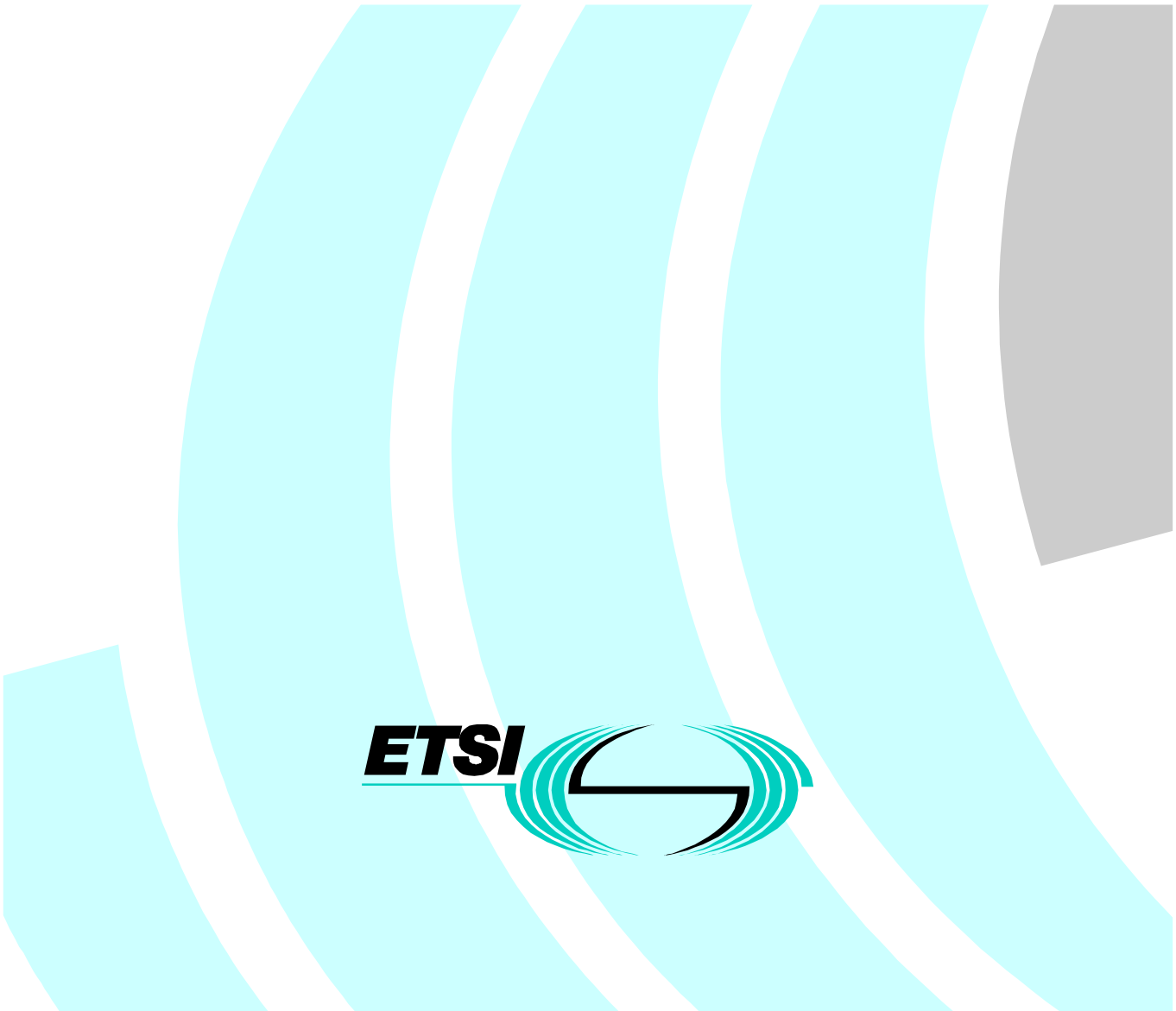
ETSI EN 301 144-1 V1.1.2 (2000-10)

European Standard (Telecommunications series)

**Integrated Services Digital Network (ISDN);
Digital Subscriber Signalling System No. one (DSS1)
and Signalling System No. 7 (SS7);
Signalling application for the mobility management service
on the alpha interface;
Part 1: Protocol specification**



Reference
DEN/SPS-05121-1

Keywords
CTM, DSS1, ISDN, protocol, SS7

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN).

The present document is part 1 of a multi-part deliverable covering the signalling application for the mobility management service on the alpha interface, as identified below:

Part 1: "Protocol specification";

Part 2: "Protocol Implementation Conformance Statement (PICS) proforma specification";

National transposition dates	
Date of adoption of this EN:	13 October 2000
Date of latest announcement of this EN (doa):	31 January 2001
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 July 2001
Date of withdrawal of any conflicting National Standard (dow):	31 July 2001

1 Scope

This first part of EN 301 144 specifies the stage 3 of the signalling application for the mobility management service on the alpha interface. The mobility management service functions include Cordless Terminal Mobility (CTM) for CTM phase 1 (DECT/GAP limitation) and DECT access to GSM via an Integrated Services Digital Network (ISDN) user-network interface at the T reference point or coincident S and T reference point (as defined in ITU-T Recommendation I.411 [18]) by means of the Digital Subscriber Signalling System No. one (DSS1) protocol. Stage three identifies the protocol procedures and switching functions needed to support a telecommunication service (see CCITT Recommendation I.130 [15]).

The signalling application for the alpha interface describes the mobility management procedures required to allow users of cordless terminals to be mobile within and between networks. Whenever radio coverage is provided and the cordless terminal has appropriate access rights, the user is able to make calls from and to receive calls at, any location within the network.

The signalling application for the alpha interface is applicable to the telephony 3,1 kHz teleservice (see ETS 300 111 [3]), speech bearer service (see ETS 300 109 [1]) and 3,1 kHz audio bearer service (see ETS 300 110 [2]).

Further parts of EN 301 144 specify the method of testing required to identify conformance to the present document.

The present document is applicable to equipment supporting the signalling application for the alpha interface, to be attached at either side of a T reference point and coincident S and T reference point when used as an access to the public ISDN or GSM network.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] ETS 300 109 (1992): "Integrated Services Digital Network (ISDN); Circuit-mode 64 kbit/s 8 kHz structured bearer service category usable for speech information transfer; Service description".

[2] ETS 300 110 (1992): "Integrated Services Digital Network (ISDN); Circuit-mode 64 kbit/s 8 kHz structured bearer service category usable for 3,1 kHz audio information transfer; Service description".

[3] ETS 300 111 (1992): "Integrated Services Digital Network (ISDN); Telephony 3,1 kHz teleservice; Service description".

[4] EN 300 175-5: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer".

[5] EN 300 175-6: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".

[6] EN 300 175-7: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".

[7] EN 300 196-1 (V1.2): "Integrated Services Digital Network (ISDN); Generic functional protocol for the support of supplementary services; Digital Subscriber Signalling System No. one (DSS1) protocol; Part 1: Protocol specification".

[8] EN 300 370: "Digital Enhanced Cordless Telecommunications (DECT); Global System for Mobile communications (GSM); DECT/GSM Interworking Profile (IWP); Access and mapping (protocol/procedure description for 3,1 kHz speech service)".

[9] EN 300 403-1 (V1.2): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

[10] EN 300 444 (V1.2): "Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)".

[11] ETS 300 557: "Digital cellular telecommunications system (Phase 2); Mobile radio interface; Layer 3 specification (GSM 04.08 version 4.19.2)".

[12] ETS 300 788: "Digital Enhanced Cordless Telecommunications (DECT); Global System for Mobile communications (GSM); Integrated Services Digital Network (ISDN); DECT access to GSM via ISDN; Functional capabilities and information flows".

[13] ITU-T Recommendation E.164 (1997): "The international public telecommunication numbering plan".

[14] ITU-T Recommendation I.112 (1993): "Vocabulary of terms for ISDNs".

[15] CCITT Recommendation I.130 (1988): "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[16] ITU-T Recommendation I.210 (1993): "Principles of telecommunication services supported by an ISDN and the means to describe them".

[17] ITU-T Recommendation I.221 (1993): "Common specific characteristics of services".

[18] ITU-T Recommendation I.411 (1993): "ISDN user-network interfaces - reference configurations".

[19] CCITT Recommendation X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)".

[20] CCITT Recommendation X.219 (1988): "Remote operations: Model, notation and service definition".

[21] ITU Recommendation X.229 (1992): "Remote operations: Protocol specification".

[22] Amendment 1 to ITU-T Recommendation X.680 (04/95): "Information technology - Abstract Syntax Notation One (ASN.1); Specification of basic notation - Amendment 1: Rules of extensibility".

[23] ITU Recommendation X.880: "Information technology - Remote Operations: Concepts, model and notation".

3 Definitions and abbreviations

3.1 Definitions

For the purpose of the present document, the following terms and definitions apply:

Authentication Code: may be held in non-volatile memory within the PP or may be manually entered by the user when required for an authentication service, depending on the application; see EN 300 175-7 [6].

access rights: an indication that the cordless terminal has appropriate access allowance to the CTM service.

Access Rights Identity: an identity which is globally unique to a service provider and which shows the access rights related to the service provider.

authentication: a security mechanism allowing the verification of the provided identity.

cipher key: see EN 300 175-7 [6] clause 3.

cordless terminal: a physical entity that provides access to the telecommunication service of a network via a radio interface.

cordless terminal mobility: the ability of a cordless terminal to be mobile within and between fixed parts; the mobility may be continuous while the terminal is accessing and using the telecommunication services offered by the network, and it may include the capability of the networks to keep track of the cordless terminal's location throughout the entire network.

core service feature: particular service feature fundamental to the telecommunication services, i.e. in the absence of this service feature, the telecommunication service does not make sense as a commercial offering to the service subscriber.

coverage area: the area within the radio coverage area in which the user has subscribed to use the mobility management service.

CTM number: number that uniquely and unambiguously identifies each CTM subscriber. It is used by a calling party to reach the CTM subscriber. The number is independent of the calling terminal, network or service used and conform to ITU-T Recommendation E.164 [13].

DECT paging: a DECT procedure which establishes a link on the DECT interface.

Fixed Part: a physical grouping that contains all elements in the cordless network between the local network and the cordless terminal air interface.

Fixed Termination: a logical group of functions that contain all of the Cordless Terminal (CT) Network specific processes and procedures on the fixed side of the air interface. A Fixed Radio Termination only includes elements that are defined in the relevant CT specifications. This includes radio transmission elements (layer1) together with a selection of layer 2 and layer 3 elements.

handover: the process by which a call in progress is maintained when the user moves with the cordless terminal with a call in progress within a network where continuous radio coverage is provided.

IMSI attach: see ETS 300 557 [11].

location area: the radio coverage area in which a cordless terminal may receive calls as a result of a single location registration.

network: the entity which provides the mobility management function and basic call functionality to the user.

network operator: an entity that provides the network operating elements and resources for the execution of the mobility management service.

optional service feature: a service feature added to core feature to optionally enhance a service offering.

portable application: a logical grouping that contains all the elements that lie beyond the CT Network boundary on the portable side.

portable identity: the identity by which a subscriber is known to the mobility management service providers and networks supporting mobility management, and used for flexibility and security purposes; identifies a subscriber unambiguously; does not need to be known by subscriber.

Portable Part: a physical grouping that contains all elements between the user and air interface; a generic term that may describe one or several physical pieces.

portable termination: a logical group of functions that contains all of the CT processes and procedures on the portable side of the CT air interface; only includes elements that are defined in the relevant CT specification.

public land mobile network: see ETS 300 788 [12].

radio coverage: the area in which cordless terminals may be used to establish and maintain telecommunication services via the radio base stations supported by the network supporting the mobility management service.

RANDom challenge: a parameter used for authentication; see EN 300 175-7 [6].

RES1: a parameter containing the result of the terminal authentication challenge; see EN 300 175-7 [6].

RES2: a parameter containing the result of the network authentication challenge, see EN 300 175-7 [6].

RS: a value used to establish authentication session keys, as defined in subclause 4.4.3 of EN 300 175-7 [6].

roaming: movement of the cordless terminal user without a call in progress from one location area to another location area within the same or between different networks supporting the mobility management service.

service feature: a specific aspect of a telecommunication service that can be used in conjunction with other telecommunication services or service features as part of a commercial offering; either a core part of a telecommunication service or an optional part offered as an enhancement to a telecommunication service.

service profile: a record containing all the service information related to a user.

service provider: an actor who provides mobility management services to its service subscribers on a contractual basis and who is responsible for the mobility management services offered; the same organization may act as a network operator and a service provider.

service subscriber: an entity that contracts for services offered by service providers.

service: that which is offered by an administration or a public or private service provider to its service subscriber in order to satisfy a telecommunication requirement.

telecommunication service: see ITU-T Recommendation I.112 [14].

terminal mobility: the ability of a terminal to access telecommunication services, while in motion, and the capability of the network to locate and identify that terminal as it moves.

User Authentication Key: secret authentication data contained within the subscriber's registration data, uniquely associated with the particular subscriber (user) and the subscription; held in non-volatile memory within the PP (or within a detachable DECT Authentication Module (DAM); see EN 300 175-7 [6].

user: the DSS1 protocol entity at the user side of the user-network interface; see EN 300 196-1 [7].

3.2 Abbreviations

For the purpose of the present document, the following abbreviations apply:

AC	Authentication Code
ARC	Access Right Class
ARD	Access Right Details
ARI	Access Right Identity
ASN.1	Abstract Syntax Notation one
BA	Basic Access
CT	Cordless Terminal
CTM	Cordless Terminal Mobility
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunication
DSSA	DECT Standard Authentication Algorithm
DSS1	Digital Subscriber Signalling System 1
FT	Fixed Termination
FP	Fixed Part
GAP	Generic Access Profile
GSM	Global System for Mobile communications
IMEI	International Mobile station Equipment Identity
IMEISV	International Mobile station Equipment Identity Software Version
IMSI	International Mobile Subscriber Identity
IPEI	International Portable Equipment Identity
IPUI	International Portable User Identity
ISDN	Integrated Services Digital Network
LE	Local Exchange
MM	Mobility Management
MSC	Mobile Switching Centre

NCICS	Networked Call Independent Connection-Oriented Signalling
NT	Network Termination
NT2	Network Termination type 2
PA	Portable Application
PARK	Portable Access Right Key
PLI	Park Length Indicator
PLMN	Public Land Mobile Network
PP	Portable Part
RAND	RANDom challenge
RBS	Radio Base Station
RE	Radio Exchange
RES	RESponse
RES1	RESponse1
RES2	RESponse2
RFPI	Radio Fixed Part Identity
Rs	Result
TMSI	Temporary Mobile Subscriber Identity
UAK	User Authentication Key

4 Void

5 Description

The Cordless Terminal Mobility (CTM) service phase 1 allows subscribers of Cordless Terminals (CTs) to be mobile within and between networks. Where radio coverage is provided and the CT has appropriate access rights the subscriber shall be able to make calls from, and to receive calls at, any location within the fixed public and/or private networks.

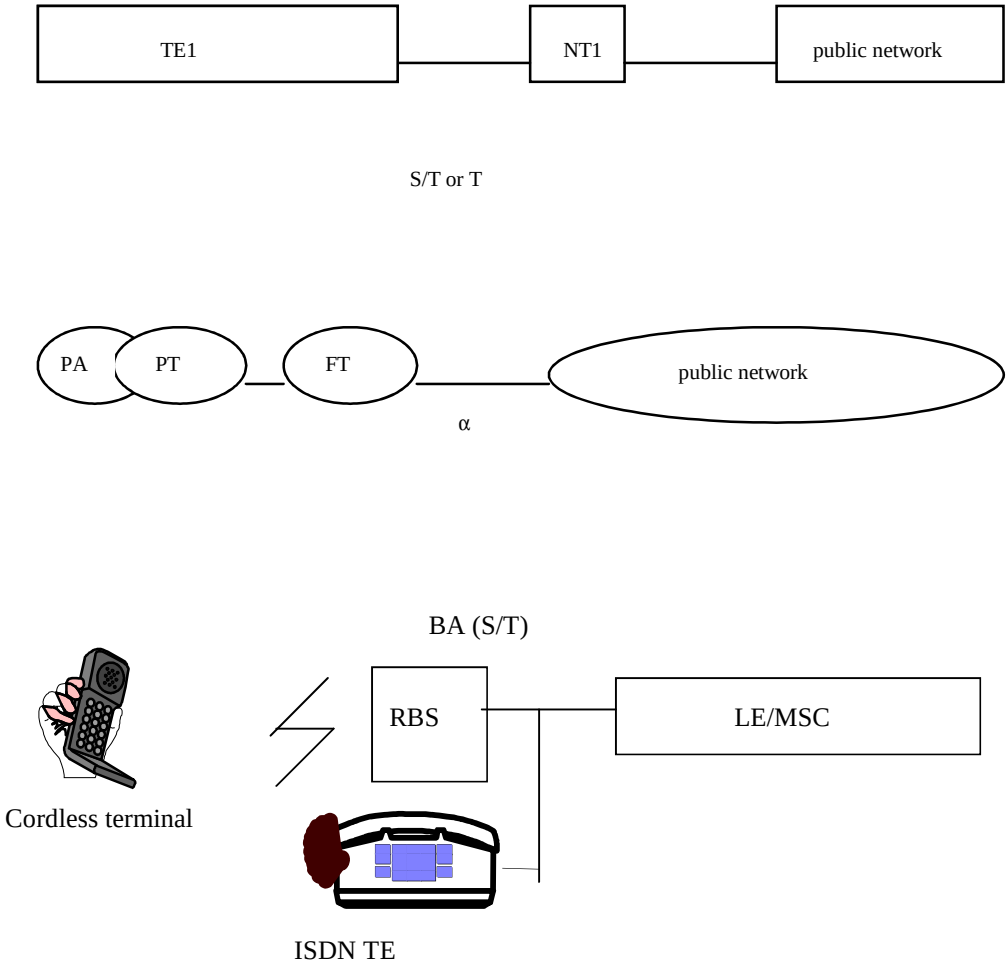
The provision of GSM basic service over the DECT air interface for the case that the DECT access network is connected with the GSM PLMN via an ISDN user-network interface enables GSM subscribers to be mobile within and between DECT access networks using the GSM PLMN infrastructure. Where DECT radio coverage is provided and the DECT portable part has appropriate access rights the subscriber shall be able to make calls from, and to receive calls at, any location within the network.

The signalling procedures in the present document are supporting features required for CTM phase 1 and features to provide GSM basic services over the DECT air interface via the public ISDN user-network interface.

Table 1: Procedures required for CTM phase 1 and DECT/GSM access

	initiated by	CTM phase 1		DECT/GSM access	
Procedure		user	network	user	network
9.1 Registration and deregistration					
Subscription registration	user	optional	optional	-	-
Subscription deregistration	network	optional	optional	-	-
9.2 Activation and deactivation					
Location registration	user	mandatory	mandatory	mandatory (note)	mandatory
Location cancellation	network	mandatory	mandatory	optional	optional
Detach	user	-	-	mandatory	mandatory
9.3 Invocation and operation					
Location Registration Suggest	network	mandatory	optional	-	-
Terminal authentication	network	mandatory	mandatory	mandatory	mandatory
Network authentication	user	mandatory	mandatory	-	-
Network initiated ciphering	network	mandatory	mandatory	mandatory	mandatory
Portable initiated ciphering	user	optional	optional	-	-
Temporary identity assignment	network	-	-	mandatory	mandatory
Linked temporary identity assignment	network	-	-	mandatory	optional
Key allocation	network	mandatory	mandatory	-	-
Identity request	network	mandatory	optional	mandatory	mandatory
Outgoing call	user	mandatory	mandatory	mandatory	mandatory
Incoming call	network	mandatory	mandatory	mandatory	mandatory
NOTE: The location update procedure as described in ETS 300 788 [12] is identical to the location registration procedure described in the present document.					

For CTM phase 1, the following reference configurations of figures 1 and 2 are applicable at the alpha interface:



The public network may be represented either as an ISDN or a PLMN.
The FT in the residential configuration is a simple single-cell Radio Base Station (RBS).
On the S/T reference point (BA), ISDN terminals may also be connected.

Figure 1: Residential configuration

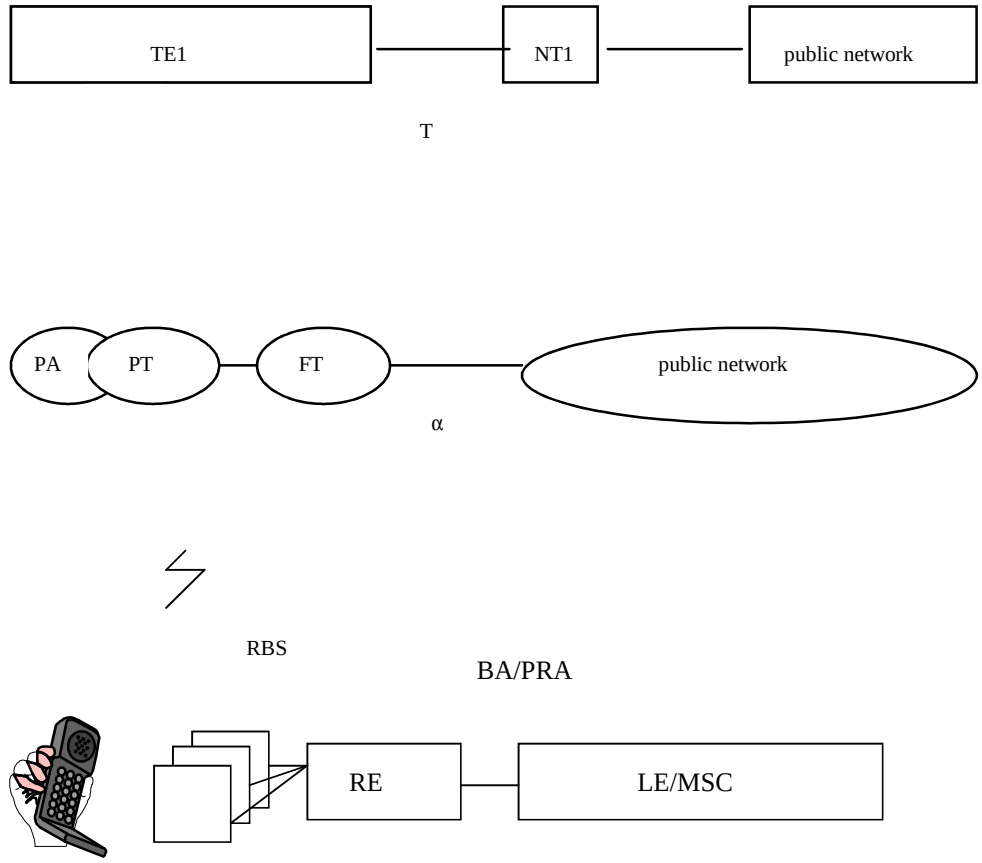


Figure 2: Public access configuration with advanced Cordless Network (NT2 without mobility management function)

Figure 2 refers to the situation where the FT is more advanced than the residential configuration and is implemented as a cluster of Radio Base Stations (RBSs) and a Radio Exchange. The Radio Exchange has an NT2 functionality without mobility management functions.

6 Operational requirements

6.1 Provision and withdrawal

The mobility management service shall be provided after prior arrangement with the service provider. The service subscriber and the service provider have a contractual relationship and agree upon the service details. As a result of this agreement, the service provider and the involved network operators shall make arrangements for service provision by the network(s).

The network shall be able to maintain a service profile for the service subscriber.

The mobility management service shall be withdrawn from a specific subscriber upon request of the service subscriber or for service provider reasons.

Table 2: Service provider option

Service provider option	Value	Meaning
Support of "CTM" mode	Yes No	
Support of "DECT access to GSM" mode	Yes No	
Support of the subscription registration procedure (NOTE 1)	Yes No	The service provider supports the on-air subscription registration procedure for CTM.
Support of the subscription deregistration procedure(NOTE 1)	Yes No	The service provider supports the on-air subscription deregistration procedure for CTM.
The call is released in case of an unsuccessful terminal authentication procedure (NOTE 1)	Yes No	
The call is released in case of an unsuccessful ciphering procedure (NOTE 1)	Yes No	
Use of the GSMTerminalAuthenticationReject procedure (NOTE 2)	Yes No	
Support of the GSMLinkedAssignIdentity procedure (NOTE 2)	Yes No	
NOTE 1: This option exists only when the value of the option 'support of "CTM" mode' is "Yes". NOTE 2: This option exists only when the value of the option 'support of " DECT access to GSM " mode' is "Yes".		

6.2 Requirements on the network A side

The requirements at the originating network side are covered in clause 9.

6.3 Requirements on the network B side

The requirements at the destination network side are covered in clause 9.

7 Coding requirements

Table 3 shows the definitions of the operations and errors required for the mobility management service using ASN.1 as specified in CCITT Recommendation X.208 [19] and using the OPERATION and ERROR macro as defined in figure 4/X.219 of ITU Recommendations X.219 [20].

The formal definitions of the component types to encode these operations and errors are provided in EN 300 196-1 [7], annex D, subclause D.1.

All components (invoke, return result, return error and reject) shall be included within a Facility information element. This Facility information element may be included in any appropriate message as specified in EN 300 196-1 [7], subclause 8.3.1.1 as enhanced by, annex E unless a more restrictive specification is given in clause 9.

The inclusion of the components in Facility information elements is defined in EN 300 196-1 [7], subclause 11.2.2.1 as enhanced by annex E.

In order to introduce extensions to the current arguments and results based on the ellipses notation (see Amendment 1 to ITU-T Recommendation X.680 [22]), a bilateral agreement shall exist between the network and the user.

Table 3: ASN.1 description of the operations and errors for the mobility management service used at the coincident S and T reference point and T reference point

```
MobilityManagement-Operations-and-Errors {ccitt identified-organization etsi(0) 1144
                                                                operations-and-errors(1)}

DEFINITIONS IMPLICIT TAGS ::=

BEGIN

EXPORTS     CTMAccessRightsRequest,
            CTMAccessRightsTerminate,
            CTMLocationRegistration,
            CTMLocationCancellation,
            CTMLocationRegistrationSuggest,
            CTMTerminalAuthentication,
            CTMNetworkAuthentication,
            CTMCiphering,
            CTMCipheringSuggest,
            CTMKeyAllocate,
            CTMIdentityRequest,
            CTMOutgoingCallMMInfo,
            CTMIncomingCallMMInfo,

            GSMLocationRegistration,
            GSMLocationCancellation,
            GSMDetach,
            GSMTerminalAuthentication,
            GSMTerminalAuthenticationReject,
            GSMCiphering,
            GSMAssignIdentity,
            GSMLinkedAssignIdentity,
            GSMIdentityRequest,
            GSMOutgoingCallMMInfo,
            GSMIncomingCallMMInfo,

            NetworkRejected,
            TerminalRejected,
            PortableIdentityUnknown,
            IdentityNotAvailable,
            Congestion,
            LocalTimerExpiry,
            PagingFailure,
            RadioConnectionFailure,
            IncompatibleCipheringState,
            PriorityRuleViolation,
            Unspecified

IMPORTS     OPERATION, ERROR
            FROM Remote-Operation-Notation
                {joint-iso-ccitt remote-operations(4) notation(0)}

            notSubscribed, resourceUnavailable
            FROM General-Errors
                {ccitt identified-organization etsi(0) 196 general-errors(2)}

            IMSI, TMSI, IMEI
            FROM MAP-CommonDataTypes
                {ccitt identified-organization(4) etsi(0) mobileDomain(0)
                gsm-Network(1) modules(3) map-CommonDataTypes(18) version3(3)}
                                    -- ETS 300 599

CTMAccessRightsRequest      ::= OPERATION
                ARGUMENT
                    cTMAccessRightsRequestArg   CTMAccessRightsRequestArg
                RESULT
                    cTMAccessRightsRequestRes   CTMAccessRightsRequestRes
                ERRORS {NetworkRejected,
                        portableIdentityUnknown,
                        congestion,
                        unspecified}
-- End of CTMAccessRightsRequest operation definition

CTMAccessRightsTerminate        ::= OPERATION
                ARGUMENT
                    cTMAccessRightsTerminateArg  CTMAccessRightsTerminateArg
                RESULT
                ERRORS {TerminalRejected,
```

```
                        pagingFailure,
                        radioConnectionFailure,
                        portableIdentityUnknown,
                        congestion,
                        localTimerExpiry,
                        priorityRuleViolation,
                        unspecified}
-- End of CTMAccessRightsTerminate operation definition

CTMLocationRegistration     ::= OPERATION
                ARGUMENT
                    cTMLocationRegistrationArg  CTMLocationRegistrationArg
                RESULT
                    cTMLocationRegistrationRes  CTMLocationRegistrationRes
                ERRORS {NetworkRejected,
                        portableIdentityUnknown,
                        congestion,
                        unspecified}
-- End of CTMLocationRegistration operation definition

GSMLocationRegistration ::=     OPERATION
                ARGUMENT
                        gSMLocationRegistrationArg  GSMLocationRegistrationArg
                RESULT
                        gSMLocationRegistrationRes  GSMLocationRegistrationRes
                ERRORS {NetworkRejected,
                        portableIdentityUnknown,
                        congestion,
                        unspecified}
                LINKED {gSMLinkedAssignIdentity}
-- End of GSMLocationRegistration operation definition

GSMLocationCancellation ::=     OPERATION
                ARGUMENT
                    gSMLocationCancellationArg      GSMLocationCancellationArg
-- End of GSMLocationCancellation operation definition

CTMLocationCancellation ::=     OPERATION
                ARGUMENT
                    cTMLocationCancellationArg      CTMLocationCancellationArg
                RESULT
                ERRORS {portableIdentityUnknown,
                        congestion,
                        unspecified}
-- End of CTMLocationCancellation operation definition

GSMDetach           ::= OPERATION
                ARGUMENT
                    gSMDetachArg    GSMDetachArg
-- End of GSMDetach operation definition

CTMLocationRegistrationSuggest  ::= OPERATION
                ARGUMENT
                    cTMLocationRegistrationSuggestArg   CTMLocationRegistrationSuggestArg
                ERRORS {portableIdentityUnknown,
                        pagingFailure,
                        radioConnectionFailure,
                        congestion,
                        priorityRuleViolation,
                        unspecified}
-- End of CTMLocationRegistrationSuggest operation definition

CTMTerminalAuthentication   ::= OPERATION
                ARGUMENT
                    cTMTerminalAuthenticationArg        CTMTerminalAuthenticationArg
                RESULT
                    cTMTerminalAuthenticationRes        CTMTerminalAuthenticationRes
                ERRORS {TerminalRejected,
                        portableIdentityUnknown,
                        congestion,
                        localTimerExpiry,
                        pagingFailure,
                        radioConnectionFailure,
                        priorityRuleViolation,
                        unspecified}
-- End of CTMTerminalAuthentication operation definition

GSMTerminalAuthentication ::=       OPERATION
```

```
                ARGUMENT
                    gSMTerminalAuthenticationArg        GSMTerminalAuthenticationArg
                RESULT
                    gSMTerminalAuthenticationRes        GSMTerminalAuthenticationRes
                ERRORS {TerminalRejected,
                        portableIdentityUnknown,
                        congestion,
                        localTimerExpiry,
                        pagingFailure,
                        radioConnectionFailure,
                        priorityRuleViolation,
                        unspecified}
-- End of GSMTerminalAuthentication operation definition

GSMTerminalAuthenticationReject ::=     OPERATION
-- End of GSMTerminalAuthenticationReject operation definition

CTMNetworkAuthentication ::=    OPERATION
                ARGUMENT
                    cTMNetworkAuthenticationArg         CTMNetworkAuthenticationArg
                RESULT
                    cTMNetworkAuthenticationRes         CTMNetworkAuthenticationRes
                ERRORS {NetworkRejected,
                        portableIdentityUnknown,
                        congestion,
                        unspecified}
-- End of CTMNetworkAuthentication operation definition

CTMCiphering    ::= OPERATION
                ARGUMENT
                    cTMCipheringArg     CTMCipheringArg
                RESULT
                ERRORS {TerminalRejected,
                        portableIdentityUnknown,
                        congestion,
                        localTimerExpiry,
                        pagingFailure,
                        radioConnectionFailure,
                        incompatibleCipheringState,
                        priorityRuleViolation,
                        unspecified}
-- End of CTMCiphering operation definition

GSMCiphering    ::= OPERATION
                ARGUMENT
                    gSMCipheringArg     GSMCipheringArg
                RESULT
                ERRORS {TerminalRejected,
                        portableIdentityUnknown,
                        congestion,
                        localTimerExpiry,
                        pagingFailure,
                        radioConnectionFailure,
                        incompatibleCipheringState,
                        priorityRuleViolation,
                        unspecified}
-- End of GSMCiphering operation definition

CTMCipheringSuggest ::=     OPERATION
                ARGUMENT
                    cTMCipheringSuggestArg  CTMCipheringSuggestArg
                ERRORS {NetworkRejected,
                        portableIdentityUnknown,
                        congestion,
                        unspecified}
-- End of CTMCipheringSuggest operation definition

GSMAssignIdentity   ::=     OPERATION
                ARGUMENT
                    gSMAssignIdentityArg    GSMAssignIdentityArg
                RESULT
-- End of GSMAssignIdentity operation definition

GSMLinkedAssignIdentity ::= OPERATION
                ARGUMENT
                    gsMLinkedAssignIdentityArg  GSMLinkedAssignIdentityArg
                RESULT
-- End of GSMLinkedAssignIdentity operation definition
```

```
CTMKeyAllocate      ::= OPERATION
                ARGUMENT
                    cTMKeyAllocateArg       CTMKeyAllocateArg
                RESULT
                    cTMKeyAllocateRes       CTMKeyAllocateRes
                ERRORS {TerminalRejected,
                        portableIdentityUnknown,
                        congestion,
                        localTimerExpiry,
                        pagingFailure,
                        radioConnectionFailure,
                        priorityRuleViolation,
                        unspecified}
                LINKED {cTMNetworkAuthentication}
-- End of CTMKeyAllocate operation definition

CTMIdentityRequest      ::= OPERATION
                ARGUMENT
                    cTMIdentityRequestArg       CTMIdentityRequestArg
                RESULT
                    cTMIdentityRequestRes       CTMIdentityRequestRes
                ERRORS {identityNotAvailable,
                        portableIdentityUnknown,
                        congestion,
                        localTimerExpiry,
                        priorityRuleViolation,
                        pagingFailure,
                        radioConnectionFailure,
                        unspecified}
-- End of CTMIdentityrequest operation definition

GSMIdentityRequest      ::= OPERATION
                ARGUMENT
                    gSMIdentityRequestArg       GSMIdentityRequestArg
                RESULT
                    gSMIdentityRequestRes       GSMIdentityRequestRes
                ERRORS {identityNotAvailable,
                        portableIdentityUnknown,
                        congestion,
                        localTimerExpiry,
                        priorityRuleViolation,
                        pagingFailure,
                        radioConnectionFailure,
                        unspecified}
-- End of GSMIdentityrequest operation definition

CTMOutgoingCallMMInfo   ::= OPERATION
                ARGUMENT
                    cTMOcInfoArg        CTMOcInfoArg}
                ERRORS {NetworkRejected,
                        portableIdentityUnknown,
                        congestion,
                        unspecified}
-- End of CTMOutgoingCallMMInfo operation definition

CTMIncomingCallMMInfo   ::= OPERATION
                ARGUMENT
                    cTMIcInfoArg        CTMIcInfoArg
                ERRORS {TerminalRejected,
                        portableIdentityUnknown,
                        congestion,
                        pagingFailure,
                        radioConnectionFailure,
                        unspecified}
-- End of CTMIncomingCallMMInfo operation definition

GSMOutgoingCallMMInfo   ::= OPERATION
                ARGUMENT
                    gSMOcInfoArg        GSMOcInfoArg
                ERRORS {NetworkRejected,
                        portableIdentityUnknown,
                        congestion,
                        unspecified}
-- End of GSMOutgoingCallMMInfo operation definition

GSMIncomingCallMMInfo   ::= OPERATION
                ARGUMENT
```

```
                    gSMIcInfoArg        GSMIcInfoArg
                ERRORS {TerminalRejected,
                        portableIdentityUnknown,
                        congestion,
                        pagingFailure,
                        radioConnectionFailure,
                        unspecified}
-- End of GSMIncomingCallMMInfo operation definition

CTMOcInfoArg            ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity,
                        cTMFixedIdentity        [1] FixedIdentity,
                        cTMBasicService         [2] BasicService
                        --,...
                        }

CTMIcInfoArg            ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity,
                        cTMSignal               [1] Signal
                        --,...
                        }

GSMOcInfoArg            ::= SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity,
                        gSMBasicService         [1] BasicService
                        --,...
                        }

GSMIcInfoArg            ::= SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity,
                        gSMSignal               [1] Signal
                        --,...
                        }

CTMAccessRightsRequestArg   ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity,
                        cTMAuthType             [1] AuthType,
                        cTMPortableCapabilities [2] PortableCapabilities
                        --,...
                        }

CTMAccessRightsRequestRes   ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity,
                        cTMFixedIdentity        [1] FixedIdentity,
                        cTMServiceClass         [2] ServiceClass OPTIONAL
                        --,...
                        }

CTMAccessRightsTerminateArg ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity,
                        cTMFixedIdentity        [1] FixedIdentity
                        --,...
                        }

CTMLocationRegistrationArg  ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity,
                        cTMOldLocationAreaIdentity
                                                [1] CTMLocationAreaIdentity,
                        cTMNewLocationAreaIdentity
                                                [2] CTMLocationAreaIdentity,
                        cTMPortableCapabilities [3] PortableCapabilities
                        --,...
                        }

CTMLocationRegistrationRes  ::= SEQUENCE {
                        NULL
                        --,...
                        }

GSMLocationRegistrationArg  ::= SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity,
                        gSMLocationRegistrationType
                                                [1] LocationRegistrationType,
                        gSMLocationAreaIdentity [2] GSMLocationAreaIdentity,
                        gSMCipherInfo           [3] CipherInfo,
                        gSMPortableCapabilities [4] PortableCapabilities
                        --,...
                        }
```

```
GSMLocationRegistrationRes  ::= SEQUENCE {
                        gSMLocationAreaIdentity [0] GSMLocationAreaIdentity
                        --,...
                        }

CTMLocationCancellationArg  ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity
                        --,...
                        }

GSMLocationCancellationArg  ::= SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity
                        --,...
                        }

GSMDetachArg                ::= SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity
                        --,...
                        }

CTMLocationRegistrationSuggestArg   ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity
                        --,...
                        }

CTMTerminalAuthenticationArg        ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity    OPTIONAL,
                        cTMAuthType             [1] AuthType,
                        cTMRand                 [2] Rand,
                        cTMRs                   [3] Rs
                        --,...
                        }

CTMTerminalAuthenticationRes        ::= SEQUENCE {
                        cTMRes                  [0] Res,
                        cTMServiceClass         [1] ServiceClass        OPTIONAL
                        --,...
                        }

GSMTerminalAuthenticationArg        ::= SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity    OPTIONAL,
                        gSMRand                 [1] Rand,
                        gSMCipherInfo           [2] CipherInfo
                        --,...
                        }

GSMTerminalAuthenticationRes        ::= SEQUENCE {
                        gSMRes                  [0] Res
                        --,...
                        }

CTMNetworkAuthenticationArg         ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity    OPTIONAL,
                        cTMAuthType             [1] AuthType,
                        cTMRand                 [2] Rand
                        --,...
                        }

CTMNetworkAuthenticationRes         ::= SEQUENCE {
                        cTMRes                  [0]     Res,
                        cTMRs                   [1]     Rs              OPTIONAL
                        --,...
                        }

CTMCipheringArg         ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity    OPTIONAL,
                        cTMCipherInfo           [1] CipherInfo,
                        cTMCipherKey            [2] CipherKey
                        --,...
                        }

GSMCipheringArg         ::= SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity    OPTIONAL,
                        gSMCipherKey            [1] CipherKey
                        --,...
                        }
```

```
CTMCipheringSuggestArg  ::= SEQUENCE{
                        cTMPortableIdentity     [0] PortableIdentity    OPTIONAL,
                        cTMCipherInfo           [1] CipherInfo
                        --,...
                        }

GSMAssignIdentityArg    ::= SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity OPTIONAL,
                        gSMLocationAreaIdentity [1] GSMLocationAreaIdentity,
                        gSMNewTMSI              [2] PortableIdentity
                        --,...
                        }

GSMLinkedAssignIdentityArg  ::= SEQUENCE {
                        gSMNewTMSI              [0] PortableIdentity
                        --,...
                        }

CTMKeyAllocateArg       ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity    OPTIONAL,
                        cTMAllocType            [1] AllocType,
                        cTMRand                 [2] Rand,
                        cTMRs                   [3] Rs
                        --,...
                        }

CTMKeyAllocateRes       ::= SEQUENCE {
                        cTMRes                  [0] Res
                        --,...
                        }

GSMIdentityRequestArg   ::= SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity    OPTIONAL,
                        gSMIdentityType         [1] IdentityType
                        --,...
                        }

CTMIdentityRequestArg   ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity    OPTIONAL,
                        cTMIdentityType         [1] IdentityType
                        --,...
                        }

GSMIdentityRequestRes   :: SEQUENCE {
                        gSMPortableIdentity     [0] PortableIdentity
                        --,...
                        }

CTMIdentityRequestRes   ::= SEQUENCE {
                        cTMPortableIdentity     [0] PortableIdentity
                        --,...
                        }

PortableIdentity    ::= CHOICE {
                                iPUI [0] IPUI,
                                iMSI [1] IMSI,
                                iMEI [2] IMEI,
                                tMSI [3] TMSI,
                                NULL
                                --,...
                                }
                    -- further details on the correct usage of the portable identity can be
                    -- found in clause 9

FixedIdentity       ::= BIT STRING          -- as encoded either in EN 300 175-5, 7.7.18,
                                            -- or ETS 300 444, table 51

IPUI                ::= BIT STRING          -- as encoded in EN 300 175-6, 6.2

AuthType            ::= OCTET STRING        -- as encoded in EN 300 175-5, 7.7.4

AllocType           ::= OCTET STRING        -- as encoded in EN 300 175-5, 7.7.2

PortableCapabilities     ::= OCTET STRING   -- as encoded in EN 300 175-5, 7.7.41
                                            -- with applicable GSM mappings as defined in
                                            -- EN 300 370, table 7

CTMLocationAreaIdentity  ::=    BIT STRING  -- containing an RFPI as encoded in EN 300 175-6
```

```
                                        -- subclause 5 figure 4, truncated to the length
                                        -- corresponding to the relevant LAL.

GSMLocationAreaIdentity ::= BIT STRING      -- as encoded in Location Area EN 300 175-5, 7.7.25

LocationRegistrationType ::= ENUMERATED {normal_updating(0), periodic_updating(1), imsi_attach(2)}

IdentityType            ::= ENUMERATED{imsi(0), tmsi(1), imei(2), imeisv(3), ipui(4), ipei(5)}

CipherKey           ::= OCTET STRING        -- as encoded in EN 300 175-7, 4.4.3.3
                                            -- with applicable GSM mappings as
                                            -- defined in EN 300 370, annex A

CipherInfo          ::= OCTET STRING        -- as encoded in EN 300 175-5, 7.7.10
                                            -- with applicable GSM mappings as defined in
                                            -- EN 300 370, 6.1.8.2.13 or 6.1.7.1.3

ServiceClass        ::= OCTET STRING        -- as encoded in EN 300 175-5, 7.7.39

BasicService        ::= OCTET STRING        -- as encoded in EN 300 175-5, 7.6.4

Rand                ::= OCTET STRING        -- as either encoded in EN 300 175-5, 7.7.32
                                            -- with applicable GSM mappings as
                                            -- defined in EN 300 370, 6.1.8.1.9 or 6.1.7.1.2.

Res                 ::= OCTET STRING        -- as encoded in EN 300 175-5, 7.7.35 with
                                            -- applicable GSM mapping as defined in
                                            -- EN 300 370, 6.1.7.25 and 6.1.8.2.14

Rs              ::= OCTET STRING            -- as encoded in EN 300 175-5, 7.7.36

RejectReason        ::= OCTET STRING        -- as encoded in EN 300 175-5, 7.7.34

Signal              ::= OCTET STRING        -- as encoded in EN 300 175-5, 7.6.8

mMOID OBJECT IDENTIFIER ::=
                        {ccitt identified-organization etsi(0) 1144 operations-and-errors(1)}

cTMAccessRightsRequest          CTMAccessRightsRequest          ::= globalValue {mMOID 1}
cTMAccessRightsTerminate        CTMAccessRightsTerminate        ::= globalValue {mMOID 2}
cTMLocationRegistration         CTMLocationRegistration         ::= globalValue {mMOID 3}
cTMLocationCancellation         CTMLocationCancellation         ::= globalValue {mMOID 4}
cTMLocationRegistrationSuggest  CTMLocationRegistrationSuggest  ::= globalValue {mMOID 5}
cTMTerminalAuthentication       CTMTerminalAuthentication       ::= globalValue {mMOID 6}
cTMNetworkAuthentication        CTMNetworkAuthentication        ::= globalValue {mMOID 7}
cTMCiphering                    CTMCiphering                    ::= globalValue {mMOID 8}
cTMCipheringSuggest             CTMCipheringSuggest             ::= globalValue {mMOID 9}
cTMKeyAllocate                  CTMKeyAllocate                  ::= globalvalue {mMOID 10}
cTMIdentityRequest              CTMIdentityRequest              ::= globalValue {mMOID 11}
cTMOutgoingCallMMInfo           CTMOutgoingCallMMInfo           ::= globalValue {mMOID 12}
cTMIncomingCallMMInfo           CTMIncomingCallMMInfo           ::= globalValue {mMOID 13}

gSMLocationRegistration         GSMLocationRegistration         ::= globalValue {mMOID 20}
gSMLocationCancellation         GSMLocationCancellation         ::= globalValue {mMOID 21}
gSMDetach                       GSMDetach                       ::= globalValue {mMOID 22}
gSMTerminalAuthentication       GSMTerminalAuthentication       ::= globalValue {mMOID 23}
gSMTerminalAuthenticationReject GSMTerminalAuthenticationReject ::= globalValue {mMOID 24}
gSMCiphering                    GSMCiphering                    ::= globalValue {mMOID 25}
gSMAssignIdentity               GSMAssignIdentity               ::= globalValue {mMOID 26}
gSMLinkedAssignIdentity         GSMLinkedAssignIdentity         ::= globalValue {mMOID 27}
gSMIdentityRequest              GSMIdentityRequest              ::= globalValue {mMOID 28}
gSMOutgoingCallMMInfo           GSMOutgoingCallMMInfo           ::= globalValue {mMOID 29}
gSMIncomingCallMMInfo           GSMIncomingCallMMInfo           ::= globalValue {mMOID 30}

networkRejected                                                 ::= globalValue {mMOID 40}
terminalRejected                                                ::= globalValue {mMOID 41}
portableIdentityUnknown                                         ::= globalValue {mMOID 42}
identityNotAvailable                                            ::= globalValue {mMOID 43}
congestion                                                      ::= globalValue {mMOID 44}
localTimerExpiry                                                ::= globalValue {mMOID 45}
pagingFailure                                                   ::= globalValue {mMOID 46}
radioConnectionFailure                                          ::= globalValue {mMOID 47}
incompatibleCipheringState                                      ::= globalValue {mMOID 48}
priorityRuleViolation                                           ::= globalValue {mMOID 49}
unspecified                                                     ::= globalValue {mMOID 50}

NetworkRejected             ::= ERROR PARAMETER RejectReason        -- RejectReason is optional
```

```
TerminalRejected            ::= ERROR PARAMETER RejectReason        -- RejectReason is optional

PortableIdentityUnknown     ::= ERROR
IdentityNotAvailable        ::= ERROR
Congestion                  ::= ERROR
LocalTimerExpiry            ::= ERROR
PagingFailure               ::= ERROR
RadioConnectionFailure      ::= ERROR
IncompatibleCipheringState  ::= ERROR
PriorityRuleViolation       ::= ERROR
Unspecified                 ::= ERROR

-- End of MobilityManagement-Operations-and-Errors
```

8 State definitions

Table 4 defines the states for the mobility management service at the user and network side of the alpha interface.

