3GPP TSG_CN
Plenary Meeting #9, Oahu, Hawaii
20th – 22nd September 2000.

Tdoc NP-000485

Source: **TSG_N WG 4**

Title: **CR to R00 Work Item Core Network (CN) Security**

Agenda item:

Document for: **APPROVAL**

Introduction:

This document contains 1 CR on R00 Work Item Core Network Security, that has been agreed by TSG_N WG4, and is forwarded to TSG_N Plenary meeting #9 for approval.

SM	TDoc	SPEC	CR	REV	PHAS	VERS	SUBJECT	CAT
CN9	N4-000543	29.002	152	1	R99	3.5.0	Clarifications for secure MAP transport	F

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

29.002 CR	**152r1**	Current Version:	**4.0.0**

GSM (AA.BB) or 3G (AA.BBB) specification number ↑   *↑ CR number as allocated by MCC support team*

For submission to:	CN#09	for approval	X	strategic		*(for SMG*
list expected approval meeting # here ↑		for information		non-strategic	X	*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG   *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects:
(at least one should be marked with an X)

(U)SIM ☐   ME ☐   UTRAN / Radio ☐   Core Network **X**

Source:	N4	**Date:**	19th July, 2000

Subject:	Clarifications for secure MAP transport

Work item:	Core Network Security

Category: F Correction **X**   **Release:**   Phase 2 ☐
A Corresponds to a correction in an earlier release ☐   Release 96 ☐
(only one category B Addition of feature ☐   Release 97 ☐
shall be marked C Functional modification of feature ☐   Release 98 ☐
with an X) D Editorial modification ☐   Release 99 ☐
    Release 00 **X**

Reason for change:	1. The current text describing the secure MAP transport services seems to indicate that a secure MAP transport error carries two copies of the security header.
	2. There is no clear basis for the decisions in the initiating and responding entities on whether unsecured transport is allowed.
	3. The responding entity needs also to check whether the protection mode for secure transport is acceptable.
	4. Two editorial errors in the SDL diagrams MAP_SRSSM3 and MAP_PSSM2 are corrected

Clauses affected:	7.3.1, 7.6.1.4, 15.2.1, 15.2.2; Figures 15.6/3/g, 15.6/3j, 15.6/7c, 15.6/8b; 17.4

Other specs affected:	Other 3G core specifications	☐	→ List of CRs:	
	Other GSM core specifications	☐	→ List of CRs:	
	MS test specifications	☐	→ List of CRs:	
	BSS test specifications	☐	→ List of CRs:	
	O&M specifications	☐	→ List of CRs:	

Other comments:	

7.3.1   MAP-OPEN service

This service is used for establishing a MAP dialogue between two MAP service-users. The service is a confirmed service with service primitives as shown in table 7.3/1.

Table 7.3/1: Service-primitives for the MAP-OPEN service

Parameters	Request	Indication	Response	Confirm
Application context name	M	M(=)	U	C(=)
Destination address	M	M(=)		
Destination reference	U	C(=)		
Originating address	U	O		
Originating reference	U	C(=)		
Specific information	U	C(=)	U	C(=)
Responding address			U	C(=)
Result			M	M(=)
Refuse-reason			C	C(=)
Provider error				O

Application context name:

This parameter identifies the type of application context being established. If the dialogue is accepted the received application context name shall be echoed. In case of refusal of dialogue this parameter shall indicate the highest version supported.

Destination address:

A valid SCCP address identifying the destination peer entity (see also clause 6). As an implementation option, this parameter may also, in the indication, be implicitly associated with the service access point at which the primitive is issued.

Destination-reference:

This parameter is a reference which refines the identification of the called process. It may be identical to Destination address but its value is to be carried at MAP level. Table 7.3/2 describes the MAP services using this parameter. Only these services are allowed to use it.

