

ETSI EN 301 143 V1.1.4 (1999-09)

European Standard (Telecommunications series)

**Intelligent network (IN);
Intelligent Network Application Protocol (INAP);
Capability Set 2 (CS2);
Cordless Terminal Mobility (CTM);
Stage 3 specifications for Service Control Function (SCF);
SCF and Call Unrelated Service Function (CUSF)/
Service Switching Function (SSF);
SCF interface**



Reference

DEN/SPS-03061 (al000ieo.PDF)

Keywords

CCS, CS2, CTM, INAP, ISDN, protocol, SS7, IN

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet

secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
<http://www.etsi.org>
If you find errors in the present document, send your
comment to: editor@etsi.fr

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1999.
All rights reserved.

Contents

Intellectual Property Rights	7
Foreword	7
Introduction	7
1 Scope	8
2 References	8
3 Definitions and abbreviations	9
3.1 Definitions	9
3.2 Abbreviations	10
4 General	11
4A Proposed functional models for the CTM procedures	13
5 CTM procedures	16
5.1 Model	16
5.2 Addressing	17
5.2.1 General	17
5.2.2 Addressing the SCF	18
5.2.2.1 During incoming call set-up	18
5.2.2.2 At location registration	19
5.2.2.3 At outgoing call set-up	19
5.3 Subscription registration in SCFmmSubscription	19
5.3.1 Procedure description	19
5.3.1.1 Introduction	19
5.3.1.2 Normal operation	19
5.3.1.3 Exceptional procedure	20
5.3.2 SDL application procedures	20
5.4 Key allocation	20
5.5 Subscription deregistration	20
5.6 Network authentication	21
5.7 Terminal authentication	21
5.8 Network initiated ciphering	21
5.9 Location registration in the SCFmmVisited	21
5.10 Location update in the SCFmmHome	21
5.10.1 Procedure description	21
5.10.1.1 Introduction	21
5.10.1.2 Normal operation	22
5.10.1.3 Exceptional procedure	22
5.10.2 SDL application procedures	23
5.11 Location cancellation in SCFmmVisited	23
5.12 Location cancellation in the FT	23
5.13 Restoration of location data in the SCFmmHome	23
5.13.1 Procedure description	23
5.13.1.1 Introduction	23
5.13.1.2 Normal operation	23
5.13.1.3 Exceptional procedure	24
5.13.2 SDL application procedures	24
5.14 Terminal authentication and/or ciphering	24
5.15 Download of security data	24
5.15.1 Procedure description	24
5.15.1.1 Introduction	24
5.15.1.2 Normal operation	25
5.15.1.3 Exceptional procedure	25
5.15.2 SDL application procedures	25

5.16	Provide roaming number.....	25
5.16.1	Procedure description.....	25
5.16.1.1	Introduction	25
5.16.1.2	Normal operation.....	26
5.16.1.3	Exceptional procedure	26
5.16.2	SDL application procedures	26
6	Extensions of INAP	27
6.1	SCF-SCF service to service extensions.....	27
6.1.1	ASN.1 module.....	27
6.1.2	Data types.....	27
6.1.3	Error types.....	27
6.1.4	Operation codes.....	27
6.1.5	Error codes	28
6.1.6	Classes.....	28
6.1.7	Object identifiers.....	28
6.1.8	Operations and arguments	29
6.1.9	SSI-SCF-SCF interface	30
6.1.10	TransferSTSIIinformation operation	32
6.1.10.1	Procedure descriptions.....	32
6.1.10.1.1	General description	32
6.1.10.1.2	Invoking entity (controlling SCF).....	33
6.1.10.1.2.1	Normal procedure.....	33
6.1.10.1.2.2	Error handling	33
6.1.10.1.3	Invoking entity (supporting SCF).....	33
6.1.10.1.3.1	Normal procedure.....	33
6.1.10.1.3.2	Error handling	33
6.1.10.1.4	Responding entity (supporting SCF).....	33
6.1.10.1.4.1	Normal procedure.....	33
6.1.10.1.4.2	Error handling	34
6.1.10.1.5	Responding entity (controlling SCF)	34
6.1.10.1.5.1	Normal procedure.....	34
6.1.10.1.5.2	Error handling	34
6.2	Mapping of CTM operations to the extended INAP	34
7	ASN.1 specification for CTM application.....	35
7.1	Mobility Management Application Timers.....	38
7.2	Application Timers	38
8	Interworking with DSS1	38
8.1	Description.....	38
8.1.1	Detection point processing	39
8.1.2	Receipt of DSS1+ messages.....	39
8.1.3	Receipt of INAP operations	39
8.1.4	Coding requirements	39
8.2	Generic procedures	39
8.2.1	USI handling procedures.....	40
8.2.1.1	GFT-control input and output for CTM.....	40
8.2.1.2	Receiving of DSS1+ operations / sending of UTSI information.....	40
8.2.1.3	Receiving of STUI information / sending of DSS1+ operations.....	40
8.2.2	INAP component handling procedures	41
8.3	Call related issues	41
8.3.1	Outgoing call.....	41
8.3.2	Emergency call.....	41
8.3.3	Incoming call.....	42
8.3.4	Call release.....	42
8.4	Call unrelated issues	42
8.4.1	User initiated association	42
8.4.2	Network initiated association	43
8.4.3	Information exchange during the association	43
8.4.4	Association release.....	43

Annex A (informative):	Message Sequence Charts.....	44
A.1	Subscription registration.....	45
A.2	Subscription deregistration.....	49
A.3	Location registration in the SCFmmVisited.....	52
A.4	Location update in the SCFmmHome.....	54
A.5	LocationCancellation in the SCFmmVisited.....	56
A.6	LocationCancellation in the FT.....	57
A.7	Download of security data.....	59
A.8	Restoration of location data in the SCFmmHome.....	60
A.9	Terminal authentication ciphering.....	62
A.10	Network Authentication.....	64
Annex B (informative):	Call control Message Sequence Charts.....	65
B.1	Outgoing call.....	65
B.2	Incoming call.....	70
Annex C (informative):	SDL model.....	73
C.1	System Type scf_scf_network.....	73
C.2	Block Type SCFVisCTM.....	79
C.3	Process Type SCF_SCF_CUSF_ASE_Visited.....	81
C.4	Procedure DetermineCtmArg.....	86
C.5	Procedure GetInvokeID.....	87
C.6	Process Type SCFmmVisitedApplication.....	88
C.7	Procedure LocationRegistrationSCF.....	89
C.8	Procedure LocationCancellationFT.....	91
C.9	Procedure DownloadSecurityData.....	93
C.10	Procedure TerminalAuthentication.....	95
C.11	Procedure Ciphering.....	97
C.12	Procedure IdentityRequest.....	99
C.13	Procedure SubscriptionRegistration.....	101
C.14	Procedure LocationRegistration.....	105
C.15	Procedure LocationRegistrationSuggest.....	108
C.16	Process Type SCFsIVisitedApplication.....	110
C.17	Procedure ProvideRoamingNumber.....	111
C.18	Process Type SCF_SCF_ASE_Visited.....	112
C.19	Procedure DetermineCtmArg_SCFVis.....	117
C.20	Block Type SCFHomCTM.....	119
C.21	Process Type SCFmmHomeApplication.....	120
C.22	Procedure LocationRegistration_SCF.....	121

C.23	Procedure SubscriptionDeregistration_SCF.....	122
C.24	Procedure RestoreData_SCF.....	125
C.25	Procedure TerminalAuthentication_SCF.....	126
C.26	Procedure Cipherring_SCF.....	128
C.27	Procedure NetworkAuthentication_SCF.....	129
C.28	Procedure KeyAllocate_SCF.....	130
C.29	Procedure LocationCancellation_SCF.....	132
C.30	Procedure SubscriptionRegistration_SCF.....	134
C.31	Procedure DownloadSecurityData_SCF.....	136
C.32	Process Type SCFslHomeApplication.....	137
C.33	Procedure ProvideRoamingNumber_SCF.....	138
	Bibliography.....	140
	History.....	141

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 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 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 Signalling Protocols and Switching (SPS).

National transposition dates	
Date of adoption of this EN:	3 September 1999
Date of latest announcement of this EN (doa):	31 December 1999
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 June 2000
Date of withdrawal of any conflicting National Standard (dow):	30 June 2000

Introduction

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

The signalling procedures provided in the present document are supporting features required for CTM phase 1 on the SCF-SCF, SSF-SCF, and CUSF-SCF interfaces. The service to service capability extensions to the core Intelligent Network Application Part (INAP) CS2 SCF-SCF interface provided in the present document are used to support the features required for CTM phase 1.

1 Scope

The present document analyses what the Cordless Terminal Mobility (CTM) specific specifications are within the generic parameters on the Service Control Function (SCF)-SCF, Call Unrelated Service Function (CUSF)-SCF and Service Switching Function (SSF)-SCF interfaces of the ETSI core Intelligent Network Application Part (INAP). These specifications ensure internetworking between CTM networks and the establishment of a multi-vendor environment for CTM.

The generic INAP protocol contains generic parameters that can convey application specific information, such as for the CTM application. Detailed CTM specifications are described by the present document using the INAP SCF-SCF, CUSF-SCF and SSF-SCF interface capabilities. The SCF-Service Data Point (SDF) and SDF-SDF interfaces are not considered in the present document.

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, subsequent revisions do apply.
- 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] EN 301 140-1 (V1.3): "Intelligent Network (IN); Intelligent Network Capability Set 2 (CS2); Intelligent Network Application Protocol (INAP); Part 1: Protocol specification".
- [2] EN 301 144-1: "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol and Signalling System No.7 protocols; Signalling application for the mobility management service on the alpha interface; Part 1: Protocol specification".
- [3] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".
- [4] ETS 300 175-7 (1995): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".
- [5] ETS 300 009-1: "Integrated Services Digital Network (ISDN); Signalling System No.7; Signalling Connection Control Part (SCCP) (connectionless and connection-oriented class 2) to support international interconnection; Part 1: Protocol specification [ITU-T Recommendations Q.711 to Q.714 and Q.716 (1993), modified]".
- [6] ITU-T Recommendation E.212: "Identification plan for land mobile stations".
- [7] ITU-T Recommendation E.214: "Structure of the land mobile global title for the signalling connection control part (SCCP)".

3 Definitions and abbreviations

3.1 Definitions

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

Authentication Code (AC): AC may be held in non-volatile memory within the PP or it may be manually entered by the user when required for an authentication service. This depends on the application; see ETS 300 175-7 [4].

access rights: indication that the cordless terminal has appropriate permission to use the CTM service.

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

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

cordless terminal mobility: 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.

CTM identity: identity by which a user is known to the CTM service providers and networks supporting CTM, and it is used for flexibility and security purposes. The CTM identity identifies a user unambiguously. The CTM identity does not need to be known by users.

CTM number: number that uniquely and unambiguously identifies each CTM user. It is used by a calling party to reach the CTM user. The number is independent of the calling terminal, network or service used and conforms to ITU-T Recommendation E.164 [3].

DECT Paging: DECT procedure which establishes a link on DECT interface.

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

Fixed Termination (FT): logical group of functions that contains 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.

FT Address: address of the FT (i.e. an E.164 address).

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

Portable Termination: logical group of functions that contains all of the CT processes and procedures on the portable side of the CT air interface. A Portable radio Termination only includes elements that are defined in the relevant CT specification.

RANdOm challenge: this parameter is used for authentication (see ETS 300 175-7 [4]).

RES1: see ETS 300 175-7 [4].

RES2: see ETS 300 175-7 [4].

RS: value used to establish authentication session keys, as defined in subclause 4.4.3 of ETS 300 175-7 [4].

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

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

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

User Authentication Key (UAK): secret authentication data contained within the subscriber's registration data. It is uniquely associated with the particular subscriber (user) and the subscription. The UAK is held in non-volatile memory within the PP (or within a detachable DECT Authentication Module (DAM)); see ETS 300 175-7 [4].

3.2 Abbreviations

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

AC	Allocation Code
ACM	Address Complete Message
ALS	Application Layer Structure
ARC	Access Right Class
ARD	Access Right Details
ARI	Access Right Identity
ASE	Application Service Entity
BCSM	Basic Call State Machine
BCUSM	Basic Call Unrelated State Machine
CCAF	Call Control Agent Function
CCF	Call Control Function
CFNR	Call Forwarding on No Reply
CLIR	Calling Line Identification Restriction
CS2	IN Capability Set No 2
CTM	Cordless Terminal Mobility
CTMid	CTM identity
CUCF	Call Unrelated Control Function
CUSF	Call Unrelated Service Function
DCK	Derived Cipher Key
DECT	Digital Enhanced Cordless Telecommunication
DN	Distinguished Name
DP	Detection Point
DSS1	Digital Subscriber Signalling System 1
EN	European Norm
FE	Functional Entity
FSM	Finite State Machine
FP	Fixed Part
FT	Fixed Termination
GAP	Generic Access Profile
GFP	Generic Functional Protocol
GFT	Generic Functional Transport
GTAI	Global Title Address Indicator
IAM	Initial Address Message
IPEI	International Portable Equipment Identity
IPUI	International Portable User Identity
IN	Intelligent Network
INAP	IN Application Protocol
ISUP	ISDN User Part
LA	Location Area
LAL	Location Area Level
LCE	Link Control Entity
LE	Local Exchange
MCID	Malicious Call IDentification
MM	Mobility Management
MMF	Mobility Management Function
MSC	Message Sequence Chart
NCICS	Networked Call Independent Connection-Oriented Signalling
NFE	Network Facility Extension
OCB	Outgoing Call Barrity
PARK	Portable Access Right Key

PID	Process Instance Identifier
PLI	PARK Length Indicator
PP	Portable Part
PT	Portable Terminal
PUN	Portable User Number
PUT	Portable User Type
RAND	RANdOm challenge
RES	RESponse
RFPI	Radio Fixed Part Identity
RS	a value used to establish authentication session keys
SACF	Single Association Control Function
SCCP	Signalling Connection Control Part
SCF	Service Control Function
SCFmm	SCF mobility management
SCFmmHome	SCF mobility management Home
SCFmmVisited	SCF mobility management Visited
SCFsl	SCF service logic
SCFslHome	SCF service logic Home
SCFslVisited	SCF service logic Visited
SCP	Service Control Point
SDF	Service Data Function
SDFmm	Service Data Function mobility management
SDFsl	Service Data Function service logic
SDL	Specification Description Language
SDP	Service Data Point
SLPI	Service Logic Program Instance
SMF	Service Management Function
SSF	Service Switching Function
SSI	Service to Service Information
SSP	Service Switching Point
ST	"end of address" delimiter Sending Termination
STUI	Service To User Information
TCAP	Transaction Capabilities Application Protocol
TDP	Trigger Detection Point
TMN	Telecommunications Management Network
UAK	User Authentication Key
USI	User to Service Information
UTSI	User To Service Information

4 General

In this stage 3 description it is considered to separate the mobility management from the service control function. In this respect the SCF mobility management (SCFmm) (Visited and Home) handles the Mobility Management (MM) procedures in connection with the Call Unrelated Service Function (CUSF), and the SCF service logic (SCFsl) (Visited and Home) handles the Call Control (e.g. provide roaming number) and CTM supplementary services (e.g. CTM-CLIR, CTM-MCID) in connection with the Service Switching Function (SSF).

To optimize the hierarchical distribution of location information and authentication data across 3 levels (see figure 1), it should be noted that in the figure the SCFmm to SDFsl and SCFsl and SDFmm interface are not required. For optimizing the hierarchical distribution of mobility management and Call Control information, it should be noted that for phase 1 SDFmm (Visited and Home) and SDFsl (Visited and Home) are assumed to be located in one node (SDFv and SDFh), and that SCFmm (Visited and Home) and SCFsl (Visited and Home) are assumed to be located in one node (SCFv and SCFh).

4A Proposed functional models for the CTM procedures

Figures 2, 3 and 4 propose the functional model for the CTM mobility management (see figure 2), outgoing CTM call (see figure 3) and incoming CTM call (see figure 4).

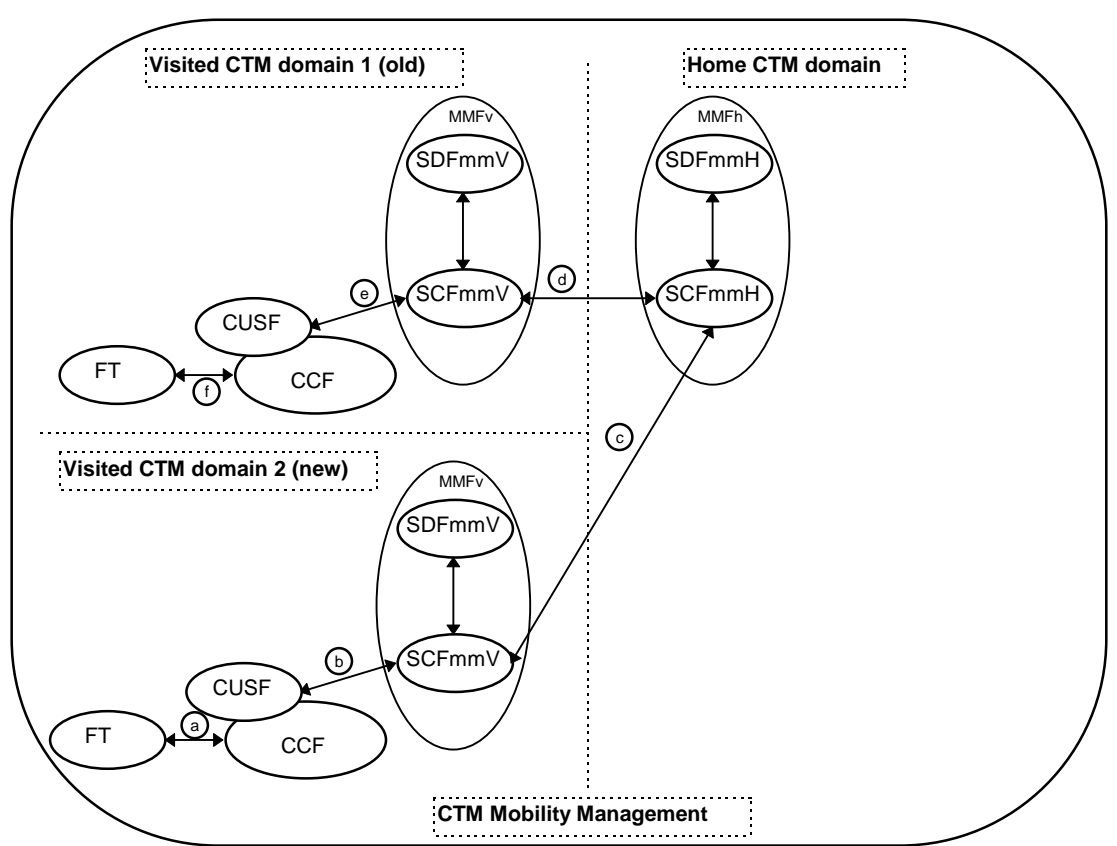


Figure 2: CTM mobility management functional domains

The following procedures are examples of the use of the indicated interfaces:

- NCICS connection with CTM mobility management information (e.g. location registration).
- User to Service Information (USI) mechanism containing CTM mobility management information (e.g. location registration).
- Static triggering (e.g. subscription registration) or triggering based on International Portable User Identity (IPUI) (e.g. location update), Service to Service Information (SSI) mechanism containing CTM mobility management information.
- Triggering of SCFmmVisited by SCFmmHome, SSI mechanism containing CTM mobility management information (e.g. location cancellation).
- USI mechanism containing CTM mobility management information (e.g. location cancellation).
- NCICS connection with CTM mobility management information (e.g. location cancellation).

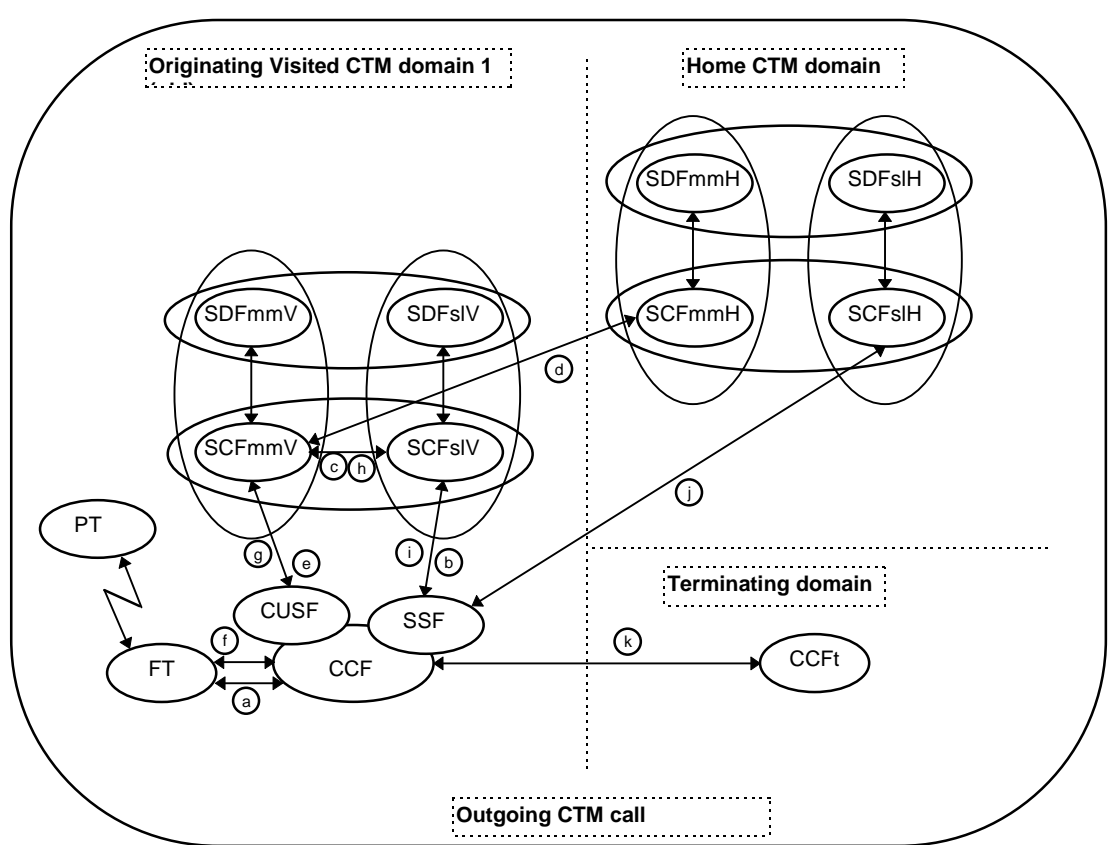


Figure 3: Outgoing CTM call functional domains

Detection and handling of emergency call setup will be completely handled in the SCFmmVisited.

The following procedures are examples of the use of the indicated interfaces:

- a) call setup;
- b) line base triggering;
- c) (optionally) initiation of authentication and/or ciphering procedures;
- d) fetching and reception of authentication data (SSI mechanism);
- e) authentication and/or ciphering, initiated by SCFmmVisited (USI mechanism);
- f) authentication and/or ciphering procedures and the result;
- g) result of authentication and/or ciphering;
- h) (optionally) action on the call setup based on the result of authentication;
- i) subsequent triggering initiated by SCFsIVvisited;
- j) triggering of SCFsIHome based on SCFid and check of CTM supplementary services, (see note 1);
- k) call establishment to the CTM user.

NOTE: Interface j1/j2 can be used in an inter-network case, interface j can be used in an intra-network case.

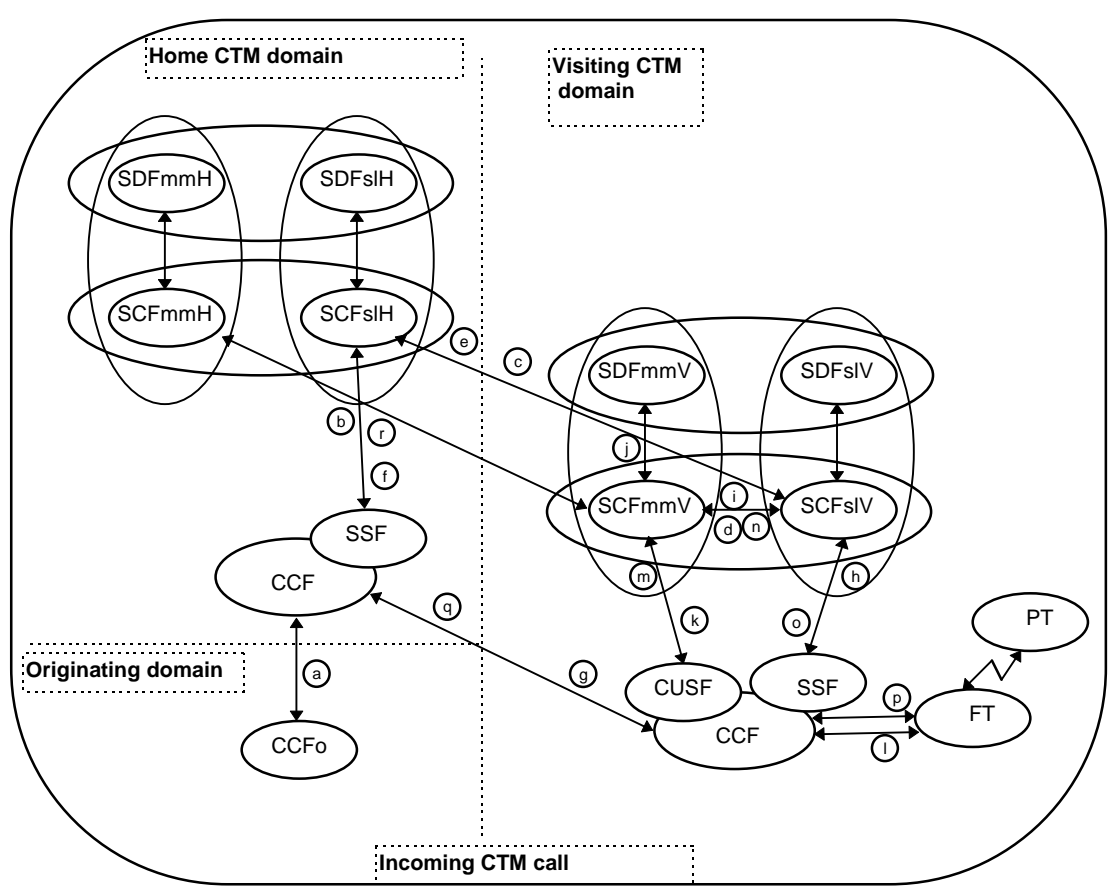


Figure 4: Incoming CTM call functional domains

For the incoming call procedure only the roaming number case is used.

The following procedures are examples of the use of the indicated interfaces:

- a) CTM call setup to CTM user using CTM-number;
- b) triggering based on CTM-number;
- c) request roaming number (SSI mechanism);
- d) (optionally) fetching of user status (e.g. not_reachable);
- e) roaming number and user status provided (SSI mechanism);
- f) call establishment to CTM user using roaming number;
- g) call setup to visiting domain using roaming number;
- h) triggering of SCFsIVisited;
- i) (optionally) initiation of authentication and/or ciphering procedures;
- j) fetching and reception of authentication data;
- k) authentication and/or ciphering procedures, initiated by SCFmmVisited;
- l) authentication and/or ciphering procedures, and result;
- m) report of authentication and/or ciphering to SCFmmVisited;
- n) (optionally) action on call setup based on result of authentication and/or ciphering;
- o) call establishment to CTM user;

- p) call setup to FT;
- q) report of call setup;
- r) report of events to SCFslHome to check CTM supplementary services.

A CTM user to CTM user call shall be a combination of a CTM outgoing call and a CTM incoming call, as they are presented in the figures.

5 CTM procedures

5.1 Model

The SDL model of the CTM network is included to the present document as an informative part of the standard in annex C. This subclause provides a short introduction to the SDL model.

The SDL diagrams reflect an Application Layer Structure (ALS) where the SACF performs the association co-ordination function.

The Visited SCF has four Application Service Entities (ASEs) namely:

- SCFVis, having process type SCF_SSF_CUSF_ASE_Visited, for communication with the SSF / CUSF in the Visited Domain.
- SCFmmVisApp, having process type SCFmmVisitedApplication, performing the service logic for the CTM Phase 1 mobility management call unrelated applications in the Visited SCF Domain.
- SCFslVisApp, having process type SCFslVisitedApplication, performing the service logic for the CTM Phase 1 call related applications in the Visited SCF Domain.
- SCF_SCFVis, having process type SCF_SCF_ASE_Visited, for communication with the SCF in the Home Domain.

The Home Domain SCF has four Application Service Entities (ASEs) namely:

- SCFHom, having process type SCF_SSF_CUSF_ASE_Home, for communication with the SSF / CUSF in the Home Domain.
- SCFmmHomApp, having process type SCFmmHomeApplication, performing the service logic for the CTM Phase 1 mobility management call unrelated applications in the Home SCF Domain.
- SCFslHomApp, having process type SCFslHomeApplication, performing the service logic for the CTM Phase 1 call related applications in the Home SCF Domain.
- SCF_SCFHom, having process type SCF_SCF_ASE_Home, for communication with the SCF in the Visited Domain.

The SCFHom and SCFVis ASEs communicate with the TCAP adaptors for the CUSF and SSF entities, while the SCF_SCFHom and SCF_SCFVis communicate with the TCAP adaptors for the peer SCF entities.

The association instance for the SCFHom and SCFVis is identified by either the cUSFdialogueID for call unrelated CUSF communication or by the sSFdialogue for call related SSF communication.

The association instance for the SCF_SCFHom and SCF_SCFVis is identified by the sCFdialogueID for communication with the peer SCF entity. The association instance for the SCFmmVisApp and SCFmmHomApp is identified by the mMdialogueID while for the SCFslVisApp and SCFslHomApp is identified by the sLdialogueID.

During one dialogue unique invoke identifiers are generated. They are obtained by calling a GetInvokeID procedure within the send signal parameter e.g. ContinueAssociationRequest((call GetInvokeID), cUSFdialogueID, conaArg).

The communication of the ASEs performing the transport functions via the SACF are given by the appropriate signal name e.g. RequestReportBCUSMEvent for the invoke component, by RequestReportBCUSMEventRes for the return result component and by RequestReportBCUSMEventErr for the return error component.

The association instances for the SCFmmVisApp, SCFmmHomApp, SCFslVisApp and SCFslHomApp ASEs are identified by the Process Instance Identifiers (PID).

Since the signals sent from or received by the transport ASEs by/from the application processes are not unique due to the fact that:

- relaying of signals from the SCFHome occur in the SCFVisited SACF; and
- embedded procedures are invoked for the same entity,

it is required that different dialogue identifiers are used. In this respect a qualifier will indicate the nesting which has occurred e.g. cUSFdialogueID.

For the ASEs the creation of an application process instance is initiated by sending a CreateASE signal with a parameter indicating the process which is addressed e.g. SCFmmVisApp. The processes addressed are indicated by a parameter value having the type:

```
TypeOfASE ::= ENUMERATED {
-- Indicates the type of ASE to be created by SACF
  SCFmmVisApp,
  SCF_SCFVis,
  SCFmmHomApp,
  SCF_SCFHom,
  SCFVis,
  SCFHom
}
```

The process instances are terminated by sending an ASETerminated(x)signal, where x designates the TypeOfASE e.g. SCFmmVisApp.

For the TCAP simulator the signal ApplicationBegin and ApplicationEnd are used.

5.2 Addressing

5.2.1 General

Each network physical entity (e.g. SCP, SDP, SSP, IP, Portable radio Termination (PT)) shall be allocated addresses to open dialogues or continue dialogues.

Addressing a functional entity (i.e. SCF) should be understood as addressing the physical entity which contains this Functional Entity (FE).

- The FEs may be at physically separate locations.
- Two or more FEs may be at the same location.
- The FE load could be shared between two or more different physically locations or a FE could have a back-up.
- Addressing of the correct FE shall be supported both in intra-domain or in inter-domain case.

Each functional entity for CTM shall be identified by a unique number. This forms the GTAI part of the global title. The unique number means this is a number that is not used by any other application.

The format and coding of address parameters carried by the SCCP shall comply with ETS 300 009-1 [5] with the following restrictions:

In case of inter-network addressing, the format and coding of address parameters carried by the SCCP across network boundaries shall comply with the following rules:

a) Called Party Address:

- SSN indicator = 1 (IN SSN always included);
- Global title indicator = 0100 (Global title includes translation type, numbering plan, encoding scheme and nature of address indicator);
- the translation type field will be coded "00000000" (Not used);
- Routeing indicator = 0 (Routeing on global title);

b) Calling Party Address:

- SSN indicator = 1 (IN SSN always included);
- Point code indicator = 0;
- Global title indicator = 0100 (Global title includes translation type, numbering plan, encoding scheme and nature of address indicator);
- the translation type field will be coded "00000000" (Not used);
- Routeing indicator = 0 (Routeing on Global Title).

If a global title translation is required for obtaining routeing information, one of the numbering plans ITU-T Recommendation E.164 [3] or ITU-T Recommendation E.214 [7] is applicable.

Either numbering plans E.164 or E.214 may be used in both the calling party address and the called party address of SCCP messages at any stage of a dialogue. The ITU-T Recommendation E.212 [6] numbering plan may only be used in SCCP primitives invoked at the originating node.

As stated in EN 301 140-1 [1], when load sharing or backup procedures are implemented, a responding application is responsible for providing an appropriate responding address in the first backward message it sends for a dialogue. This address shall uniquely identify the node where this application resides.

5.2.2 Addressing the SCF

There are several cases where an SCF has to be addressed. In case of SCF-SCF relation the SCCP address (Global Titles (GT) field) of an assisting SCF is retrieved from the SCFhome by the controlling SCF. This information is used as a global title.

5.2.2.1 During incoming call set-up

When a call is initiated, user related information shall be retrieved from the SCFhome. The criteria for non-geographical numbering plan to access the SCFhome is based on the B number analysis of the CTM number and performed by the O-BCSM. For the geographical numbering plan the triggering of the SCFhome shall be performed via a triggering table associated to the CTM number and done by a line based triggering of the T-BCSM. In order to address the SCFhome, the CTM number is used to be translated to a Global Title. Based on the IPUI the SCFhome shall obtain the roaming number and the user status (e.g. not reachable) from the SCFvisited. The SCFhome shall instruct the SSF by sending a connect operation to route the call to the visited domain based on this roaming number.

5.2.2.2 At location registration

When a CTM user registers for the first time in an area, the SCFvisited has to initiate the modification of location information in the SCFhome.

The only data for addressing the SCFhome is contained in the CTMid part of the IPUI, and addressing information for SCCP has to be derived from it. This means that the SCFvisited has to be able to address the SCFhome based:

- on an E.214 mobile global title originally derived by the SCFvisited from the CTMid; or
- on an E.164 SCF address; or
- in the case of intra-IN domain signalling, on an SPC.

The SCFvisited requests the SCFhome to update its database with its SCFvisited address.

5.2.2.3 At outgoing call set-up

The SCFvisited needs to be interrogated with the trigger criteria for DP-originating-attempt set to CTM-specific.

For accessing the user profile triggering will be based on a trigger in the O-BCSM on DP_analyzed_information. The SCFid is derived from the CTMid part of the IPUI in order to address the SCFhome using the TC global title routing and is put into the SCFid, and the CTM number is used for addressing the service profile in the SCFhome.

5.3 Subscription registration in SCFmmSubscription

An example for this procedure can be found in clause A.1.

5.3.1 Procedure description

5.3.1.1 Introduction

This procedure allows the CTM user to get his subscription data (IPUI and Portable Access Right Key (PARK)) from a dedicated SCF, called SCFmmSubscription. Since more than one SCFmmSubscription can exist in a network, the addressing of the appropriate SCFmmSubscription shall be defined by command in each SCFmmVisited.

Two options are defined for searching the IPUI/PARK pair:

- 1) based on the IPEI. Such IPEI shall be known in advance by the operator (when the CTM user takes his/her subscription);
- 2) based on the generated authentication data. Precalculated sets of authentication data are used to find the CTM user by initiating a terminal authentication and comparing the terminal authentication result with the precalculated authentication result.

5.3.1.2 Normal operation

In order to obtain the subscription data from the SCFmmSubscription, the SCFmmVisited shall send a cTMAccessRightsRequestSCF invoke component to the SCFmmSubscription by using the SSI mechanism of the SCF-SCF interface.

The following parameters have to be included:

- IPEI, identifying the equipment identity and only used in option 1;
- cTMAuthType, indicating the authentication algorithm (DSSA), the authentication key type (AC or UAK) and the authentication key number;
- cTMPortableCapabilities, to convey the cordless terminal's capabilities (tone, display, etc.).

If both the terminal authentication (initiated by either SCFmmVisited or SCFmmSubscription) and the ciphering procedures (optional procedures) are successful, and if the network authentication (initiated by the PP) is successful, then the SCFmmSubscription shall send a cTMAccessRightsRequestSCF return result component to the SCFmmVisited, using the SSI mechanism of the SCF-SCF interface with the following parameters:

- iPUI, containing the newly assigned identity of the cordless terminal;
- cTMFixedIdentity, indicating the type (PARK), the AccessRightClass (ARC), the AccessRightDetails (ARD), and the length of the identity;
- cTMServiceClass (optional), indicating the service class of the cordless terminal.

5.3.1.3 Exceptional procedure

If the SCFmmSubscription is not able to perform a subscription registration, it shall send a cTMAccessRightsRequestSCF return error component to the SCFmmVisited, using the SSI mechanism of the SCF-SCF interface with the following error values:

- portableIdentityUnknown, if the identity of the cordless terminal (IPEI), for which the request has been initiated, is not known by the SCFmmVisited;
- unspecified, if the requested procedure fails for any other reason.

5.3.2 SDL application procedures

No normative SDL application procedures are given. For an informative model see annex C.

5.4 Key allocation

In case of a subscription registration procedure, SCFmmSubscription may optionally initiate a ciphering procedure.

The cTMCiphering invoke, return result and return error are imported from the DSS1 protocol specification; see EN 301 144-1 [2], clause "Invocation and operation", subclause "User initiated ciphering".

The cTMCiphering invoke component sent by SCFmmSubscription using the SSI mechanism over the SCF-SCF interface to SCFmmVisited will be transferred transparently by SCFmmVisited over the CUSF-SCF interface using the USI mechanism.

5.5 Subscription deregistration

An example for the procedure can be found in clause A.2.

The cTMAccessRightsTerminate invoke, return result and return error are imported from the DSS1 protocol specification (see EN 301 144-1 [2], clause "Registration and deregistration", subclause "Subscription deregistration").

When a subscription is removed to a CTM user, SCFmmHome initiates a cTMAccessRightsTerminate invoke component to SCFmmVisited using the SSI mechanism over the SCF-SCF interface. The invoke component is transferred transparently to the CUSF via the USI mechanism over the SCF-CUSF interface.

5.6 Network authentication

In case of both the subscription registration and subscription deregistration procedures, the PP may initiate a network authentication. It should be noted that the cordless terminal may invoke the network authentication procedure at any time, to verify that the identity provided by the network is the one claimed. See also clause A.10 for an example for the Network authentication procedure.

The `cTMNetworkAuthentication` invoke, return result and return error are imported from the DSS1 protocol specification (see EN 301 144-1 [2], clause "Invocation and operation" subclause "Network authentication").

The `cTMNetworkAuthentication` invoke component received by `SCFmmVisited` over the CUSF-SCF interface using the USI mechanism is transferred transparently to `SCFmmHome` using the SSI mechanism over the SCF-SCF interface.

5.7 Terminal authentication

In case of a subscription registration procedure, `SCFmmSubscription` may optionally initiate a Terminal Authentication.

The `cTMTerminalAuthentication` invoke, return result and return error are imported from the DSS1 protocol specification (see EN 301 144-1 [2], clause "Invocation and operation" subclause "Terminal authentication").

The `cTMTerminalAuthentication` invoke component sent by `SCFmmSubscription` using the SSI mechanism over the SCF-SCF interface to `SCFmmVisited` will be transferred transparently by `SCFmmVisited` over the CUSF-SCF interface using the USI mechanism.

5.8 Network initiated ciphering

In case of a subscription registration procedure, `SCFmmSubscription` may optionally initiate a ciphering procedure.

The `cTMCiphering` invoke, return result and return error are imported from the DSS1 protocol specification; see EN 301 144-1 [2], clause "Invocation and operation" subclause "User initiated ciphering".

The `cTMCiphering` invoke component sent by `SCFmmSubscription` using the SSI mechanism over the SCF-SCF interface to `SCFmmVisited` will be transferred transparently by `SCFmmVisited` over the CUSF-SCF interface using the USI mechanism.

5.9 Location registration in the SCFmmVisited

An example for the procedure can be found in clause A.3.

The `cTMLocationRegistration` invoke, return result and return error are imported from the DSS1 protocol specification (see EN 301 144-1 [2], clause "Activation and deactivation", subclause "Location registration").

5.10 Location update in the SCFmmHome

An example for the procedure can be found in clause A.4.

5.10.1 Procedure description

5.10.1.1 Introduction

The CTM 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. The location update procedure shall provide during a location registration procedure in order to update the home domain and to check whether the CTM user is allowed to roam in the visited domain.

5.10.1.2 Normal operation

Location update procedure is used to make the cordless terminal location known to the network when a cordless terminal is roaming from a defined location area to a new one.

The SCFmmVisited shall translate the PUN part of the cTMPortableIdentity (E.212 number) received during the location registration procedure into a "mobile global title" (E.214 number) and may store it as sCFmmHomeID.

NOTE: The SCFmmHomeID is used later during the outgoing call procedure in order that the SCFmmVisited can initiate a subsequent triggering of the SCFmmHome for checking the outgoing CTM supplementary services.

In order to make the cordless terminal location known to the SCFmmHome and to perform a location update procedure, the SCFmmVisited shall send a cTMLocationUpdateSCF invoke component by using the SSI mechanism of the SCF-SCF interface.

The following parameters shall be included:

- iPUI, indicating the identity of the cordless terminal;
- sCFmmVisitedID, containing the global title of the SCFmmVisited to be addressed by the SCFmmHome.

On receiving the cTMLocationUpdateSCF invoke component, the SCFmmHome shall use the received parameters to perform the location update procedure.

Before sending the cTMLocationRegistrationSCF return result component to the SCFmmVisited, the SCFmmHome shall initiate one or more of the following procedures:

- the SCFmmHome shall check whether the CTM user is allowed to roam into the SCFmmVisited area;
- the SCFmmHome shall check whether the CTM user was previously registered in another SCFmmVisited. If registered the SCFmmHome shall initiate a location cancellation procedure in old SCFmm Visited.

The SCFmmHome having concluded that the CTM user is allowed to roam into the visited domain the location update procedure shall send a CTMLocationUpdateSCF return result component to the SCFmmVisited, by using the using the SSI mechanism of the SCF-SCF interface.

The following parameters shall be included:

- cTMNumber, indicating the E.164 number that uniquely and unambiguously identifies the CTM subscriber;
- cTMFixedIdentity, containing the PARK.

5.10.1.3 Exceptional procedure

If the CTM user is not allowed to roam into the SCFmmVisited, the SCFmmHome shall send a CTMLocationUpdateSCF return error component to SCFmmVisited, by using the SSI mechanism of the SCF-SCF interface, indicating one of the following error values:

- portableIdentityUnknown, if the identity of the cordless terminal, for which the request has been initiated, is not known to the home network;
- cTMDataMissing, if the network cannot provide the security data due to unavailability of the information;
- cTMRoamingNotAllowed, if the user of the cordless terminal is not allowed to roam in the visited network;
- unspecified, if the requested procedure fails for any other reason.

If the SCFmmVisited receives a reject component from the SCFmmHome it shall close the association for location registration.

If during the location registration procedure a release association is received from the CTM user or the FT, this event may be reported to the SCFmmVisited by arming the EDP-R "AssociationReleaseRequested" Basic Call Unrelated State Machine (BCUSM) Event. The arming is performed by means of an RequestReportBCUSMEvent operation and the reporting is performed by means of the eventReportBCUSM operation. The "CTM-user / FT release" shall not be reported to the SCFmmHome and shall close the association for location registration.

5.10.2 SDL application procedures

No normative SDL application procedures are given. For an informative model see annex C.

5.11 Location cancellation in SCFmmVisited

An example for the procedure can be found in clause A.5.

The cTMLocationCancellation invoke, return result and return error are imported from the DSS1 protocol specification (see EN 301 144-1 [2], clause "Activation and deactivation", subclause "Location cancellation").

When the SCFmmHome initiates a cTMLocationCancellation invoke component to SCFmmVisited using the SSI mechanism over the SCF-SCF interface, the invoke component is transferred transparently by SCFmmVisited to CUSF via the USI mechanism over the SCF-CUSF interface.

5.12 Location cancellation in the FT

An example for the procedure can be found in clause A.6.

The cTMLocationCancellation invoke, return result and return error are imported from the DSS1 protocol specification (see EN 301 144-1 [2], clause "Activation and deactivation", subclause "Location cancellation").

5.13 Restoration of location data in the SCFmmHome

An example for the procedure can be found in clause A.8.

5.13.1 Procedure description

5.13.1.1 Introduction

This procedure allows the SCFmmHome to restore the location information for all CTM users belonging to it when this data is corrupted.

5.13.1.2 Normal operation

- 1) The SCFmmHome has a table of all the SCFmmVisited addresses where the CTM users may roam. If the location data gets corrupted in the SCFmmHome e.g. after restart, the SCFmmHome shall send a message to all SCFmmVisited by means of a cTMRestoreDataSCF invoke component using the SSI mechanism over the SCF-SCF interface. This invoke component indicates to the addressed SCFmmVisited that the restoration of location data in the SCFmmHome shall take place and shall have the sCFmmHomeId parameter.
- 2) Each SCFmmVisited, on receipt of the cTMRestoreDataSCF invoke component shall mark <restoration of location info in SCFmmHome required> for all CTM users belonging to that SCFmmHome. To find all CTM users, the SCFmmVisited shall compare the SCFmmHomeId stored at the location update result procedure in the SCFmmVisited with the one received in the restoration of location data procedure.
- 3) When the CTM user performs an "Outgoing call" procedure or a "location registration in the SCFmmVisited" procedure, the SCFmmVisited shall initiate a "location update in the SCFmmHome" procedure and shall set mark <restoration of location info in SCFmmHome not required>. This option implies that CTM users will not be reachable until either they initiate an outgoing call or perform a location registration.

5.13.1.3 Exceptional procedure

No return result is expected for this procedure, since action on the reception of the cTMRestoreDataSCF invoke component will be performed later (only at CTM outgoing call and location registration).

No return error is expected for this procedure, since SCFmmHome is in an unstable situation.

5.13.2 SDL application procedures

No normative SDL application procedures are given. For an informative model see annex C.

5.14 Terminal authentication and/or ciphering

An example for the procedures can be found in clause A.9.

The cTMTerminalAuthentication and cTMCiphering invoke, return result and return error are imported from the DSS1 protocol specification (see EN 301 144-1 [2], clause "Invocation and operation", subclause "Terminal authentication and network initiated ciphering").

5.15 Download of security data

An example for the procedure can be found in clause A.7.

5.15.1 Procedure description

5.15.1.1 Introduction

The authentication and the ciphering procedures shall always be processed by an independent dialogue using the call unrelated concept and shall always be performed by the SCFmmVisited (see note).

Terminal authentication and/or ciphering procedures shall be able to be initiated in the following cases:

- CTM outgoing call;
- CTM incoming call;
- location registration procedure;
- subscription registration procedure.

Network authentication procedure shall be able to be initiated in the following cases:

- subscription registration procedure;
- subscription deregistration procedure.

For the ciphering and authentication the updating shall be performed by an independent procedure where e.g. a set of pre-calculated quadruplet values is transferred independently from the call set-up procedures where a set of quadruplet instances will be consumed when the ciphering and authentication procedures are invoked.

The terminal authentication and/or ciphering procedures may be processed in parallel or in series with the call set-up. In case the ciphering procedure is done in parallel, the dialled digits may not be ciphered. In case the ciphering procedure is done in series, the old Derived Cipher Key (DCK) may be used.

Since two independent procedures for terminal authentication / ciphering and call set-up are done, co-ordination has to be performed in the SCFmmVisited using the CTMid (part of the IPU). For example, if the authentication failed, the call related part shall be released.

The terminal authentication result (if ignored) will be ignored in case of an emergency call.

NOTE: In case of subscription registration procedure, as an option it may be possible to be initiated from the SCFmmSubscription instead of SCFmmVisited.

5.15.1.2 Normal operation

In order to obtain the security data for authentication and ciphering from the SCFmmHome, the SCFmmVisited shall send a cTMProvideSecurityDataSCF invoke component by using the SSI mechanism of the SCF-SCF interface.

The following parameter shall be included:

- CTMid (part of the IPU), indicating the identity of the cordless terminal.

The SCFmmHome on receipt of the cTMProvideSecurityDataSCF invoke component shall retrieve a number of sets of authentication and optionally ciphering data from SCFmmHome and shall send to the SCFmmVisited an cTMProvideSecurityDataSCF return result component using the SSI mechanism of the SCF-SCF interface.

The following parameter shall be included:

- securityDataSets, containing the number or sets {RAND, RS, XRES1, DCK, cTMAuthType) that have been generated.

5.15.1.3 Exceptional procedure

If the provide security data procedure fails, the SCFmmHome shall send a cTMProvideSecurityDataSCF return error component to the SCFmmVisited, by using the SSI mechanism of the SCF-SCF interface, indicating one of the following error values:

- portableIdentityUnknown, if the identity of the cordless terminal for which the request has been initiated is not known;
- unspecified, if the requested procedure fails for any other reason.

5.15.2 SDL application procedures

No normative SDL application procedures are given. For an informative model see annex C.

5.16 Provide roaming number

An example for the procedure can be found in clause B.2.

5.16.1 Procedure description

5.16.1.1 Introduction

This procedure shall allow the SCFsIHome to retrieve during an incoming call the roaming number of the CTM dialled subscriber in the SSFsIVisited.

For the CTM incoming call the originating party dials the directory number of a mobile terminal (CTM number).

If the CTM number is a non-geographical number the call shall be routed to the nearest SSF of the calling party.

If a CTM number is a geographical number the call shall be routed to the Call Control Function (CCF) / SSFHome.

The SSF shall trigger the SCFsI in the home domain. The SCFsIHome shall retrieve the address of the visited SCFmm. With the obtained SCFmm address, the SCFsIHome shall request the SCFsIVisited for the roaming number.

The SCFslVisited shall check if the subscriber is registered and reachable, shall select a roaming number, shall make an association between the retrieved roaming number and the IPUI, shall start a timer for the supervision of the use of the roaming number, and shall return the roaming number to the SCFslHome.

The SCFslHome shall instruct the originating SSF to route the call with the obtained number by e.g. ISUP procedures to the visited CCF/SSF, where the call is triggered.

The visited SSF shall query the SCFslVisited based on the roaming number in order to get the FT address and the IPUI/PARK. The SCFslVisited shall release the roaming number, stop the supervision timer and shall ask the visited CCF/SSF to route the call towards the identified FT. The FT shall then page the PT.

