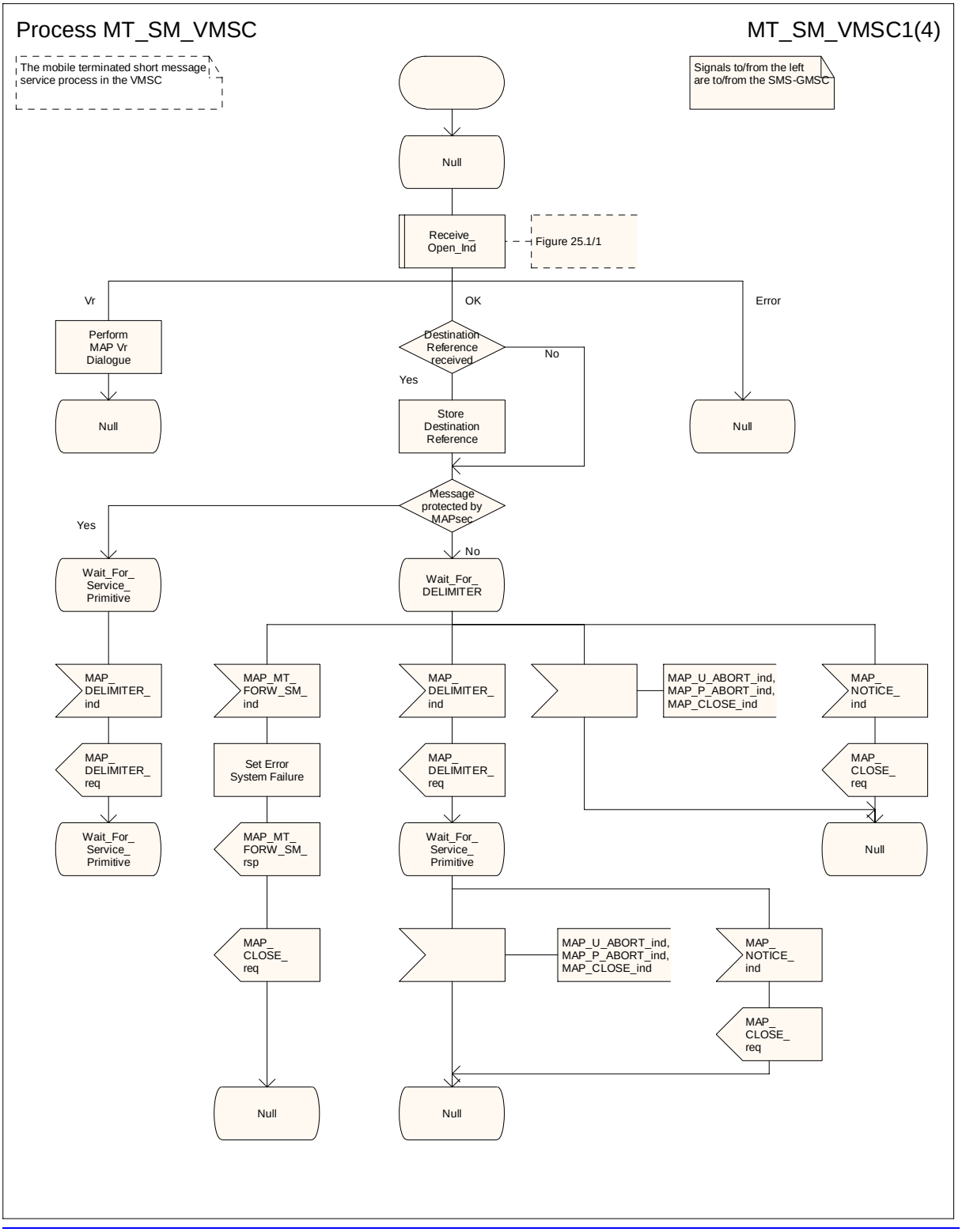