Table 7.3/2: Use of the destination reference

MAP service	Reference type	Use of the parameter
MAP-REGISTER-SS	IMSI	Subscriber identity
MAP-ERASE-SS	IMSI	Subscriber identity
MAP-ACTIVATE-SS	IMSI	Subscriber identity
MAP-DEACTIVATE-SS	IMSI	Subscriber identity
MAP-INTERROGATE-SS	IMSI	Subscriber identity
MAP-REGISTER-PASSWORD	IMSI	Subscriber identity
MAP-PROCESS-UNSTRUCTURED-SS-REQUEST	IMSI	Subscriber identity
MAP-UNSTRUCTURED-SS-REQUEST	IMSI	Subscriber identity
MAP-UNSTRUCTURED-SS-NOTIFY	IMSI	Subscriber identity
MAP-FORWARD-SHORT-MESSAGE	IMSI (note)	Subscriber identity
MAP-REGISTER-CC-ENTRY	IMSI	Subscriber identity
MAP-ERASE-CC-ENTRY	IMSI	Subscriber identity

NOTE: Only when the IMSI and the LMSI are received together from the HLR in the mobile terminated short message transfer.

Originating address:

A valid SCCP address identifying the requestor of a MAP dialogue (see also clause 6). As an implementation option, this parameter may also, in the request, be implicitly associated with the service access point at which the primitive is issued.

Originating-reference:

This parameter is a reference which refines the identification of the calling process. It may be identical to the Originating address but its value is to be carried at MAP level. Table 7.3/3 describes the MAP services using the parameter. Only these services are allowed to use it. Processing of the Originating-reference shall be performed according to the supplementary service descriptions and other service descriptions, e.g. operator determined barring.

Table 7.3/3: Use of the originating reference

MAP service	Reference type	Use of the parameter
MAP-REGISTER-SS	ISDN-Address-String	Originated entity address
MAP-ERASE-SS	ISDN-Address-String	Originated entity address
MAP-ACTIVATE-SS	ISDN-Address-String	Originated entity address
MAP-DEACTIVATE-SS	ISDN-Address-String	Originated entity address
MAP-INTERROGATE-SS	ISDN-Address-String	Originated entity address
MAP-REGISTER-PASSWORD	ISDN-Address-String	Originated entity address
MAP-PROCESS-UNSTRUCTURED-SS-REQUEST	ISDN-Address-String	Originated entity address
MAP-REGISTER-CC-ENTRY	ISDN-Address-String	Originated entity address
MAP-ERASE-CC-ENTRY	ISDN-Address-String	Originated entity address

Specific information:

This parameter may be used for passing any user specific information. Establishment and processing of the Specific information is not specified by GSM and shall be performed according to operator specific requirements.

Responding address:

An address identifying the responding entity. The responding address is included if required by the context (e.g. if it is different from the destination address).

Result:

This parameter indicates whether the dialogue is accepted by the peer.

Refuse reason:

This parameter is ~~only~~ present only if the Result parameter indicates that the dialogue is refused. It takes one of the following values:

- Application-context-not-supported;

- Invalid-destination-reference;

- Invalid-originating-reference;

- No-reason-given;

- Remote node not reachable;

- Potential version incompatibility;

- Secured transport not possible:

- Transport protection not adequate.

7.6.1.4   User error

This parameter can take values as follows:

    NOTE: The values are grouped in order to improve readability; the grouping has no other significance.

a) Generic error:

- system failure, i.e. a task cannot be performed because of a problem in another entity. The type of entity or network resource may be indicated by use of the network resource parameter;

- data missing, i.e. an optional parameter required by the context is missing;

- unexpected data value, i.e. the data type is formally correct but its value or presence is unexpected in the current context;

- resource limitation;

- initiating release, i.e. the receiving entity has started the release procedure;

- facility not supported, i.e. the requested facility is not supported by the PLMN;

- incompatible terminal, i.e. the requested facility is not supported by the terminal.

b) Identification or numbering problem:

- unknown subscriber, i.e. no such subscription exists;

- number changed, i.e. the subscription does not exist for that number any more;

- unknown MSC;

- unidentified subscriber, i.e. if the subscriber is not contained in the database and it has not or cannot be established whether or not a subscription exists;

- unallocated roaming number;

- unknown equipment;

- unknown location area.

c) Subscription problem:

- roaming not allowed, i.e. a location updating attempt is made in an area not covered by the subscription;

- illegal subscriber, i.e. illegality of the access has been established by use of authentication procedure;