5.16.1.2 Normal operation

The SCFslHome shall request for a roaming number in the SCFslVisited, by sending a cTMProvideRoamingNumberSCF invoke component by using the SSI mechanism of the SCF-SCF interface.

The following parameter shall be included:

- IPUI, indicating the identity of the cordless terminal.

If the CTM user is registered in the SCFslVisited, the SCFslVisited shall return the CTMProvideRoamingNumber return result component using the SSI mechanism of the SCF-SCF interface having the following parameters:

- roamingNumber, containing the roaming number to be used for routing in the ISUP to the visited CCF/SSF;
- userStatus, set to userReachable.

If the CTM user is not registered in the SCFslVisited, the SCFslVisited shall return the cTMProvideRoamingNumberSCF return result component using the SSI mechanism of the SCF-SCF interface having the following parameter:

- userStatus, set to userNotReachable or userUnknown.

The SCFsl can execute the CTM supplementary service CFNRc, if active for the user.

5.16.1.3 Exceptional procedure

If the provide roaming number procedure fails, the SCFslVisited shall send a cTMProvideRoamingNumberSCF return error component to the SCFslHome, by using the SSI mechanism of the SCF-SCF interface, indicating one of the following error values:

- cTMFacilityNotSupported;
- cTMNoRoamingNumberAvailable;
- portableIdentityUnknown, if the identity of the cordless terminal, for which the request has been initiated, is not known to the visited network;
- unspecified, if the requested procedure fails for any other reason.

5.16.2 SDL application procedures

No normative SDL application procedures are given. For an informative model see annex C.

6 Extensions of INAP

6.1 SCF-SCF service to service extensions

6.1.1 ASN.1 module

6.1.2 Data types

```

SSI-SCF-SCF-datatypes {ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) modules(1)
datatypes(25) version1(0)}

DEFINITIONS ::=

BEGIN

IMPORTS
    SSI-PARAMETERS-BOUND,
FROM SSI-SCF-SCF-classes {ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3)
modules(1) classes (22) version1(0)}

STSIInformation {SSI-PARAMETERS-BOUND : SSI-bound} ::= OCTET STRING (SIZE (
    SSI-bound.&minSSIInformationLength..SSI-bound.&maxSSIInformationLength))

-- The STSIInformation contains the service information associated with the
agreementFeatureIndicator. provided by the
-- Service Logic of the invoking SCF to be transferred to the Service Logic of the responding SCF.s
-- For USI-SSI interworking the maxUSIInformationLength and the maxSSIInformationLength shall be the
same.
-- The maximum of those values are depending also on the used TCAP version.
AgreementFeatureIndicator {SSI-PARAMETERS-BOUND : SSI-bound} ::= CHOICE {
    global OBJECT IDENTIFIER,
    local OCTET STRING (SIZE (
        SSI-bound.&minAgreementFeatureIndicatorLength..
        SSI-bound.&maxAgreementFeatureIndicatorLength))
    }

--This AgreementFeatureIndicator indicates the service application for which the Seville data is to
be provided.

END

```

6.1.3 Error types

-- No new error types are defined for SSI SCF-SCF in addition to CS2.

6.1.4 Operation codes

```

SSI-SCF-SCF-operationcodes {ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3)
modules(1) operationcodes(21) version1(0)}

DEFINITIONS ::=

BEGIN

IMPORTS
    Code
FROM Remote-Operations-Information-Objects ros-InformationObjects

ros-InformationObjects FROM IN-CS2-object-identifiers
    { ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-network(1) CS-2(20) modules(0)
in-cs2-object-identifiers(17) version1(0) }

-- SCF/SCF interface including transferSTSI

opcode- transferSTSI          Code ::= local : 200

END

```

6.1.5 Error codes

-- No new error codes are to be defined SSI SCF-SCF.

6.1.6 Classes

```
SSI-SCF-SCF-classes {ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) modules(1)
classes (22) version1(0)}
DEFINITIONS ::=
BEGIN

SSI-PARAMETERS-BOUND ::= CLASS
{
    &minSTSIInformationLength      INTEGER,
    &maxSTSIInformationLength      INTEGER,
    -- The maxSTSIInformationLength and shall not exceed the maximum value allowed such that the
    -- STSIInformation can be transferred by the used TCAP.
    &minAgreementFeatureIndicatorLength  INTEGER,
    &maxAgreementFeatureIndicatorLength  INTEGER

WITH SYNTAX
{
    MINIMUM-FOR-STSI-INFORMATION      &minSTSIInformationLength
    MAXIMUM-FOR-STSI-INFORMATION      &maxSTSIInformationLength
    MINIMUM-FOR-AGREEMENT-INDICATOR  &minAgreementFeatureIndicatorLength
    MAXIMUM-FOR-AGREEMENT-INDICATOR  &maxAgreementFeatureIndicatorLength

-- The following instance of the parameter bound is just an example
sSI-networkSpecificBoundSet SSI-PARAMETERS-BOUND ::= {
    MINIMUM-FOR-STSI-INFORMATION      1
    MAXIMUM-FOR-STSI-INFORMATION      4
    MINIMUM-FOR-AGREEMENT-INDICATOR  1
    MAXIMUM-FOR-AGREEMENT-INDICATOR  2
}
END
```

6.1.7 Object identifiers

```
SSI-SCF-SCF-object-identifiers {ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3)
modules(1) object-identifiers(20) version1(0)}
DEFINITIONS ::=
BEGIN
-- This module assigns object identifiers for SSI SCF-SCF interface

-- For SSI-SCF-SCF Modules
sSI-SCF-SCF-datatypes      OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) modules(1) datatypes(25)
version1(0)}
sSI-SCF-SCF-operationcodes OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) modules(1) operationcodes(21)
version1(0)}
sSI-SCF-SCF-classes       OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) modules(1) classes (22)
version1(0)}
sSI-SCF-SCF-Operations    OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) modules(1) ops_and_args(23)
version1(0)}
sSI-SCF-SCF-Protocol      OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) modules(1) sSI-SCF-SCF-pkgs-
contracts-ac(24) version1(0)}

-- SSI-SCF-SCF Application Context
id-ac-SSI-scf-scfOperationsAC OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) ac(3) 20 version1(0)}
-- SSI-SCF-SCF Contract
id-contract-SSI-scf-scf      OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) contract(26) 20 version1(0)}
-- SSI-SCF-SCF Operation Packages
id-package-transferSTSI     OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) package(27) 20 version1(0)}
-- SSI-SCF-SCF Abstract Syntaxes
id-as-SSI-scf-scfOperationsAS OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) as(5) 20 version1(0)}
END
```

6.1.8 Operations and arguments

```
-- SSI Specific CS2 operations and arguments
SSI-SCF-SCF-ops-args {ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3) modules(1)
ops-and-args(23) version1(0)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

    OPERATION, ERROR
FROM Remote-Operations-Information-Objects ros-InformationObjects
    SecurityParameters,
    securityError
FROM DirectoryAbstractService directoryAbstractService

    OPTIONALLY-PROTECTED{}
FROM EnhancedSecurity enhancedSecurity

    opcode-transferSTSI
FROM SSI-operationcodes sSI-SCF-SCF-operationcodes

    PARAMETERS-BOUND
FROM IN-CS2-classes classes

    SSI-PARAMETERS-BOUND,
FROM SSI-SCF-SCF-classes sSI-SCF-SCF-classes

    ExtensionField {}
FROM IN-CS2-datatypes datatypes

    AgreementFeatureIndicator {}
    STSIInformation {},
FROM SSI-SCF-SCF-datatypes sSI-SCF-SCF-datatypes

    missingParameter,
    parameterOutOfRange,
    systemFailure,
    unexpectedDataValue,
    unexpectedParameter,
FROM IN-CS2-errortypes errortypes

    scfTaskRefused,
    SCFQOP
FROM IN-CS2-SCF-SCF-ops-args scf-scf-Operations

    ros-InformationObjects, ds-UsefulDefinitions, classes, errortypes, datatypes,
    scf-scf-Operations
FROM IN-CS2-object-identifiers { ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-
network(1) CS-2(20) modules(0) in-cs2-object-identifiers(17) version1(0) }

    directoryAbstractService, enhancedSecurity
FROM UsefulDefinitions ds-UsefulDefinitions

    sSI-SCF-SCF-datatypes,
    sSI-SCF-SCF-operationcodes,
    sSI-SCF-SCF-classes
FROM SSI-SCF-SCF-object-identifiers {ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-
ctm(3) modules(1) object-identifiers(20) version1(0)}

transferSTSI {PARAMETERS-BOUND : bound, SSI-PARAMETERS-BOUND : SSI-bound} OPERATION ::= {
    ARGUMENT      TransferSTSIArg {bound, SSI-bound}
    RETURN RESULT FALSE
    ERRORS        {missingParameter |
                    systemFailure |
                    scfTaskRefused
                    unexpectedDataValue |
                    unexpectedParameter |
                    parameterOutOfRange |
                    securityError
                    }
    CODE          opcode-transferSTSI
}

-- Direction : controlling SCF -> supporting SCF (or IAF), or
-- supporting SCF (or IAF) -> controlling SCF, T imer T_tsi
-- This operation is used by the invoking SCF to request or report service information from / to the
responding SCF,

TransferSTSIArg {PARAMETERS-BOUND : bound, SSI-PARAMETERS-BOUND : SSI-bound} ::= OPTIONALLY-
PROTECTED {SEQUENCE {
    sSIInfo SSIInfo {SSI-bound},
```

```

securityParameters [2] SecurityParameters OPTIONAL,
extensions [3] SEQUENCE SIZE (1..bound.&numOfExtensions)
                OF ExtensionField {bound} OPTIONAL,
...
},
SCFQOP.&scfArgumentQOP{@scfqop}
}
}
SSInfo{SSI-PARAMETERS-BOUND : SSI-bound} ::= SEQUENCE {
  agreementFeatureIndicator [0]AgreementFeatureIndicator {SSI-bound} OPTIONAL,
  sTSIIInformation [1] STSIIInformation {SSI-bound}
}
}
END

```

The following value ranges do apply for operation specific timers in INAP:

short: 1 to 10 s

Table 1 below lists all operation timers and the value range for each timer. The definitive value for each operation timer may be network specific and has to be defined by the network operator.

Table 1

TransferSTSI	Tttsi	short
--------------	-------	-------

6.1.9 SSI-SCF-SCF interface

```

SSI-SCF-SCF-pkgs-contracts-acsc {ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-ctm(3)
modules(1) sSI-SCF-SCF-pkgs-contracts-acsc(24) version1(0)}

```

```

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

```

```

-- This module describes the operation-packages, contracts and application-contexts used
-- over the SCF-SCF interface for SSI.

```

```

IMPORTS

```

```

    PARAMETERS-BOUND,
    networkSpecificBoundSet
FROM IN-CS2-classes classes

```

```

    SSI-PARAMETERS-BOUND,
    sSI-networkSpecificBoundSet
FROM SSI-SCF-SCF-classes sSI-SCF-SCF-classes

```

```

    CONTRACT, OPERATION-PACKAGE, CONNECTION-PACKAGE, OPERATION
FROM Remote-Operations-Information-Objects ros-InformationObjects

```

```

    TCMessage {}
FROM TCAPMessages tc-Messages

```

```

    APPLICATION-CONTEXT, dialogue-abstract-syntax
FROM TC-Notation-Extensions tc-NotationExtensions

```

```

    establishChargingRecord {},
    confirmedReportChargingInformation {},
    confirmedNotificationProvided {},
    handlingInformationRequest {},
    handlingInformationResult {},
    networkCapability {},
    notificationProvided {},
    provideUserInformation {},
    reportChargingInformation {},
    requestNotification {},
FROM IN-CS2-SCF-SCF-ops-args scf-scf-Operations

```

```

    transferSTSI {}
FROM SSI-SCF-SCF-ops-args sSI-SCF-SCF-operations

```

```

    ds-UsefulDefinitions,
    tc-Messages, tc-NotationExtensions,
    ros-InformationObjects,
    scf-scf-Operations, scf-scf-Protocol,
    ssf-scf-Operations, ssf-scf-Protocol

```

```

FROM IN-CS2-object-identifiers { ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-
network(1) CS-2(20) modules(0) in-cs2-object-identifiers(17) version1(0) }

```

```

sSI-SCF-SCF-classes,
sSI-SCF-SCF-operations,
id-ac-SSI-scf-scfOperationsAC
id-contract-SSI-scf-scf
id-package-transferSTSI
id-as-SSI-scf-scfOperationsAS
FROM SSI-SCF-SCF-object-identifiers {ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-
ctm(3) modules(1) object-identifiers(20) version1(0)}

activityTest
FROM IN-CS2-SSF-SCF-ops-args ssi-scf-Operations

activityTestPackage
FROM IN-CS2-SSF-SCF-pkgs-contracts-acs ssi-scf-Protocol

scf-scfConnectionPackage,
activityTestPackage,
chargingInformationPackage,
handlingInformationPackage
networkCapabilityPackage,
notificationPackage,
userInformationPackage
FROM IN-CS2-SCF-SCF-pkgs-contracts-acs scf-scf-Protocol
;

-- Contracts, Packages and Application Contexts

-- Application Context --

SSI-scf-scfOperationsAC APPLICATION-CONTEXT ::= {
CONTRACT          SSI-scf-scfContract
DIALOGUE MODE     structured
TERMINATION       basic
ABSTRACT SYNTAXES {dialogue-abstract-syntax |
                   SSI-scf-scfOperationsAbstractSyntax}
APPLICATION CONTEXT NAME      id-ac-SSI-scf-scfOperationsAC
}

-- Contract --

SSI-scf-scfContract CONTRACT ::= {
CONNECTION scf-scfConnectionPackage(networkSpecificBoundSet)
INITIATOR CONSUMER OF {
activityTestPackage |
handlingInformationPackage{networkSpecificBoundSet} |
transferSTSIPackage{networkSpecificBoundSet, sSI-networkSpecificBoundSet }
RESPONDER OF {
activityTestPackage |
handlingInformationPackage{networkSpecificBoundSet} |
chargingInformationPackage {networkSpecificBoundSet}|
networkCapabilityPackage {networkSpecificBoundSet}|
notificationPackage {networkSpecificBoundSet}|
userInformationPackage {networkSpecificBoundSet}
transferSTSIPackage{networkSpecificBoundSet, sSI-networkSpecificBoundSet }
ID id-contract-SSI-scf-scf
}

-- transferSTSI package --

transferSTSIPackage {PARAMETERS-BOUND : bound, SSI-PARAMETERS-BOUND : SSI-bound} OPERATION-PACKAGE
::= {
CONSUMER INVOKES {transferSTSI {bound, SSI-bound }}
SUPPLIER INVOKES {transferSTSI {bound, SSI-bound }}
ID id-package-transferSTSI
}

-- abstract syntaxes --

SSI-scf-scfOperationsAbstractSyntax ABSTRACT-SYNTAX ::= {
BasicSSI-SCF-SCF-PDUs
IDENTIFIED BY id-as-SSI-scf-scfOperationsAS}
BasicSSI-SCF-SCF-PDUs ::= TCMessages{{SSI-SCF-SCF-Invokable},{SSI-SCF-SCF-Returnable}}
SSI-SCF-SCF-Invokable {PARAMETERS-BOUND : bound, SSI-PARAMETERS-BOUND : SSI-bound} OPERATION ::= {
activityTest |
establishChargingRecord {bound}|
confirmedNotificationProvided {bound}|
confirmedReportChargingInformation {bound} |
handlingInformationRequest {bound} |
handlingInformationResult {bound}|
networkCapability {bound}|
notificationProvided {bound}|
provideUserInformation {bound}|

```

```

    reportChargingInformation {bound}|
    requestNotification {bound}
    transferSTSI {bound, SSI-bound }
}
SSI-SCF-SCF-Returnable {PARAMETERS-BOUND : bound, SSI-PARAMETERS-BOUND : SSI-bound} OPERATION ::= {
    activityTest |
    establishChargingRecord {bound}|
    confirmedNotificationProvided {bound}|
    confirmedReportChargingInformation {bound}|
    handlingInformationRequest {bound}|
    handlingInformationResult {bound} |
    networkCapability {bound}|
    provideUserInformation {bound}|
    requestNotification {bound}
    transferSTSI {bound, SSI-bound }
}
END

```

6.1.10 TransferSTSIInformation operation

6.1.10.1 Procedure descriptions

6.1.10.1.1 General description

This operation may be used from the controlling SCF to the supporting SCF - and vice versa - to exchange service information. The received service information will be used in the SCF to determine how the service is to be proceeded. The type of service information is used to assist the service logic execution and may consists of e.g. call unrelated as well as call related data.

The operation may be used to request service data and report service data results. It may be sent during establishment of an relationship after an HandlingInformationRequest operation has been issued or it may be sent during an established relationship. If a result is requested the correlation between send service data request and reported service data result is to be made on the service application level.

6.1.10.1.1.1 Parameters

- sSIInfo

This parameter identifies a service application (e.g. a service feature) within the service logic type supported across the SCF -SCF interface which is indicated in the agreement ID in the SCF bind operation. This parameter also contains associated service information.

The agreement feature indicator may correspond to a service application which is standardized at the ITU level or by any regional standardization body (i.e. global). It may also correspond to a service application which is significant only within one network or group of co-operating networks in which the service application identified is significant (i.e. local):

- agreementFeatureIndicator:

This parameter indicates the service application for which the associated service information within the agreement ID is to be provided. The scope of the agreementFeatureIndicator is local to an AgreementID and applicable within the context of an requested type.

- sTSIInformation:

This parameter conveys service information provided by the service logic of the invoking SCF to the service logic of the responding SCF.

- securityParameter:

This is an optional parameter that conveys security related information.

6.1.10.1.2 Invoking entity (controlling SCF)

6.1.10.1.2.1 Normal procedure

SCF precondition:

- 1) a relationship has been requested by the controlling SCF and a HandlingInformationRequest operation has been issued, otherwise the relationship has been already established between the two SCFs;
- 2) the SLPI has identified the need for sending service information from the controlling SCF;
- 3) in the first case of 1) the SCF FSM is in the state "Waiting for Bind Result" (controlling SCF), in the second case of 1) the SCF FSM is in the state "Assisted mode" (controlling SCF).

SCF postcondition:

- 1) SLPI execution continues;
- 2) the SCF FSM remains in the same state.

6.1.10.1.2.2 Error handling

Generic error handling for the operation related errors is described in EN 301 140-1 [1], clause 16 and the TCAP services which are used for reporting operation errors are described in EN 301 140-1 [1], clause 18.

6.1.10.1.3 Invoking entity (supporting SCF)

6.1.10.1.3.1 Normal procedure

SCF precondition:

- 1) a relationship has been established between the two SCFs;
- 2) the SLPI has identified the need for sending service information from the supporting SCF;
- 3) the SCF FSM is in the state "Assisting mode" (supporting SCF).

SCF postcondition:

- 1) SLPI execution continues;
- 2) the SCF FSM remains in the same state.

6.1.10.1.3.2 Error handling

Generic error handling for the operation related errors is described in EN 301 140-1 [1], clause 16 and the TCAP services which are used for reporting operation errors are described in EN 301 140-1 [1], clause 18.

6.1.10.1.4 Responding entity (supporting SCF)

6.1.10.1.4.1 Normal procedure

SCF precondition:

- 1) a relationship has been established between the two SCFs;
- 2) the SCF FSM is in the "Assisting mode" (supporting SCF).

SCF postcondition:

- 1) SLPI execution continues;
- 2) the SCF FSM remains in the same state.

6.1.10.1.4.2 Error handling

Generic error handling for the operation related errors is described in EN 301 140-1 [1], clause 16 and the TCAP services which are used for reporting operation errors are described in EN 301 140-1 [1], clause 18.

6.1.10.1.5 Responding entity (controlling SCF)

6.1.10.1.5.1 Normal procedure

SCF precondition:

- 1) a relationship has been established between the two SCFs;
- 2) the SCF FSM is in the "Assisted mode" (controlling SCF).

SCF postcondition:

- 1) SLPI execution continues;
- 2) the SCF FSM remains in the same state.

6.1.10.1.5.2 Error handling

Generic error handling for the operation related errors is described in EN 301 140-1 [1], clause 16 and the TCAP services which are used for reporting operation errors are described in EN 301 140-1 [1], clause 18.

6.2 Mapping of CTM operations to the extended INAP

Table 2 indicates the mapping of the CTM messages / operations to the INAP operation for every concerned interface, where the following abbreviations apply:

- InitialAssDP: InitialAssociationDP;
- InitiateAssoc: InitiateAssociation.

Table 2

	operation on INAP interfaces			
	CUSF/SSF-SCF		SCF-SCF	
CTM operation	invoke	result	invoke	result
cTMAccessRightsRequest	InitialAssDP	SendSTUI	n/a	n/a
cTMAccessRightsRequestSCF	n/a	n/a	TransferSTSI	TransferSTSI
cTMAccessRightsTerminate	InitiateAssoc	ReportUTSI	TransferSTSI	TransferSTSI
cTMLocationRegistration	InitialAssDP	SendSTUI	n/a	n/a
cTMLocationUpdateSCF	n/a	n/a	TransferSTSI	TransferSTSI
cTMLocationCancellation	InitiateAssoc	ReportUTSI	TransferSTSI	TransferSTSI
cTMProvideSecurityDataSCF	n/a	n/a	TransferSTSI	TransferSTSI
cTMNetworkAuthentication	ReportUTSI	SendSTUI	TransferSTSI	TransferSTSI
cTMTerminalAuthentication	InitiateAssoc/ SendSTUI (note 1)	ReportUTSI	TransferSTSI (note 2)	TransferSTSI
cTMKeyAllocate	SendSTUI	ReportUTSI	TransferSTSI	TransferSTSI
cTMCiphering	InitiateAssoc / SendSTUI *	ReportUTSI	TransferSTSI (note 2)	TransferSTSI
cTMOutgoingCallMobility ManagementInfo	InitialDP	n/a	n/a	n/a
cTMIncomingCallMobility ManagementInfo	SendSTUI	n/a	n/a	n/a
cTMProvideRoaming NumberSCF	n/a	n/a	TransferSTSI	TransferSTSI
ProvideSecurityData	tbc		TransferSTSI	TransferSTSI
cTMRestoreDataSCF	n/a	n/a	TransferSTSI	TransferSTSI

NOTE 1: This is dependent on whether a call unrelated dialogue is already open.
NOTE 2: This corresponds to the case where the SCFmmSubscription initiates the terminal authentication and/or ciphering during the subscription registration procedures.

7 ASN.1 specification for CTM application

```
-- CTM Mobility Management Application Module
```

```
CTM-appl-ops-args{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-Ctm(3) modules(1) cTM-
appl-ops-and-args(30) version1(0)}
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
IMPORTS
    OPERATION, Code, ERROR
FROM Remote-Operations-Information-Objects ros-InformationObjects

    -- Operations
    cTMAccessRightsTerminate,
    cTMLocationCancellation,
    cTMTerminalAuthentication,
    cTMNetworkAuthentication,
    cTMCiphering,
    cTMKeyAllocate,

    -- Data Types
    AuthType,
    CipherKey,
    FixedIdentity,
    IPUi,
    IPEI,
    PortableCapabilities,
    PortableIdentity,
    Rand,
    Rs,
    Res,
    ServiceClass,
    -- Errors
    unspecified,
    portableIdentityUnknown
FROM CTM_Operations_and_Arguments{ccitt identified-organization etsi (0) 1 444 operations-and-
errors(1) }
    CalledPartyNumber,
    CallingPartyNumber,
    ScfID
```

```

FROM IN-CS2-datatypes { ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-network(1)
CS-2(20) modules(0) in-cs2-datatypes (0) version1(0)};
CTMAccessRightsRequestSCF OPERATION ::= {
  ARGUMENT SEQUENCE {
    iPEI [0] IPEI OPTIONAL,
    cTMAuthType [1] AuthType,
    cTMPortableCapabilities [2] PortableCapabilities,
    ...}
  RESULT SEQUENCE {
    iPUI [0] IPUI,
    cTMFixedIdentity [1] FixedIdentity,
    cTMServiceClass [2] ServiceClass OPTIONAL,
    ...}
  ERRORS {pPortableIdentityUnknown |
    uUnspecified
  }
}
CODE opcode-CTMAccessRightsRequestSCF
}

-- End of SCFAccessRightsRequest operation definition
CTMLocationUpdateSCF OPERATION ::= {
  ARGUMENT SEQUENCE {
    iPUI [0] IPUI,
    sCFmmVisitedId [1] ScfID,
    ..}
  RESULT SEQUENCE {
    cTMNumber [0] CallingPartyNumber,
    cTMFixedIdentity [1] FixedIdentity,
    ...}
  ERRORS { cTMDataMissing |
    portableIdentityUnknown |
    unspecified |
    cTMRoamingNotAllowed}
  CODE opcode-CTMLocationUpdateSCF
}
-- End of LocationUpdate operation definition

CTMProvideRoamingNumberSCF OPERATION ::= {
  ARGUMENT SEQUENCE {
    iPUI [0] PortableIdentity,
    ...}
  RESULT SEQUENCE {
    roamingNumber [0] CalledParty OPTIONAL,
    userStatus [1] UserStatus,
    ...}
  ERRORS {cTMDataMissing |
    cTMFacilityNotSupported |
    cTMNoRoamingNumberAvailable |
    portableIdentityUnknown}
  CODE opcode-CTMProvideRoamingNumberSCF
}
-- End of ProvideRoamingNumber operation definition

CTMProvideSecurityDataSCF OPERATION ::= {
  ARGUMENT SEQUENCE{
    iPUI [0] IPUI,
    ...}
  RESULT SEQUENCE {
    securityDataSets [2] SIZE (1.. maxSetsOfAuthenticationData) OF AuthenticationData,
    ...}
  ERRORS{
    portableIdentityUnknown |
    unspecified
  }
  CODE opcode-CTMProvideSecurityDataSCF
}
-- End of ProvideSecurityData operation definition
CTMRestoreDataSCF OPERATION ::= {
  ARGUMENT SEQUENCE{
    sCFmmHomeId ScfID,
    ...}
  RETURN RESULT FALSE
  ERRORS FALSE
  CODE opcode-CTMRestoreDataSCF
}
-- End of SCF_RestoreData operation definition

-- Data Types

```

```

AuthenticationData ::= SEQUENCE {
    authType AuthType,
    rand Rand OPTIONAL,
    rs Rs OPTIONAL,
    ks Ks OPTIONAL,
    res Res OPTIONAL,
    cipherKey CipherKey OPTIONAL
}

Ks ::= OCTETSTRING(SIZE(16))
UserStatus ::= ENUMERATED{userUnknown(0), userReachable(1), userNotReachable(2), ... }
-- Error Types

cTMRoamingNotAllowed ERROR ::= {
    CODE errcode-CTMRoamingNotAllowed
}
cTMFacilityNotSupported ERROR ::= {
    CODE errcode-CTMFacilityNotSupported
}
cTMNoRoamingNumberAvailable ERROR ::= {
    CODE errcode-CTMNoRoamingNumberAvailable
}
cTMDataMissing ERROR ::= {
    CODE errcode-CTMDataMissing
}

-- CTM Mobility Management operation codes

opcode-CTMAccessRightsRequestSCF Code ::= global : { cTM-SCF-SCF-application 1}
opcode-CTMLocationUpdateSCF Code ::= global : { cTM-SCF-SCF-application 2}
opcode-CTMProvideRoamingNumberSCF Code ::= global : { cTM-SCF-SCF-application 3}
opcode-CTMProvideSecurityDataSCF Code ::= global : { cTM-SCF-SCF-application 4}
opcode-CTMRestoreDataSCF Code ::= global : { cTM-SCF-SCF-application 5}

-- CTM Mobility Management error codes

errcode-CTMDataMissing Code ::= global : { cTM-SCF-SCF-application 51}
errcode-CTMFacilityNotSupported Code ::= global : { cTM-SCF-SCF-application 52}
errcode-CTMNoRoamingNumberAvailable Code ::= global : { cTM-SCF-SCF-application 53}
errcode-CTMRoamingNotAllowed Code ::= global : { cTM-SCF-SCF-application 54}

CTM-APPL-PARAMETERS-BOUND ::= CLASS
{
    &maxSetsOfAuthenticationData INTEGER
    -- The maxSetsOfAuthenticationData shall not exceed the maximum sets allowed to be transferred
    by the
    -- used TCAP.
}
WITH SYNTAX
{
    MAXIMUM-FOR-SETS-OF-AUTHENTICATION-DATA &maxSetsOfAuthenticationData
}
-- The following instance of the parameter bound is just an example
networkSpecificCTMBoundSet PARAMETERS-BOUND ::=
{
    MAXIMUM-FOR-SETS-OF-AUTHENTICATION-DATA 4 -- e.g. maximum for Bluebook TCAP
}

-- Object Identifiers

-- This module assigns object identifiers for CTM

cTM-SCF-SCF-application OBJECT IDENTIFIER ::=
{ccitt(0) identified-organization(4) etsi(0) inDomain(1) in-Ctm(3) modules(1) cTM-appl-
ops_and_args(30) version1(0)}
id-CTM-ServiceFunctionIndicator OBJECT IDENTIFIER ::= { ccitt(0) identified-organization(4) etsi(0)
inDomain(1) in-Ctm(3) interfaces(100) ctmAgreement(2)}.
-- This value shall be used for the USIServiceIndicator and the AgreementFeatureIndicator.
-- NOTE: Also operation codes and error codes as defined are object identifiers.
-- Timer values

END

```

The following value ranges apply:

- short: 1 second to 10 seconds;
- medium: 1 second to 60 seconds;
- long: 1 second to 30 minutes.

7.1 Mobility Management Application Timers

Table 3 lists all mobility management application timers and the value range for each timer. The definitive value for each timer may be network specific and has to be defined by the network operator.

The default value for T-MM shall be 15 sec.

Table 3

DSS1+ defined operations	T-MM	medium
cTMAccessRightsRequestSCF	T_{carrs}	medium
cTMLocationUpdateSCF	T_{clus}	medium
cTMPProvideRoamingNumberSCF	T_{cprns}	medium
cTMPProvideSecurityDataSCF	T_{cpsds}	long
cTMRestoreDataSCF	T_{crds}	short

7.2 Application Timers

Table 4 lists all application specific timers and the value range for each timer. The definitive value for each operation timer may be network specific and has to be defined by the network operator.

Table 4

RoamingNumberTimer	T_{crn}	medium
--------------------	-----------	--------

8 Interworking with DSS1

8.1 Description

The following figure shows in a simplified manner the call related and the call unrelated signalling configurations to be considered in the present document.

In general the term SSP is used to consider both the call related as well as the call unrelated configuration.

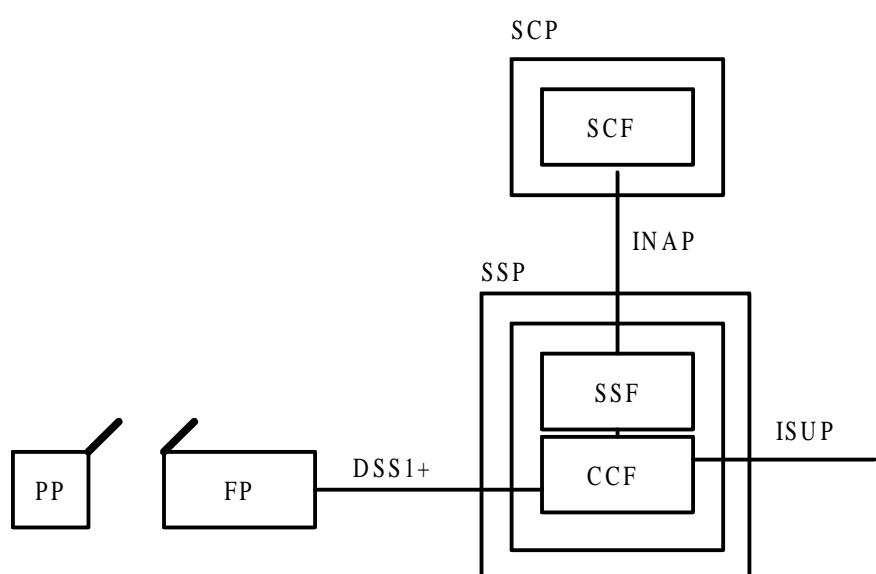
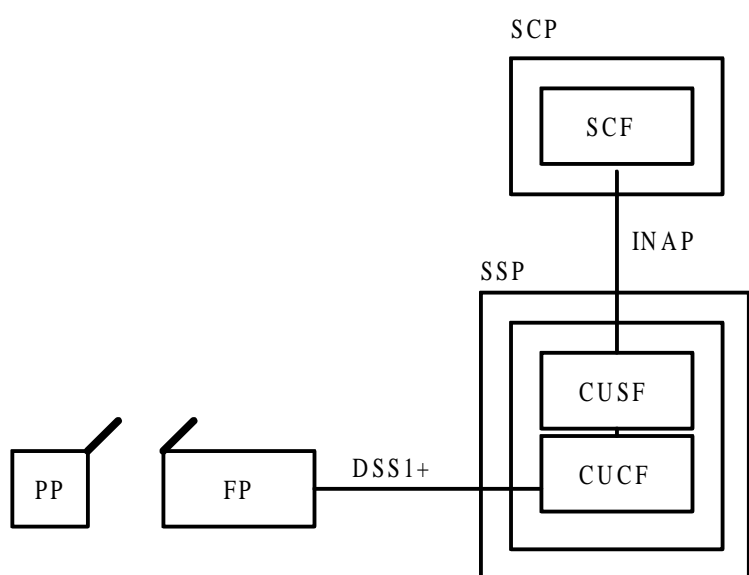


Figure 5: Signalling call related configuration



CUCF (Call Unrelated Control Function): The part of CCF necessary for the CUSF.

Figure 6: Signalling call unrelated configuration

8.1.1 Detection point processing

The normal call related and call unrelated detection points are applicable for CTM.

Of course, the triggering of the CTM service is service specific.

8.1.2 Receipt of DSS1+ messages

In general the procedures as described in EN 301 144-1 [2] and EN 301 140-1 [1] are applicable. Specific aspects are defined in the following.

8.1.3 Receipt of INAP operations

In general the procedures as described in EN 301 144-1 [2] and EN 301 140-1 [1] are applicable. Specific aspects are defined in the following.

8.1.4 Coding requirements

The CTM operations transferred in DSS1+ and INAP shall not exceed either the maximum size for the component part of the Facility information element or the maximum size of the octet string content of the uSIInformation. It has to be considered that the size of an INAP operation shall not exceed the maximum length capable of being transferred by TCAP.

8.2 Generic procedures

This subclause specifies the interworking on a procedural level.

The procedures as described in EN 301 144-1 [2] and EN 301 140-1 [1] are applicable. Those procedures define which messages and operations are applicable in which circumstances. The CTM specific use of IN procedures and operations flows are defined in the present document.

8.2.1 USI handling procedures

For CTM, the uSIServiceIndicator for USI transfer to be used shall be the following object identifier:

id-CTM-ServiceFunctionIndicator as defined in the CTM application module in this specification.

This subclause describes the USI related issues. Which message will be used to send this information is context dependent. The IN procedures as defined in clause 17 of en 301 140-1 [1] are to be taken into account.

8.2.1.1 GFT-control input and output for CTM

The GFT-control receives and provides respectively the value of the serviceFunction of the network facility extension in the Facility information element. This value shall be as defined in EN 301 144-1 [2].

The sourceEntity received by the CUCF (user to SCP direction) will be stored as destinationEntity and will be sent later (SCP to user direction).

8.2.1.2 Receiving of DSS1+ operations / sending of UTSI information

UTSI information can be received by the SSP by the Facility information element in the following DSS1+ messages: SETUP or FACILITY.

UTSI information shall be sent to the SCP using one of the following operations for CTM as appropriate: InitialDP, InitialAssociationDP or ReportUTSI.

If and only if the SSP receives a Facility information element with a protocol profile set to "Networking extensions" and if the GFT-control has determined that the serviceFunction is to be provided locally, then the SSP shall send an appropriate IN operation to the SCP and the mapping of information shall be as follows:

- The uSIServiceIndicator of the INAP operation shall be set to id-CTM-ServiceFunctionIndicator.
- The octet string content of the uSIInformation shall be set to the sequence of octets which are building the "Service Components" part (octets 4 etc.) of the Facility information element.
- The other argument parameters shall be set as appropriate.

Table 5 summarizes the mapping in respect to the USI information.

Table 5: Mapping of DSS1+ operations to UTSI information

DSS1+			INAP	
Facility i.e.		→	USI	
Protocol profile	= Networking extensions			
Network Facility Extension serviceFunction			uSIServiceIndicator	= id-CTM-ServiceFunctionIndicator =
sourceEntity	= endTerminal			
sourceEntityAddress <opt.>				
destinationEntity				
destinationEntityAddress <opt.>				
Service Components	= components		uSIInformation	= Service Components <same as received>
NOTE: opt. means optional.				

8.2.1.3 Receiving of STUI information / sending of DSS1+ operations

STUI information can be received by the SSP by the following INAP operations: InitiateAssociation or SendSTUI operation.

STUI information will be sent to the DSS1 user using one of the following messages as appropriate: SETUP or FACILITY.

If and only if the SSP receives an IN operation including STUI information with the uSIServiceIndicator set to id-CTM-ServiceFunctionIndicator and if the SSP is in the state possible to send this information to the user then the SSP shall send an appropriate DSS1+ message including a Facility information element. The mapping of information shall be as follows:

- The protocol profile of the Facility information element shall be set to "networking extensions".
- The serviceFunction of the network facility extension in the Facility information element shall be set as defined in EN 301 144-1 [2].
- The octet content of the "service components" part of the Facility information element, i.e. "octets 4 etc.", shall be set to the service components received in the sequence of octets content of the uSIInformation.

Table 6 summarizes the mapping in respect to the USI information.

Table 6: Mapping of STUI information to DSS1+ operations

DSS1+			INAP	
Facility i.e.		←	USI	
Protocol profile	= Networking extensions			
Network Facility Extension				
serviceFunction	<serviceFunction>		uSIServiceIndicator	= id-CTM-ServiceFunctionIndicator
sourceEntity	<not applicable>			
sourceEntityAddress <opt.>	<not applicable>			
destinationEntity	= "endTerminal" or <provided by CUCF as previously received>			
destinationEntityAddress <opt.>	-			
Service Components	= <same as received>		uSIInformation	= Service Components

NOTE: opt. means optional.

8.2.2 INAP component handling procedures

Not required for CTM.

8.3 Call related issues

In general the procedures as described in EN 301 144-1 [2] (DSS1+) and EN 301 140-1 [1] (ETSI INAP CS2) are applicable.

8.3.1 Outgoing call

The user shall send a SETUP message which includes the CTMOutgoingCallMobilityManagement operation. The SSP initiates an InitialDP operation as defined in EN 301 140-1 [1]. The content of the Facility information element shall be mapped to the UTSI information according to subclause 8.2.1.2 "Receiving of DSS1+ operations / sending of UTSI information". The serviceKey shall be set as agreed for the service.

8.3.2 Emergency call

In principle the same interworking as for the normal call is applicable.

8.3.3 Incoming call

The SSP initiates an InitialDP operation as defined in EN 301 140-1 [1].

The SCP shall send SendSTUI operation including the CTMIncomingCallMobilityManagement operation. The CTMIncomingCallMobilityManagement operation shall be stored until the Connect operation is received. If the SSP receives a Connect operation the SSP shall send a SETUP message which includes the received CTMIncomingCallMobilityManagement operation. The Connect operation contains a destinationRoutingAddress set to the FT_address of the called user.

8.3.4 Call release

If the SCF sends a ReleaseCall operation then the call will be released immediately, that is without waiting for outstanding user responses.

8.4 Call unrelated issues

In the following specific interworking issues for the call unrelated case are mentioned.

As defined in EN 301 144-1 [2] the user or the network initiates a DSS1 GFP NCICS connection by the CTM application using the SETUP message. EN 301 144-1 [2] states that "The first message establishing the NCICS connection (SETUP) shall always contain the CTM-id/PT-id and an invoke component indicating the requested operation."

8.4.1 User initiated association

The SETUP message is received from the user and shall contain a Facility information element. The SSP shall send an InitialAssociationDP operation to the SCP.

The content of the Facility information element shall be mapped to the UTSI information according to subclause 8.2.1.2 "Receiving of DSS1+ operations / sending of UTSI information". The Network Facility Extension in the Facility information element shall be used, if at all, to route the Facility information to the SCF. It will not be included in the InitialAssociationDP operation for CTM.

The SETUP message and the InitialAssociationDP operation shall contain the information and use the mapping as indicated in the table 7. Further information may be included as appropriate.

The cUApplicationIndication parameter shall not be included.

Table 7: User initiated association

DSS1+			INAP	
SETUP		→	InitialAssociationDP	
			serviceKey	= <service specific>
			eventTypeBCUSM	= activation Received and Authorized
Bearer capability	= "Call independent Signalling Connection"		bearerCapability	= "Call independent Signalling Connection"
Calling party number	= FT_Address <optional>		callingPartyNumber	= FT_Address (note)
Called party number	<not used>			
Facility i.e.			USI (s. table 5)	
NOTE: In case, that the FT_Address is not provided by DSS1+ the default number of the access will be used as FT_Address in the InitialAssociationDP operation.				

8.4.2 Network initiated association

The InitiateAssociation operation is received from the SCP and shall contain STUI information. The SSP shall send a SETUP message to the user. The STUI information shall be mapped to the content of the Facility information element in the SETUP message according to subclause 8.2.1.3 "Receiving of STUI information / sending of DSS1+ operations".

The SETUP message and the InitiateAssociation operation shall contain the information and use the mapping as indicated in table 8. Further information may be included as appropriate.

Table 8: Network initiated association

DSS1+			INAP	
SETUP		←	InitiateAssociation	
Bearer capability	= "Call independent Signalling Connection"			
Calling party number	<not used>			
Called party number	= FT_Address <optional>		calledPartyNumber	= FT_Address
Facility i.e. (see table 6)			USI	

8.4.3 Information exchange during the association

The USI information exchange during the association shall use the procedures as defined in subclause 8.2.1 "USI handling procedures".

If the SSP receives USI information in the FACILITY message it will send those information to the SCP using the ReportUTSI operation.

If the SSP receives USI information in the SendSTUI operation it will send those information to the DSS1+ user using the FACILITY message.

8.4.4 Association release

The association release shall be as defined in EN 301 140-1 [1].

The SCP shall use cause #31 "normal, unspecified" in the ReleaseAssociation operation. This cause shall be send to the user in the RELEASE message towards the user.

If the CUSF receives a ReleaseAssociation operation, then the DSS1+ association will be released immediately, i.e. without waiting for user responses.

Annex A (informative): Message Sequence Charts

This annex contains all MSCs and the related textual descriptions for the CTM mobility management procedures. They describe example cases for all possible procedures. The MSCs and their description are informative information only.

A.1 Subscription registration

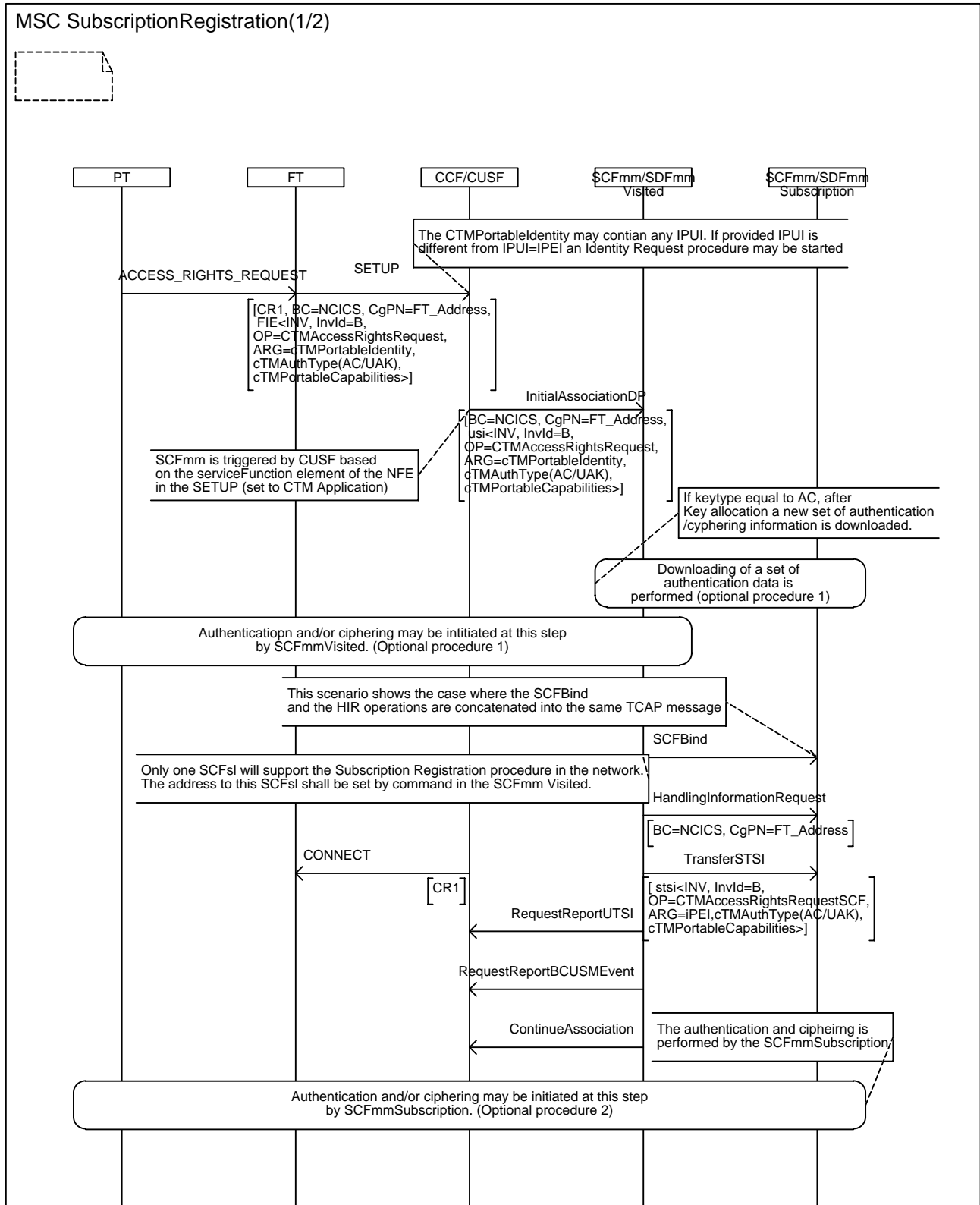


Figure A.1

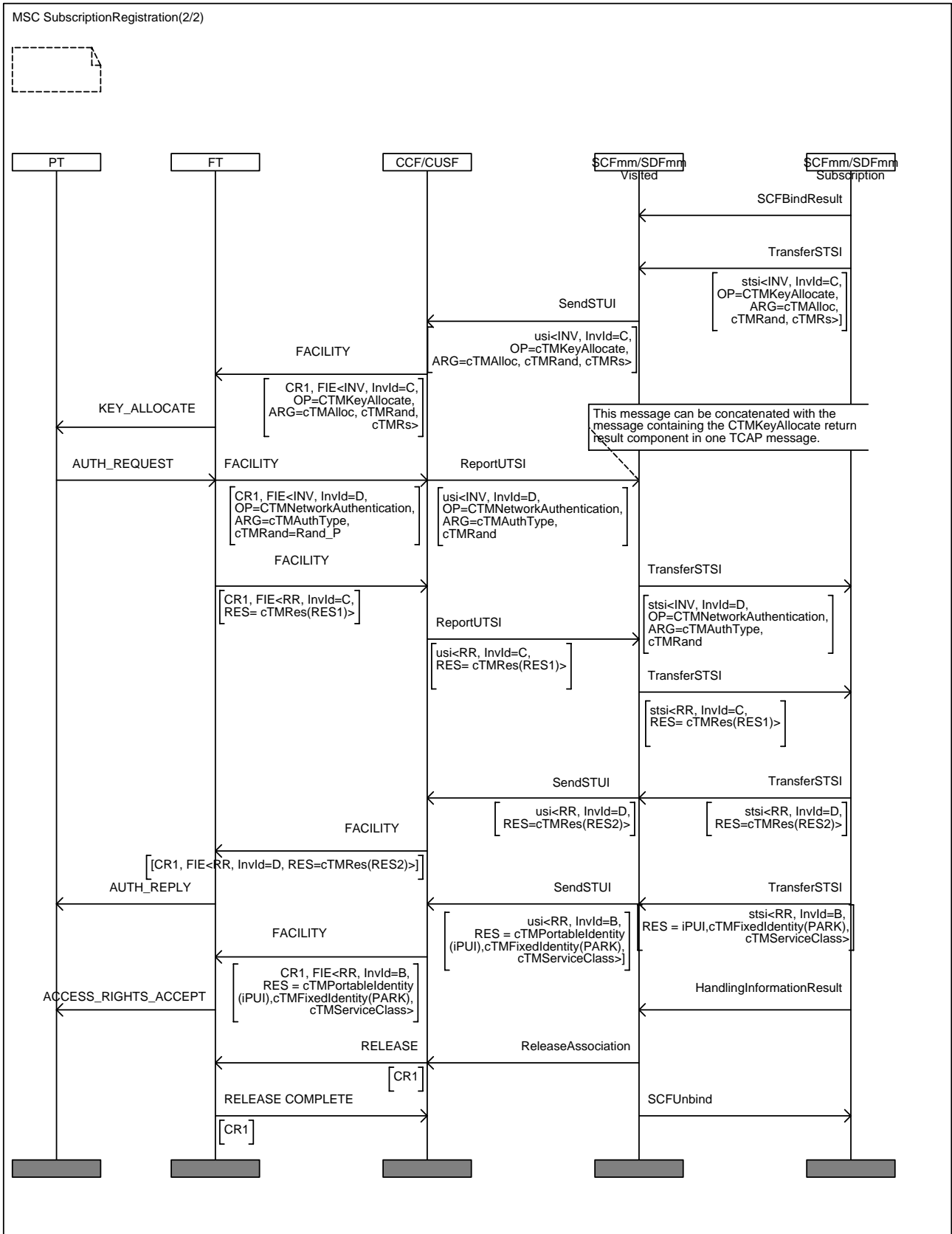


Figure A.2

Normal operation

- 1) The PT initiates the subscription registration procedure when allowed by FT by sending an <cTMAccessRightsRequestSCF> invoke operation to the CUSF.