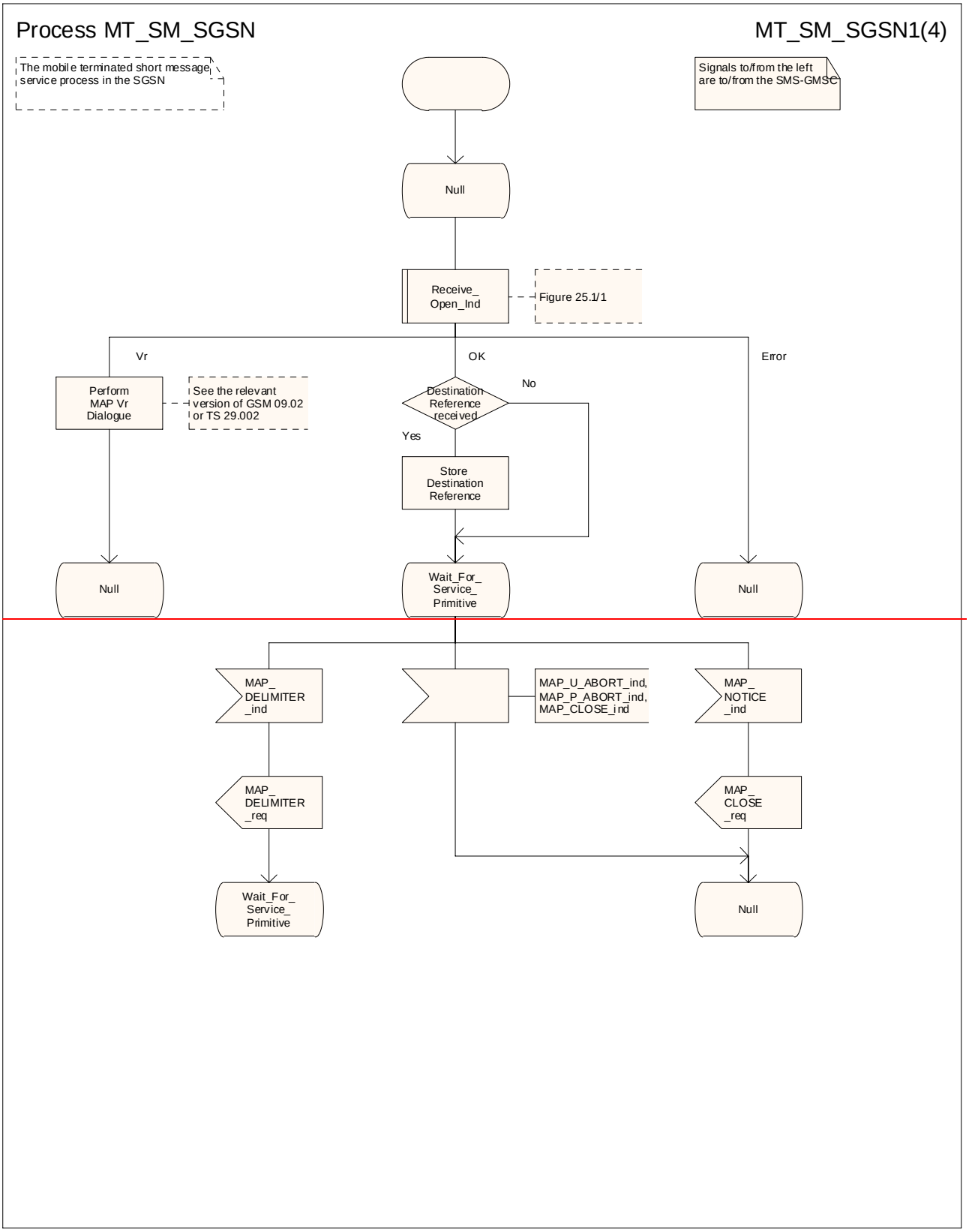