Table 4: States for the alpha interface

User side (FP) states	
Idle:	Process is not running.
Wait_CTM_Subscription_Registration:	The user is waiting for response from the network on CTM access rights request.
Wait_CTM_Subscription_Deregistration:	The user is waiting for response from the application on CTM access rights terminate.
Wait_CTM_Location_Registration:	The user is waiting for response from the network on CTM location registration request.
Wait_GSM_Location_Registration:	The user is waiting for response from the network on GSM location registration request or a GSM linked assign identity request.
Wait_GSM_Location_Registration_2:	The user is waiting for response from the network on GSM location registration request.
Wait_GSM_Linked_Assign_Identity_Request:	The user is waiting for GSM linked assign identity request from the network.
Wait_GSM_Linked_Assign_Identity:	The user is waiting for response from the application on GSM linked assign identity request.
Wait_CTM_Location_Cancellation:	The user is waiting for response from the application on CTM location cancellation request.
Wait_CTM_Location_Registration_Suggest_Response:	The user is waiting for response from the application on CTM location registration suggest request.
Wait_CTM_Terminal_Authentication:	The user is waiting for response from the application on the CTM terminal authentication request.
Wait_GSM_Terminal_Authentication:	The user is waiting for response from the application on the GSM terminal authentication request.
Wait_GSM_Terminal_Authentication_Reject:	The user is waiting for a GSM terminal authentication reject from the network
Wait_CTM_Network_Authentication:	The user is waiting for response from the network on the CTM network authentication request.
Wait_CTM_Ciphering_Response:	The user is waiting for response from the application on the CTM ciphering request.
Wait_GSM_Ciphering:	The user is waiting for response from the application on the GSM ciphering request.
Wait_CTM_Ciphering:	The user is waiting for a response from the network on the CTM ciphering suggest.
Wait_GSM_Identity_Assign:	The user is waiting for a response from the application on the GSM identity request.

Wait_CTM_Key_Allocate:	The user is waiting for a response from the application on the CTM key allocate request.
Wait_CTM_Identity_Response:	The user is waiting for a response from the application on the CTM identity request.
Wait_GSM_Identity_Response:	The user is waiting for a response from the application on the GSM identity request.

Network states

Idle:	Process is not running.
Wait_CTM_Subscription_Registration:	The network is waiting for response from the application on CTM access rights request.
Wait_CTM_Subscription_Deregistration:	The network is waiting for response from the user on CTM access rights terminate.
Wait_CTM_Location_Registration:	The network is waiting for response from the application on CTM location registration request.
Wait_GSM_Location_Registration:	The network is waiting for response from the application on GSM location registration request.
Wait_GSM_Linked_Assign_Identity:	The network is waiting for response from the user on GSM linked assign identity request.
Wait_CTM_Location_Cancellation:	The network is waiting for response from the user on CTM location cancellation request.
Wait_CTM_Location_Registration_Suggest_Response:	The network is waiting for response from the user on CTM location registration suggest request.
Wait_CTM_Terminal_Authentication:	The network is waiting for response from the user on the CTM terminal authentication request.
Wait_GSM_Terminal_Authentication:	The network is waiting for response from the user on the GSM terminal authentication request.
Wait_GSM_Terminal_Authentication_Reject:	The network is waiting for a GSM terminal authentication reject from the application
Wait_CTM_Network_Authentication:	The network is waiting for response from the application on the CTM network authentication request.
Wait_CTM_Ciphering_Response:	The network is waiting for response from the user on the CTM ciphering request.
Wait_GSM_Ciphering:	The network is waiting for response from the user on the GSM ciphering request.
Wait_CTM_Ciphering:	The network is waiting for a response from the application on the CTM ciphering suggest.
Wait_GSM_Identity_Assign:	The network is waiting for a response from the user on the GSM identity request.
Wait_CTM_Key_Allocate:	The network is waiting for a CTM network authentication request from the user.

Wait_CTM_Key_Allocate_2:	The network is waiting for a response from the user on the CTM key allocate request.
Wait_CTM_Identity_Response:	The network is waiting for a response from the user on the CTM identity request.
Wait_GSM_Identity_Response:	The network is waiting for a response from the user on the GSM identity request.
Timer_Running:	The network has started T-MM and is waiting for a response from the user or expiry of timer T-MM.

9 Signalling procedures at the coincident S and T reference point

When the PortableIdentity is provided as a parameter in any of the operations specified in this clause and the IPUI type is used as described in table 3, any of the IPUI types specified in EN 300 175-6 [5], subclause 6.2 may be transported across the alpha interface.

If specific constraints apply to the type of IPUI that is to be transported in the PortableIdentity parameter for a specific operation, then the constraint is to be explicitly identified in the parameter description of that operation.

When reception of a component (invoke, return result) is described in a "Normal operation" subclause, it is assumed that it is correctly encoded and has been delivered as specified in annex B.

The signalling entity at the user side checks only the syntactical correctness of the received operations and parameters before passing them on the air interface. Semantical checks are not performed at this level.

All information sent from the user to the network are generated by mapping from information received from the air interface. Exceptions to this rule are directly identified in the following text.

9.1 Subscription registration and subscription deregistration

If the service provider option "support of the subscription registration procedure" has the value "yes", the network shall support the procedures for on-air subscription registration. described in this subclause.

If the service provider option "support of the subscription deregistration procedure" has the value "yes", the network shall support the procedures for on-air subscription deregistration. described in this subclause.

Before the CTM user gets access to the service, the CT may perform a subscription registration procedure according to the procedure of subclause 9.1.1 by means of an on-air procedure. This procedure may be used by the CT to gain access to the network in order to make calls or to receive calls.

Access rights for a CT may be terminated by the network by following a subscription deregistration procedure according to subclause 9.1.2.

If a subscription registration or deregistration is performed then this shall be valid throughout the area of service provision, i.e. a roaming CTM subscriber shall not be required to perform a new subscription registration while roaming among networks.

9.1.1 Subscription registration

9.1.1.1 Normal operation

The subscription registration procedure is initiated by the CT to obtain access rights from the network.

To perform an on-air subscription registration request procedure, the user shall send a CTMAccessRightsRequest invoke component to the network. The following parameters shall be included:

- cTMPortableIdentity, indicating the identity of the CT (IPUI);
- cTMAuthType, indicating the authentication algorithm (DSSA), the authentication key type (AC or UAK) and the authentication key number, related to the IPUI/PARK pair; and
- cTMPortableCapabilities to convey the CT capabilities (tone capability, display capability, profile indicator and control codes).

On receipt of the CTMAccessRightsRequest invoke component by the network, depending on the received authentication key type field (which is contained in the cTMAuthenticationType parameter), two options exist:

1) If the received authentication key type field indicates Authentication Code (AC), the network may initiate a key allocation procedure as described in subclause 9.3.7. (This procedure embeds a mutual network and terminal authentication procedure).
2) Independent of the received authentication key type field, the network may as an option, initiate the terminal authentication procedure as described in subclause 9.3.2 and/or start ciphering as described in subclause 9.3.4.

   When the procedures has successfully been performed, the network shall send a CTMAccessRightsRequest return result component to the user, by using the procedure described in annex B. The following parameters shall be included:

- cTMPortableIdentity, indicating the newly assigned identity (IPUI) of the CT, which requested the subscription registration; and
- cTMFixedIdentity, indicating the type (PARK), the AccessRightClass (ARC), AccessRightDetails (ARD) and the length of the identity (PLI), related to the indicated IPUI.

  As an option, the following parameter may be included:

- cTMServiceClass, indicating the service class of the CT related to the provided IPUI.

  When the user receives an CTMAccessRightsRequest return result component, then the user shall accept the provided information.

9.1.1.2 Exceptional procedure

If the network is unable to perform the subscription registration, the network shall send a CTMAccessRightsRequest return error component to the user, using the procedure described in annex B. One of the following error values shall be included:

- networkRejected, if the network rejects the requested procedure and wants to include a RejectReason to be sent on the air interface. In this case the RejectReason parameter may be included indicating the reject reason to be transported via the air interface;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known to the network;
- congestion, if the network is overloaded and cannot process the request; or
- unspecified, if the requested procedure fails for any other reason.

  If the user receives a reject component that it can associate with the previously sent invoke component, the user shall consider the procedure as unsuccessful.

  If the network receives a reject component from the user, the network shall take no action.

9.1.2 Subscription deregistration

The subscription deregistration procedure is initiated by the network to terminate access rights for a CT. This procedure enables the network to remove a specific IPUI and all information related to it from a CT.

9.1.2.1 Normal operation

To perform the subscription deregistration procedure, the network shall send a CTMAccessRightsTerminate invoke component to the user, using the procedures described in annex B, and start timer T-MM. The following parameters shall be included:

- cTMPortableIdentity , indicating the identity of the CT (IPUI); and
- cTMFixedIdentity, indicating the PARK.

On receipt of the CTMAccessRightsTerminate invoke component, the user may start a Network Authentication procedure as described in subclause 9.3.3.

The user shall use the received parameters to perform the requested access rights termination (delete PARK and/or IPUI).

If the user has successfully performed the access rights termination, the user shall send a CTMAccessRightsTerminate return result component to the network, using the procedure described in annex B, without any parameter.

If the network receives a CTMAccessRightsTerminate return result component, the network shall consider the subscription deregistration procedure as completed and shall stop timer T-MM, if running.

9.1.2.2 Exceptional procedure

If the user is unable to perform the subscription deregistration, the user shall send a CTMAccessRightsTerminate return error component to the network, indicating one of the following error values:

- terminalRejected, if the rejectReason has been received from the air interface. In this case the RejectReason parameter may be included indicating the reject reason that has been received via the air interface;
- pagingFailure, if the paging on the air interface fails for any reason;
- radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
- congestion, if the fixed part is overloaded and cannot process the request;
- localTimerExpiry, if the supervision timer for the requested procedure expires before a response has been received;
- priorityRuleViolation, if a mobility management procedure of equal priority has been requested, while the ongoing procedure has not yet been finished; or
- unspecified, if the requested procedure fails for any other reason.

On receiving the CTMAccessRightsTerminate return error component or a reject component (if the network can associate the reject component with the invoke component) from the user, the network shall stop timer T-MM.

If the user receives a reject component that it can associate with the previously sent return result or return error component, the user shall take no action.

If timer T-MM expires the network shall consider the subscription deregistration procedure as unsuccessful.

9.2 Activation and deactivation

The mobility management service provided by the network to the subscriber shall be activated when the subscriber makes its location known to the network by the location registration procedure for the first time or after a period of deactivation.

9.2.1 Location registration

The location registration procedure is used to make the CT's location known to the network.

a) If the user and network support the "DECT access to GSM" mode, three cases can be distinguished:

- normal updating (when a CT roams from one location area to another);
- periodic updating (when a CT has been required to indicate its location after a predefined period even if it is not roaming);
- IMSI attach (when a CT is switched on in the same location area).

b) If the user and network support the "CTM" mode, only the normal location update procedure applies.

9.2.1.1 Normal operation

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

In order to make the CT's location known to the network, the user shall send a GSMLocationRegistration invoke component to the network by using the procedure described in annex B. The following parameters shall be included:

- gSMPortableIdentity, indicating the identity of the CT, which is the TMSI if available in the CT, otherwise the IMSI;
- gSMLocationRegistrationType, indicating whether the location registration type is "normal updating", "periodic updating" or "IMSI attach";
- gSMLocationAreaIdentity, identifying the old location area of the CT;
- gSMCipherInfo, indicating the cipher key sequence number; and
- gSMPortableCapabilities, indicating the Mobile Station Classmark 1 information element;

On receiving the GSMLocationRegistration invoke component, the network shall use the received parameters to perform the location registration procedure.

Before sending the GSMLocationRegistration return result component to the user, the network may initiate one or more of the following procedures:

- identity request procedure to request for an identity, as described in subclause 9.3.8;
- terminal authentication procedure to authenticate the terminal, as described in subclause 9.3.2;
- network initiated ciphering procedure to initiate ciphering, as described in subclause 9.3.4; or
- temporary identity assignment procedure to assign a temporary identity to the CT, as described in subclause 9.3.6.

The network, having successfully performed the location registration shall send a GSMLocation Registration return result component to the user, by using the procedure described in annex B. The following parameter shall be included:

- gSMLocationAreaIdentity, indicating the new location area.

Upon receipt of the GSMLocationRegistration return result component, the user shall accept the provided information, linked with the information contained in GSMLinkedAssignIdentity invoke component, if previously sent by the network according to annex B. The user shall then respond with a GSMLinkedAssignIdentity return result component as described in subclause 9.3.6.1.2.

NOTE: The network may then initiate the location cancellation procedure towards the previous location, according to the procedure defined in subclause 9.2.2.

b) If the user and network support the "CTM" mode, the following procedure shall apply:

In order to make the CT location known to the network, the user shall send a CTMLocationRegistration invoke component to the network by using the procedure described in annex B. The following parameters shall be included:

- cTMPortableIdentity, indicating the identity of the CT which is the IPUI;
- cTMOldLocationAreaIdentity, indicating the old location area;
- cTMNewLocationAreaIdentity, indicating the new location area, as generated by the FP; and
- cTMPortableCapabilities, indicating the characteristics of the CT;

On receiving the CTMLocationRegistration invoke component, the network shall use the received parameters to perform the location registration procedure.

Before sending the CTMLocationRegistration return result component to the user, the network may initiate one or more of the following procedures:

- terminal authentication procedure to authenticate the terminal, as described in subclause 9.3.2; or
- key allocation procedure to allocate an authentication key to the user, as described in subclause 9.3.7.

The network, having successfully performed the location registration shall send a CTMLocation Registration return result component to the user, by using the procedure described in annex B, without any parameters.

The network shall then initiate the location cancellation procedure towards the previous location, according to the procedures defined in subclause 9.2.2.

9.2.1.2 Exceptional procedure

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

If the network is unable to perform a location registration procedure, the network shall send a GSMLocationRegistration return error component to the user, by using the procedure described in annex B, indicating one of the following error values:

- networkRejected, if the network rejects the requested procedure and wants to include a RejectReason to be sent on the air interface. In this case the RejectReason parameter may be included indicating the reject reason to be transported via the air interface;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known to the network;
- congestion, if the network is overloaded and cannot process the request; or
- unspecified, if the requested procedure fails for any other reason.

If the network receives a reject component from the user, the network shall take no action.

If the user receives either:

- a GSMLocationRegistration return error component; or
- a reject component that it can associate with the GSMLocationRegistration invoke component;

the user shall consider the location registration procedure as unsuccessful and not respond to a possible previously received GSMLinkedAssignIdentity invoke component (as described in subclause 9.3.6.2.2.

b) If the user and network support the "CTM" mode, the following procedure shall apply:

If the network is unable to perform a location registration procedure, the network shall send a CTMLocationRegistration return error component to the user, by using the procedure described in annex B, indicating one of the following error values:

- networkRejected, if the network rejects the requested procedure and wants to include a RejectReason to be sent on the air interface. In this case the RejectReason parameter may be included indicating the reject reason to be transported via the air interface;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known to the network;
- congestion, if the network is overloaded and cannot process the request; or
- unspecified, if the requested procedure fails for any other reason.

If the network receives a reject component from the user, the network shall take no action.

If the user receives either:

- a CTMLocationRegistration return error component; or
- a reject component that it can associate with the CTMLocationRegistration invoke component;

the user shall consider the location registration procedure as unsuccessful.

9.2.2 Location cancellation

9.2.2.1 Normal operation

The location cancellation procedure shall be initiated by the network towards the user to delete all data related to a CT e.g. because the terminal has moved to another location area. Location cancellation is only an administrative action in the FP, no message will be sent to the CT.

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

   To initiate a location cancellation the network shall send the GSMLocationCancellation invoke component to the user, by using the procedure described in annex B. The following parameter shall be included:

   - gSMPortableIdentity, indicating the identity of the CT which is the IMSI or TMSI.

   When the user receives a correctly encoded GSMLocationCancellation invoke component, the user shall accept the provided information and not respond to the network.

b) If the user and network support the "CTM" mode, the following procedure shall apply:

   To initiate a location cancellation the network tshall send the CTMLocationCancellation invoke component to the user, by using the procedure described in annex B, and shall start timer T-MM. The following parameter shall be included:

   - cTMPortableIdentity, indicating the identity of the CT (IPUI).

When the user receives a correctly encoded CTMLocationCancellation invoke component, the user shall accept the provided information and shall respond to the network by sending a CTMLocationCancellation return result component without parameters.

On receiving the CTMLocationCancellation return result component from the user, the network shall stop timer T-MM, if running.

9.2.2.2 Exceptional procedure

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply: If the user is unable to act on the GSMLocationCancellation Invoke component, the user shall take no action.

   If the network receives a reject component, the network shall take no action.

b) If the user and network support the "CTM" mode, the following procedure shall apply:

If the user is unable to act on the CTMLocationCancellation invoke component, the user shall send a CTMLocationCancellation return error component to the network, using the procedures as described in annex B. One of the following error values shall be included:

- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
- congestion, if the fixed part is overloaded and cannot process the request; or
- unspecified, if the requested procedure fails for any other reason.

On receiving the CTMLocationCancellation return error component or a reject component (if the network can associate the reject component with the invoke component) from the user, the network shall stop timer T-MM.

If the user receives a reject component that it can associate with the previously sent return result or return error component, the user shall take no action.

If timer T-MM expires the network shall consider the location cancellation procedure as unsuccessful.

9.2.3 Detach

If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

9.2.3.1 Normal operation

If the CT is unable to receive incoming calls (e.g. the terminal is switched off), the user shall send a GSMDetach invoke component to the network, using the procedure described in annex B. The following parameter shall be included:

- gSMPortableIdentity, indicating the identity of the CT which is the TMSI if available, otherwise the IMSI.

Upon receiving a correctly encoded GSMDetach invoke component, the network shall accept the received information and shall consider the terminal as not reachable. The network shall not respond to the user.

9.2.3.2 Exceptional procedure

If the network is unable to act on the GSMDetach invoke component, the network shall take no action.

If the user receives a reject component that it can associate with the previously sent invoke component, the user shall consider the procedure as unsuccessful.

9.3 Invocation and operation

9.3.1 Location registration suggest

If the user and network support "CTM" mode, the following procedure shall apply:

NOTE: When the location of a CT is no longer known in the network or the network did not receive any activities from a CT for a certain time, the network may request the CT to perform a location registration procedure as described in subclause 9.2.1. When the CT still does not react, the network may take appropriate actions (e.g. performing a location cancellation procedure in the latest known fixed part).

The network may initiate a location registration suggest procedure at any time.

9.3.1.1 Normal operation

The network shall initiate a location registration suggest procedure by sending a CTMLocationRegistrationSuggest invoke component to the user, using the procedure described in annex B. The following parameter shall be included:

- cTMPortableIdentity, indicating the identity of the CT (IPUI).

When the user receives a correctly encoded CTMLocationRegistrationSuggest invoke component, the user shall accept the provided information and not respond to the network.

As a result, the user may afterwards initiate a location registration procedure as described in subclause 9.2.1.

9.3.1.2 Exceptional procedure

If the user is unable to act on the CTMLocationRegistrationSuggest invoke component, the user may send a CTMLocationRegistrationSuggest return error component to the network, indicating one of the following error values:

- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
- pagingFailure, if the paging on the air interface fails for any reason;
- radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason;
- congestion, if the fixed part is overloaded and cannot process the request;
- priorityRuleViolation, if a mobility management procedure with of equal priority has been requested, while the ongoing procedure has not yet been finished; or
- unspecified, if the requested procedure fails for any other reason.

  If the network receives a reject component or a CTMLocationRegistrationSuggest return error component from the user, the network shall take no action.

  If the user receives a reject component that it can associate with the previously sent return error component, the user shall take no action.

9.3.2 Terminal authentication

At any time the CT is registered in the network, terminal authentication may be invoked by the network. Invoking the terminal authentication, the network verifies that the identity provided by the CT is the one claimed.

The network may initiate a terminal authentication procedure at any time.

9.3.2.1 Normal operation

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

   To initiate a terminal authentication procedure, the network shall send a GSMTerminalAuthentication invoke component to the user, using the procedures described in annex B and shall start timer T-MM. The following parameters shall be included:

   - gSMRand, indicating the RAND number, which is used for calculation of the terminal authentication result; and
   - gSMCipherInfo, indicating the cipher key sequence number.

     If the terminal authentication procedure is not embedded in another procedure, the following parameter shall also be included:

   - gSMPortableIdentity, indicating the identity of the CT (IMSI).

   On receiving the correctly encoded GSMTerminalAuthentication invoke component, delivered as specified in annex B, to perform the authentication process, the user shall use the received parameters. If the result is calculated, the user shall send a GSMTerminalAuthentication return result component to the network by using the procedure described in annex B. The following parameter shall be included:

   - gSMRes, indicating the calculated result of the authentication, containing the SRES parameter.

   On receiving the GSMTerminalAuthentication return result component, the network shall stop timer T-MM, if running and shall check the validity of the authentication result. If the result is correct the network shall consider the terminal authentication procedure as successful.

b) If the user and network support the "CTM" mode, the following procedure shall apply:

To initiate a terminal authentication procedure, the network shall send a CTMTerminalAuthentication invoke component to the user, using the procedures described in annex B, and shall start timer T-MM. The following parameters shall be included:

- cTMAuthType, indicating the authentication key type (AC or UAK), the authentication algorithm, and the authentication key number related to the IPUI to use for calculation of the authentication result; if the derived cipher key shall be stored by the CT, the related cipher key number is also indicated;

- cTMRand, indicating the random number RAND, which is used for calculation of the terminal authentication result;

- cTMRs, indicating the RS number, which is used for calculation of the authentication result.

If the terminal authentication procedure is not embedded in another procedure, the following parameter shall also be included:

- cTMPortableIdentity, indicating the identity of the CT (IPUI).

On receiving the correctly encoded CTMTerminalAuthentication invoke component, to perform the authentication process, the user shall use the received parameters. If the result is calculated, the user shall send a CTMTerminalAuthentication return result component to the network by using the procedure described in annex B. The following parameter shall be included:

- cTMRes, indicating the calculated result of the authentication, containing the RES1 parameter.

As an option the following parameter may also be included:

- cTMServiceClass, indicating the service class of the CT related to the current active IPUI.

On receiving the CTMTerminalAuthentication return result component, delivered as described in annex B, the network shall stop timer T-MM, if running and shall check the validity of the authentication result. If the result is correct the network shall consider the terminal authentication procedure as successful.

9.3.2.2 Exceptional procedure

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

   If the user is unable to perform the requested authentication procedure, the user shall send a GSMTerminalAuthentication return error component to the network. One of the following error values shall be included:

   - terminalRejected, if the rejectReason has been received from the air interface. In this case the RejectReason parameter may be included indicating the reject reason received via the air interface;

   - portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;

   - congestion, if the fixed part is overloaded and cannot process the request;

   - localTimerExpiry, if the supervision timer for the requested procedure expires before a response has been received;

   - pagingFailure, if the paging on the air interface fails for any reason;

   - radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason;

   - priorityRuleViolation, if a mobility management procedure of equal priority has been requested, while the ongoing procedure has not yet been finished; or

   - unspecified, if the requested procedure fails for any other reason.

If the network receives a TerminalAuthentication return result component with an incorrect parameter value, the network shall stop timer T-MM, consider the terminal authentication procedure as unsuccessful and may send a GSMTerminalAuthenticationReject invoke component if the service provider option "use of the GSMTerminalAuthenticationReject procedure" is set to "yes".

On receiving the GSMTerminalAuthenticationReject invoke component from the network, the user shall consider the terminal authentication as unsuccessful. The user shall not respond to the GSMTerminalAuthenticationReject invoke component.

On receiving the GSMTerminalAuthentication return error component or a reject component (if the network can associate the reject component with the invoke component) from the user, the network shall stop timer T-MM and consider the terminal authentication as unsuccessful.

If the user receives a reject component that it can associate with the previously sent return result or return error component, the user shall take no action.

If timer T-MM expires the network shall consider the terminal authentication procedure as unsuccessful.

When the terminal authentication is considered as unsuccessful, the network may take appropriate action on the ongoing transactions, as specified in ETS 300 557 [11].

b) If user and network support the "CTM" mode, the following procedure shall apply:

   If the user is unable to perform the requested authentication procedure, the user shall send a CTMTerminalAuthentication return error component to the network. One of the following error values shall be included:

   - terminalRejected, if the rejectReason has been received from the air interface. In this case the RejectReason parameter may be included indicating the reject reason received via the air interface;
   - portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
   - congestion, if the fixed part is overloaded and cannot process the request;
   - localTimerExpiry, if the supervision timer for the requested procedure expires before a response has been received;
   - pagingFailure, if the paging on the air interface fails for any reason;
   - radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason;
   - priorityRuleViolation, if a mobility management procedure of equal priority has been requested, while the ongoing procedure has not yet been finished; or
   - unspecified, if the requested procedure fails for any other reason.

   Upon receipt of:

   - A CTMTerminalAuthentication return result component with a parameter not acceptable to the network (e.g. incorrect cTMRes);
   - A CTMTerminalAuthentication return error component; or
   - A reject component (if the network can associate the reject component with the CTMTerminalAuthentication invoke component);

   the network shall stop Timer T-MM and consider the terminal authentication procedure as being unsuccessful.

If the user receives a reject component that it can associate with the previously sent return result or return error component, the user shall take no action.

If timer T-MM expires, the network shall consider the terminal authentication procedure as being unsuccessful.

9.3.3 Network authentication

If the user and network support the "CTM" mode, the following procedure shall apply:

The CT may invoke the network authentication procedure at any time, to verify that the identity provided by the network is the one claimed.

9.3.3.1 Normal operation

To request the network authentication procedure, the user shall send a CTMNetworkAuthentication invoke component to the network, using the procedure described in annex B. The following parameters shall be included:

- cTMAuthenticationType, indicating the authentication key type, the authentication algorithm, and the authentication key number to use for calculation of the network authentication result; and
- cTMRand, indicating the random number RAND, to be used for calculation of the network authentication result.

If the network authentication procedure is not embedded in another procedure, the following parameter shall also be included:

- cTMPortableIdentity, indicating the identity of the CT (IPUI).

On receiving the CTMNetworkAuthentication invoke component, to perform the network authentication, the network shall use the received parameters. The network, having successfully performed the network authentication procedure shall send a CTMNetworkAuthentication return result component to the user, using the procedure described in annex B. The following parameter shall be included:

- cTMRes, indicating the calculated result RES2.

If the cTMRs parameter has not already been sent to the user as part of the Key allocation procedure (as specified in subclause 9.3.7.1), the following parameter shall also be included:

- cTMRs, indicating the random session number the network has used to calculate the RES2 value.

On receiving the CTMNetworkAuthentication return result component, delivered as described in annex B, the user shall use the cTMRand and cTMRs parameters to check the validity of the cTMRes parameter. If the result is correct the user shall consider the network authentication procedure as successful.

9.3.3.2 Exceptional procedure

If the network is unable to perform a network authentication, the network shall send a CTMNetworkAuthentication return error component to the user, by using the procedure as described in annex B, indicating one of the following error value:

- networkRejected, if the network rejects the requested procedure and wants to include a RejectReason to be sent on the air interface. In this case the RejectReason parameter may be included indicating the reject reason to be transported via the air interface;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known to the network;
- congestion, if the network is overloaded and cannot process the request; or
- unspecified, if the requested procedure fails for any other reason.

On receiving a CTMNetworkAuthentication return result component with an incorrect cTMRes parameter from the network, the user shall consider the network authentication as unsuccessful.

On receiving the CTMNetworkAuthentication return error component from the network as response to the CTMNetworkAuthentication invoke component, the user shall consider the network authentication as unsuccessful.

If the network receives a reject component from the user, the network shall take no action.

If the user receives a reject component that it can associate with the previously sent invoke component, the user shall consider the procedure as unsuccessful.

9.3.4 Encryption - network initiated ciphering

The network initiates the encryption activation to engage ciphering and to define the cipher parameters.

The network may initiate a ciphering procedure at any time.

9.3.4.1 Normal operation

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

The network initiates a network initiated ciphering procedure (encryption activation) by sending a GSMCiphering invoke component to the user, using the procedure described in annex B and shall start timer T-MM. The following parameter shall be included:

- gSMCipherKey, indicating the cipher key value (Kc) to be used by the FP.

If the ciphering procedure is a not embedded procedure, the following parameter shall also be included:

- gSMPortableIdentity, indicating the IMSI or TMSI.

On receiving the correctly encoded GSMCiphering invoke component, the user shall use the cipher key sequence number received in the previous terminal authentication procedure. The user shall enable ciphering and shall respond to the network, by sending a GSMCiphering return result component, without any parameter.

On receiving the GSMCiphering return result component from the user, the network shall accept it as a confirmation of the encryption of the air interface and shall stop timer T-MM, if running.

b) If the user and network supports the "CTM" mode, the following procedure shall apply:

The network initiates a network initiated ciphering procedure (encryption activation) by sending a CTMCiphering invoke component to the user, using the procedure described in annex B and shall start timer T-MM. The following parameters shall be included:

- cTMCipherInfo, indicating the cipher key type, cipher key number and the cipher algorithm, related to the IPUI; and

- cTMCipherKey, indicating the numeric value of the ciphering key to be used by the FP.

If the ciphering procedure is a not embedded procedure, the following parameter shall also be included:

- cTMPortableIdentity, indicating the IPUI.

On receiving the correctly encoded CTMCiphering invoke component, delivered as specified in annex B, the user shall check whether it supports the indicated cipher key type, cipher key number and cipher algorithm. If the user accepts the cipher request, the user shall enable ciphering and shall respond to the network, by sending a CTMCiphering return result component, without any parameter.

On receiving the CTMCiphering return result component, delivered as specified in annex B, the network shall accept it as a confirmation of the encryption of the air interface and shall stop timer T-MM, if running.

9.3.4.2 Exceptional procedure

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

If the user is unable to perform the Ciphering request, the user shall send a GSMCiphering return error component to the network, using the procedure as described in annex B. One of the following error values shall be included:

- terminalRejected, if the rejectReason has been received from the air interface. In this case the RejectReason parameter may be included indicating the reject reason received via the air interface;

- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;

- congestion, if the fixed part is overloaded and cannot process the request;

- localTimerExpiry, if the supervision timer for the requested procedure expires before a response has been received;

- pagingFailure, if the paging on the air-interface fails for any reason;

- radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason;

- incompatibleCipheringState, returned if ciphering is requested for an already ciphered connection;
- priorityRuleViolation, if a mobility management procedure of equal priority has been requested, while the ongoing procedure has not yet been finished; or
- unspecified, if the requested procedure fails for any other reason.

On receiving the GSMCiphering return error component or a reject component (if the network can associate the reject component with the invoke component) from the user, the network shall stop timer T-MM and consider the ciphering procedure as unsuccessful.

If the user receives a reject component that it can associate with the previously sent return result or return error component, the user shall take no action.

If timer T-MM expires the network shall consider the ciphering procedure as unsuccessful.

b) If the user and network support the "CTM" mode, the following procedure shall apply:

   If the user is unable to perform the Ciphering request, the user shall send a CTMCiphering return error component to the network, using the procedure as described in annex B. One of the following error values shall be included:

   - terminalRejected, if the rejectReason has been received from the air interface. In this case the RejectReason parameter may be included indicating the reject reason received via the air interface;
   - portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
   - congestion, if the fixed part is overloaded and cannot process the request;
   - localTimerExpiry, if the supervision timer for the requested procedure expires before a response has been received;
   - pagingFailure, if the paging on the air-interface fails for any reason;
   - radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason;
   - incompatibleCipheringState, returned if ciphering is requested for an already ciphered connection;
   - priorityRuleViolation, if a mobility management procedure of equal priority has been requested, while the ongoing procedure has not yet been finished; or
   - unspecified, if the requested procedure fails for any other reason.

On receiving the CTMCiphering return error component or a reject component (if the network can associate the reject component with the invoke component) from the user, the network shall stop timer T-MM and consider the ciphering procedure as unsuccessful.

If the user receives a reject component that it can associate with the previously sent return result or return error component, the user shall take no action.

If timer T-MM expires the network shall consider the ciphering procedure as unsuccessful.

9.3.5 Encryption - portable initiated ciphering

If the user and network support the "CTM" mode, the following procedure shall apply:

The user may initiate the encryption suggest procedure at any time, to request the network to enable ciphering and to define the cipher parameters.

9.3.5.1 Normal operation

The user initiates a portable initiated ciphering procedure (encryption activation) by sending a CTMCipheringSuggest invoke component to the network, using the procedure described in annex B. The following parameter shall be included:

- cTMCipherInfo, to enable ciphering and to indicate the cipher key type, the cipher key number and the cipher algorithm, related to the IPUI.

If the ciphering suggest procedure is a stand-alone procedure, the following parameter shall also be included:

- cTMPortableIdentity, indicating the IPUI.

On receiving a correct encoded CTMCipheringSuggest invoke component, the network shall use the received parameter. The network shall initiate the network initiated ciphering procedure as specified in subclause 9.3.4.

9.3.5.2 Exceptional procedure

If the network is unable to perform the portable initiated ciphering request, the network shall send a CTMCipheringSuggest return error component to the user, using the procedure as described in annex B. One of the following error values shall be included:

- networkRejected, if the network rejects the requested procedure and wants to include a RejectReason to be sent on the air interface. In this case the Rejectreason parameter may be included indicating the reject reason to be transported via the air interface;

- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known to the network;

- congestion, if the network is overloaded and cannot process the request; or

- unspecified, if the requested procedure fails for any other reason.

As an option, upon receiving a CTMCipheringSuggest return error component, the user may either release the transaction to be ciphered or proceed in the existing mode.

If the network receives a reject component from the user, the network shall take no action.

If the user receives a reject component that it can associate with the previously sent invoke component, the user shall consider the procedure as unsuccessful.

9.3.6 Temporary identity assignment

If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

The network may assign a TMSI at any time by using the temporary identity assignment procedure.

9.3.6.1 Normal operation

9.3.6.1.1 Temporary identity assignment

The network shall initiate an assign identity procedure by sending a GSMAssignIdentity invoke component to the user, using the procedure described in annex B and shall start timer T-MM. The following parameters shall be included:

- gSMNewTMSI, including a new TMSI which has to be assigned to the CT, or the special TMSI value as - specified in table 6 of EN 300 370 [8] indicating that the TMSI, already assigned in the CT shall be deleted; and

- gSMLocationAreaIdentity, indicating the location area for which the newly to be assigned temporary identity is valid.

If the Temporary identity assignment procedure is a stand-alone procedure, the following parameter shall also be included:

- gSMPortableIdentity parameter, including the identity of the CT (IMSI).

On receiving the correctly encoded GSMAssignIdentity invoke component, the user shall use the received parameters. The user having successfully performed the allocation of a new temporary identity or the deletion of the current temporary identity, shall send a GSMAssignIdentity return result component to the network without any parameters, using the procedures described in annex B. On receiving the GSMAssignIdentity return result component, the network shall stop timer T-MM, if running and shall consider the new temporary identity (TMSI) as valid, or if the special TMSI value as specified in table 6 of EN 300 370 [8] was used, considers the old temporary identity (TMSI) as deleted.

9.3.6.1.2 Linked temporary identity assignment

When the network wants to assign a new temporary identity to the CT as a response to the location registration request, the network may use the linked temporary identity assignment procedure. Use of this procedure instead of the temporary identity assignment procedure (see subclause 9.3.6.1.1) allows the network:

- not to send twice the gSMLocationAreaIdentity parameter; and
- to receive an acknowledgement of the location registration procedure.

The network shall initiate a linked assign identity procedure by sending a GSMLinkedAssignIdentity invoke component to the user, using the procedure described in annex B and shall start timer T-MM. The following parameter shall be included:

- gSMNewTMSI including a new TMSI which has to be assigned to the CT, or the special TMSI value as specified in table 6 of EN 300 370 [8] indicating that the TMSI already assigned in the CT shall be deleted.

On receiving the correctly encoded GSMLinkedAssignIdentity invoke component, the user shall keep the received parameter until reception of the GSMLocationRegistration return result component (see subclause 9.2.1.1). The user having successfully performed the allocation of a (new) temporary identity or the deletion of the current temporary identity, shall send a GSMLinkedAssignIdentity return result component to the network without any parameters, using the procedures described in annex B.

On receiving the GSMLinkedAssignIdentity return result component, the network shall stop timer T-MM if running, and shall consider the new temporary identity (TMSI) as valid, or if the special TMSI value as specified in table 6 of EN 300 370 [8] was used, consider the old temporary identity (TMSI) as deleted.

9.3.6.2 Exceptional procedure

9.3.6.2.1 Temporary identity assignment

On receiving a reject component (if the network can associate the reject component with the invoke component) from the user, the network shall stop timer T-MM and consider the procedure as unsuccessful.

If the user is unable to perform the assign identity procedure, the user shall take no action.

If the user receives a reject component that it can associate with the previously sent return result component, the user shall take no action.

If timer T-MM expires the network shall consider the procedure as unsuccessful and take action as specified in subclause 4.4.4.6 of ETS 300 557 [11].

9.3.6.2.2 Linked temporary identity assignment

On receiving a reject component (if the network can associate the reject component with the invoke component) from the user, the network shall stop timer T-MM and consider the procedure as unsuccessful.

If the user is unable to perform the assign identity procedure, the user shall take no action.

If the user receives a reject component that it can associate with the previously sent return result component, the user shall take no action.

If timer T-MM expires the network shall consider the procedure as unsuccessful and take action as specified in subclause 4.4.4.6 of ETS 300 557 [11].

If the linked GSMRegistration procedure fails (see subclause 9.2.1), the user shall delete the parameter received in the GSMLinkedAssignIdentity invoke component and not respond to the network.

9.3.7 Key allocation

The key allocation procedure is initiated by the network to replace the Authentication Code (AC) by a more secure User Authentication Key (UAK).

The key allocation procedure may be embedded within a subscription registration procedure.

If the user and network support the "CTM" mode, the following procedure shall apply:

9.3.7.1 Normal operation

To initiate a key allocation procedure, the network shall send a CTMKeyAllocate invoke component to the user, using the procedure described in annex B and shall start timer T-MM. The following parameters shall be included:

- cTMAllocType, indicating the authentication algorithm, the number of the used Authentication Code (AC) and the number to be given to the allocated User Authentication Key (UAK);
- cTMRand, indicating the random number RAND, which is used for calculation of the terminal authentication result; and
- cTMRs, indicating the Rs number used to calculate the terminal authentication session key which shall be used, together with the provided cTMRand value, for calculation of the terminal authentication result.

If the key allocation procedure is a stand-alone procedure, the following parameter shall also be included:

- cTMPortableIdentity, indicating the identity of the CT (IPUI).

On receiving the correctly encoded CTMKeyAllocate invoke component, the user shall use the received parameters to calculate the terminal authentication result RES1 and initiate a network authentication procedure as described in subclause 9.3.3.1. The user shall afterwards send a CTMKeyAllocate return result component to the network, using the procedure described in annex B. The following parameter shall be included:

- cTMRes, indicating the RES1 number to provide the terminal authentication result calculated by the CT.

On receiving the CTMNetworkAuthentication invoke component, the network shall delay the request until reception of the response to the key allocation procedure.

On receiving the CTMKeyAllocate return result component from the user, the network shall stop timer T-MMand perform the network authentication as described in subclause 9.3.3.1. The network shall use the random session number previously indicated to the user in the cTMRs parameter of the CTMKeyAllocate invoke component.

On receiving the CTMNetworkAuthentication return result component with the correct result, the user shall replace the AC value by the UAK.

The network will consider the UAK successfully allocated only after a successful subsequent terminal authentication using this UAK.

9.3.7.2 Exceptional procedure

If the user is unable to perform the key-allocate procedure, the user shall send a CTMKeyAllocate return error component to the network, using the procedure as described in annex B. One of the following error values shall be included:

- terminalRejected, if a RejectReason has been received on the air interface. In this case the RejectReason parameter may be included indicating the reject reason received via the air interface;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
- congestion, if the fixed part is overloaded and cannot process the request;

- localTimerExpiry, if the supervision timer for the requested procedure expires before a response has been received;
- pagingFailure, if the paging on the air interface fails for any reason;
- radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason;
- priorityRuleViolation, if a mobility management procedure of equal priority has been requested, while the ongoing procedure has not yet been finished; or
- unspecified, if the requested procedure fails for any other reason.

If the user returns a CTMKeyAllocate return error component or a reject component in response to the CTMKeyAllocate invoke component, no network authentication procedure shall be initiated.

The network shall consider the key allocation procedure as unsuccessful on:

- reception of a CTMKeyAllocate return error component;
- reception of a reject component (if the network can associate the reject component with the invoke component);
- reception of a CTMKeyAllocate return result component with an incorrect result (the authentication of the user fails);
- reception of a CTMKeyAllocate return result component without previous reception of a network authentication request; or
- timer T-MM expiry.

The network shall then:

- stop timer T-MM if needed; and
- respond with a CTMNetworkAuthentication return error, including the error value "networkRejected", to a previously received network authentication request.

If either the key allocation procedure or the network authentication procedure are not successful, the AC value shall not be replaced by the UAK.

If the user receives a reject component that it can associate with the previously sent return result or return error component, the user shall take no action.

9.3.8 Identity request

The identification request procedure is initiated by the network to request the user to provide specific identification parameters of a CT to the network.

The identity request procedure may be initiated by the network at any time.

9.3.8.1 Normal operation

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

The network shall initiate an identity request procedure by sending a GSMIdentityRequest invoke component to the user, using the procedure described in annex B and shall start timer T-MM. The following parameter shall be included:

- gSMIdentityType, indicating a specific identity, which is requested by the network (IMSI, TMSI, IMEI or IMEISV).

If the procedure is not embedded in another procedure, the following parameter shall also be included:

- gSMPortableIdentity, including the identification of the user from which the additional identity is requested (IMSI).

On receipt of the GSMIdentityRequest invoke component the user shall perform the requested identification and shall send a GSMIdentityRequest return result component to the network, by using the procedure described in annex B. The following parameter shall be included:

- gSMPortableIdentity, indicating the requested identity, depending on which type has been requested in the gSMIdentityType.

On receiving the GSMIdentityRequest return result component from the user, the network shall stop timer T-MM, if running.

b) If the user and network support the "CTM" mode, the following procedure shall apply:

The network shall initiate an identity request procedure by sending a CTMIdentityRequest invoke component to the user, by using the procedure described in annex B and shall start timer T-MM. The following parameter shall be included:

- cTMIdentityType, indicating a specific identity, which is requested by the network (IPUI or IPEI).

If the procedure is not embedded in another procedure, the following parameter shall also be included:

- cTMPortableIdentity, including the identification of the user from which the additional identity is requested (IPUI).

On receipt of the CTMIdentityRequest invoke component the user shall perform the requested identification and send a CTMIdentityRequest return result component to the network, by using the procedure described in annex B. The following parameter shall be included:

- cTMPortableIdentity, indicating the requested identity, depending on which type has been requested in the cTMIdentityType.

On receiving the CTMIdentityRequest return result component from the user, the network shall stop timer T-MM, if running.

9.3.8.2 Exceptional procedure

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

If the user is not able to perform the identity procedure, the user shall send a GSMIdentityRequest return error component to the network, by using the procedure described in annex B. One of the following error values shall be included:

- identityNotAvailable, if the requested identity is not available;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
- congestion, if the fixed part is overloaded and cannot process the request;
- localTimerExpiry, if the supervision timer for the requested procedure expires before a response has been received;
- priorityRuleViolation, if a mobility management procedure of equal priority has been requested, while the ongoing procedure has not yet been finished;
- pagingFailure, if the paging on the air interface fails for any reason;
- radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason; or
- unspecified, if the requested procedure fails for any other reason.

On receiving the GSMIdentityRequest return error component or a reject component (if the network can associate the reject component with the invoke component) from the user, the network shall stop timer T-MM and consider the procedure as unsuccessful.

If the user receives a reject component that it can associate with the previously sent return result or return error component, the user shall take no action.

If timer T-MM expires the network shall consider the procedure as unsuccessful.

b) If the user and network support the "CTM" mode, the following procedure shall apply:

If the user is not able to perform the identity procedure, the user shall send a CTMIdentityRequest return error component to the network, by using the procedure described in B. One of the following error values shall be included:

- identityNotAvailable, if the requested identity is not available;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
- congestion, if the fixed part is overloaded and cannot process the request;
- localTimerExpiry, if the supervision timer for the requested procedure expires before a response has been received;
- priorityRuleViolation, if a mobility management procedure of equal priority has been requested, while the ongoing procedure has not yet been finished;
- pagingFailure, if the paging on the air interface fails for any reason;
- radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason; or
- unspecified, if the requested procedure fails for any other reason.

On receiving the CTMIdentityRequest return error component or a reject component (if the network can associate the reject component with the invoke component) from the user, the network shall stop timer T-MM and consider the procedure as unsuccessful.

If the user receives a reject component that it can associate with the previously sent return result or return error component, the user shall take no action.

If timer T-MM expires the network shall consider the procedure as unsuccessful.

9.3.9 Outgoing call

9.3.9.1 Normal operation

Call establishment at the originating interface proceeds as described in subclause 5.1 of EN 300 403-1 [9] with the following precisions and modifications:

If the network receives a request for an outgoing call and afterwards the network wants to cipher the called party number on the air-interface, the network shall initiate a network initiated ciphering procedure as soon as possible. The previously Derived Cipher Key (DCK) may be used, without terminal authentication before. If the network wants to use a new derived cipher key (DCK), the terminal authentication procedure shall be completed before the network initiates the ciphering procedure.

NOTE: Called party number digits transmitted before the ciphering procedure has been completed are not ciphered.

The Calling party number information element containing the address of the FP (which is an E.164 number) may be included in the SETUP message as described in subclause 3.1.14 of EN 300 403-1 [9].

The user shall include a GSMOutgoingCallMMInfo invoke component or CTMOutgoingCallMMInfo invoke component, respectively in a Facility information element, as described in EN 300 196-1 [7], in the SETUP message.

a) If the user and network support the "DECT access to GSM" mode, the GSMOutgoingCallMMInfo invoke component shall contain the following parameters:

- gSMPortableIdentity, indicating the identity of the CT, which is the TMSI if available, otherwise the IMSI; and
- gSMBasicService, indicating a normal call-setup.

The network, accepting the provided information in the SETUP message shall proceed the call request according to the procedure as described in subclause 5.1 of EN 300 403-1 [9].

b) If the user and network support the "CTM" mode, the CTMOutgoingCallMMInfo invoke component shall contain the following parameters:

- cTMPortableIdentity, indicating the identity of the CT, which is the IPUI;
- cTMBasicService, indicating a normal call-setup; and
- cTMFixedIdentity, indicating the PARK of the CT.

The network, accepting the provided information in the SETUP message shall proceed the call request according to the procedure as described in subclause 5.1 of EN 300 403-1 [9].

9.3.9.2 Exceptional procedure

a) If the user and network support the "DECT access to GSM" mode, the following procedure shall apply:

If the network determines that:

- the received GSMOutgoingCallMMInfo invoke component is incorrect; or
- the terminal authentication procedure fails (as described in subclause 9.3.2.2) and, according to ETS 300 557 [11], the call has to be released;

the network shall send a GSMOutgoingCallMMInfo return error component in a facility information element to the user. The network shall release the call according to the procedures described in subclause 5.3 of EN 300 403-1 [9] with cause #31, "normal unspecified".

An emergency call shall not be released due to the failure of the terminal authentication procedure. The network shall assure that the called party number received (or to be received) cannot be an emergency number before releasing the call due to the failure of the terminal authentication procedure.

One of the following error values shall be included in the GSMOutgoingCallMMInfo return error component:

- networkRejected, if the network rejects the requested procedure and wants to include a RejectReason to be sent on the air interface. In this case the RejectReason parameter may be included indicating the reject reason to be transported via the air interface;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known to the network;
- congestion, if the network is overloaded and cannot process the request; or
- unspecified, if the requested procedure fails for any reason.

If the network receives a reject component that it can associate with the previously sent return error component, the network shall take no action.

If the user receives a reject component that it can associate with the previously sent invoke component, the user shall take no action.

b) If the user and network support the "CTM" mode, the following procedure shall apply:

If the network determines that:

- the received CTMOutgoingCallMMInfo invoke component is incorrect;
- the terminal authentication procedure fails and the service provider option 'The call is released in case of an unsuccessful terminal authentication' is set to 'Yes'; or
- the network initiated ciphering procedure fails and the service provider option 'The call is released in case of an unsuccessful ciphering procedure' is set to 'Yes';

the network shall send a CTMOutgoingCallMMInfo return error component in a Facility information element to the user. The network shall release the call according to the procedures described in subclause 5.3 of EN 300 403-1 [9] with cause #31, "normal unspecified".

An emergency call shall not be released due to the failure of the terminal authentication procedure. The network shall assure that the called party number received (or to be received) cannot be an emergency number before releasing the call due to the failure of the terminal authentication procedure.