This invoke operation includes the following parameters:

- cTMPortableIdIdentity depends on the value previously assigned to the subscription record in the PT. If no value has been stored, the default IPUI-N=IPEI is used. If the IPEI is not provided an IdentityRequest procedure may be started by the SCFmmVisited.
 - cTMAuthType containing the authentication algorithm (DSSA), the authentication key type (AC or UAK since the PT may contain either an AC or UAK before the subscription registration procedure is initiated) which is stored in the PT and the authentication key number.
 - cTMPortableCapabilities to convey the cordless terminal capabilities such as tone capability, display capability, profile indicator and control codes.
- 2) The SCFmmVisited is triggered by the CUSF by means of an InitialAssociationDP operation based on the Service Function field of the NFE received in the DSS1 SETUP message with TDP "ActivationReceivedAndAuthorized" and as Triggering Criteria equal to CTM Application.
 - 3) Prior to initiating the <cTMAccessRightsRequestSCF> in an SCFmmSubscription the SCFmmVisited may as a first possible option ask the SCFmmSubscription for the authentication data to be used for ciphering the key allocate procedure and to authenticate the CTM user. The SCFmmVisited then initiates authentication and/or ciphering. If authentication data is related to the AC Key a new set of authentication data is needed after the Key allocation procedure.
 - 4) Since one or more dedicated SCFmmSubscription will support the Subscription Registration procedure in a network, one SCFmmSubscription shall be addressed. The SCFmmVisited shall send the <cTMAccessRightsRequestSCF> invoke operation to the SCFmmSubscription by means of the SSI mechanism.
 - 5) The SCFmmSubscription may as another option initiate authentication and/or ciphering, first authenticate the CTM user and then cipher the Key Allocation procedure.
 - 6) The SCFmmSubscription shall now initiate the key allocation procedure by translating the AC value stored in the SCFmmSubscription and the PT into the UAK. The key allocation procedure is initiated by the network to replace the Authentication Code (AC) by a more secure User Authentication Key (UAK).
 - 7) The SCFmmSubscription sends the <cTMKeyAllocate > invoke operation to the SCFmmVisited including Alloc_type (in cTMAllocType), RAND_F (in cTMRand) and Rs (in cTMRs) via the SSI mechanism and this operation is transported to the PT via the USI mechanism of the CUSF.
 - 8) If the content of the received parameters is acceptable for the PT, the PT responds with:
 - a <cTMKeyAllocate> return result operation including the cTMRes parameter indicating the RES1 number to provide the terminal authentication result calculated by the cordless terminal, and;
 - a <cTMNetworkAuthentication> invoke operation which includes the AuthType (in the cTMAuthenticationType) in addition to the RAND_P (in cTMRand) value. The <cTMNetworkAuthentication> operation is transported to the SCFmmSubscription using the CUSF and SCF-SCF interface.

These <cTMKeyAllocate> and <cTMNetworkAuthentication> components are transported in respectively sendSTUI and reportUTSI messages over the CUSF-SCF interfaces and via TransferSTSI over the SCF-SCF interface.

- 9) The SCFmmSubscription checks if the RES1 value corresponds with the XRES1 for the valid subscription.

The SCFmmSubscription on receiving the cTMNetworkAuthentication invoke component reuses the random session number cTMRs previously generated for key allocation and use the received random parameter. The SCFmmSubscription, having successfully performed the network authentication procedures, sends a cTMNetworkAuthentication return result to the SCFmmVisited via the SSI mechanism and this operation is transported to the PT via the USI mechanism of the CUSF. The cTMNetworkAuthentication return result includes as parameters the calculated result RES2.

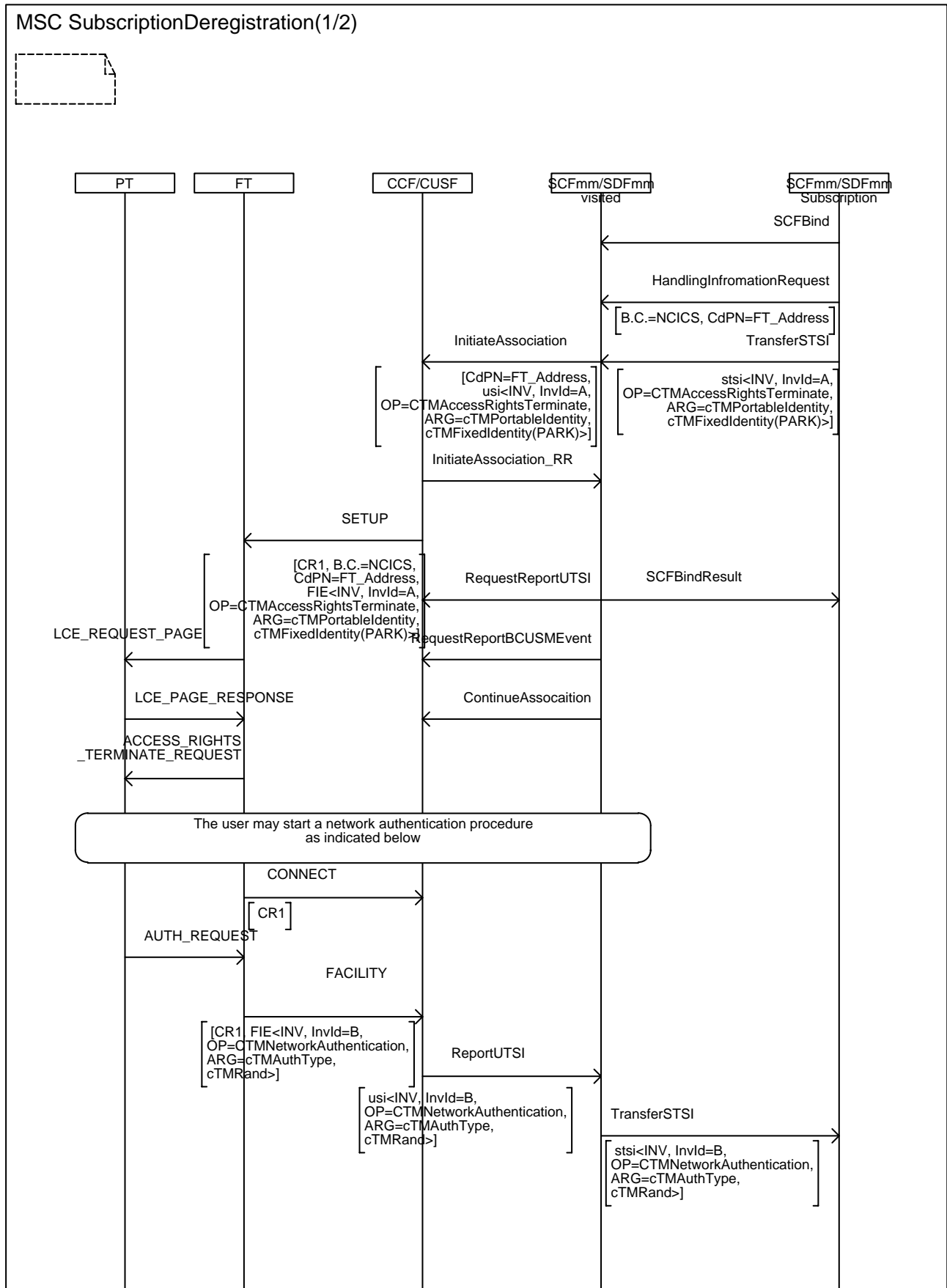
- 10) The SCFmmSubscription performs the access rights procedure by sending a cTMAccessRightsRequestSCF return result component containing the following parameters:
- a cTMPortableIdentity which contains in the IPUI the PUT and PUN of the cordless terminal which requested the subscription registration;
 - cTMFixedIdentity containing the type PARK, the AccessRightClass (ARC), AccessRightDetails (ARD) and the length of the identity (PLI). The pair IPUI and PARK provides the network with a unique cordless terminal identity;
 - cTMServiceClass which is the service class related to the current active IPUI.

The cTMAccessRightsRequestSCF return result component is sent via the SSI mechanism on the SCFmmSubscription to SCFmmVisited interface and transported to the PT via the USI mechanism of the CUSF.

Exceptional procedure

- 11) If the PT is unable to perform the key-allocate procedure, a cTMKeyAllocate return error operation is sent via a ReportUTSI message via the CUSF and via a TransferSTSI over the SCF-SCF interface containing one of the following error values:
- terminal reject; with this value an optional additional parameter cTMTerminalRejectValue indicating the reject reason received on the air interface may be sent;
 - pagingFailure (only if key allocate procedure is not embedded);
 - radioConnectionFailure.
- 12) If the SCFmmSubscription detects on receipt of the cTMKeyAllocate return result operation that the RES1 value does not correspond with the XRES1 for the valid subscription, a cTMNetworkAuthentication return error component with value "networkRejected" and a cTMAccessRightsRequest return error component with value "networkRejected" shall be sent via the SSI mechanism on the SCFmmSubscription to SCFmmVisited interface and these operations are transported to the PT via the USI mechanism of the CUSF.
- 13) If the SCFmmSubscription is unable to perform a network authentication, it sends a cTMNetworkAuthentication return error with value "networkRejected" and will subsequently forward a cTMAccessRightsRequest return error with value "networkRejected" via the SSI mechanism on the SCFmmSubscription to SCFmmVisited interface, and these operations are transported to the PT via the USI mechanism of the CUSF.

A.2 Subscription deregistration



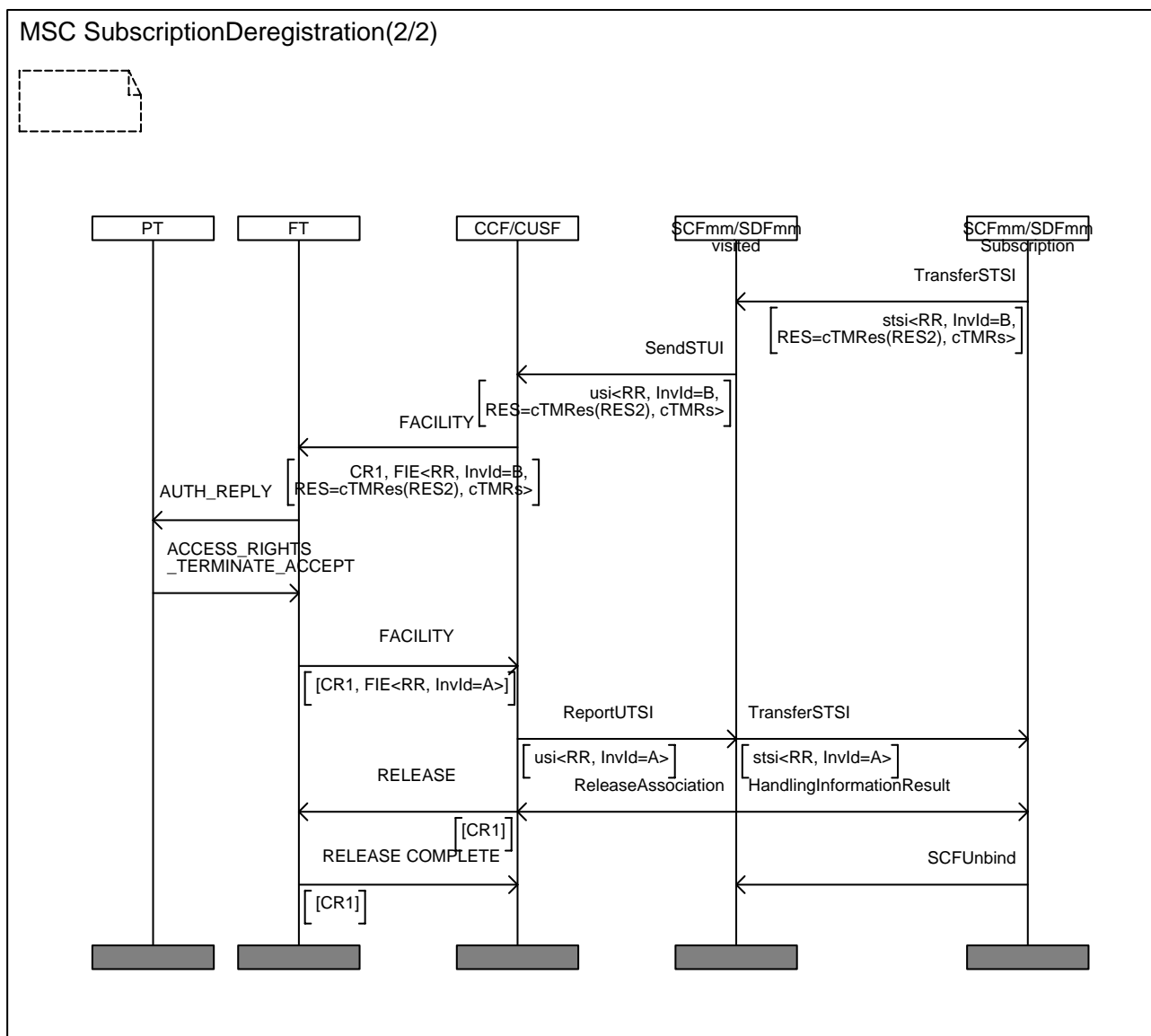


Figure A.3

Normal operation

- 1) This procedure is initiated by the network to cancel a subscription. At the end of the procedure execution, the subscriber data will be erased in the PT.

To perform the subscription deregistration procedure, the SCFmmHome sends a cTMAccessRightsTerminate invoke component to the SCFmmVisited including in cTMPortableIdentity the IPUI and the PARK (in cTMFixedIdentity).
- 2) The SCFmmVisited forwards the cTMAccessRightsTerminate invoke component to the CUSF using the USI mechanism.
- 3) The CUSF sends the cTMAccessRightsTerminate invoke component to the SCUAF. The SCUAF then performs paging to the PT. The PT may start a Network Authentication procedure.
- 4) To perform a network authentication, the SCUAF sends a cTMNetworkAuthentication invoke component to the CUSF using the USI mechanism by means of a ReportUTSI message. The cTMNetworkAuthentication invoke component contains the cTMAuthenticationType, the cTMRand and optionally the cTMPortableIdentity.
- 5) The CUSF forwards the cTMNetworkAuthentication invoke component to the SCFmmVisited using the USI mechanism by means of a ReportUTSI message.

- 6) The SCFmmVisited forwards the cTMNetworkAuthentication invoke component to the SCFmmHome using the SSI mechanism by means of a TransferSTSI message.
- 7) The SCFmmHome, on receiving the cTMNetworkAuthentication invoke component, performs authentication and sends a cTMNetworkAuthentication return result component to the SCFmmVisited containing the calculated result RES2 (in cTMRes) and the random session number the network has used to calculate the RES2 value (in cTMRs). The SCFmmHome forwards the cTMNetworkAuthentication return result component to the SCFmmVisited using the SSI mechanism by means of a TransferSTSI message.
- 8) The SCFmmVisited forwards the cTMNetworkAuthentication return result component to the CUSF using the USI mechanism by means of a SendSTUI message.
- 9) The CUSF forwards the cTMNetworkAuthentication return result component to the SCUAF.
- 10) If the authentication of the network is successful, the user deletes PARK and IPUI and sends an cTMAccessRightsTerminate return result component to the SCUAF. The SCUAF forwards the cTMAccessRightsTerminate return result component towards the CUSF.
- 11) The CUSF forwards the cTMAccessRightsTerminate return result component to the SCFmmVisited using the USI mechanism by means of a ReportUTSI message.

Exceptional procedure

- 12) The SCFmmVisited forwards the cTMAccessRightsTerminate return result component to the SCFmmHome using the SSI mechanism by means of a TransferSTSI message.
- 13) If the PT is unable to perform the access rights terminate procedure, an cTMAccessRightsTerminate return error operation is sent via a ReportUTSI message via the CUSF and via TransferSTSI over the SCF-SCF interface containing one of the following error values:
 - terminalRejected (with this value an optional parameter cTMTerminalRejectValue indicating the reject reason received on the air interface may be sent);
 - pagingFailure;
 - radioConnectionFailure.

The SCFmmHome takes action as appropriate.

- 14) If the SCFmmHome is unable to perform a network authentication, the SCFmmHome sends a cTMcTMNetworkAuthentication return error with the value "networkRejected".

A.3 Location registration in the SCFmmVisited

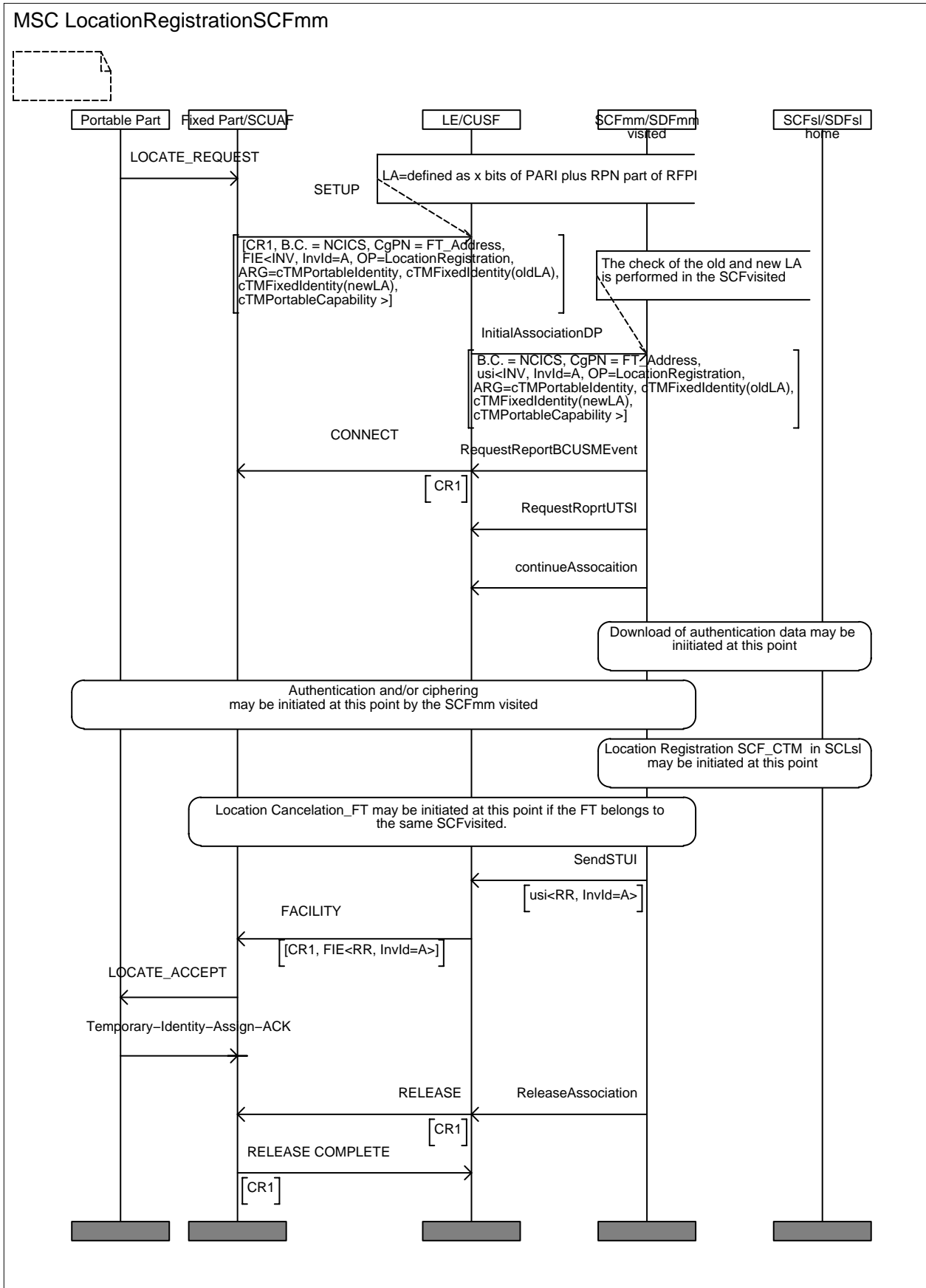


Figure A.4

Normal operation

- 1) The cTMLocationRegistration invoke component is sent from the FT via the CUSF to the SCFmmVisited using the USI mechanism; this component contains the following parameters:
 - cTMPortableIdentity indicating the IPUI (identity of the portable terminal);
 - cTMOldLocationAreaIdentity and cTMNewLocationAreaIdentity containing the old and new LA (where LA is defined as the LAL of RFPI and the RFPI);
 - cTMPortableCapabilities indicating the characteristics of the cordless terminal.

NOTE 1: The CUSF provides the CUSFID as Calling Party Address in the TC-BEGIN message.

NOTE 2: The FT_Address is provided in the CallingPartyNumber of the CUSF InitialAssociationDP operation.

- 2) The CUSF triggers the SCFmmVisited based on the Service Function field of the NFE received in the DSS1 SETUP message with TDP "ActivationReceivedAndAuthorized" and as Triggering Criteria equal to CTM Application.
- 3) The SCFmmVisited may at this point download authentication data from the SCFmmHome e.g. if not yet registered.
- 4) The SCFmmVisited may perform authentication and/or ciphering procedure.
- 5) If PT is already registered in the SCFmmVisited:
 - the SCFmmVisited shall check the "Active LA" and "Active FT address".
- 6) If the "Active FT Address" differs from the received "FT Address" the SCFmmVisited shall initiate a cTMLocation Cancellation_FT (see relevant MSC).
- 7) If the "Active LA" differs from the "Old LA" received the SCFmmVisited shall initiate a location update SCFmmHome (see relevant MSC).
- 8) If data restoration procedure for the addressable SCFmmHome is ongoing, the SCFmmVisited shall initiate a location update SCFmmHome(see relevant MSC).
- 9) If the PT is not yet registered in the SCFmmVisited, the SCFmmVisited shall initiate a location update SCFmmHome (see relevant MSC).
- 10) If the SCFmmVisited / SCFmmHome has successfully performed the location registration / update, the SCFmmVisited sends via a CUSF SendSTUI operation a cTMLocationRegistration return result component to the PT without parameters. The SCFmmVisited stores the "New LA" as "Active LA" and the received FT address as the Active FT Address.

Exceptional procedure

- 11) If the terminal authentication fails, or the location update SCFmmHome fails than the SCFmmVisited sends a LocationRegistration return error component via an SendSTUI operation to the CUSF with the value "NetworkRejected".
- 12) If during the location registration procedure a release association is received from the CTM user or the FT, this event may be reported to the SCFmmVisited by arming the EDP-R "AssociationReleaseRequested" BCUSM Event. The arming is performed by means of a requestReportBCUSMEvent operation and the reporting is performed by means of the eventReportBCUSM operation.

A.4 Location update in the SCFmmHome

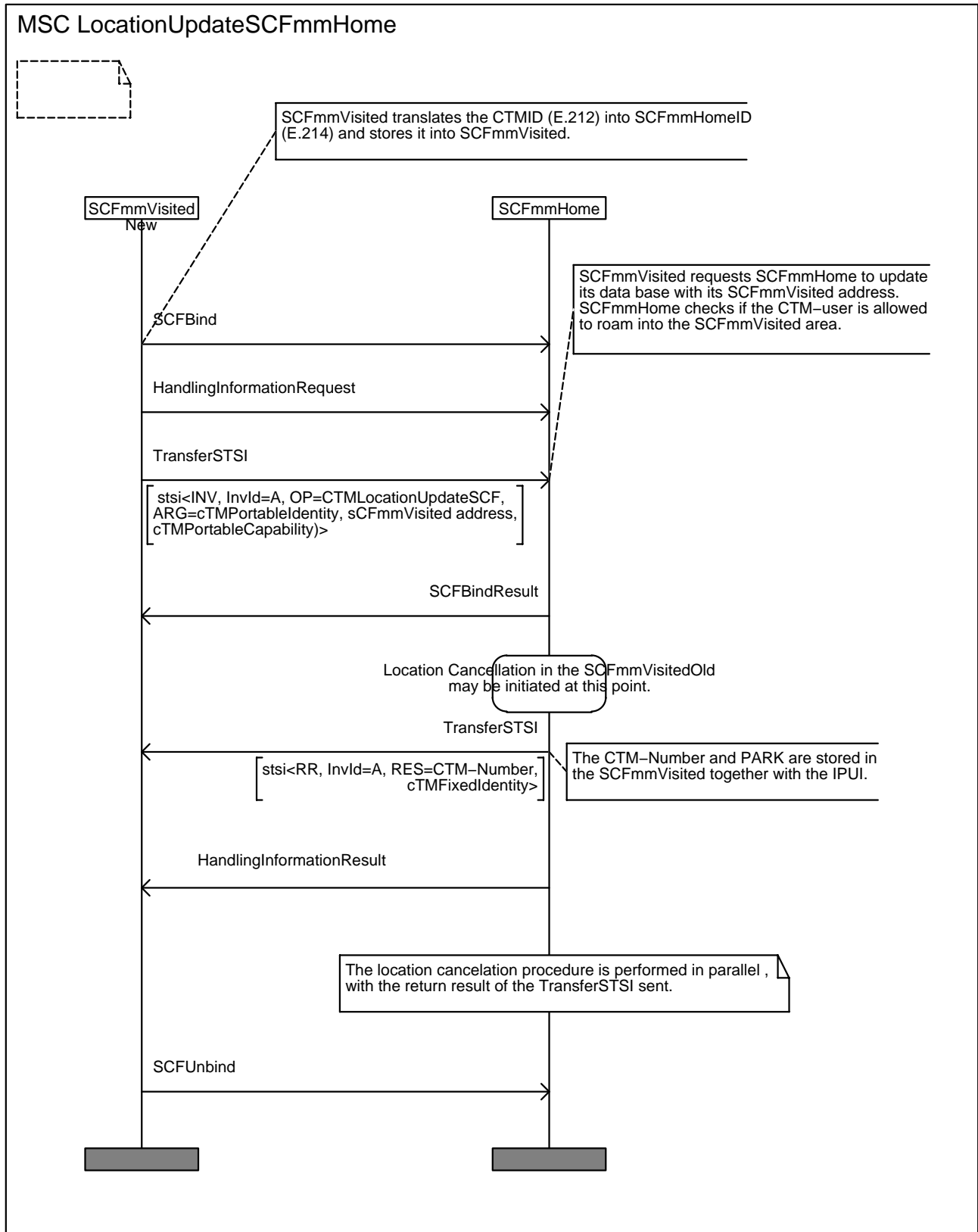


Figure A.5

Normal operation

- 1) The SCFmmVisited translates the PUN part of the cTMPortableIdentity (E.212 number) into a "Mobile global title" (E.214 number) and stores it as SCFmmHomeId. The SCFmmHomeId will be used later during the outgoing call procedure in order that the SCFmmVisited can initiate a subsequent triggering of the SCFmmHome for checking the outgoing CTM supplementary services. The SCFmmVisited shall send a cTMLocationUpdateSCF invoke operation using the SSI mechanism of the SCF-SCF interface containing its SCFmmVisitedId together with the associated IPUI.
- 2) The SCFmmHome shall check whether the CTM user is allowed to roam into the SCFmmVisited area; if so a cTMLocationUpdateSCF return result is sent with the cTMNumber and the type PARK.
- 3) The SCFmmHome shall check whether the CTM user was previously registered in another SCFmmVisited. If registered, the SCFmmHome initiates a location cancellation in SCFmmVisited procedure.

Exceptional procedure

- 4) If the CTM user is not allowed to roam into the SCFmmVisited area, on receipt of an cTMLocationUpdateSCF invoke operation the SCFmmHome sends a cTMLocationUpdateSCF return error operation to the SCFmmVisited using the SSI mechanism of the SCF-SCF interface.
- 5) If during the location registration procedure a release association is received from the CTM user or the FT, this event may be reported to the SCFmmVisited by arming the EDP-R "AssociationReleaseRequested" BCUSM Event. The arming is performed by means of an requestReportBCUSMEvent operation and the reporting is performed by means of the eventReportBCUSM operation.

A.5 LocationCancellation in the SCFmmVisited

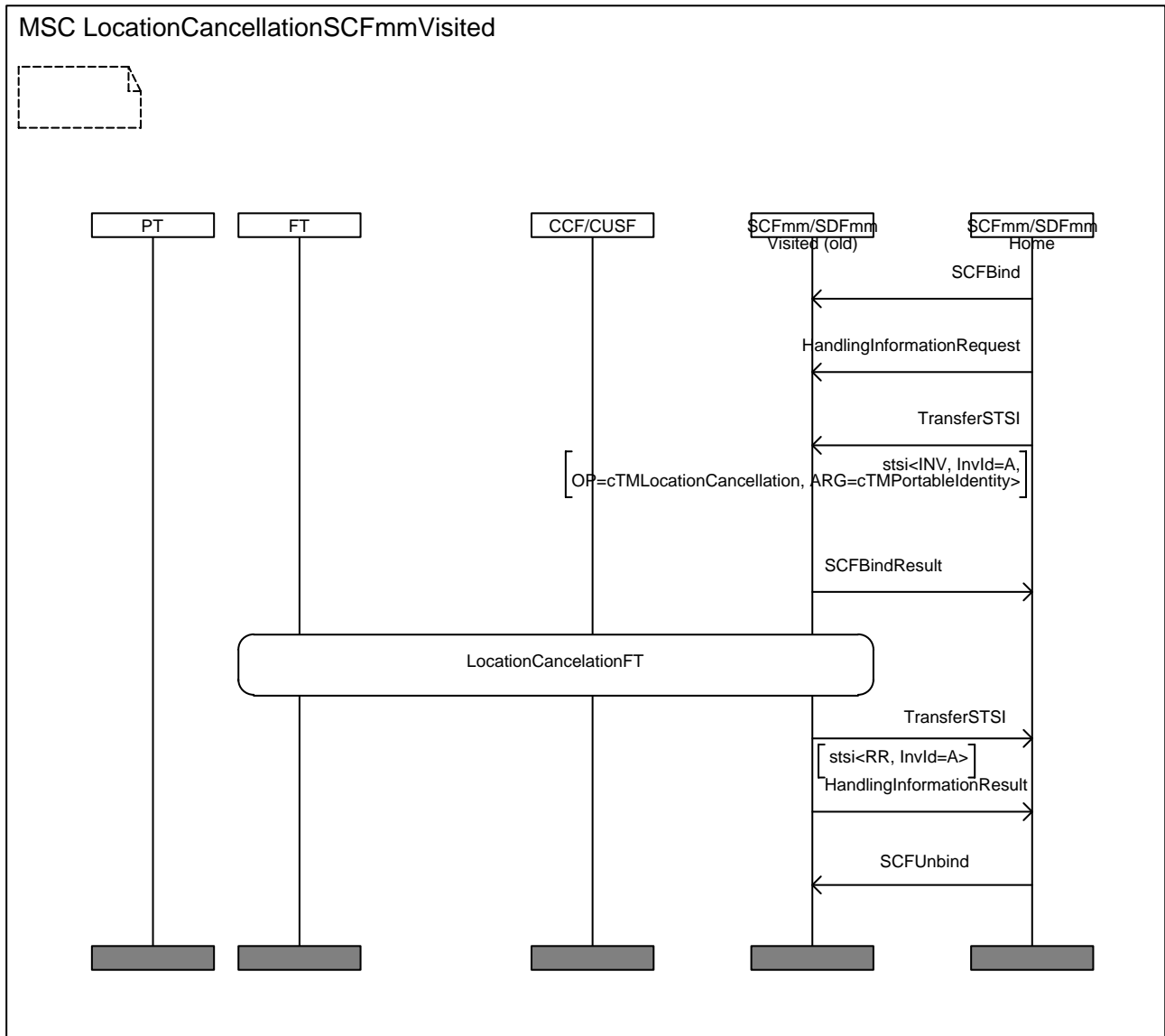


Figure A.6

Normal operation

- 1) The SCFmmHome sends a cTMLocationCancellation invoke component using the SSI mechanism of the SCF-SCF interface containing as parameter the cTMPortableIdentity.
- 2) The SCFmmVisited removes, on receipt of the LocationCancellation invoke component, the cTMPortableIdentity and sends a cTMLocationCancellation return result to the SCFmmHome.

A.6 LocationCancellation in the FT

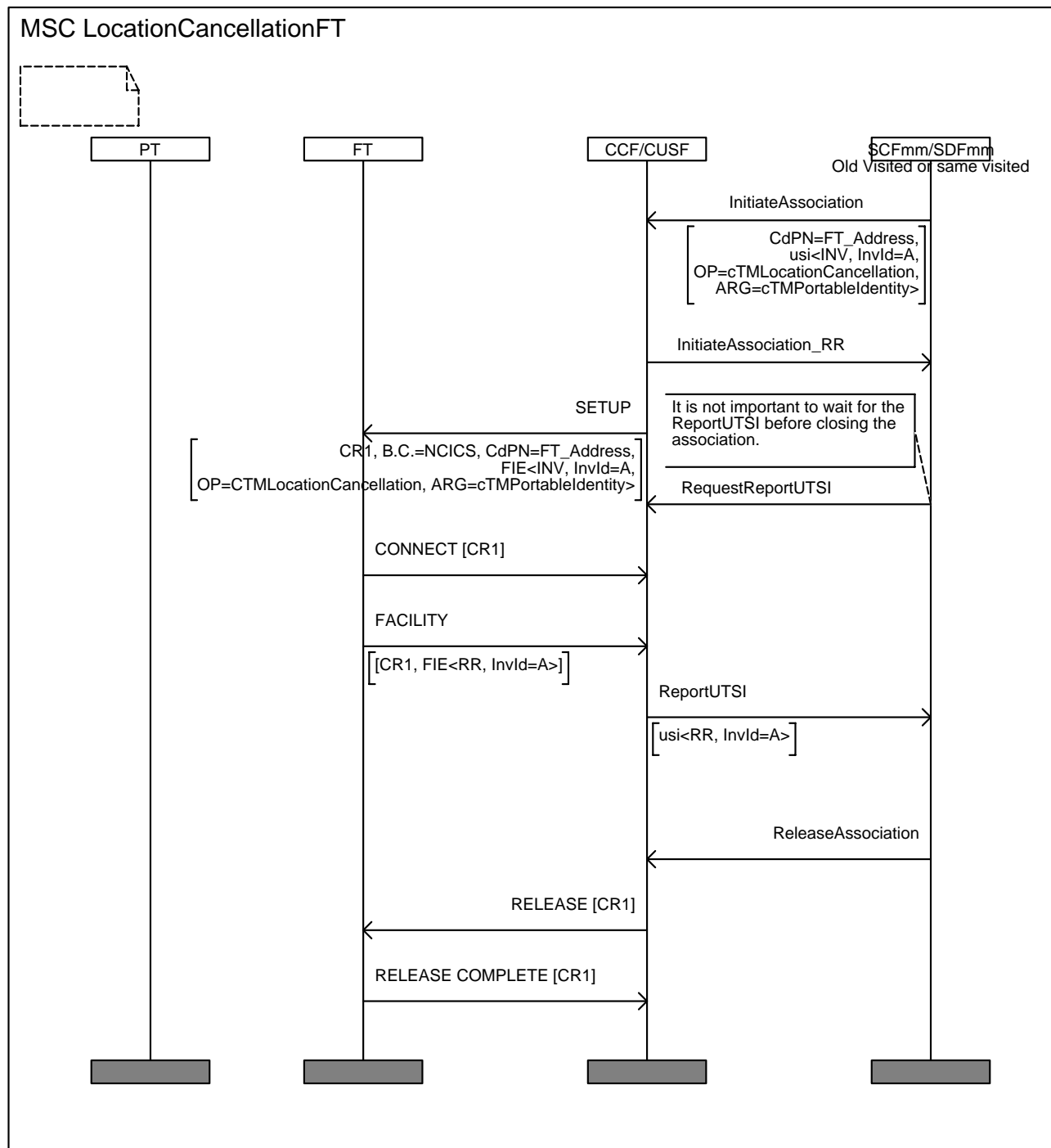


Figure A.7

Normal operation

- 1) The location cancellation procedure is initiated by the SCFmmVisited towards the old FT to delete all data related to a Cordless Terminal e.g. because the terminal has moved to another location area.

The SCFmmVisited sends a cTMLocationCancellation invoke component using the CUSF USI mechanism. The cTMLocationCancellation component contains the cTMPortableIdentity indicating the IPU. The CUSF forwards the cTMLocationCancellation invoke component to the FT where the cTMPortableIdentity was previously registered.

- 2) The SCUAF removes the cTMPortableIdentity from its data base and responds by sending a cTMLocationCancellation return result component without parameters. This component is send via the CUSF to the SCFmmVisited using the USI mechanism.

Exceptional procedure

- 3) If during the location cancellation procedure a release association is received from the CTM user or the FT, this event may be reported to the SCFmmVisited by arming the EDP-R "AssociationReleaseRequested" BCUSM Event. The arming is performed by means of an requestReportBCUSMEvent operation and the reporting is performed by means of the eventReportBCUSM operation.
- 4) If the FT is unable to act on the cTMLocationCancellation invoke component, the FT sends a cTMLocationCancellation return error component via the CUSF to the SCFmmVisited using the USI mechanism. The component contains the portableIdentityUnknown error value if the location cancellation is not successfully performed due to the fact that the cTMPortableIdentity to be cancelled is not present.

A.7 Download of security data

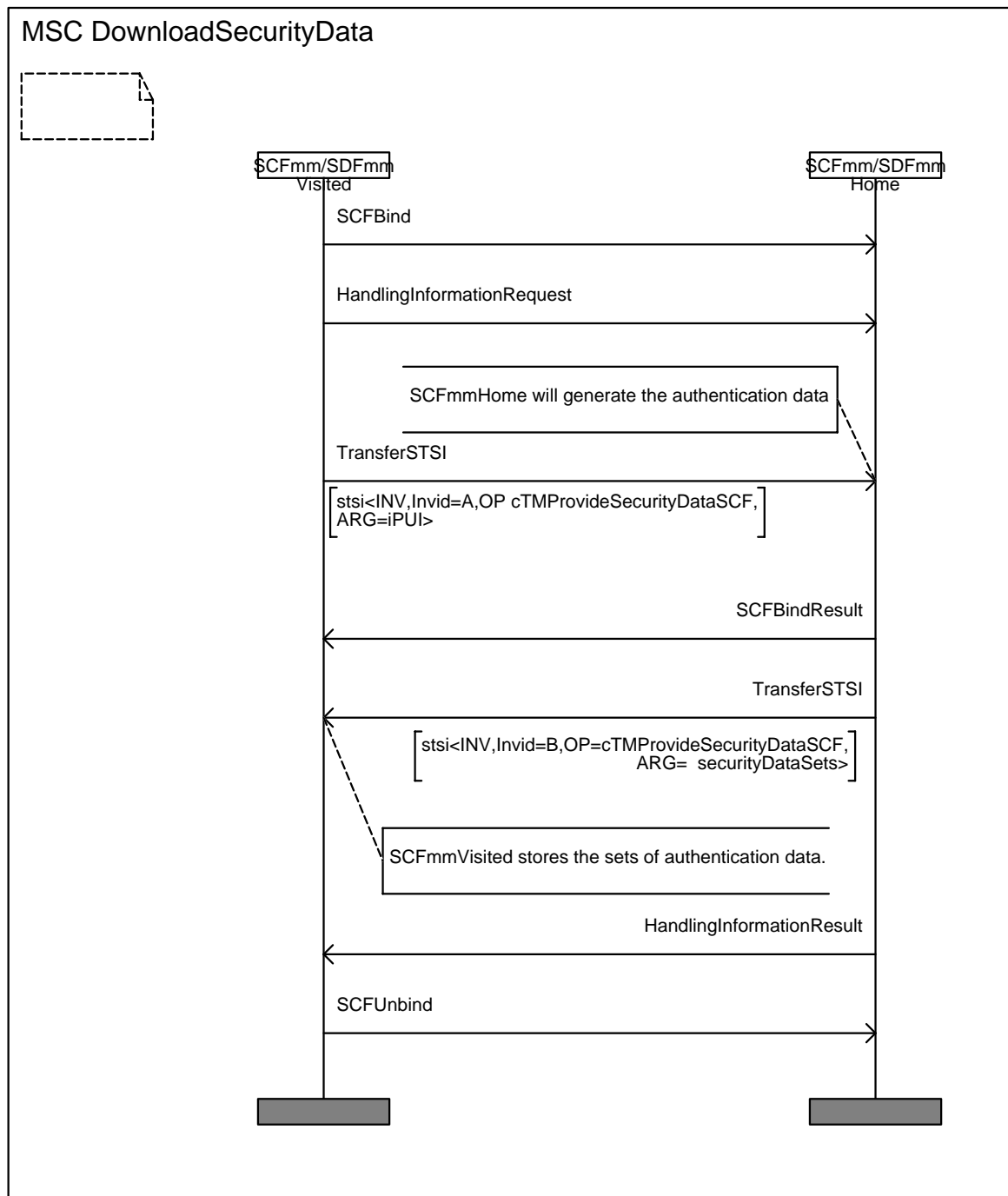


Figure A.8

Normal operation

- 1) The SCFmmVisited requests authentication and/or ciphering data from the SCFmmHome by sending a cTMProvideSecurityDataSCF invoke component using the SSI mechanism of the SCF_SCF interface. This component contains the IPUI.
- 2) The SCFmmHome, on receipt of the cTMProvideSecurityDataSCF invoke component, generates a number of sets of authentication and/or ciphering data and sends to the SCFmmVisited a cTMProvideSecurityDataSCF return result component using the SSI mechanism of the SCF_SCF interface. This component contains the sets of Authentication Data (RAND, RS, XRES1, DCK, cTMAuthType) that have been generated.

A.8 Restoration of location data in the SCFmmHome

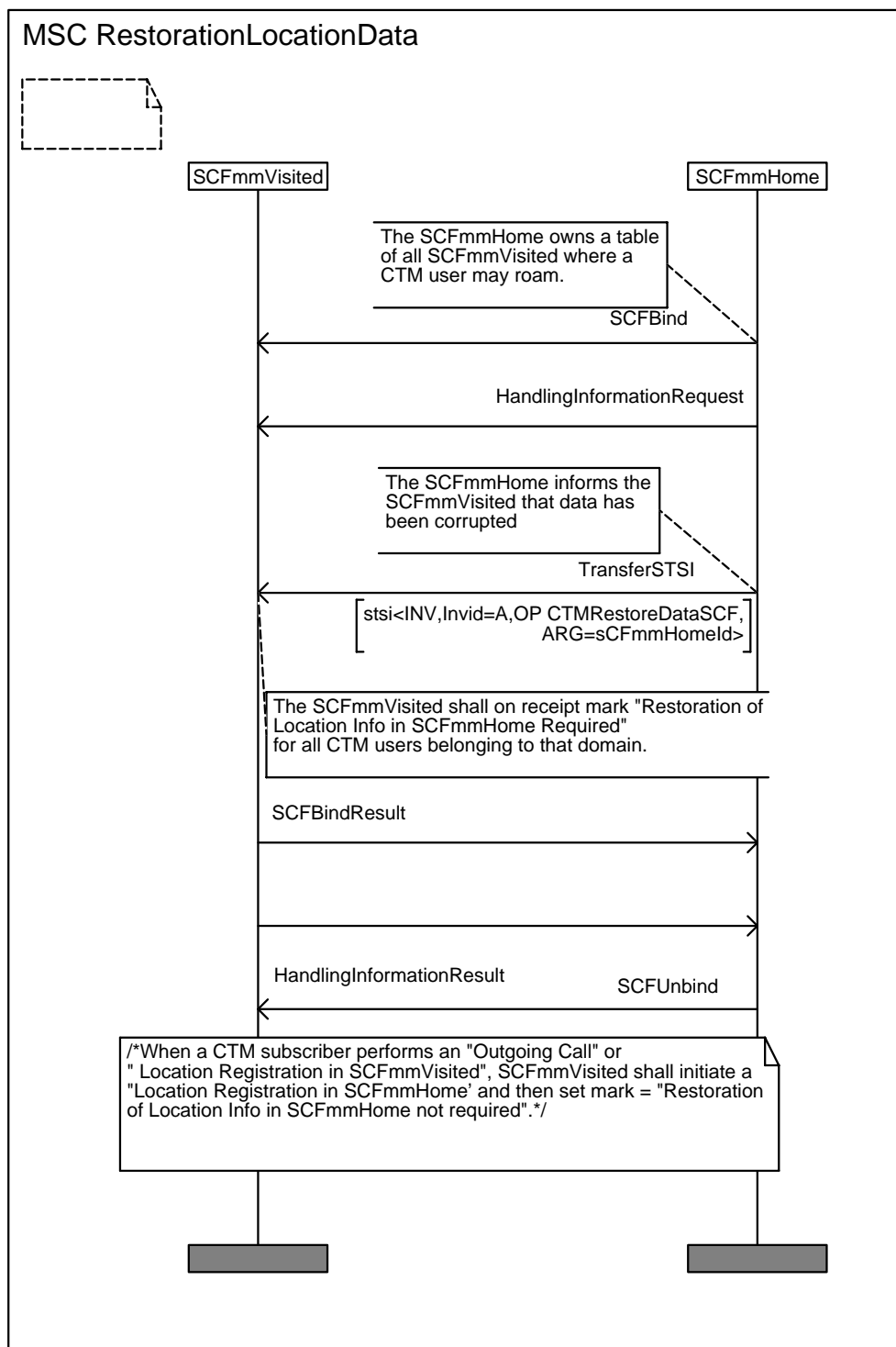


Figure A.9

Normal operation

- 1) The SCFmmHome has a table of all the SCFmmVisited addresses where the CTM subscribers may roam. If the location data gets corrupted in the SCFmmHome (e.g. after restart), the SCFmmHome sends a message to all SCFmmVisited by means of a cTMRestoreDataSCF invoke component using the SSI mechanism over the SCF-SCF interface. This invoke component indicates to the addressed SCFmmVisited that the restoration of location data in the SCFmmHome shall take place and shall have the SCFmmHomeID parameter.

- 2) The SCFmmVisited, on receipt of the cTMRestoreDataSCF invoke component, marks <restoration of location info in SCFmmHome required> for all subscribers belonging to that SCFmmHome. To find all users belonging to the SCFmmHome, the invoked SCFmmVisited compares the SCFmmHomeID stored at the location registration in the SCFmmHome procedure with the one received in the restoration of location data procedure.
- 3) When the CTM subscriber performs an "outgoing call" procedure or a "location registration SCFmmVisited" procedure, the SCFmmVisited initiates a "location update SCFmmHome" procedure and sets mark <restoration of location info in SCFmmHome not required>. This option implies that CTM users will not be reachable until either they initiate an outgoing call or perform a location registration.

A.9 Terminal authentication ciphering

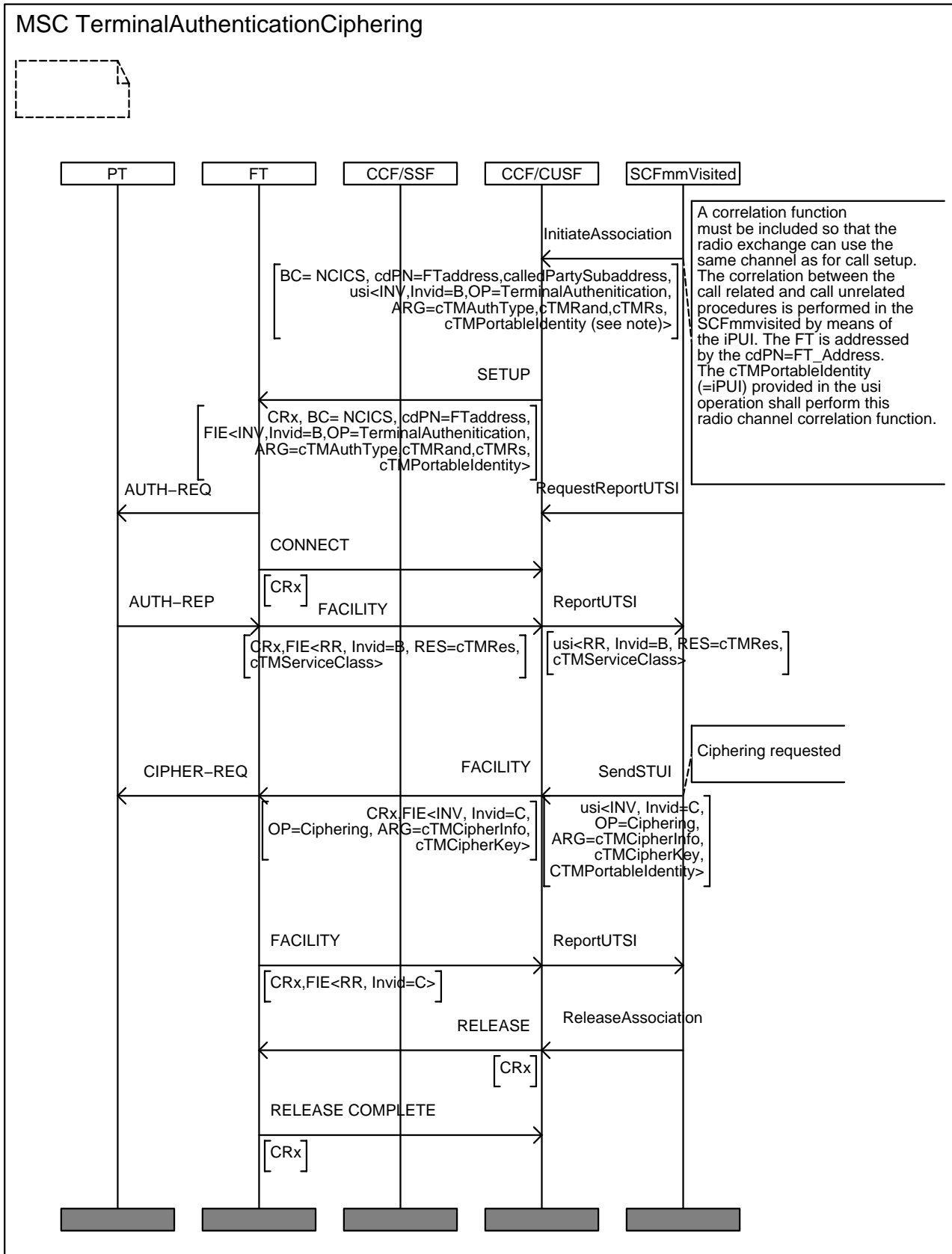


Figure A.10

Normal operation

- 1) The SCFmmVisited may initiate an Terminal Authentication by sending a cTMTerminalAuthentication invoke component using the USI mechanism on CUSF-SCF interface. If a call-unrelated dialogue is already open, the same dialogue will be used for the Terminal Authentication, and the invoke component will be sent via a sendSTUI operation.

If a call-unrelated dialogue is not open, a call-unrelated dialogue will be opened, and the invoke component will be sent via the initiateAssociation operation.

The cTMTerminalAuthentication component shall contain the following information:

- cTMAuthType, indicating the authentication key type (AC and UAK), the authentication algorithm, and the authentication key number related to the iPUI to use for calculation of the authentication result;
 - cTMRand, indicating the RAND number, which is used for calculation of the authentication result;
 - cTMRs, indicating the Rs number, which is used for calculation of the authentication result;
 - cTMPortableIdentity, identifying the cordless terminal.
- 2) The result of the terminal authentication (cTMRes) will be sent in the cTMTerminalAuthentication return result component. Optionally the service class (cTMSERVICECLASS) may be included in the return result.
 - 3) Independently from the Terminal Authentication procedure (for example, old cipher key can be used), the SCFmmVisited may initiate a ciphering procedure by sending a cTMCiphering invoke component using the USI mechanism on CUSF-SCF interface. If a call-unrelated dialogue is already open, the same dialogue will be used for the ciphering, and the invoke component will be sent via a sendSTUI operation.

If a call-unrelated dialogue is not open, a call-unrelated dialogue will be opened, and the invoke component will be sent via the initiateAssociation operation.