Figure 23.3/6 (sheet 1 of 4): Procedure MT_SM_VMSC

****


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

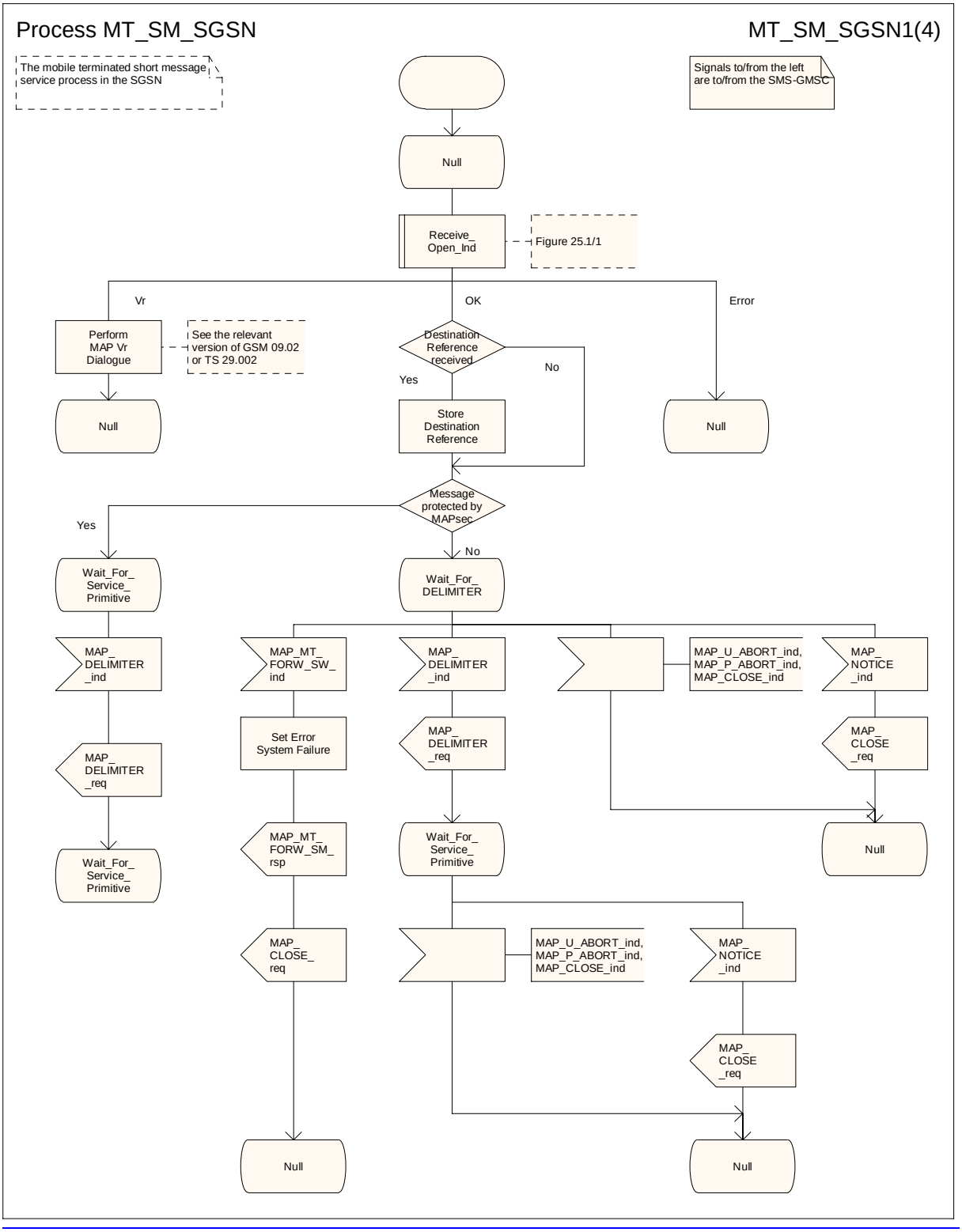


Figure 23.3/10 (sheet 1 of 4): Process MT_SM_SGSN