One of the following error values shall be included in the CTMOutgoingCallMMInfo return error component:

- networkRejected, if the network rejects the requested procedure and wants to include a RejectReason to be sent on the air interface. In this case the RejectReason parameter may be included indicating the reject reason to be transported via the air interface;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known to the network;
- congestion, if the network is overloaded and cannot process the request; or
- unspecified, if the requested procedure fails for any reason.

If the network receives a reject component that it can associate with the previously sent return error component, the network shall take no action.

If the user receives a reject component that it can associate with the previously sent invoke component, the user shall take no action.

9.3.10 Incoming call

9.3.10.1 Normal operation

Call establishment at the terminating interface proceeds as described in subclause 5.2 of EN 300 403-1 [9] with the following precisions and modifications.

If the network wants to use a new derived cipher key (DCK), the terminal authentication procedure shall be completed before the network initiates the ciphering procedure.

The network shall include a GSMIncomingCallMMInfo invoke component or CTMIncomingCallMMInfo invoke component, respectively in a Facility information element, as described in EN 300 196-1 [7], in the SETUP message.

a) If the user and network support the "DECT access to GSM" mode, the GSMIncomingCallMMInfo invoke component shall contain the following parameters:

   - gSMPortableIdentity, indicating the identity of the CT, which is the TMSI if available, otherwise the IMSI; and
   - gSMSignal, indicating the signal to be generated by theCT.

   The user, accepting the provided information in the SETUP message shall proceed the call request according to the procedure as described in subclause 5.2 of EN 300 403-1 [9].

b) If the user and network support the "CTM " mode, the CTMIncomingCallMMInfo invoke component shall contain following parameters:

   - cTMPortableIdentity, indicating the identity of the CT, which is the IPUI; and
   - cTMSignal, indicating the signal to be generated by the CT.

   The user, accepting the provided information in the SETUP message shall proceed the call request according to the procedure as described in subclause 5.2 of EN 300 403-1 [9].

9.3.10.2 Exceptional procedures

a) If the network and user support the "DECT access to GSM" mode, the following procedure shall apply:

If the user has received the GSMIncomingCallMMInfo invoke component in the SETUP message and does not accept it for any reason, the user shall send a GSMIncomingCallMMInfo return error component to the network within a Facility information element. One of the following error values shall be included:

- terminalRejected, if the rejectReason has been received from the air interface. In this case the RejectReason parameter may be included indicating the reject reason received via the air interface;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
- congestion, if the fixed part is overloaded and cannot process the request;
- pagingFailure, if the paging on the air interface fails for any reason;
- radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason; or
- unspecified, if the requested procedure fails for any other reason.

If the user receives a reject component that it can associate with the previously sent return error component, the user shall take no action.

If the network:

- determines that the terminal authentication procedure fails; and according to ETS 300 557 [11] the call has to be released; or
- receives a GSMIncomingCallMMInfo return error component;

the network shall release the call according to the procedures described in subclause 5.3 of EN 300 403-1 [9] with cause #31, "normal unspecified"..

If the network receives a reject component from the user that it can associate with the GSMIncomingCallMMInfo invoke component, the network shall take appropriate actions.

b) If the network and user support the "CTM" mode, the following procedure shall apply:

If the user has received the CTMIncomingCallMMInfo invoke component in the SETUP message and does not accept it for any reason, the user shall send a CTMIncomingCallMMInfo return error component to the network within a Facility information element. One of the following error values shall be included:

- terminalRejected, if the rejectReason has been received from the air interface. In this case the RejectReason parameter may be included indicating the reject reason received via the air interface;
- portableIdentityUnknown, if the identity of the CT, for which the request has been initiated, is not known;
- congestion, if the fixed part is overloaded and cannot process the request;
- pagingFailure, if the paging on the air interface fails for any reason;
- radioConnectionFailure, if the signalling connection on the air interface is interrupted for any reason; or
- unspecified, if the requested procedure fails for any other reason.

If the user receives a reject component that it can associate with the previously sent return error component, the user shall take no action.

If the network:

- determines that the terminal authentication procedure fails and as a service provider option the call has to be released;
- determines that the network initiated ciphering procedure fails and as a service provider option the call has to be released;

- receives a CTMIncomingCallMMInfo return error component; or
- receives a reject component from the user that it can associate with the CTMIncomingCallMMInfo invoke component;

the network shall release the call according the procedures described in subclause 5.3 of EN 300 403-1 [9] with cause #31, "normal unspecified".

10 Procedures for interworking with private ISDNs

An NT2 functional entity without CTM mobility management functions shall be connected to the ISDN or PLMN using the T reference point via the alpha interface. The mobility management procedures are described in clause 9 of the present document.

The transport mechanism applicable on the T reference point to convey the mobility management information is described in annex B.

An NT2 functional entity with mobility management functions shall be connected to the ISDN or PLMN via the beta interface. The beta interface is described in another standard.

11 Interactions with other networks

Not applicable.

12 Interactions with other supplementary services

Outside the scope of the present document.

13 Parameter values (timers)

MobilityManagement application timer T-MM:

This timer is started by the network after sending a mobility management related invoke component (e.g. terminal authentication) to the user.

The default value of this timer is 15 seconds.

14 Dynamic description (SDL diagrams)

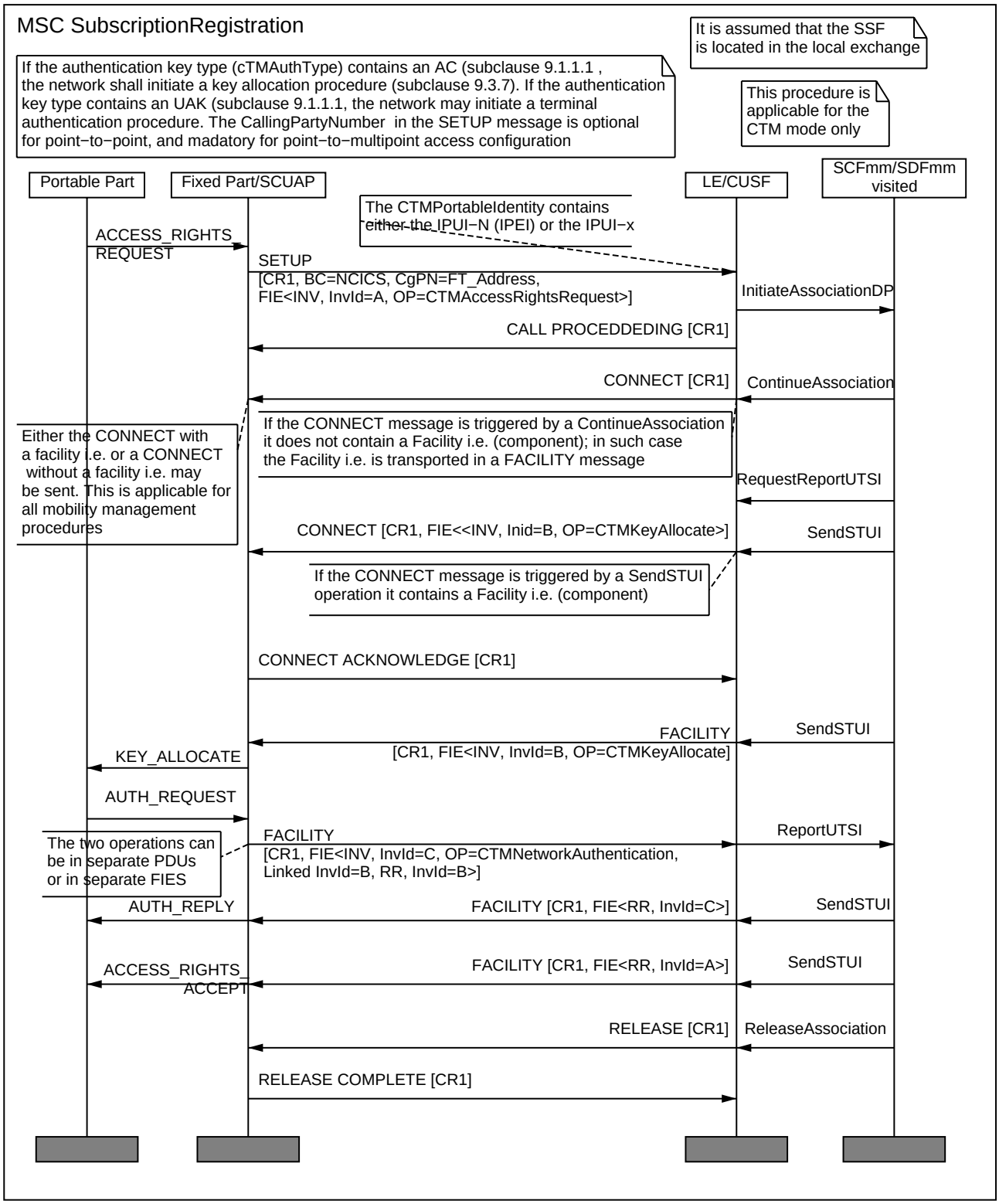
NOTE: In several states other mobility management procedures may be initiated. The SDL processes show single procedures and not all possible embedded procedures.

Annex A (informative): Signalling flows for mobility management

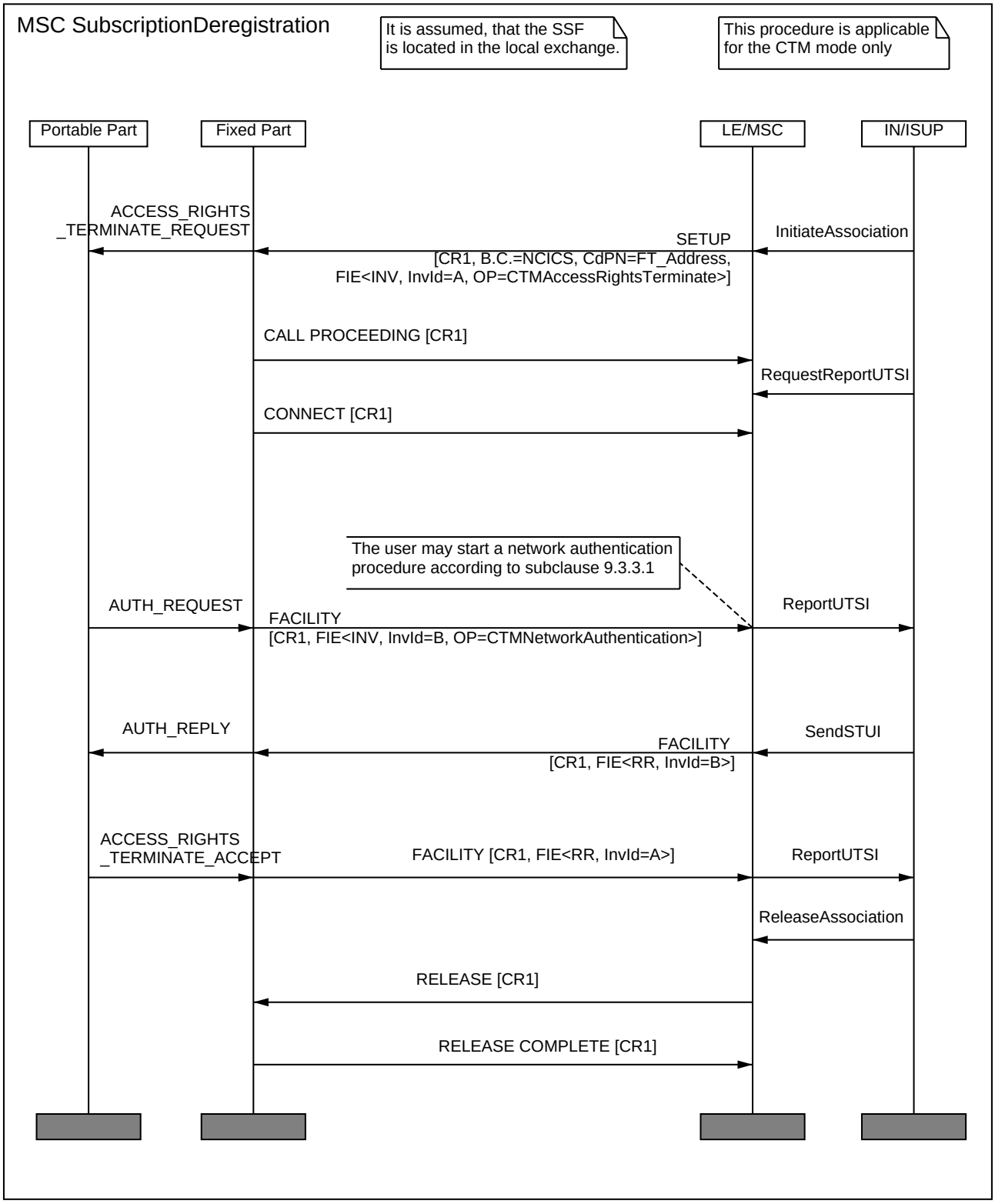
This annex contains the signalling flows for the mobility management procedures at the alpha interface.

A.1 Registration and deregistration

A.1.1 Subscription registration

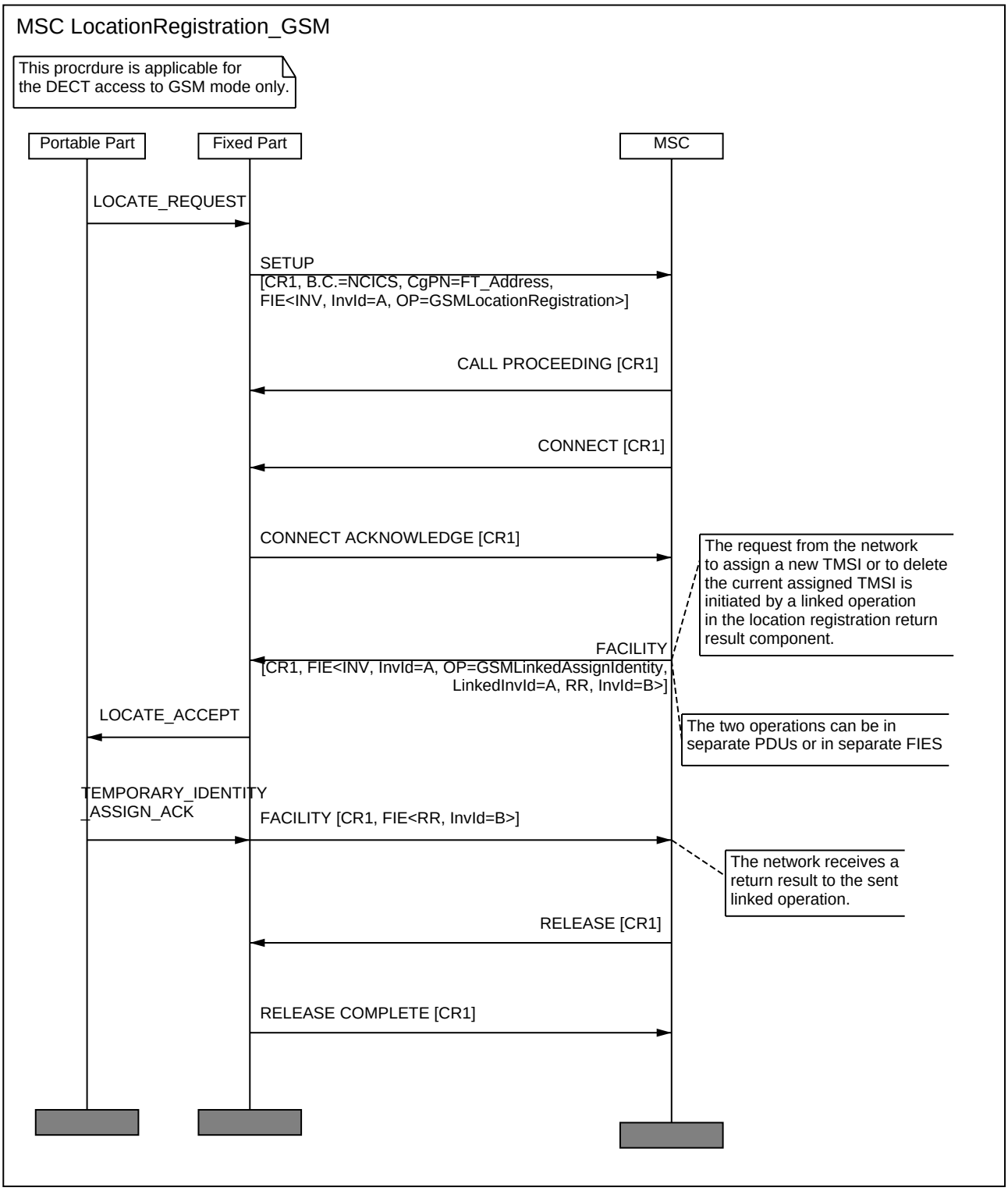


A.1.2 Subscription deregistration

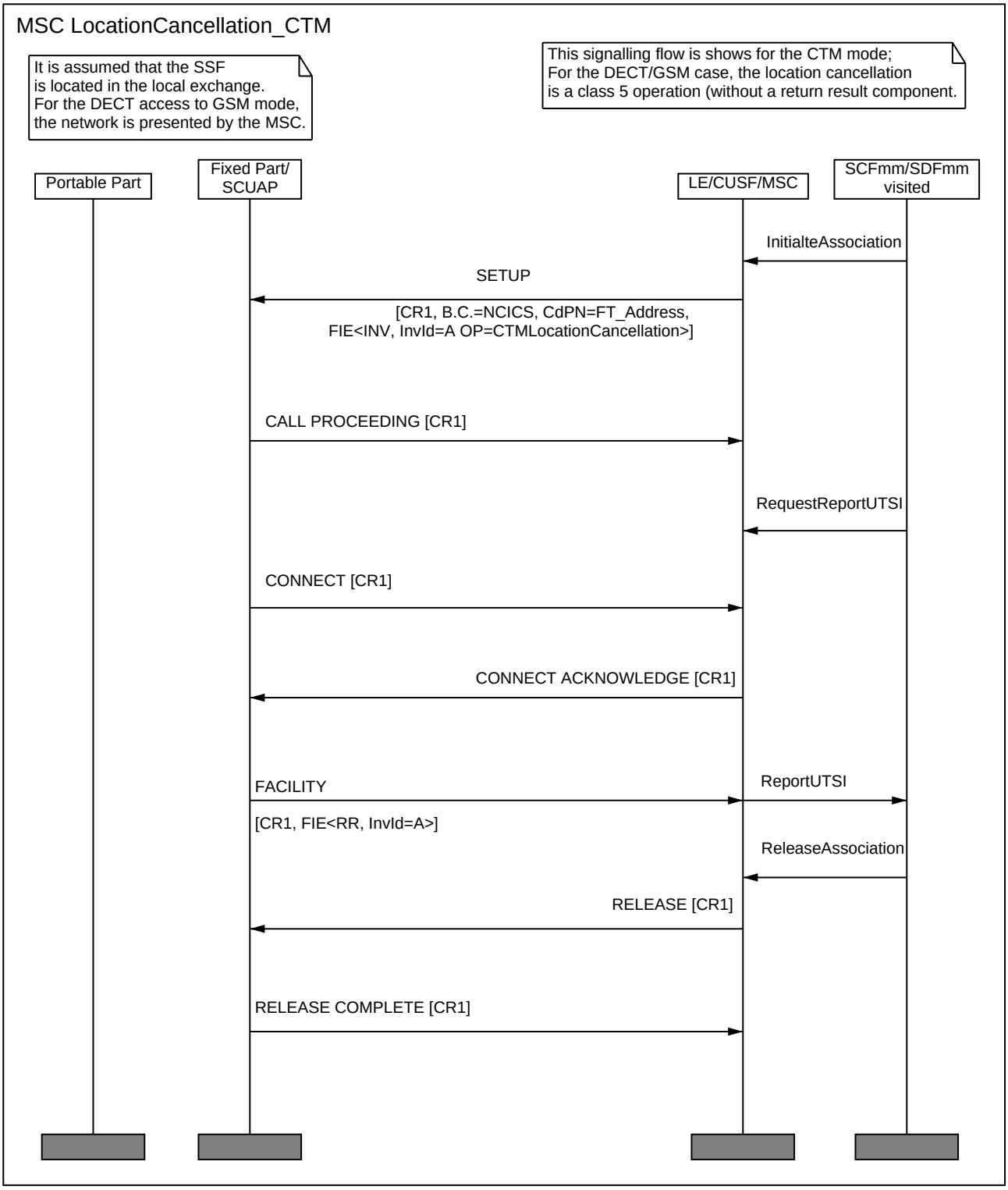


A.2 Activation and deactivation

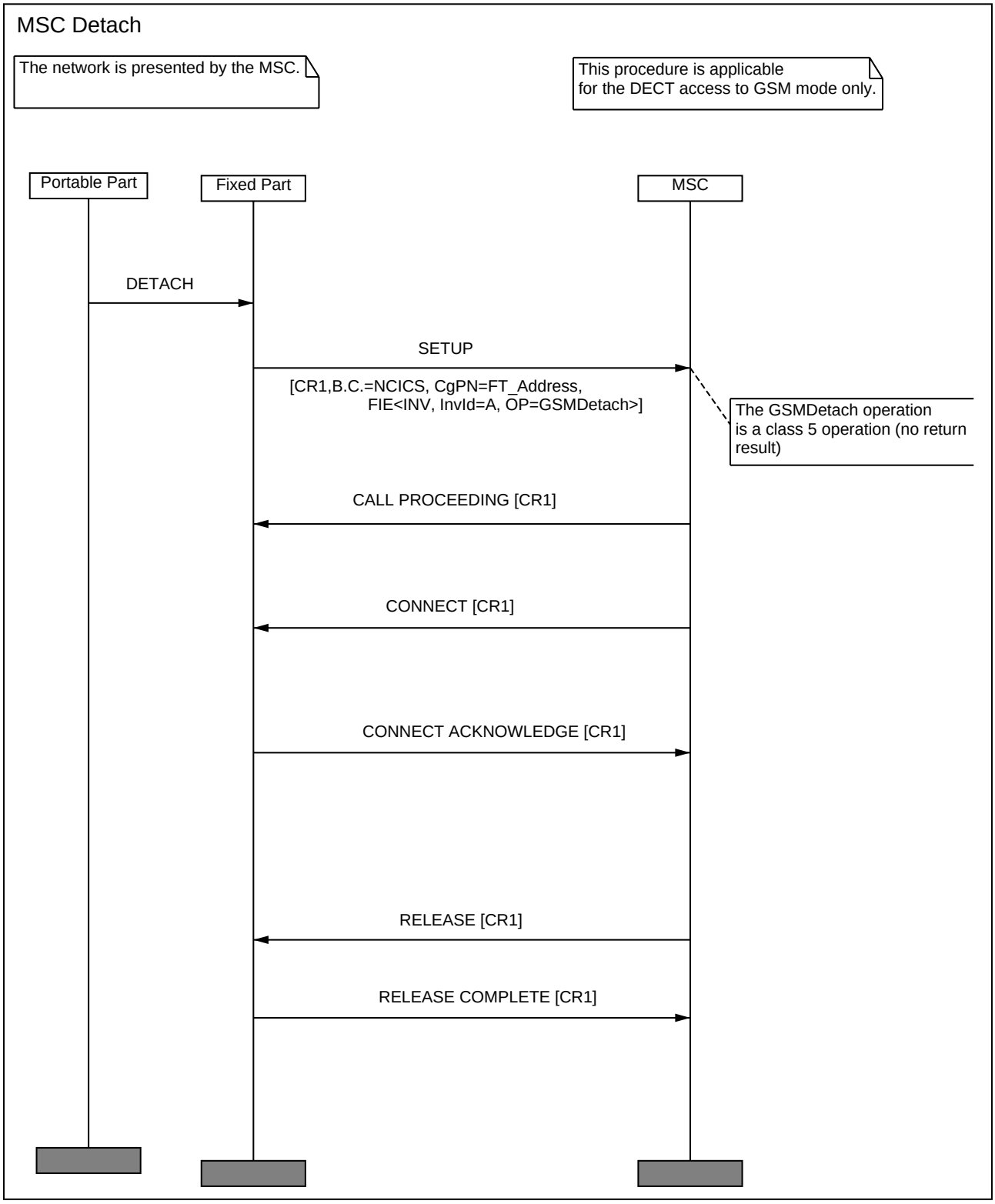
A.2.1 Location registration - GSM



A.2.2 Location cancellation - CTM



A.2.3 Detach


MSC Detach
The network is presented by the MSC.
This procedure is applicable for the DECT access to GSM mode only.
Portable Part
Fixed Part
MSC
DETACH
SETUP
[CR1,B.C.=NCICS, CgPN=FT_Address, FIE<INV, InvId=A, OP=GSMDetach>]
The GSMDetach operation is a class 5 operation (no return result)
CALL PROCEEDING [CR1]
CONNECT [CR1]
CONNECT ACKNOWLEDGE [CR1]
RELEASE [CR1]
RELEASE COMPLETE [CR1]

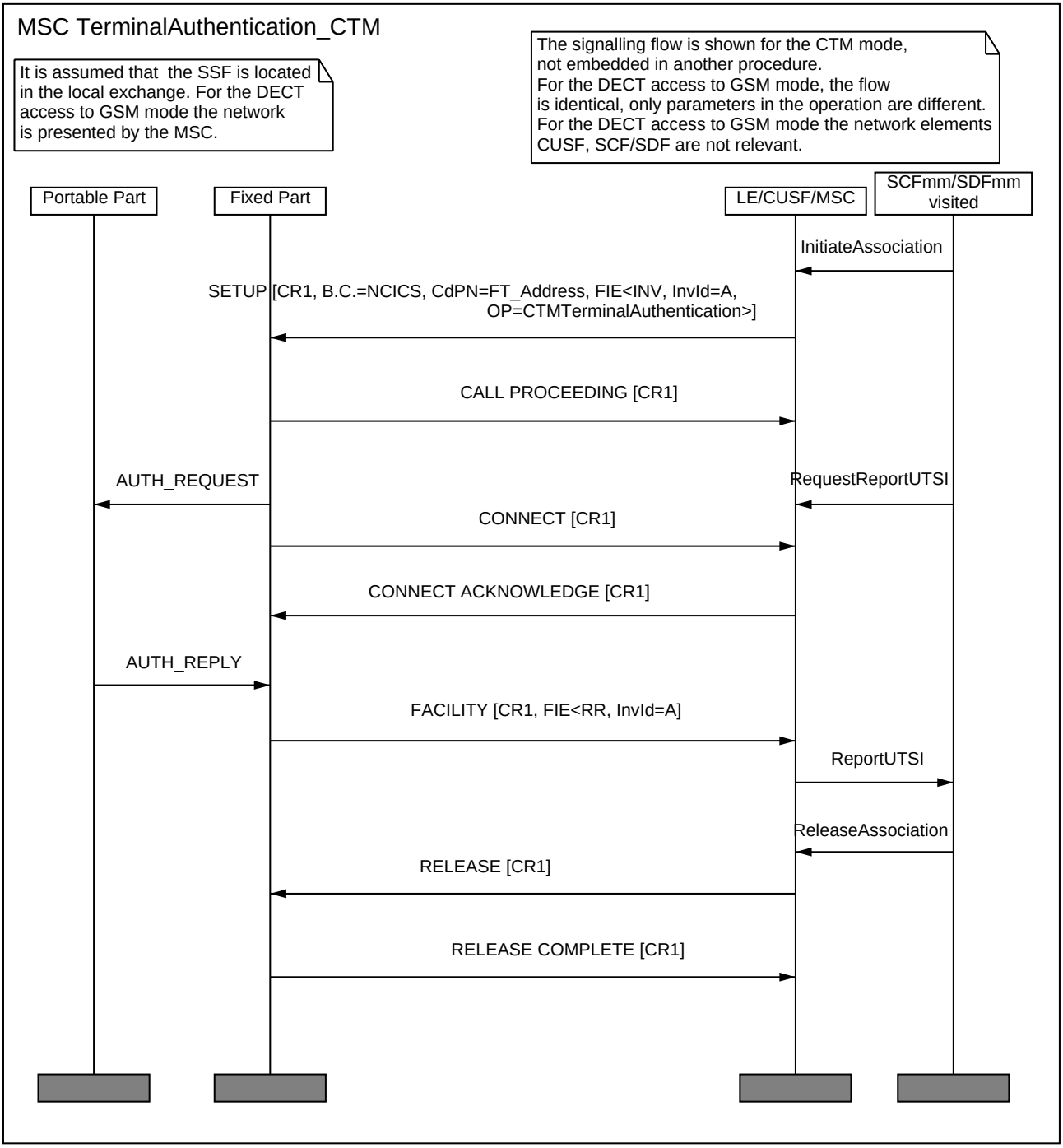
A.3 Invocation and operation

A.3.1 Location registration suggest

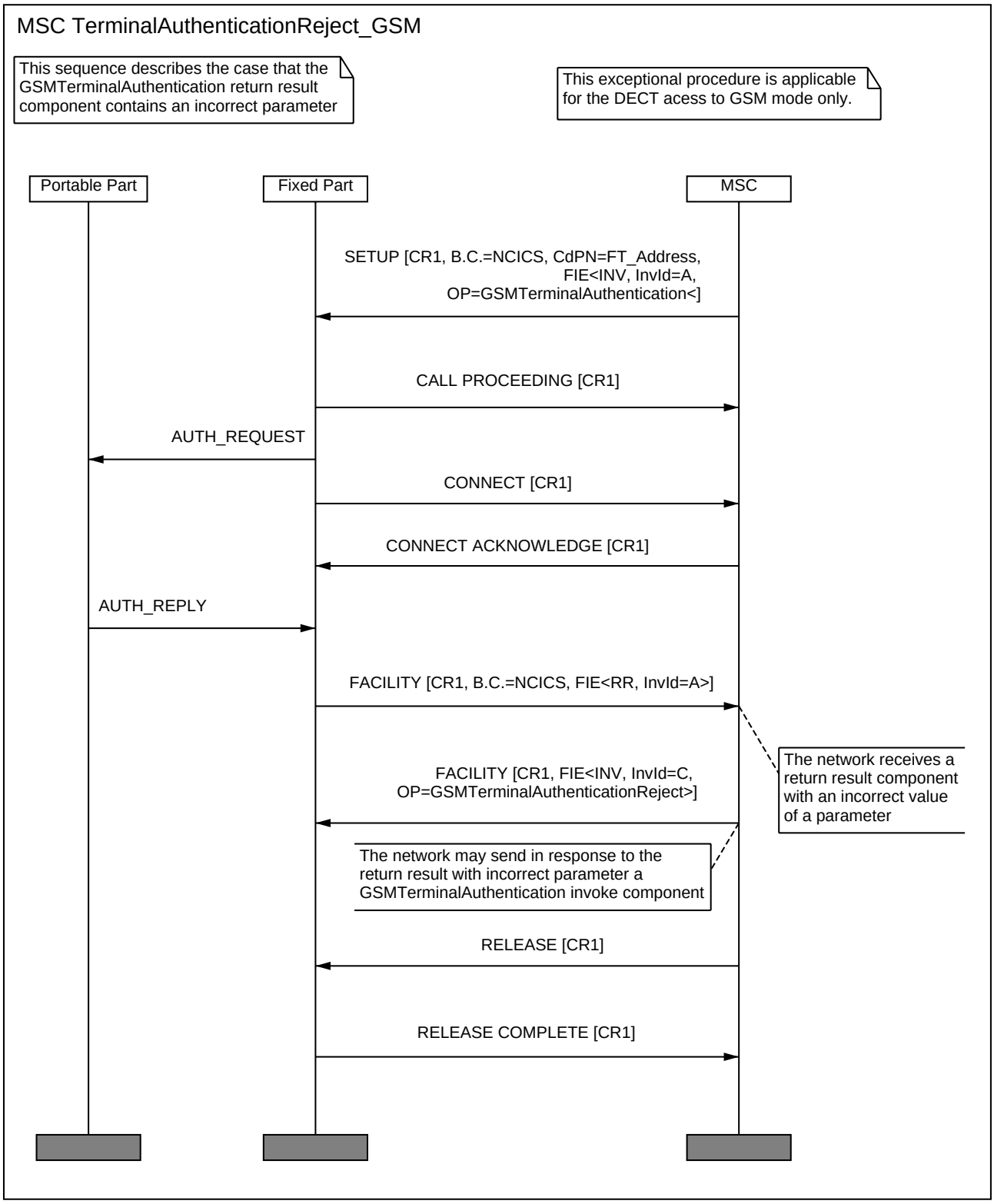
No diagram is provided.

A.3.2 Terminal authentication

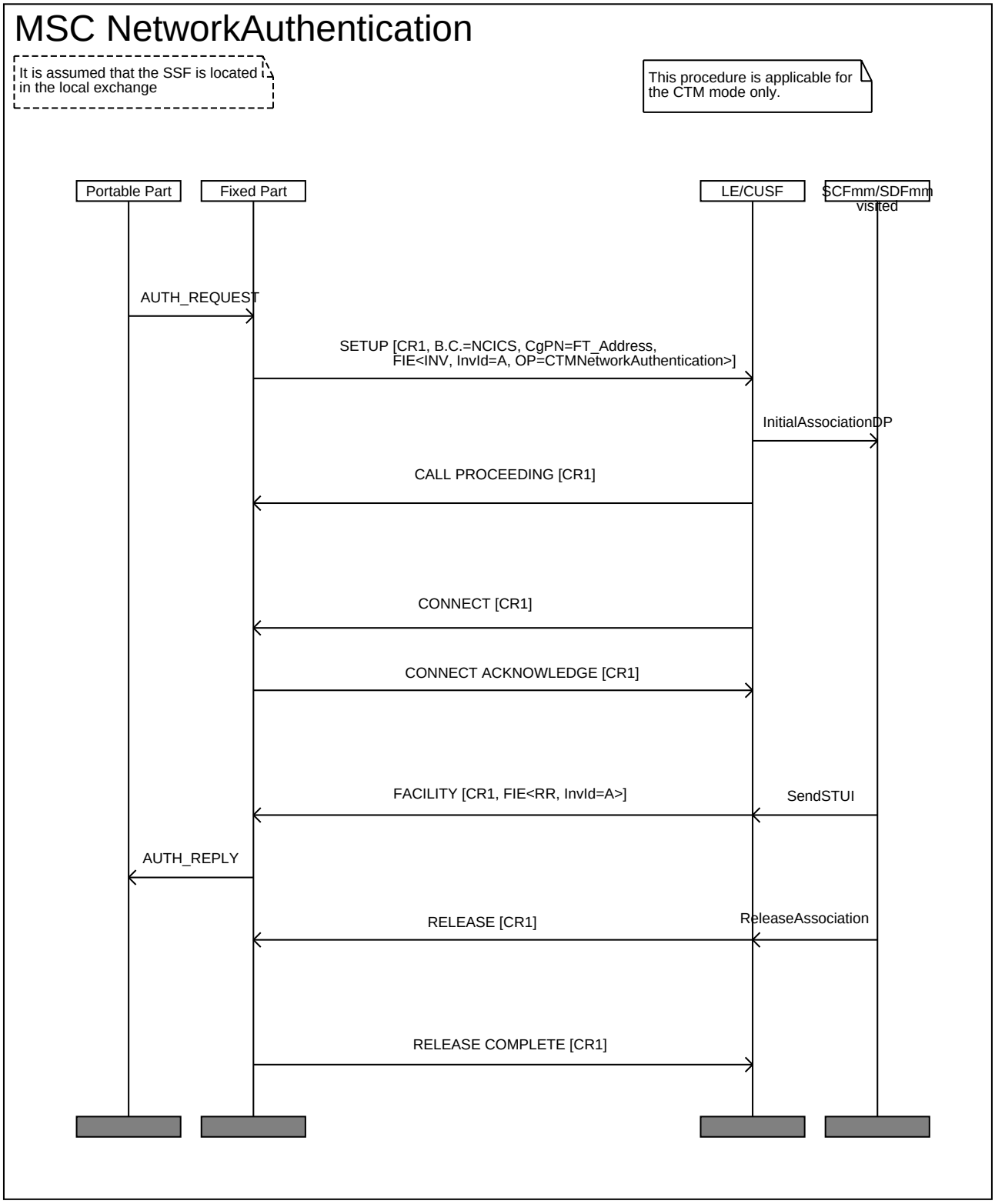
A.3.2.1 Terminal authentication - CTM



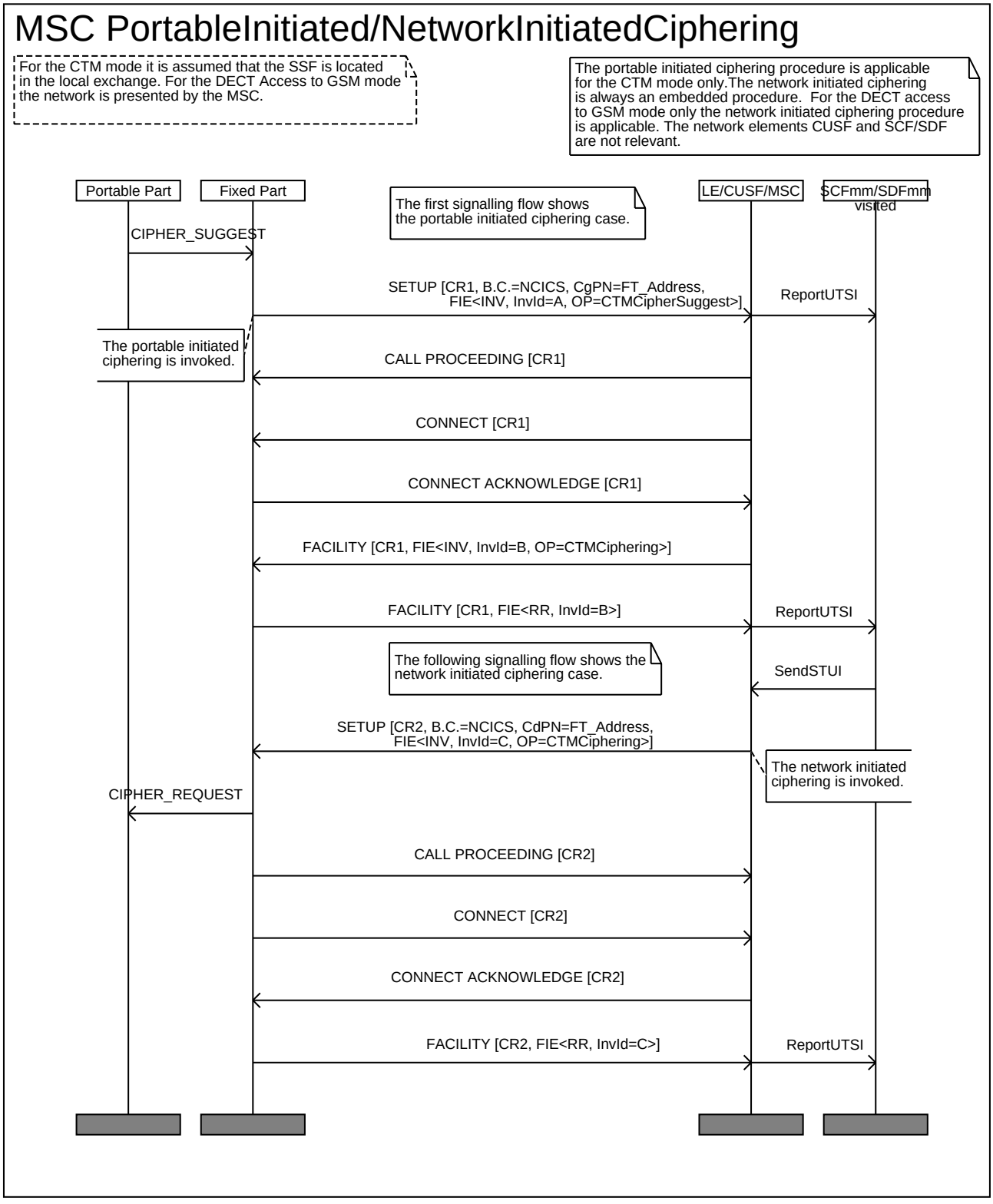
A.3.2.2 Terminal authenticationReject - GSM



A.3.3 Network authentication



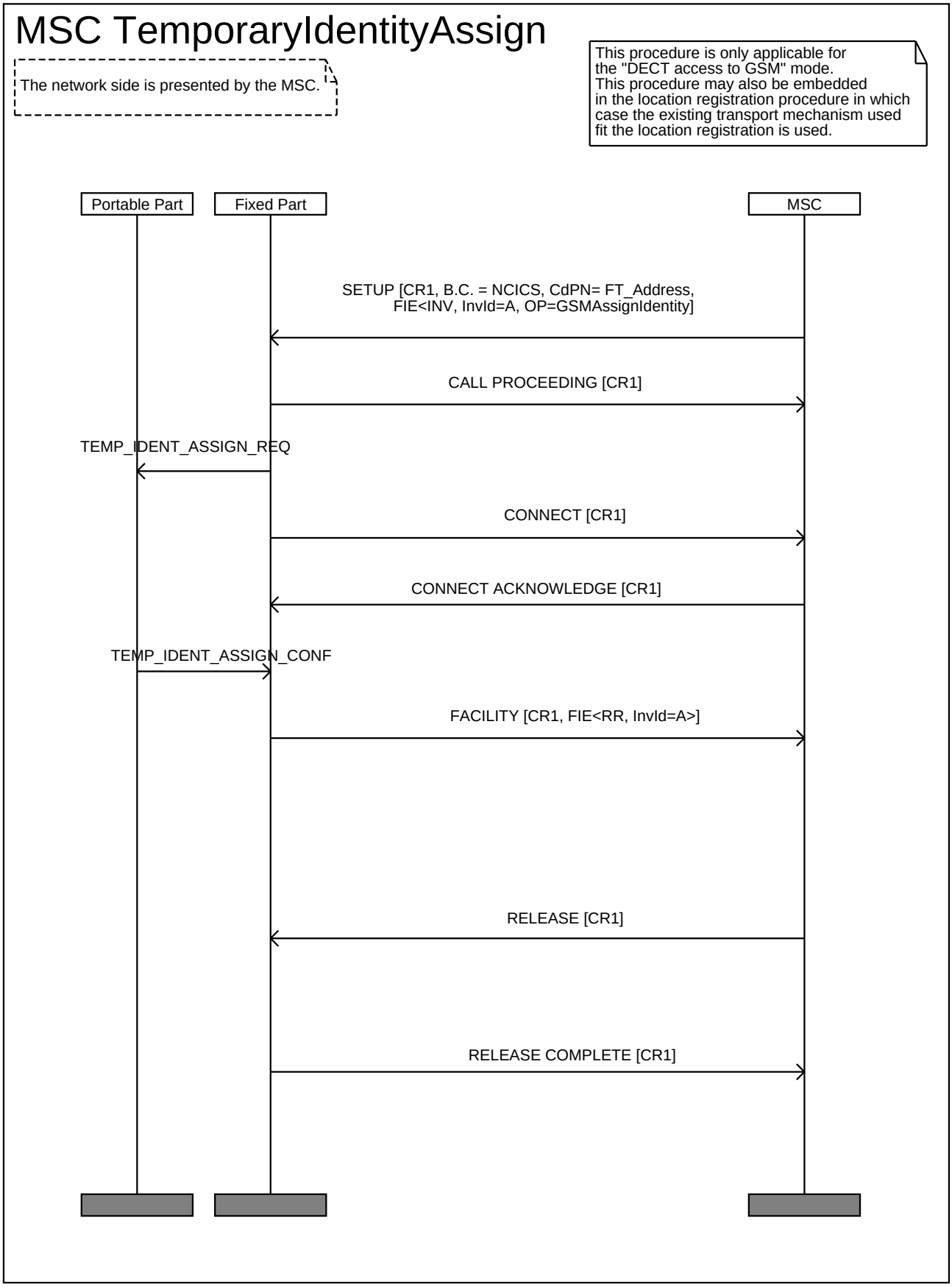
A.3.4 Network initiated ciphering



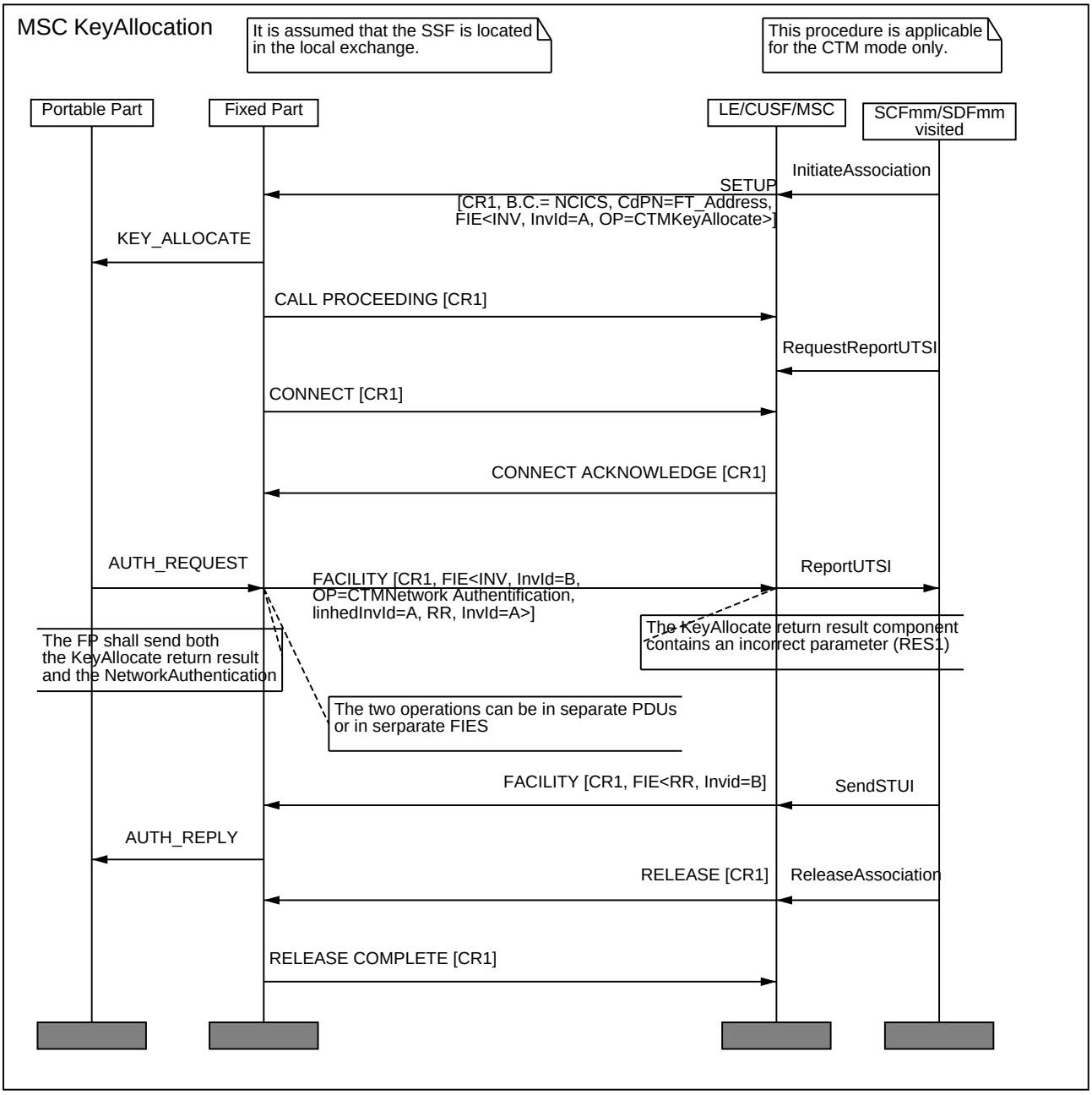
A.3.5 Portable initiated ciphering

The diagram is provided in the message flow of the previous subclause.