The cTMCiphering component contains the following information:

- cTMCipherInfo, indicating the cipher key type, cipher key number and the ciphering algorithm, related to the iPUI;
 - cTMCipherKey, indicating the numeric value of the ciphering key to be used by the FP;
 - cTMPortableIdentity (optionally), indicating the IPUI.
- 4) As soon as the ciphering is completed, the FT will initiate a cTMCiphering return result component without any parameter.

A.10 Network Authentication

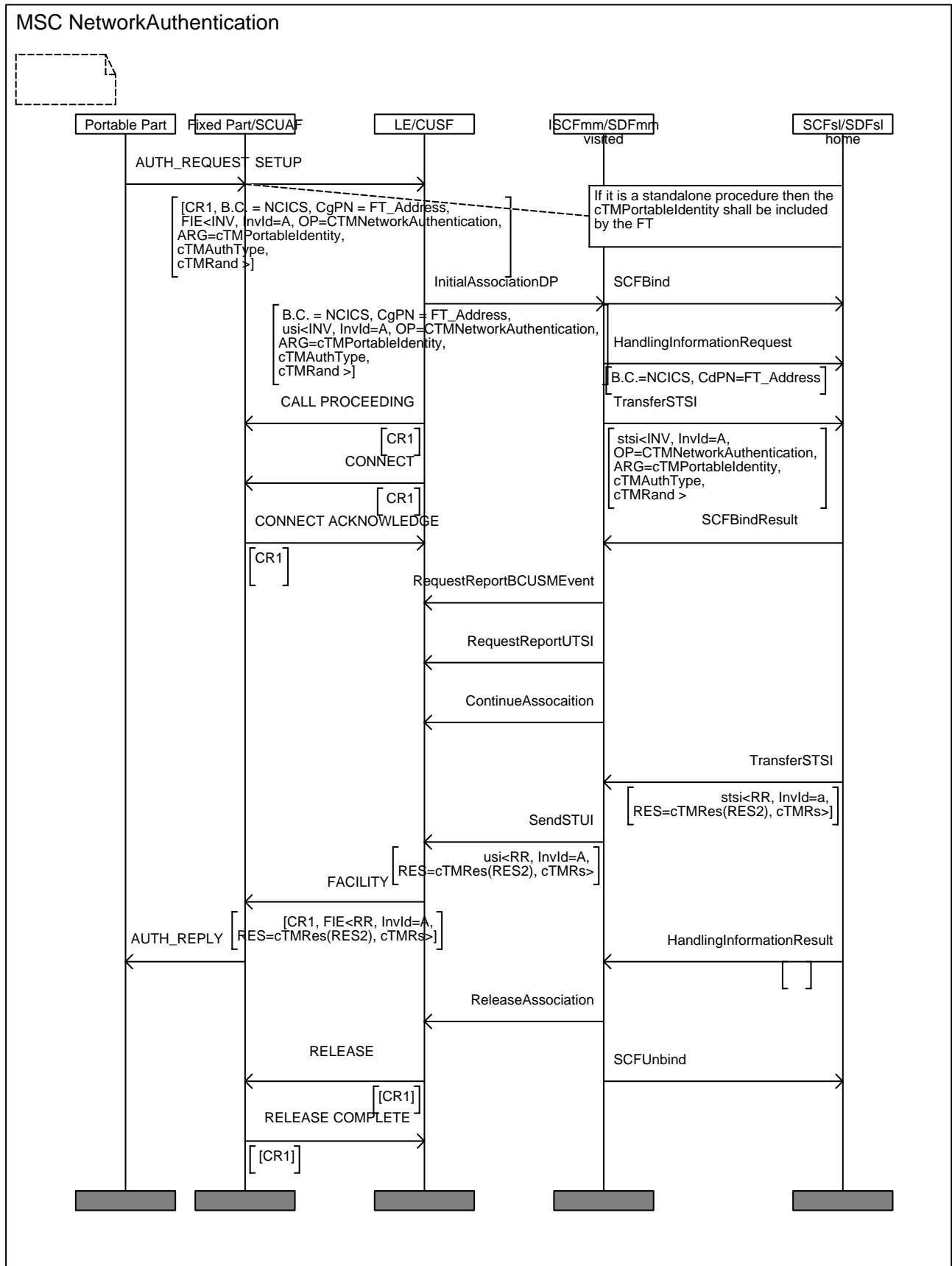


Figure A.11

Annex B (informative): Call control Message Sequence Charts

This annex contains all MSCs and the related textual descriptions for the CTM Call Control procedures. They describe example cases for all possible procedures. The MSCs and their description are informative only.

B.1 Outgoing call

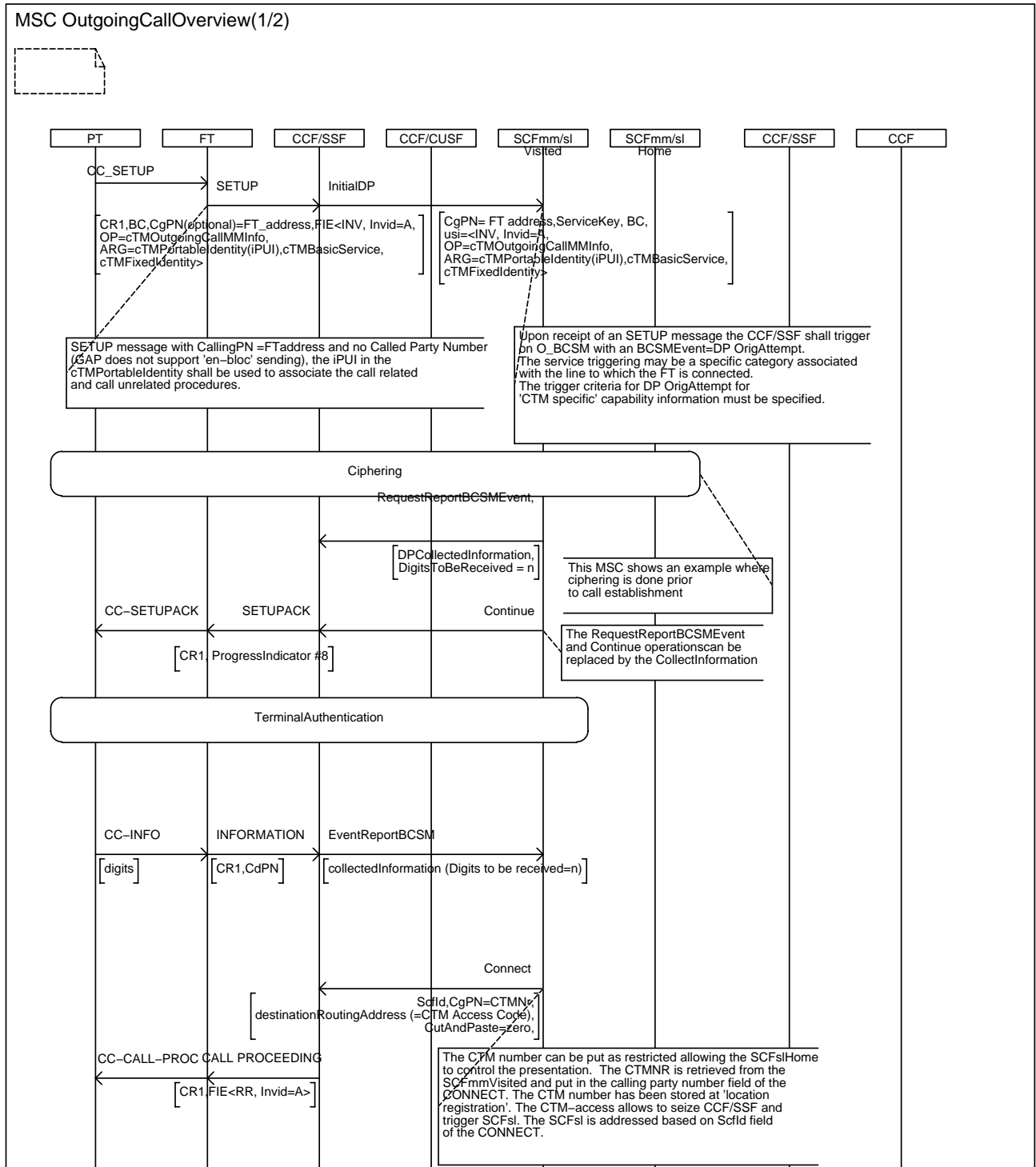


Figure B.1

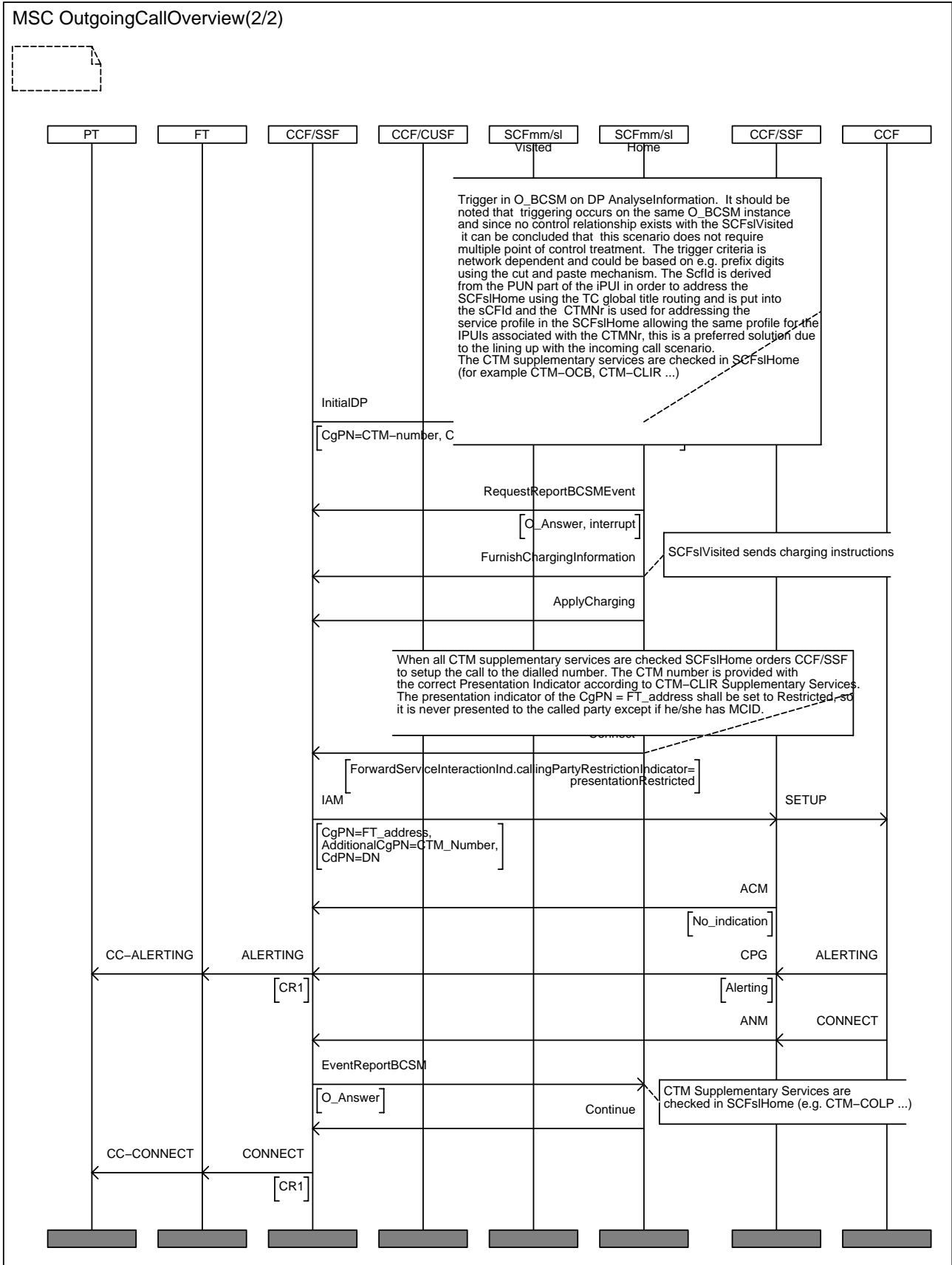


Figure B.2

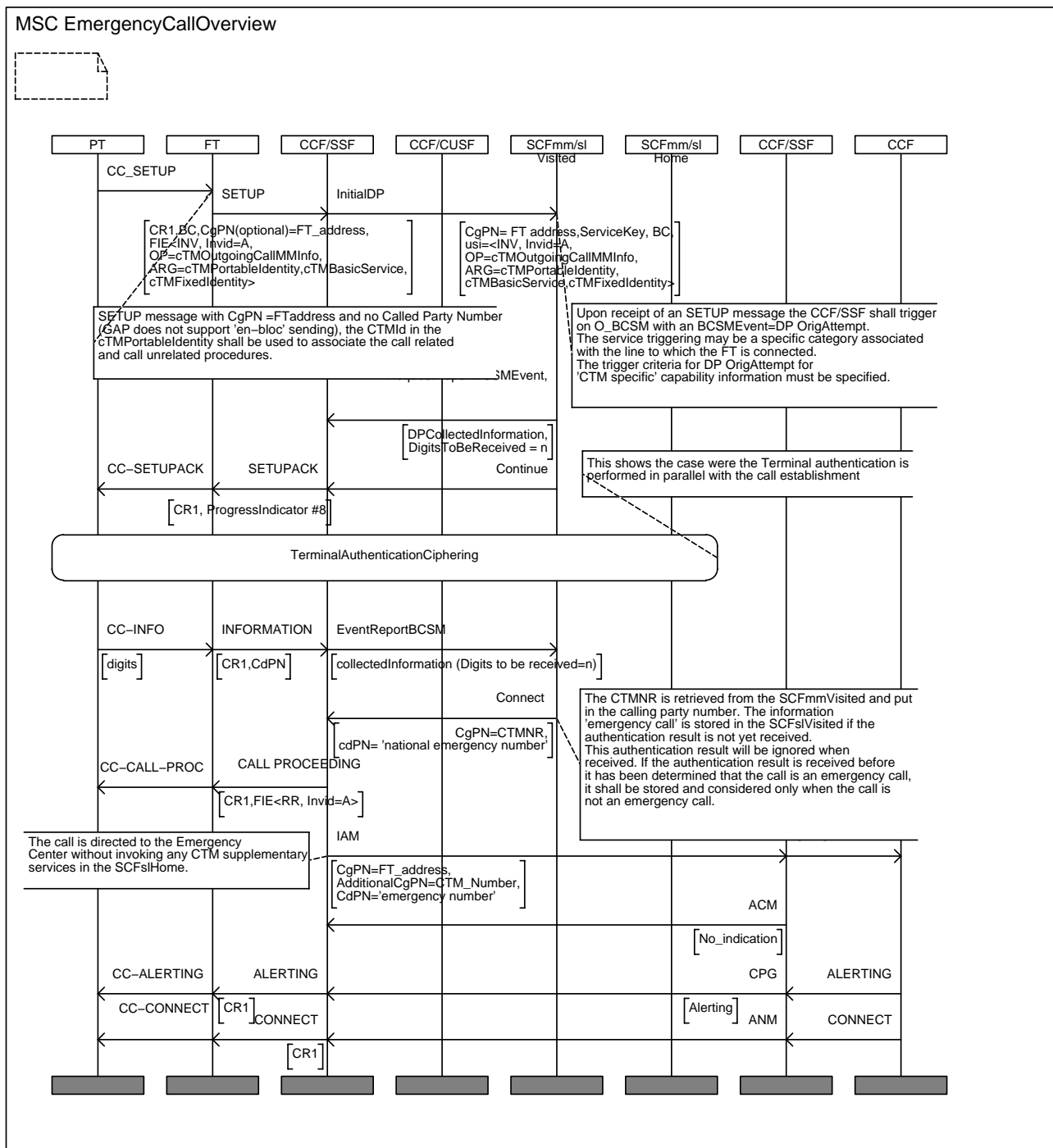


Figure B.3

Normal operation

- When the CTM user initiates a call, the FT may include in the SETUP message the FT Address as Calling Party Number, the cTMOutgoingCallMobilityManagementInfo invoke component and no Called Party Number since the GAP profile does not support en-bloc sending. The cTMOutgoingCallMobilityManagementInfo shall contain the following parameters:
 - cTMPortableIdentity: indicating the IPU (PUT and PUN), which shall be used to associate the call related and call unrelated procedures so that the same radio channel is used;
 - cTMBasicService indicating normal call setup;
 - cTMFixedIdentity indicating the PARK of the cordless terminal.

The call is routed to the CCF/SSF.

- 2) The SSF triggers the SCFslVisited on the O_BCSM in DP Originating_Attempt_Authorized with the trigger criteria based on the Service Function (part of the Facility information element of the MobilityManagementInfo) equal to CTM application. A InitialDP operation is sent to the SCFslVisited transferring the cTMOutgoingCallMobilityManagementInfo component via the USI mechanism.
- 3) The SCFslVisited may initiate terminal authentication and/or ciphering via the CUSF mechanism. The service script in the SCFslvisited decides whether authentication and ciphering is to be performed in parallel or in sequence with the call establishment or ciphering is performed prior to call establishment. The correlation between the call related procedures (normal call setup) and the call unrelated procedures (authentication, ciphering) is performed via the IPUI (PUN). The authentication result is considered when it is determined that the call is a normal call.
- 4) The SCFslVisited requests, by means of e.g. a RequestReportBCSMEvent (DPCollectedInformation, DigitsToBeReceived = n) operation or a CollectInformation operation, the appropriate number of digits in order to be able to identify that the call is an emergency call. If the SCFmmVisited has decided that the ciphering is to be performed in sequence with the call establishment, the sending of SETUPACK message over the air interface and the alpha interface is coupled with the receipt of an appropriate INAP operation (e.g. CollectInformation) and/or associated ServiceInteractionIndicatorsTwo element of the continue.
- 5) When the requested digits are received in the CCF/SSF, an EventReportBCSM operation is sent to the SCFslVisited containing in the calledPartyNumber of the collectedInfoSpecificInfo the requested digits. The SCFslVisited checks the dialled digits with regard to the standard emergency number (in Europe, "112").
- 6) If the digits match, then the SCFslVisited orders the CCF/SSF to route the call towards the emergency centre by sending a connect operation. The result of the authentication procedure SCFmmVisited is ignored and the check on CTM supplementary services (for example CTM-OCB) in the SCFslHome is not performed. The SCFslVisited provides in the connect operation the CTM-Number, if available, as CallingPartyNumber (this CTM number has been stored previously during location registration). The FT address (E.164) and the CTM-Number (E.164) are sent in the IAM message towards the emergency centre as respectively calling party number and as generic number (additional calling party number).
- 7) If the digits do not match and the terminal authentication check fails then the call is released (see exceptional procedures) by SCFmmVisited through SCFslVisited.
- 8) If the digits do not match and the terminal authentication check does not fail, the SCFslVisited will order to the CCF/SSF a subsequent triggering of the SCFslHome.

The SCFslVisited includes the following parameters in the Connect operation sent to the SSF:

- the SCFmmHomeIdd which was previously stored during the location registration and place it in the SCFId parameter;
 - the CTM-number of the calling CTM user in the CallingPartyNumber with the Presentation Indicator set to restricted;
 - the "CTM access code" is added before the dialled digits in the SSF using the CutAndPaste parameter (CalledPartyNumber = "CTM access code + DN") in order to seize CCF/SSF and trigger the SCFslHome. In order to perform the above, the SCFslVisited puts the "CTM access code" into the destinationRoutingAddress parameter and sets the cutAndPaste parameter to zero in the connect operation. The SSF now pastes the remaining dialled digits received in overlap from the CTM calling user on to the end of the "CTM access code" digits received in the destinationRoutingAddress parameter from the SCFslVisited. The "CTM access code" is deleted from the CalledPartyNumber by the CCF/SSF after triggering of the SCFslHome.
- 9) The CCF/SSF triggers in O_BCSM on DP AnalysedInformation based on the trigger criterion "CTM access code", previously received in the calledPartyNumber of the Connect operation from the SCFslVisited. The O_BCSM is re-triggered on the same instance but another service key is indicated in the InitialDP. Since no control relationship exists with the SCF it can be concluded **that this scenario does not require multiple point of control**. A monitor relationship will be maintained for the case where authentication is performed in parallel so that the SCFmmVisited can send a releaseCall operation if the authentication fails.

The SCFId parameter of the Connect operation is used to address the SCFslHome while the CTM-number is used to access the CTM user's Service Profile in the SDFslHome. This number is passed as AdditionalCallingPartyNumber in the InitialDP operation to the SCFslHome.

- 10) The SCFslHome checks the Service Profile of the CTM-user in order to invoke the CTM supplementary service (for example, the presentationIndicator of the FT_address will be set to restricted by the SCFslHome, so that it is not presented to the called user; the Presentation Indicator of the CTM-number is set according to the CTM-CLIR service) and sends a Connect operation to the CCF/SSF in order to establish the call towards the dialled number (DN). The CCF/SSF sets up the call towards the DN by sending an IAM message, including the FT_address as CallingPartyNumber and the CTM number as AdditionalCallingPartyNumber.

Exceptional procedure

- 1) If the SCFslVisited determines that the received cTMOngoingCallMobilityManagementInfo invoke component part of the USI parameter of the InitialDP operation is incorrect, or the SCFmmVisited does not receive an expected terminal authentication result for normal calls, the SCFslVisited sends a cTMOngoingCallMobilityManagementInfo return error component with error value "networkRejected" in the SendSTUI operation and releases the call by sending a ReleaseCall operation to the SSF. The ReleaseCall operation contains no specific cause so that the cause value (#31) "Normal, unspecified" is sent towards the CTM user. The SCFslVisited is also able to perform a ReleaseCall operation during the active phase of a call (for the case where authentication is performed in parallel with the call); therefore a monitor relationship will be maintained.
- 2) When the check in the SCFslVisited of the requested collected dialled digits with regard to the standard emergency number (in Europe, "112") does match and the terminal authentication check fails the SCFslVisited does not release the call. The SCFslVisited ensures that the called party number received cannot be an emergency number before releasing the call due to the failure of the terminal authentication procedure.
- 3) When the SCFmm receives the Ciphering return error component, the SCFslVisited may either release the call or proceed in the existing mode.

B.2 Incoming call

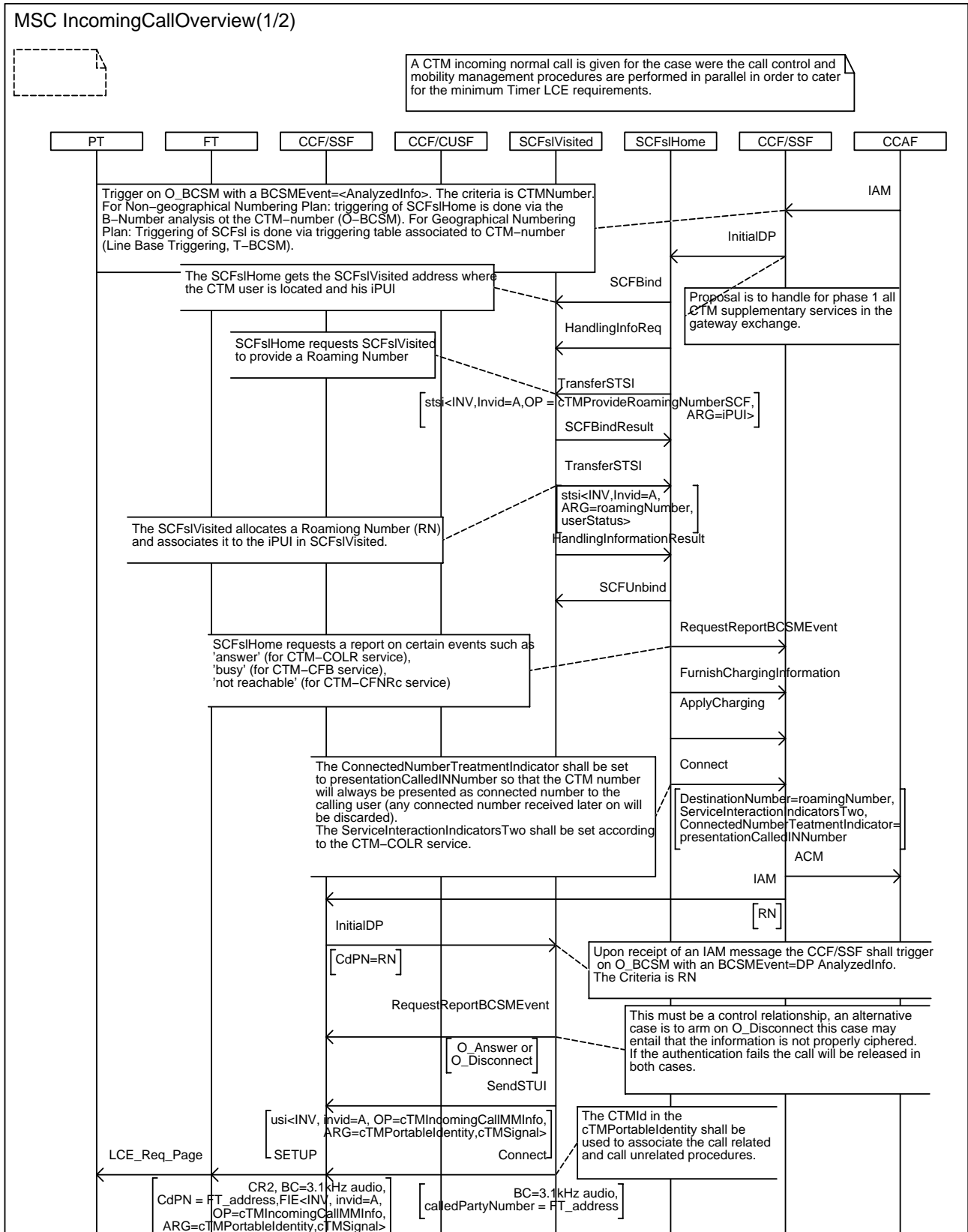


Figure B.4

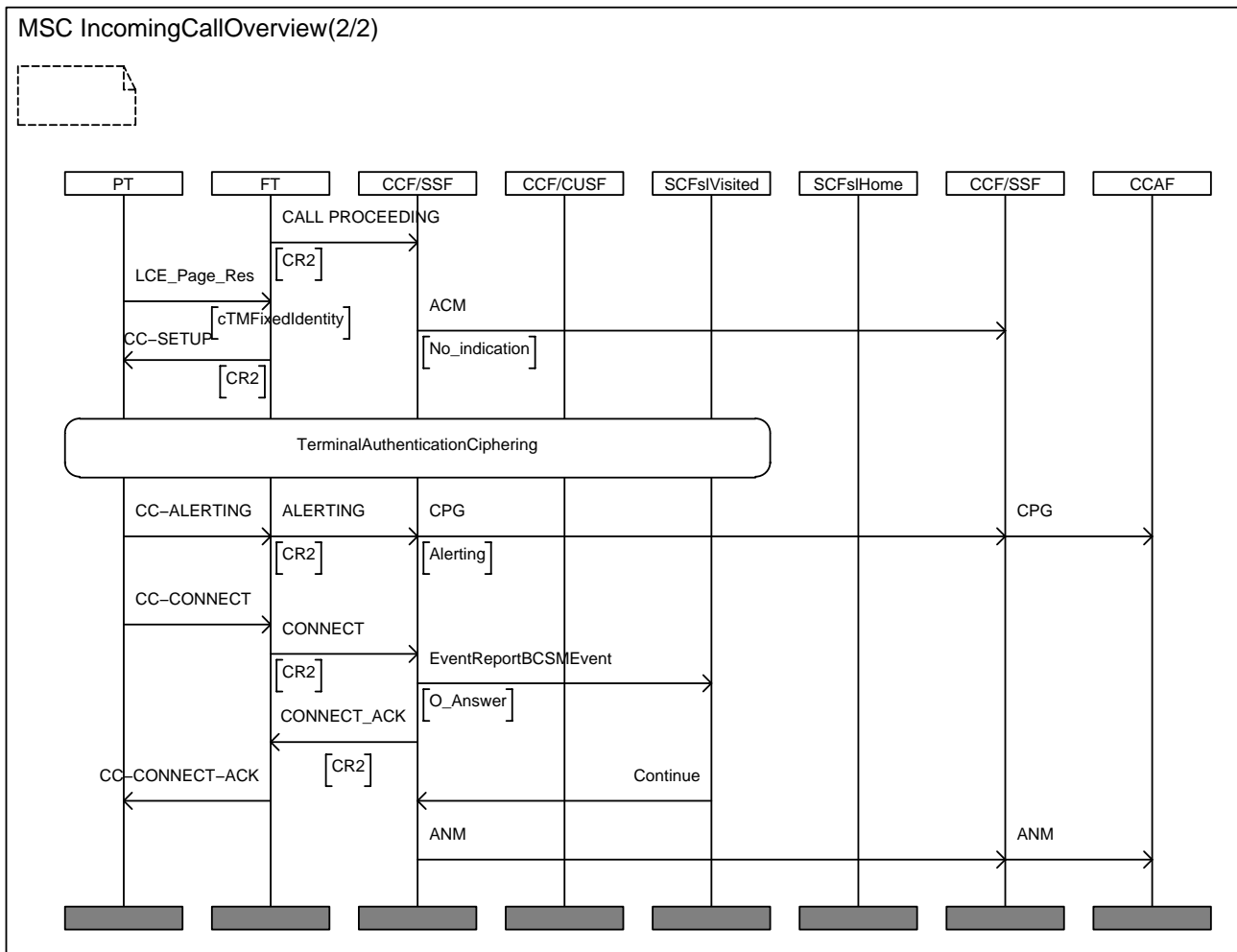


Figure B.5

Normal operation

- 1) When a CTM-number is received the call is routed by means of the ISUP IAM message to the nearest CCF/SSF.
- 2) The SSF triggers the SCFslHome by sending an InitialDP and is based on whether the CTM-number is belonging to a geographical or non-geographical numbering plan.

For the non-geographical numbering plan, the SSF triggers based on the B party analysis on the O_BCSM with a BCSMEvent equal to AnalysedInformation and the service criteria is based on the CTM-number.

For the geographical numbering, plan the SSF triggers based on a triggering table associated with the CTM-number (line based triggering) on the T_BCSM with the BCSMEvent equal to TerminationAttempt and the service criteria is based on the CTM-number.

In order to address the SCFslHome, the CTM-number is used to be translated to a global title.

- 3) The SCFslHome requests the SCFslVisited for a Roaming Number (RN) by sending an cTMProvideRoamingNumberSCF invoke component using the SSI mechanism on the SCF-SCF interface. The cTMProvideRoamingNumberSCF invoke component contains the IPUI as parameter.
- 4) On receipt of the cTMProvideRoamingNumberSCF, the SCFslVisited checks whether the CTM user is registered or not.

If the CTM user is defined as not reachable in the SCFslVisited, the SCFslVisited returns the cTMProvideRoamingNumberSCF return result component using the SSI mechanism on the SCF-SCF interface, containing the status of the user (userNotReachable).The SCFslHome can execute the CTM supplementary service CTM-CFNRc, if active for the user.

The SCFslHome in the Gateway will be the network where all terminating CTM supplementary services are executed (e.g. CTM-COLR, CTM-CLIP, CTM Call Forwarding services). For this reason the SCFslHome requests via a requestReportBCSMEvent operation Basic Call State Machine (BCSM) events such as O_Answer, O_NoAnswer, O_NotReachable, O_Busy, O_Disconnect.

- 5) The SCFslHome instructs the SSF by sending a Connect operation to route the call with the following parameters:
 - DestinationNumber containing the roaming number;
 - ServiceInteractionIndicatorsTwo indicating that the dialled number is to be used as connected number;
 - ConnectedNumberTreatmentIndicator set to presentationRestricted if the CTM user has CTM-COLR.
- 6) The call is routed towards the local exchange where the CTM user is located.
- 7) In the visited domain the CCF/SSF triggers the SCFslVisited on the O_BCSM with a BCSMEvent equal to AnalysedInfoDP and the service criteria is based on the roaming number.
- 8) The SCFslVisited releases the roaming number and the SCFmmVisited initiates terminal authentication and/or ciphering via the CUSF mechanism. The SCFmmVisited service script decides whether the authentication and/or ciphering is to be performed in parallel or in sequence with the call setup. A correlation function is performed between the call related and call unrelated procedures by means of the IPUI parameter.

If the terminal authentication and ciphering is run in sequence to the call setup, the call may in some cases not be ciphered because the DECT GAP "Link maintain timer": LCE.02 may be set to zero in the PP. This causes the radio link to be taken down when the ciphering is completed and before the call setup is sent to the PP.

If the terminal authentication and ciphering is run in parallel to the call setup, the signalling information on the air is not ciphered before the cipher request is sent to the PP.

It is noted that for non-geographical numbers **in the case the CTM user has not roamed away from the node where the SCFslHome was triggered, there will be a multiple point of control for the AnalysedInformation DP.**

The SCFslVisted generates an announcement towards the A subscriber if the call setup takes too long a time and an early Address Complete Message (ACM) message in the ISUP protocol will be generated.

- 9) The SCFslVisited requests the CCF/SSF to route the call towards the towards the FT by sending a connect operation containing a calledPartyNumber equal to the FT_address. The SCFslVisited includes the cTMIncomingCallMobilityManagementInfo invoke component using the USI mechanism in the SendSTUI operation.

The cTMIncomingCallMobilityManagementInfo invoke component contains the following parameters:

- cTMPortableIdentity containing the IPUI;
- cTMSignal containing the signal to be generated by the portable.

- 10) The CCF/SSF routes the call towards the FT.

Annex C (informative): SDL model

This annex contains the SDL model of the CTM application. The SDL model is informative only.

C.1 System Type scf_scf_network

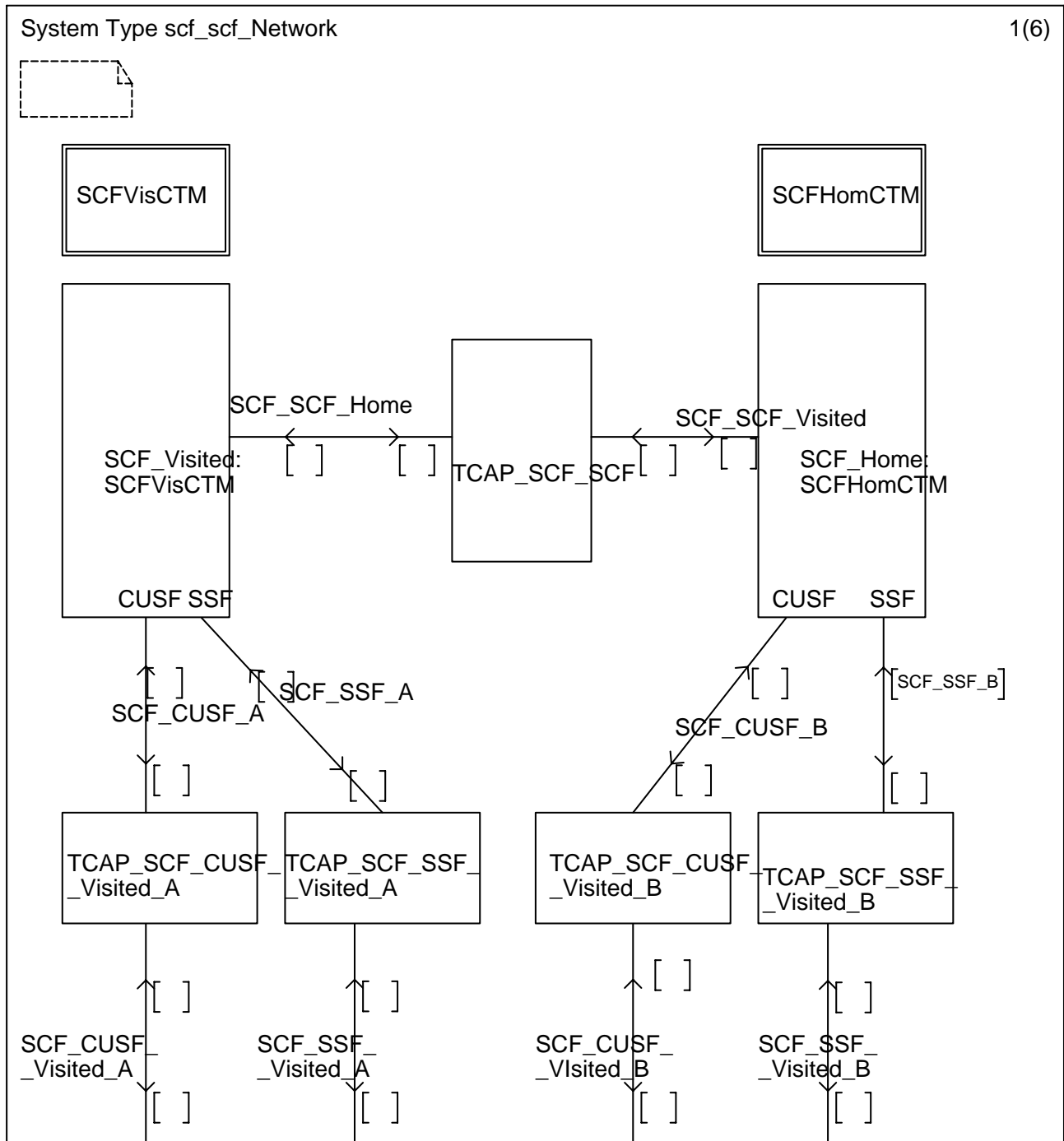


Figure C.1

System Type scf_scf_Network

2(6)



/*
 The SDL diagrams reflect an Application Layer Structure (ALS) where the SACF performs the association co-ordination function.
 The Visited SCF has four Application Service Entities (ASEs) namely:

SCFVis	having process type SCF_SSF_CUSF_ASE_Visited, for communication with the SSF/CUSF in the Visited Domain.
SCFmmVisApp	having process type SCFmmVisitedApplication, performing the service logic for the CTM Phase 1 mobility management call unrelated applications in the Visited SCF Domain.
SCFslVisApp	having process type SCFslVisitedApplication, performing the service logic for the CTM Phase 1 call related applications in the Visited SCF Domain.
SCF_SCFVis	having process type SCF_SCF_ASE_Visited, for communication with the SCF in the Home Domain.

The Home Domain SCF has four Application Service Entities (ASEs) namely:

SCFHom	having process type SCF_SSF_CUSF_ASE_Home, for communication with the SSF/CUSF in the Home Domain.
SCFmmHomApp	having process type SCFmmHomeApplication, performing the service logic for the CTM Phase 1 mobility management call unrelated applications in the Home SCF Domain.
SCFslHomApp	having process type SCFslHomeApplication, performing the service logic for the CTM Phase 1 call related applications in the Home SCF Domain.
SCF_SCFHom	having process type SCF_SCF_ASE_Home, for communication with the SCF in the Visited Domain.

The SCFHom and SCFVis ASEs communicate with the TCAP adaptors for the CUSF and SSF entities, while the SCF_SCFHom and SCF_SCFVis communicate with the TCAP adaptors for the peer SCF entities.

The association instance for the SCFHom and SCFVis is identified by either the cUSFdialogueID for call unrelated CUSF communication or by the sSFdialogueID for call related SSF communication.
 The association instance for the SCF_SCFHom and SCF_SCFVis is identified by the sCFdialogueID for communication with the peer SCF entity. The association instance for the SCFmmVisApp and SCFmmHomApp is identified by the mMdialogueID while for the SCFslVisApp and SCFslHomApp is identified by the sLdialogueID.

During one dialogue unique invoke identifiers are generated. They are obtained by calling a GetInvokeID procedure within the send signal parameter e.g. ContinueAssociationRequest((call GetInvokeID), cUSFdialogueID, conaArg)

The communication of the ASEs performing the transport functions via the SACF are given by the appropriate signal name e.g. RequestReportBCUSMEvent for the invoke component, by RequestReportBCUSMEventRes for the return result component and by RequestReportBCUSMEventErr for the return error component.

The association instances for the SCFmmVisApp, SCFmmHomApp, SCFslVisApp and SCFslHomApp ASEs are identified by the Process Instance Identifiers (PID).
 Since the signals send from or received by the transport ASEs by/from the application processes are not unique due to the fact that :

- * relaying of signals from the SCFHome occur in the SCFVisited SACF, and;
- * embedded procedures are invoked for the same entity

it is required that different dialogue identifiers are used. In this respect a qualifier will indicate the nesting which has occurred e.g. cUSF1dialogueID.

For the ASEs the creation of an application process instance is initiated by sending a CreateASE signal with a parameter indicating the process which is addressed e.g. SCFmmVisApp.
 The processes addressed are indicated by a parameter value having the type
 TypeOfASE ::= ENUMERATED { -- Indicates the type of ASE to be created by SACF
 SCFmmVisApp,
 SCF_SCFVis,
 SCFmmHomApp,
 SCF_SCFHom,
 SCFVis,
 SCFHom
 }
 The process instances are terminated by sending an ASETerminated(x) signal, where x designates the TypeOfASE e.g. SCFmmVisApp.

For the TCAP simulator the signal ApplicationBegin and ApplicationEnd are used.