- bearer service not provisioned;

- teleservice not provisioned;

- illegal equipment, i.e. the IMEI check procedure has shown that the IMEI is blacklisted or not whitelisted.

d) Handover problem:

- no handover number available;

- subsequent handover failure, i.e. handover to a third MSC failed for some reason.

e) Operation and maintenance problem:

- tracing buffer full, i.e. tracing cannot be performed because the tracing capacity is exceeded.

f) Call set-up problem:

- no roaming number available, i.e. a roaming number cannot be allocated because all available numbers are in use;

- absent subscriber, i.e. the subscriber has activated the detach service or the system detects the absence condition. This error may be qualified to indicate whether the subscriber was IMSI detached, in a restricted area or did not respond to paging;

- busy subscriber. This error may be qualified to indicate that the subscriber was busy due to CCBS and that CCBS is possible;

- no subscriber reply;

- forwarding violation, i.e. the call has already been forwarded the maximum number of times that is allowed;

- CUG reject, i.e. the call does not pass a CUG check; additional information may also be given in order to indicate rejection due to e.g. incoming call barred or non-CUG membership.

- call barred. Optionally, additional information may be included for indicating either that the call meets a barring condition set by the subscriber or that the call is barred for operator reasons. In the case of barring of Mobile Terminating Short Message, the additional information may indicate a barring condition due to "Unauthorised Message Originator".

- optimal routeing not allowed, i.e. the entity which sends the error does not support optimal routeing, or the HLR will not accept an optimal routeing interrogation from the GMSC, or the call cannot be optimally routed because it would contravene optimal routeing constraints.

- forwarding failed, i.e. the GMSC interrogated the HLR for forwarding information but the HLR returned an error.

g) Supplementary services problem:

- call barred;

- illegal SS operation;

- SS error status;

- SS not available;

- SS subscription violation;

- SS incompatibility;

- negative password check;

- password registration failure;

- Number of Password Attempts;

- USSD Busy;

- Unknown Alphabet.

- short term denial;

- long term denial.

For definition of these errors see GSM 04.80.

h) Short message problem:

- SM delivery failure with detailed reason as follows:

    - memory capacity exceeded;

    - MS protocol error;

    - MS not equipped;

    - unknown service centre (SC);

    - SC congestion;

    - invalid SME address;

    - subscriber is not an SC subscriber;

    - and possibly detailed diagnostic information, coded as specified in TS GSM 03.40, under SMS-SUBMIT-REPORT and SMS-DELIVERY-REPORT. If the SM entity which returns the SM Delivery Failure error includes detailed diagnostic information, it shall be forwarded in the MAP_MO_FORWARD_SHORT_MESSAGE and in the MAP_MT_FORWARD_SHORT_MESSAGE response.

- message waiting list full, i.e. no further SC address can be added to the message waiting list;

- Subscriber busy for MT SMS, i.e. the mobile terminated short message transfer cannot be completed because:

    - another mobile terminated short message transfer is going on and the delivery node does not support message buffering; or

    - another mobile terminated short message transfer is going on and it is not possible to buffer the message for later delivery; or

    - the message was buffered but it is not possible to deliver the message before the expiry of the buffering time defined in GSM 03.40;

- Absent Subscriber SM, i.e. the mobile terminated short message transfer cannot be completed because the network cannot contact the subscriber. Diagnostic information regarding the reason for the subscriber's absence may be included with this error.

i) Location services problem:

- Unauthorized Requesting Network

- Unauthorized LCS Client with detailed reason as follows

- Unauthorzied Privacy Class

- Unauthoized Call Unrelated External Client

- Unauthorized Call Related External Client

- Privacy override not applicable

- Position method failure with detailed reason as follows:

  - Congestion

  - Insufficient resources

  - Insufficient Measurement Data

  - Inconsistent Measurement Data

- Location procedure not completed

- Location procedure not supported by target MS

- QoS not attainable

- Unknown or unreachable LCS Client

j) Problem detected by an application using secure transport:

- Secure transport error. This error indicates that the application using secure transport returned an error. The parameters of the error indicates:

  ~~The security header (see subclause 7.6.12);~~

  - The protected payload, which carries the result of applying the protection function specified in TS 33.102 to the encoding of the parameter of the original error.