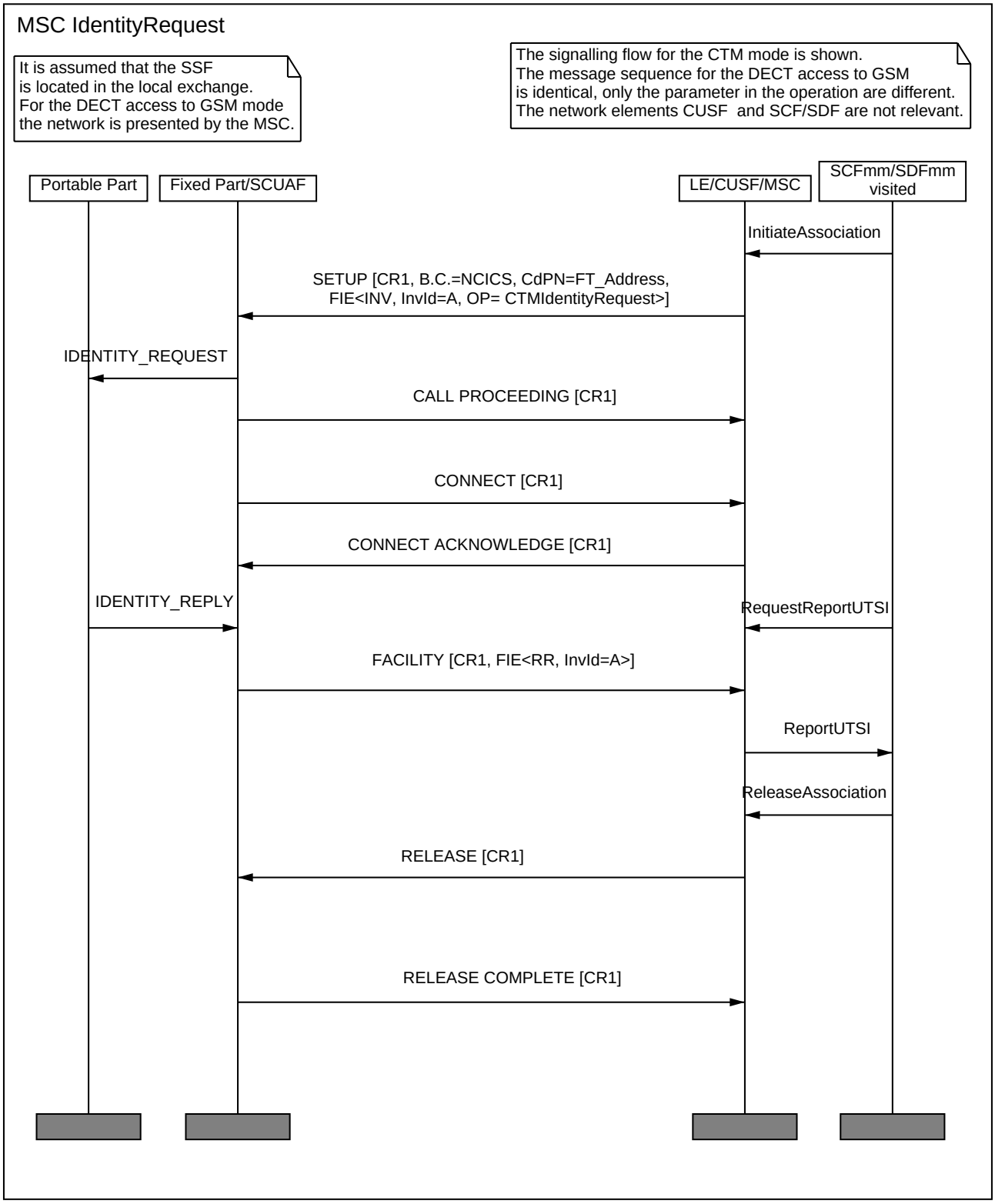
A.3.6 Temporary identity assignment



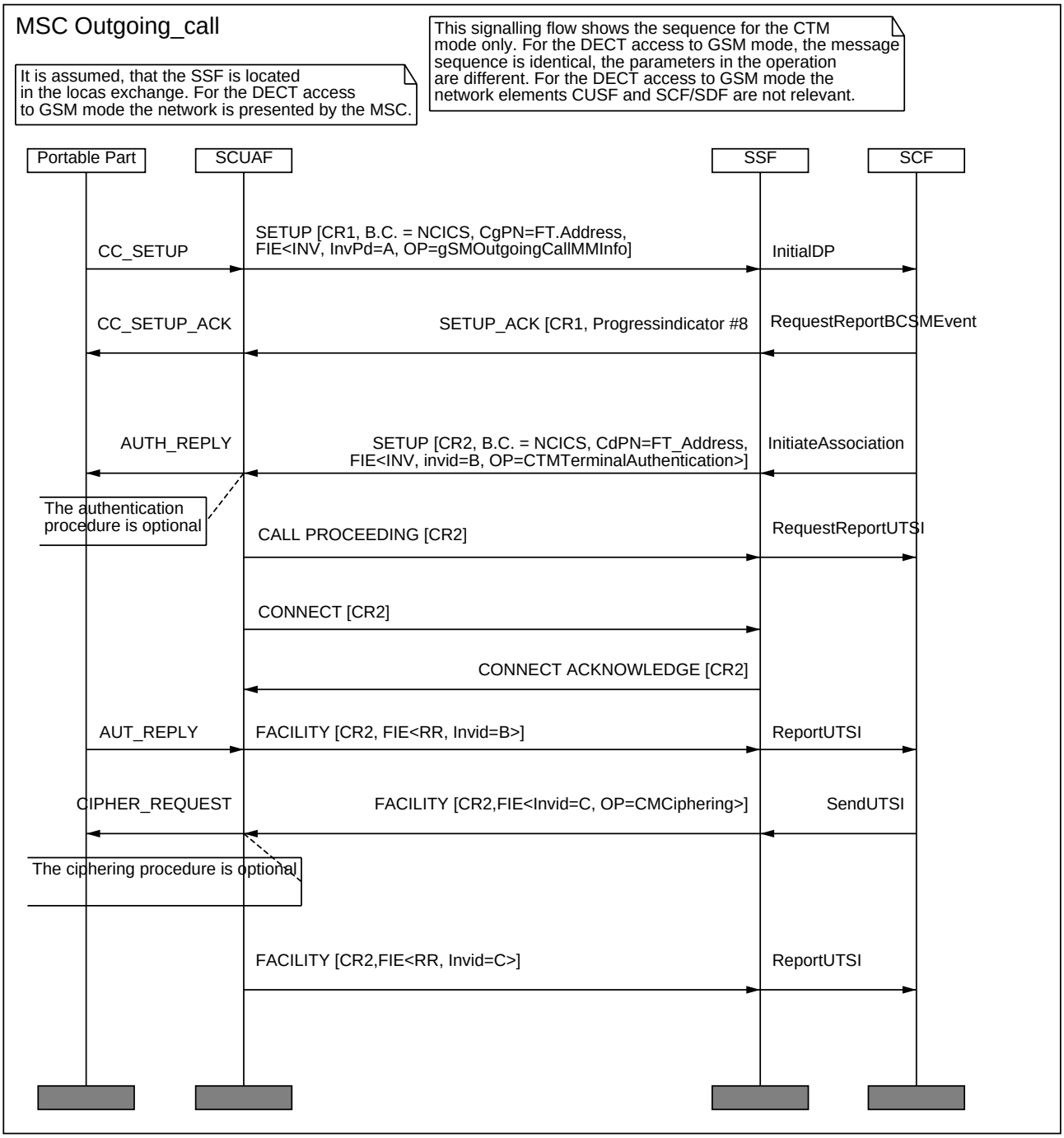
A.3.7 Key allocation



A.3.8 Identity request

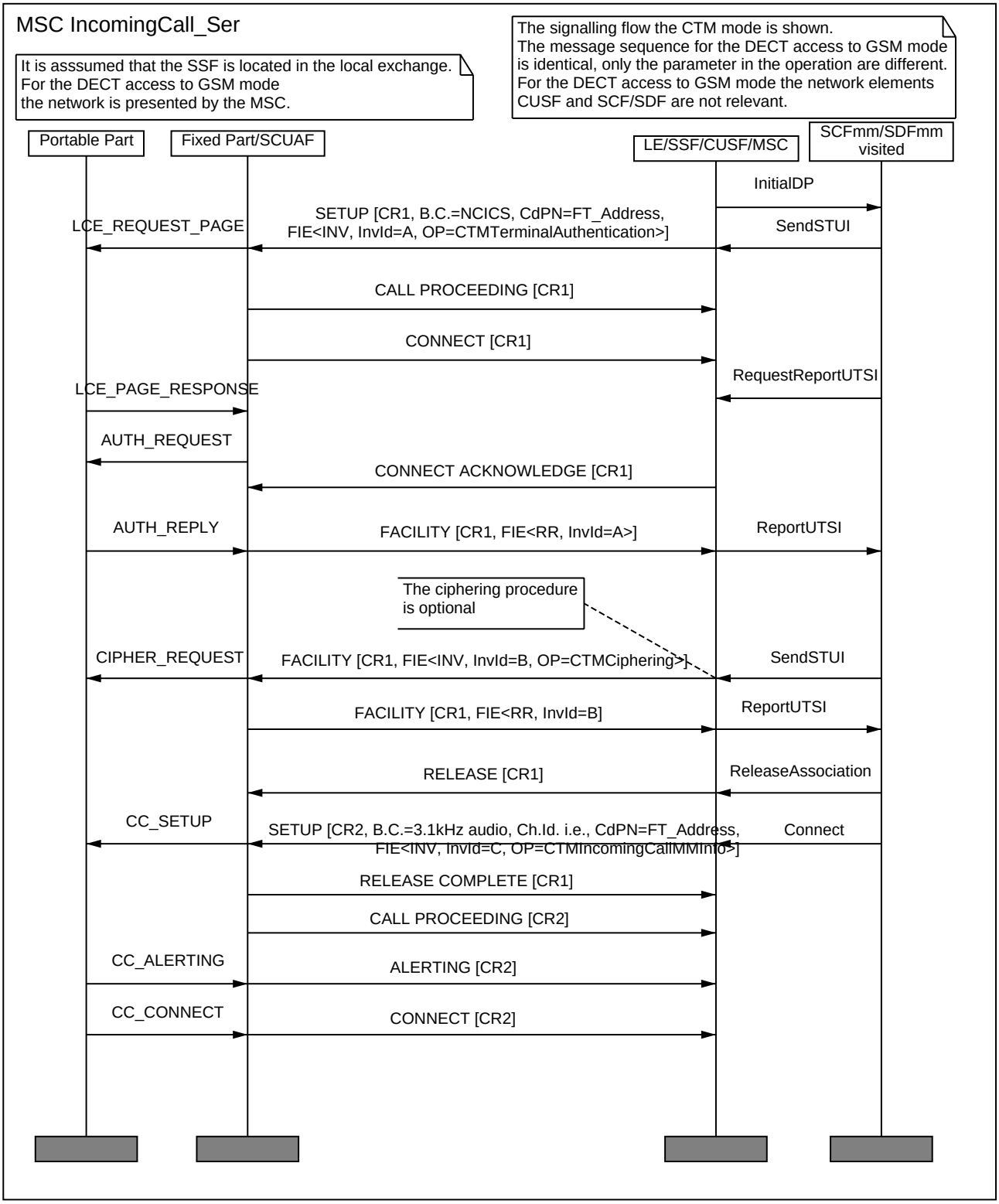


A.3.9 Outgoing call

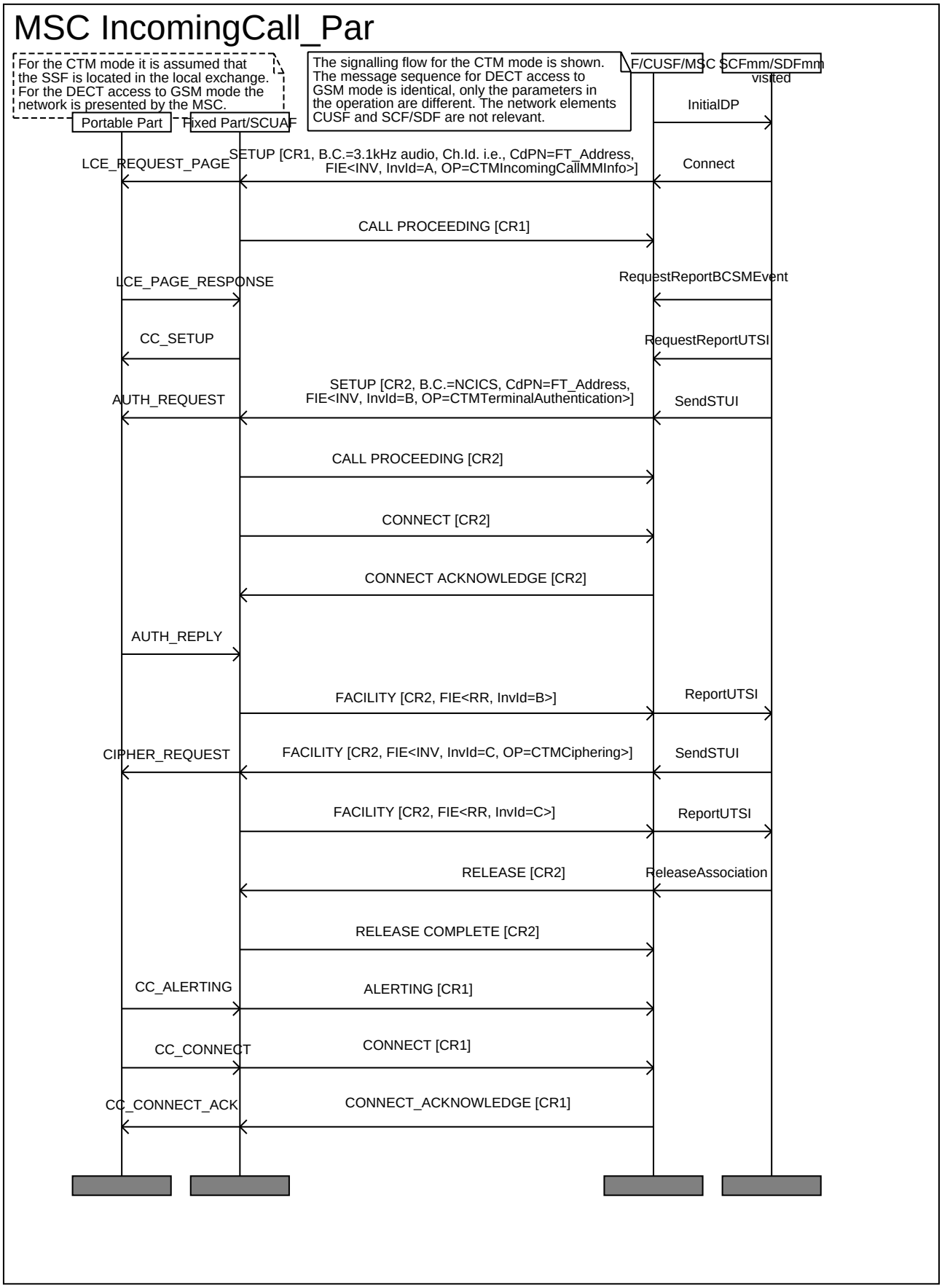


A.3.10 Incoming call

A.3.10.1 Incoming call serial



A.3.10.2 Incoming call parallel



Annex B (normative): Specific transport mechanism requirements for mobility management

This annex is designed to provide the informative material over and above EN 300 196-1 [7] for the transport of PDUs within the present document for signalling application for the mobility management service on the alpha interface.

B.1 Normative references

[E1] EN 301 061-1: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Generic functional protocol for the support of supplementary services at the "b" service entry point or Virtual Private Network (VPN) applications; Part 1: Protocol specification".

B.2 General

The mobility management application uses GFP procedures, Networked Call Independent Connection-Oriented Signalling (NCICS) connections, for transporting mobility management information.

The mobility management information is modelled as remote operations as specified in ITU-T Recommendations X.219 [20] and X.229 [21]. The remote operation components will be transported in Facility information elements on NCICS connections with <protocol profile> "Network Routing".

This annex describes the usage of the GFP NCICS connections by the mobility management application.

B.3 NCICS connection establishment

B.3.1 Normal NCICS connection establishment

Both the network and the user can initiate establishment of an NCICS connection.

The SETUP message, establishing the NCICS connection, shall always contain the a Facility information element with an invoke component indicating the Portable Identity and the requested operation. If mobility management procedures for different Portable Identities are initiated in parallel, different NCICS connections shall be established.

The coding of the Bearer capability information element shall be extended as specified in subclause 11.2.3 of EN 301 061-1 [E1].

The coding of the Channel identification information element shall be extended as specified in subclause 11.2.4 of EN 301 061-1 [E1].

B.3.2 NCICS connection establishment collision

If both network and user initiate NCICS connection establishment at the same time (collision of SETUP messages), two NCICS connections for the same Portable Identity may exist.

B.4 Information transfer on NCICS connection

An established NCICS connection shall be used by both network and user for all the mobility management procedures requested for the same Portable Identity. Therefore mobility management information related to several signalling procedures can be transported on the same NCICS connection (using one Call Reference).

In the case of NCICS connection establishment collision, all information related to one signalling procedure shall be transported using the same NCICS connection.

B.5 NCICS connection release

The RELEASE or RELEASE-COMPLETE messages shall not be used for exchange of any mobility management information.

B.5.1 Normal NCICS connection release

Both the network and the user may initiate the release of an NCICS connection.

It is preferred that the network initiates the release of the NCICS connection. In this case the user shall not initiate the release of the NCICS connection.

B.5.1.1 Radio interface loss

Even in case of radio interface loss at the user side, the normal release scenario applies.

In case of radio loss, the user shall inform the network about failure of all ongoing network initiated transactions by sending an appropriate return error invoke component, indicating the error value = "Radio connection failure". After having received the return error component, the network may decide to release the NCICS connection.

B.5.2 Abnormal NCICS release

In exceptional situations, e.g. if the user or network have lost information related to ongoing signalling procedures, an abnormal NCICS release shall be executed.

The message sequence is identical to the normal network initiated NCICS release. On receipt of the NCICS connection release request the receiver shall consider all signalling procedures which were using the concerning NCICS connection as terminated.

NOTE: Signalling procedure termination may involve informing the PP or other network elements.

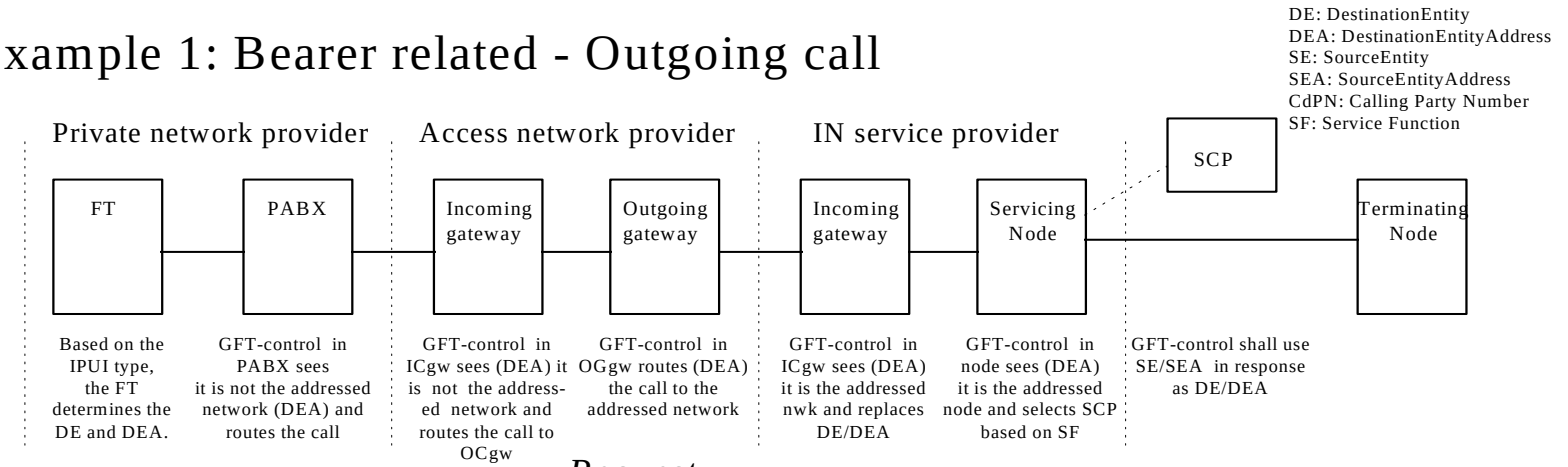
B.5.3 Collision case

Situations may arise in which a RELEASE message and a FACILITY message containing an invoke component collide. In this case the sender of the RELEASE message shall ignore the information received in the FACILITY message.

NOTE: The sender of the invoke component may decide to establish a new NCICS connection to retransmit the invoke component.

Annex C (informative): Information flow for the generic functional protocol

Example 1: Bearer related - Outgoing call



Request

CdPN	-	-	CdPN	CdPN	CdPN	CdPN
SE	endTerminal	endTerminal	endTerminal	endTerminal	endTerminal	endTerminal
SEA	-	-	-	-	-	-
DE	anyTypeOfNetwork	anyTypeOfNetwork	anyTypeOfNetwork	anyTypeOfNetwork	anyTypeOfNode	N/A
DEA	E.164 of IN service prov nwk	E.164 of IN service prov nwk	E.164 of IN service prov nwk	E.164 of IN service prov nwk	E.164 of IN servicing node	N/A
SF	CTM phase1	CTM phase1	CTM phase1	CTM phase1	CTM phase1	CTM phase1

Response

SE	anyTypeOfNode	anyTypeOfNode	anyTypeOfNode	anyTypeOfNode	anyTypeOfNode	N/A
SEA	E.164 of IN servicing node	E.164 of IN servicing node	E.164 of IN servicing node	E.164 of IN servicing node	E.164 of IN servicing node	N/A
DE	endTerminal	endTerminal	endTerminal	endTerminal	endTerminal	endTerminal
DEA	-	-	-	-	-	-
SF	CTM phase1	CTM phase1	CTM phase1	CTM phase1	CTM phase1	CTM phase1

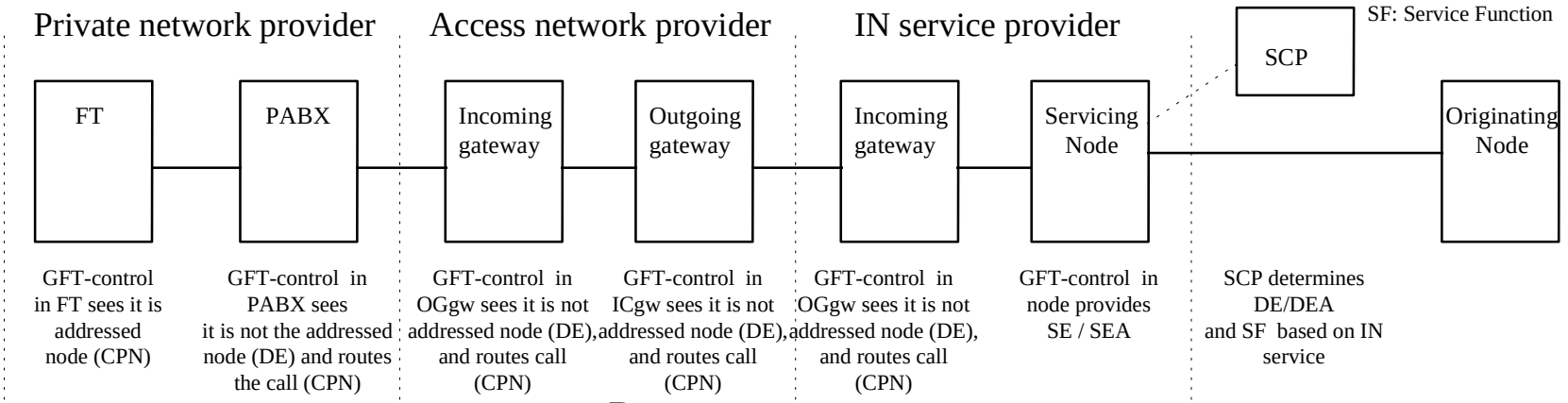
General assumptions

Servicing Node -> SCP:
It is assumed that the SE and the SEA (SEA empty for CTM) are provided to the SCP. The DE and DEA will not be provided to the SCP since the SCP will be aware of the address of the node it is connected to.

SCP -> Servicing Node:
It is assumed that the the DE and the DEA (DEA empty for CTM) are provided by the SCP. The SE and SEA will not be provided by the SCP since the Servicing node will be aware of it's own address.

Example 2: Bearer related - Incoming call

DE: DestinationEntity
DEA: DestinationEntityAddress
SE: SourceEntity
SEA: SourceEntityAddress
CdPN: Calling Party Number
SF: Service Function



Request

CdPN	CdPN	CdPN	CdPN	CdPN	CdPN	CdPN	CdPN
SE	anyType OfNode	anyType OfNode	anyType OfNode	anyType OfNode	anyType OfNode	N/A	
SEA	E.164 of IN servicing node	E.164 of IN servicing node	E.164 of IN servicing node	E.164 of IN servicing node	E.164 of IN servicing node	N/A	
DE	endTerminal	endTerminal	endTerminal	endTerminal	endTerminal	endTerminal	
DEA	-	-	-	-	-	-	
SF	CTM phase1	CTM phase1	CTM phase1	CTM phase1	CTM phase1	CTM phase1	

Response

SE	endTerminal	endTerminal	endTerminal	endTerminal	endTerminal	endTerminal	
SEA	-	-	-	-	-	-	
DE	anyTypeOfNode	anyTypeOfNode	anyTypeOfNode	anyTypeOfNode	anyTypeOfNode	N/A	
DEA	E.164 of IN servicing node	E.164 of IN servicing node	E.164 of IN servicing node	E.164 of IN servicing node	E.164 of IN servicing node	N/A	
SF	CTM phase1	CTM phase1	CTM phase1	CTM phase1	CTM phase1	CTM phase1	

<u>General assumptions</u>

Servicing Node -> SCP:
It is assumed that the SE and the SEA (SEA empty for CTM) are provided to the SCP. The DE and DEA will not be provided to the SCP since the SCP will be aware of the address of the node it is connected to.

SCP -> Servicing Node:
It is assumed that the the DE and the DEA (DEA empty for CTM) are provided by the SCP. The SE and SEA will not be provided by the SCP since the Servicing node will be aware of it's own address.

Annex D (informative): CTM versus DECT/GSM conventions

Equivalence between the parameters used for CTM and those used in DECT and GSM are shown in table D.1:

Table D.1: Parameters used in mobility management procedures

CTM	DECT (EN 300 175-5) [4]	GSM
CTMPortableId	IPUI	IMSI,TMSI,IMEI
CTMNewTemporaryId	-	IMSI,TMSI
CTMIdentityType	Identity type (7.7.19)	IMSI, TMSI, IMEI, IMEISV
CTMCipherInfo	Cipher Info (7.7.10)	Cipher key sequence number
CTMCipherKey	-	GSM Ciphering key (Kc)
CTMLocationAreaId	Location area (7.7.25)	Location area identity
CTMLocationRegistrationType	-	normal updating, periodic updating, IMSI attach
CTMAuthType	Auth type (7.7.4)	-
CTMFixedId	Fixed Identity (7.7.18) (RFPI, PARK)	-
CTMRAND	RAND (7.7.32)	RAND
CTMRs	RS (7.7.36)	-
CTMRES	RES (7.7.35)	SRES
CTMServiceClass	Service class (7.7.39)	-
CTMPortableCapabilities	Terminal capabilities (7.7.41)	Mobile Station Classmark 1
CTMBasicService	Basic service (7.6.4)	-
CTMAllocType	Allocation type (7.7.2)	-
CTMSignal	Signal (7.6.8)	-

Annex E (normative): Additions to the generic functional protocol for mobility management

This annex is designed to provide the minimum requirements over and above EN 300 196-1 [7] (and annex E) for the transport of PDUs within the present document for signalling application for the mobility management service on the alpha interface.

It is intended that this annex will be removed when a later version of EN 300 196-1 is developed.

E.1 Normative references

[E1] EN 301 061-1: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Generic functional protocol for the support of supplementary services at the "b" service entry point or Virtual Private Network (VPN) applications; Part 1: Protocol specification".

E.2 Definitions

AnyIntraNetworkNode: two cases exist:

- when specified without an address, the requested service functionality is to be provided at the next service provision point along the path of the transport mechanism that supports the service within the same service provider. For this value an outgoing gateway node or end node acts to provide end GFT-Control functionality; or,
- when specified with an associated address, the requested service functionality is to be provided at the next service provision point along the path of the transport mechanism within the same service provider. Where the first service provision point that has the given address does not wish to provide the service, it can alter the address to that of another service provision point either within the same service provider or within a different service provider. For this value an outgoing gateway node or end node that is not addressed discards the information.

NOTE: This is equivalent to the PSS1 value "anyTypeOfPINX" when used in a PSS1 environment with the exception that an interworking point with another protocol will also act as an gateway PINX.

AnyNode: two cases exist:

- when specified without an address, the requested service functionality is to be provided at the next service provision point along the path of the transport mechanism that supports the service within the same or any subsequent service provider. For this value an end node acts to provide end GFT-Control functionality; or,
- when specified with an associated address, the requested service functionality is to be provided at the next service provision point along the path of the transport mechanism within the same or any subsequent service provider that has the given address. Where the first service provision point that has the given address does not wish to provide the service, it can alter the address to that of another service provision point either within the same service provider or within a different service provider. For this value an end node that is not addressed discards the information.

EndIntraNetworkNode: the requested service functionality is to be provided at the last service provision point along the path of the transport mechanism within the current service provider. For this value an outgoing gateway node or end node acts to provide end GFT-Control functionality.

NOTE: This is equivalent to the PSS1 value "endPINX" when used in a PSS1 environment with the exception that an interworking point with another protocol will also act as an gateway PINX.

EndNode: the requested service functionality is to be provided at the last service provision point along the path of the transport mechanism before a terminal is reached. This may be within the current service provider or in any subsequent service provider. For this value an end node acts to provide end GFT-Control functionality.

EndTerminal: two cases exist:

- when specified without an address, the requested service functionality is to be provided at the terminal along the path of the transport mechanism. This terminal can be attached to the current service provider or to any subsequent service provider; or,

- when specified with an associated address, the requested service functionality is to be provided at the terminal along the path of the transport mechanism that has the given address. This terminal can be attached to the current service provider or to a subsequent service provider.

terminal address: an address assigned to the terminal by the network to which it is attached,

service address: an address that identifies the service provision point. This can be any valid address within the available numbering plan and is assigned by the service provider.

NOTE: The following considerations can apply:

- for addressing from outside a service provider, an address that does not represent a geographical location is preferable, so that the service provision point can be changed to a different geographical location without resulting in a need to change the assigned number. This non-geographic address may identify either an individual service within the service provider, the entire service provider, or any appropriate grouping of functionality in between.

- for addressing within the network of a service provider, the same constraints do not apply, and therefore geographic addresses can be used. This is an issue for the service provider as to how routeing within the service provider's domain is reconfigured.

end node: the node that is at either: the end point of the transport mechanism; or at the end PINX or Local Exchange (LE); whichever comes first along the path of the transport mechanism.

service provision point: a node capable of providing service functionality, and where checking should therefore be performed to see if the specific requested service is provided.

terminal: the equipment provided at the user side of the coincident S and T reference point or at the user side of the S reference point.

E.3 Abbreviations

APM	Application Transport Message
ASE	Application Service Element
COBI	Call Oriented Bearer Independent
CO-DSS1	Connection oriented DSS1
CUSF	Call Unrelated Service Function
CUSP	Call Unrelated Service Point
GFT	Generic Function Transport
INAP	Intelligent Network Application Protocol
SCF	Switch and Control Function
SCP	Service Control Point
SSF	Service Specific Function
SSP	Service Switching Point
TCAP	Transaction Capability Application Part
VPN	Virtual Private Network

E.4 Description

Figures E.1 and E.2 show the protocol ASEs used for the transport of information relating to the CTM ASE.

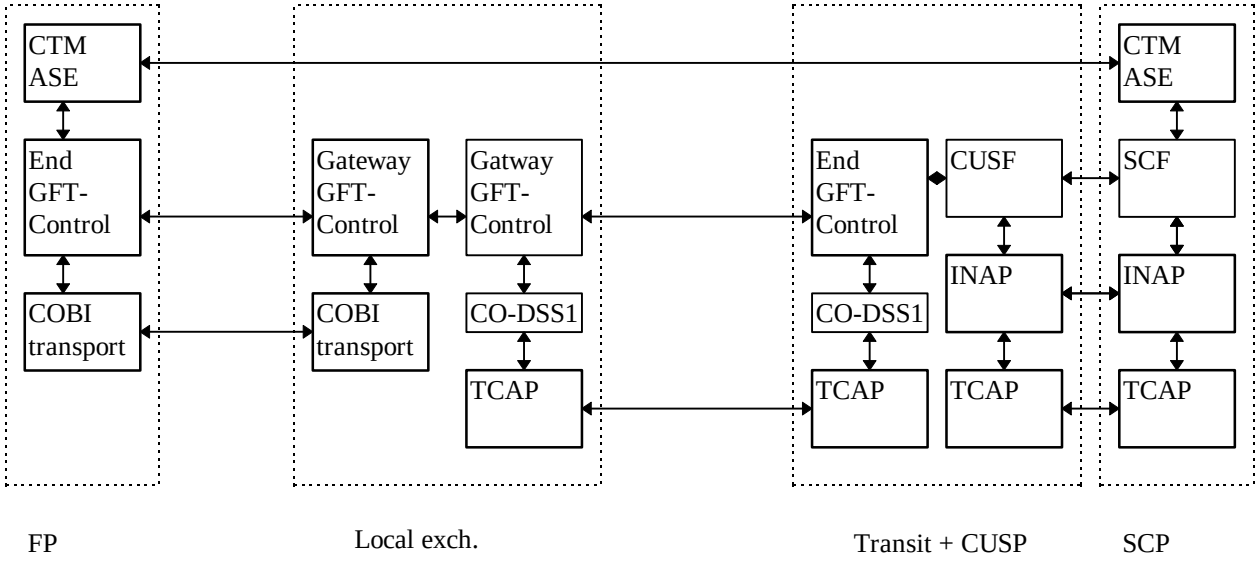


Figure E.1: Bearer-independent transport of CTM information

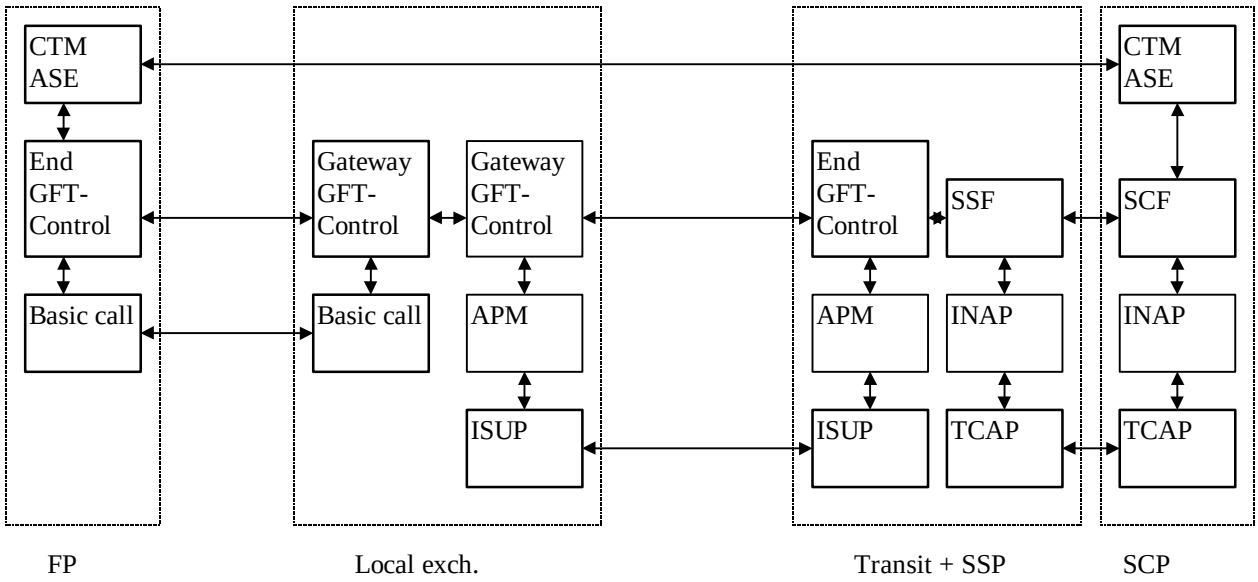


Figure E.2: Bearer-related transport of CTM information

Within these diagrams, the following descriptions apply:

1) Transport mechanism. For DSS1, this is either:

   - the existing basic call, for bearer-related transport, as defined in EN 300 196-1 [7].
   - the new Connection-Oriented Bearer-Independent (COBI) transport mechanism.

Both mechanism are link by link, i.e. a separate state machine exists at each node that is passed through that controls the establishment, use and release of this mechanism. The transport mechanism is routed by the Called party number information element, and in the absence of information is routed based on information from GFT-control. The transport mechanisms for SS#7 are ISUP (with the use of the APM) or TCAP. As the mechanism is link by link, any protocol that is defined as a local acknowledgement, rather than of end significance, should not be delayed by remote activities (e.g. in an SCF).

2) GFT-control. This provides an entity that analyses whether service functionality should be provided locally, or should be provided at some entity further along a transport mechanism (either existing or yet to be created, possibly further created based on information from GFT-control). In DSS1 this information is present within the Protocol profile field of the Facility information element and within the network facility extension APDU within the component part of the Facility information element. In ISUP this information would be transported as part of a TCAP user ASE or as part of an APM user ASE but this functionality has yet to be discussed within technical subcommittee SPS1. Special actions of GFT-Control occur at incoming gateways to networks.

3) ROSE. This is as defined by Recommendation X.219/X.229 and is equivalent to the functionality used within TCAP and Recommendation X.880 [23]. In an IN implementation, we understand that this functionality will be within the SCF for mobility management specific APDUs. Other APDUs that are not related to mobility management in the same message may be handled differently.

4) Mobility management ASE. This provides the mobility management specific protocol for the alpha interface. If IN provides this functionality, it is located within the SCP. INAP is assumed to transport the information transparently and the INAP ASE passes information to this ASE within the SCF. The ASE is that defined within the DSS1 specification for the network side.

The LE and the IN SSP may be co-located within the same exchange. Between the FP and the LE, a private network may be inserted, which provides functionality at the GFT-control and transport mechanism level.

This annex provides the additional requirements to support the above for interfaces using the DSS1 protocol.

E.5 Coding requirements

E.5.1 Transport mechanism

See annex B.

E.5.2 GFT-control

The Facility information element shall be extended as shown in subclause 11.2.1 of EN 301 061-1 [E1] to include the network facility extension APDU. Inclusion of the network facility extension APDU shall be permitted based on the coding of the protocol profile field as defined in subclause 11.2.1 of EN 301 061-1 [E1].

The definition of the network facility extension APDU required for the mobility management service using ASN.1 as specified in ITU Recommendations X.208 [19] is given in subclause E.7.2.1.

This APDU shall be included within a Facility information element. This Facility information element may be included in any appropriate message as specified in EN 300 196-1 [7], subclause 8.3.1.1, unless a more restrictive specification is given in clause 9.

The inclusion of the components in Facility information elements is defined in EN 300 196-1 [7], subclause 11.2.2.1.

E.5.2.1 Network facility extension

Table E.1: Network facility extension

```
Network-Facility-Extension
                        {itu-t identified-organisation etsi(0) 1144 network-facility-extension(2)}

DEFINITIONS ::=
EXPORTS NetworkFacilityExtension;
    IMPORTS PartyNumber FROM Addressing-Data-Elements
                       { ccitt( 0) identified-organization
                        etsi(0) 196 addressing-data-elements(6) };
BEGIN

NetworkFacilityExtension    ::=     [10] IMPLICIT SEQUENCE
        { sourceEntity              [0] IMPLICIT EntityType,
          sourceEntityAddress       [1] IMPLICIT AddressInformation OPTIONAL,
          destinationEntity         [2] IMPLICIT EntityType,
          destinationEntityAddress  [3] IMPLICIT AddressInformation OPTIONAL,
          serviceFunction           [4] IMPLICIT ServiceFunction OPTIONAL
        }

EntityType  ::= ENUMERATED
          { endIntraNetworkNode (0),
            anyIntraNetworkNode (1),
            endNode (2),
            anyNode (3),
            endTerminal (4)
          }

AddressInformation    ::=   PartyNumber

ServiceFunction          ::=        OBJECT IDENTIFIER

END     -- of Network Facility Extension
```

E.5.2.2 Service function values

Table E.2: Service function values

```
Service-Function-Values
                        {itu-t identified-organisation etsi(0) 1144 service-function(3)}

DEFINITIONS ::=
EXPORTS cTM, dECTAccessToGSM;

BEGIN

cTM::= globalValue {itu-t(0) identified-organisation etsi(0) serviceFunction(2) 1}
dECTAccessToGSM ::= globalValue {itu-t(0) identified-organisation etsi(0) serviceFunction(2) 2}

END     -- Service-Function-Values
```

E.6 Signalling procedures at the coincident S and T reference point

E.6.1 GFT-control

E.6.1.1 Requirements for sending mobility management APDUs

Table E.2 below identifies the setting of the contents of the network facility extension APDU to be used by the sending mobility management ASE in either the fixed part or the network.

NOTE: The network facility extensions APDU for CTM is different from the network facility extensions APDU for VPN.

Table E.3: Contents of the network facility extension APDU

	Bearer related		**Bearer unrelated**	
IE/parameter	USER -> NWK	NWK -> USER	USER -> NWK	NWK -> USER
Bearer Capability	- "telephony 3,1kHz" - "speech" - "3,1 kHz audio"	- "telephony 3,1kHz" - "speech" - "3,1 kHz audio"	"Call independent Signalling Connection"	"Call independent Signalling Connection"
Called Party Number	- (shall not be send1))	FT address (cond to be send (MSN,DDI))	E.164 of servicing network (normally not included, use destEntityAddress if not received)	FT address (cond to be send (MSN,DDI))
Calling Party Number	E.164 number of FT (optional to be send, required to be handled)	E.164 of originating party (cond based on CLIP subscription)	E.164 number of FT (optional to be send, required to be handled)	- (shall not be sent, discard if received)
Facility				
Protocol Profile	"Networking Extensions"	"Networking Extensions"	"Networking Extensions"	"Networking Extensions"
Network Facility Extension				
Service function	"CTM" or "DECT access to GSM" (mandatory)	"CTM" or "DECT access to GSM"(mandatory)	"CTM" or "DECT access to GSM" (mandatory)	"CTM" or "DECT access to GSM" (mandatory)
sourceEntity	"endTerminal" (mandatory)	"anyNode" (mandatory)	"endTerminal" (mandatory)	"anyNode" (mandatory)
SourceEntityAddress	- (absent)	Address of serving node	- (absent)	Address of serving node
destinationEntity	"anyNode" (mandatory)	"endTerminal" (mandatory)	"anyNode" (mandatory)	"endTerminal" (mandatory)
destinationEntityAddr	Service address	- (absent)	Service address	- (absent)

NWK: Network
CLIP: Calling Line Identity Presentation
MSN: Multiple Subscriber Number
DDI: Direct Dialling In
PSS1: Private Signalling System No. one
NOTE: If bearer exists already (column 2,3,4,5):
DestinationEntity: SourceEntity of APDU responded to
DestinationEntityAddress: SourceEntityAddress of APDU responded to
1) Note that for CTM the number of the requested destination party (E.164) will be sent later in overlap sending.

E.6.1.2 Requirements for receiving mobility management APDUs

Table E.3 identifies the actions to be performed by a receiving GFT-control entity when a Facility information element is received at the coincident S and T reference point. When reading the table the following should be understood.

- Rows should be processed from first to last. The order of processing is:
  - to check the syntactic correctness of the first three octets of the Facility information element;
  - process the value of the protocol profile field;
  - to check the syntactic correctness of the included network facility extension APDU;
  - to process the network facility extension APDU and its contents and as a result, to decide that the mobility management functionality is provided locally (i.e. end GFT-control) or that the mobility management functionality is not provided locally (i.e. transit GFT-control);
- Italicised text indicates the expected normal values for reception. Other values are exceptional values but may still result in successful processing and provision of a mobility management ASE.
- Procedures are intended to be consistent with those for PSS1 GFT-control, acknowledging that additional values have been provided.
- The following mobility management specific assumptions have been made:
  - Mobility management ASE (User side) is always provided in the user side of an S reference point or the user side of a coincident S and T reference point. A private network does not provide CTM functionality that crosses the T reference point.
  - Mobility management ASE (Network side) is always provided in the public network supporting the T reference point or in the coincident S and T reference point.
  - This table covers no generic transfer service provision rights that may need to be checked at each incoming network gateway.

Table E.4: Actions on reception of network facility extension at the coincident S and T reference point

	Action on reception	
Received parameter or field	**User at coincident S and T reference point**	**Network at coincident S and T reference point**
Protocol profile	**If** *value = networking extensions then continue processing* **else** treat according to EN 300 196-1 [7]	**If** *value = networking extensions then continue processing* **else** treat according to EN 300 196-1 [7]
Network facility extension APDU	**If** absent, then provide CTMα APDUs to ROSE and mobility management ASE **else if** present and incorrectly coded then discard contents of Facility information element **else** *if present and correctly coded then process as below*	**If** absent, and a mobility management ASE is present at this LE then provide mobility management APDUs to ROSE and mobility management ASE **else if** absent, and a mobility management ASE is not present at this LE then discard contents of Facility information element **else if** present and incorrectly coded then discard contents of Facility information element **else** *if present and correctly coded then process as below*
DestinationEntity	**If** value ≠ endTerminal then discard contents of Facility information element **else if** *value = endTerminal process as below*	**If** value = anyNode then process as below **else** action to be performed are outside the scope of the present document
DestinationEntityAddress	**If** *absent, then process as below* **else if** present and value is E.164 number of terminal then process as below **else** if present and value is not E.164 number of terminal then discard contents of Facility information element	**If** *absent then process as (A) below* **else if** *present and address = this service provider then process as (A) below* **else** if present and address ≠ this service provider then pass contents of Facility information element including address to SS#7 GFT-Control or equivalent for onward transmission
Received parameter or field	**User at coincident S and T reference point**	**Network at coincident S and T reference point**
ServiceFunction	**If** absent then provide mobility management APDUs to ROSE and mobility management ASE **else if** *present and value is cordlessTerminalMobility then provide* mobility management *APDUs to ROSE and* mobility management *ASE* **else** send reject component and discard contents of Facility information element	**(A)** *Check ServiceFunction value (if absent use default entry) against internal serviceFunction location list.* **If** *local provided the provide* mobility management *APDUs to ROSE and* mobility management *ASE* **else if** *not local then encode new NFE with values appropriate to serviceFunction location list and pass contents of Facility information element including address to SS#7 GFT-Control or equivalent for onward transmission*

E.7 Procedures for interworking with private ISDNs

E.7.1 GFT-control

E.7.1.1 Requirements for sending mobility management APDUs

The mobility management ASE cannot exist within the user side of the T reference point, but only within an FP beyond the private network. The private network therefore relays information within the network facility extension APDU unchanged unless the private network itself is addressed, and does not itself send mobility management APDUs.

For the network side, the requirements specified in subclause E.6.2.1 shall apply.

E.7.1.2 Requirements for receiving mobility management APDUs

Table E.4 identifies the actions to be performed by a receiving GFT-control entity when a Facility information element is received at the T reference point. When reading the table the following should be understood.

- Rows should be processed from first to last. The order of processing is:
  - to check the syntactic correctness of the first three octets of the Facility information element;
  - process the value of the protocol profile field;
  - to check the syntactic correctness of the included network facility extension APDU;
  - to process the network facility extension APDU and its contents and as a result, to decide that the mobility management functionality is provided locally (i.e. end GFT-control) or that the mobility management functionality is not provided locally (i.e. transit GFT-control).
- Italicised text indicates the expected normal values for reception. Other values are exceptional values but may still result in successful processing and provision of a mobility management ASE.
- Procedures are intended to be consistent with those for PSS1 GFT-control, acknowledging that additional values have been provided.
- The following mobility management specific assumptions have been made:
  - Mobility management ASE (User side) is always provided in the user side of an S reference point or the user side of a coincident S and T reference point. A private network does not provide mobility management functionality that crosses the T reference point.
  - Mobility management ASE (Network side) is always provided in the public network supporting the T reference point or in the coincident S and T reference point.
  - This table covers no generic transfer service provision rights that may need to be checked at each incoming network gateway.