Figure C.2

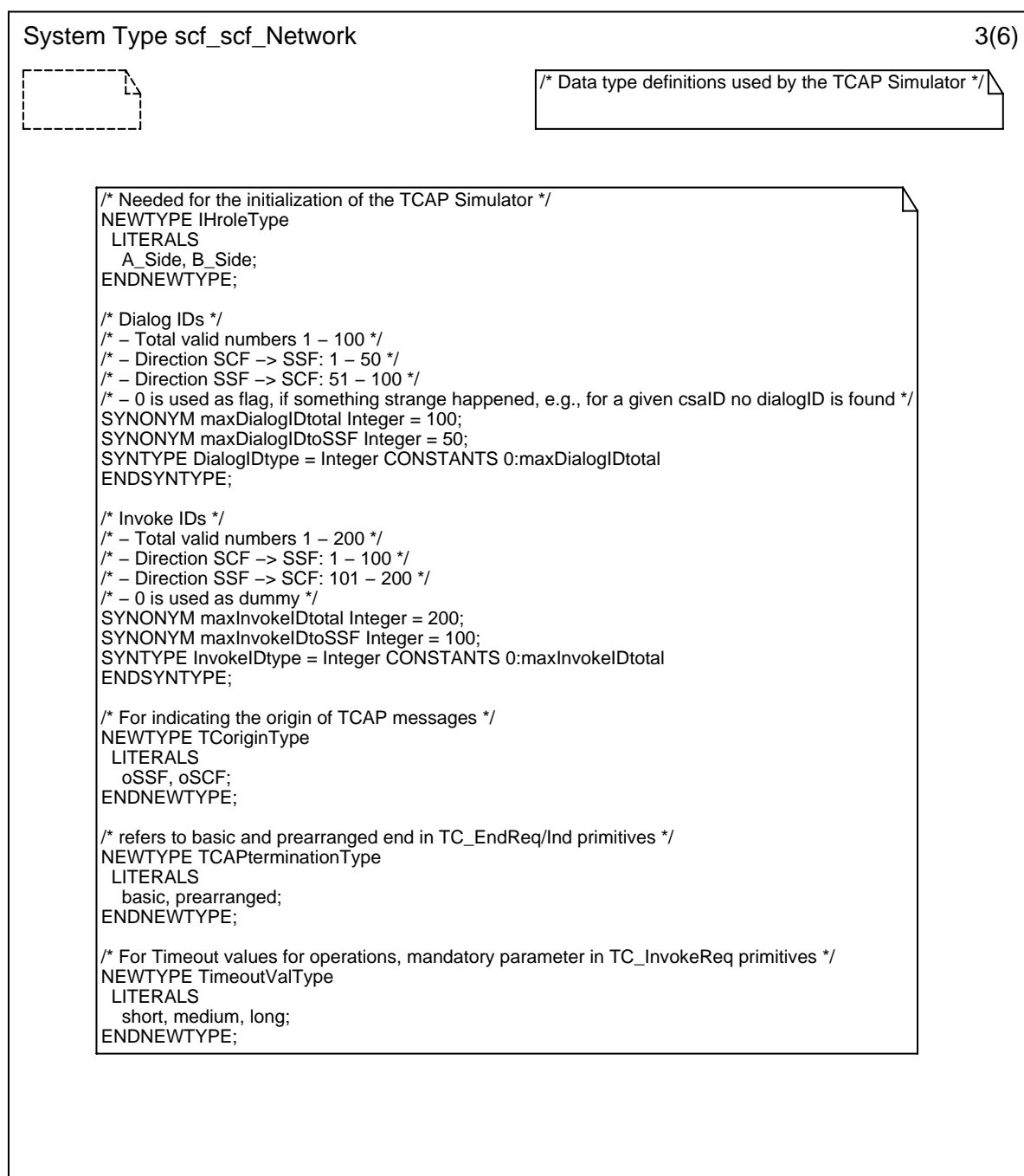


Figure C.3

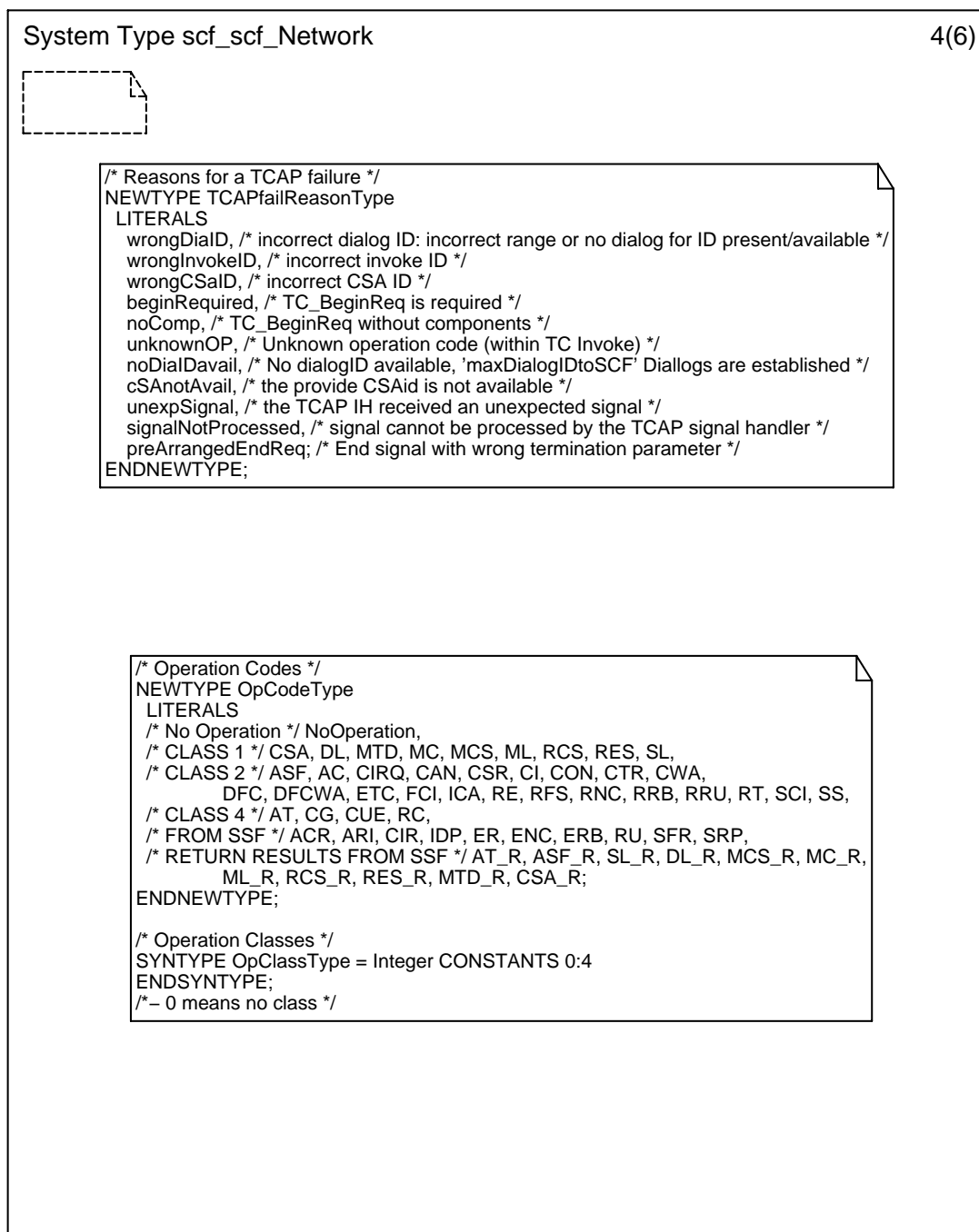


Figure C.4

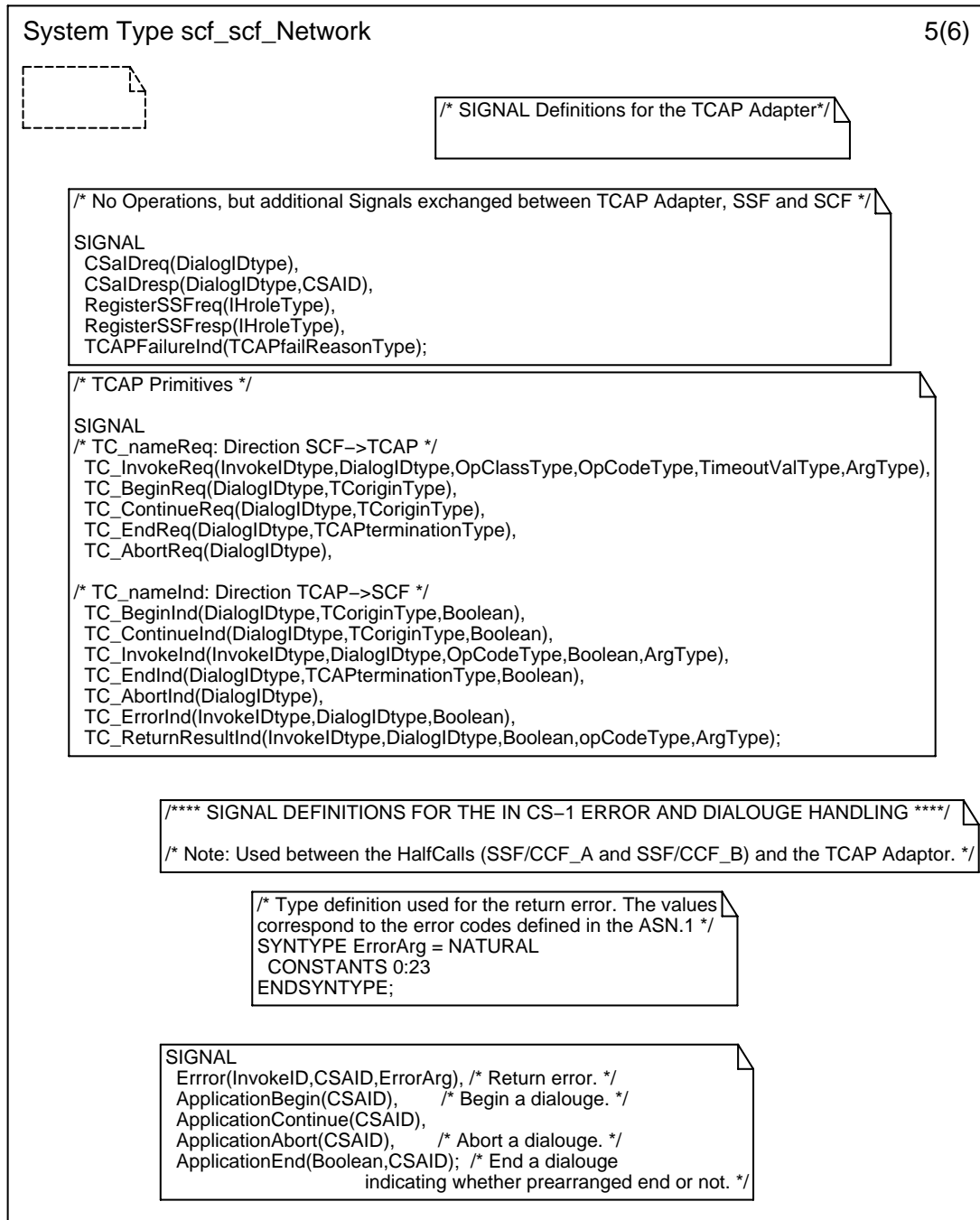


Figure C.5

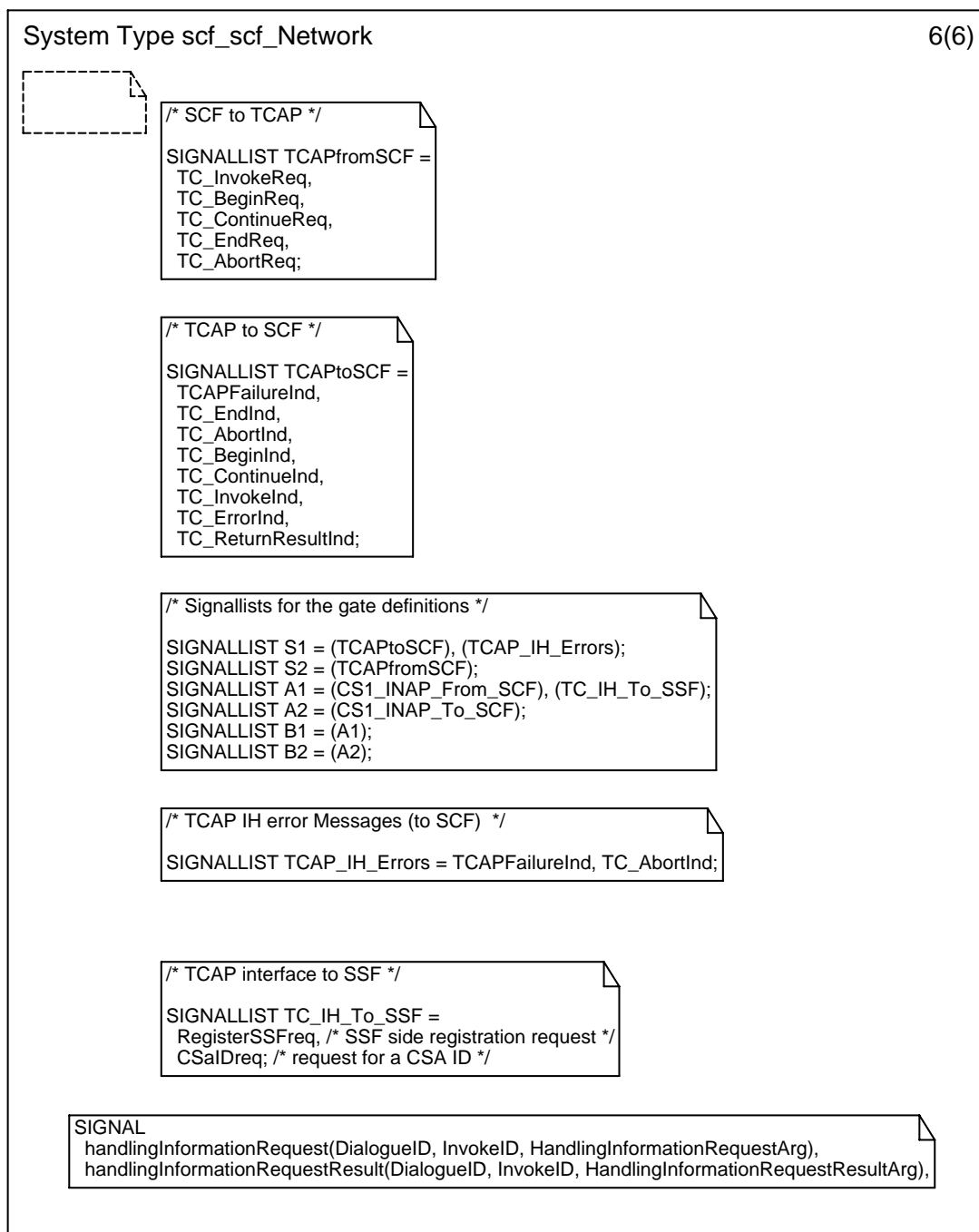


Figure C.6

C.2 Block Type SCFVisCTM

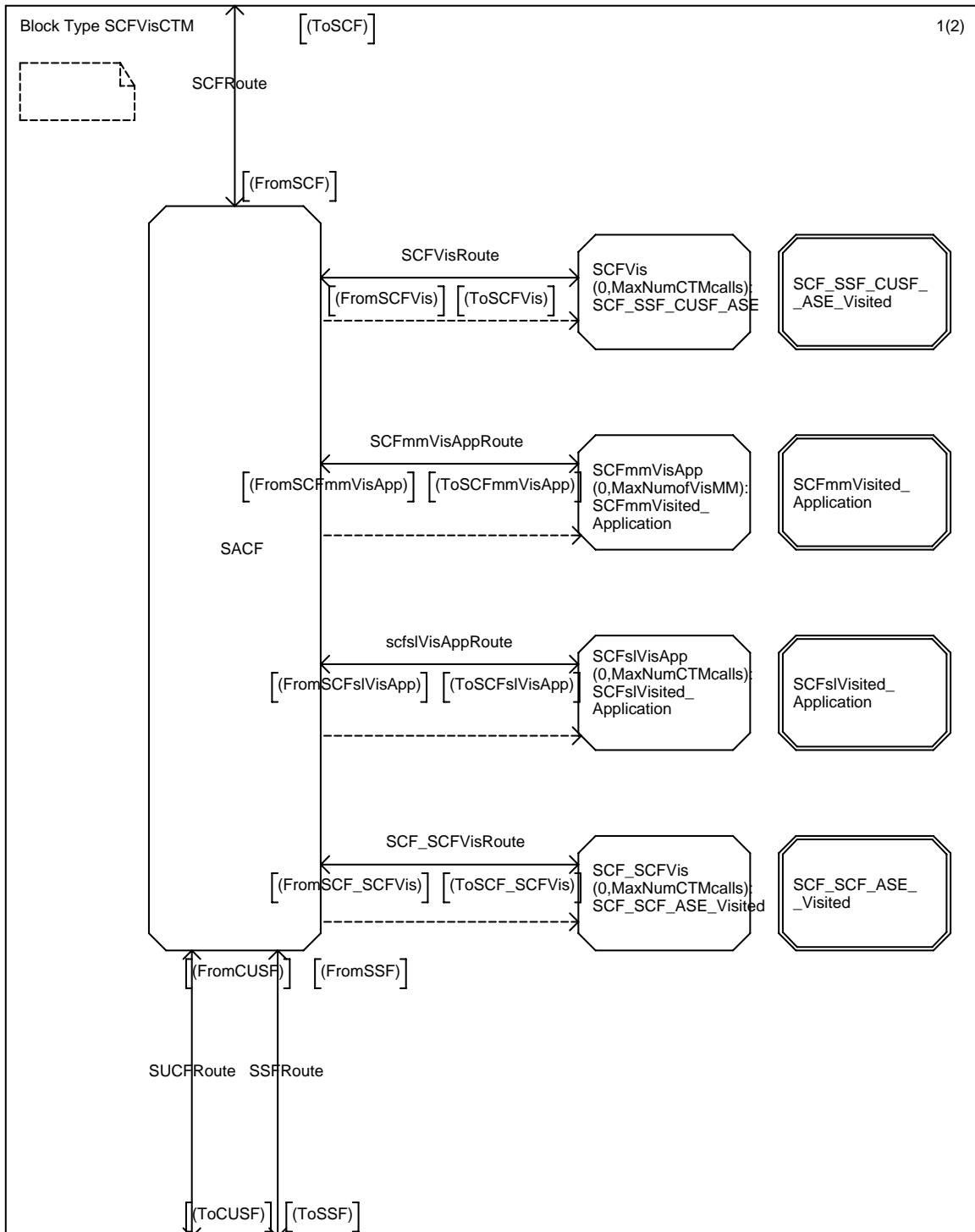


Figure C.7

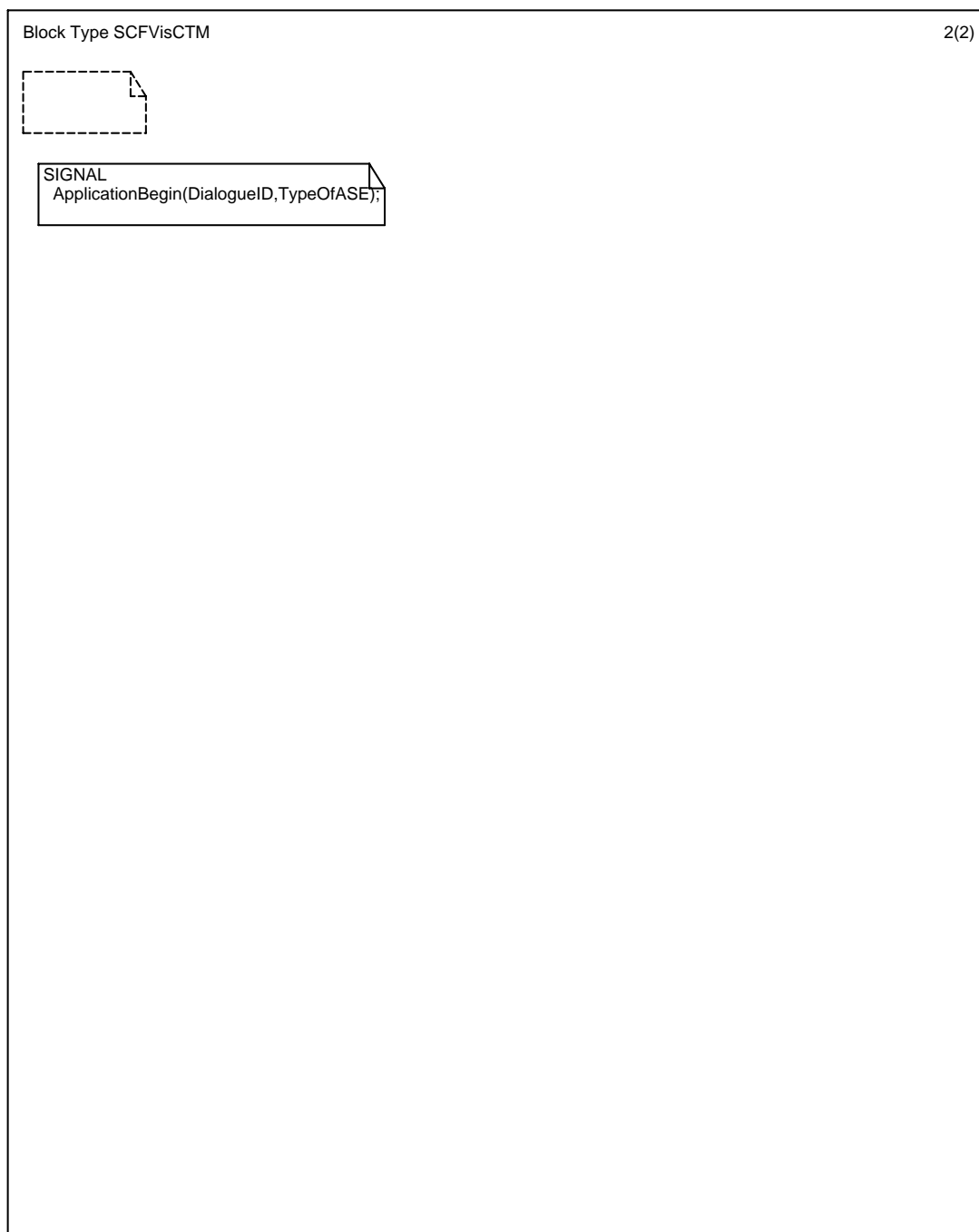


Figure C.8

C.3 Process Type SCF_SCF_CUSF_ASE_Visited

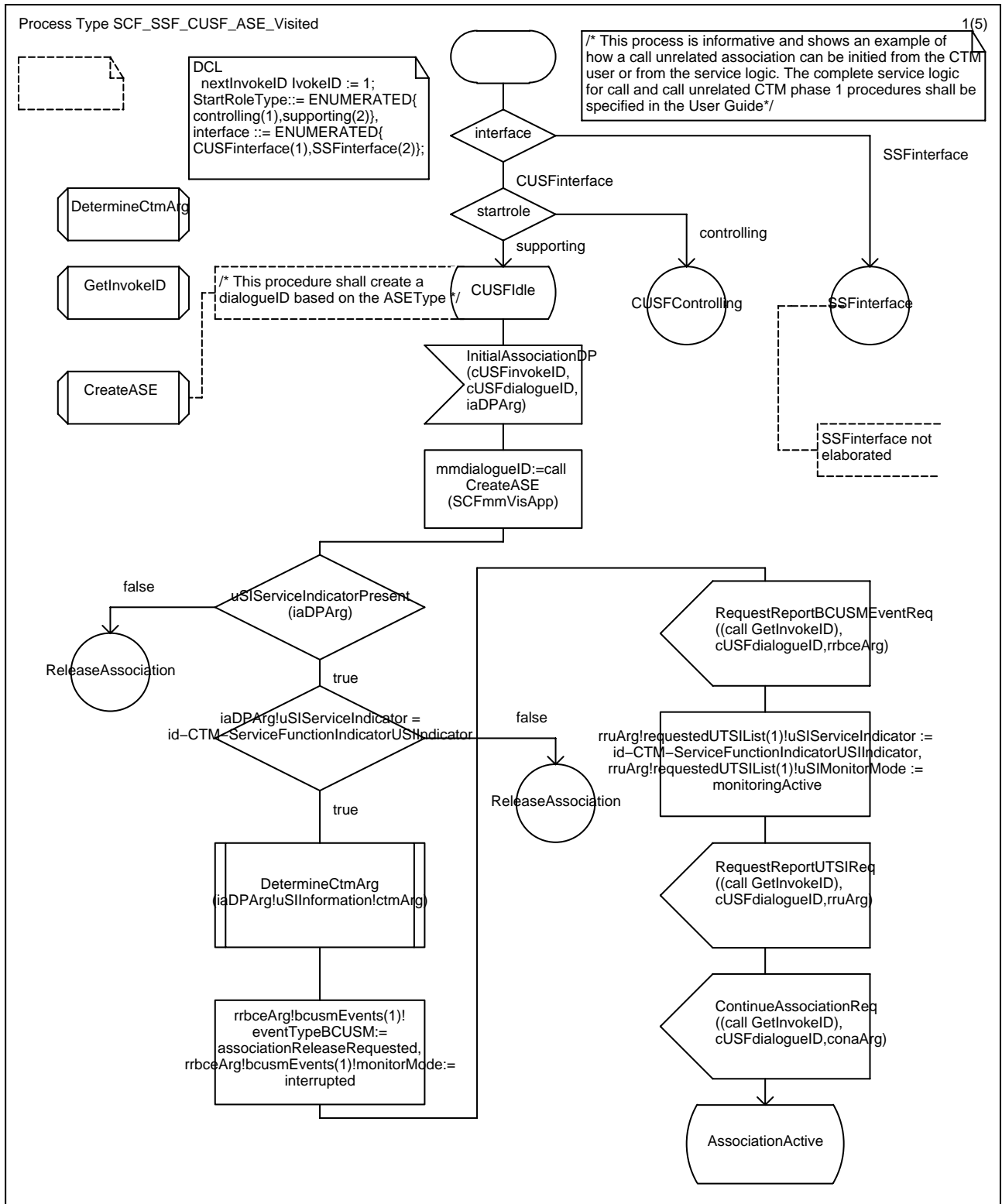


Figure C.9

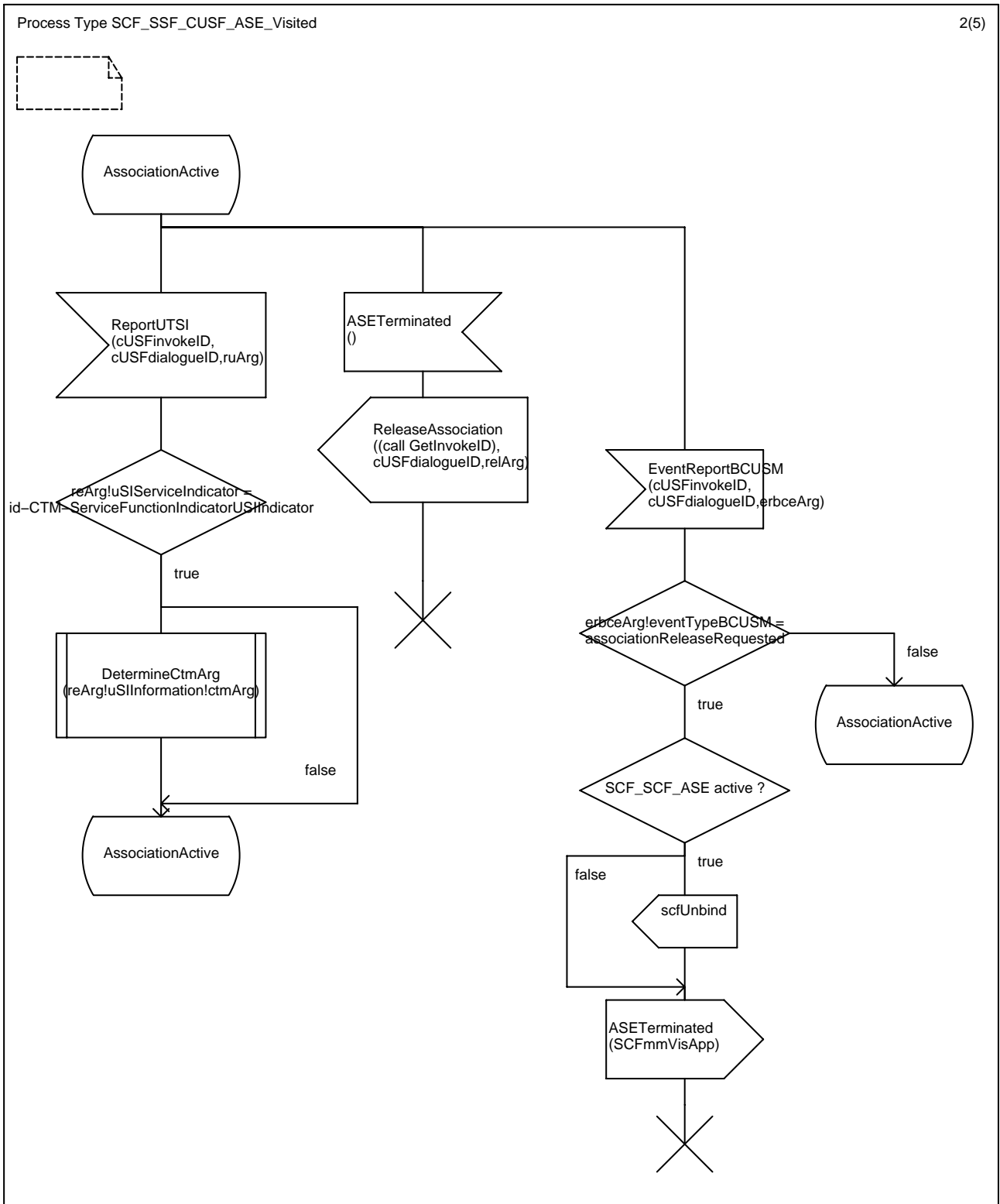


Figure C.10

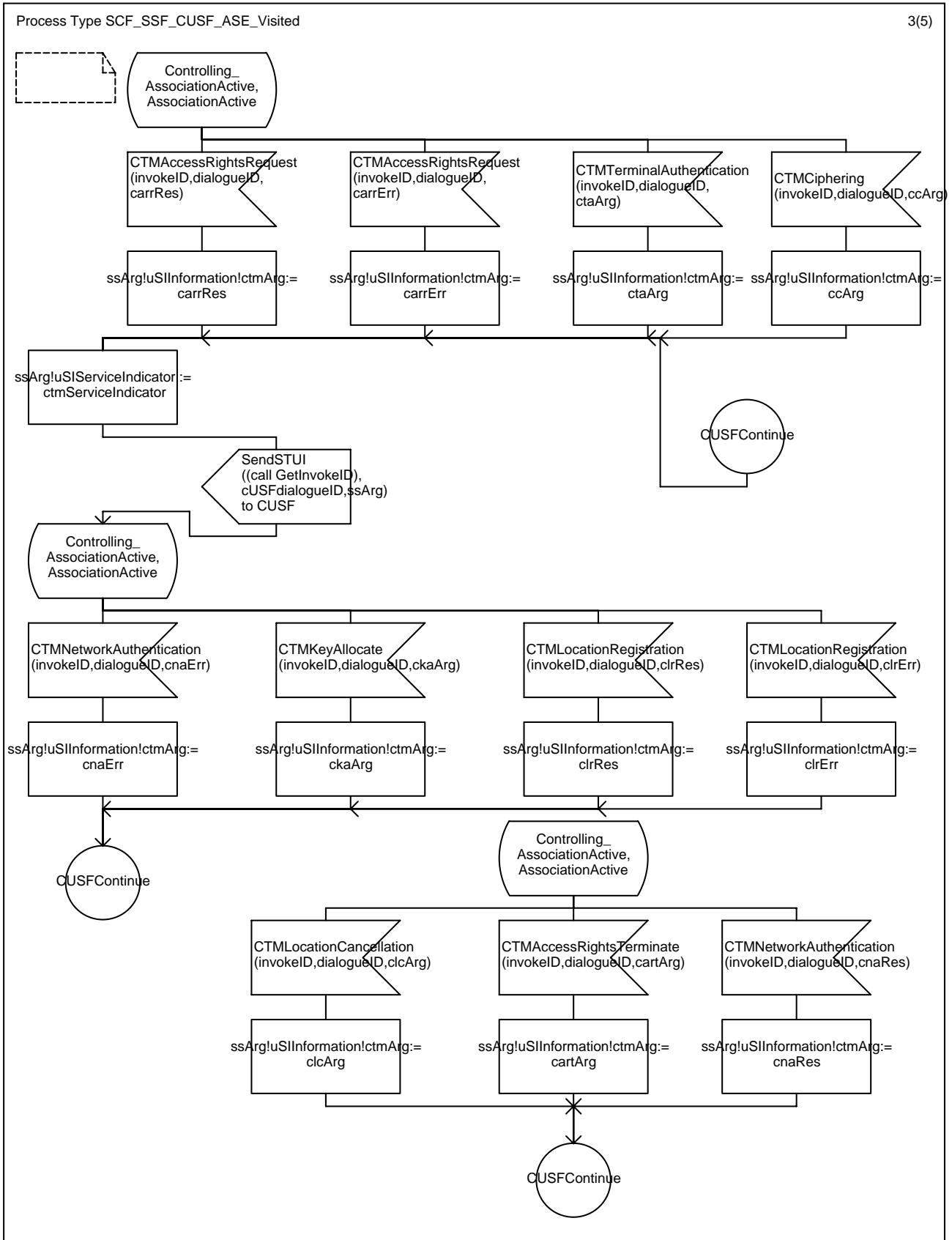


Figure C.11

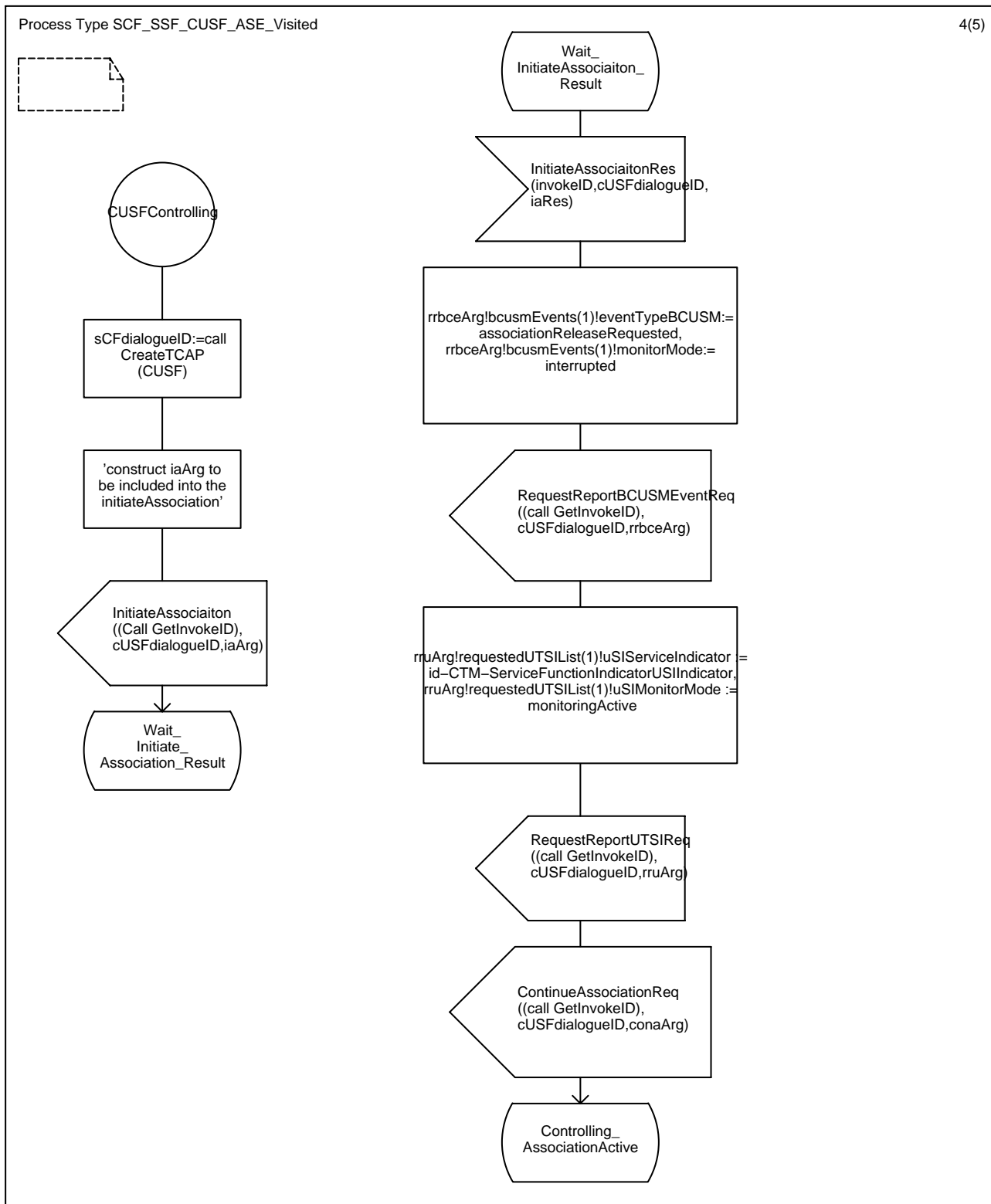


Figure C.12

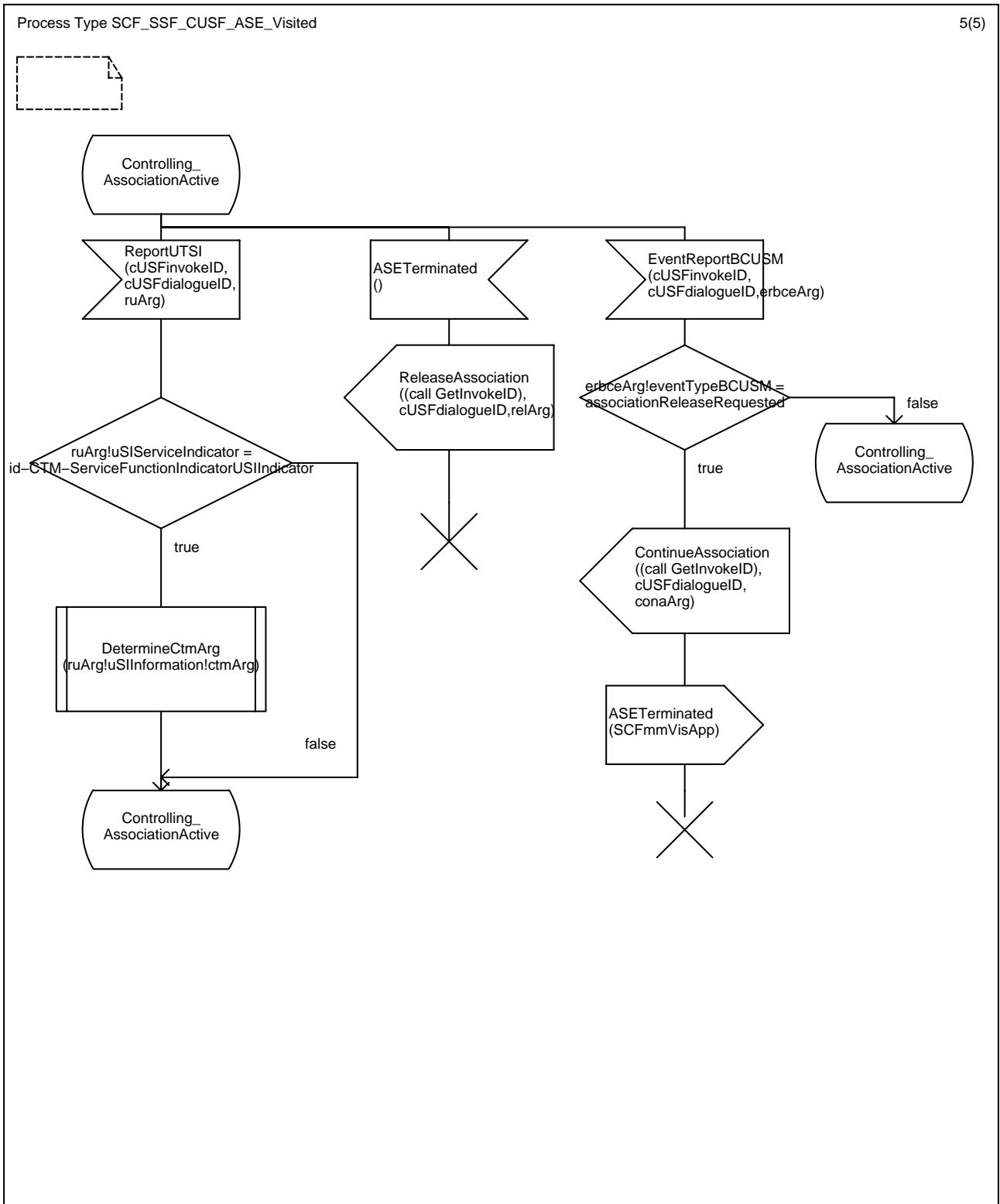


Figure C.13

C.4 Procedure DetermineCtmArg

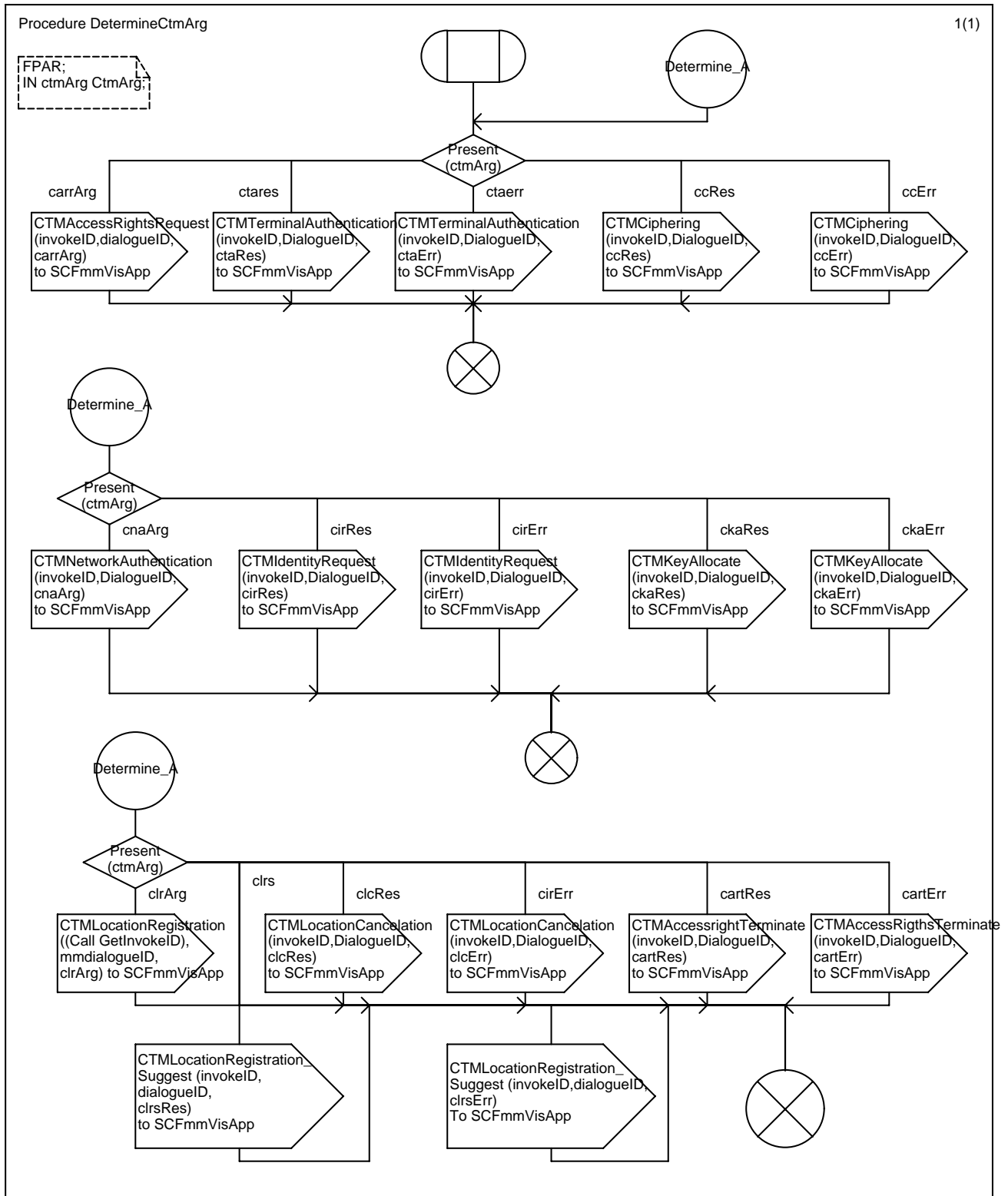


Figure C.14

C.5 Procedure GetInvokeID

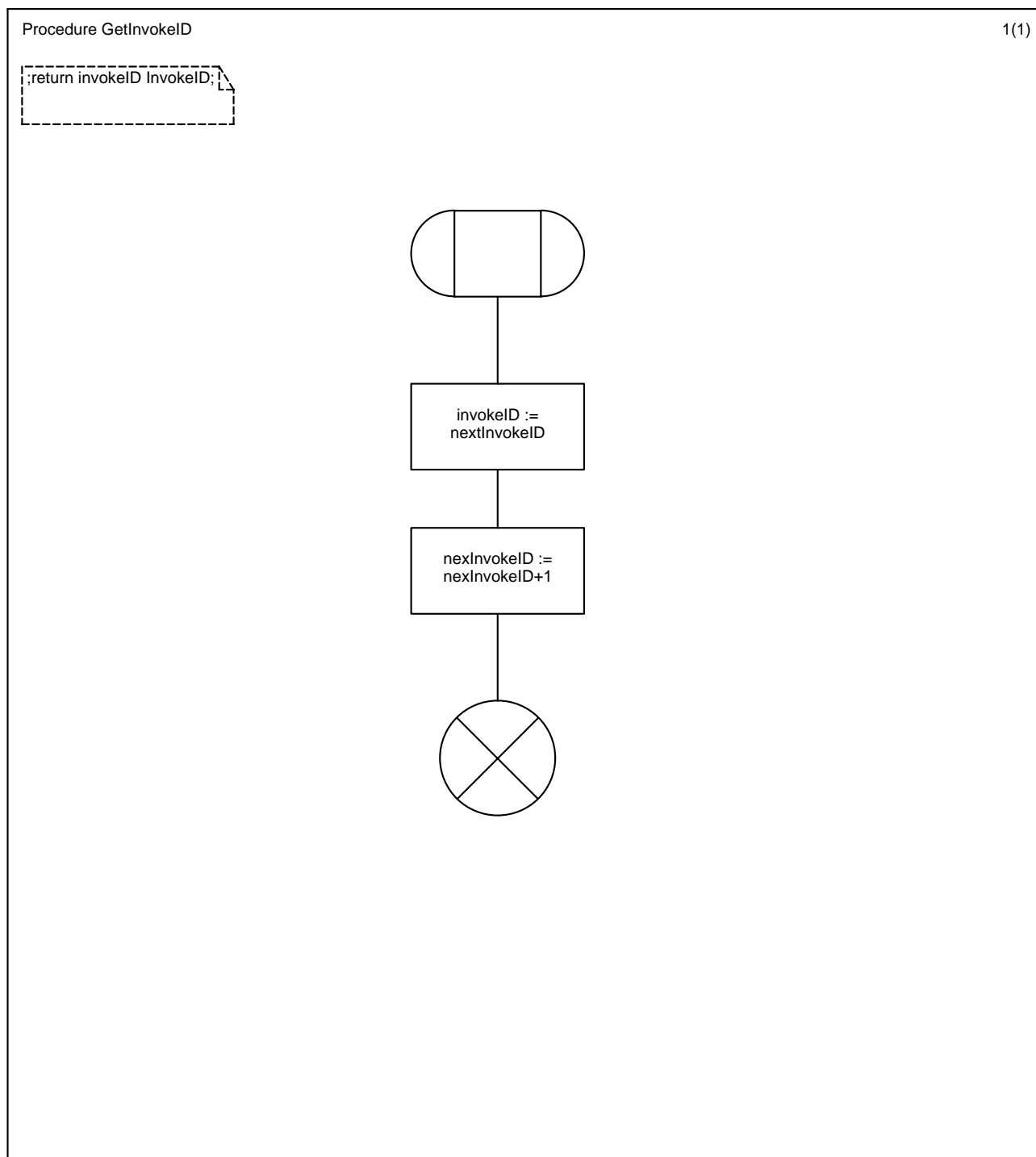


Figure C.15

C.6 Process Type SCFmmVisitedApplication

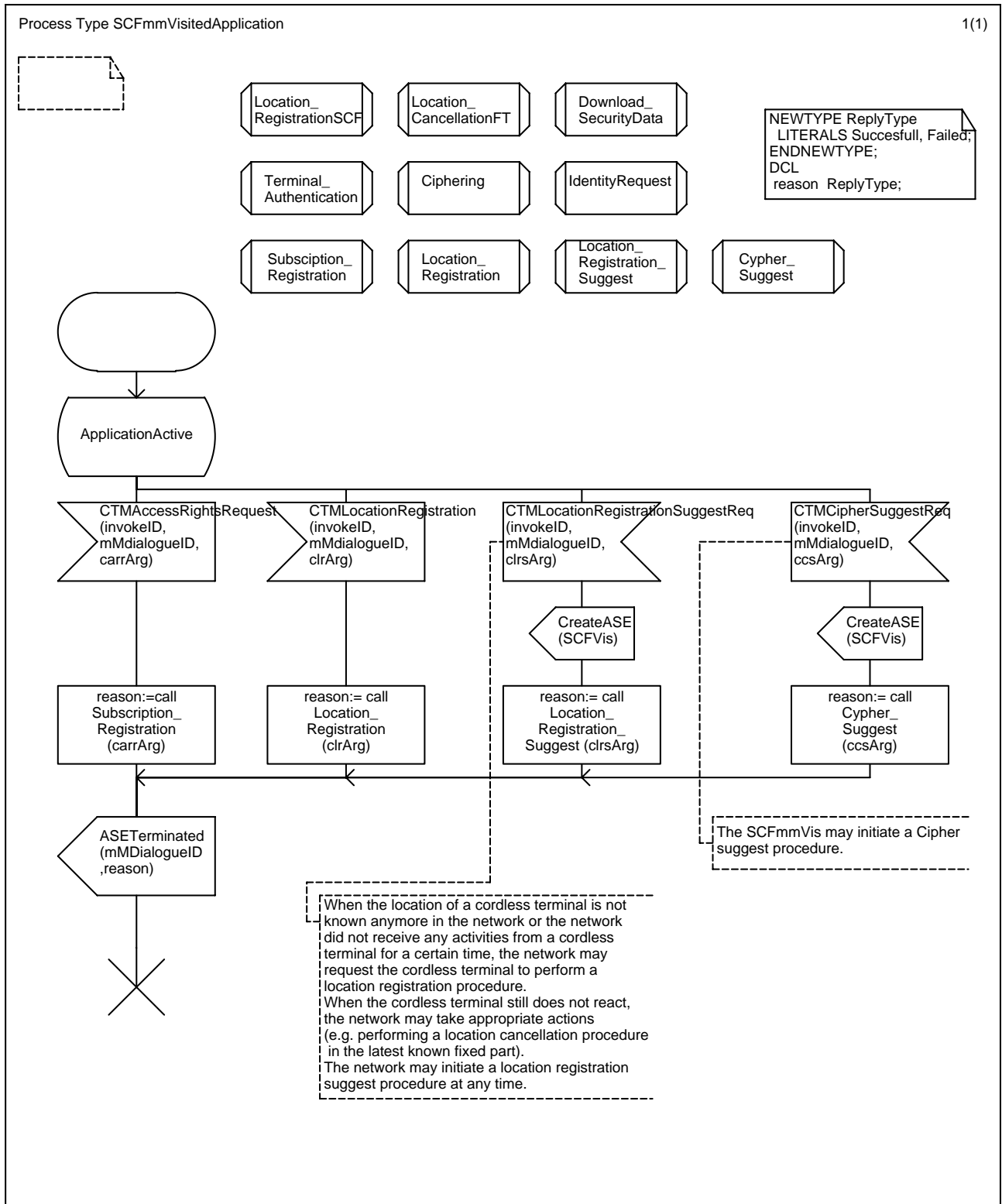


Figure C.16

C.7 Procedure LocationRegistrationSCF

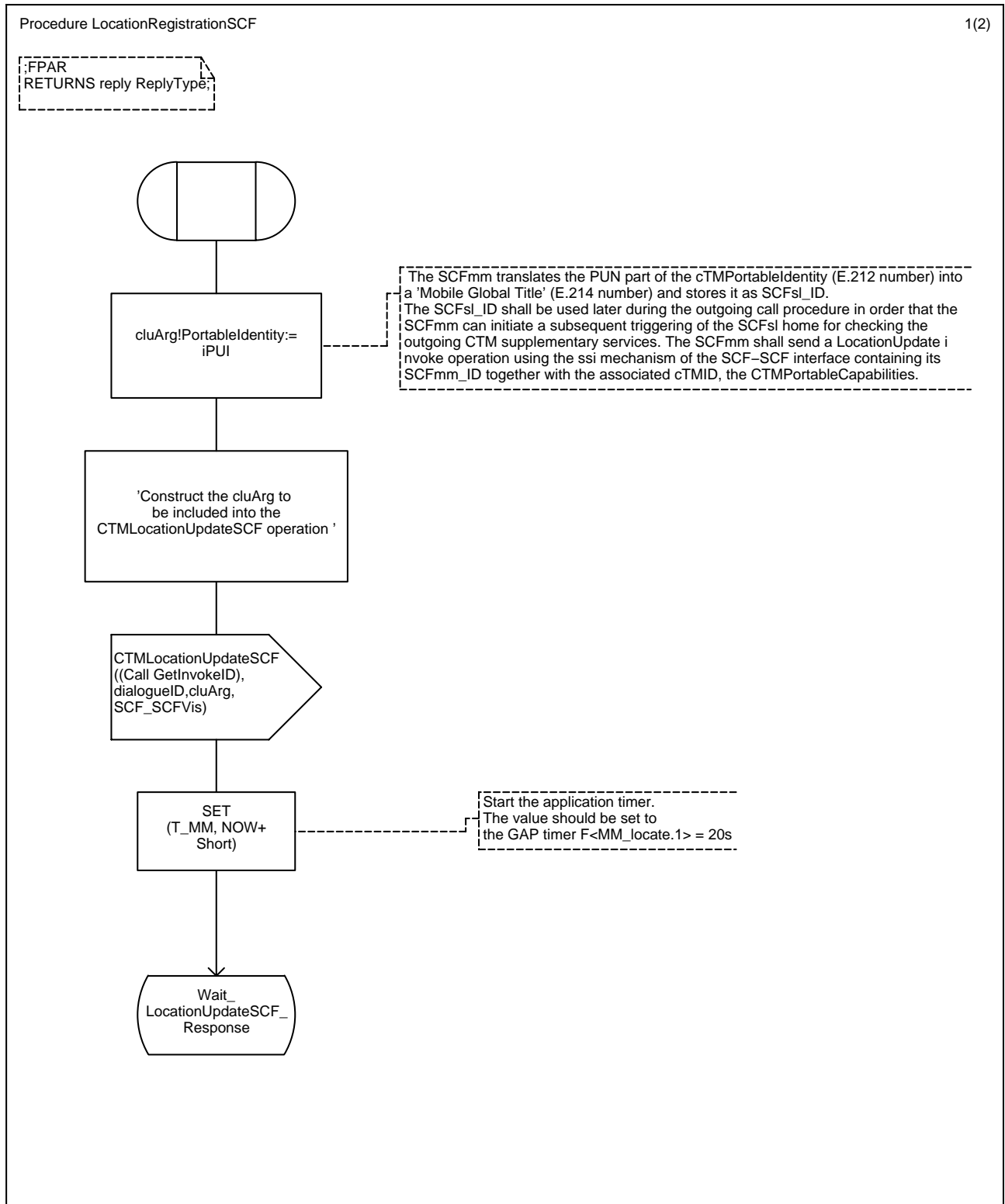