**** Next modified section ****

15.2.1   Behaviour at the initiating side

The behaviour of the MAP dialogue state machine at the initiating side is defined in sheets 1 – 9 of the process Secure_MAP_DSM.

Sheet 1: The MAP protocol machine decides according to the application context name received in the MAP-OPEN request and the identity of the responder whether secure transport of the MAP dialogue is required, and if so what level of protection is required. This decision is based on bilateral agreements between the operators of the network entities concerned; it requires the dialogue initiating entity to store configuration information on which the decision is based. If secure transport is required, the MAP protocol machine builds a protected dialogue portion (including the AC name and any user information received in the MAP-OPEN request, encoded as user information for the TC-BEGIN) for the TC-BEGIN; otherwise it builds a normal dialogue portion using the application context name and any user data included in the MAP-OPEN request.

Sheet 2: If secure transport is used, each MAP specific service request is stored in case drop-back to unsecured transport is to be invoked.

Sheet 2: If secure transport is required, each MAP specific service request triggers the creation of an instance of the Secure_Requesting_MAP_SSM to handle the secure transport of the request. If secure transport is not

required, each MAP specific service request triggers the creation of an instance of the Requesting_MAP_SSM to handle the transport of the request.

Sheet 3: When the the MAP dialogue state machine at the initiating side is waiting for a response from the responding side, a TC-END indication which echoes the AC name which was sent in the TC-BEGIN indicates acceptance of the dialogue. If secure transport is required, acceptance of the dialogue opening request which was transported in the secure dialogue opening request is indicated by the encapsulated AC name transported in the user information of the TC-END being equal to the encapsulated AC which was included in the user information of the TC-BEGIN. Mismatch of either the AC name or the encapsulated AC name indicates failure of the dialogue opening.

Sheet 3: If the dialogue opening is accepted, any components included in the TC-END are processed and passed to the MAP-Service User. The dialogue is closed by sending a MAP-CLOSE to the MAP-Service User.

Sheet 3, sheet 4, sheet 5, sheet 6, sheet 7, sheet 8, sheet 9: when a dialogue is terminated, the MAP dialogue state machine terminates all instances of the Requesting_MAP_SSM or Secure_Requesting_MAP_SSM which are active for this dialogue.

Sheet 4, sheet 5: It is a matter for agreement between the operators of the network entities involved whether fallback to unsecured transport is acceptable if secured transport is not possible. This requires the dialogue initiating entity to store configuration information on which this decision is based.

Sheet 4: A TC-P-ABORT with an abort parameter Incorrect- Transaction- Portion indicates that the responding side does not support a MAP version higher than 1. If secure transport is not required, this triggers a MAP-OPEN confirm indicating that the dialogue is refused, with a refuse reason potential version incompatibility. The MAP-Service User may then decide to retry the dialogue at MAP version 1. If secure transport is required and fallback to unsecured transport is acceptable, the dialogue machine retries the dialogue with unsecured transport. If secure transport is required and fallback to unsecured transport is not acceptable, this triggers a MAP-OPEN confirm indicating that the dialogue is refused, with a refuse reason secured transport not possible. No retry of the dialogue with a lower version is allowed.

Sheet 5: If the intiating side receives a TC-U-ABORT with an abort reason AC not supported and secure transport is required, then secured transport is not possible. If fallback to unsecured transport is acceptable, the dialogue machine retries the dialogue with unsecured transport. If fallback to unsecured transport is not acceptable, this triggers a MAP-OPEN confirm indicating that the dialogue is refused, with a refuse reason secured transport not possible. No retry of the dialogue with a lower version is allowed.

Sheet 7: A TC-U-ABORT with a user-specific abort reason leads to a check of the user information. User information carrying a MAP-Refuse PDU with a refuse reason encapsulated AC not supported means that the responding entity supports the secure transport AC, but not the AC required for the protected request. This triggers a MAP-OPEN confirm indicating that the dialogue is refused, with a refuse reason AC not supported. The MAP-Service User may then decide to retry the dialogue with a lower AC version; this will again use secure transport. User information carrying a MAP-Refuse PDU with a refuse reason transport protection not adequate means that the responding entity is not prepared to accept a dialogue with the protection mode offered by the initiating entity: either unsecured transport or secured transport with an inadequate protection mode.