Table E.5: Actions on reception of network facility extension at the T reference point

	Action on reception	
Received parameter or field	**User at T reference point**	**Network at T reference point**
Protocol profile	**If** *value = networking extensions then continue processing* **else** treat according to EN 300 196-1 [7]	The procedures at the coincident S and T reference point apply
Network facility extension APDU	**If** absent then discard contents of Facility information element (could process if mobility management ASE is available locally but this situation does not exist) **else if** present and incorrectly coded then discard contents of Facility information element **else** *if present and correctly coded then process as below*	The procedures at the coincident S and T reference point apply
DestinationEntity	**If** *value = endTerminal then process as below* **else** actions are outside the scope of the present document	The procedures at the coincident S and T reference point apply
DestinationEntityAddress	*ignore address and pass contents of Facility information element including address to PSS1 GFT-Control or equivalent for onward transmission*	The procedures at the coincident S and T reference point apply
ServiceFunction	Not applicable	The procedures at the coincident S and T reference point apply

Annex F (Informative): SDL system structure description

The system is structure like that:

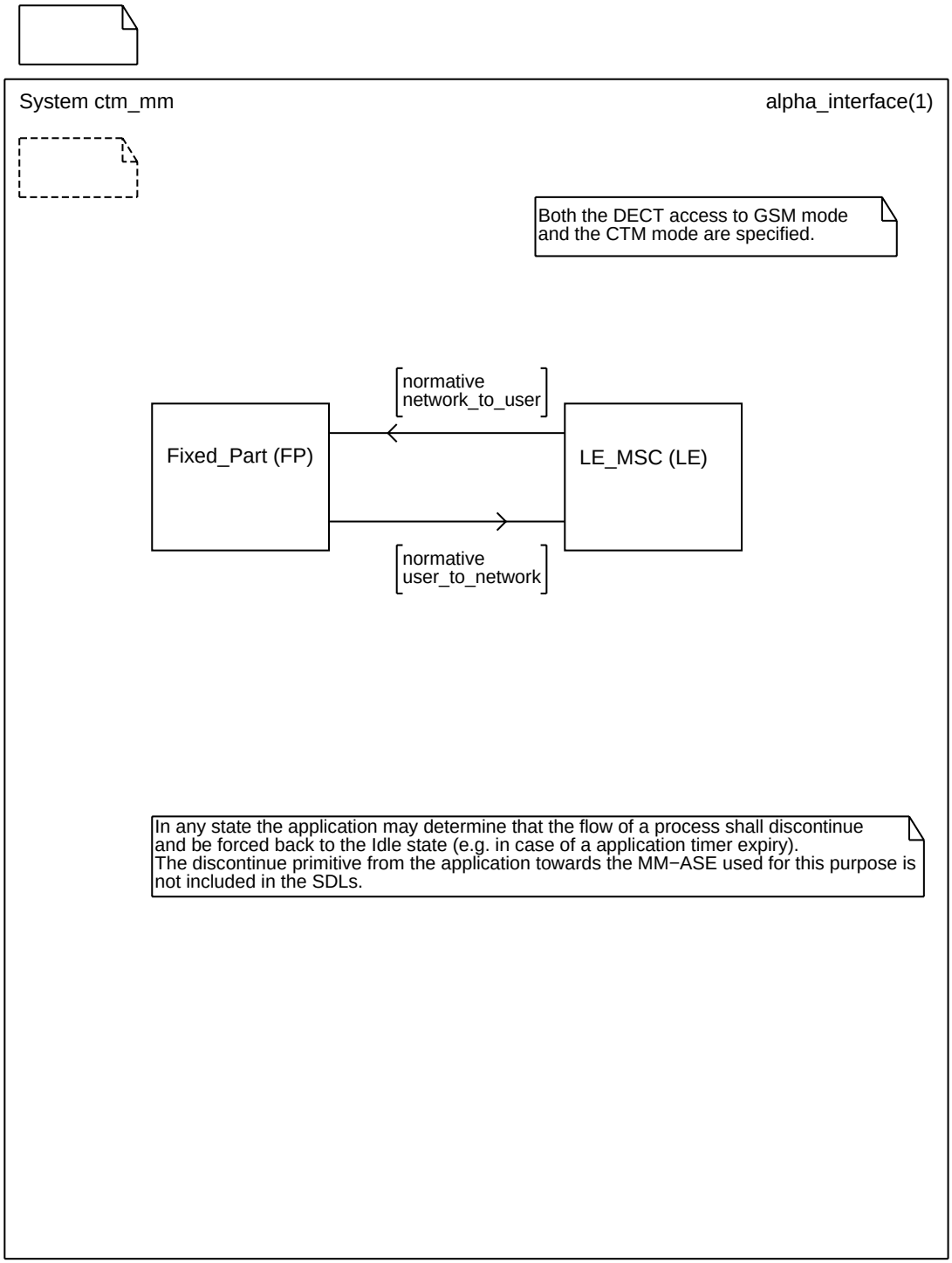


Figure F.1: Alpha interface

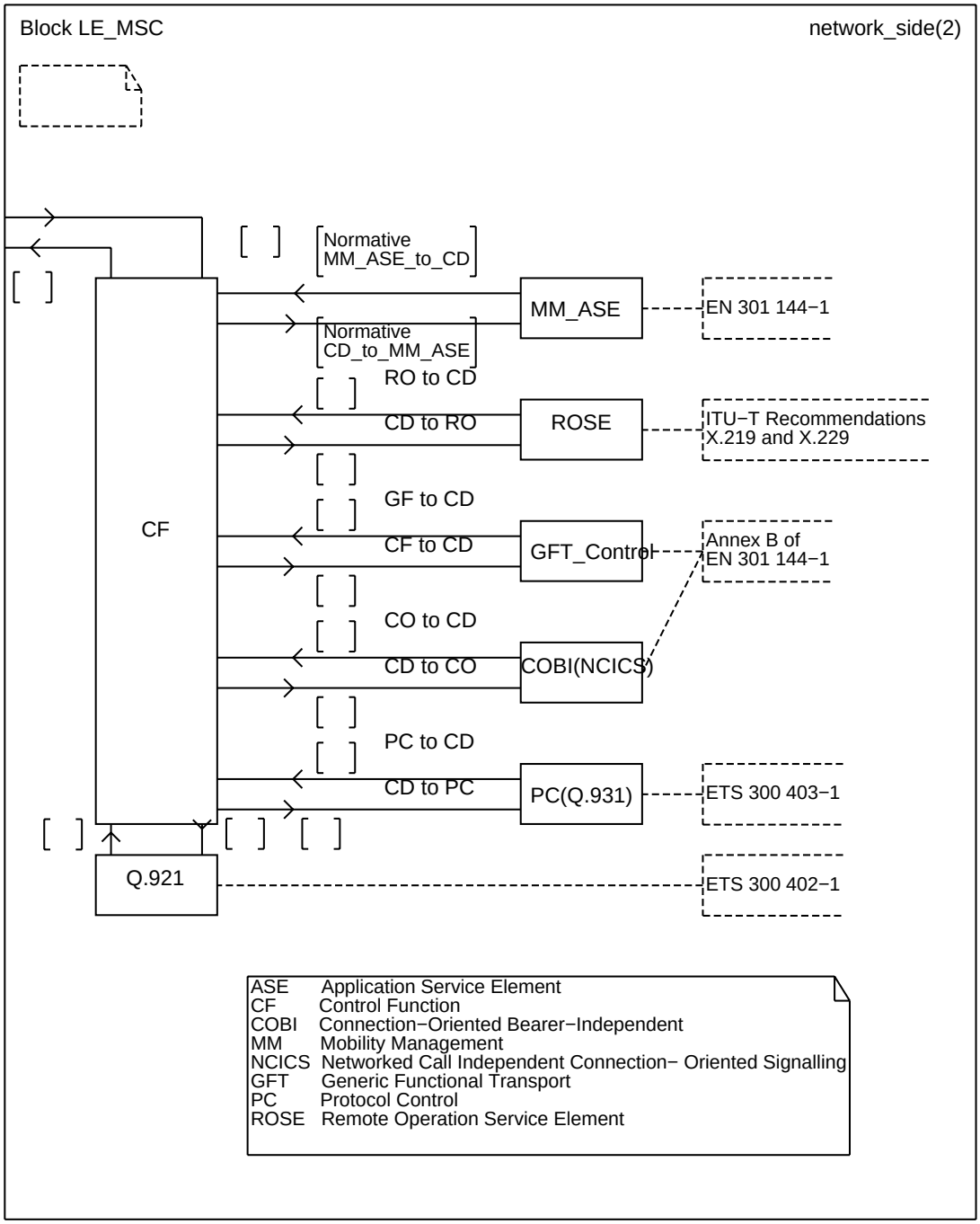


Figure F.2: Network side

Figure F.3: Block LE MSC

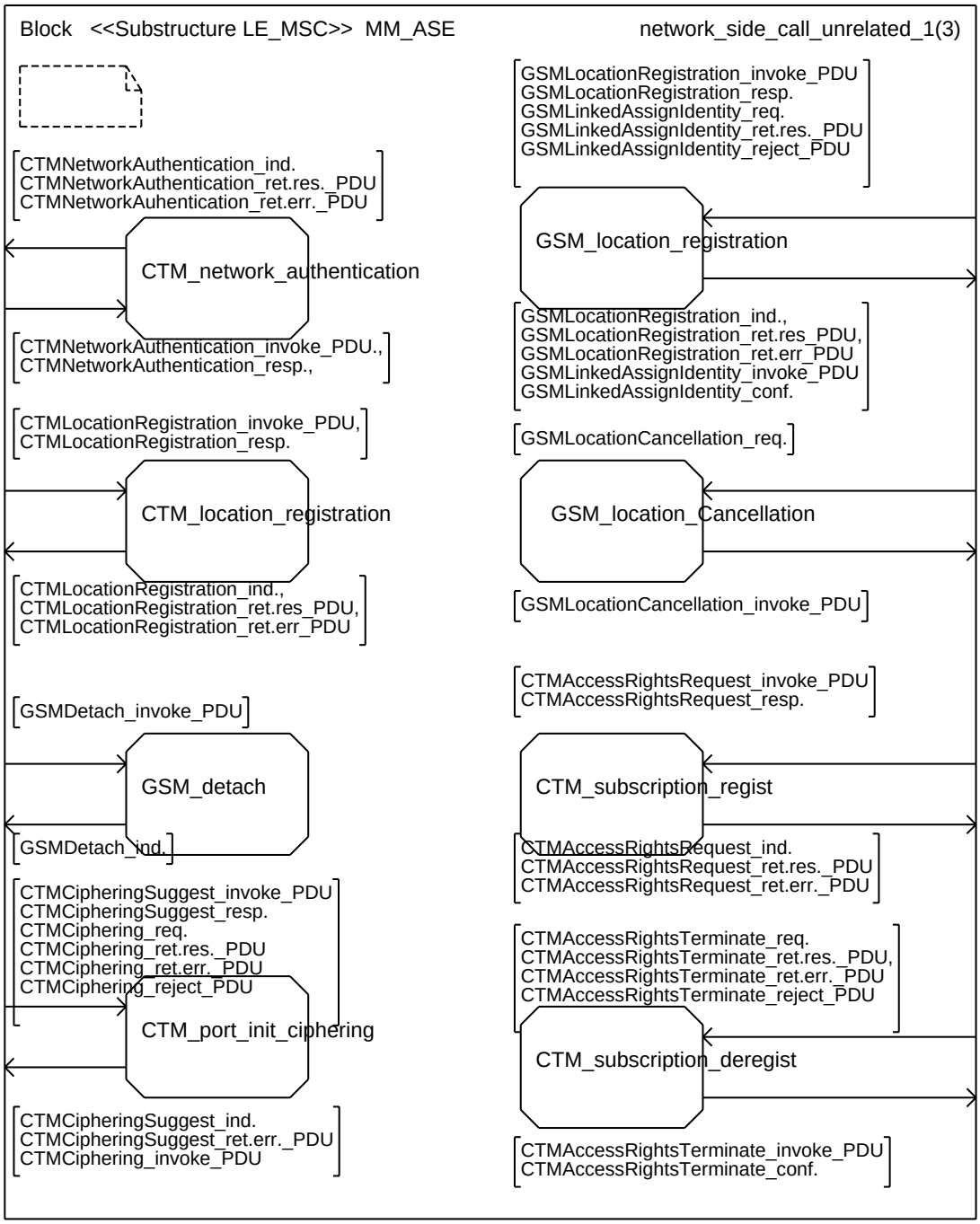


Figure F.4: Network side call unrelated (1 of 3)

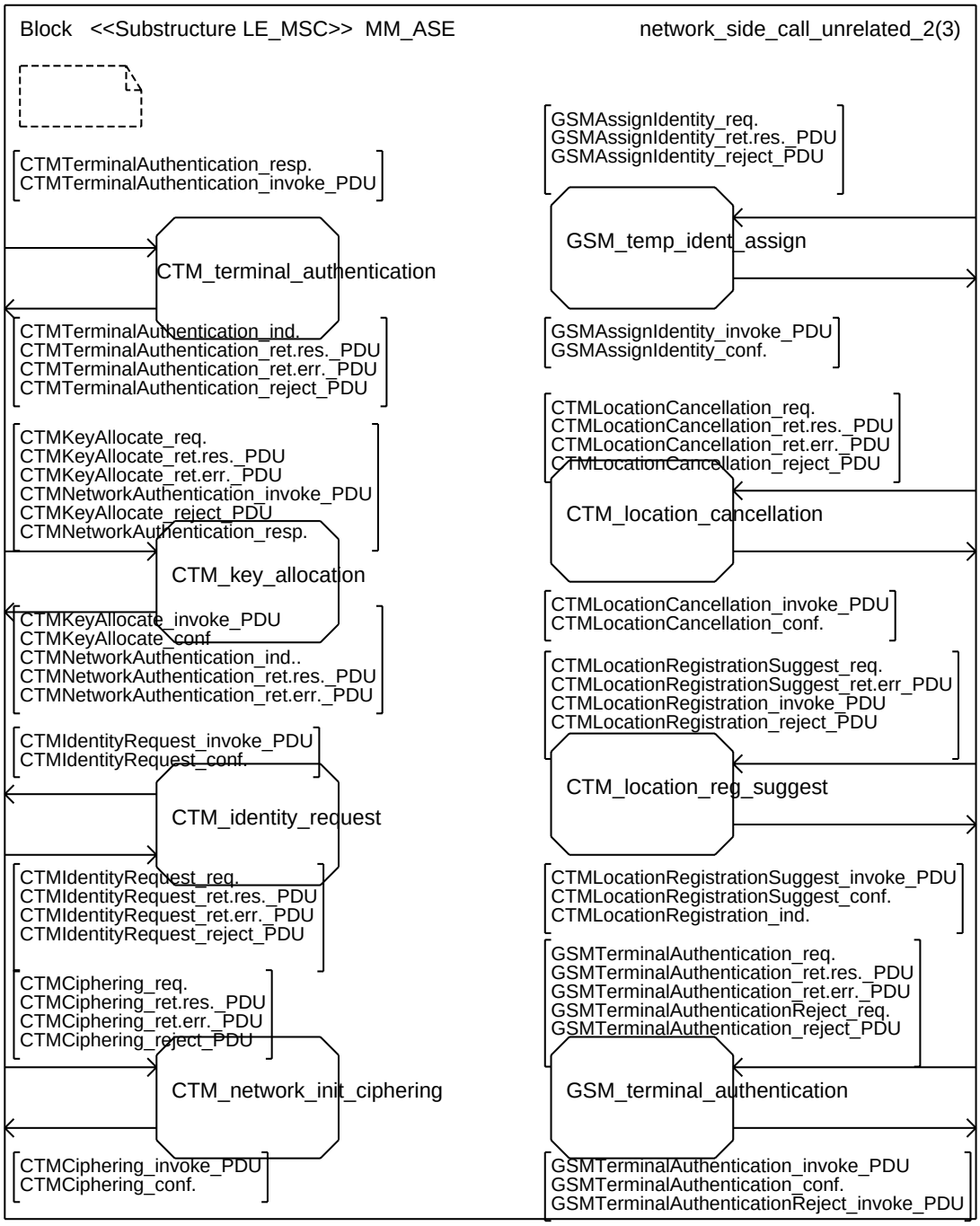


Figure F.5: Network side call unrelated (2 of 3)

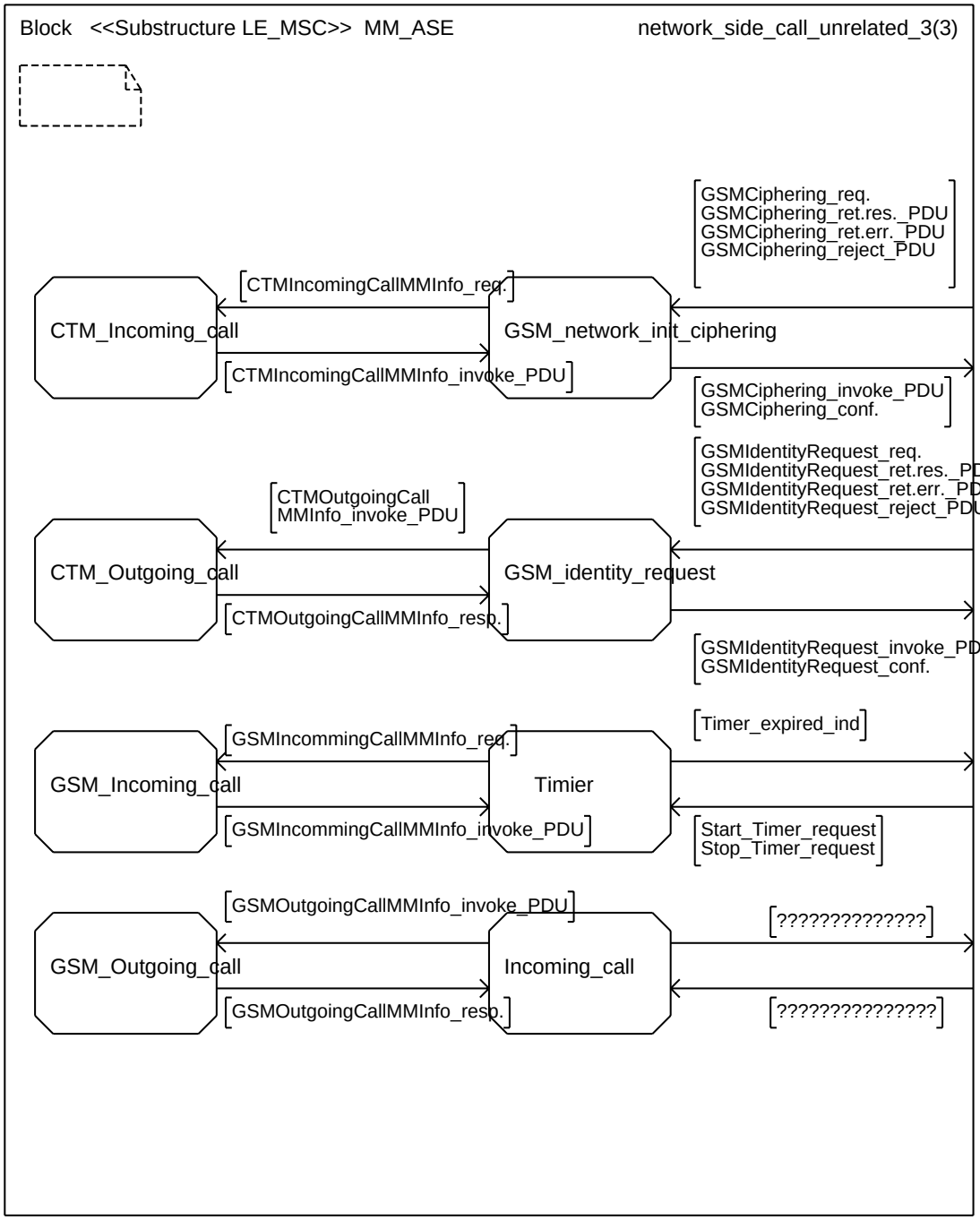


Figure F.6: Network side call unrelated (3 of 3)

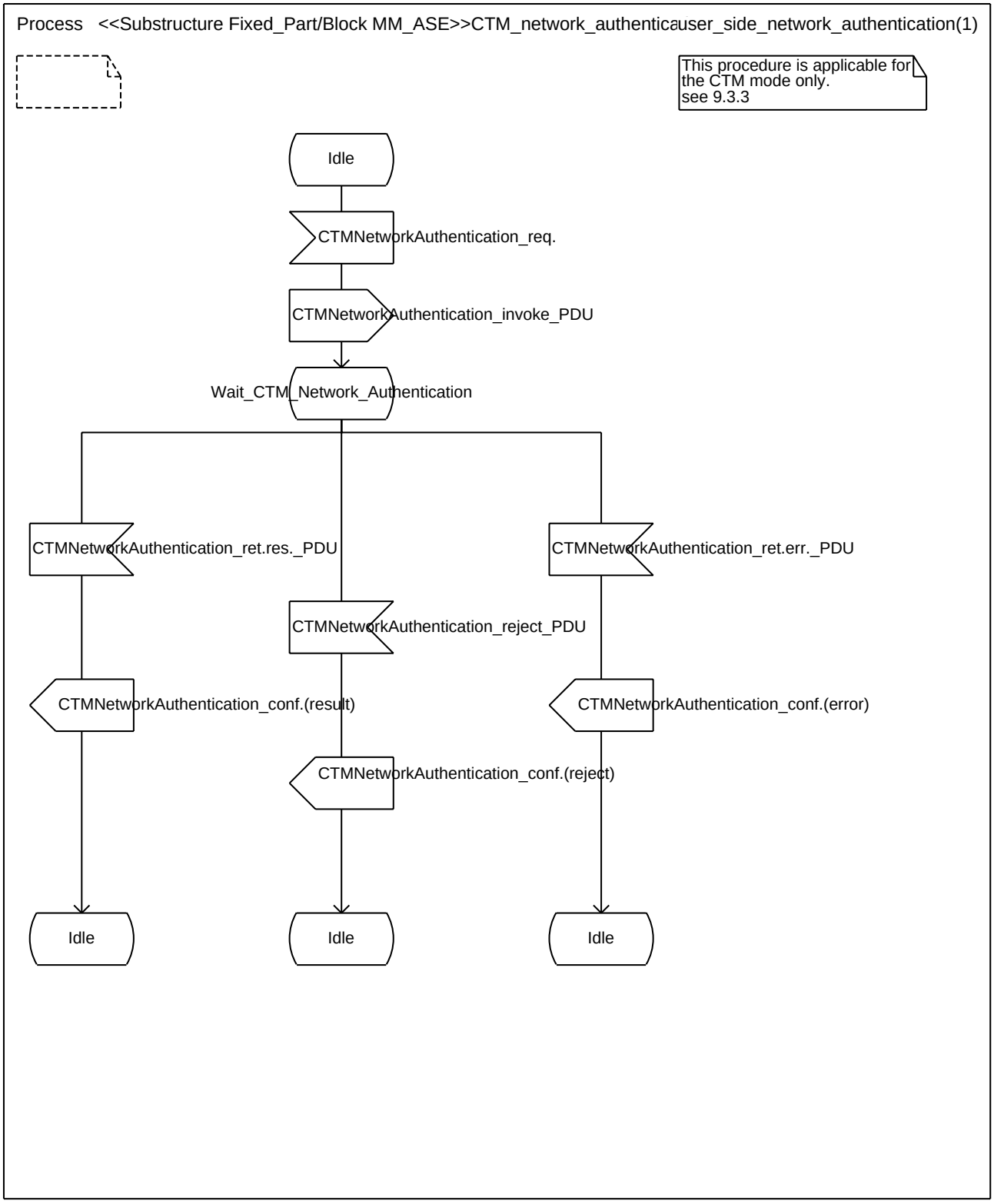


Figure F.7: User side network authentication

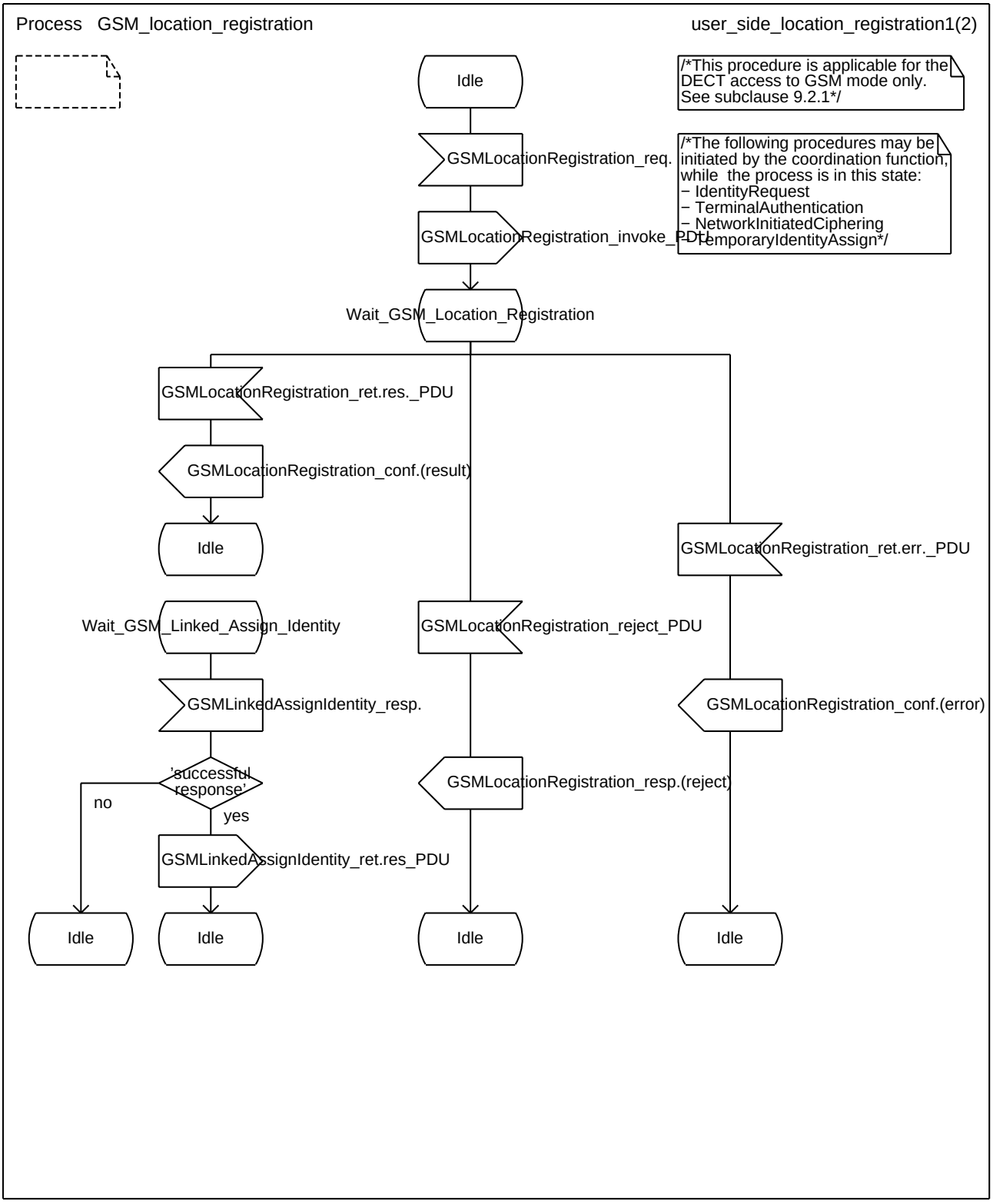


Figure F.8: User side location registration (GSM) (1 of 2)

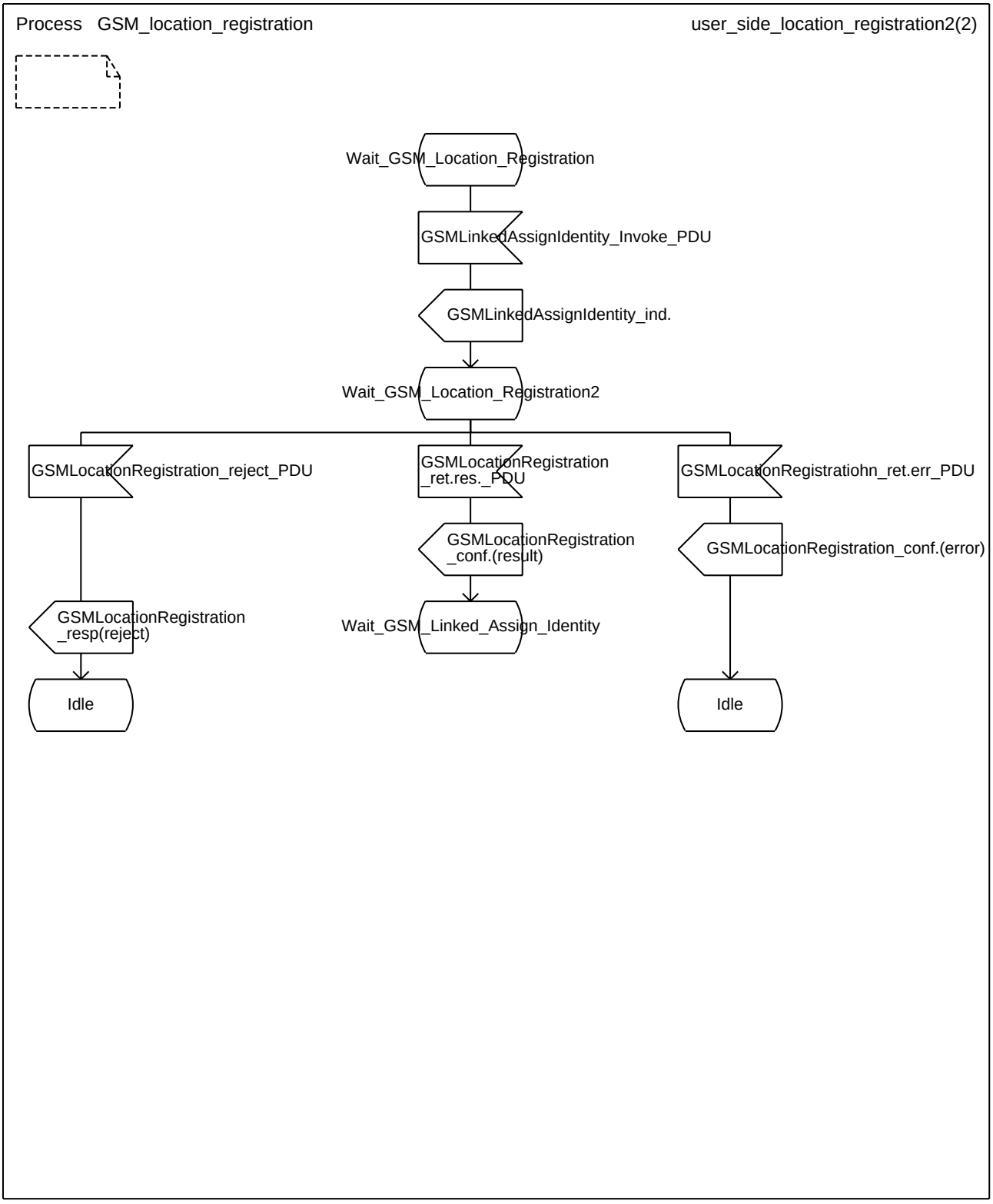


Figure F.9: User side location registration (GSM) (2 of 2)

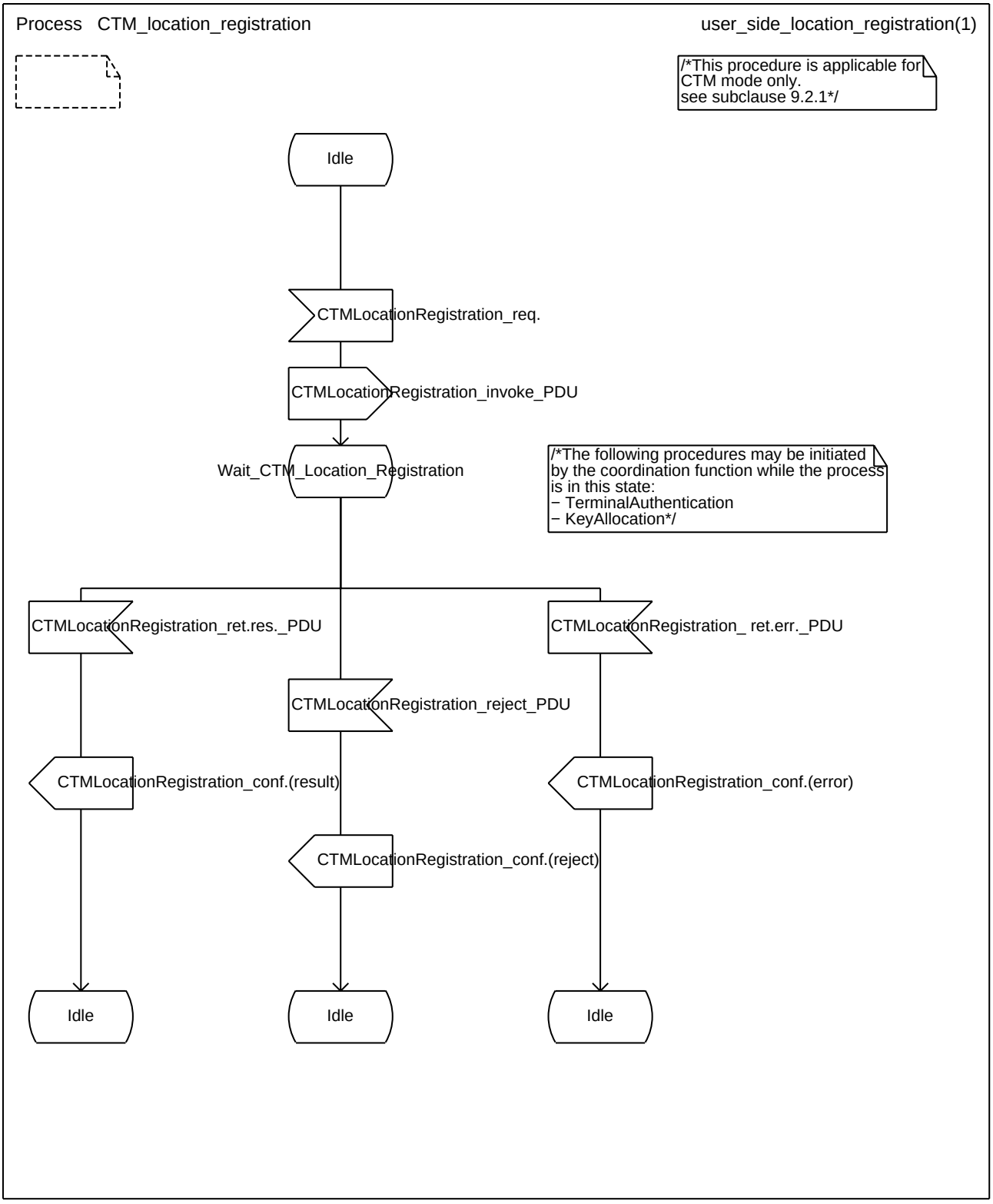


Figure F.10: User side location registration (CTM)