Figure C.17

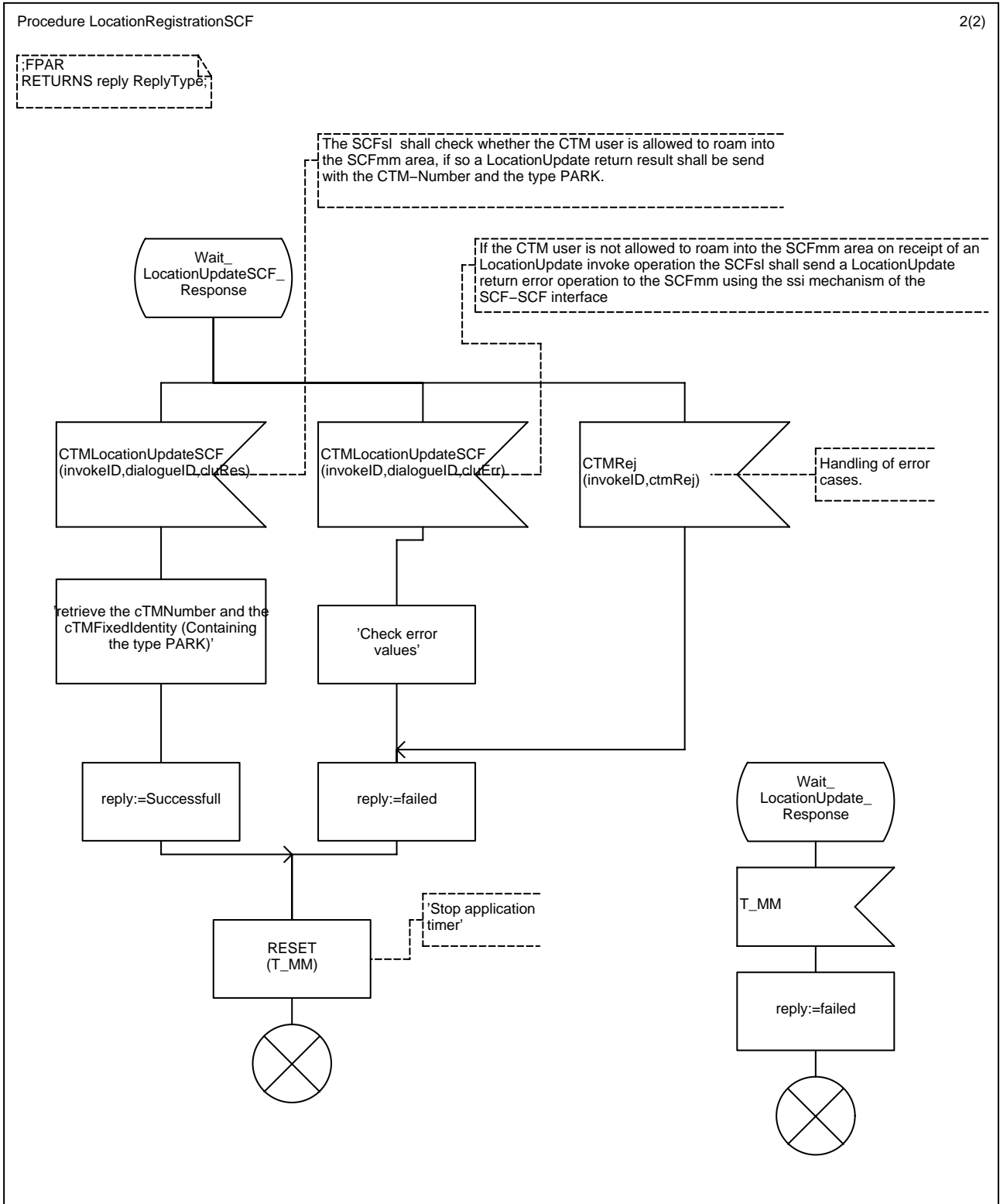


Figure C.18

C.8 Procedure LocationCancellationFT

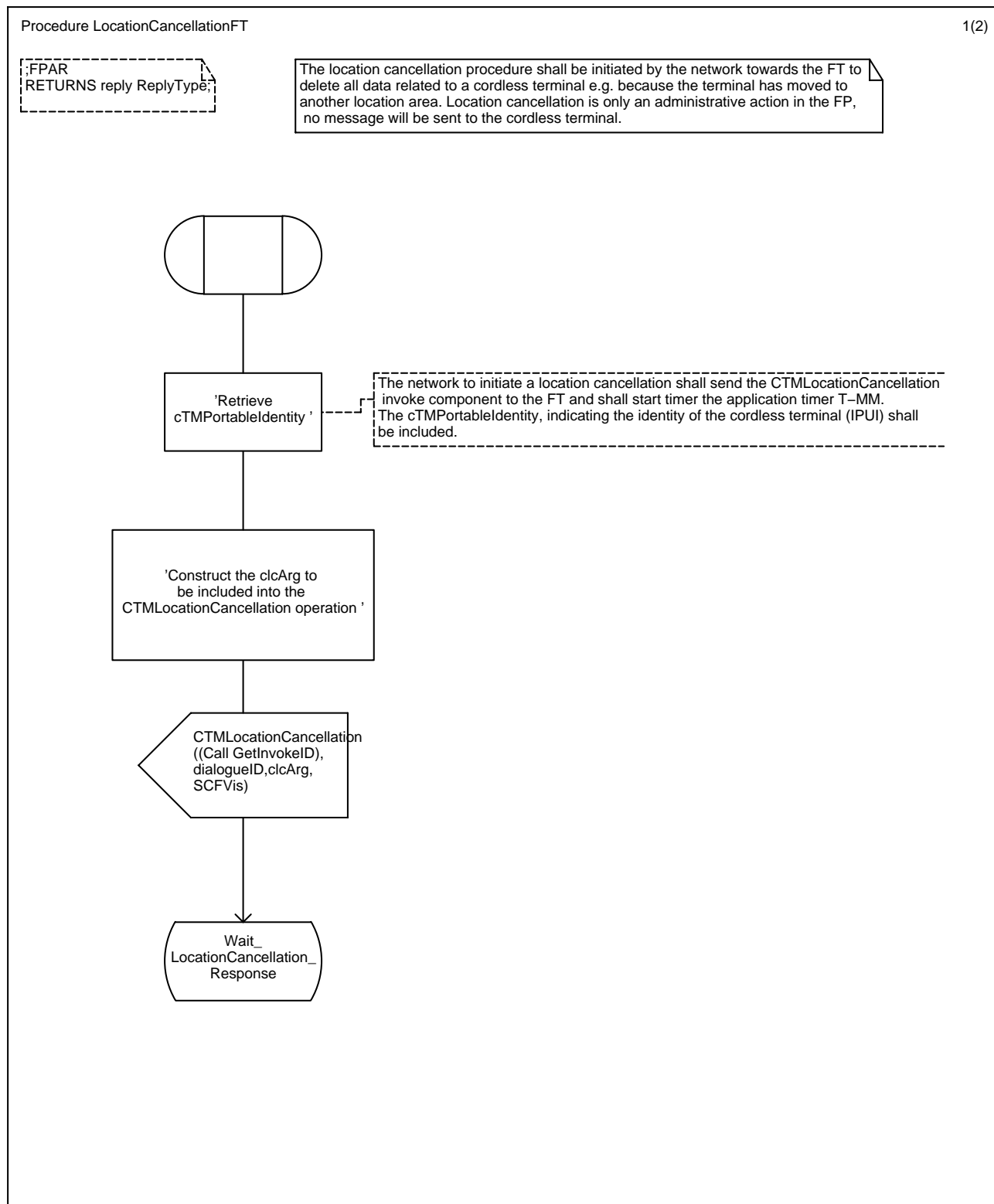


Figure C.19

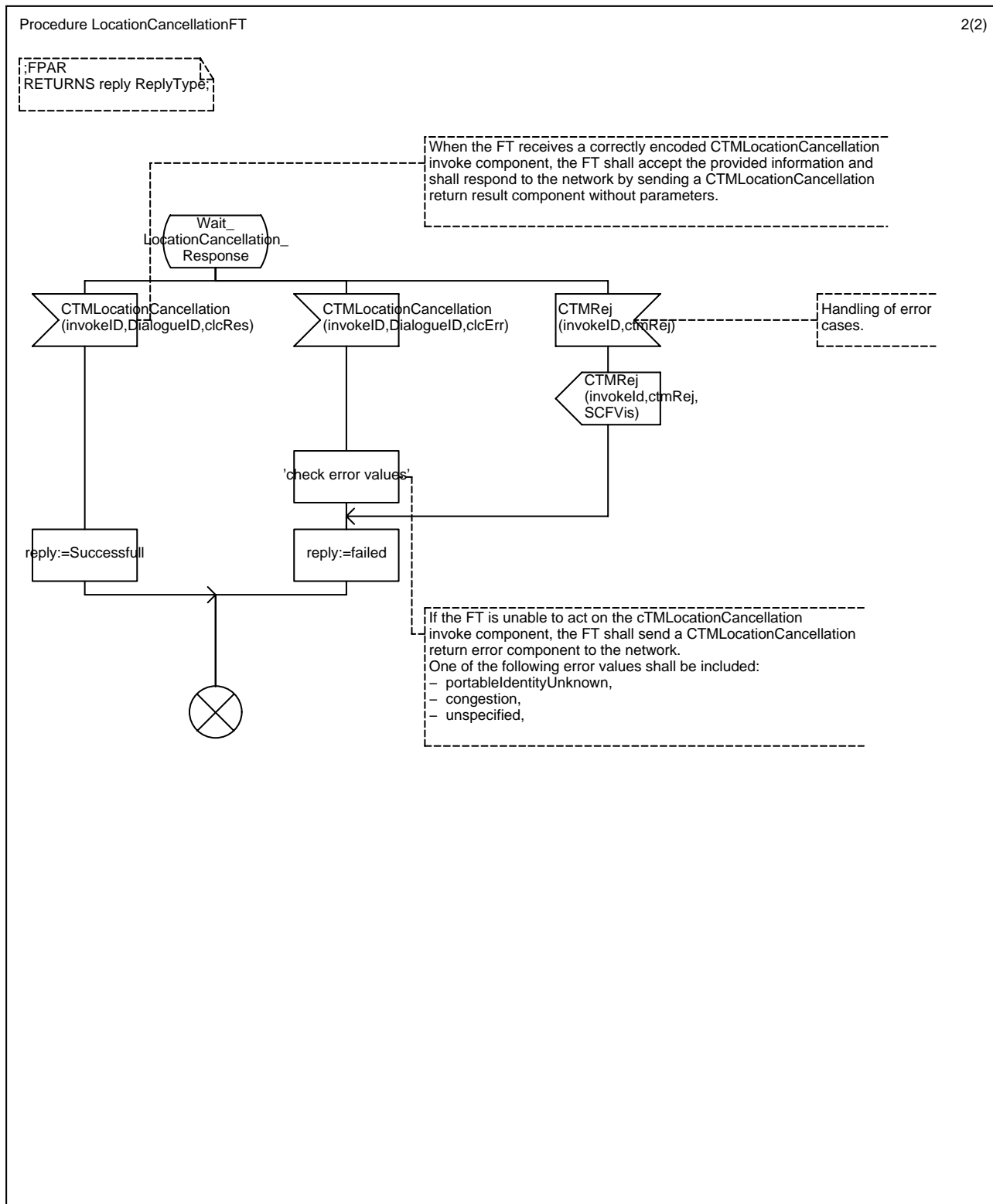


Figure C.20

C.9 Procedure DownloadSecurityData

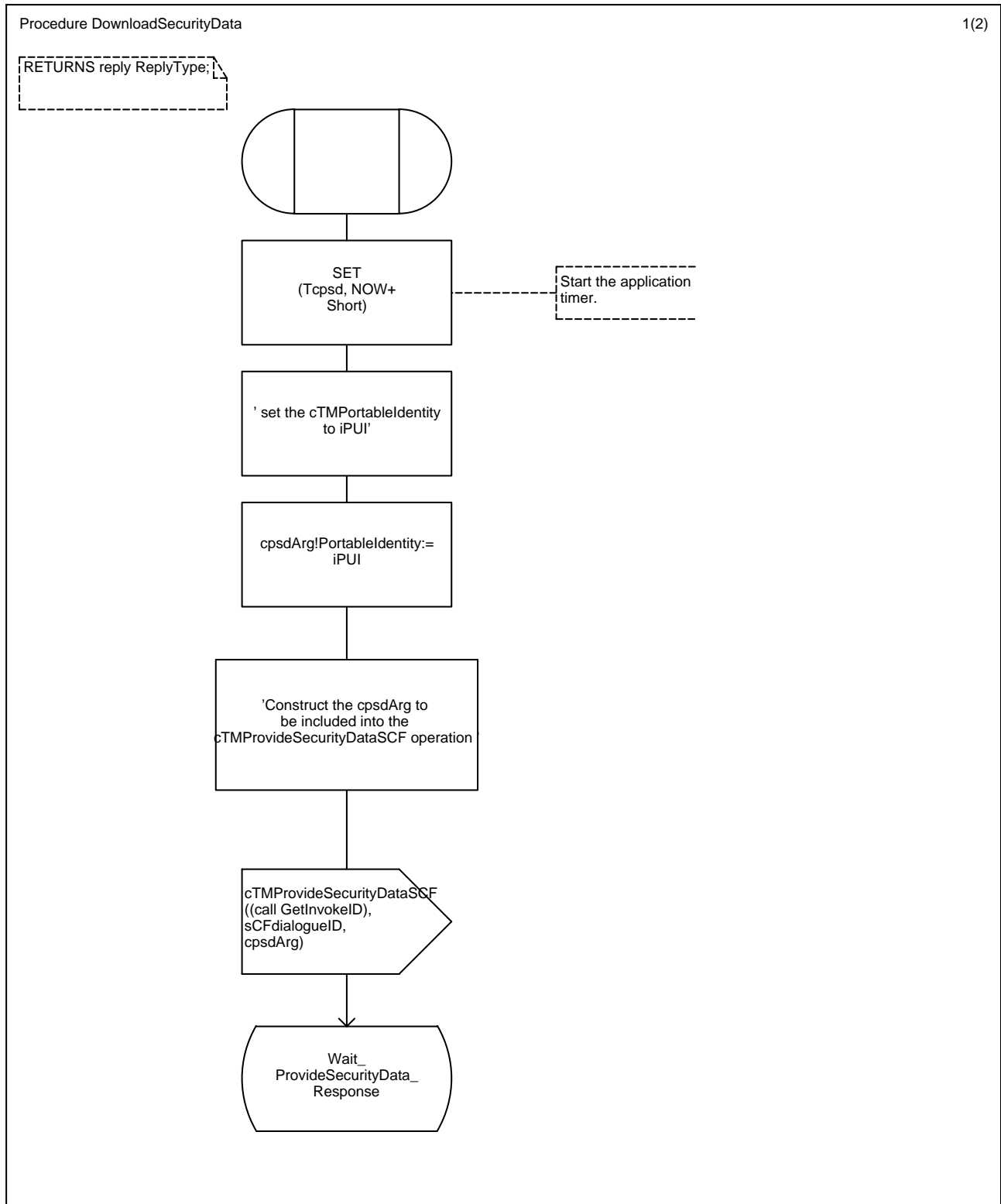


Figure C.21

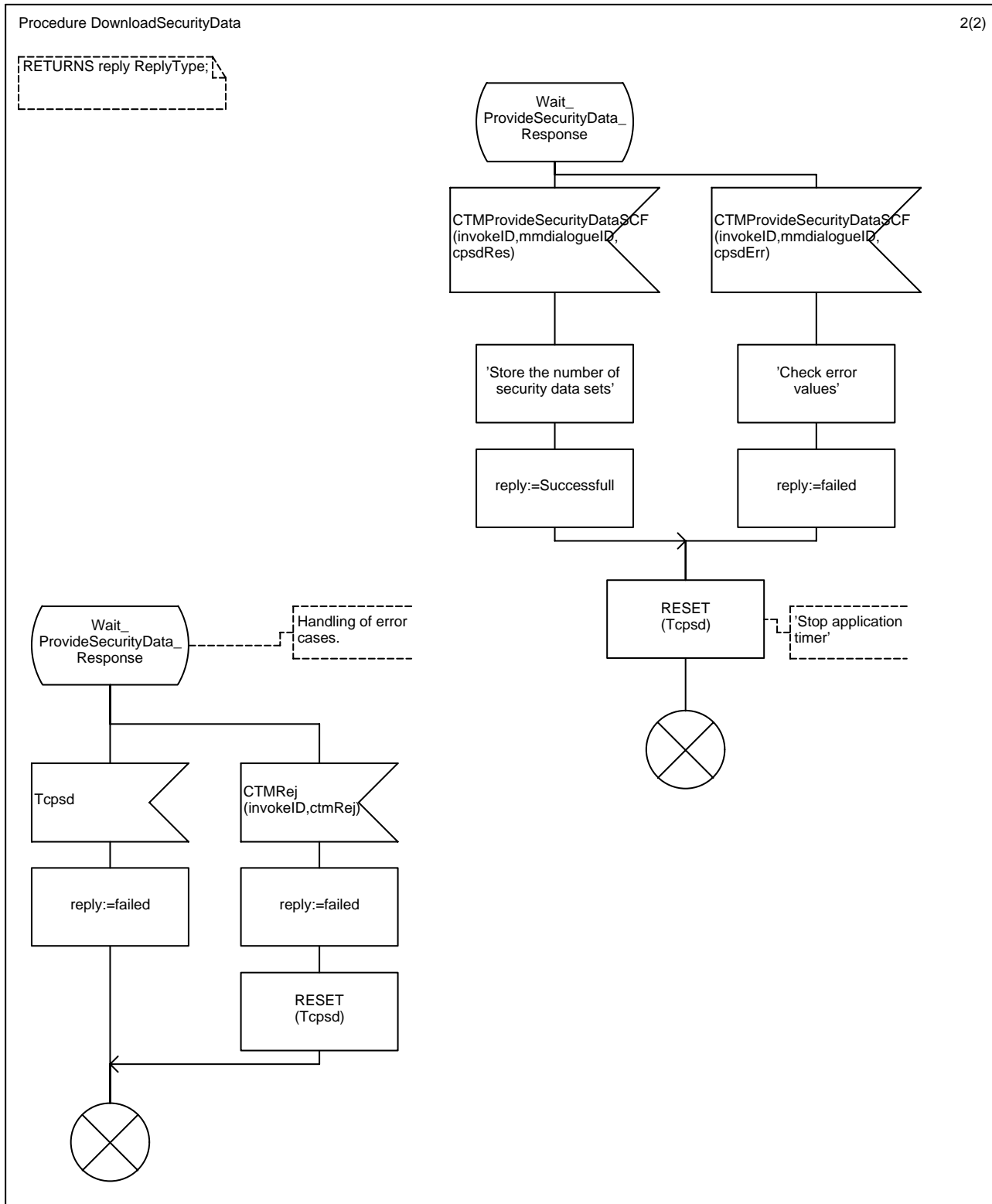


Figure C.22

C.10 Procedure TerminalAuthentication

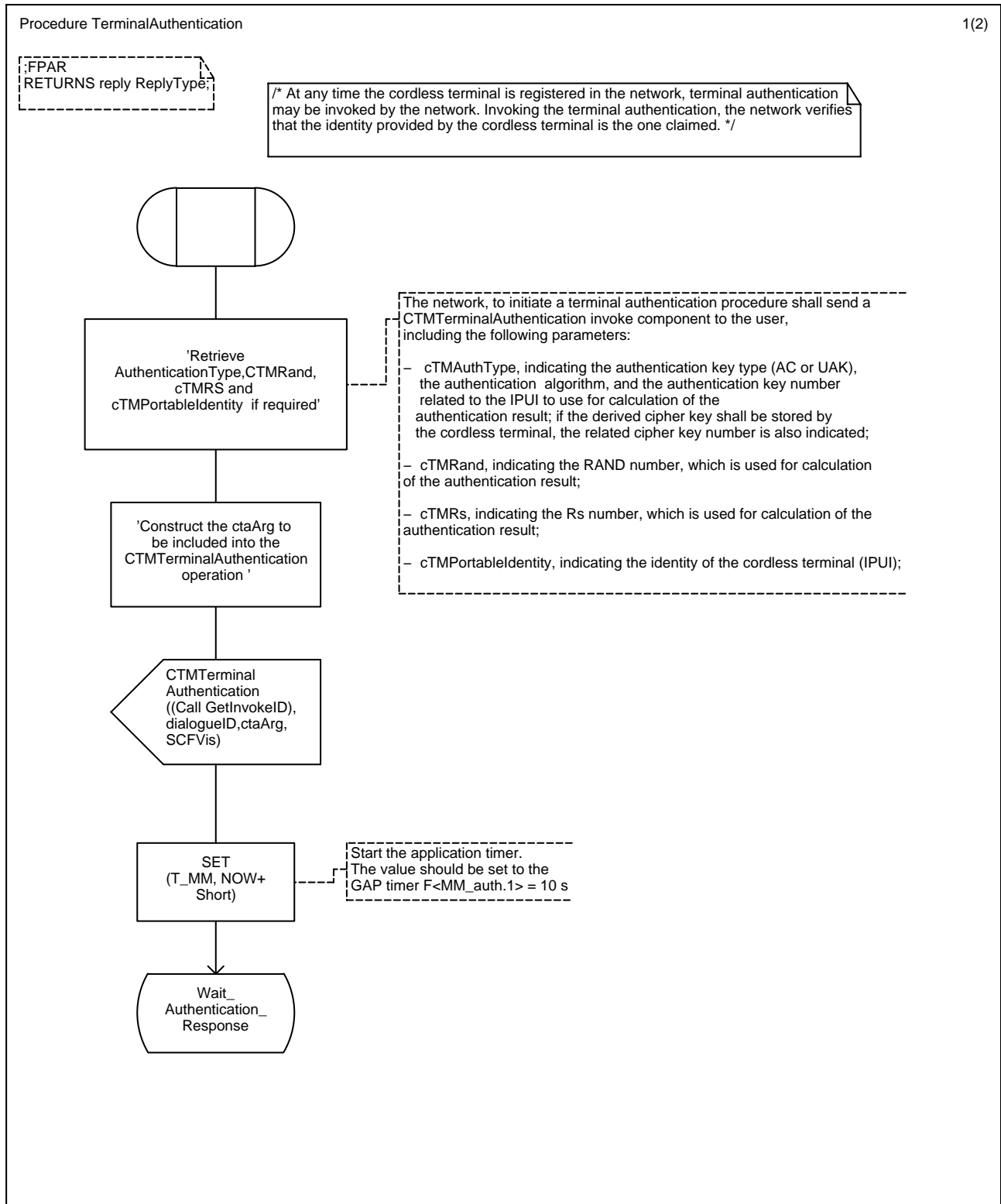


Figure C.23

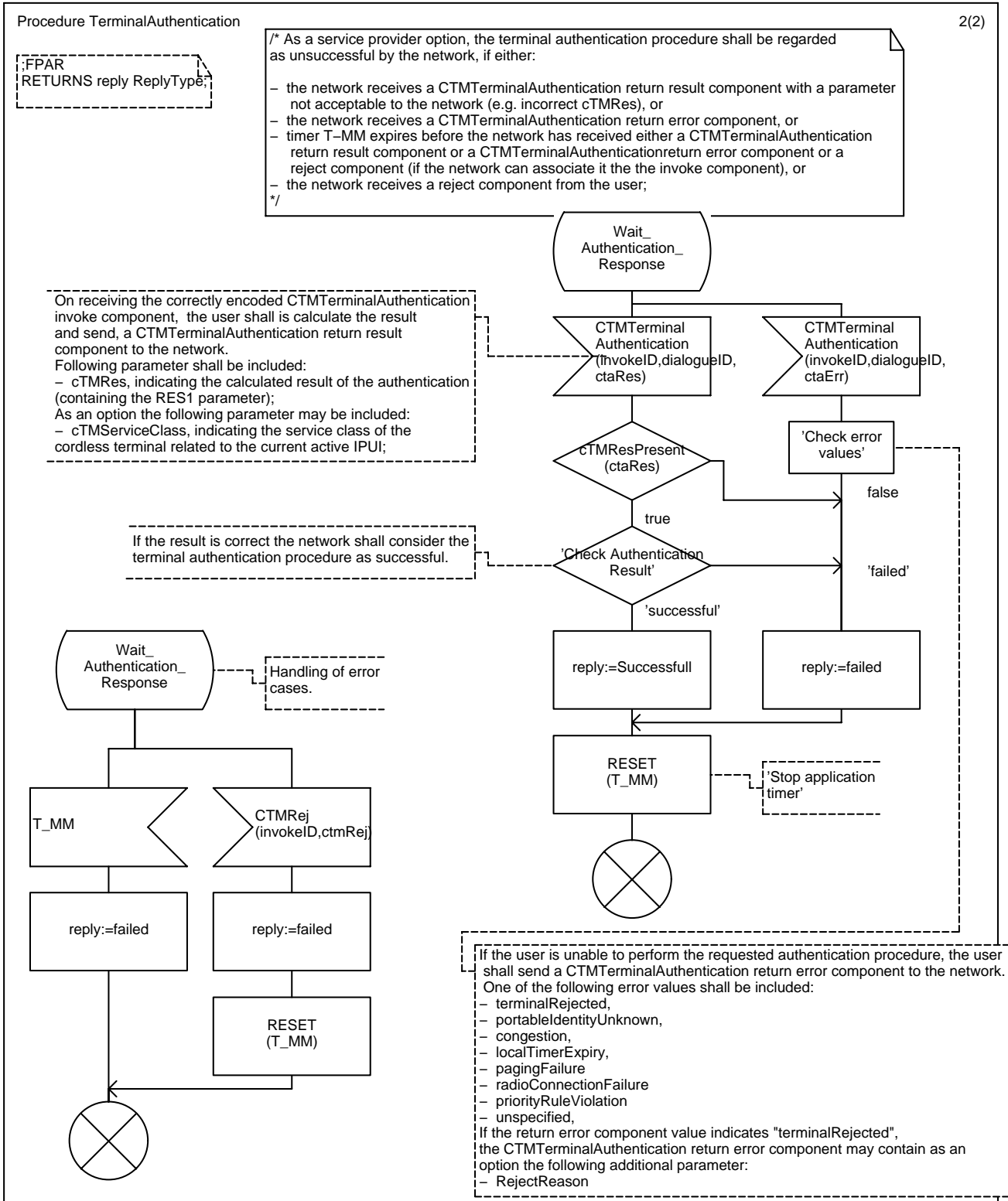


Figure C.24

C.11 Procedure Ciphering

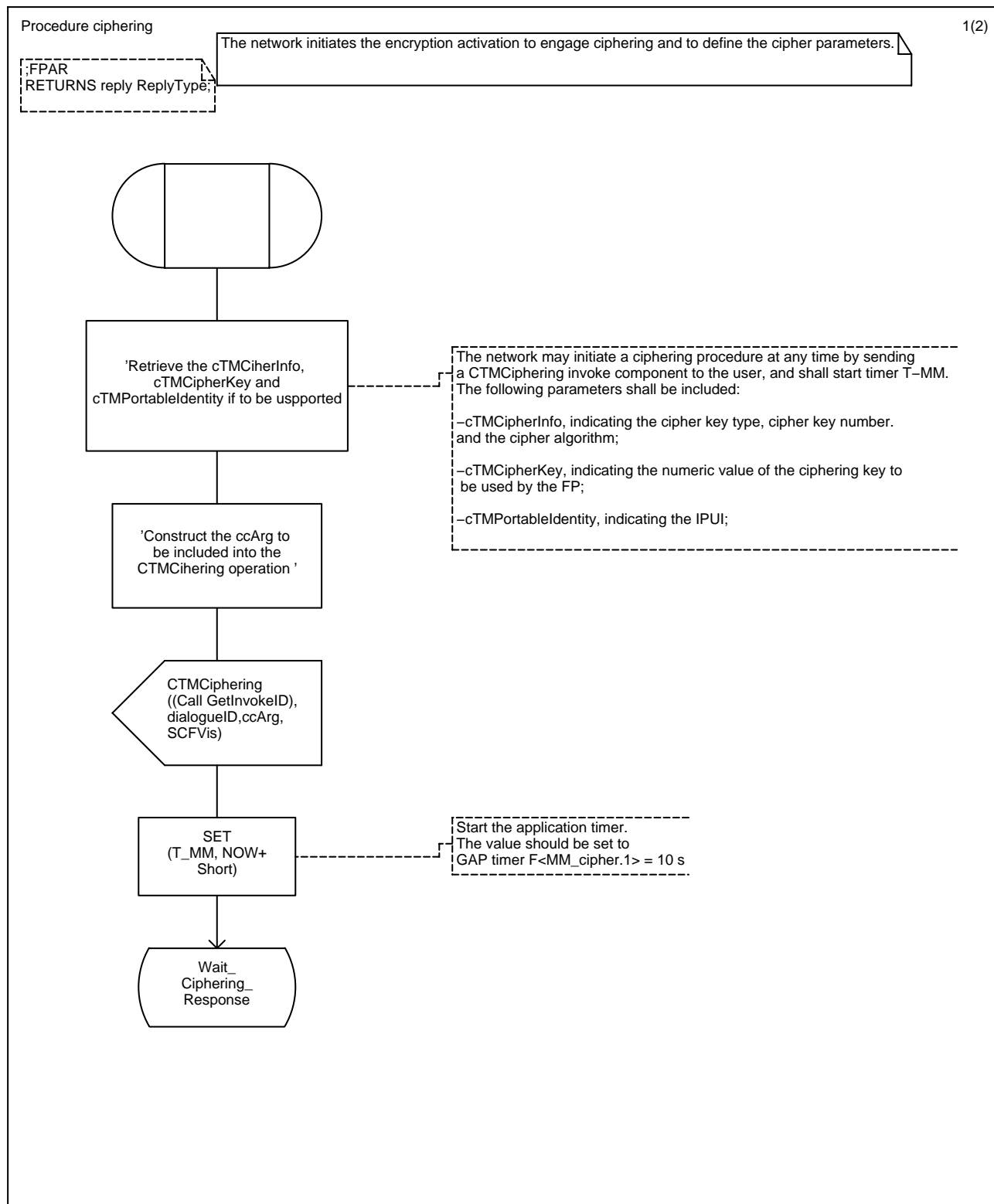


Figure C.25

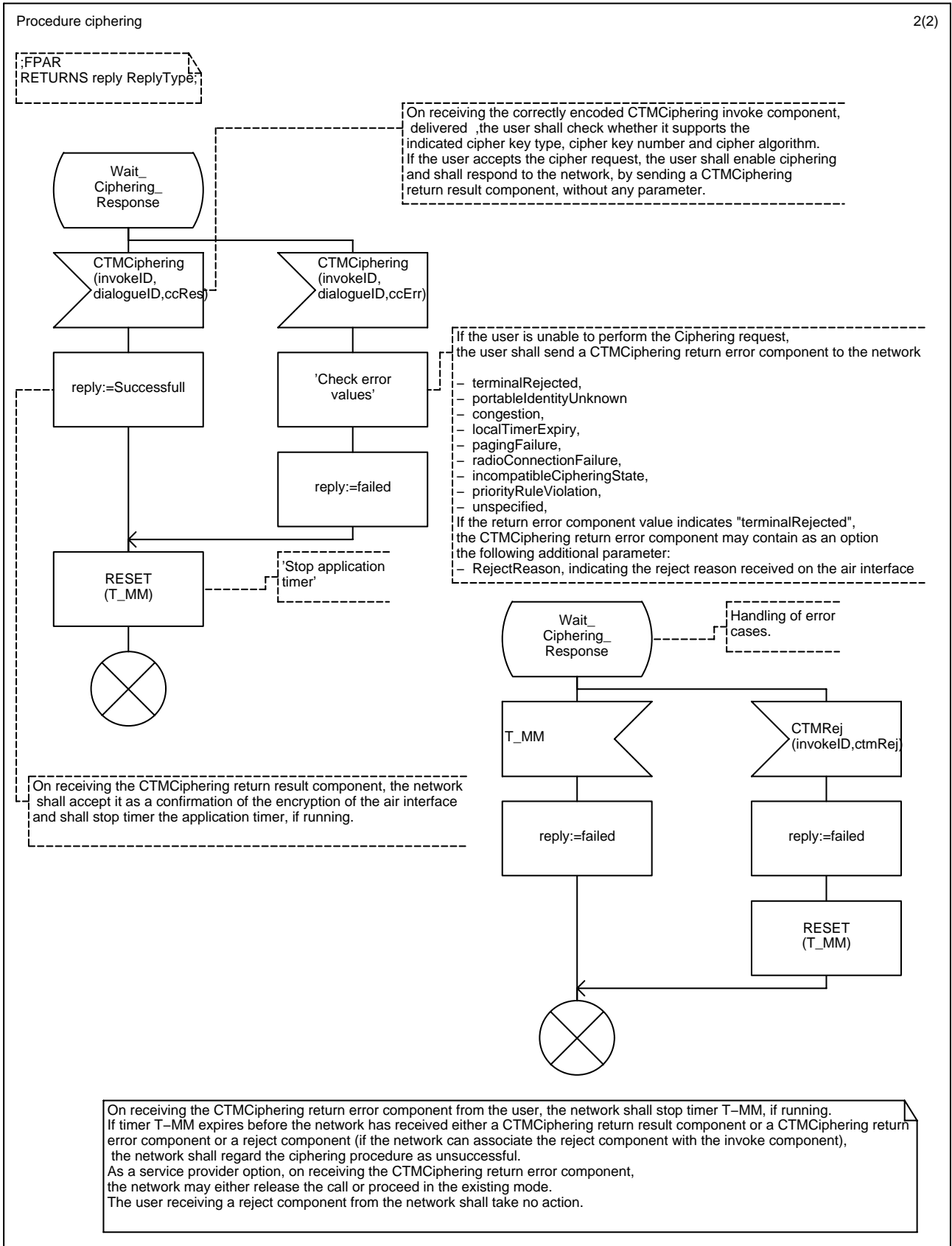


Figure C.26

C.12 Procedure IdentityRequest

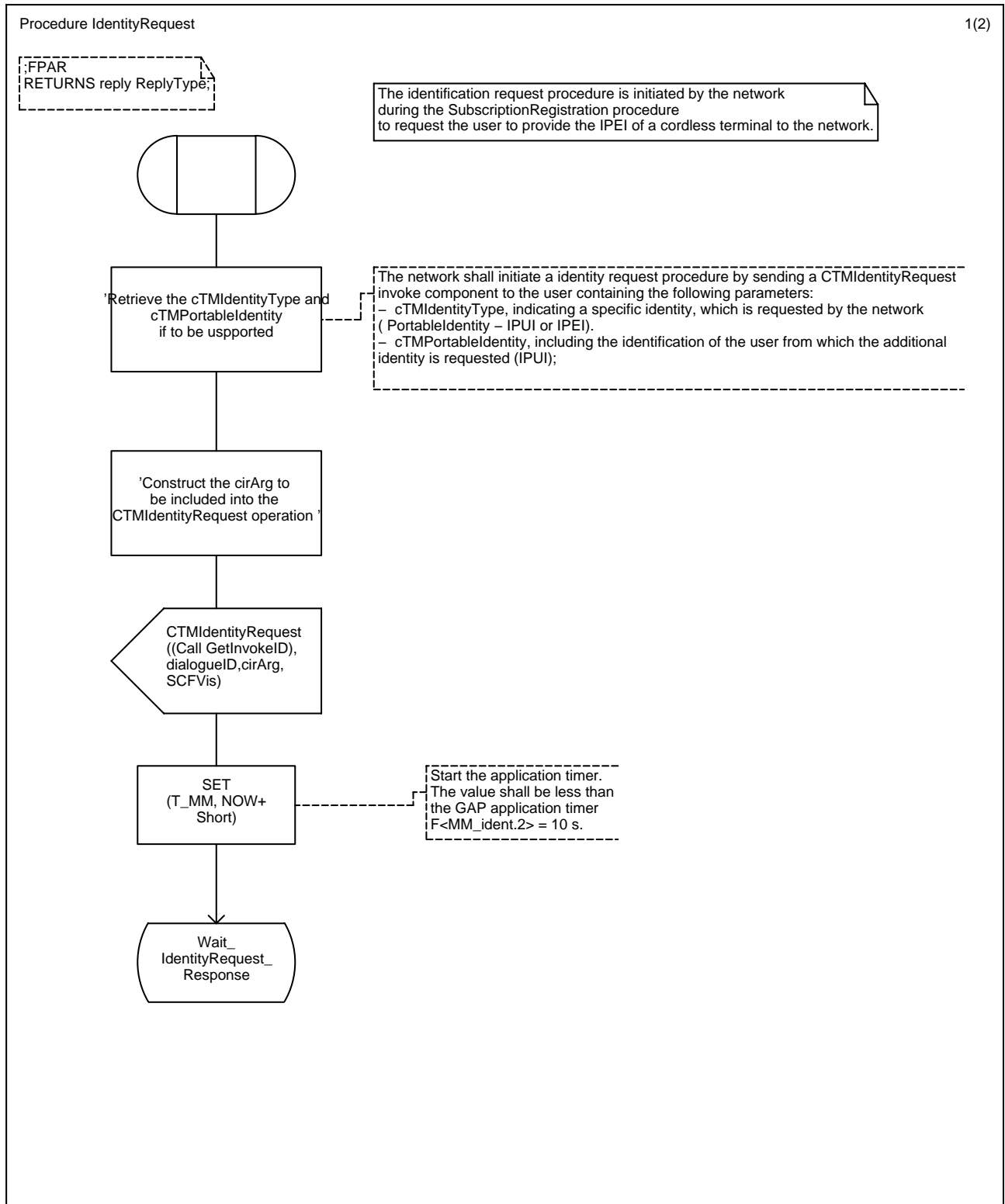


Figure C.27

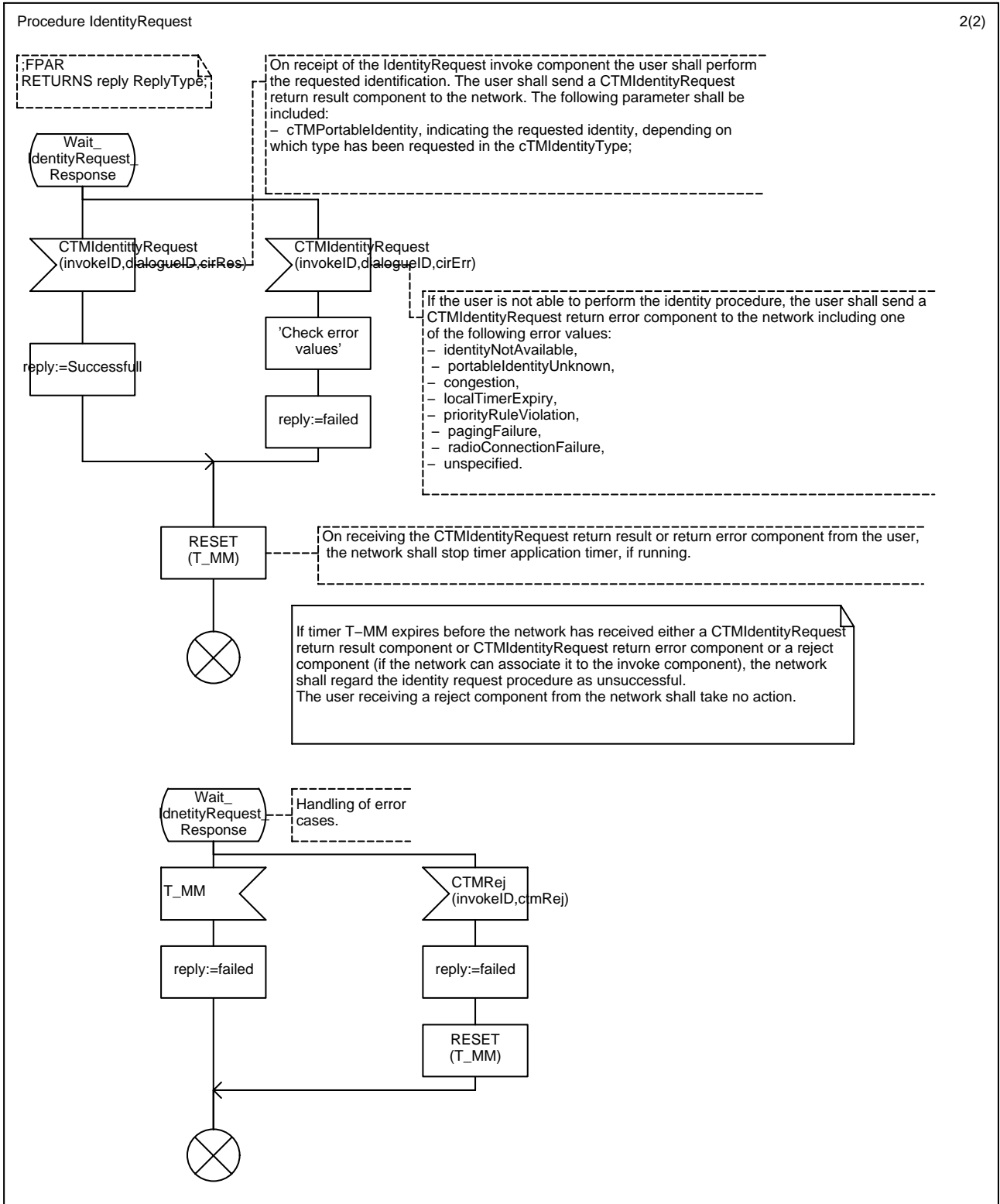


Figure C.28

C.13 Procedure SubscriptionRegistration

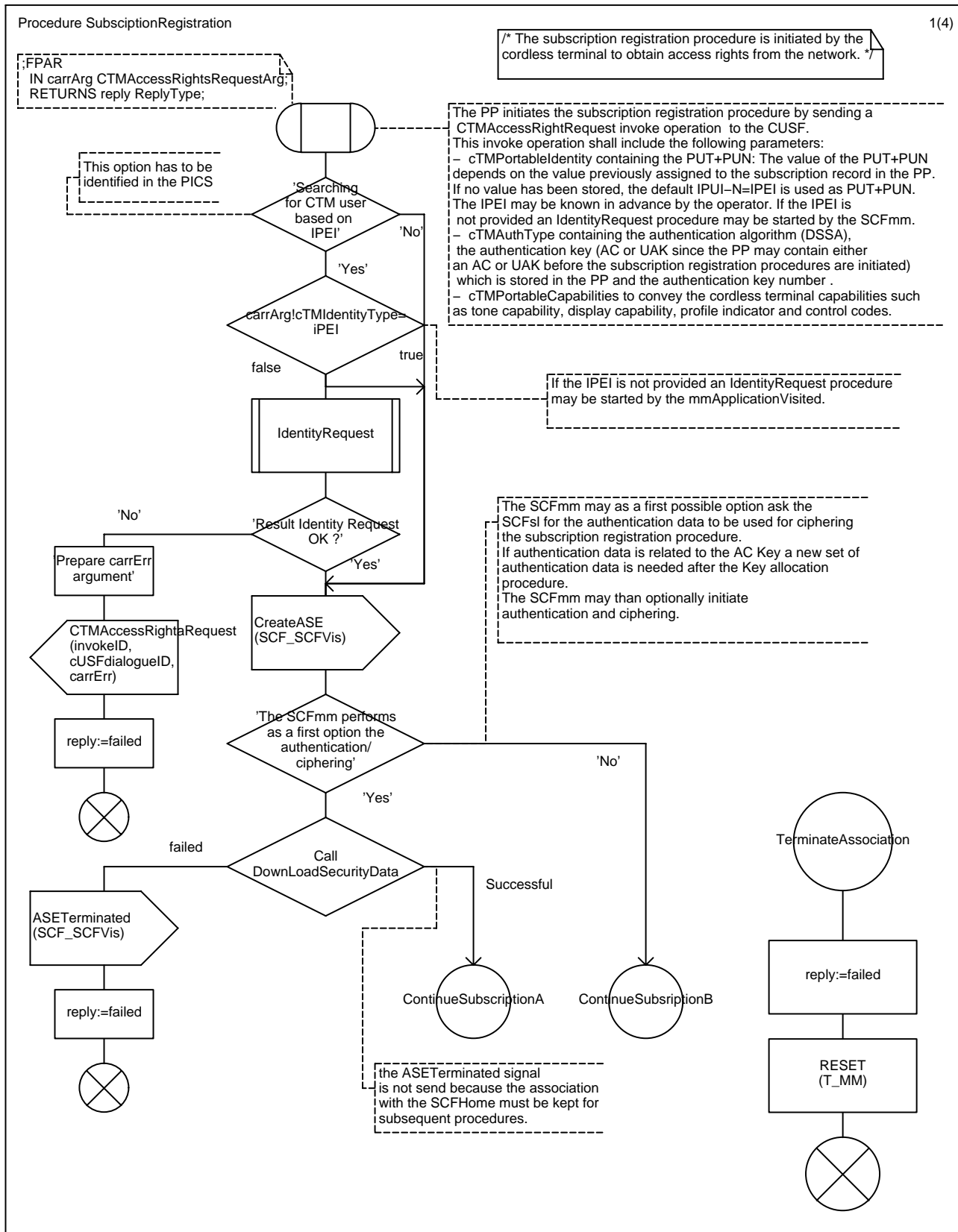


Figure C.29

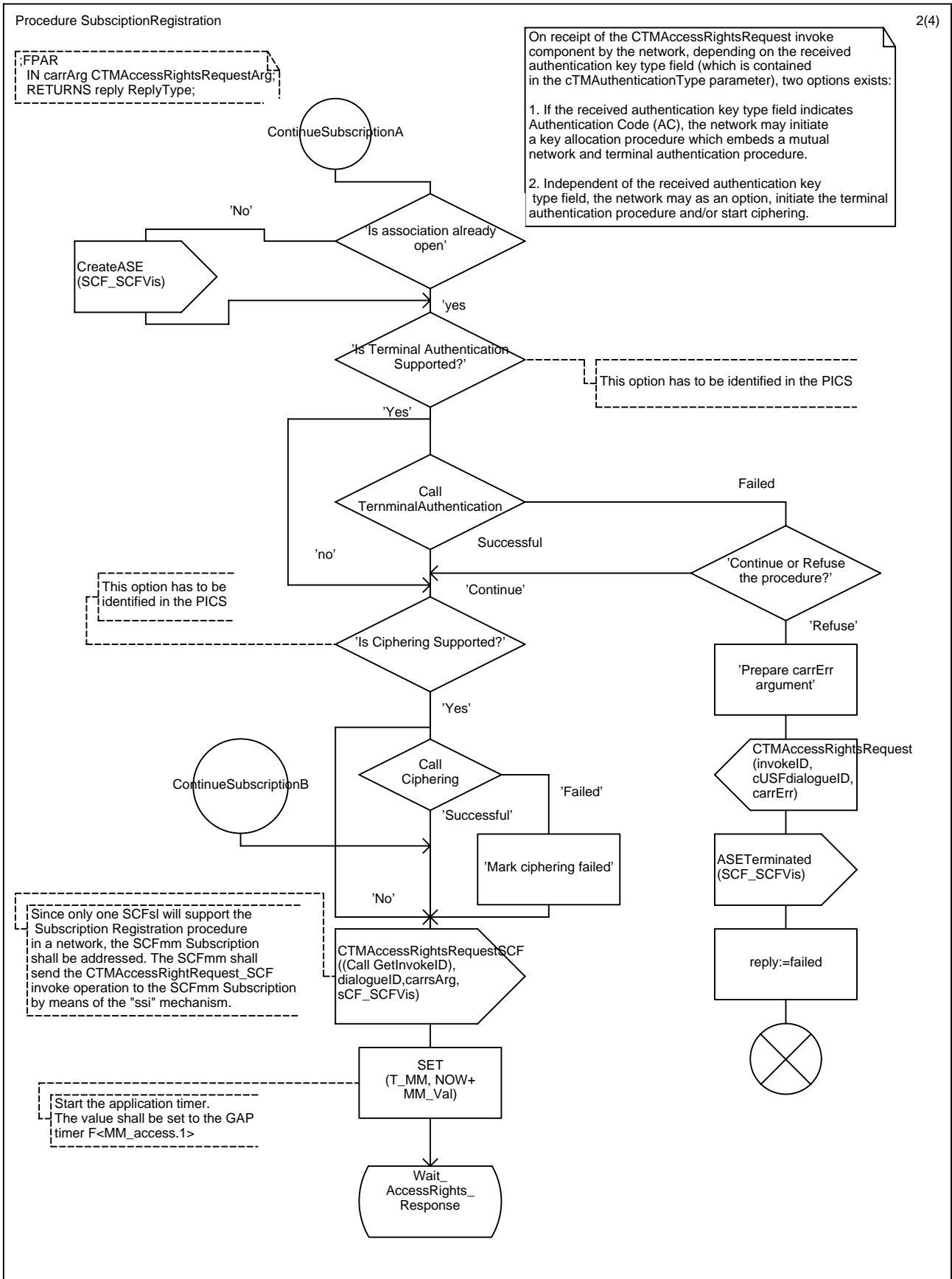


Figure C.30

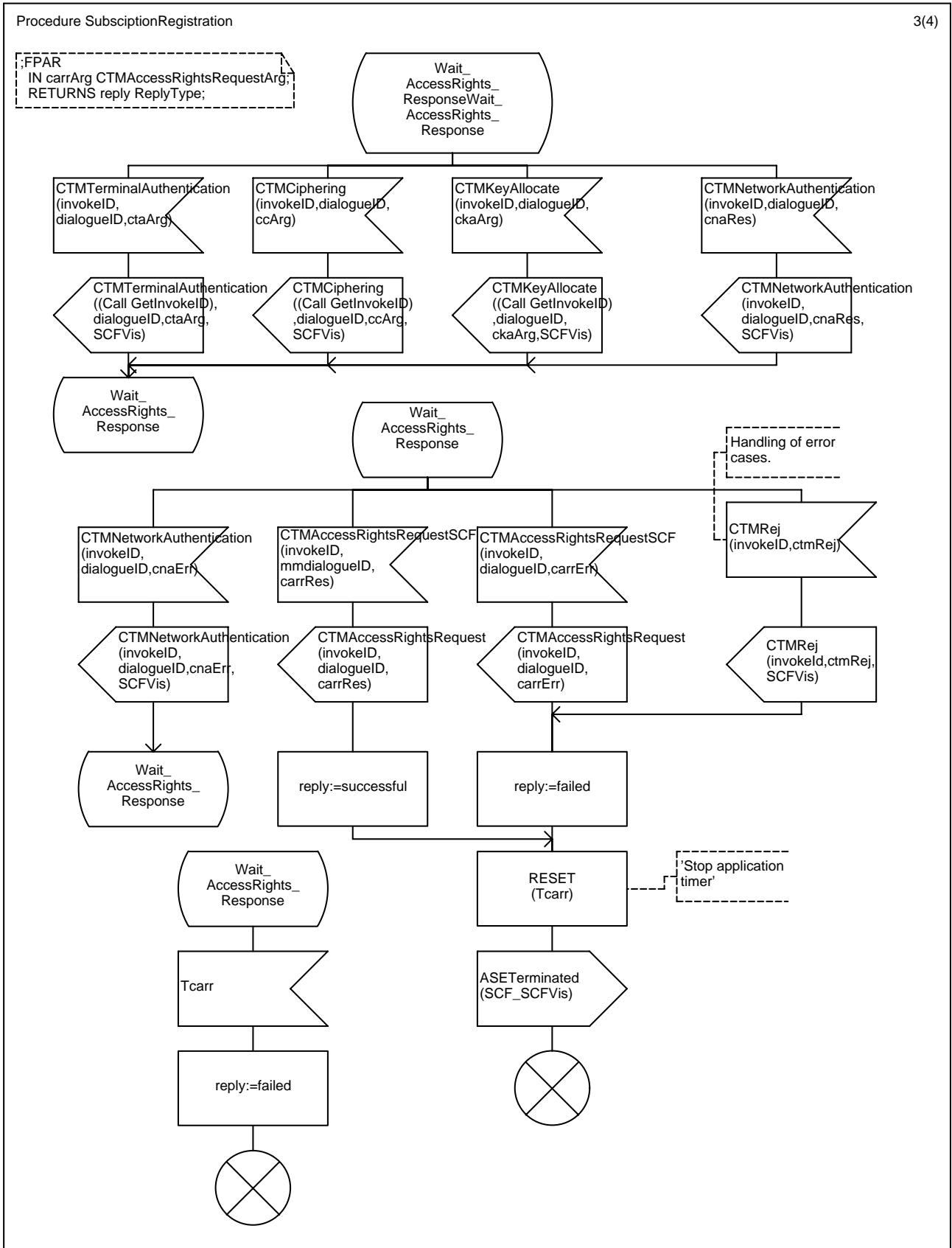