Sheet 9: When the the MAP dialogue state machine at the initiating side is waiting for a response from the responding side, a TC-CONTINUE indication which echoes the AC name which was sent in the TC-BEGIN indicates acceptance of the dialogue. If secure transport is required, acceptance of the dialogue opening request which was transported in the secure dialogue opening request is indicated by the encapsulated AC name transported in the user information of the TC- CONTINUE being equal to the encapsulated AC which was included in the user information of the TC-BEGIN. Mismatch of either the AC name or the encapsulated AC name indicates failure of the dialogue opening.

Sheet 9: If the dialogue opening is accepted, any components included in the TC-CONTINUE are processed and passed to the MAP-Service User. The dialogue has then reached the established state.

15.2.2   Behaviour at the responding side

The behaviour of the MAP dialogue state machine at the responding side is defined in sheets 10 – 14 of the process Secure_MAP_DSM.

Sheet 10: If no application context information is included in the TC-BEGIN indication, this implies a MAP version 1 dialogue. An explicit application context indicating version 1 is treated as abnormal behaviour.

Sheet 10, sheet 11: The test "Unsecured_Transport_Permitted" takes the "True" exit if there is an agreement between the operators of the dialogue initiating entity and the dialogue responding entity to allow unsecured transport for the application context for the requested dialogue. This requires the dialogue responding entity to store configuration information on which this decision is based.

Sheet 10: The task "Extract_User_Information" includes decryption of the protected user information if confidentiality protection has been applied.

Sheet 10: The test "Protection mode correct" takes the "yes" exit if the protection mode is acceptable to the receiving entity, based on the identity of the sending entity and the encapsulated application context for the requested dialogue.

Sheet 11: The v1 application context name which corresponds to a v1 operation is derived using the information in table 15.2/1.

Table 15.2/1: Mapping of V1 operation codes on to application-context-names

Operation	Application-context-name (note 1)
updateLocation	networkLocUpContext-v1
cancelLocation	locationCancellationContext-v1
provideRoamingNumber	roamingNumberEnquiryContext-v1
insertSubscriberData	subscriberDataMngtContext-v1
deleteSubscriberData	subscriberDataMngtContext-v1
sendParameters	infoRetrievalContext-v1
	networkLocUpContext-v1 (note 2)
beginSubscriberActivity	networkFunctionalSsContext-v1
sendRoutingInfo	locationInfoRetrievalContext-v1
performHandover	handoverControlContext-v1
reset	resetContext-v1
activateTraceMode	tracingContext-v1
deactivateTraceMode	tracingContext-v1
sendRoutingInfoForSM	shortMsgGatewayContext-v1
forwardSM	shortMsgRelayContext-v1
reportSM-deliveryStatus	shortMsgGatewayContext-v1
noteSubscriberPresent	mwdMngtContext-v1
alertServiceCentreWithoutResult	shortMsgAlertContext-v1
checkIMEI	EquipmentMngtContext-v1

NOTE 1: These symbolic names refer to the object identifier value defined in clause 17 and allocated to each application-context used for the MAP.

NOTE 2: The choice between the application contexts is based on the parameters received in the operation.

Sheet 12: If the AC name received in the TC-BEGIN indicated that secure transport is required, the MAP dialogue state machine checks whether the encapsulated application context name is supported. If it is supported, the dialogue can be accepted. If the encapsulated AC name is not supported, the MAP dialogue machine indicates this by sending a TC-U-ABORT with a user-specific abort reason and user information indicating that the encapsulated AC name is not supported.

Sheet 12: If the dialogue is accepted, each component present in the TC-BEGIN is forwarded to an instance of a Performing_MAP_SSM or Secure_Performing MAP_SSM, by executing the procedure Process_Components.

Sheet 13: If the MAP dialogue state machine receives a MAP-OPEN confirm with a result accepted, it waits for any MAP specific service request or response primitives or a MAP-DELIMITER request.