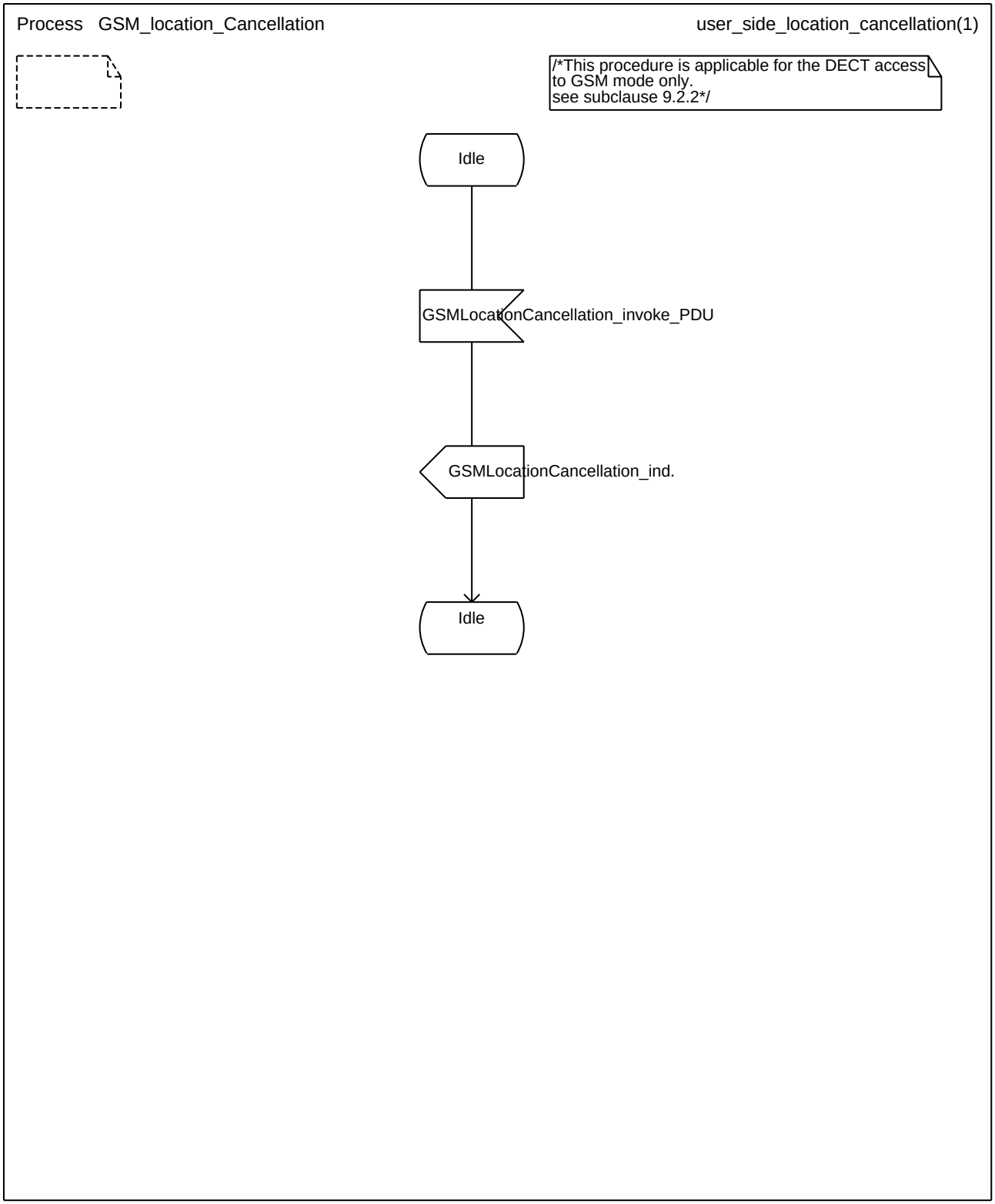


Figure F.11: User side location cancellation

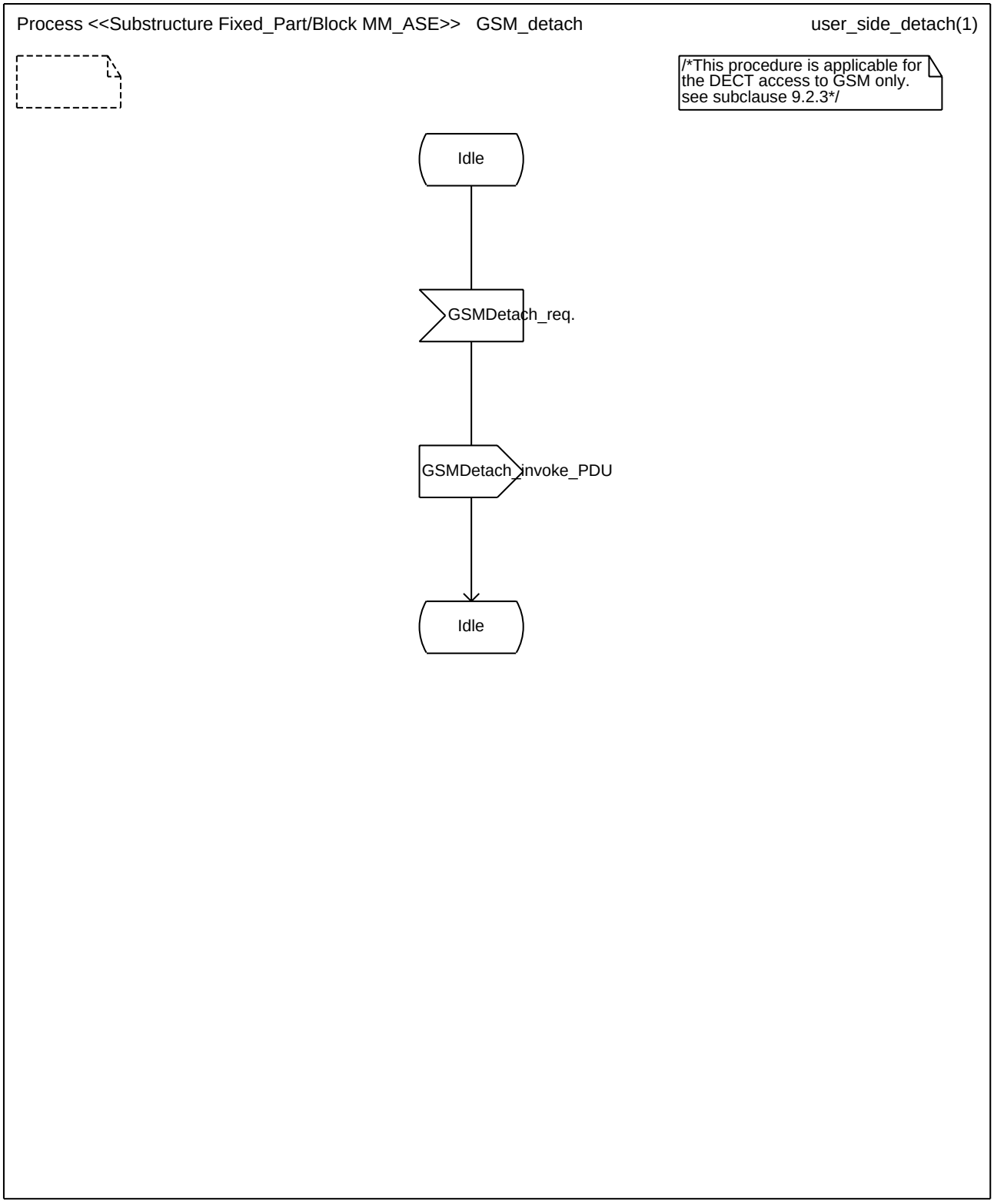


Figure F.12: User side detach

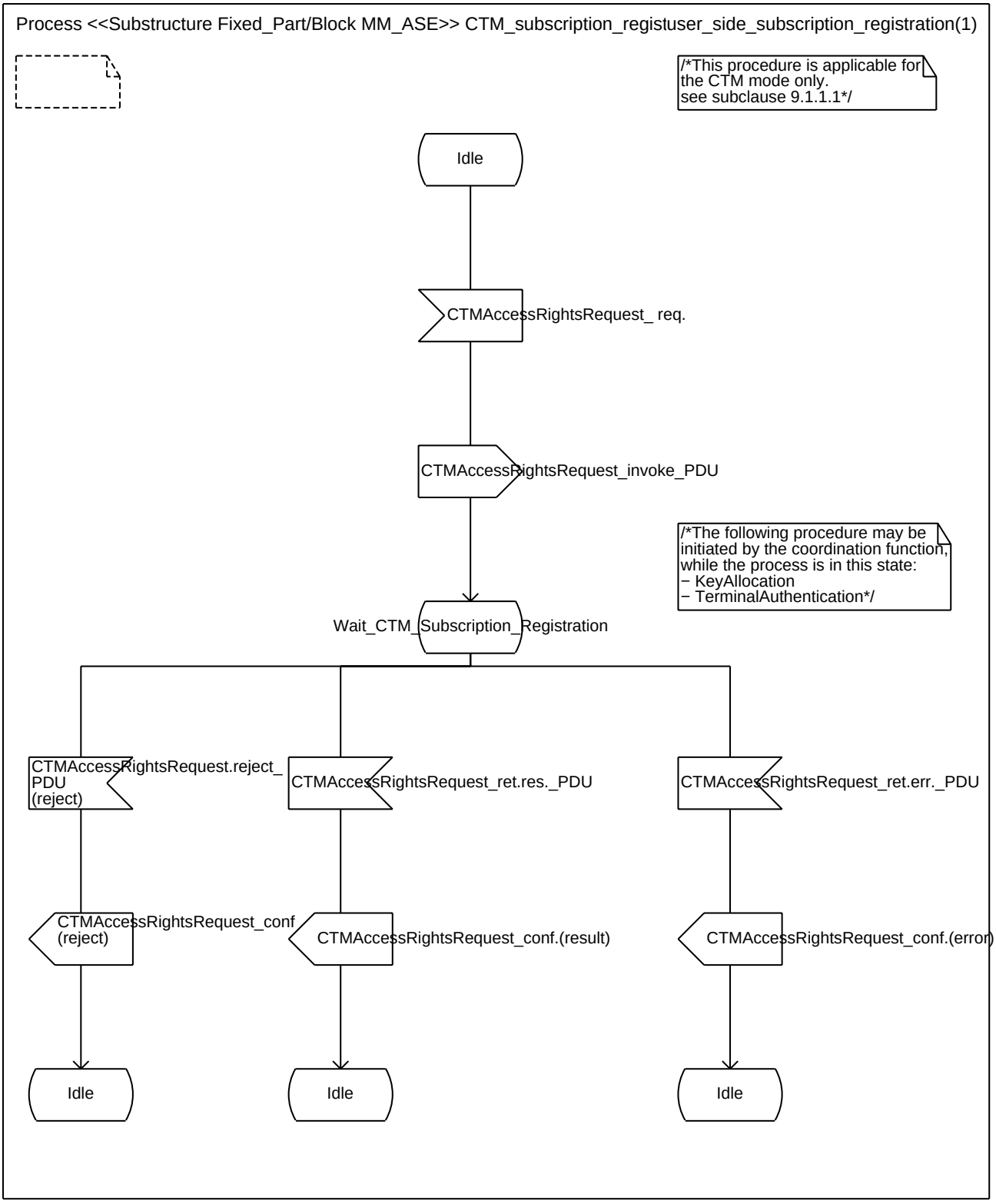


Figure F.13: User side subscription registration

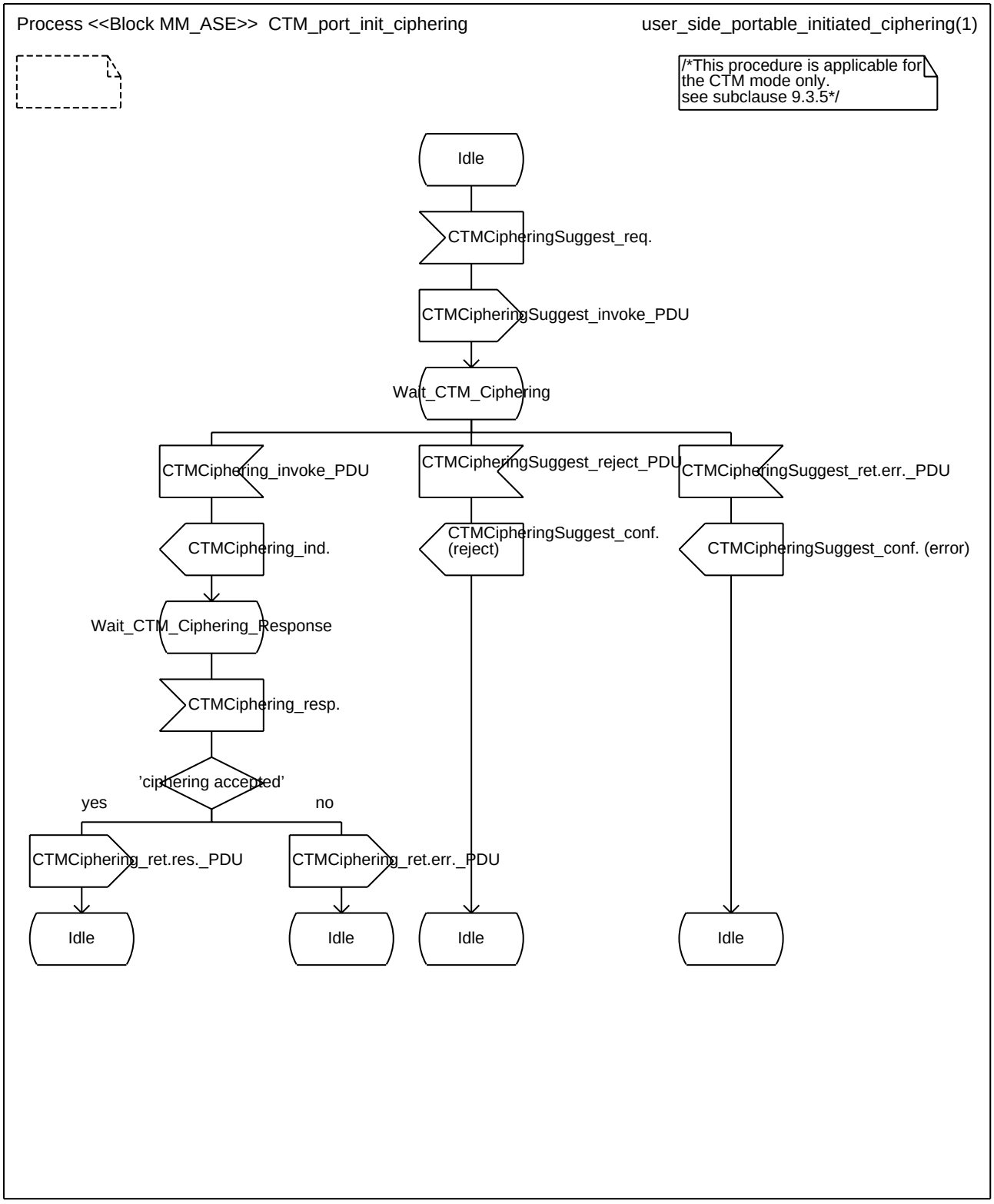


Figure F.14: User side portable initiated ciphering

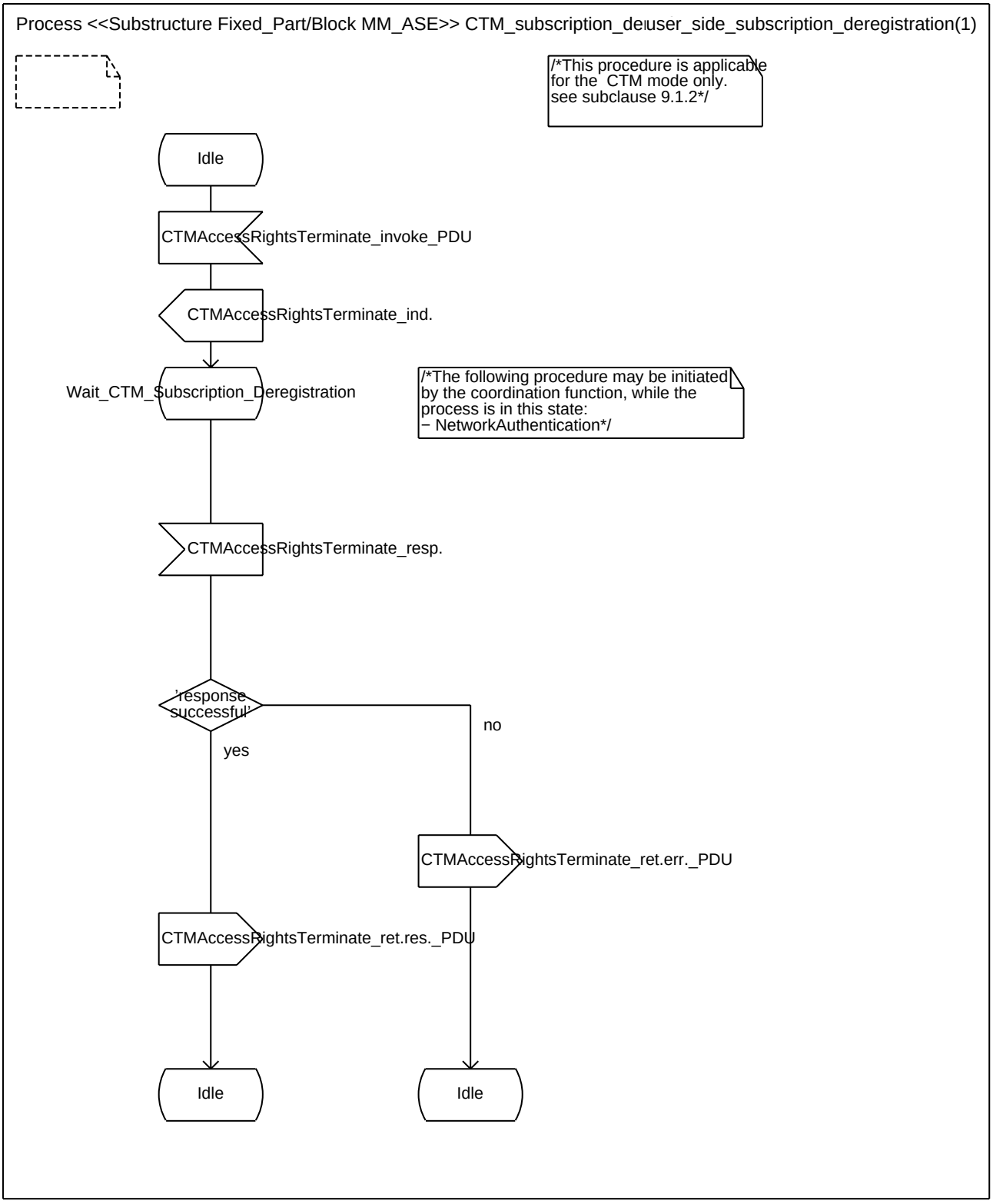


Figure F.15: User side subscription deregistration

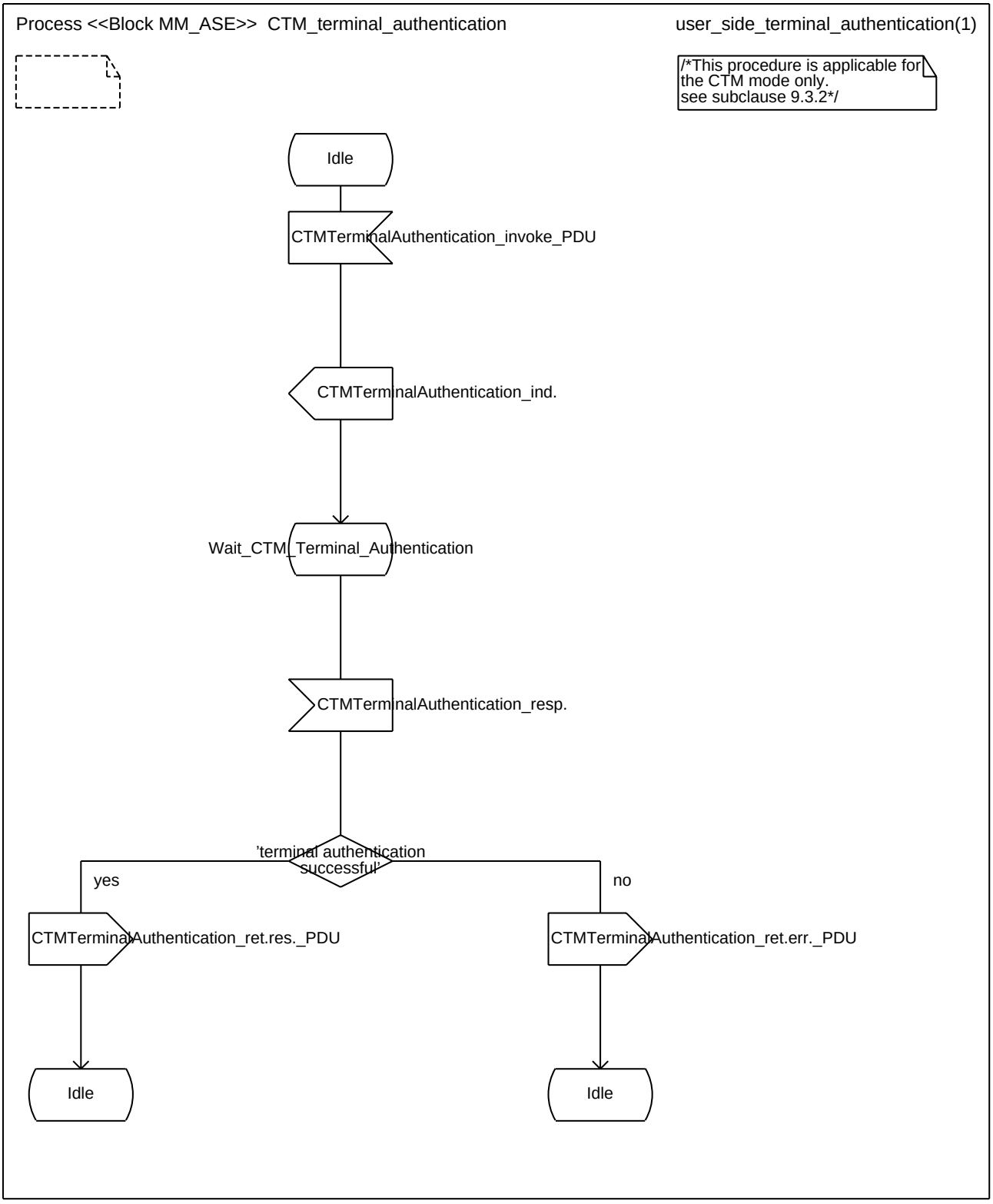


Figure F.16: User side terminal authentication

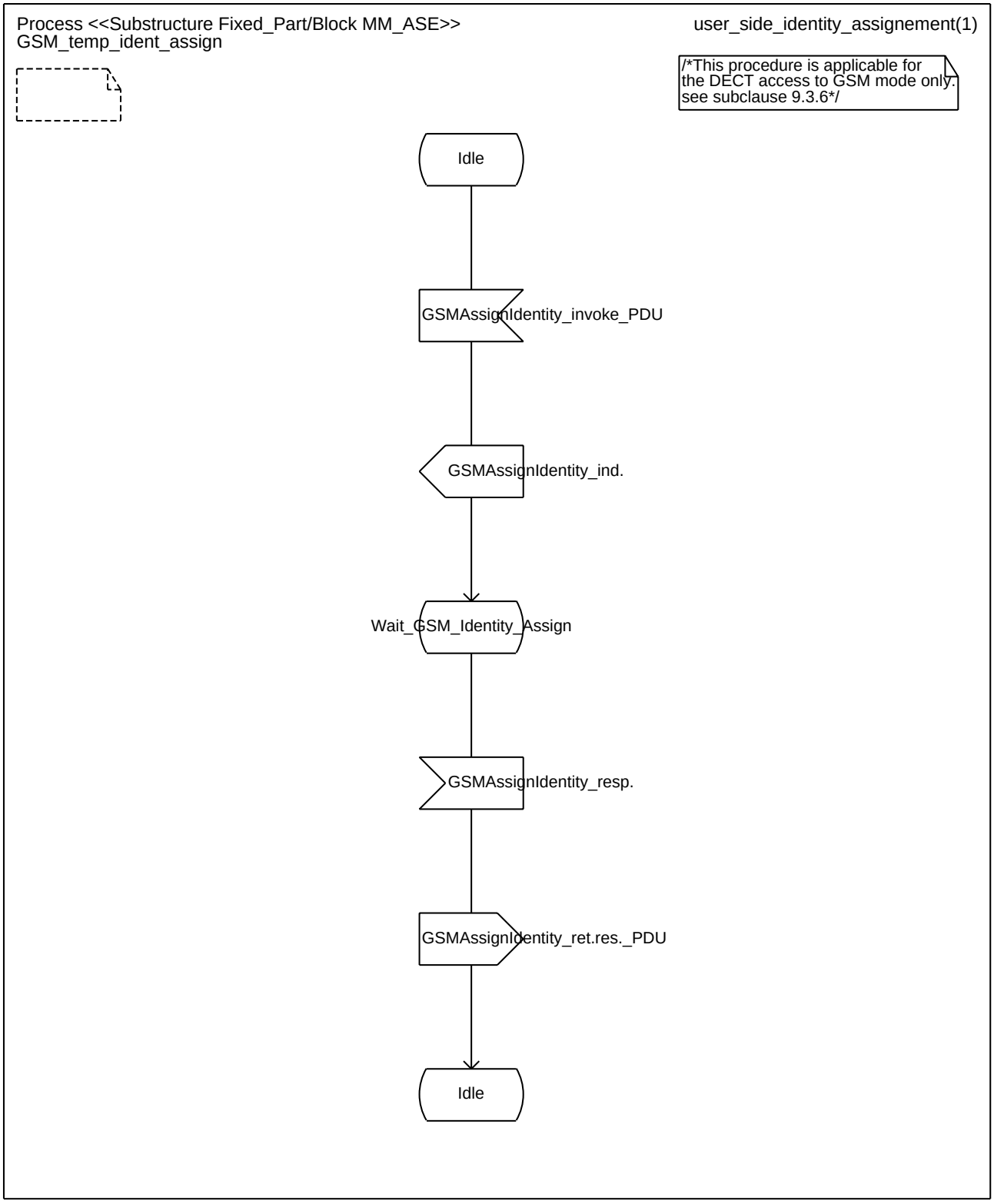


Figure F.17: User side identity assignement

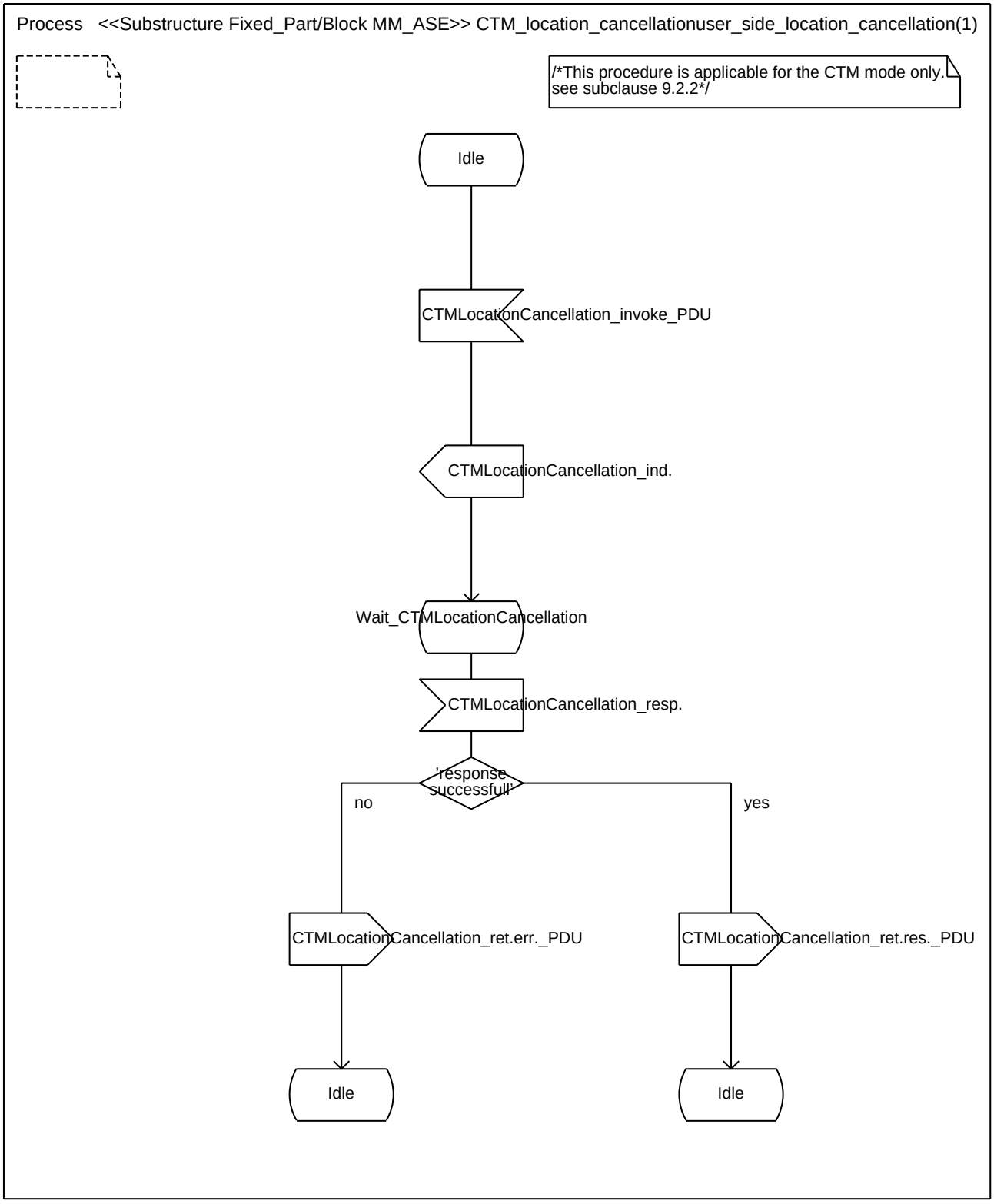


Figure F.18: User side location cancellation

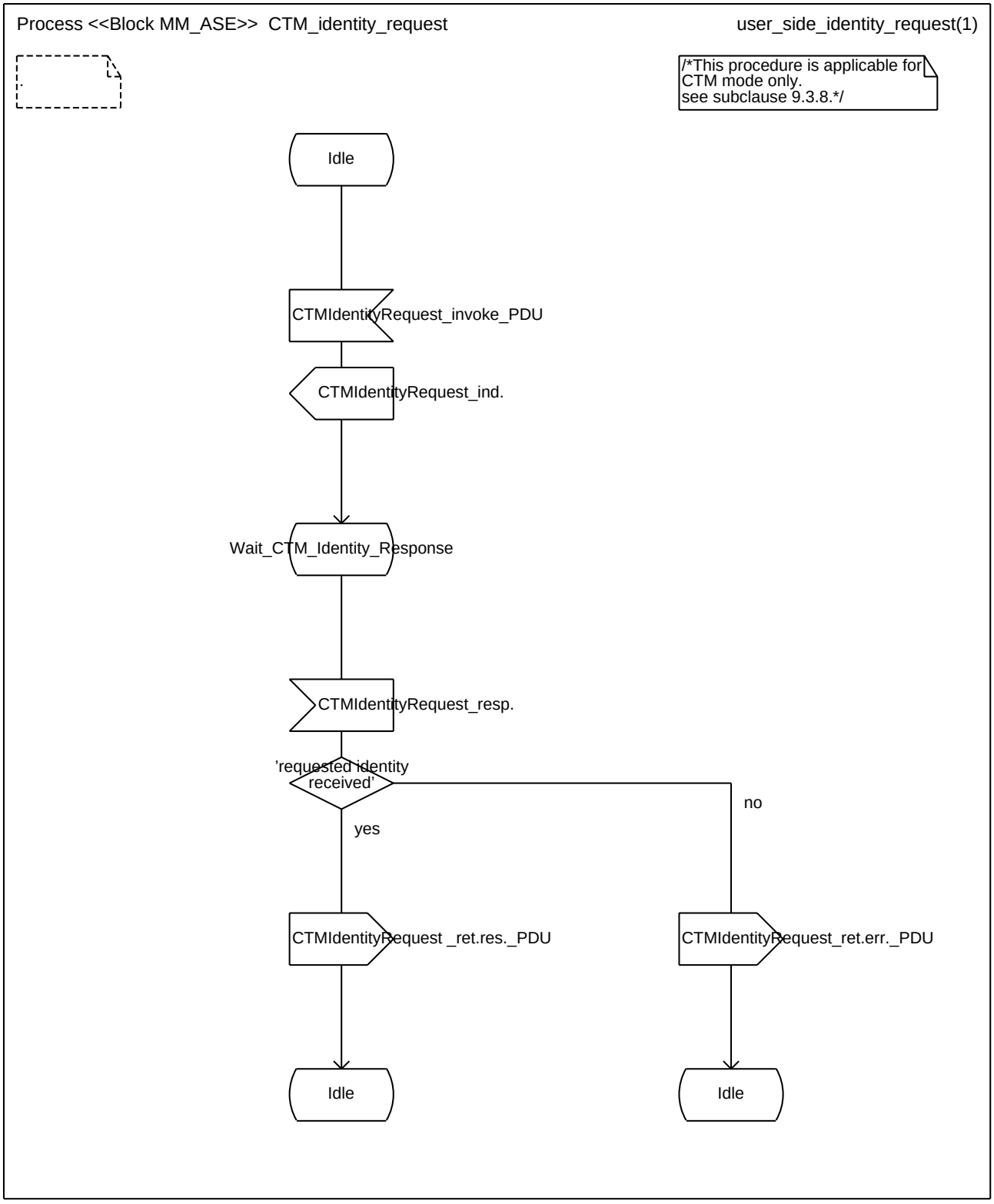


Figure F.19: User side identity request

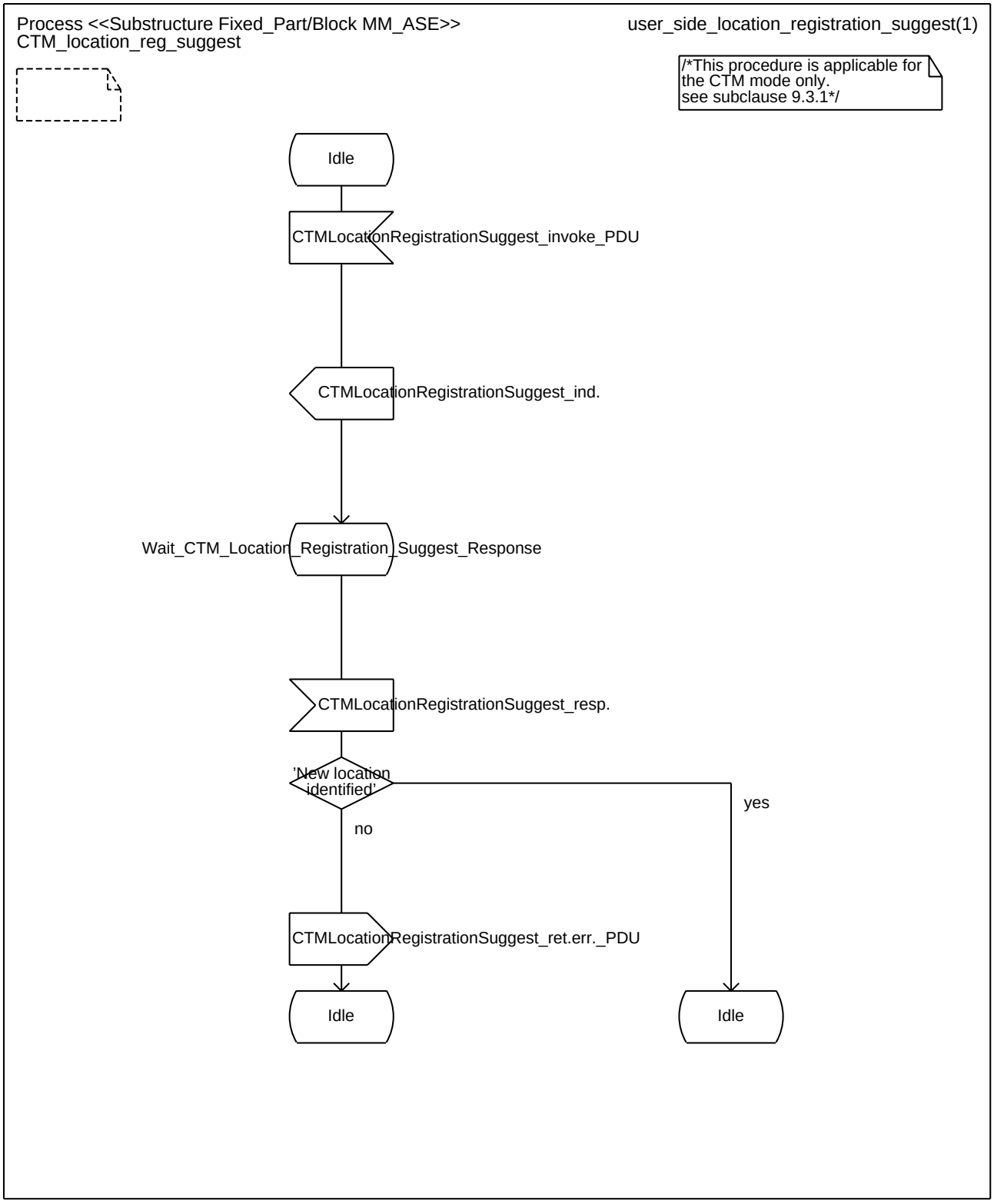


Figure F.20: User side location registration suggest

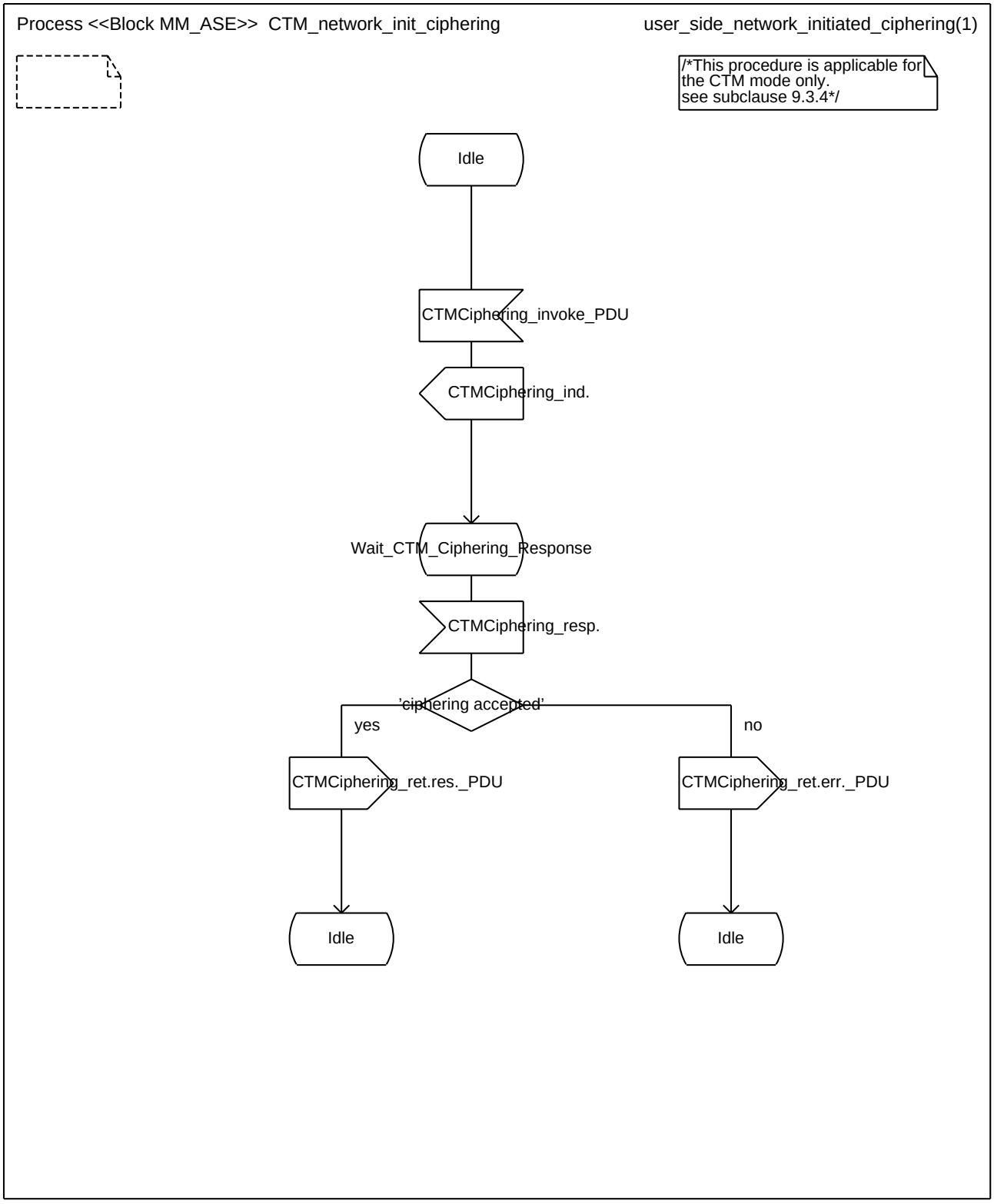


Figure F.21: User side network initiated ciphering

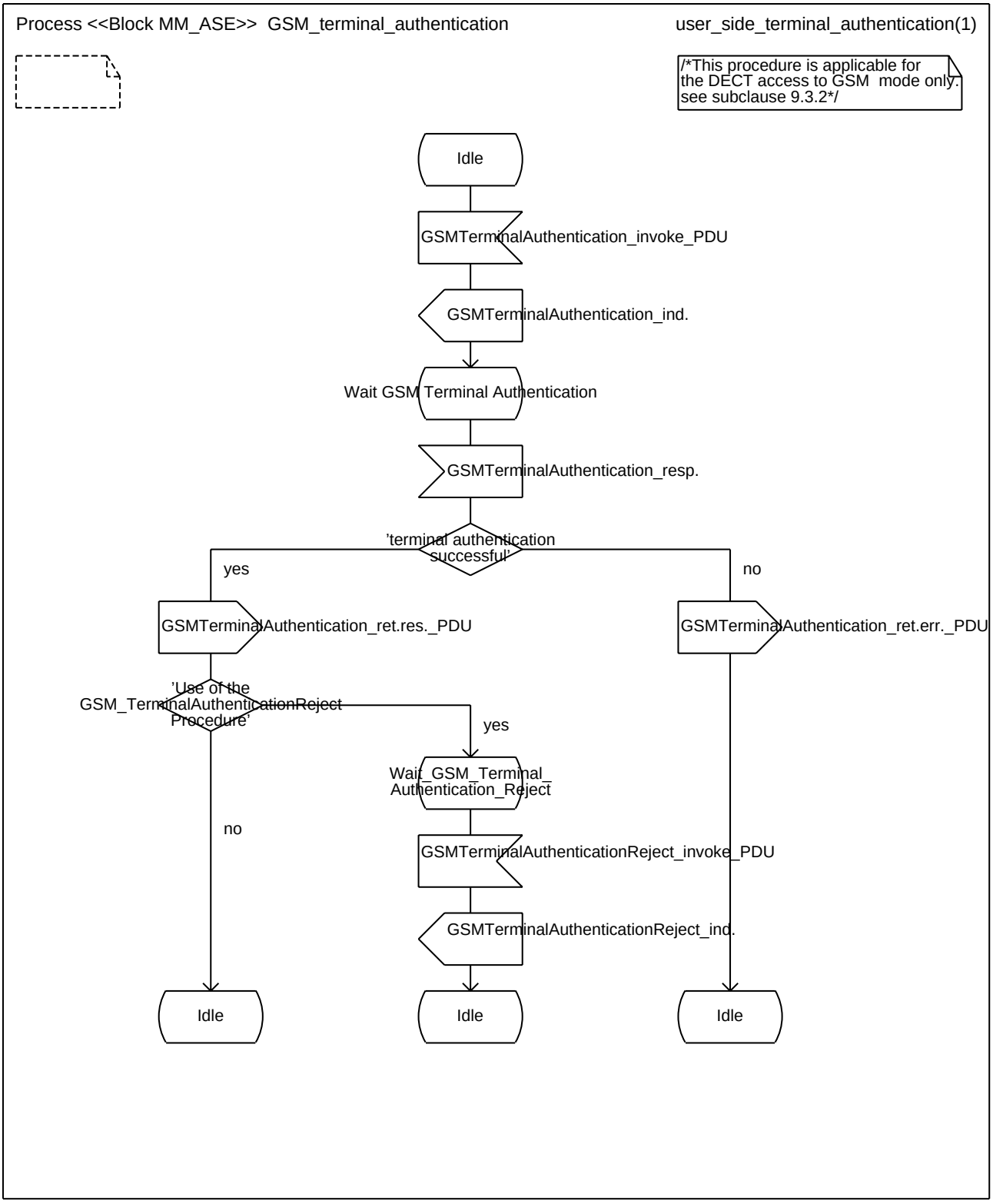


Figure F.22: User side terminal authentication

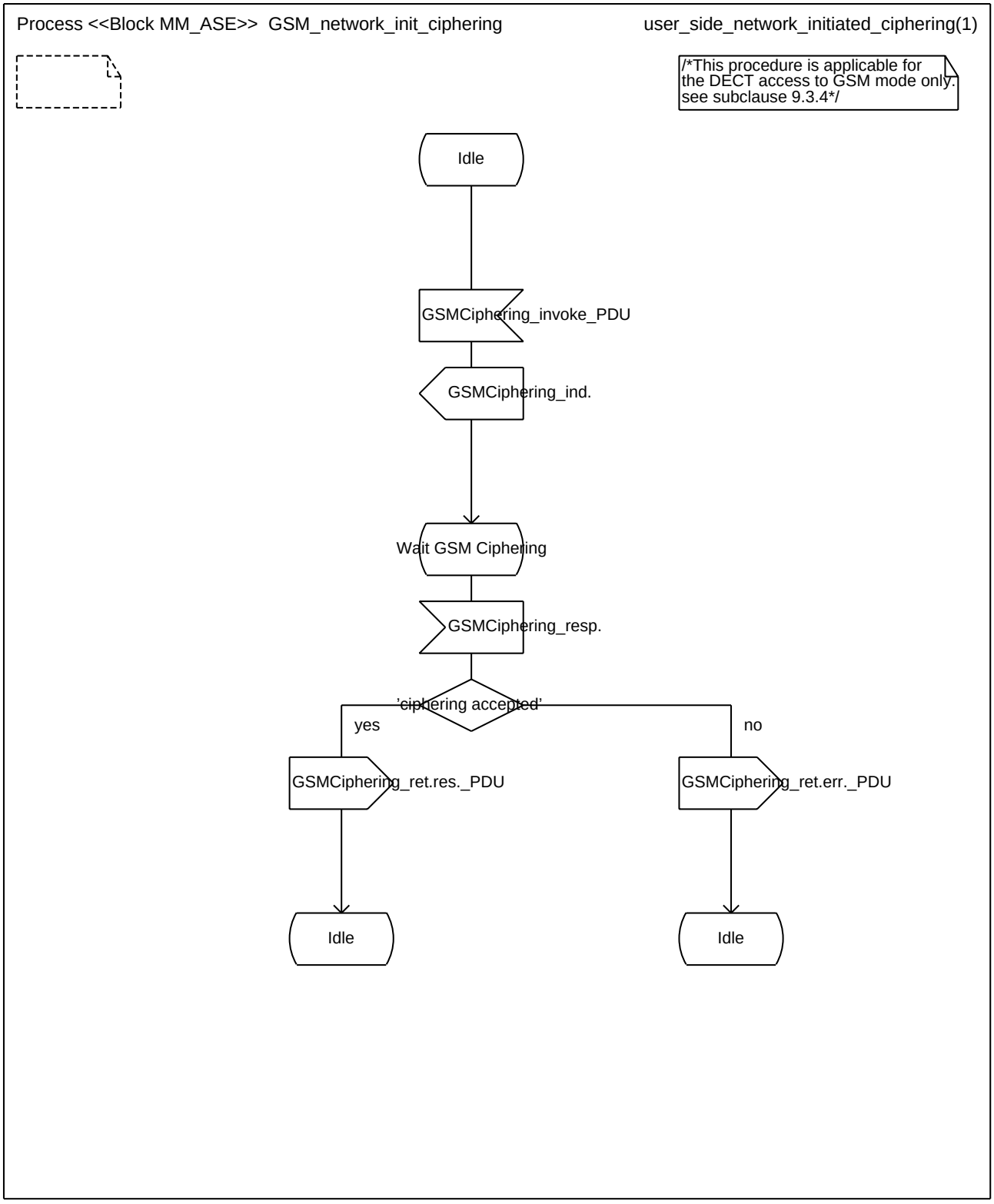


Figure F.23: User side network initiated ciphering

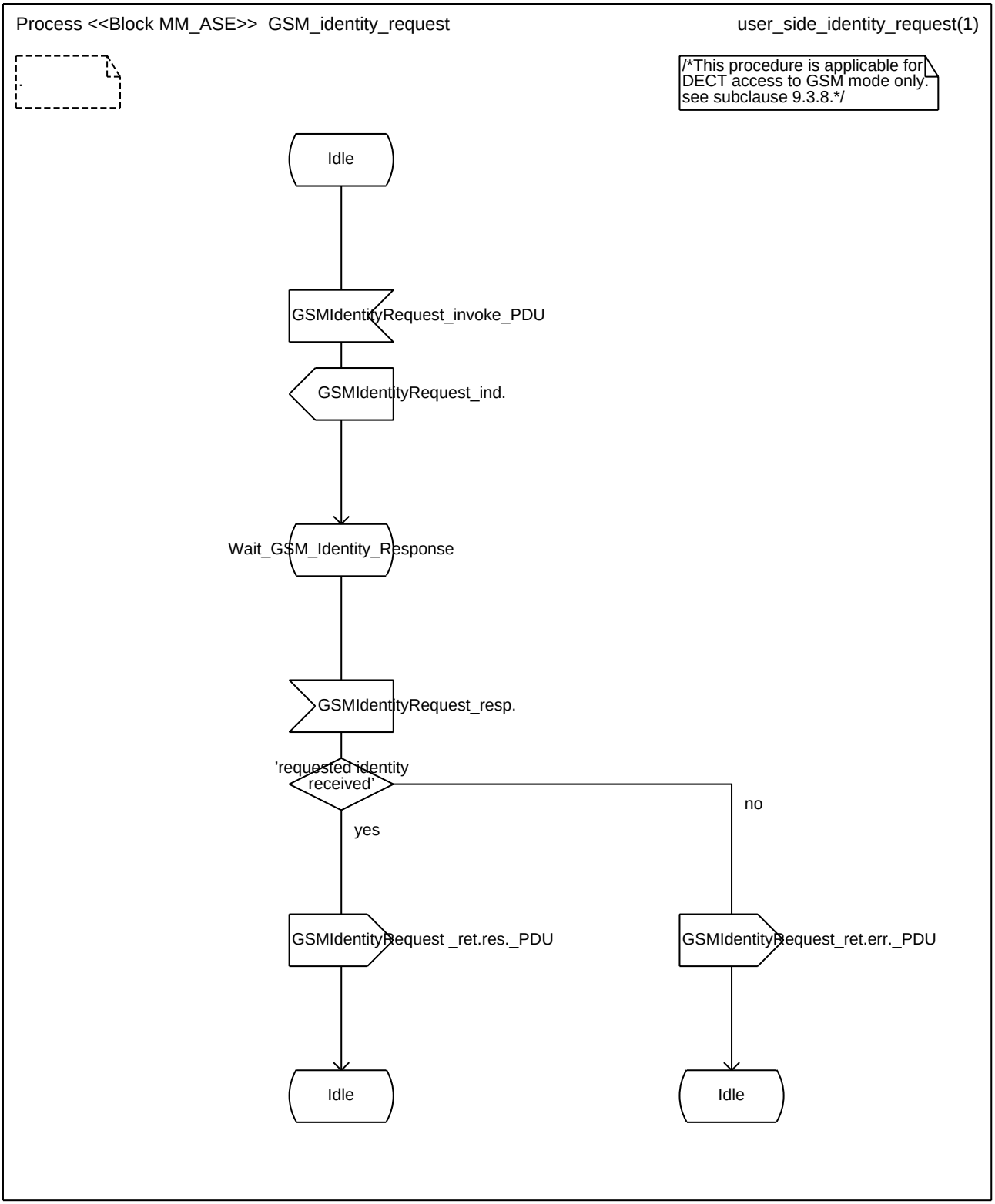