Figure C.31

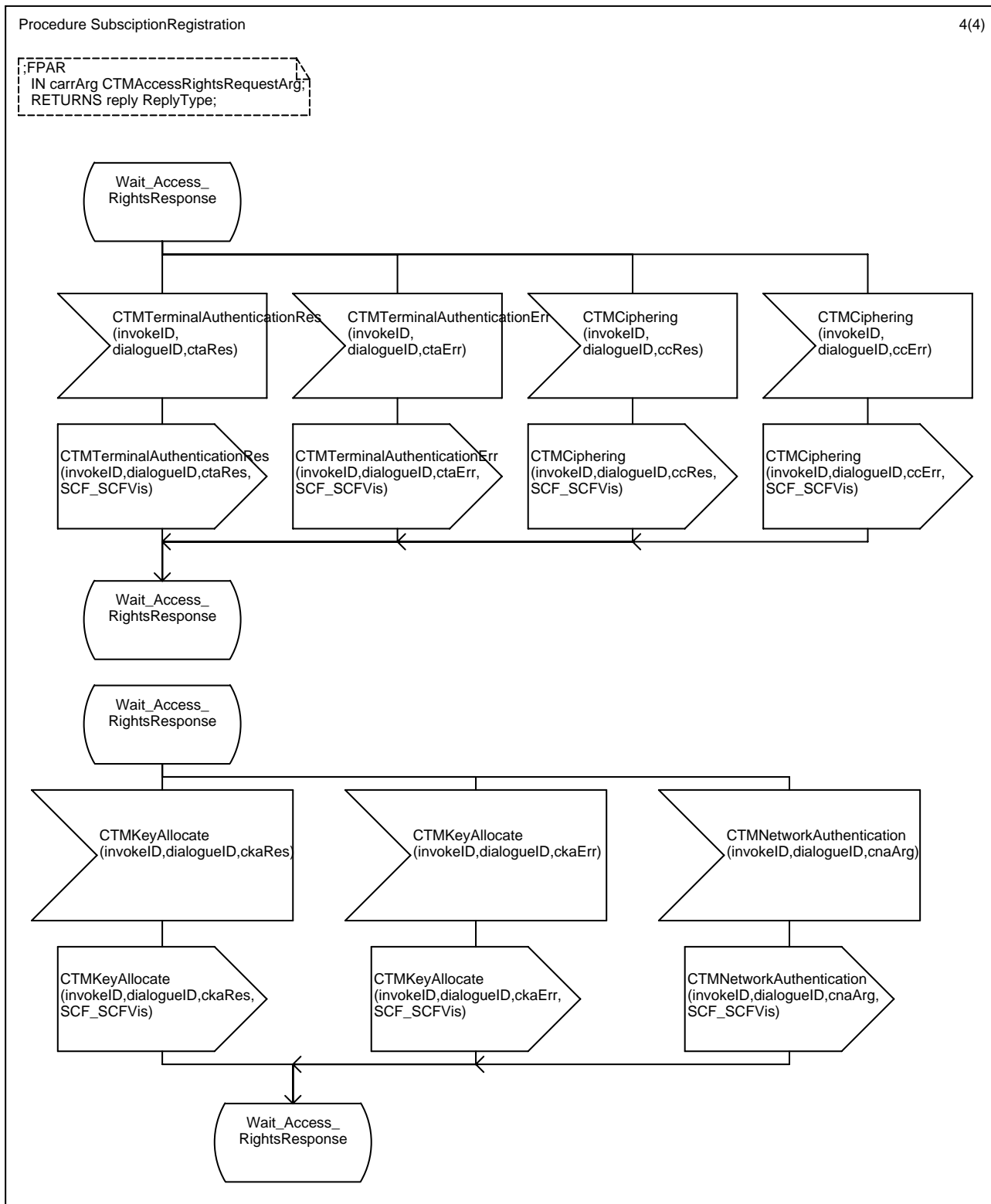


Figure C.32

C.14 Procedure LocationRegistration

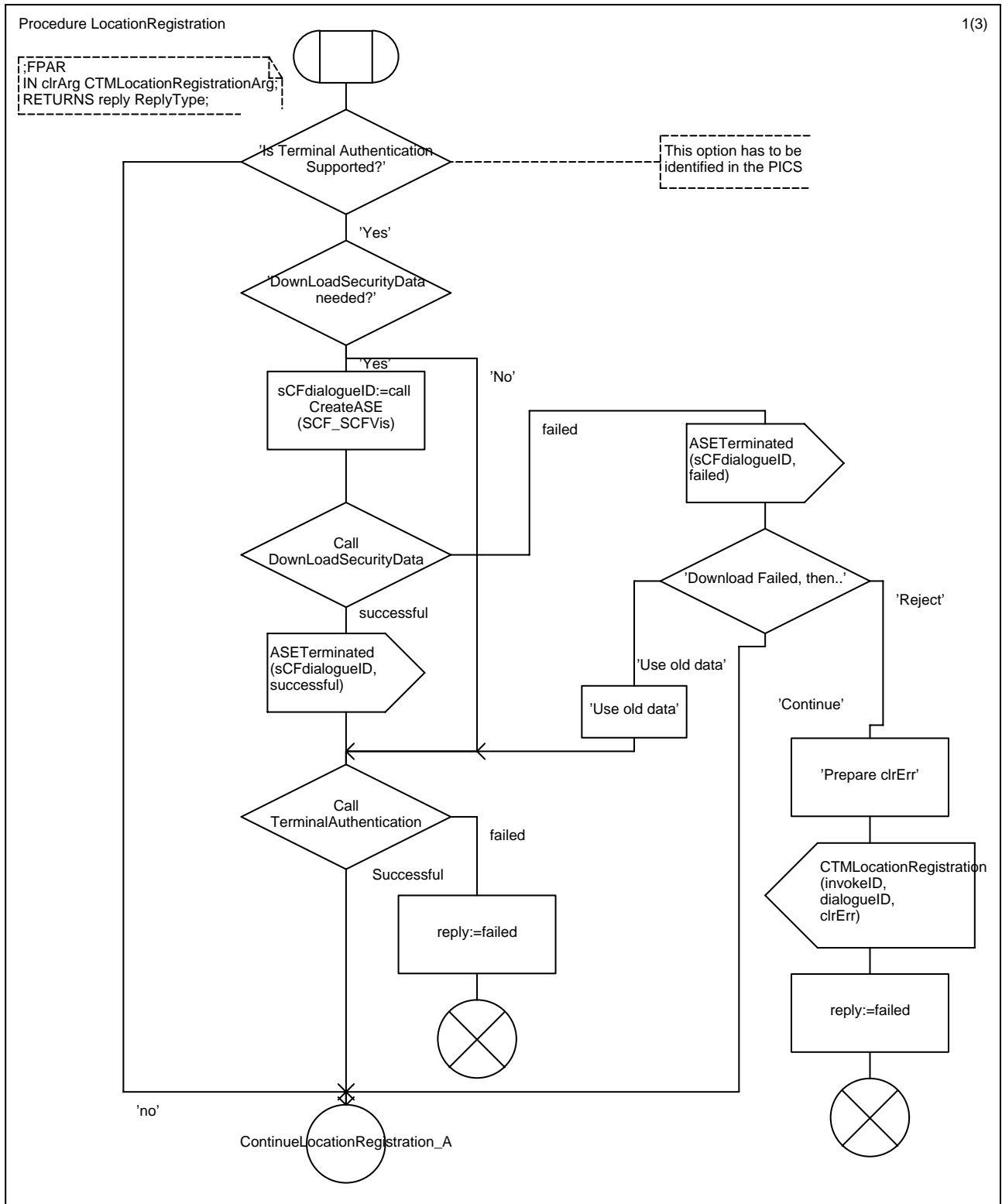


Figure C.33

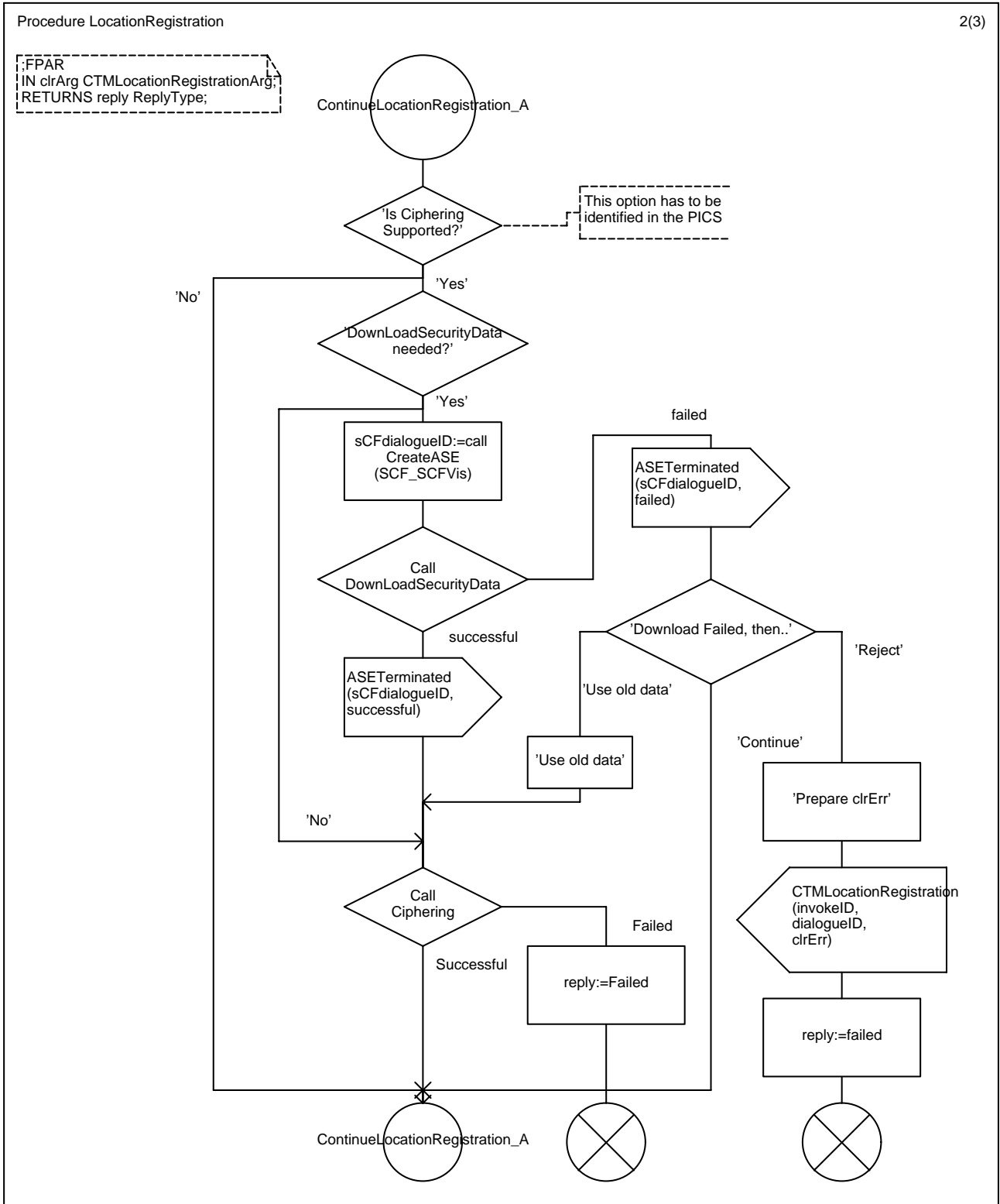


Figure C.34

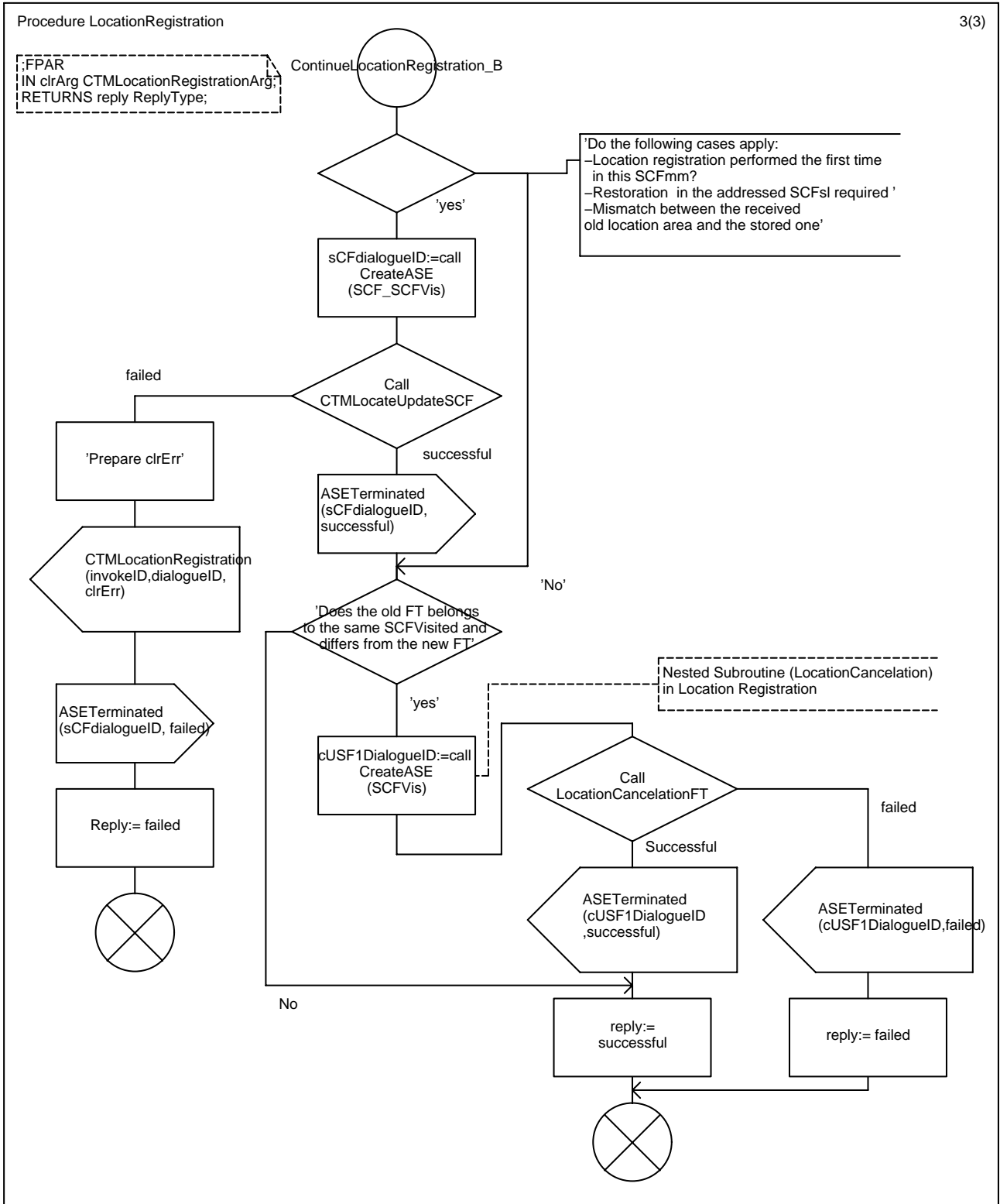


Figure C.35

C.15 Procedure LocationRegistrationSuggest

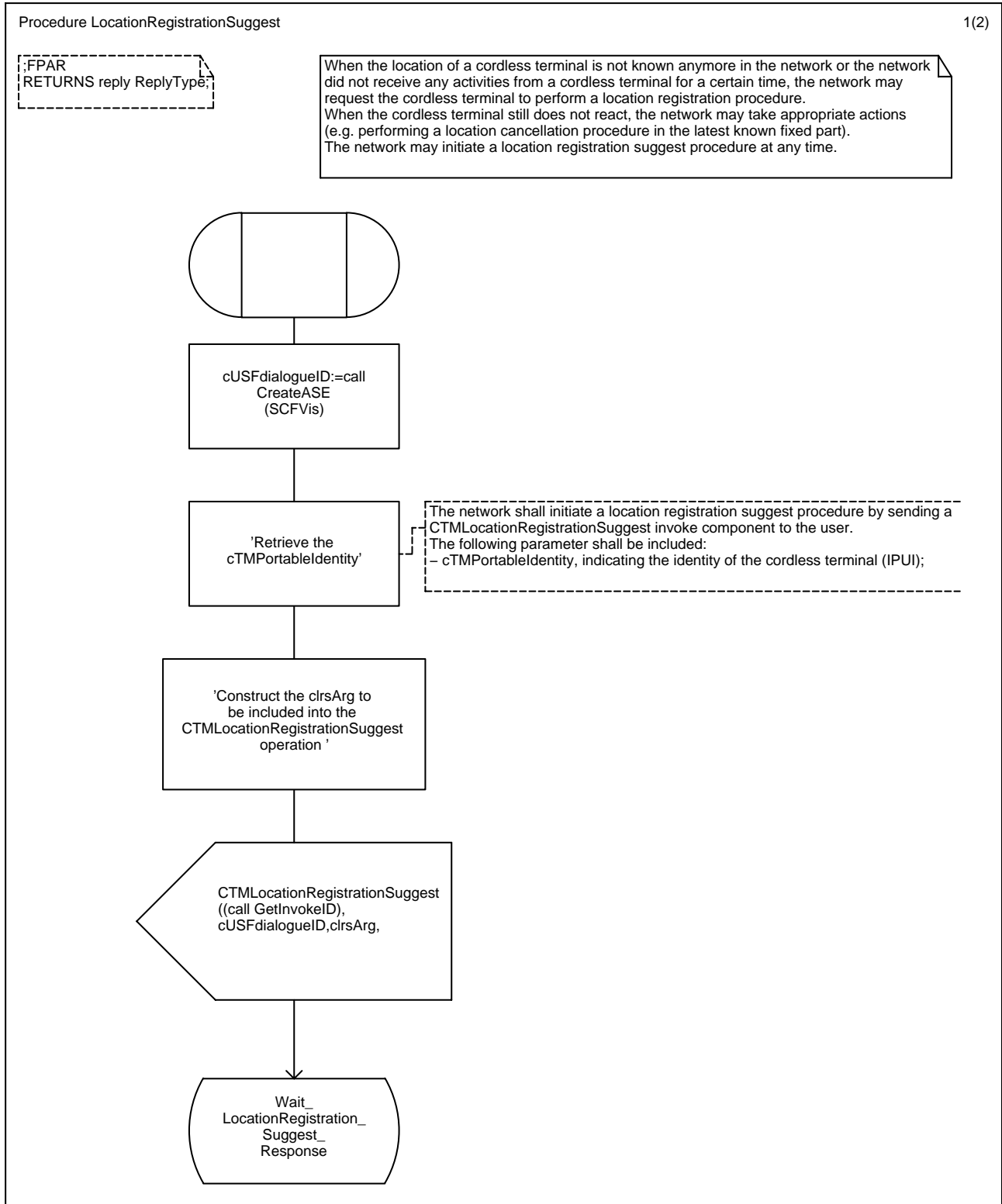


Figure C.36

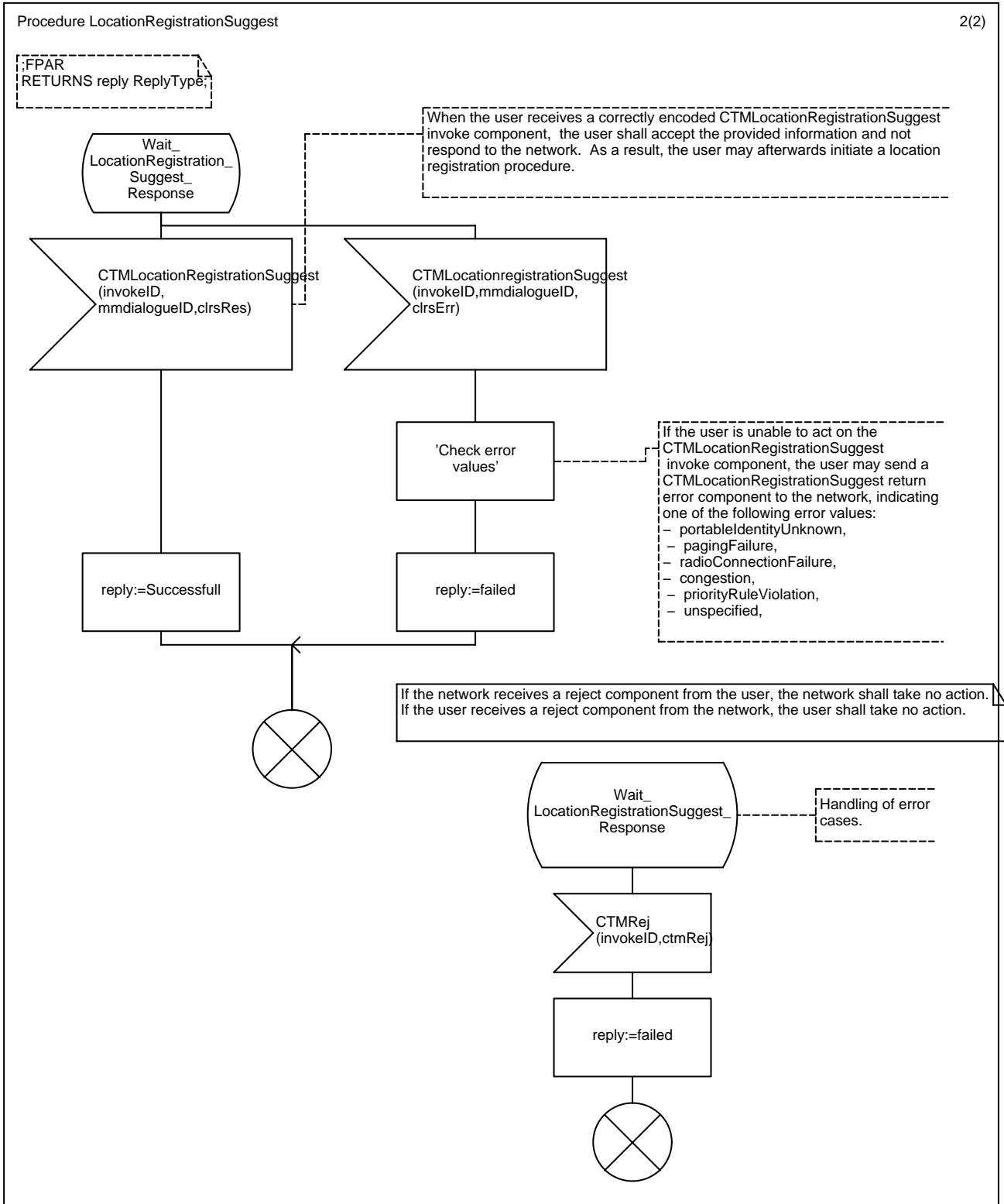


Figure C.37

C.16 Process Type SCFsIVisitedApplication

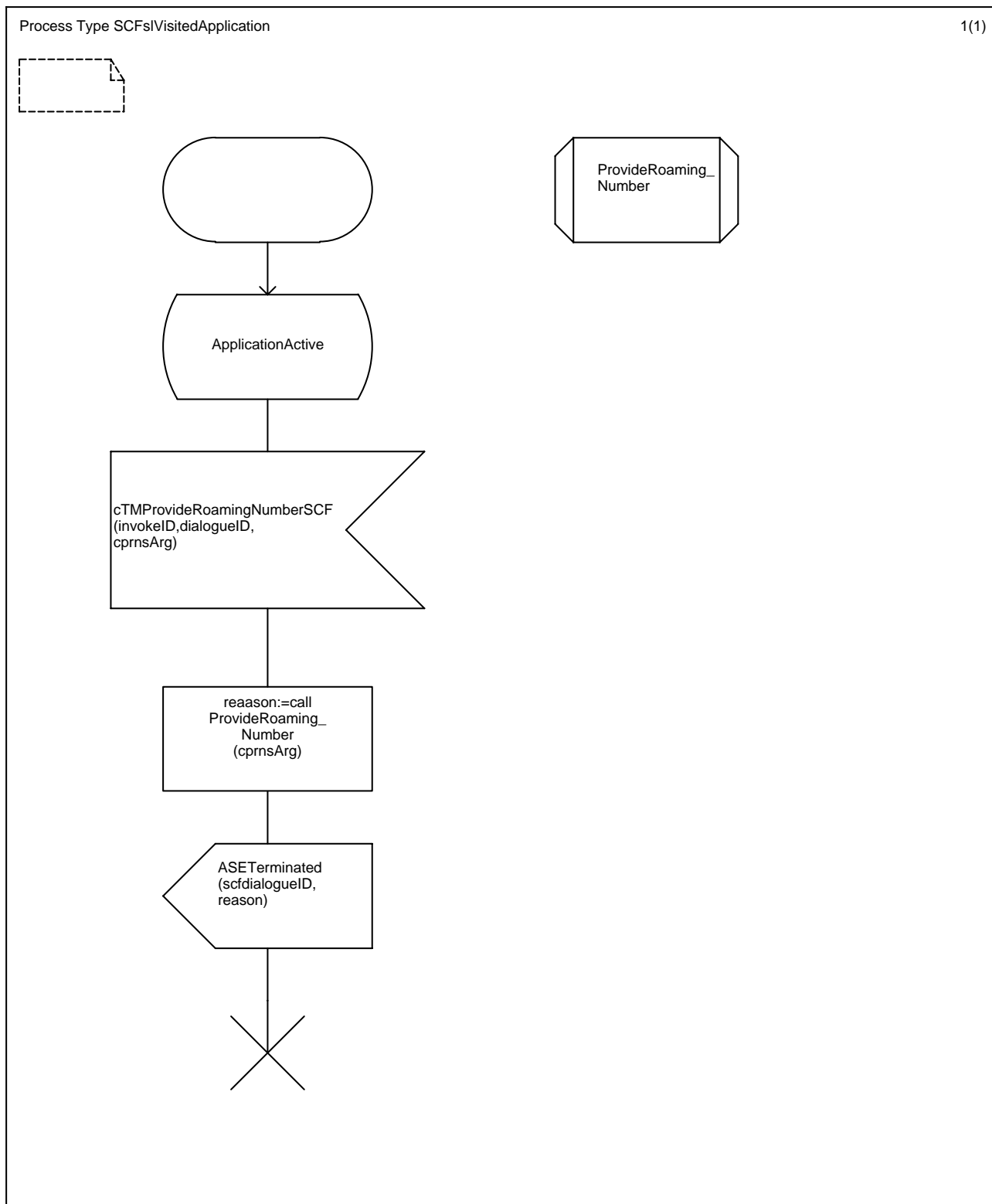


Figure C.38

C.17 Procedure ProvideRoamingNumber

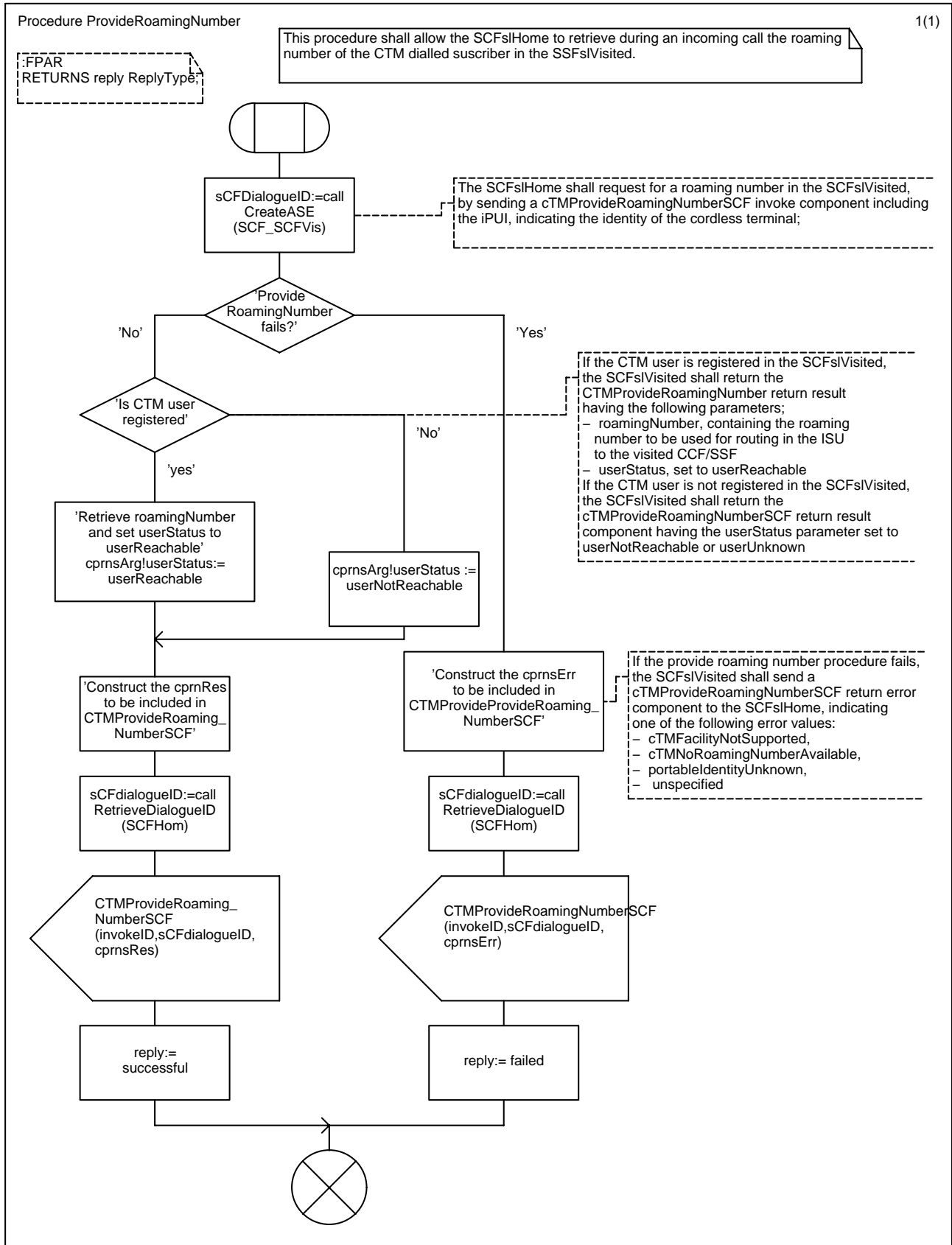


Figure C.39

C.18 Process Type SCF_SCF_ASE_Visited

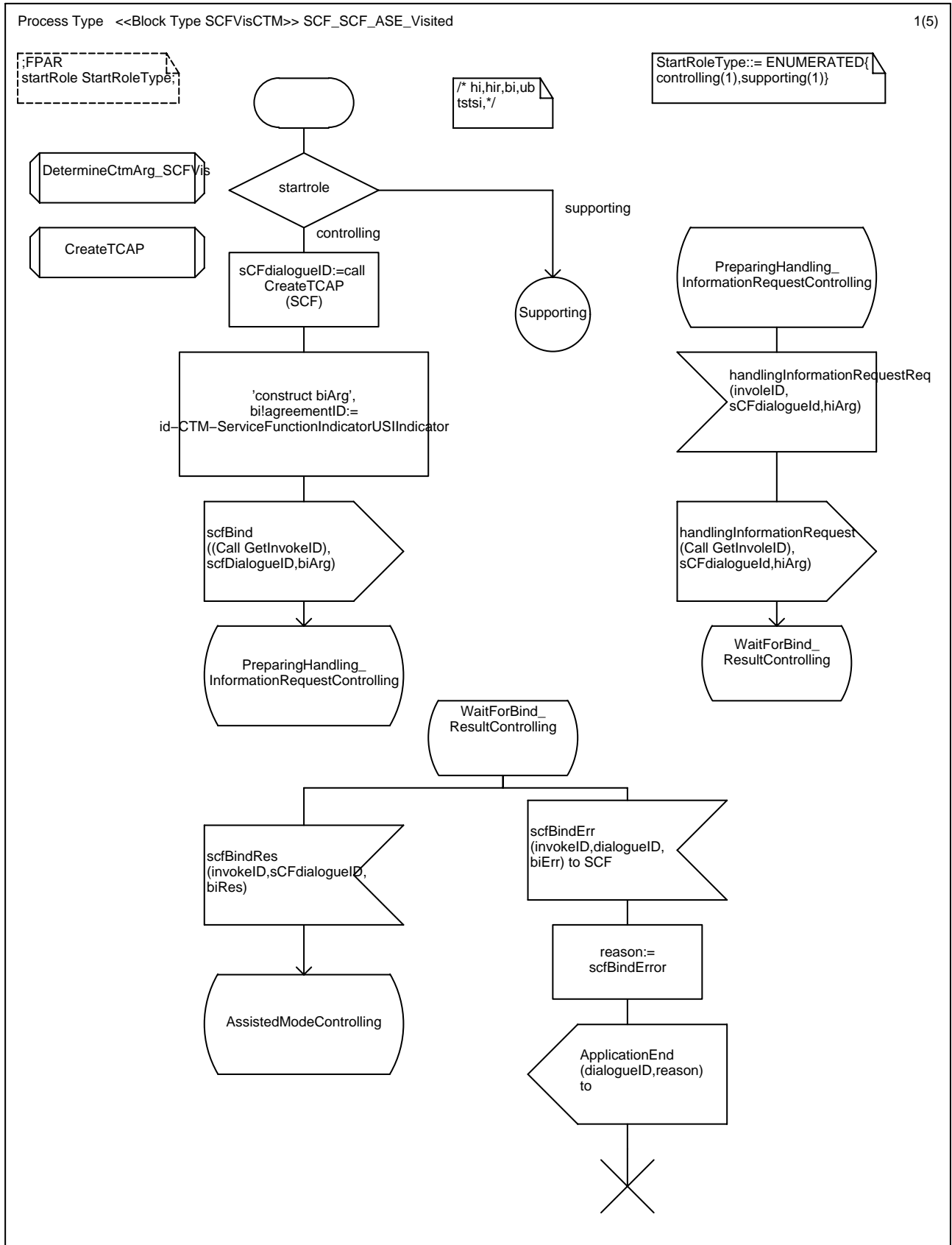


Figure C.40

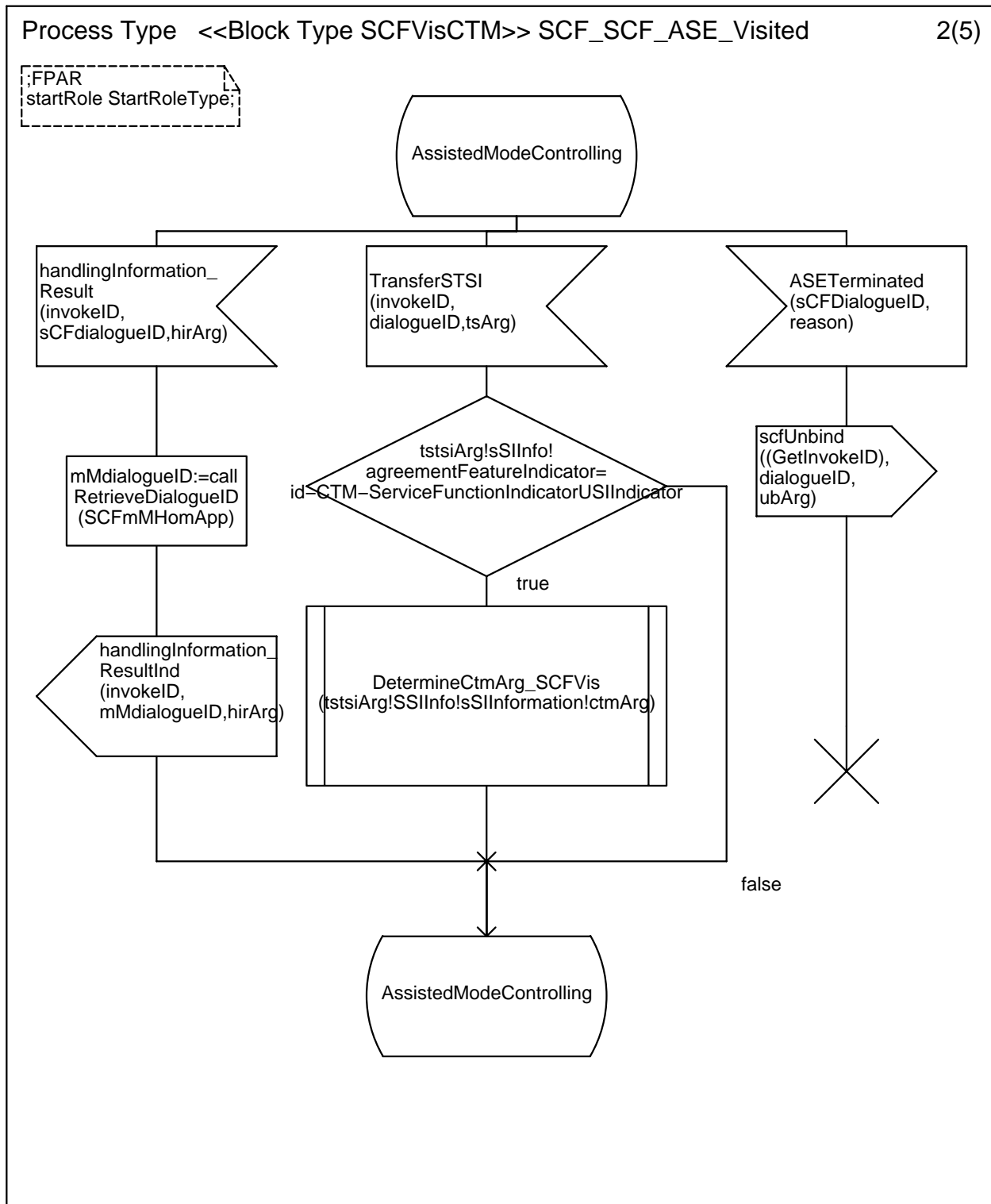


Figure C.41

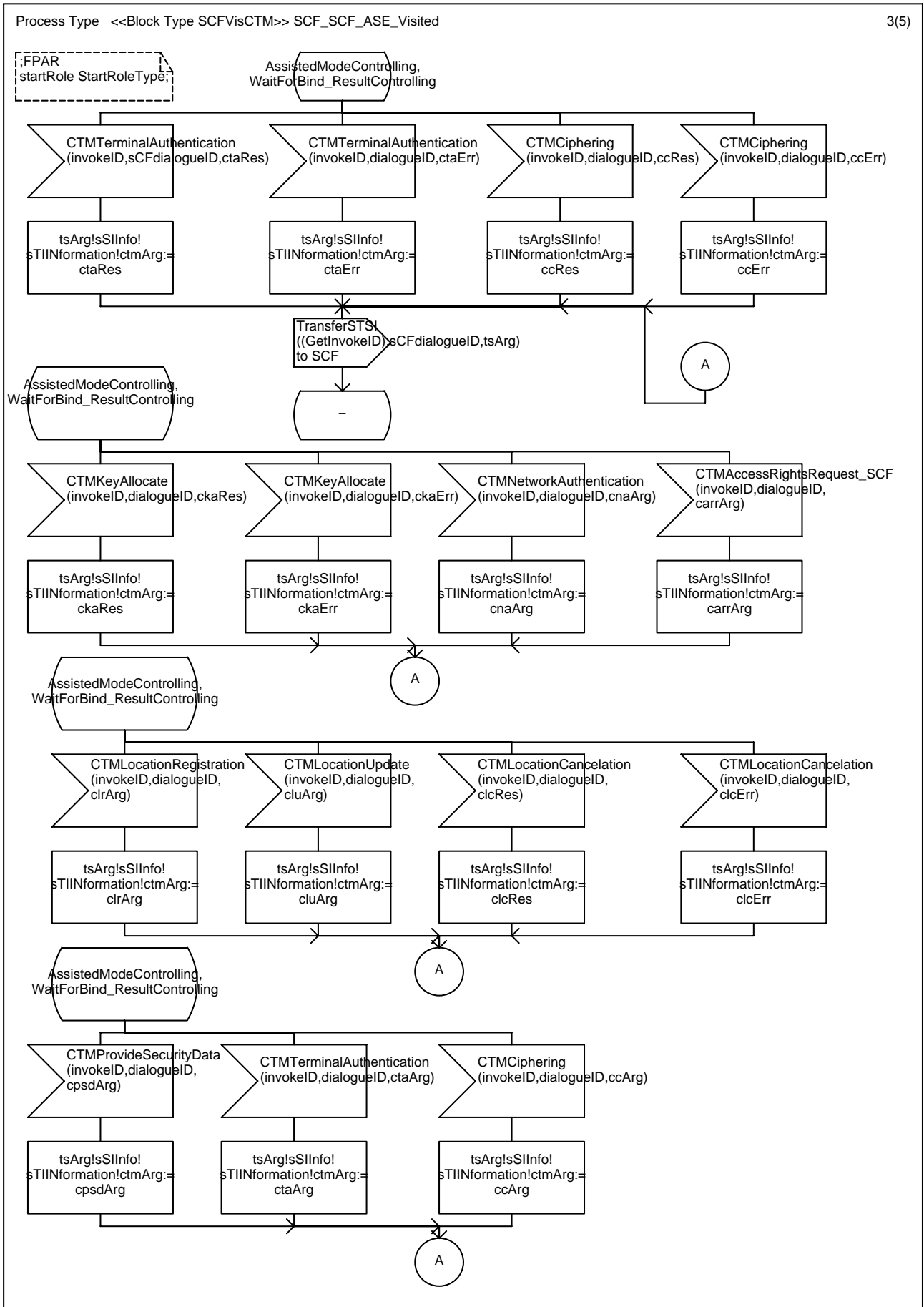


Figure C.42

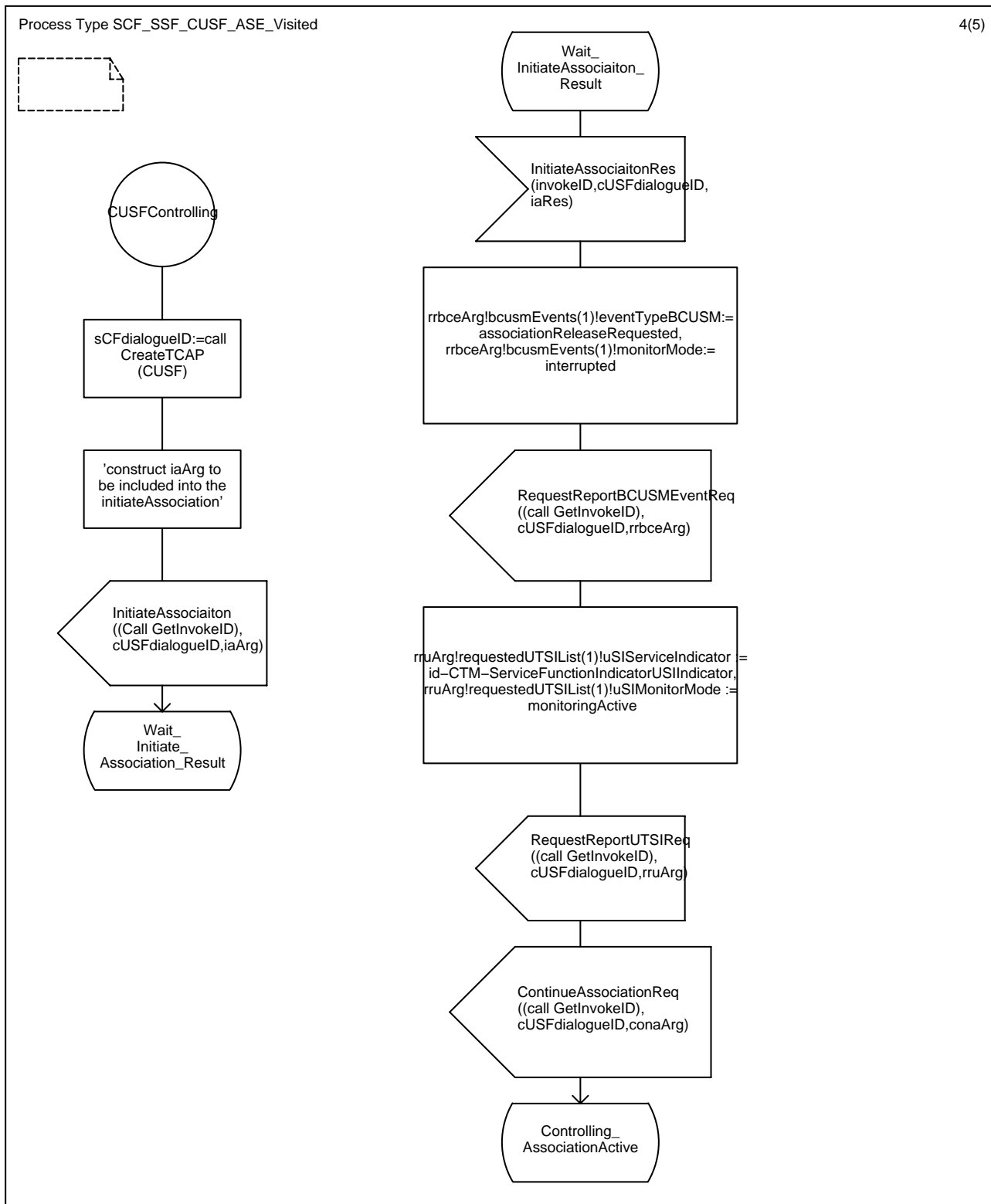


Figure C.43

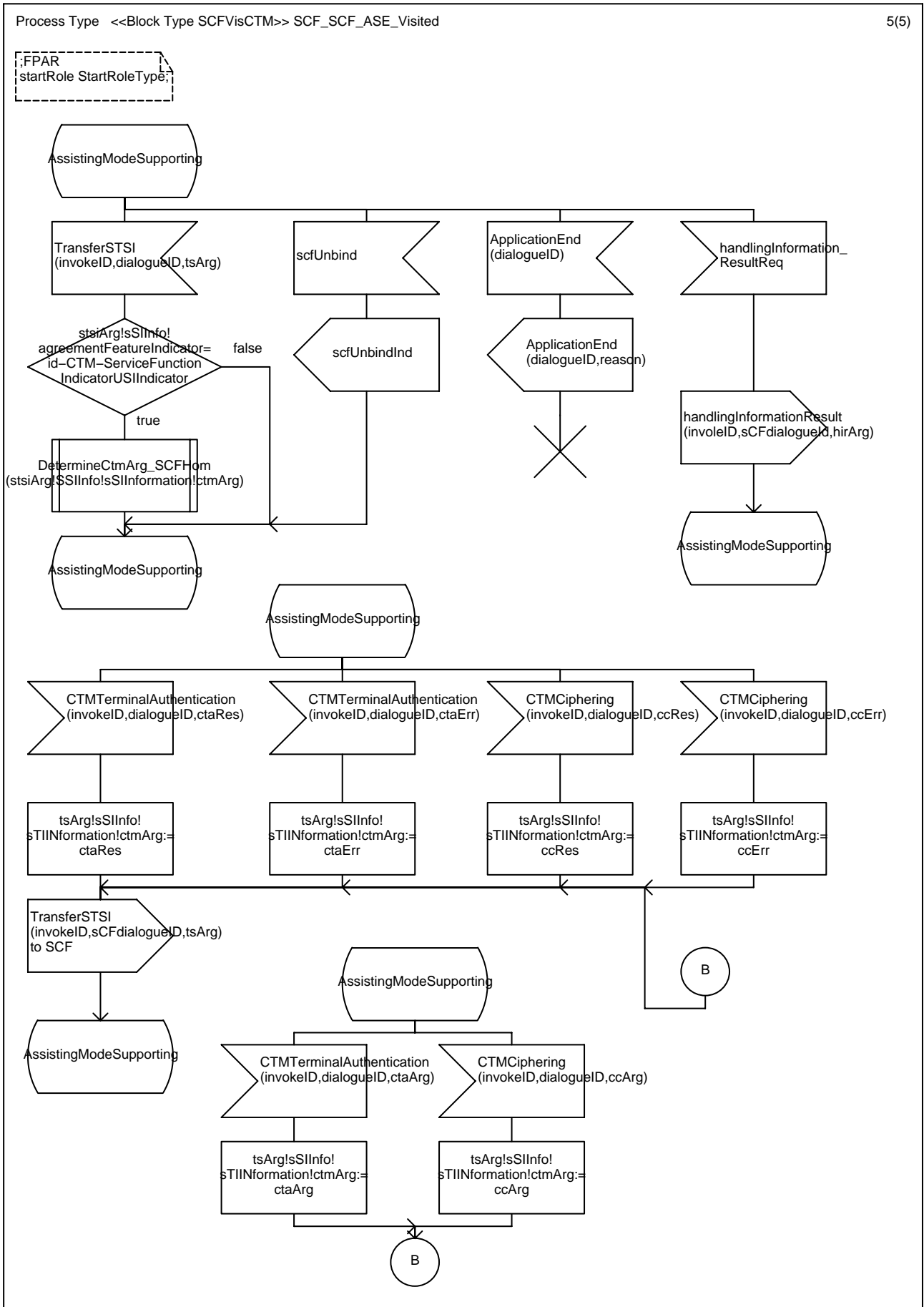


Figure C.44

C.19 Procedure DetermineCtmArg_SCFVis

Procedure DetermineCtmArg_SCFVis

1(1)