Sheet 14: A MAP-DELIMITER request triggers a TC-CONTINUE request to accept the dialogue. The dialogue has then reached the established state.

Sheet 13, sheet 14: When a dialogue is terminated, the MAP dialogue state machine terminates all instances of the Requesting_MAP_SSM, Secure_Requesting_MAP_SSM, Performing_MAP_SSM or Secure_Performing_MAP_SSM which are active for this dialogue.

Process Secure_MAP_DSM   MAP_DSM7(17)

Process to manage
a MAP dialogue

(4)

User_
Information

| User_Abort_PDU | Provider_Abort_PDU | Dialogue_Refused | No_User_Info |

Set_Result:
Dialogue_
Refused

Set_Result:
Dialogue_
Refused

MAP_
Refuse_PDU_
Error

| Encapsulated_ AC_Not_ Supported | Invalid_ Destination_ Reference | Invalid_ Originating_ Reference | No_ Reason_ Given |

Set_Refuse_
Reason: AC_
Not_Supported

Set_Refuse_Reason:
Invalid_Destination_
Reference

Set_Refuse_Reason:
Invalid_Originating_
Reference

Set_Refuse_Reason:
No_Reason_Given

Set_Refuse_Reason:
Potential_Version
_Incompatibility

MAP_U_ABORT
_Ind via USER2

MAP_P_ABORT_
Ind via USER2

MAP_OPEN_
cnf_VIA_User2

(FALSE)
Secure_
Transport_
Required

(TRUE)

To all active RSSMs

Terminated_
VIA_Intern2

Terminated_
VIA_Intern4

To all active SRSSMs

IDLE

IDLE

Process to manage
a MAP dialogue

4

User_
Information

User_Abort_PDU   Provider_Abort_PDU   Dialogue_Refused   No_User_Info

Set_Result: Set_Result:
Dialogue_   Dialogue_
Refused   Refused

MAP_
Refuse_PDU_
Error

Encapsulated_   Invalid_   Invalid_   Transport_   No_
AC_Not_   Destination_   Originating_   Protection_   Reason_
Supported   Reference   Reference   Not_Adequate   Given

Set_Refuse_   Set_Refuse_Reason: Set_Refuse_Reason: Set_Refuse_Reason: Set_Refuse_Reason:
Reason: AC_   Invalid_Destination_ Invalid_Originating_ Transport_Protection_ No_Reason_Given
Not_Supported   Reference   Reference   Not_Adequate

Set_Refuse_Reason:
Potential_Version
_Incompatibility

MAP_U_ABORT   MAP_P_ABORT_   MAP_OPEN_
_Ind via USER2   Ind via USER2   cnf_VIA_User2

(FALSE)   Secure_
Transport_
Required

(TRUE)

To all active RSSMs   Terminated_   Terminated_   To all active SRSSMs
                       VIA_Intern2   VIA_Intern4

IDLE   IDLE

Figure 15.6/3g: Process Secure_MAP_DSM (sheet 7)

Process to manage
a MAP dialogue

IDLE

TC_BEGIN_
ind

AC_
Included
(FALSE)
(TRUE)

AC_Version
=1
(FALSE)
(TRUE)

AC_Name=
Secure_
Transport
(TRUE)   (FALSE)

MAP_Protected_
Dialogue_PDU
included
(FALSE)   (TRUE)

Unsecured_
Transport_
Permitted
(FALSE)   (TRUE)

User_Info
required for
encapsulated AC?
Yes

Extract_User_
Information

6

Map_Dialogue_
PDU
included
(FALSE)   (TRUE)

Extract_User_
Information

MAP-OPEN
Dialogue
PDU?
No

Yes

Invalid
Parameter?
Yes

MAP-OPEN
Dialogue
PDU?
No

Yes

No

3

No

Invalid
Parameter?