Figure F.24: User side identity request

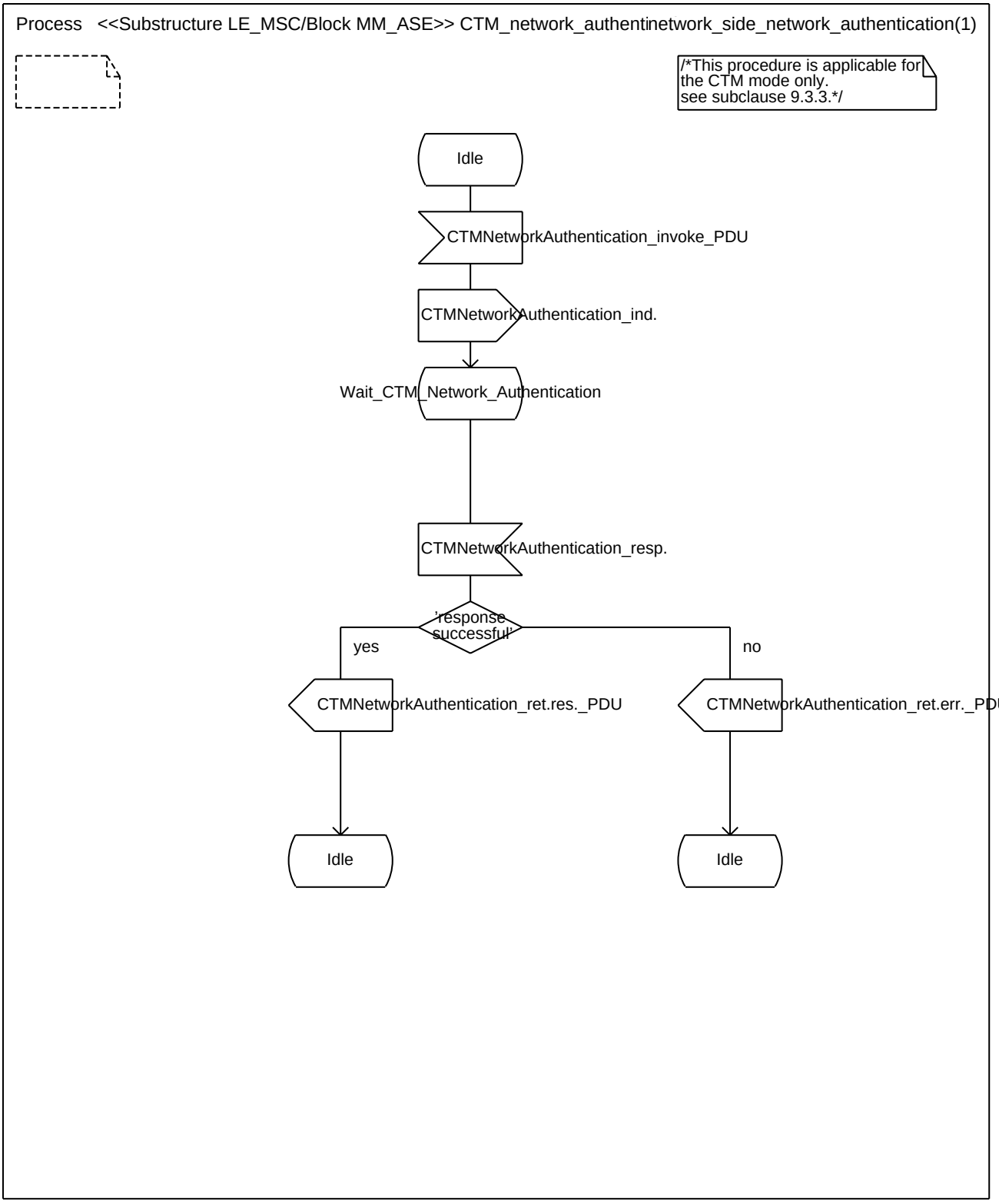


Figure F.25:Network side network authentication

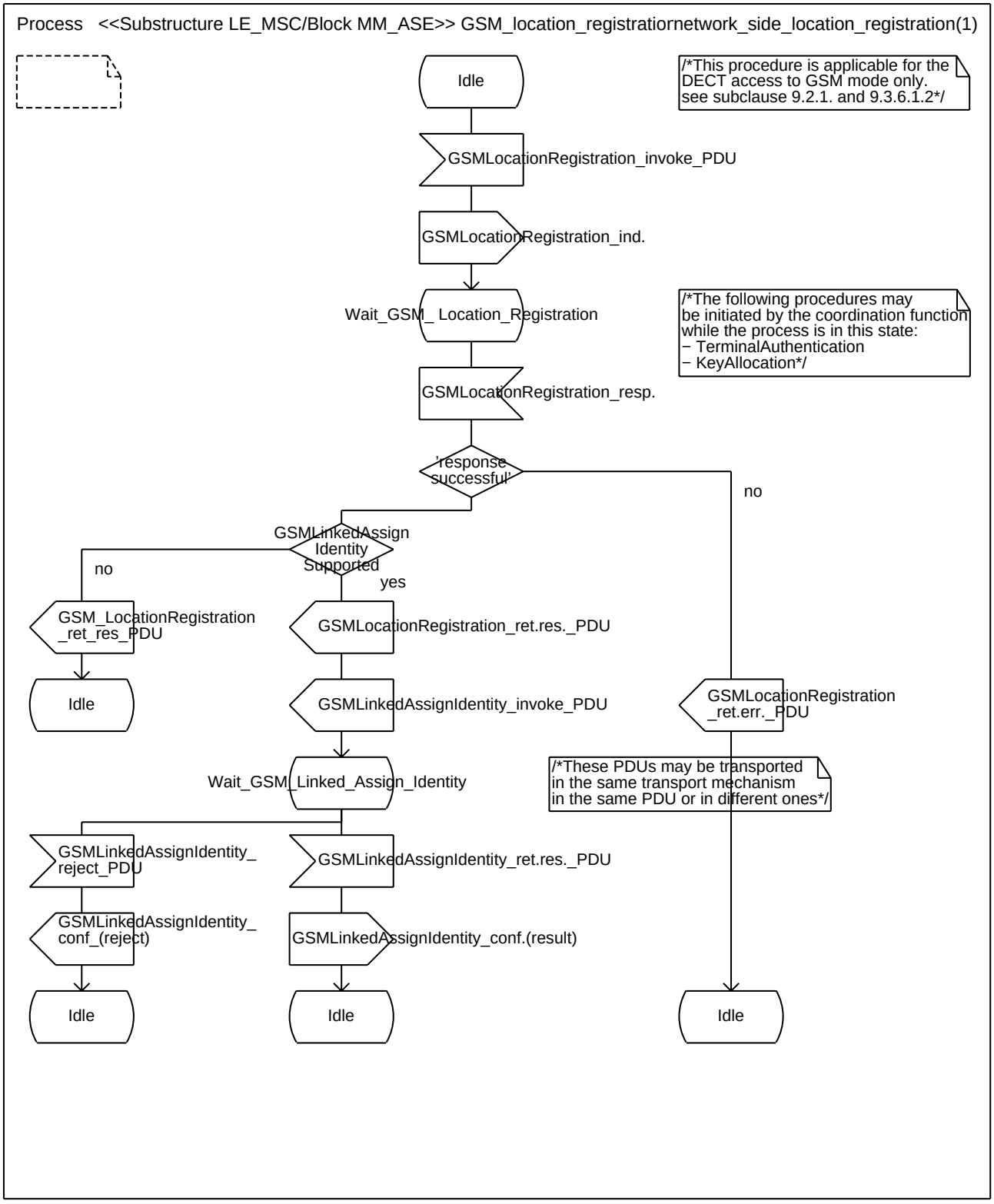


Figure F.26: Network side location registration

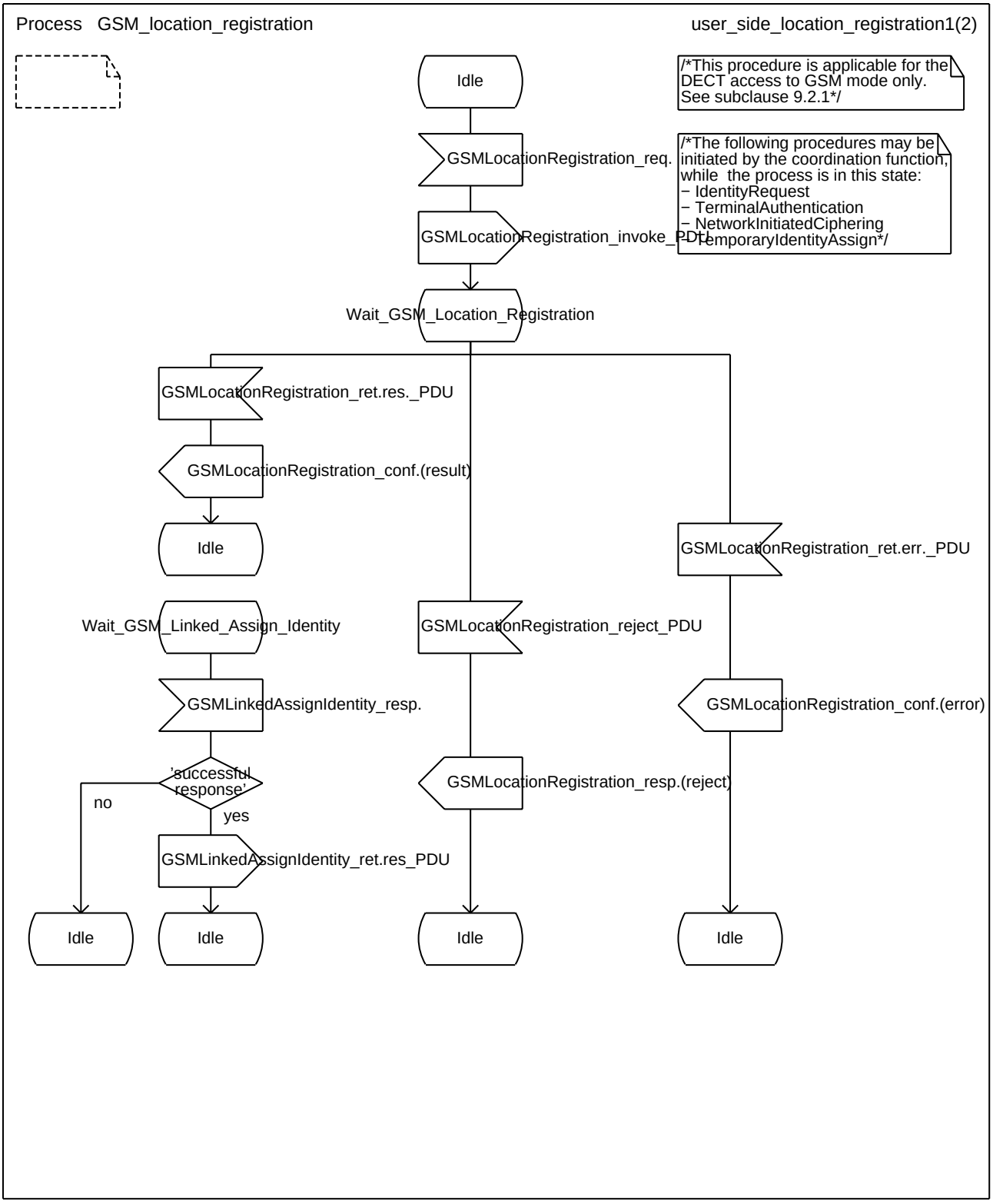


Figure F.27: User side location registration

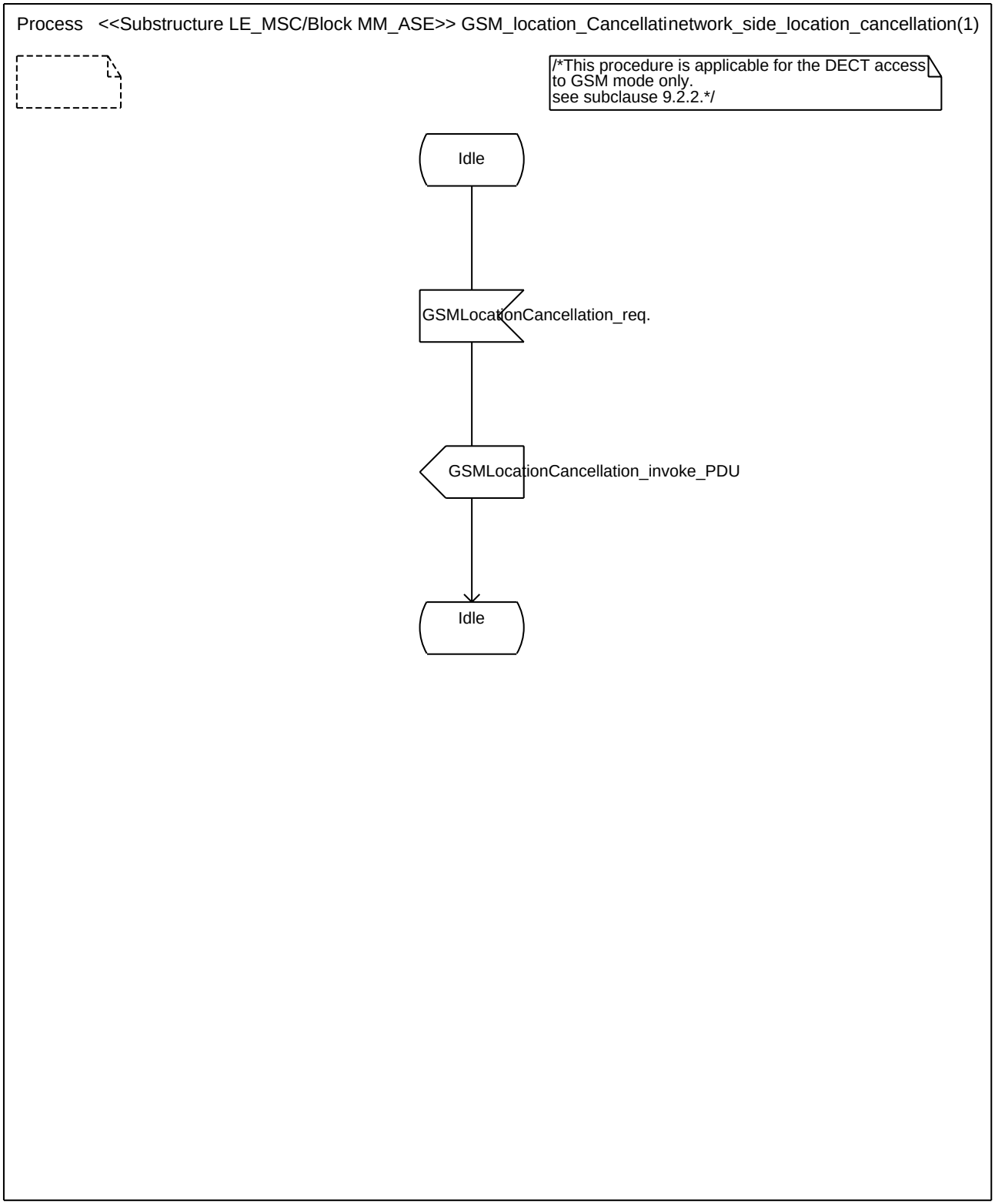


Figure F.28: Network side location cancellation

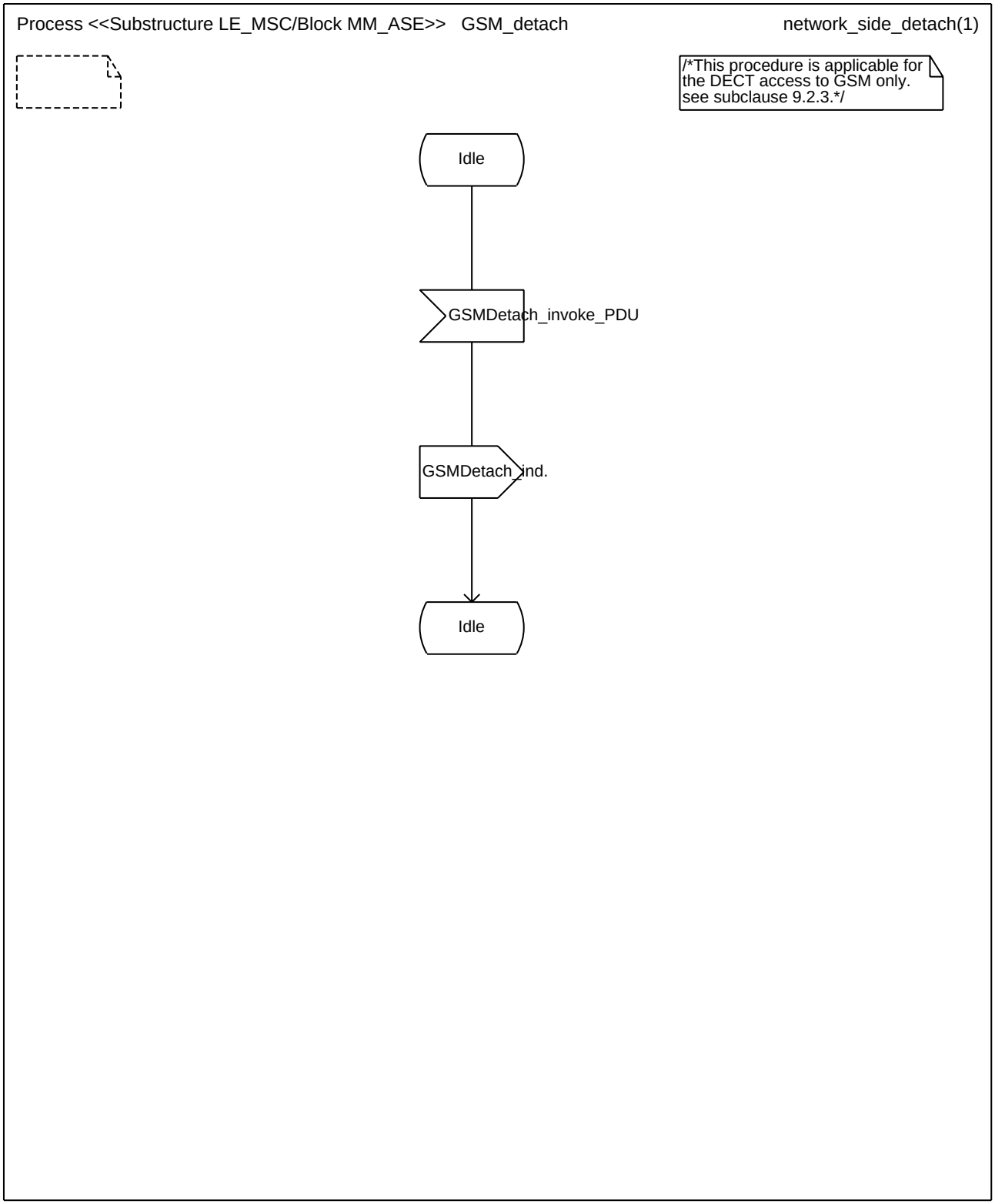


Figure F.29: Network side detach

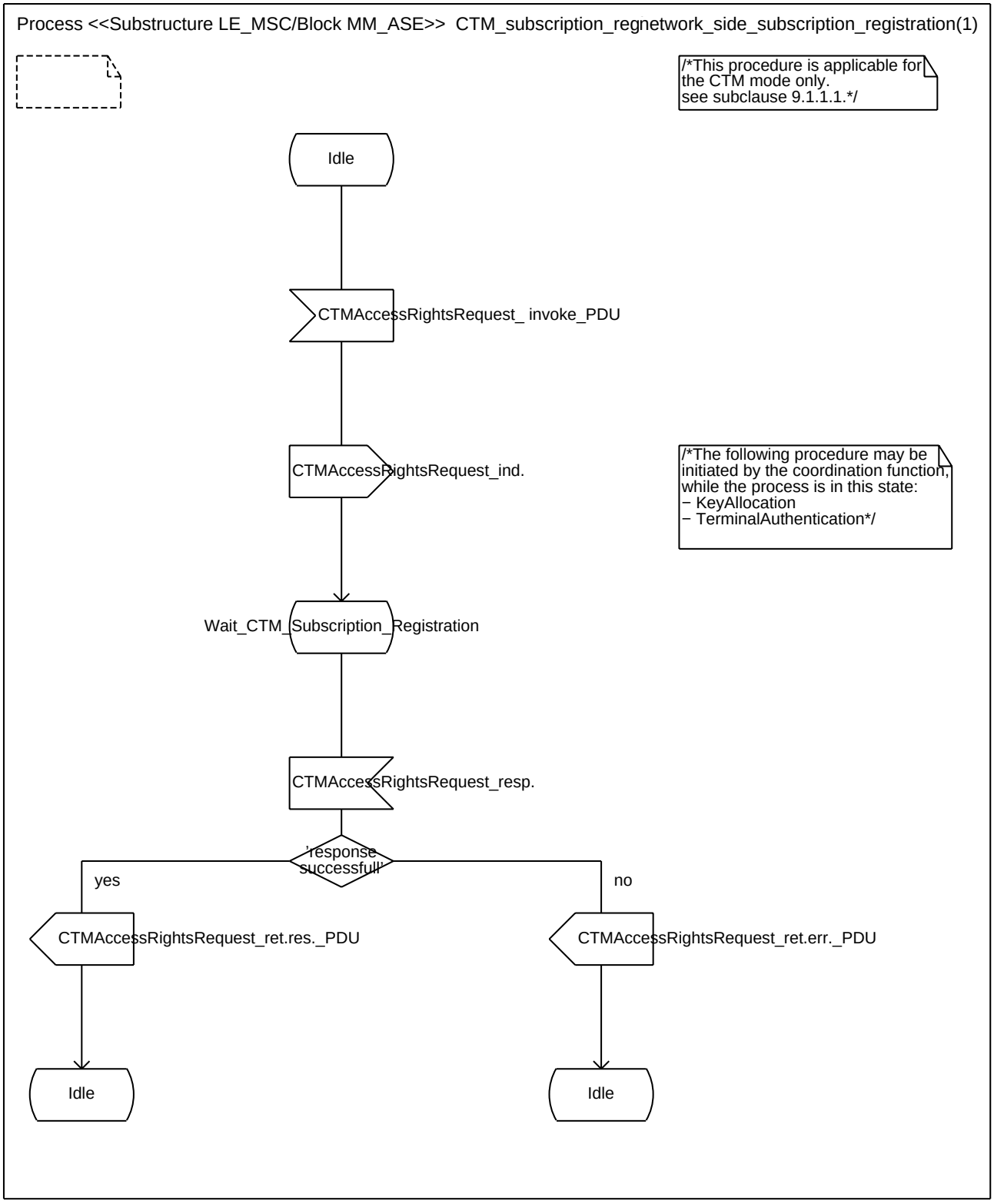


Figure F.30: Network side subscription registration

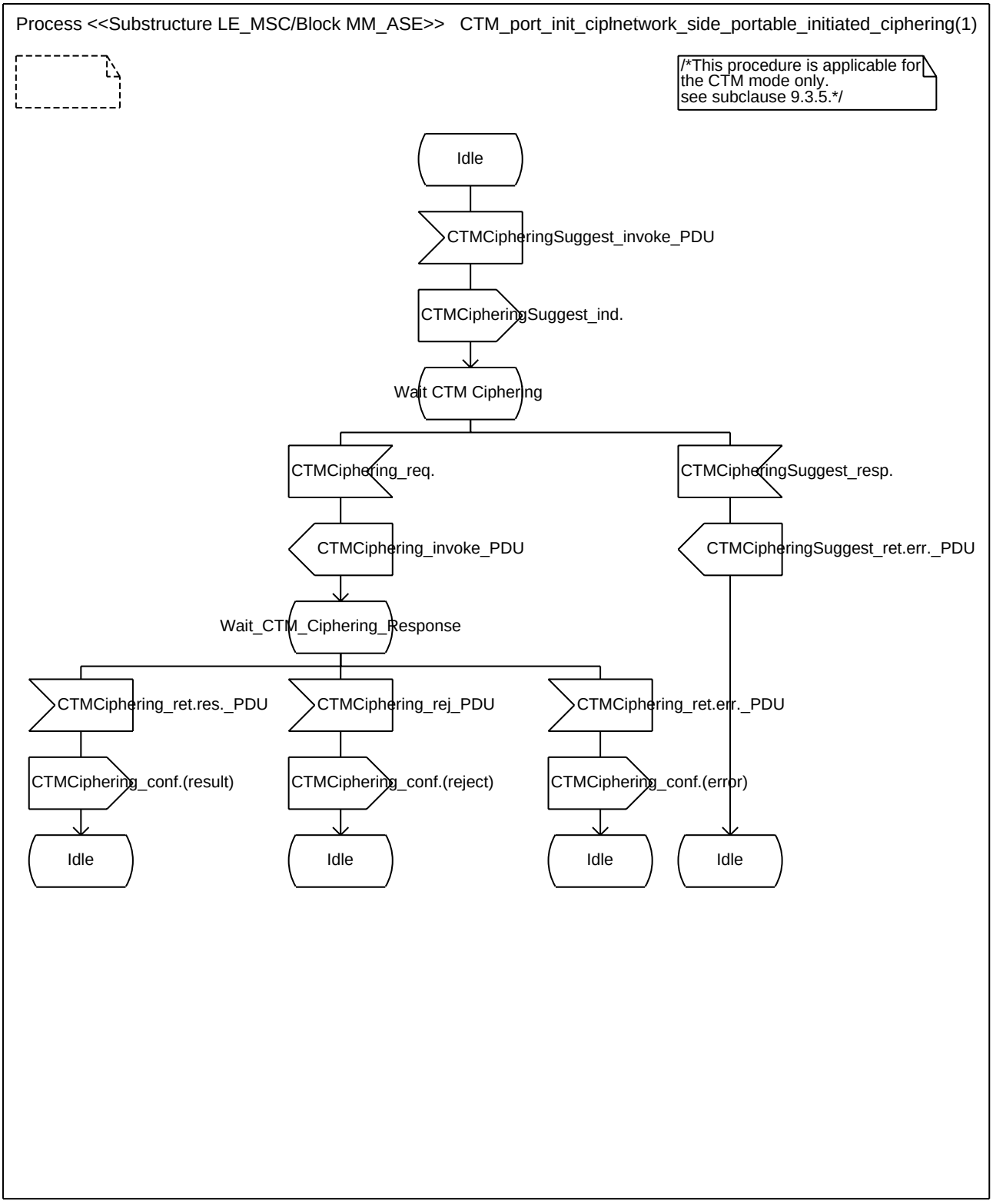


Figure F.31: Network side portable initiated ciphering

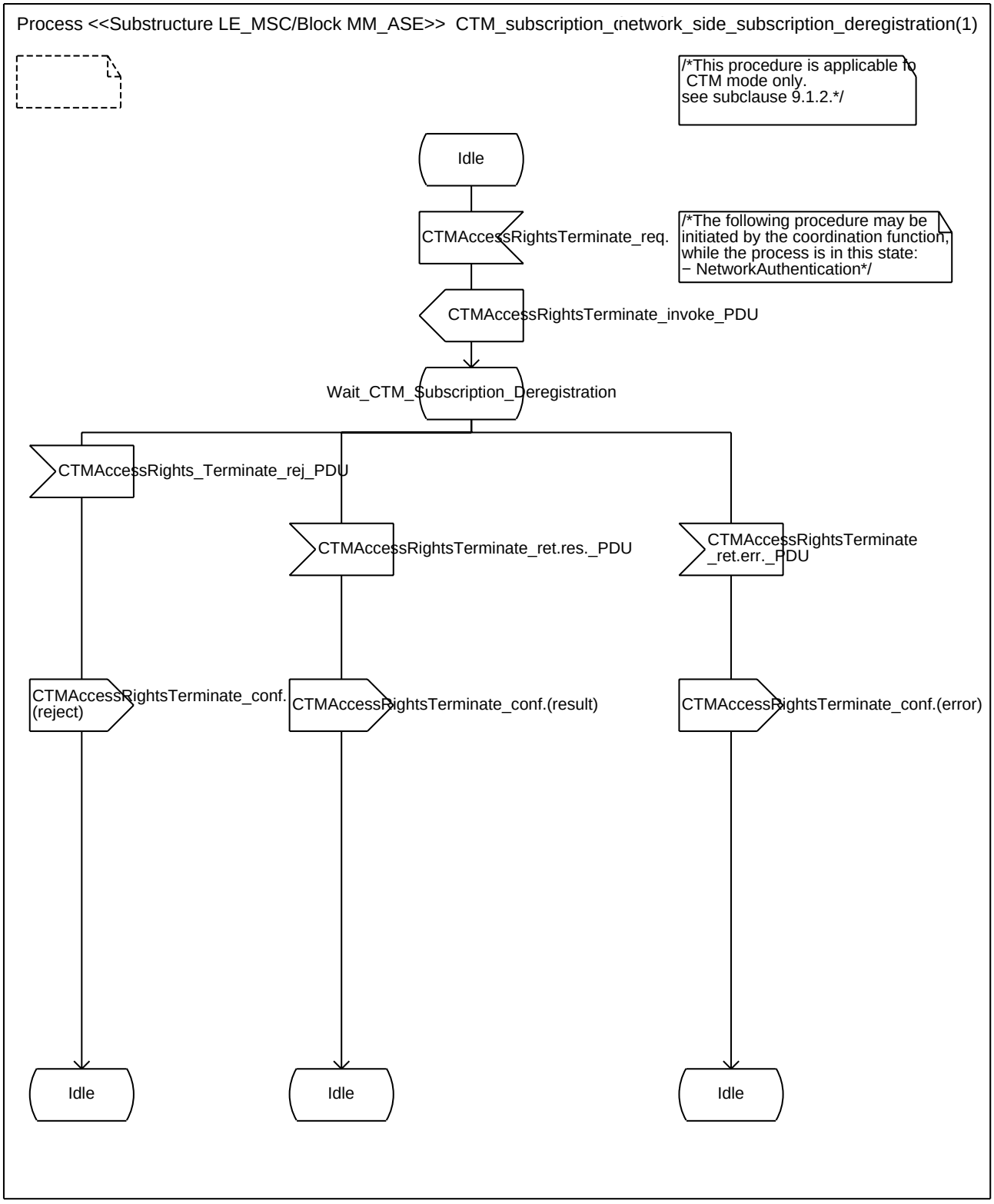


Figure F.32: Network side subscription deregistration

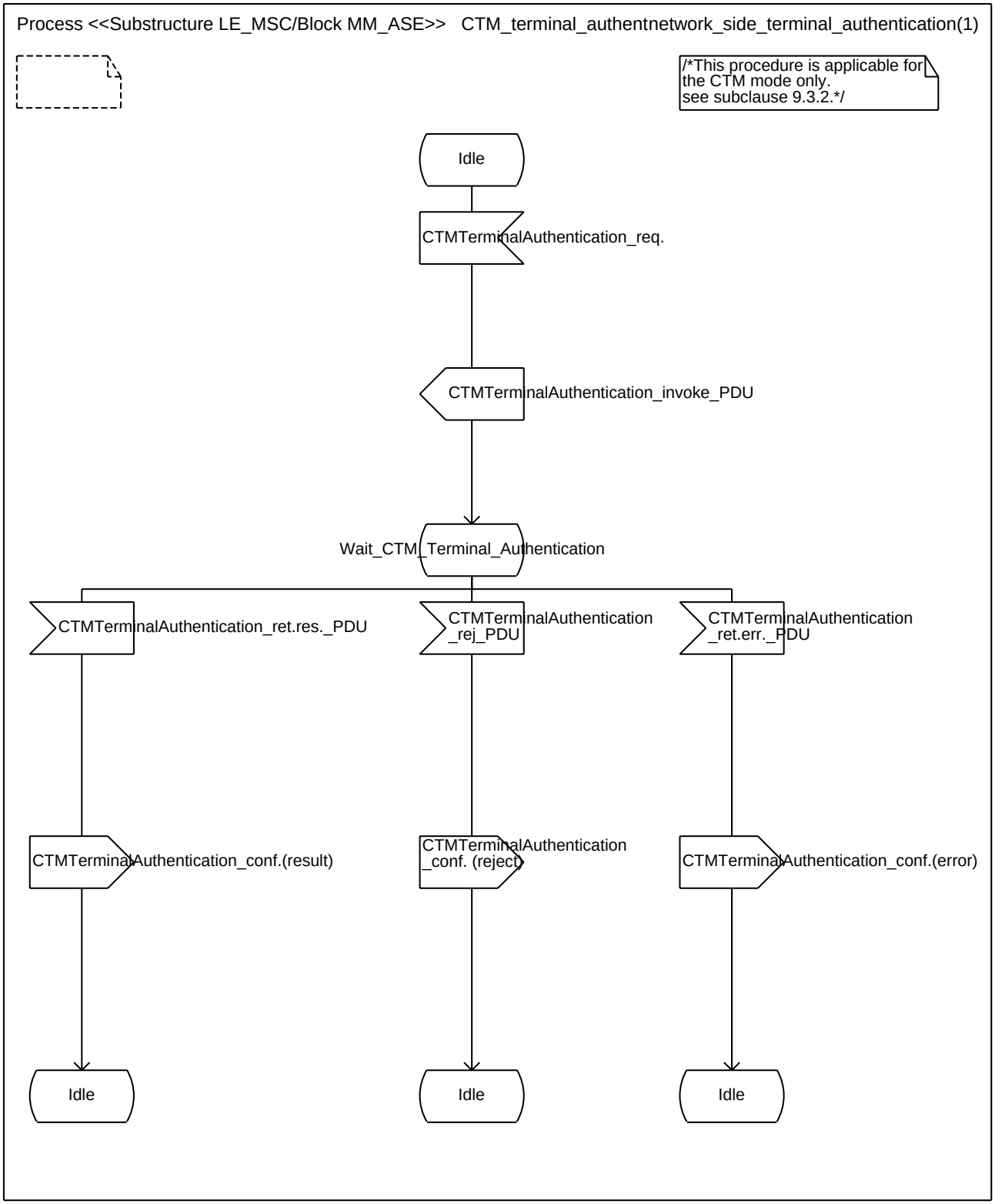


Figure F.33: Network side terminal authentication

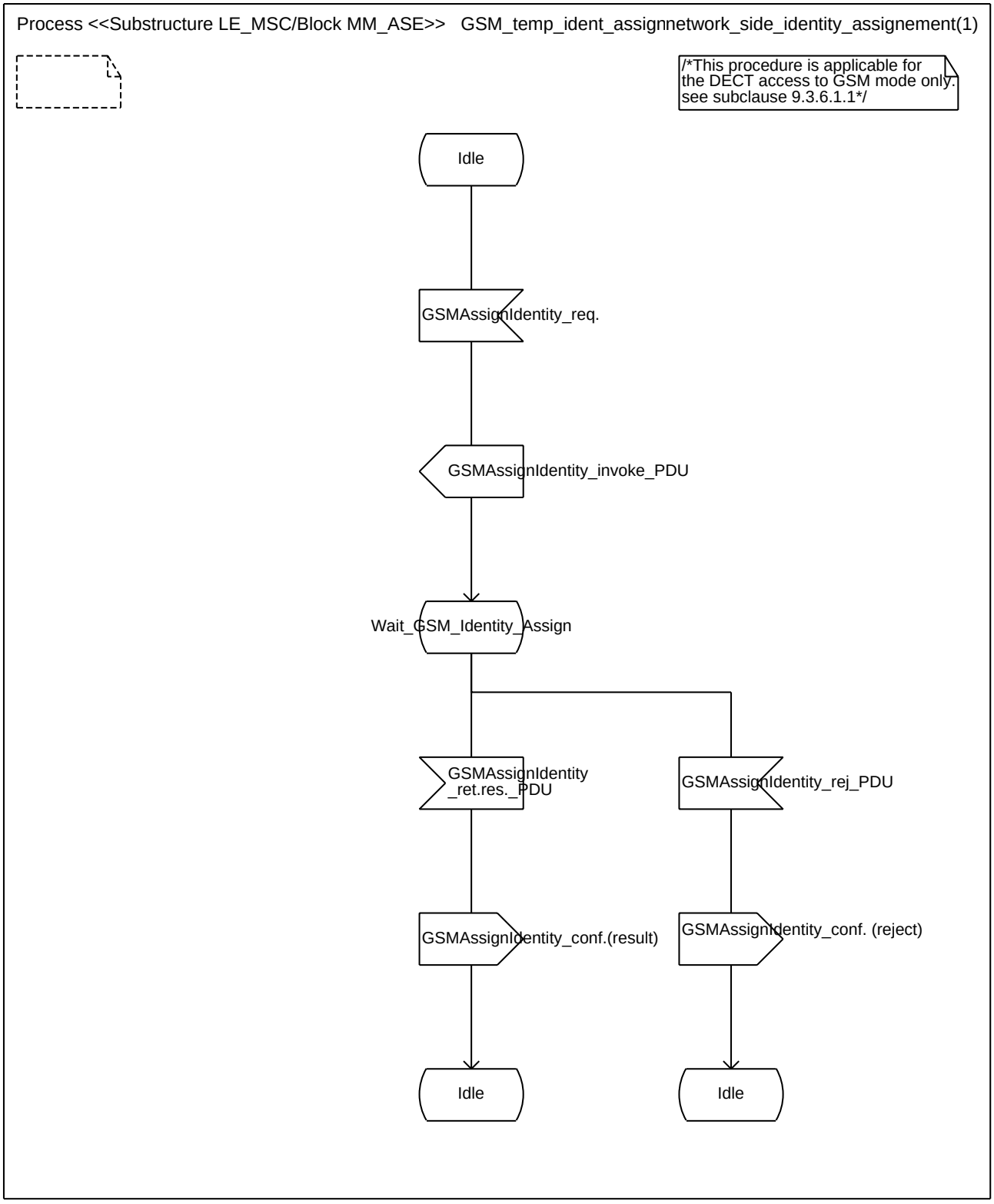


Figure F.34: Network side identity assignement

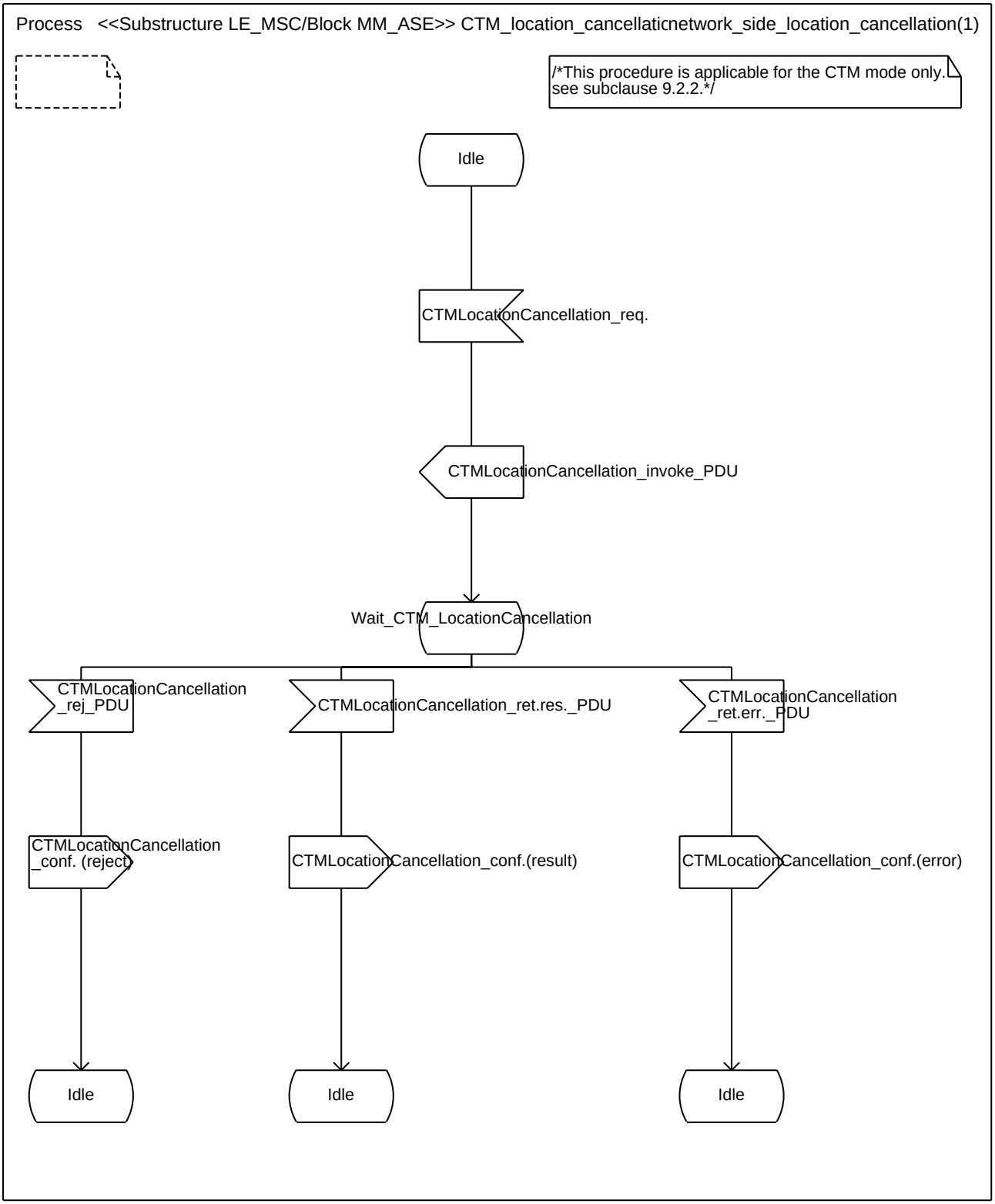


Figure F.35: Network side location cancellation

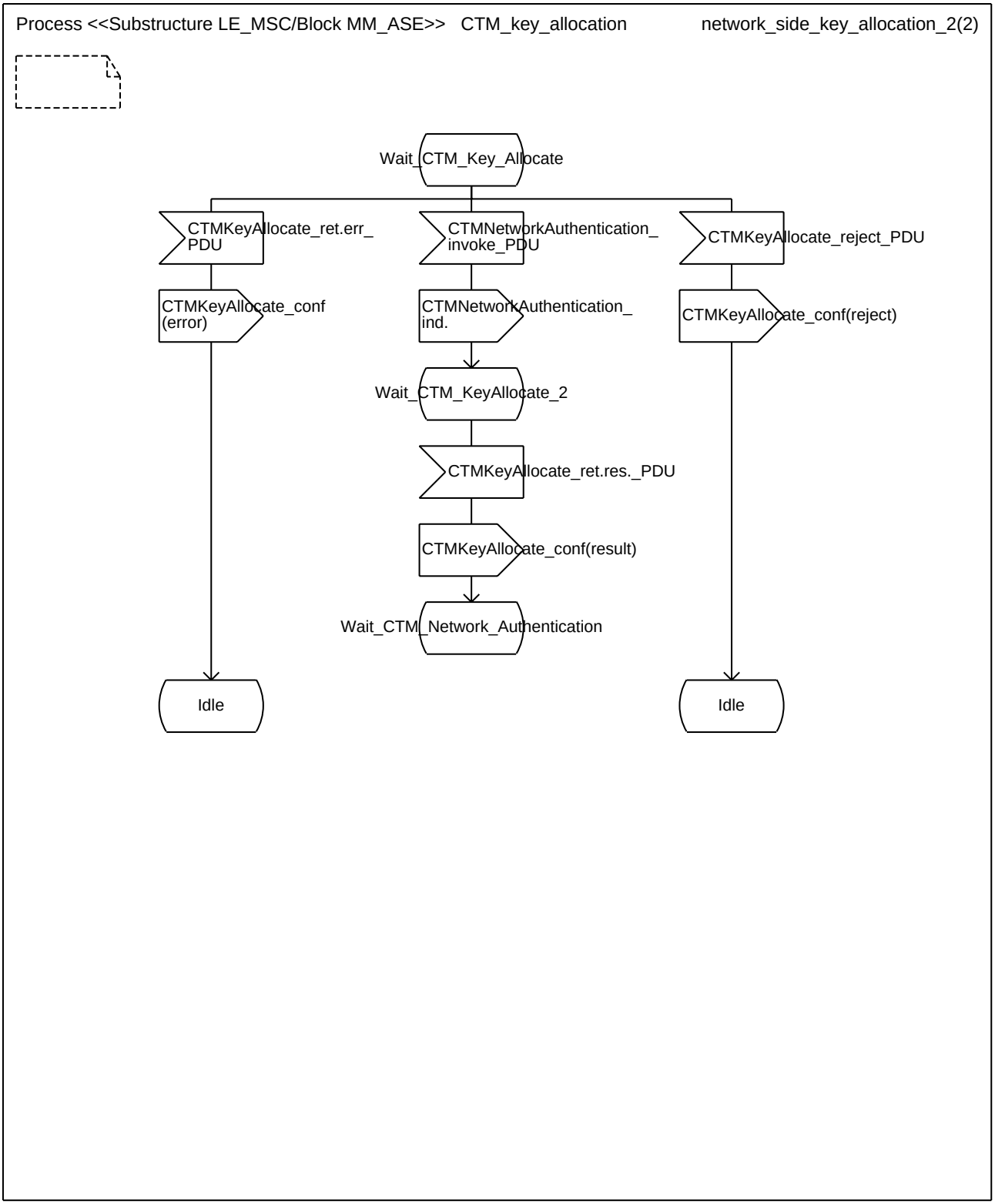


Figure F.36: Network side key allocation (1 of 2)

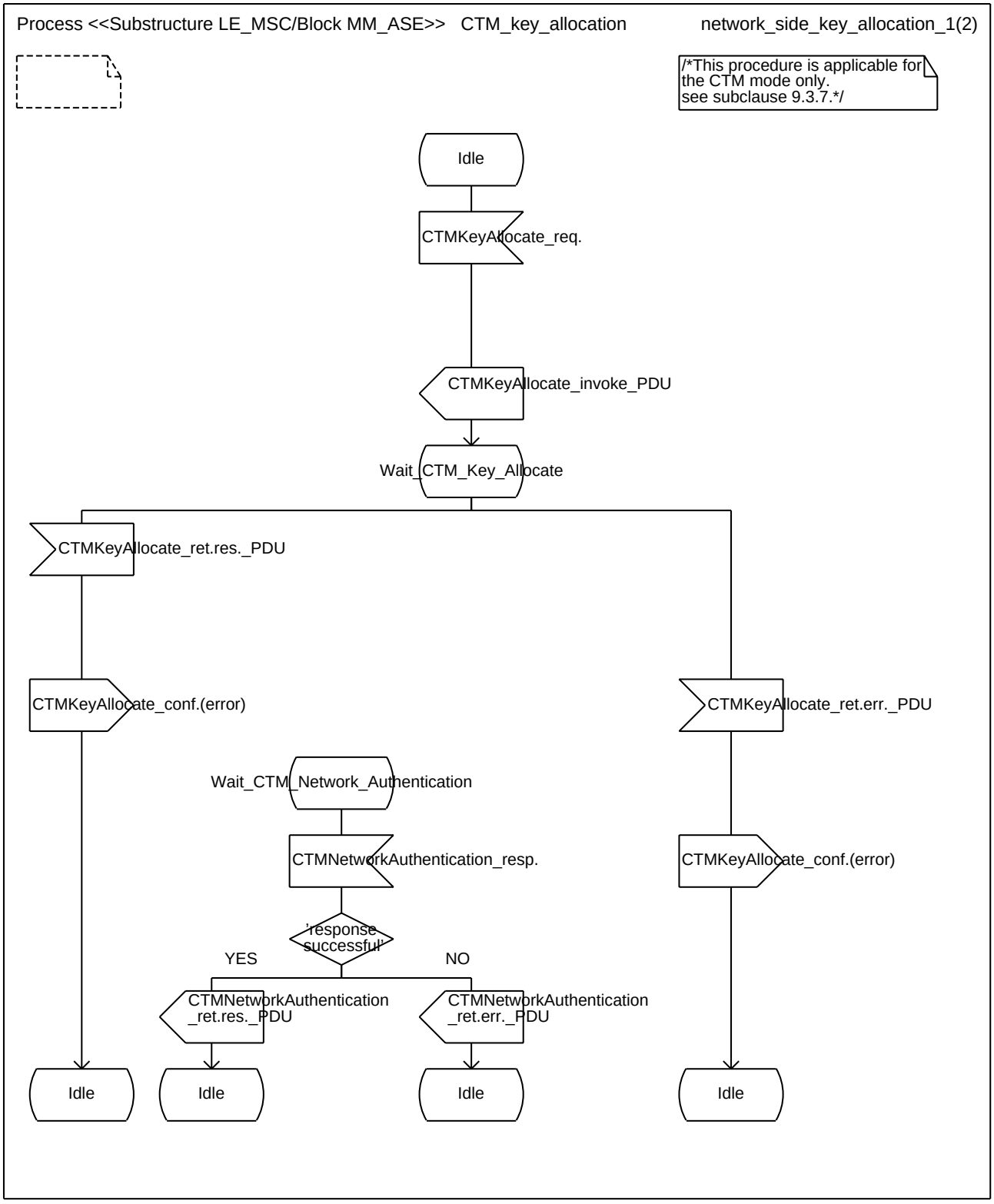


Figure F.37: Network side key allocation (2 of 2)

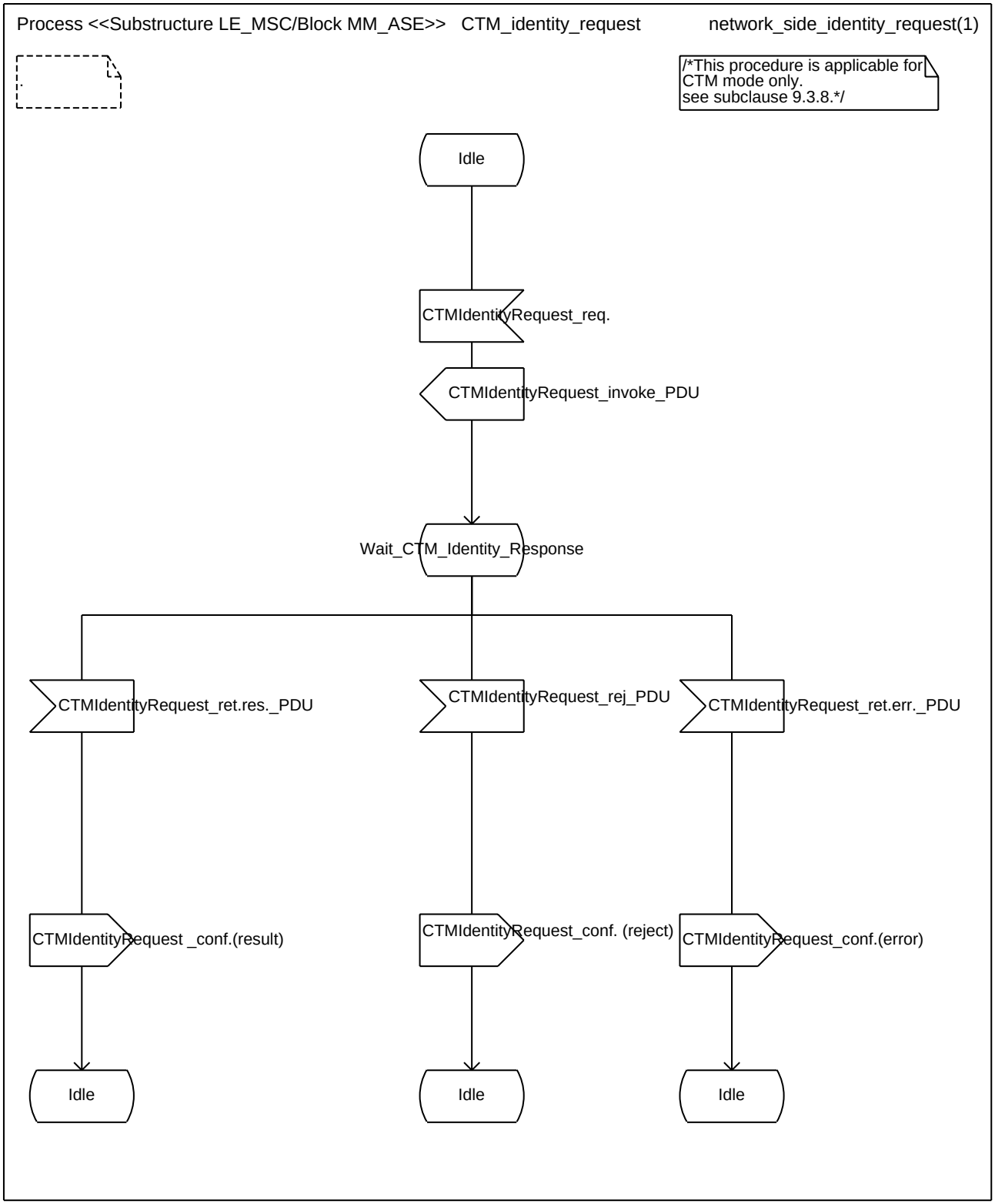


Figure F.38: Network side identity request

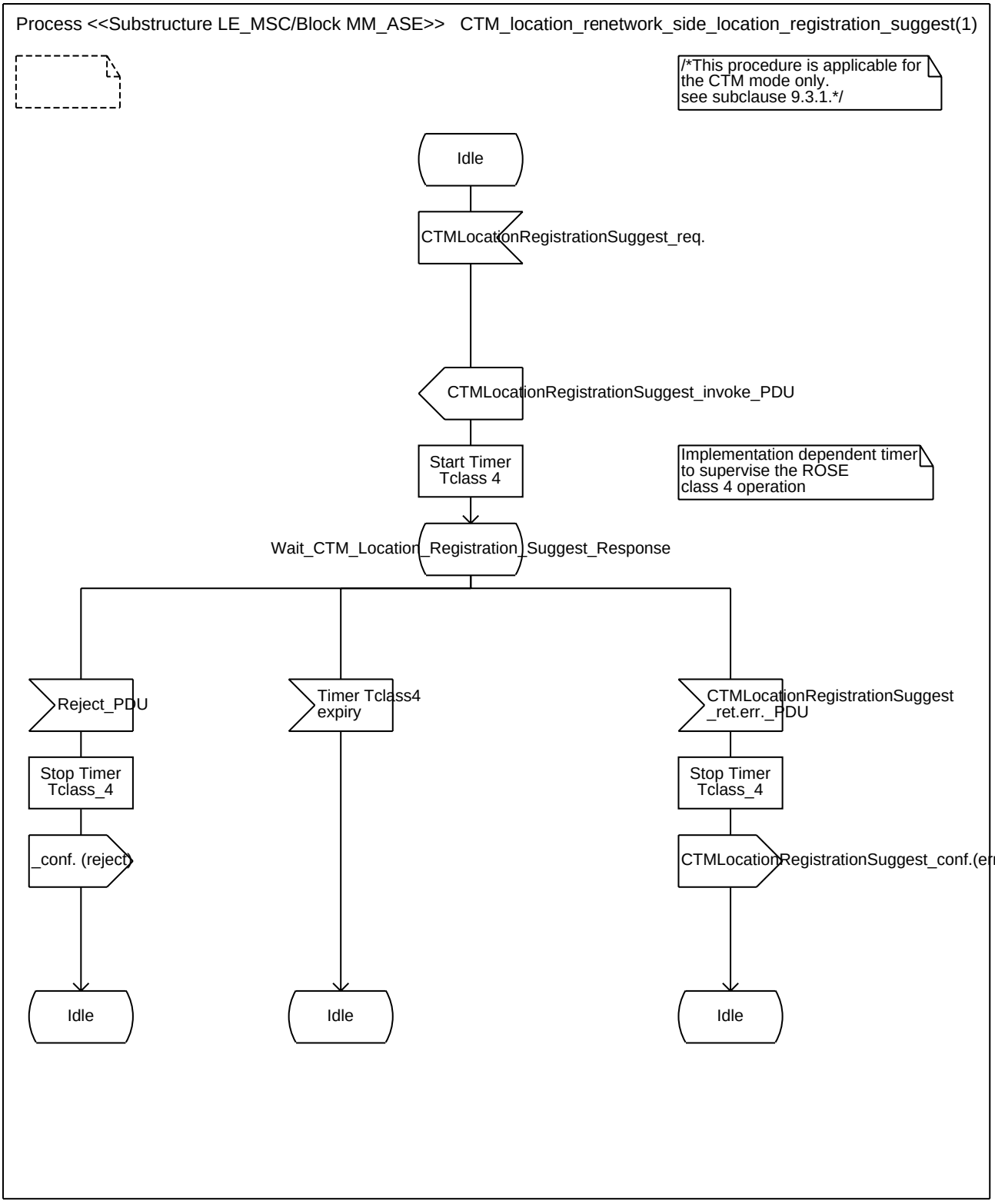


Figure F.39: Network side location registration suggest

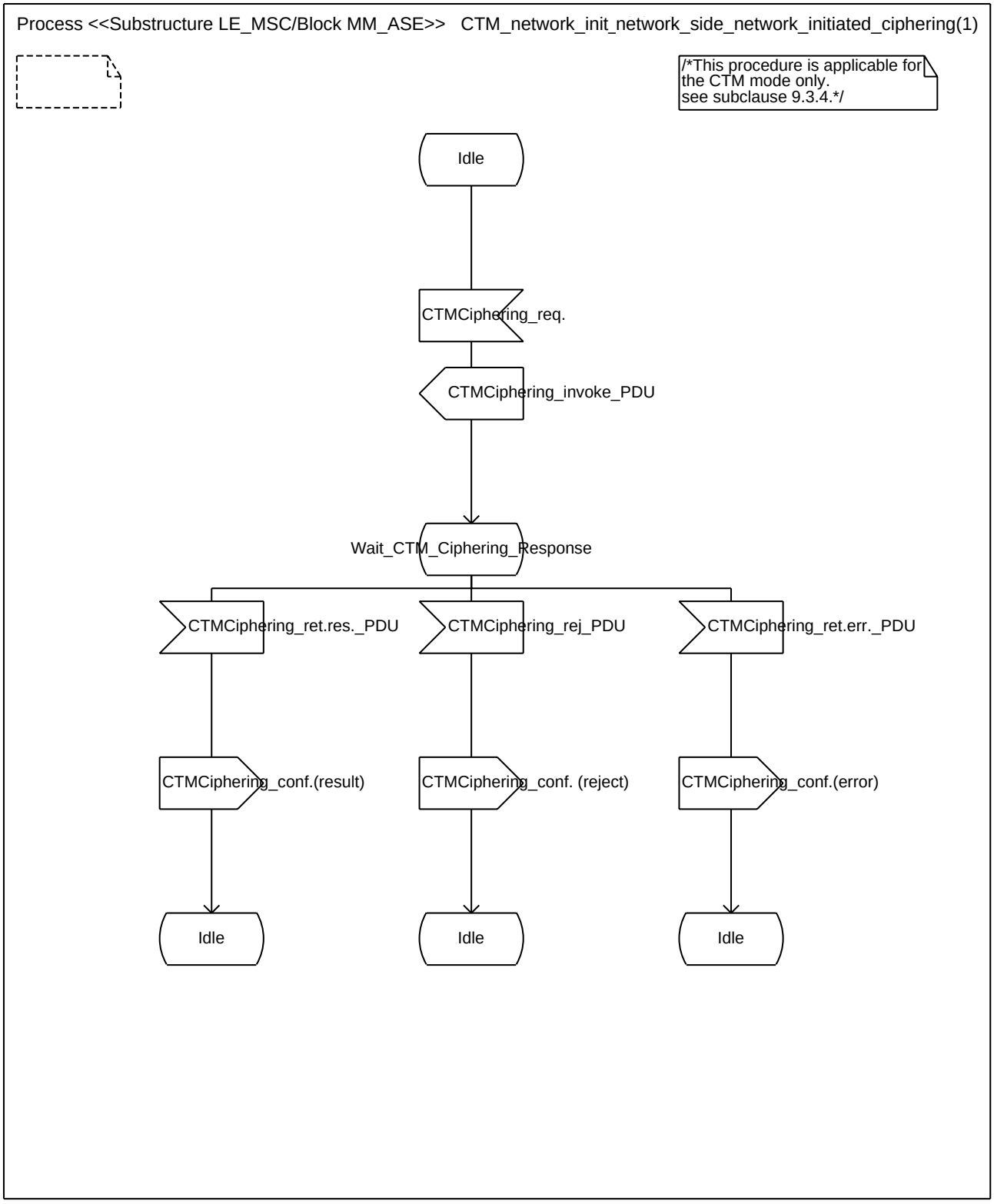


Figure F.40: Network side network initiated ciphering

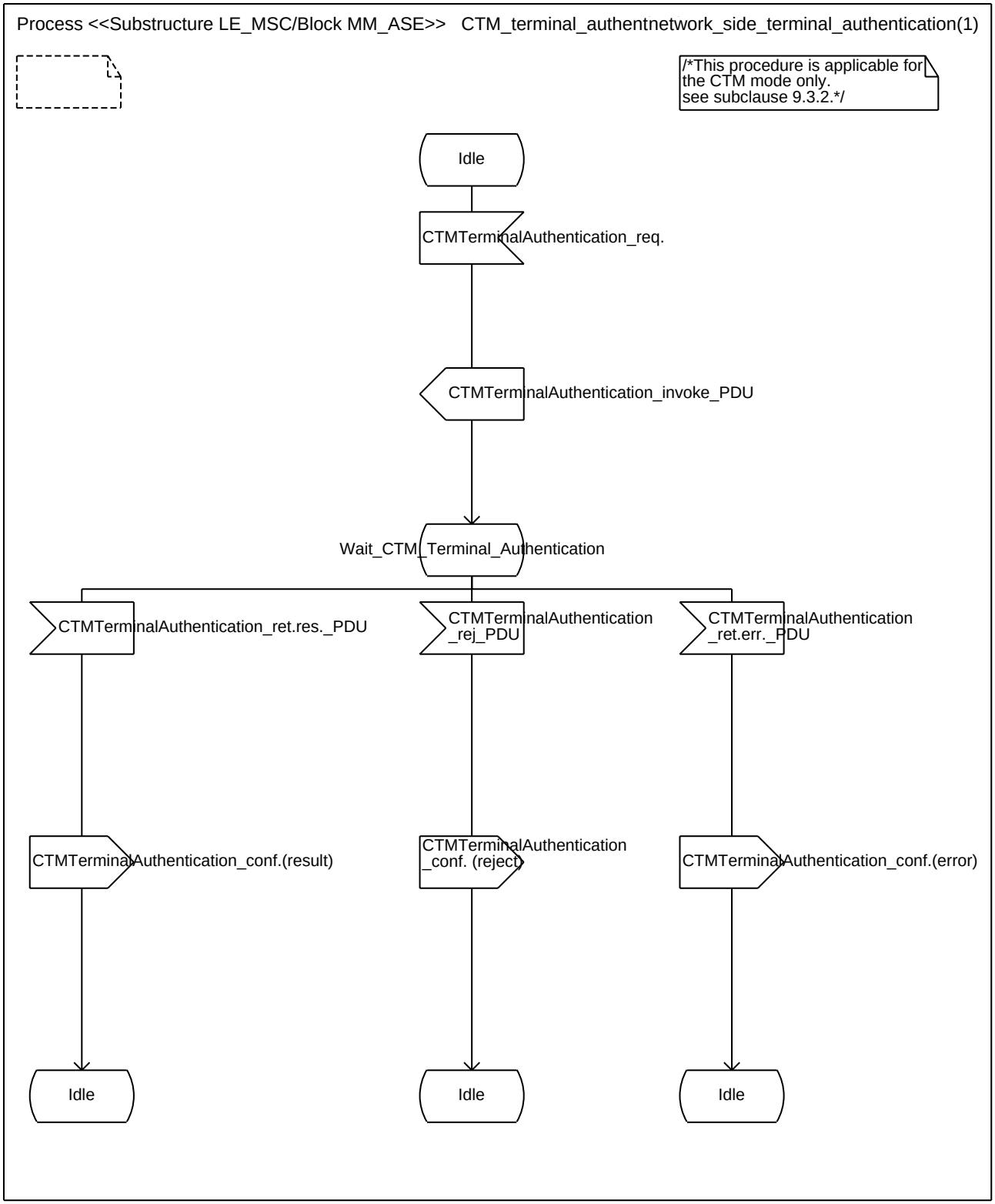


Figure F.41: Network side terminal authentication

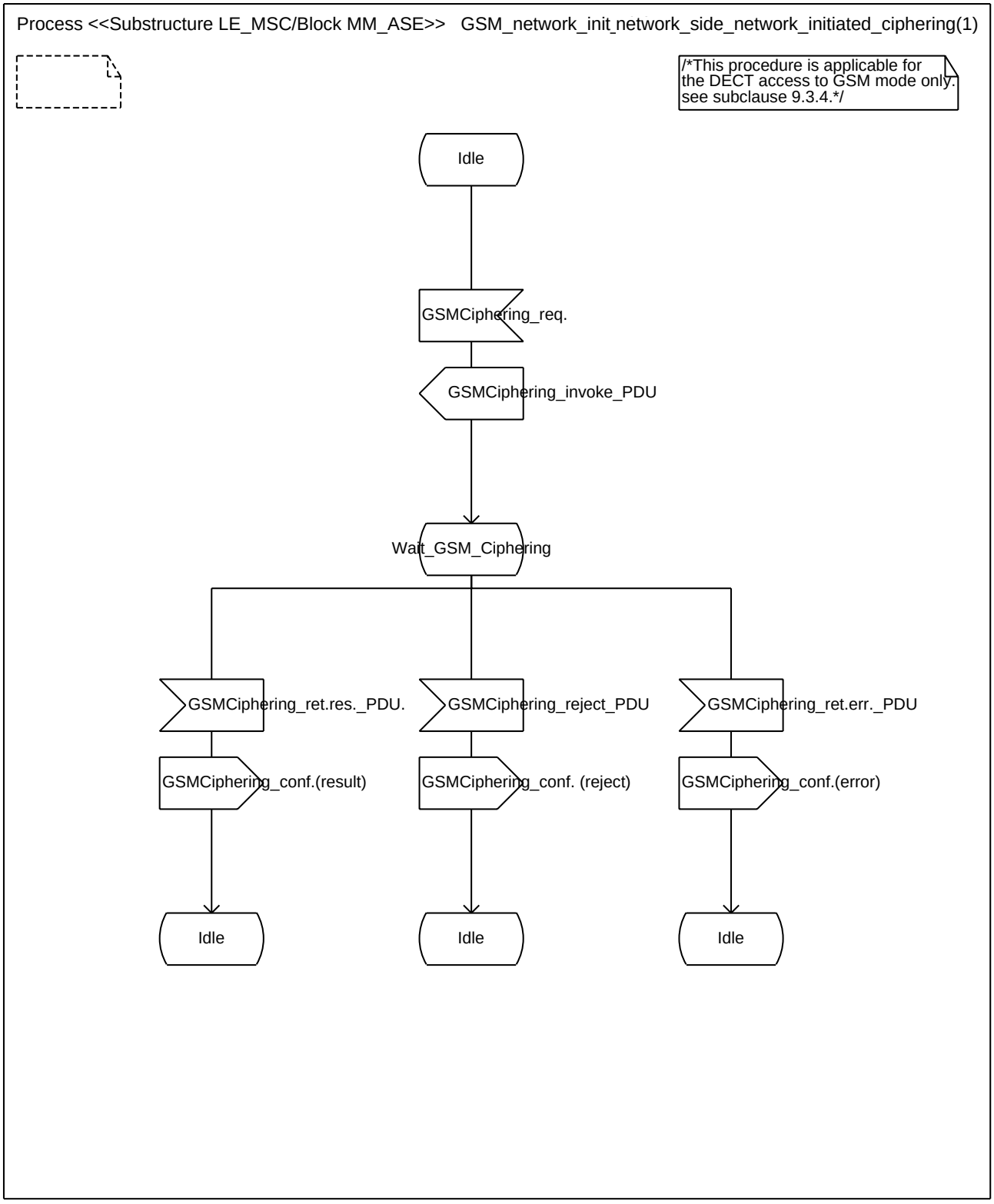


Figure F.42: Network side network initiated ciphering (GSM)

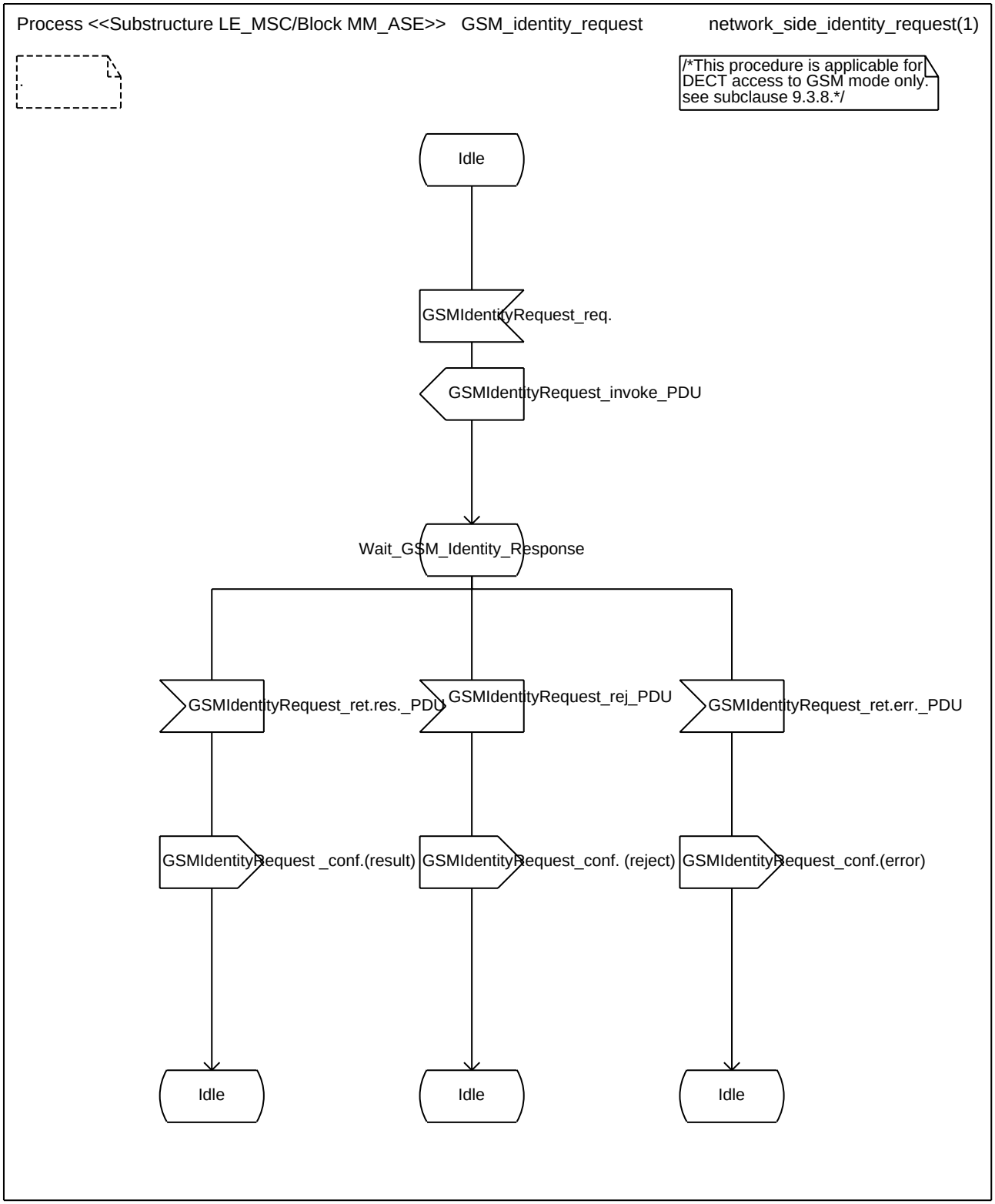


Figure F.43: Network side identity request

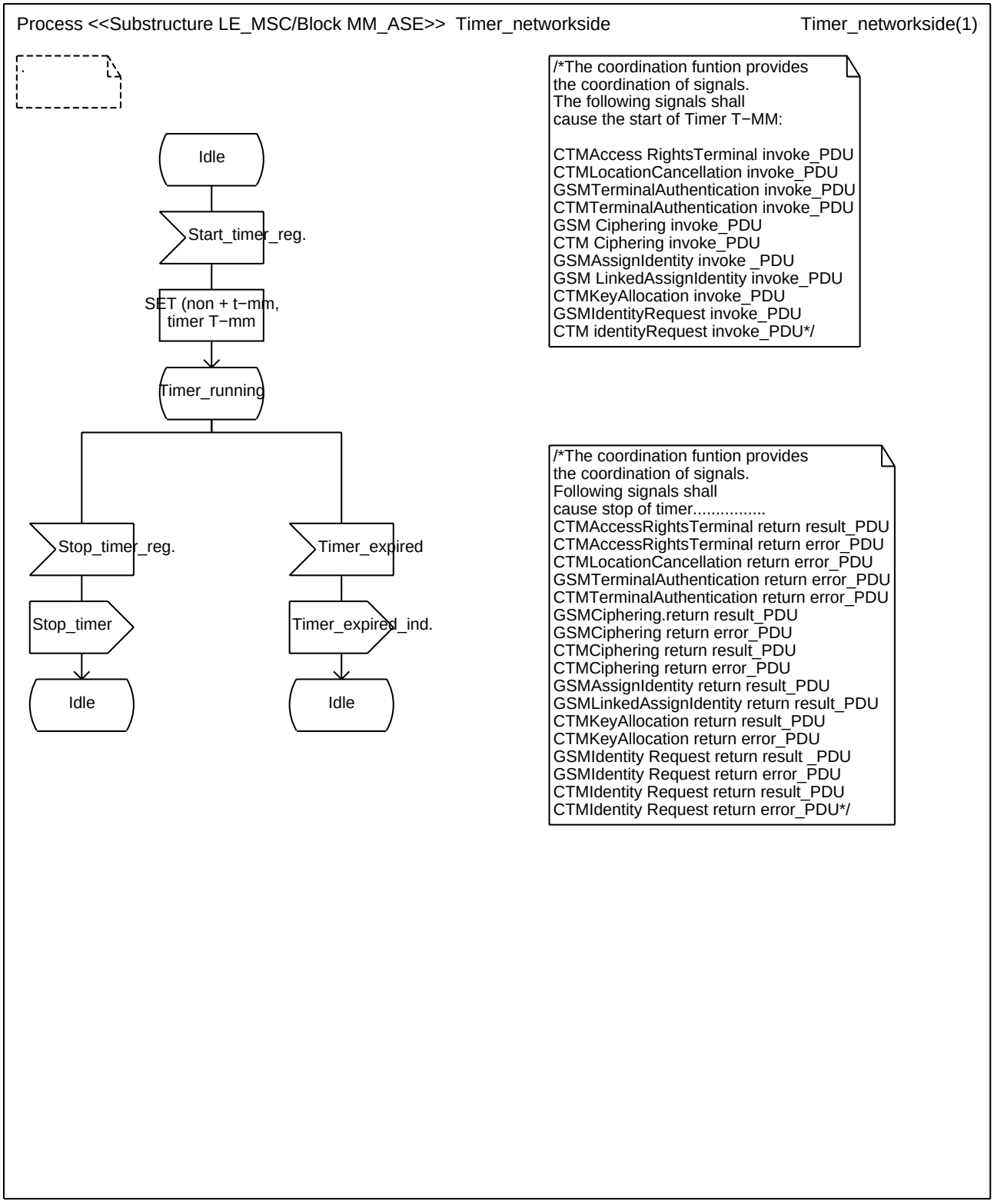


Figure F.44: Timer networkside

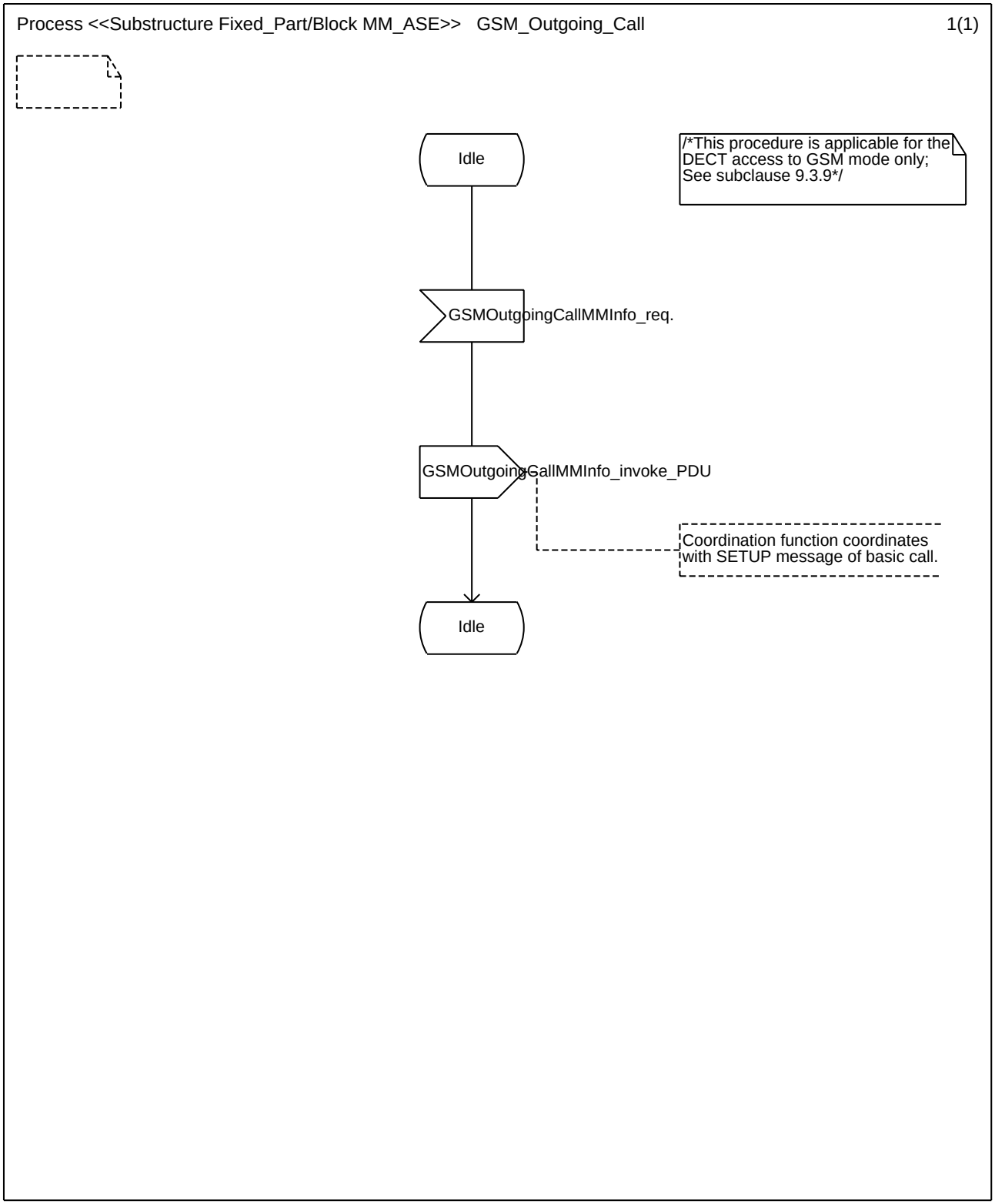


Figure F.45: GSM outgoing call

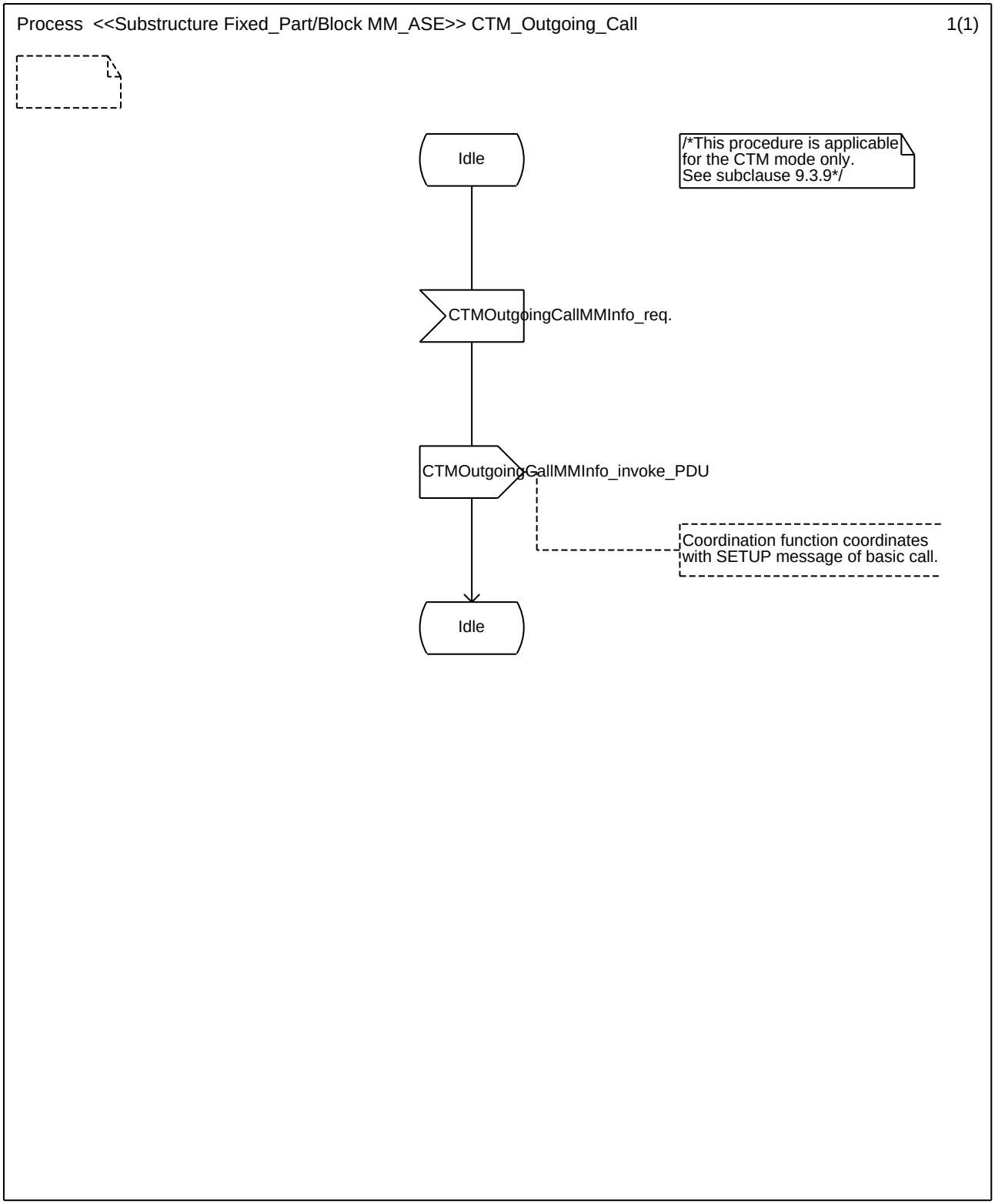


Figure F.46: CTM outgoing call

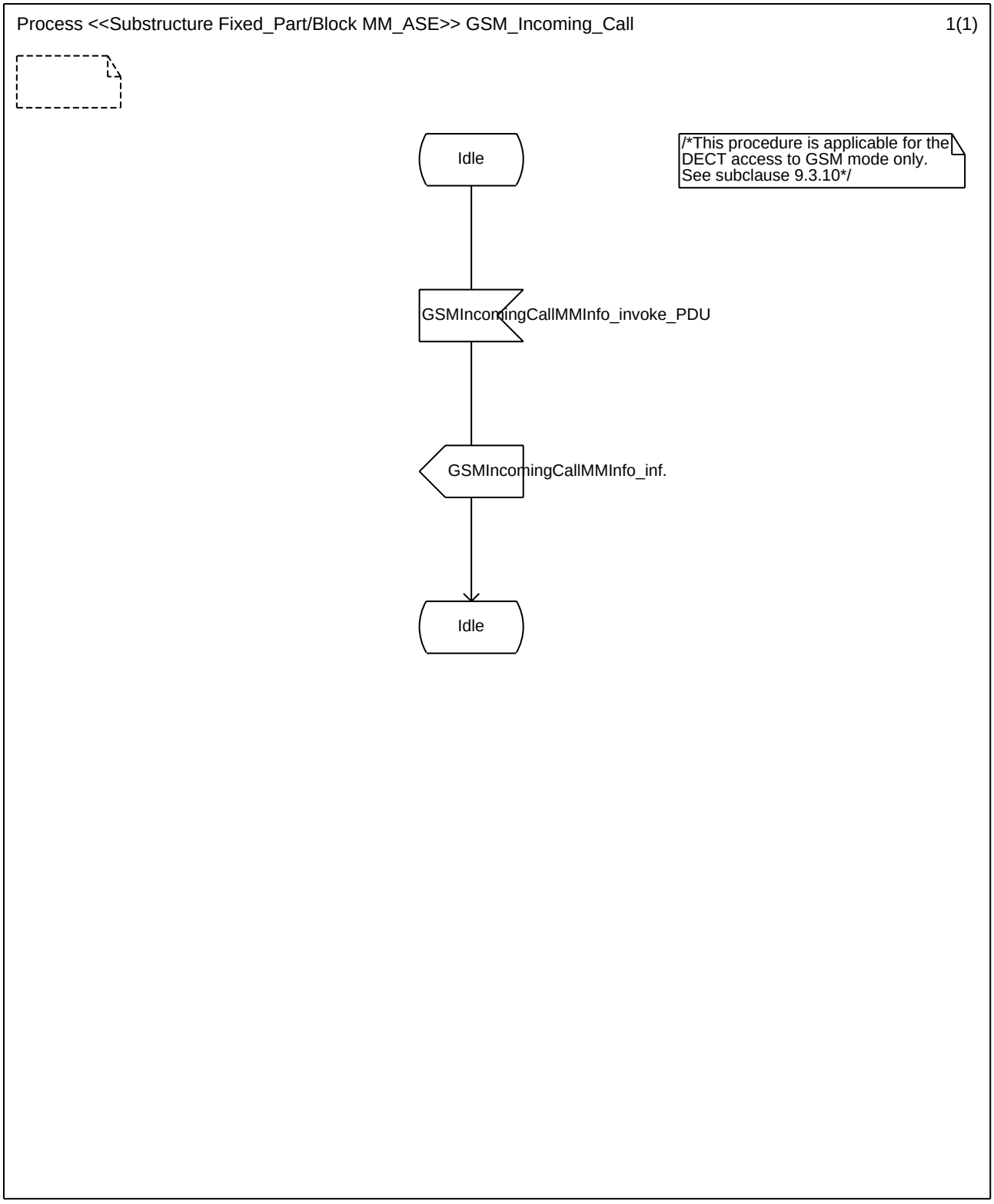


Figure F.47: GSM incoming call

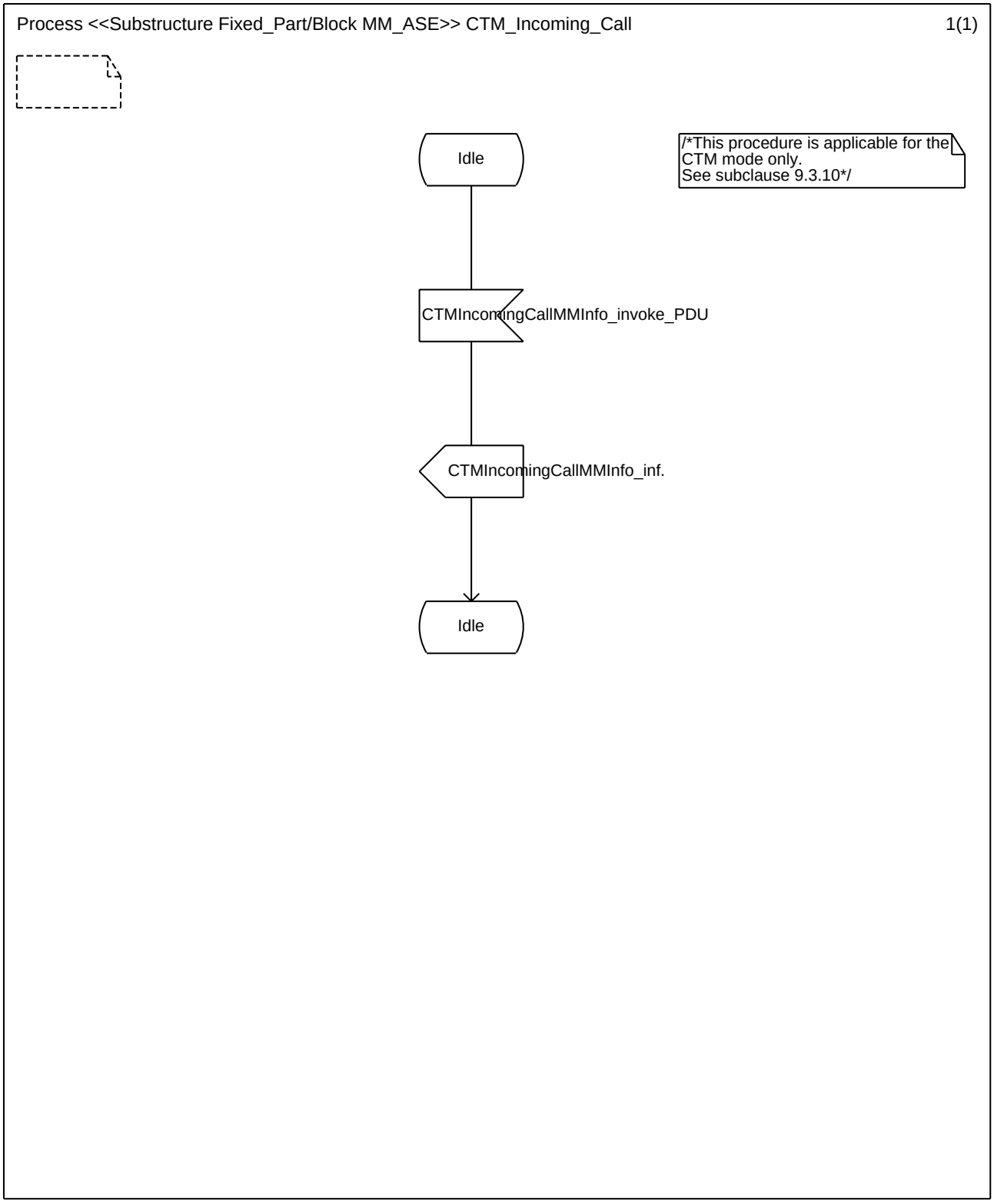


Figure F.48: CTM incoming call

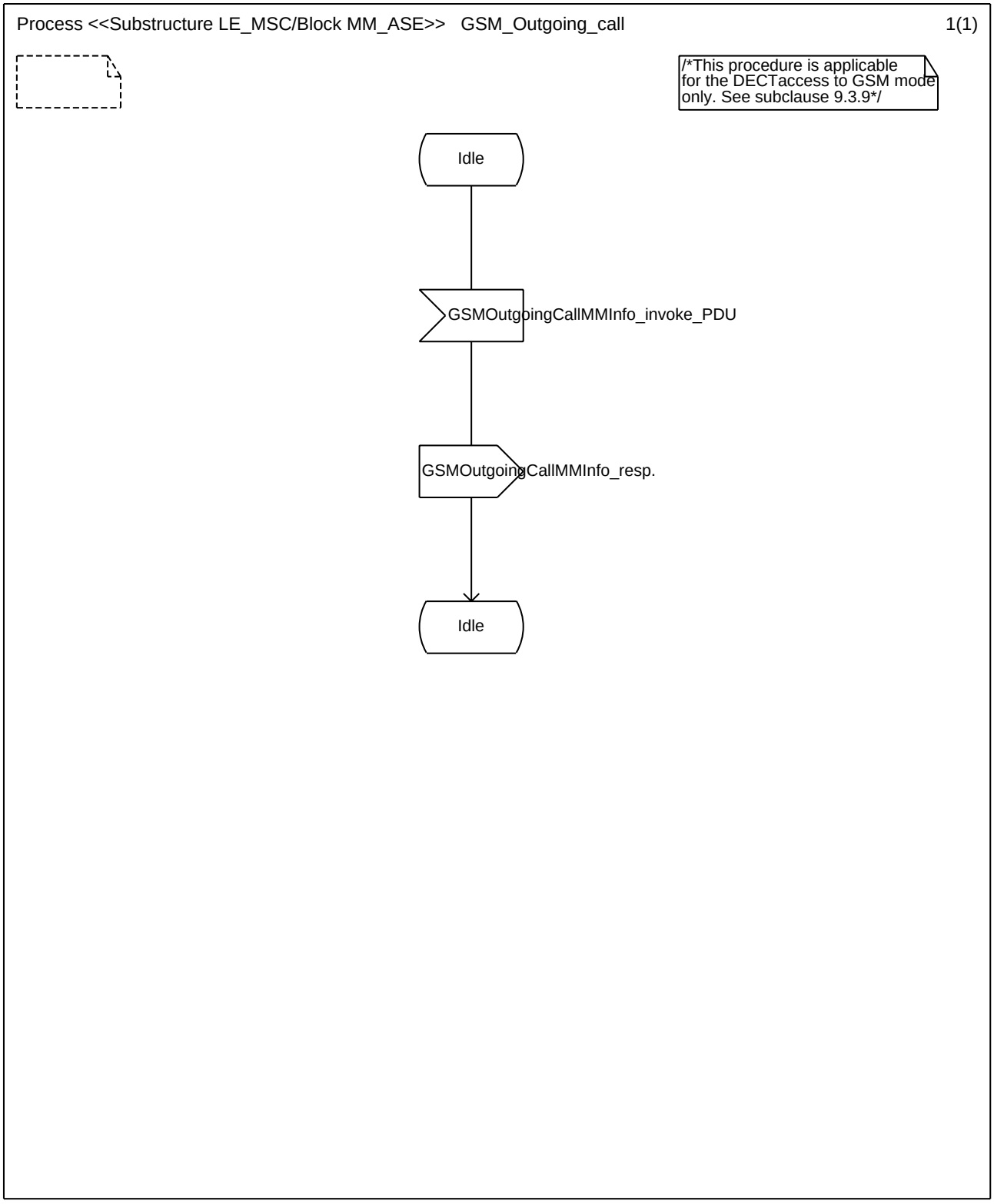


Figure F.49: GSM outgoing call

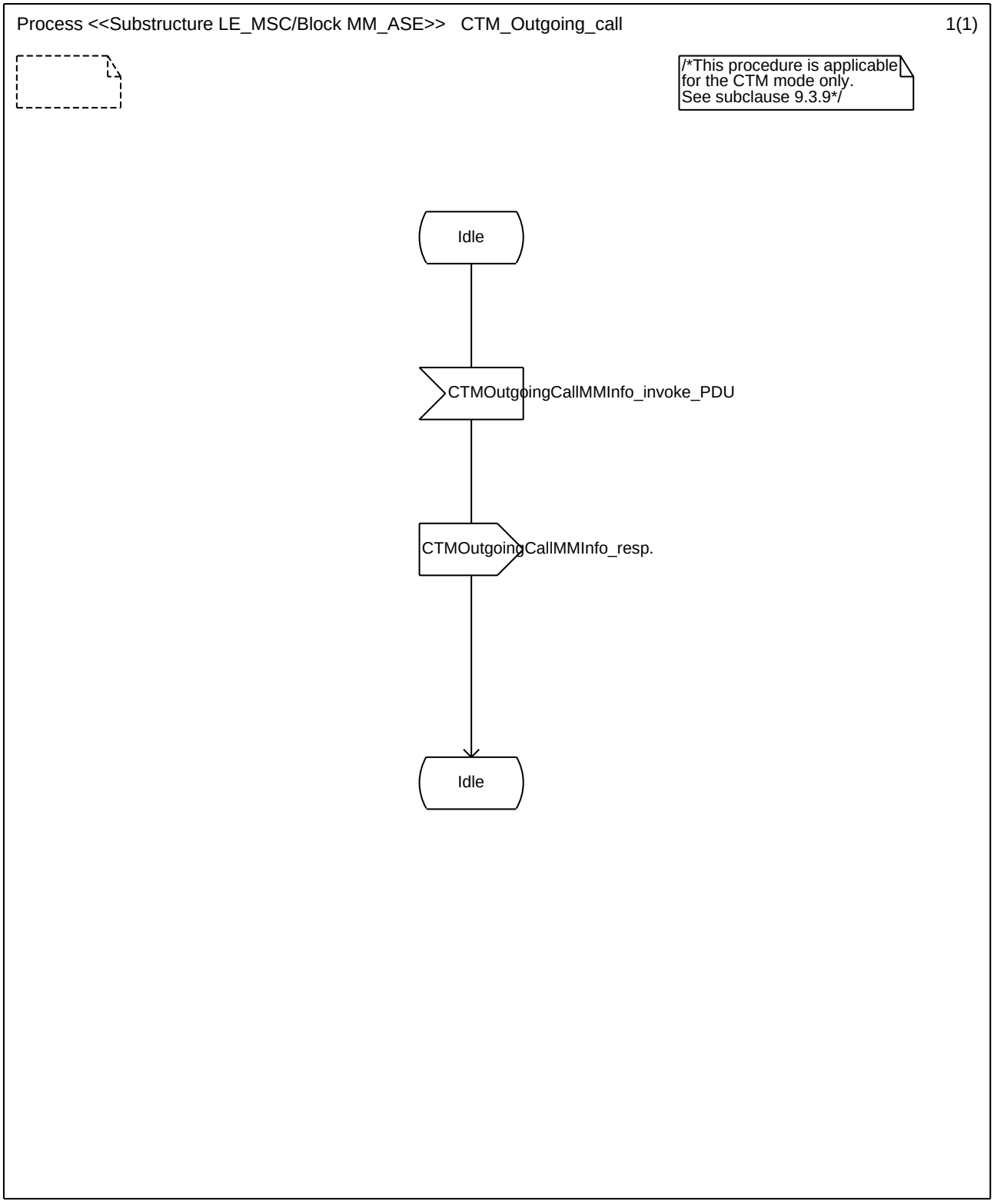


Figure F.50: CTM outgoing call

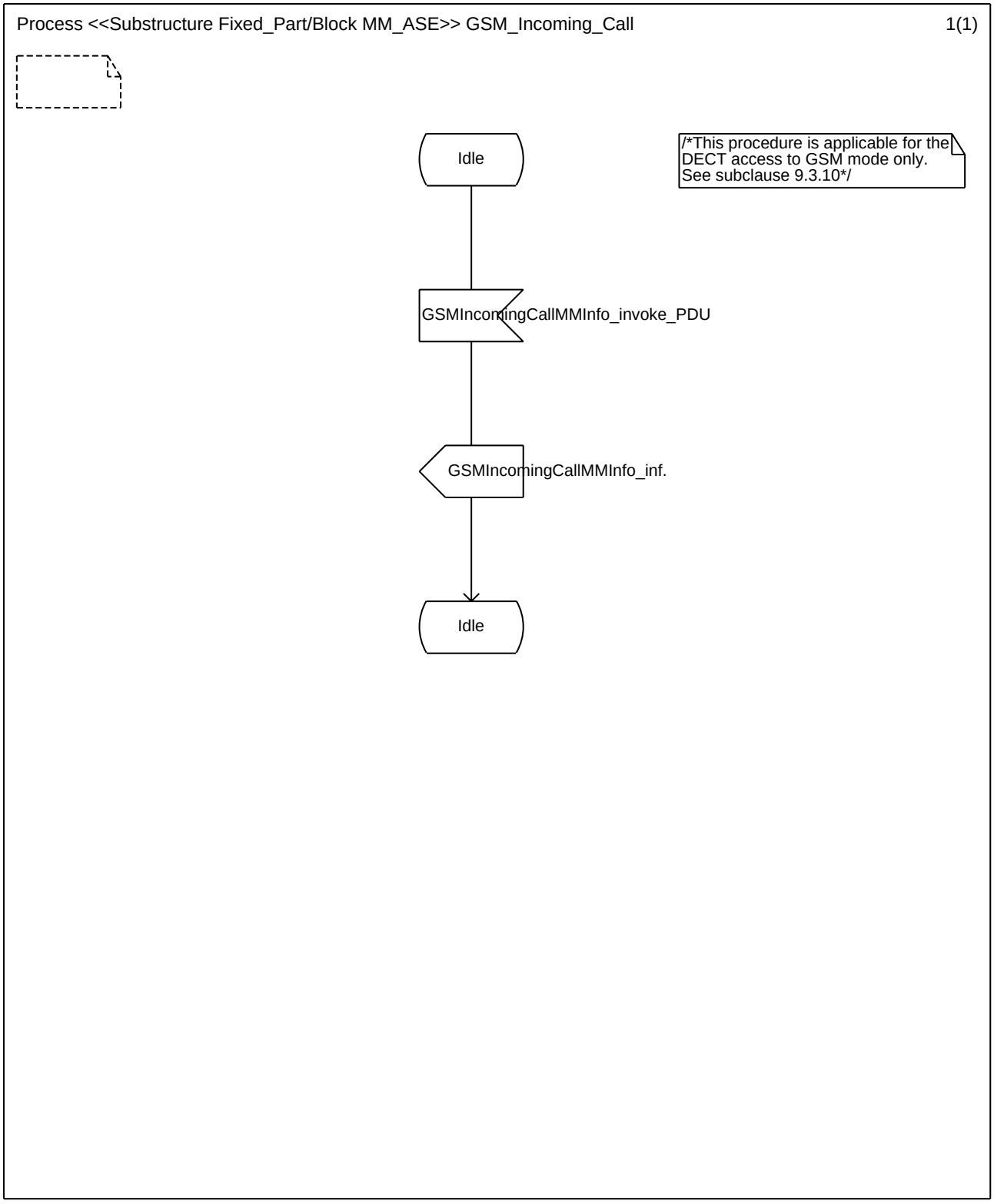


Figure F.51: GSM incoming call

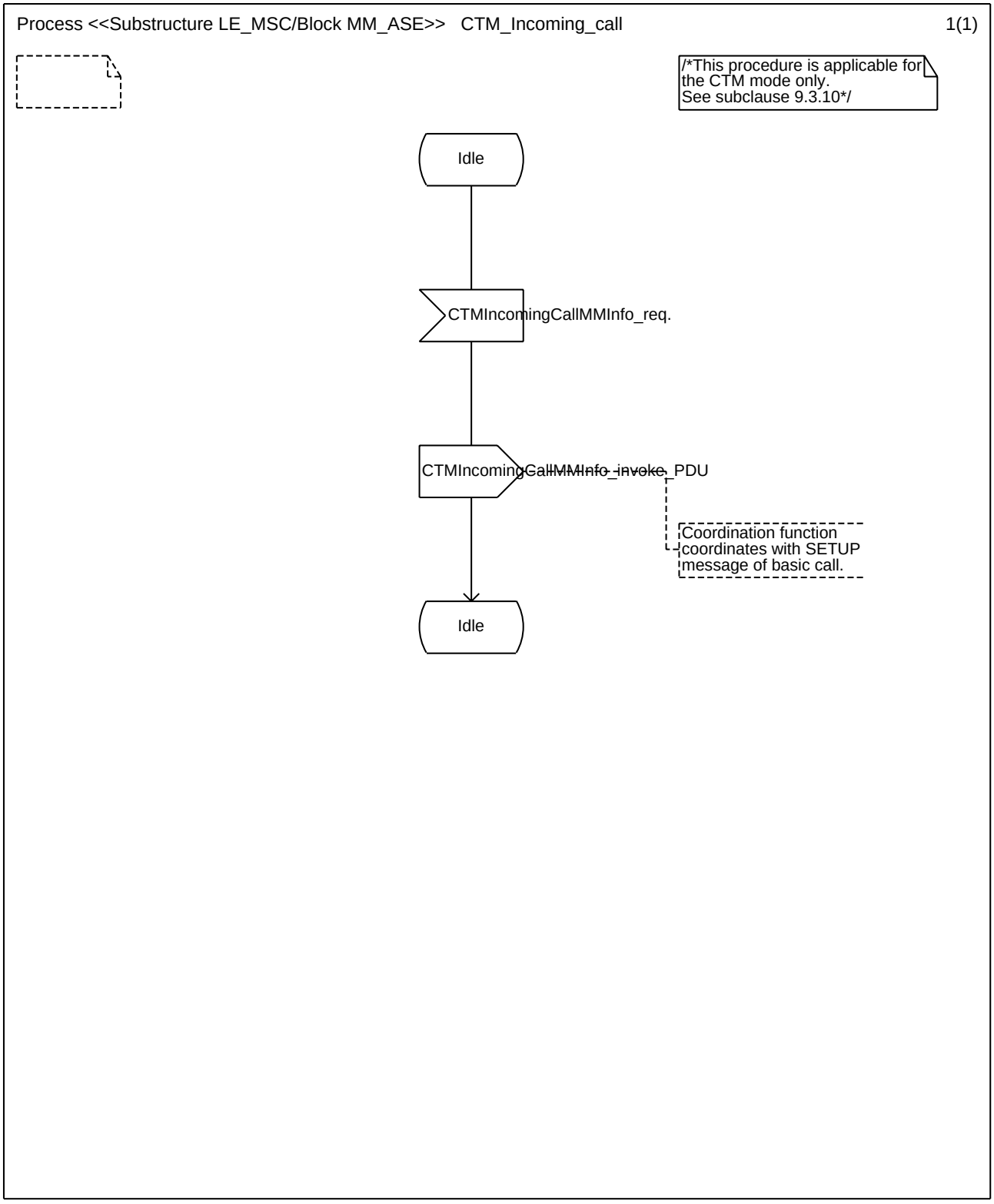


Figure F.52: CTM incoming call

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

- ITU-T Recommendation Q.9 (1988): "Vocabulary of switching and signalling terms".
- ITU-T Recommendation Z.100 (1988): "Specification and Description Language (SDL)".
- ETS 300 403-2 (1995): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 2: Specification and Description Language (SDL) diagrams".
- ETS 300 590: "Digital cellular telecommunications system (Phase 2); Mobile-services Switching Centre - Base Station System (MSC - BSS) interface; Layer 3 specification (GSM 08.08)".
- ETS 300 787: "Digital Enhanced Cordless Telecommunications (DECT); Global System for Mobile communications (GSM); Integrated Services Digital Network (ISDN); DECT access to GSM via ISDN; General description of service requirements".
- EN 301 175 (V1.1): "Cordless Terminal Mobility (CTM); Phase 1; Service description".
- EG 201 096-1 (V1.1): "Intelligent Network (IN); Cordless Terminal Mobility (CTM); IN architecture and functionality for the support of CTM; Part 1: CTM phase 1 for single public network case".

History

Document history			
V1.1.1	January 1998	Public Enquiry	PE 9822: 1998-01-30 to 1998-05-29
V1.1.2	August 2000	Vote	V 20001013: 2000-08-16 to 2000-10-15
V1.1.2	October 2000	Publication	