3

Check_Load
_VIA_Load1

Yes

WAIT_FOR_
LOAD_CHECK_
RESULT1

6

User_Info
required
for AC?
Yes

No

Set_User_Info:
MAP_Refuse_PDU

Set_MAP_Provider_
Abort_Reason:
Abnormal_Dialogue

Set_Refuse_Reason_
Unsecured_Transport_
Not_Allowed

Set_User_Info:
MAP_Provider_
Abort_Info

Set_Abort_Reason:
User_Specific

Set_Abort_Reason:
User_Specific

Components_
Present
(FALSE)

(TRUE)

TC_U_ABORT_
req_VIA_TC1

Check_Load
_VIA_Load1

TC_U_ABORT_
req_VIA_TC1

IDLE

WAIT_FOR_
LOAD_CHECK_
RESULT1

IDLE

WAIT_FOR_
INIT_DATA

Figure 15.6/3j: Process Secure_MAP_DSM (sheet 10)

Process to handle MAP
service requests and the
responses from the distant
entity, using secure transport

WAIT_FOR_
CONFIRM

Linked_
Request_
Received

Linked_
Service_
Invoked

User_
Reject_
Received

Terminated

Extract_
Protected_
Request

Implicit_Cnf:=
TRUE

Terminated_
VIA_User6

Linked_
Request_
Received_
VIA_User6

Linked_
Service_
Invoked_
VIA_User6

WAIT_FOR_
CONFIRM

MAP_
Initiated

(FALSE)

(TRUE)

Set_Provider_
Error

Set_User_
Error

MAP_cnf_
VIA_User6

Terminated_
VIA_Intern6

Process to handle MAP
service requests and the
responses from the distant
entity, using secure transport

WAIT_FOR_
CONFIRM

Linked_
Request_
Received

Linked_
Service_
Invoked

User_
Reject_
Received

Terminated

Extract_
Protected_
Request

Implicit_Cnf:=
TRUE

Terminated_
VIA_Intern6

Linked_
Request_
Received_
VIA_User6

Linked_
Service_
Invoked_
VIA_User6

WAIT_FOR_
CONFIRM

MAP_
Initiated

(FALSE)

(TRUE)

Set_Provider_
Error

Set_User_
Error

MAP_cnf_
VIA_User6

Terminated_
VIA_Intern6

Figure 15.6/7c: Process Secure_Requesting_MAP_SSM (sheet 3)

Process to handle an invoke
component received from the
peer and the response from the user

WAIT_FOR_
RESPONSE

Guard_
Timer_
Expired

Response_
Issued   - by the MAP user

Terminated

User_Error_   (TRUE)
Present

(FALSE)

(FALSE)   Linked_
Request   Specific_   (FALSE)
Error

(TRUE)   (TRUE)

(TRUE)   Length_
O.K.

(FALSE)

Split_   2
info

TC_
RESULT_NL_
req_VIA_TC3

(FALSE)   more_   Set_Operation_   Set_Error_   Set_Problem_
data   Code_and_   Code   Code
TCAP_Param

(TRUE)

TC_   2   TC_INVOKE_   TC_U_ERROR_   TC_U_REJECT_
RESULT_L_   req_VIA_TC3   req_VIA_TC3   req_VIA_TC3
req_VIA_TC3

Process to handle an invoke
component received from the
peer and the response from the user

WAIT_FOR_
RESPONSE

Guard_
Timer_
Expired

Response_
Issued

by the MAP user or
the Secure_
Performing_MAP_SSM

Terminated

User_Error_
Present

(TRUE)

(FALSE)

(FALSE) Linked_
Request

(TRUE)

Specific_
Error

(FALSE)

(TRUE)

(TRUE)

Length_
O.K.

(FALSE)

Split_
info

2

TC_
RESULT_NL_
req_VIA_TC3

(FALSE)
more_
data

(TRUE)

TC_
RESULT_L_
req_VIA_TC3

2

Set_Operation_
Code_and_
TCAP_Param

Set_Error_
Code

Set_Problem_
Code

TC_INVOKE_
req_VIA_TC3

TC_U_ERROR_
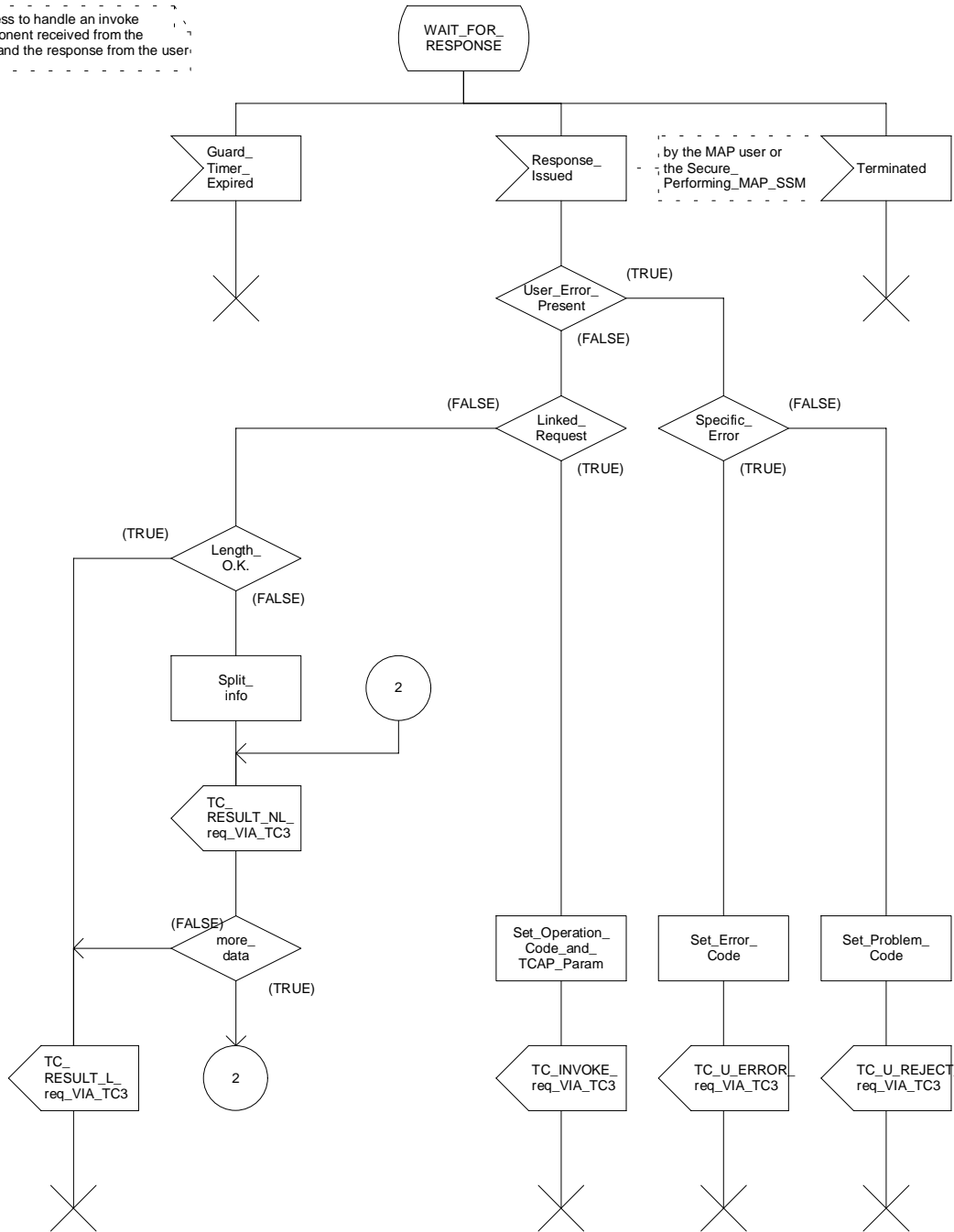req_VIA_TC3

TC_U_REJECT_
req_VIA_TC3

Figure 15.6/8b: Process Performing_MAP_SSM (sheet 2)

**** Next modified section ****

17.4   MAP Dialogue Information

```
MAP-DialogueInformation {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-DialogueInformation (3) version6 (6)}
.

.

.
```

```
Reason ::= ENUMERATED {
    noReasonGiven  (0),
    invalidDestinationReference        (1),
    invalidOriginatingReference        (2),
    encapsulatedAC-NotSupported        (3),
    transportProtectionNotAdequate        (4)}
    -- encapsulatedAC-NotSupported and transportProtectionNotAdequate must not be used
    -- in dialogues with an AC different from secureTransportHandling
```