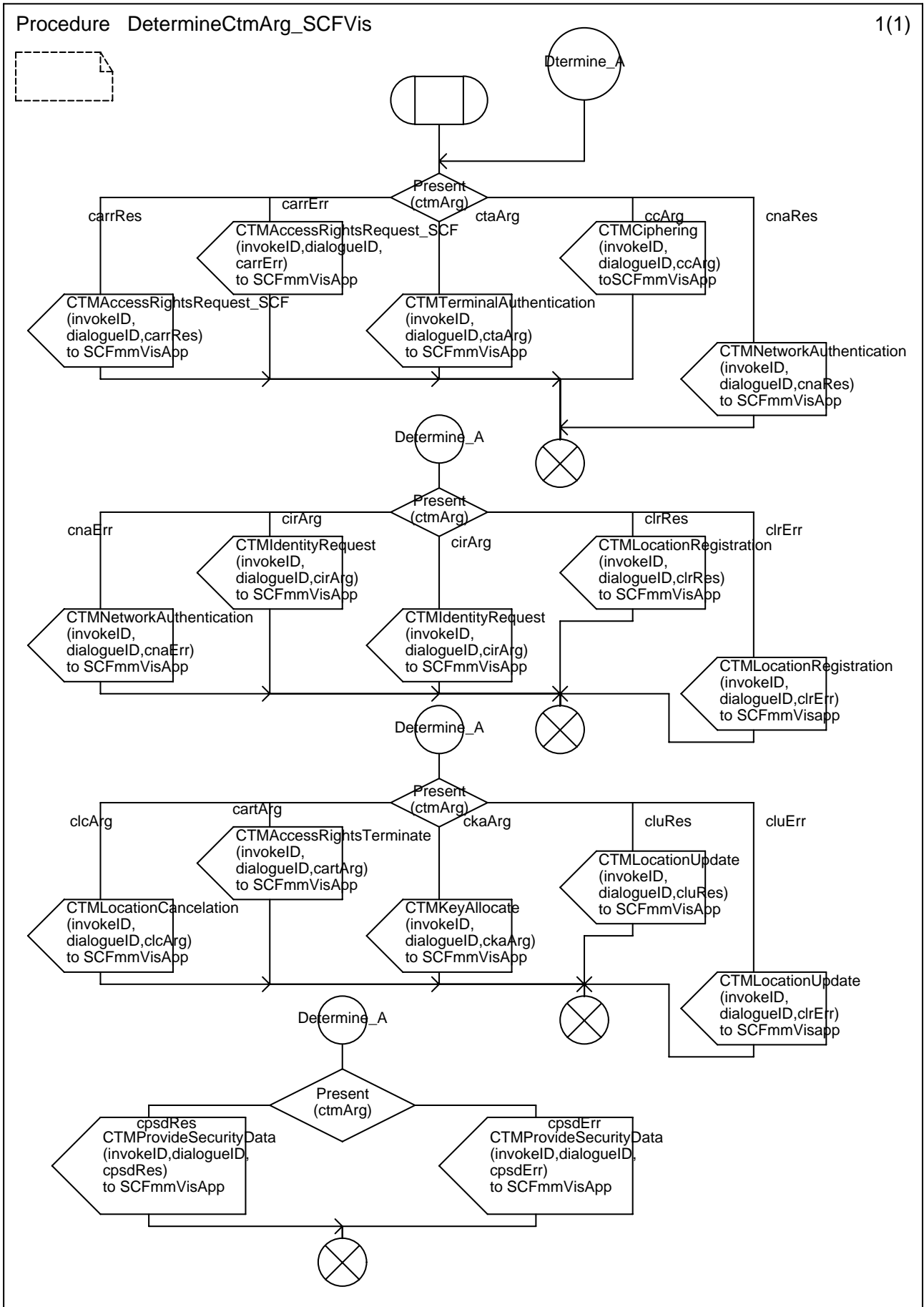


Figure C.45

C.20 Block Type SCFHomCTM

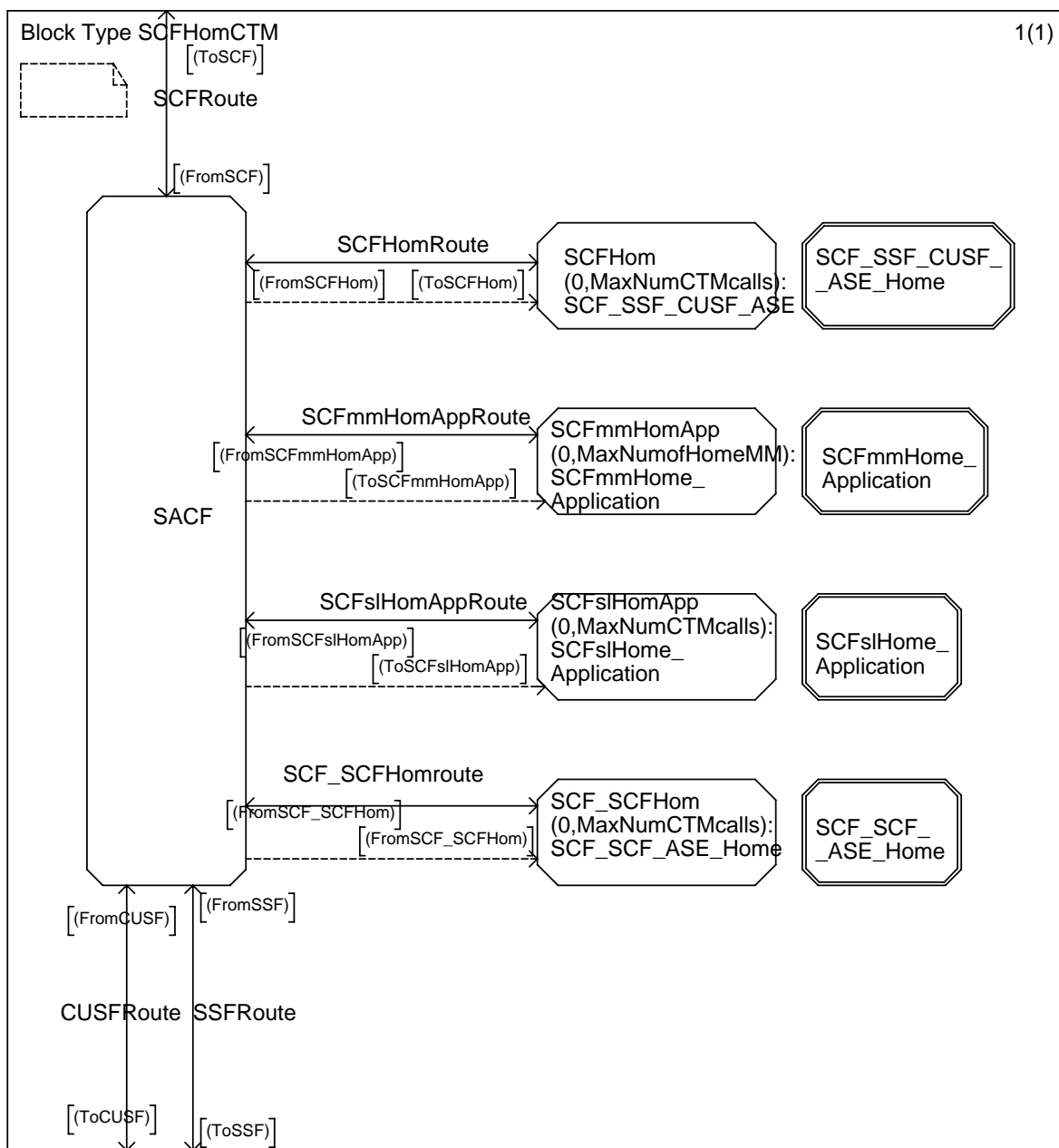


Figure C.46

C.21 Process Type SCFmmHomeApplication

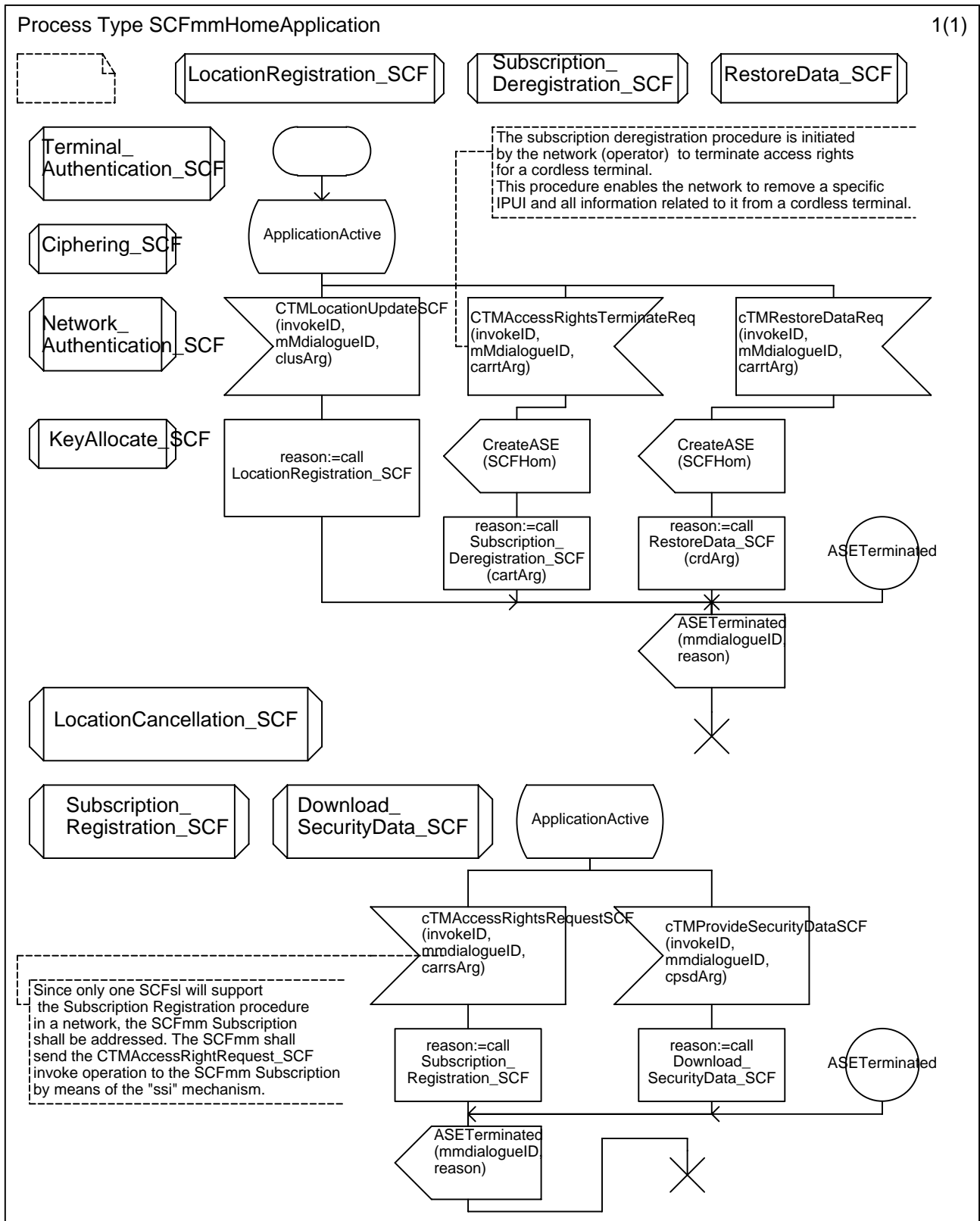


Figure C.47

C.22 Procedure LocationRegistration_SCF

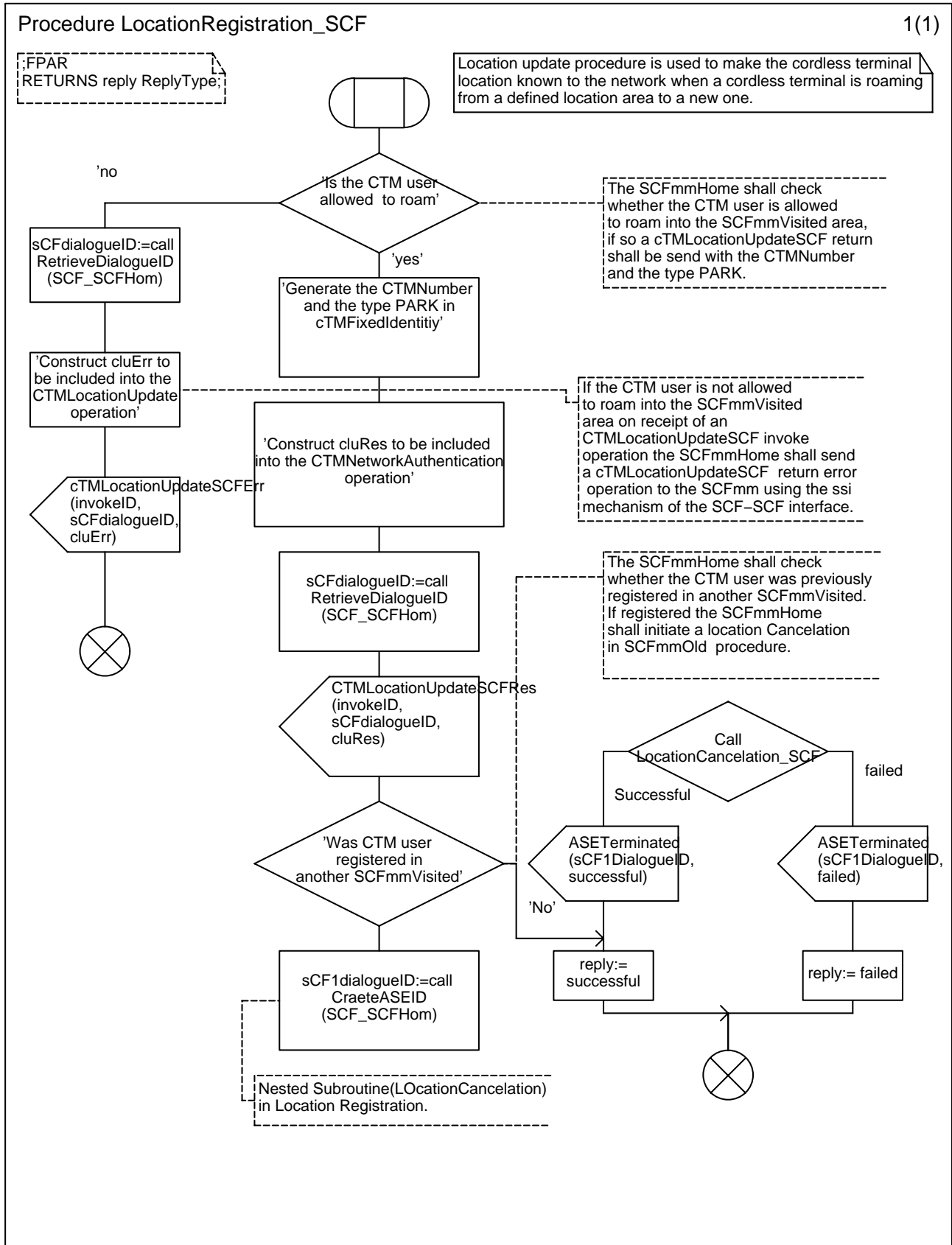


Figure C.48

C.23 Procedure SubscriptionDeregistration_SCF

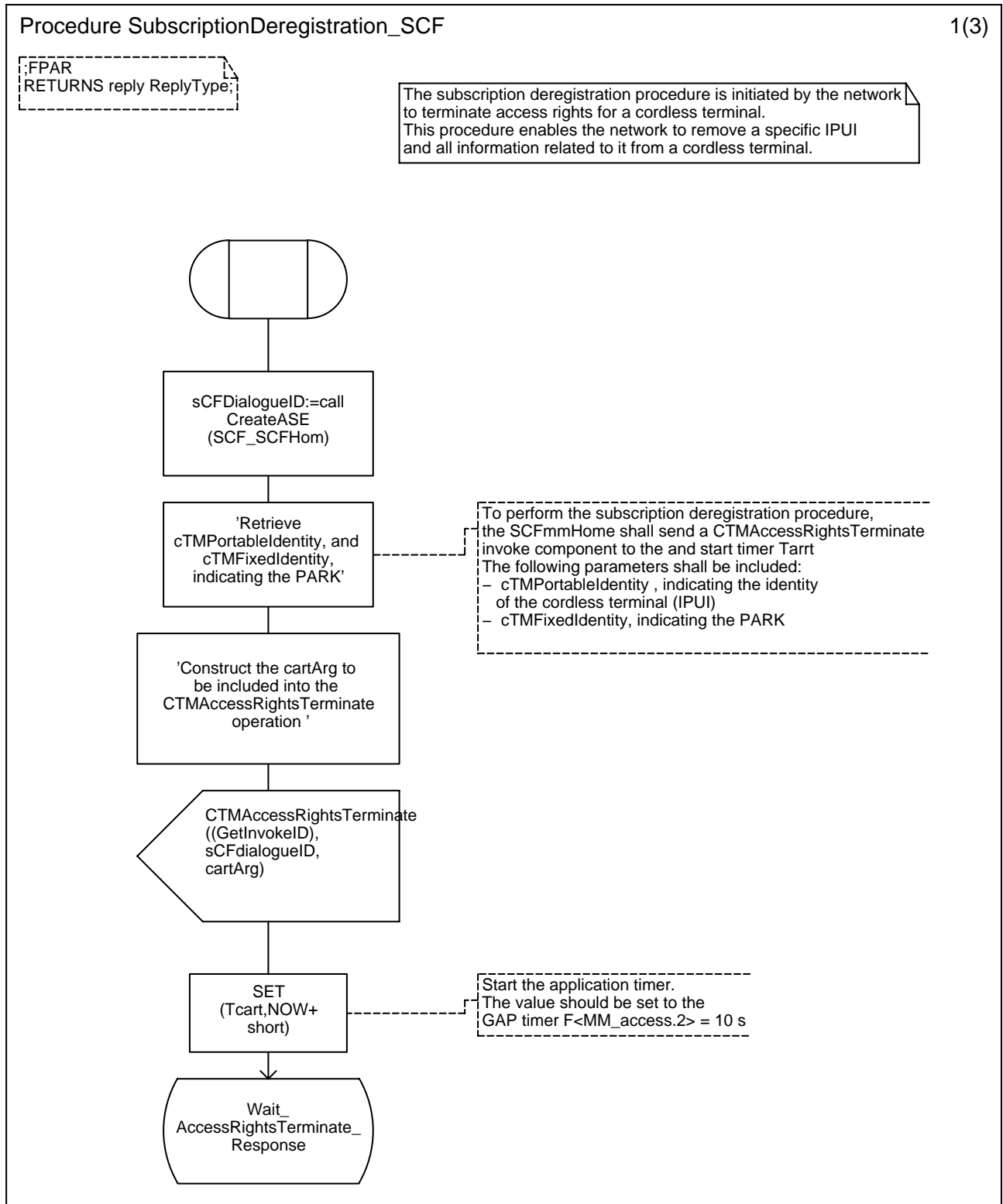


Figure C.49

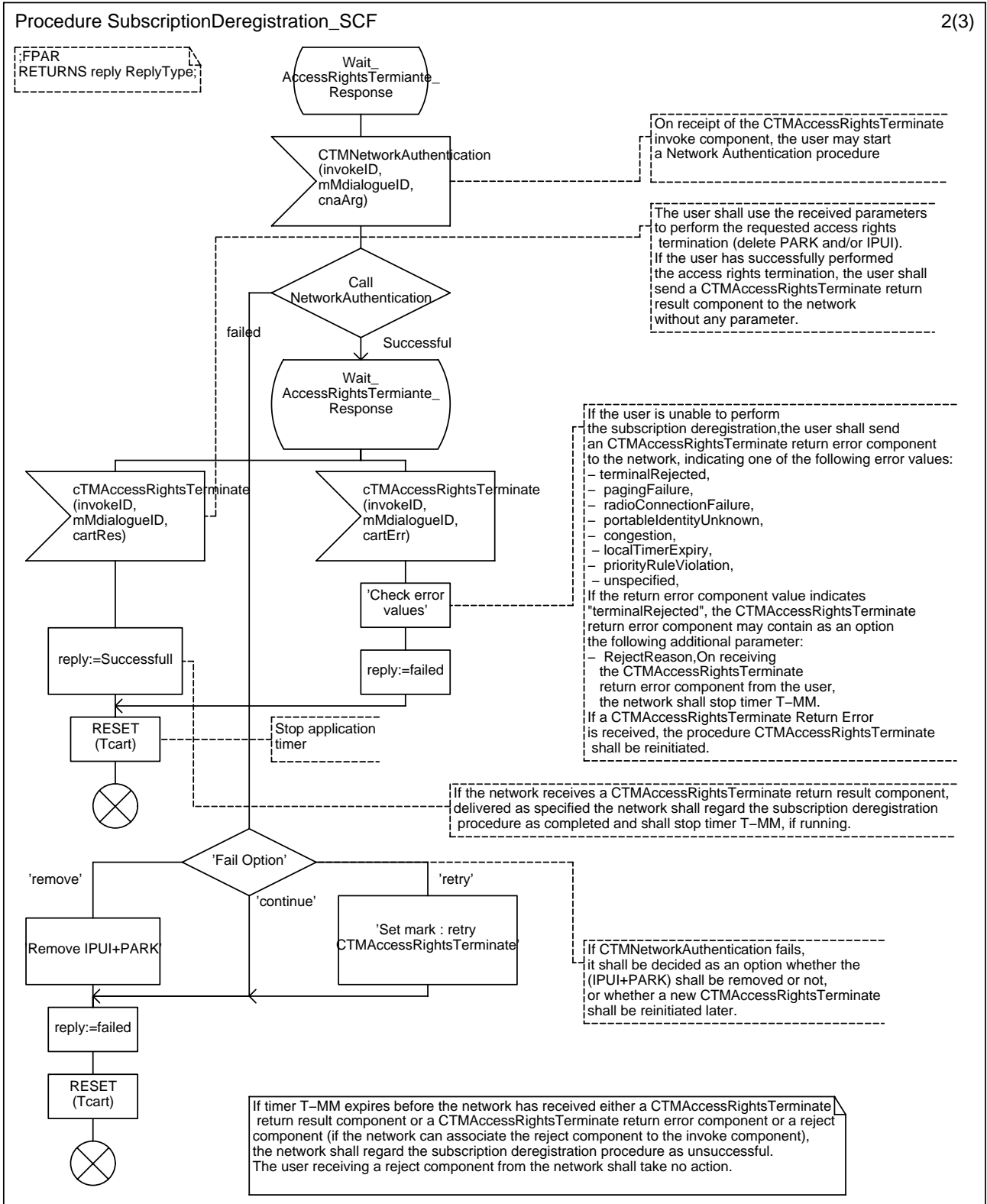


Figure C.50

Procedure SubscriptionDeregistration_SCF

3(3)

;FPAR
RETURNS reply ReplyType;

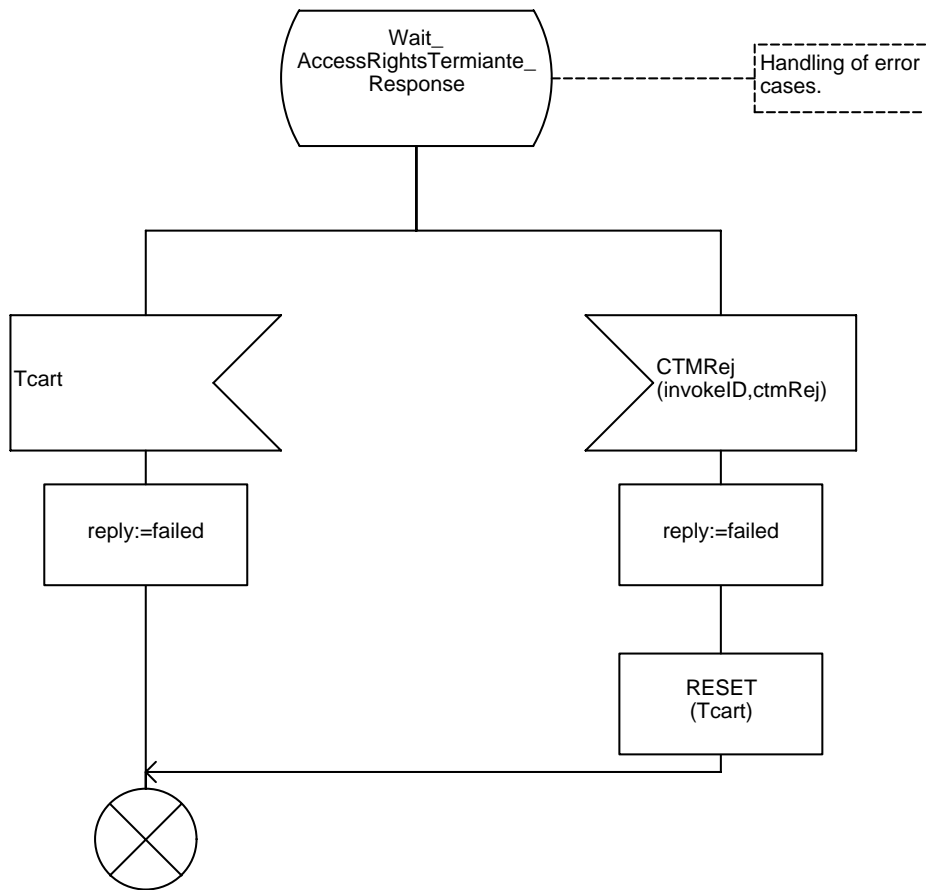


Figure C.51

C.24 Procedure RestoreData_SCF

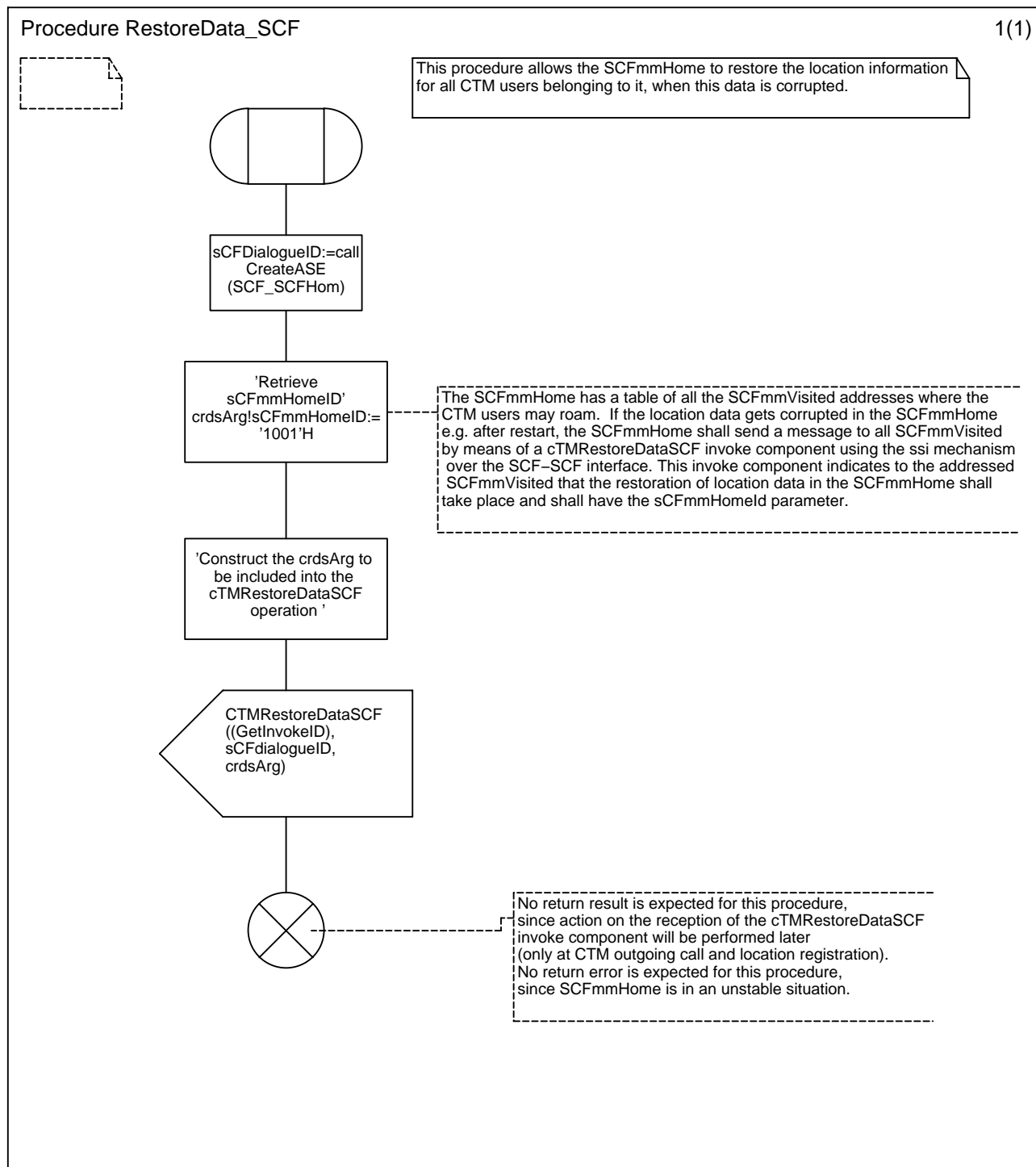


Figure C.52

C.25 Procedure TerminalAuthentication_SCF

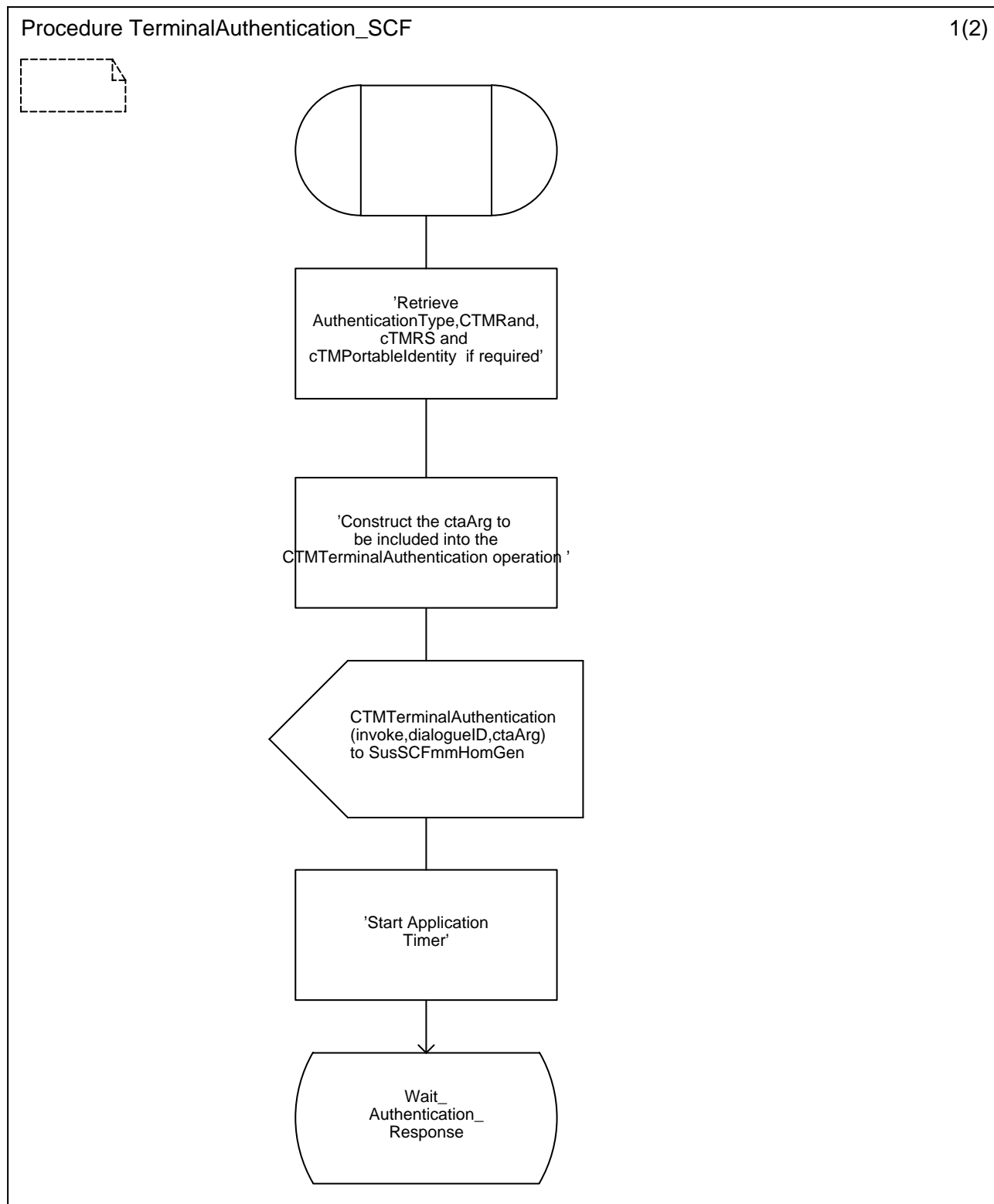


Figure C.53

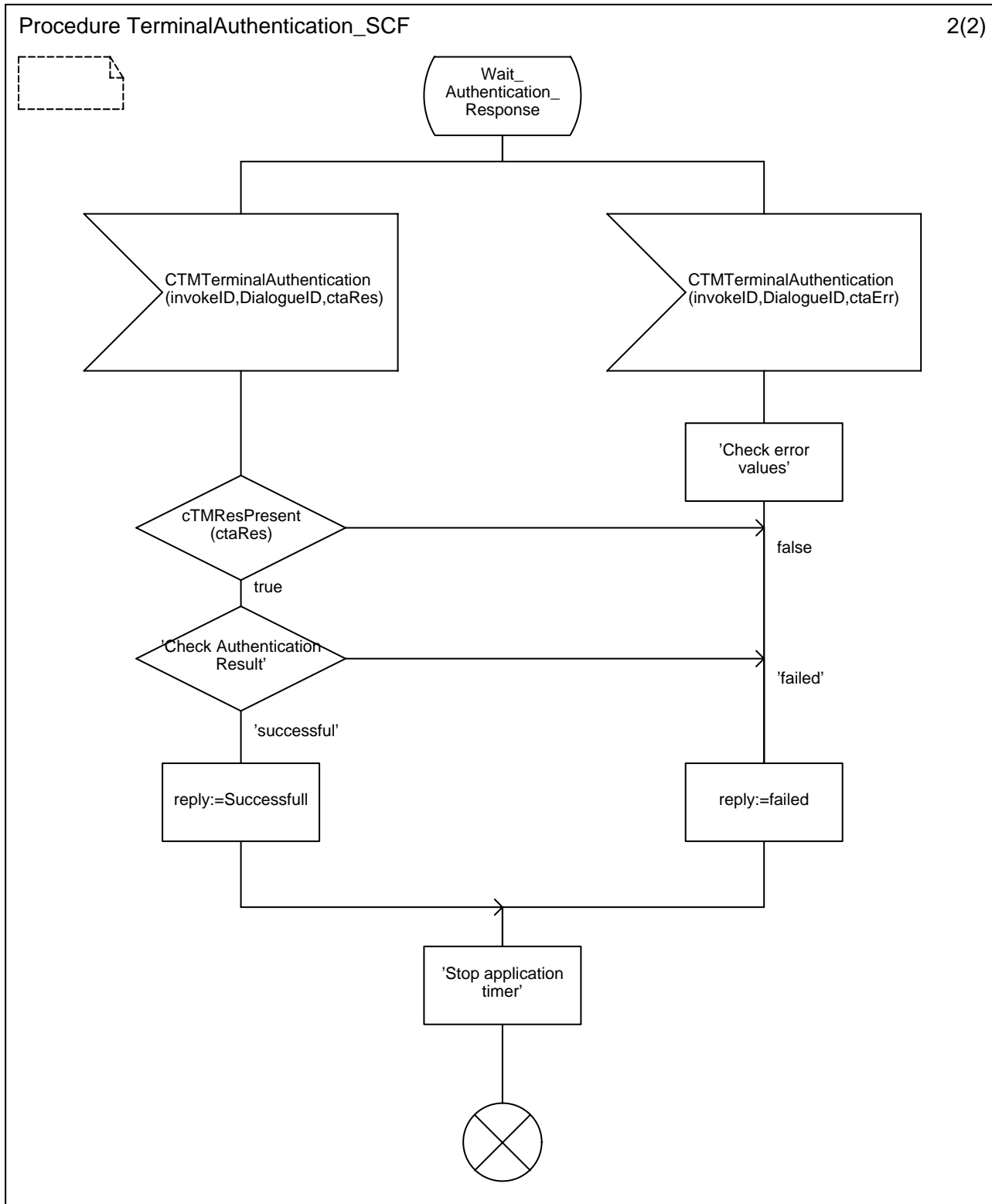


Figure C.54

C.26 Procedure CIPHERING_SCF

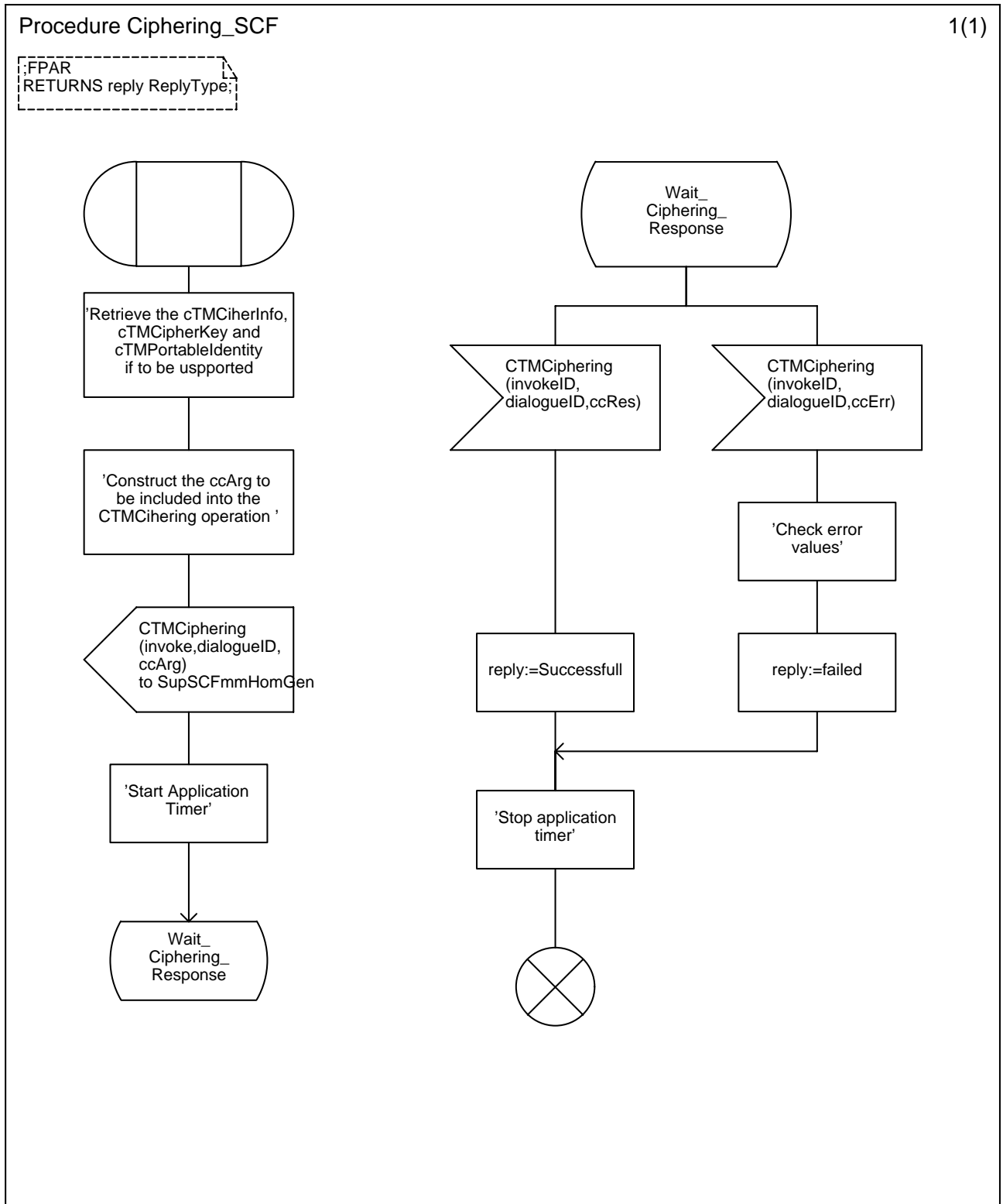


Figure C.55

C.27 Procedure NetworkAuthentication_SCF

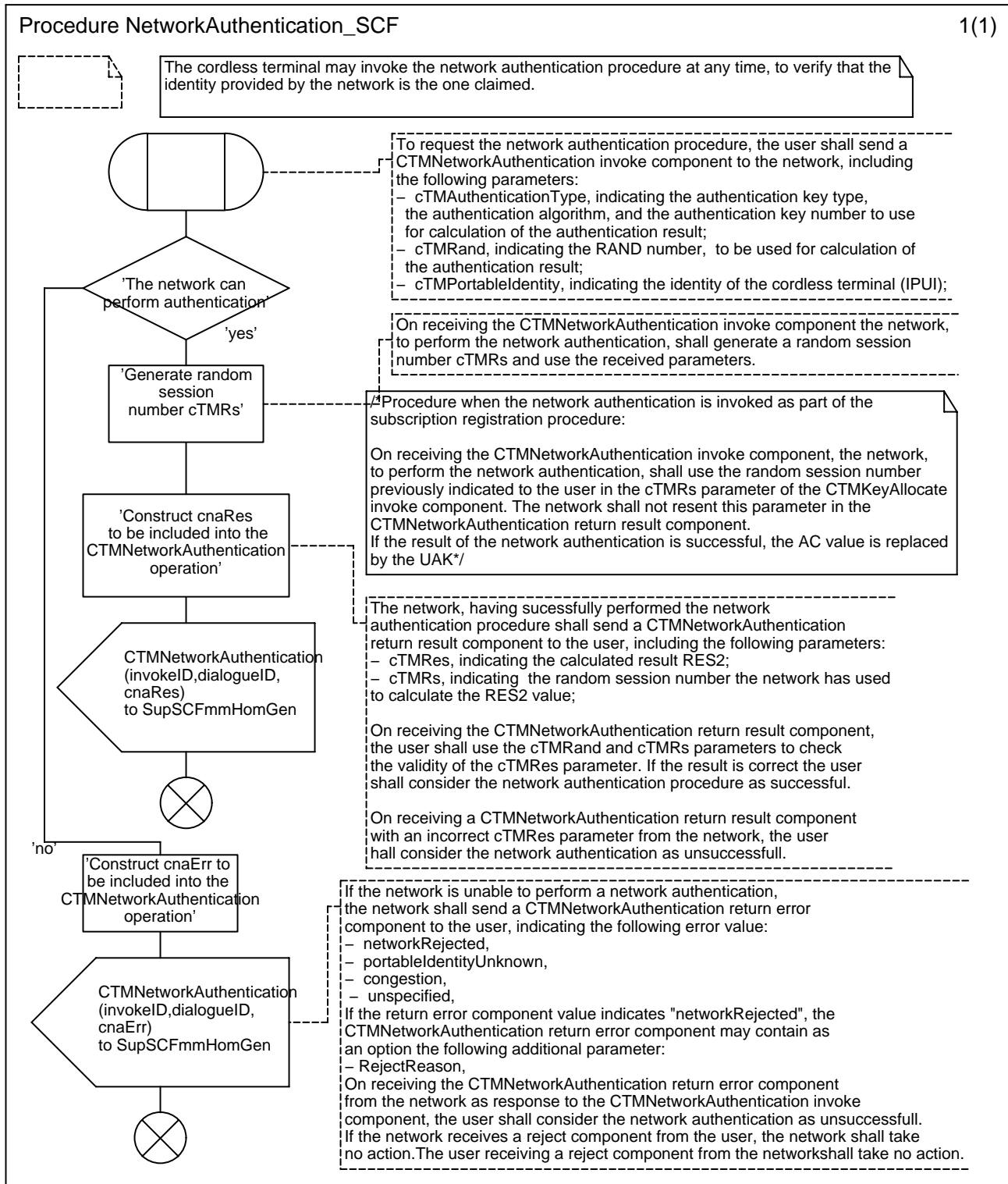


Figure C.56

C.28 Procedure KeyAllocate_SCF

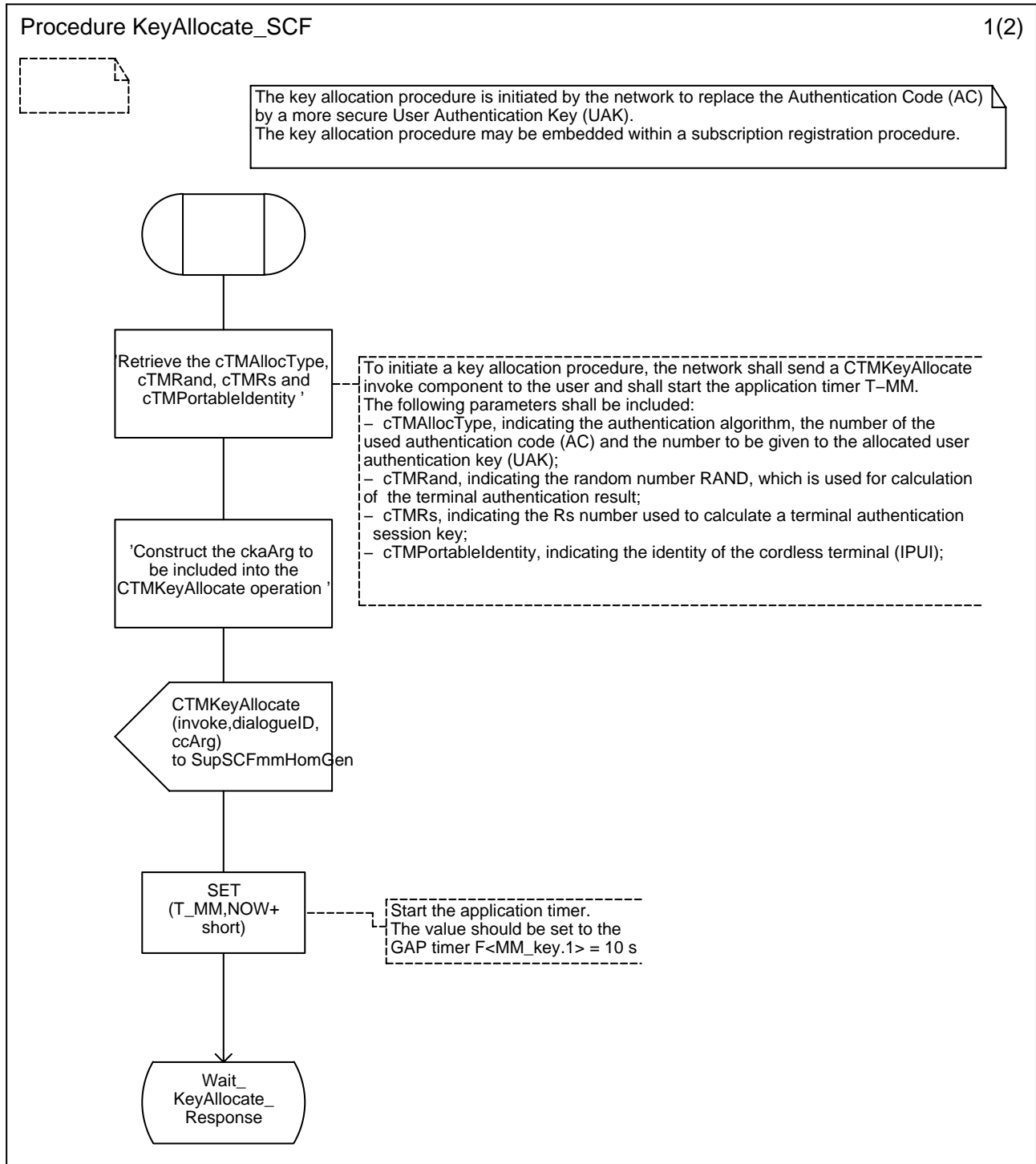


Figure C.57

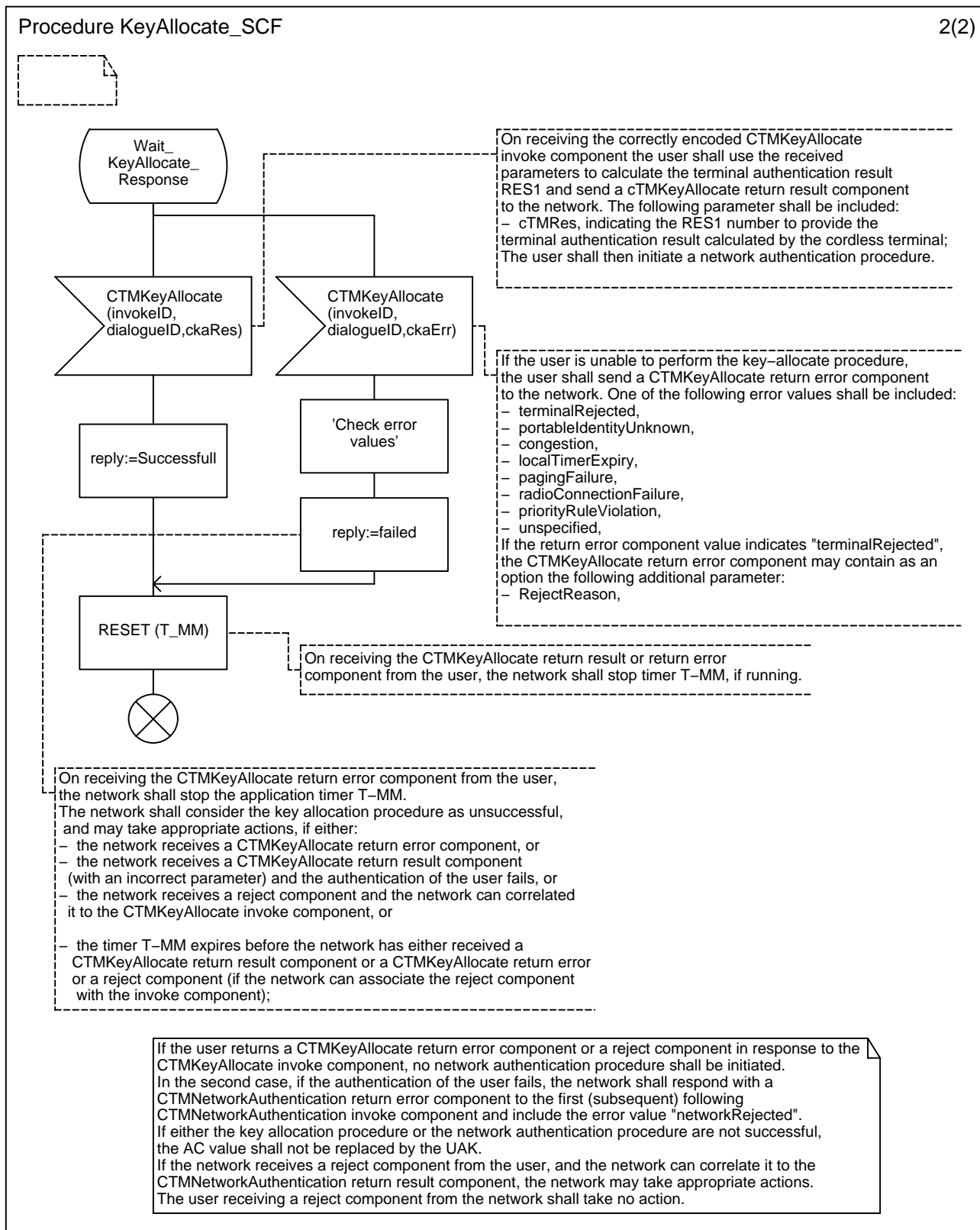


Figure C.58

C.29 Procedure LocationCancellation_SCF

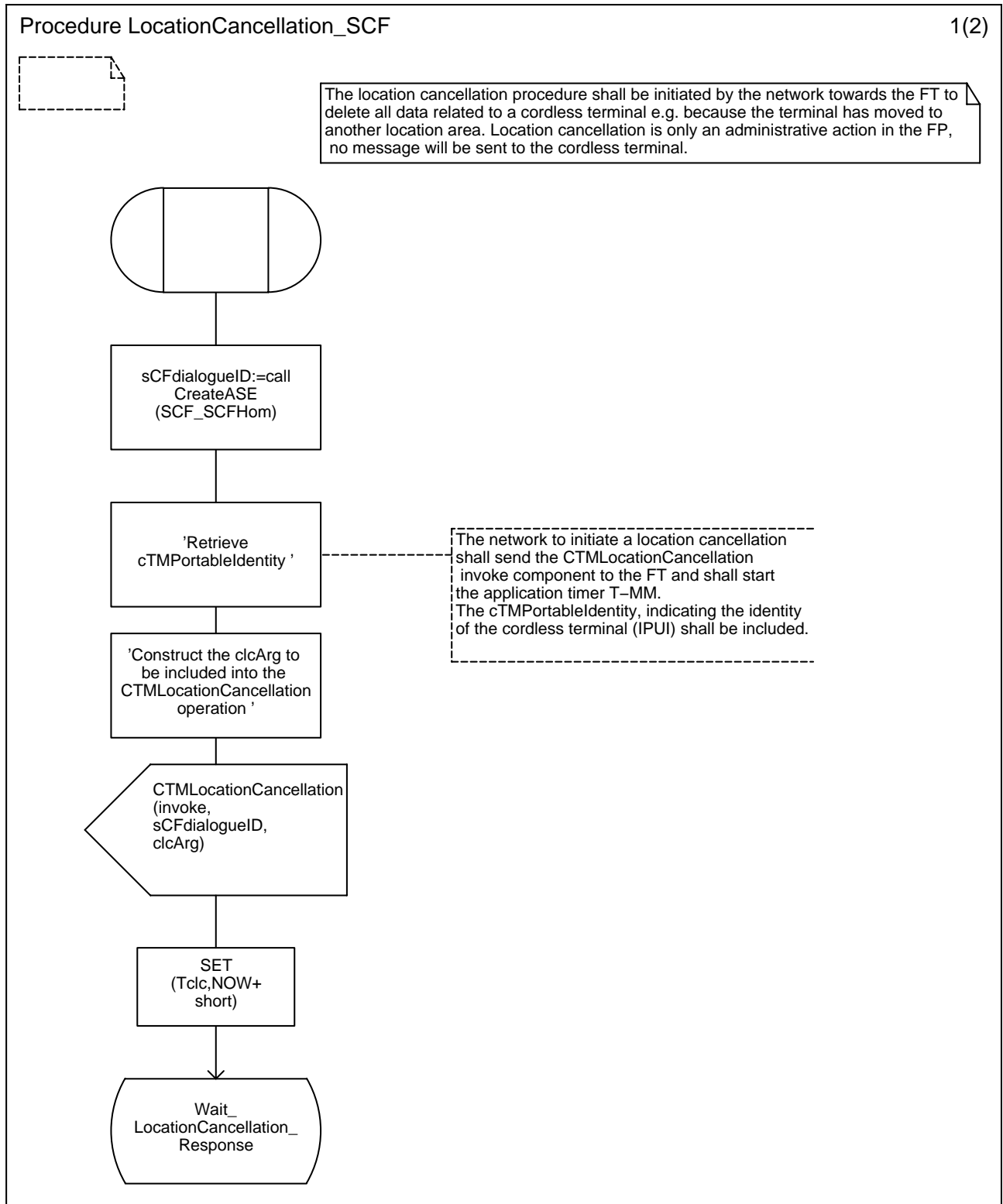


Figure C.59

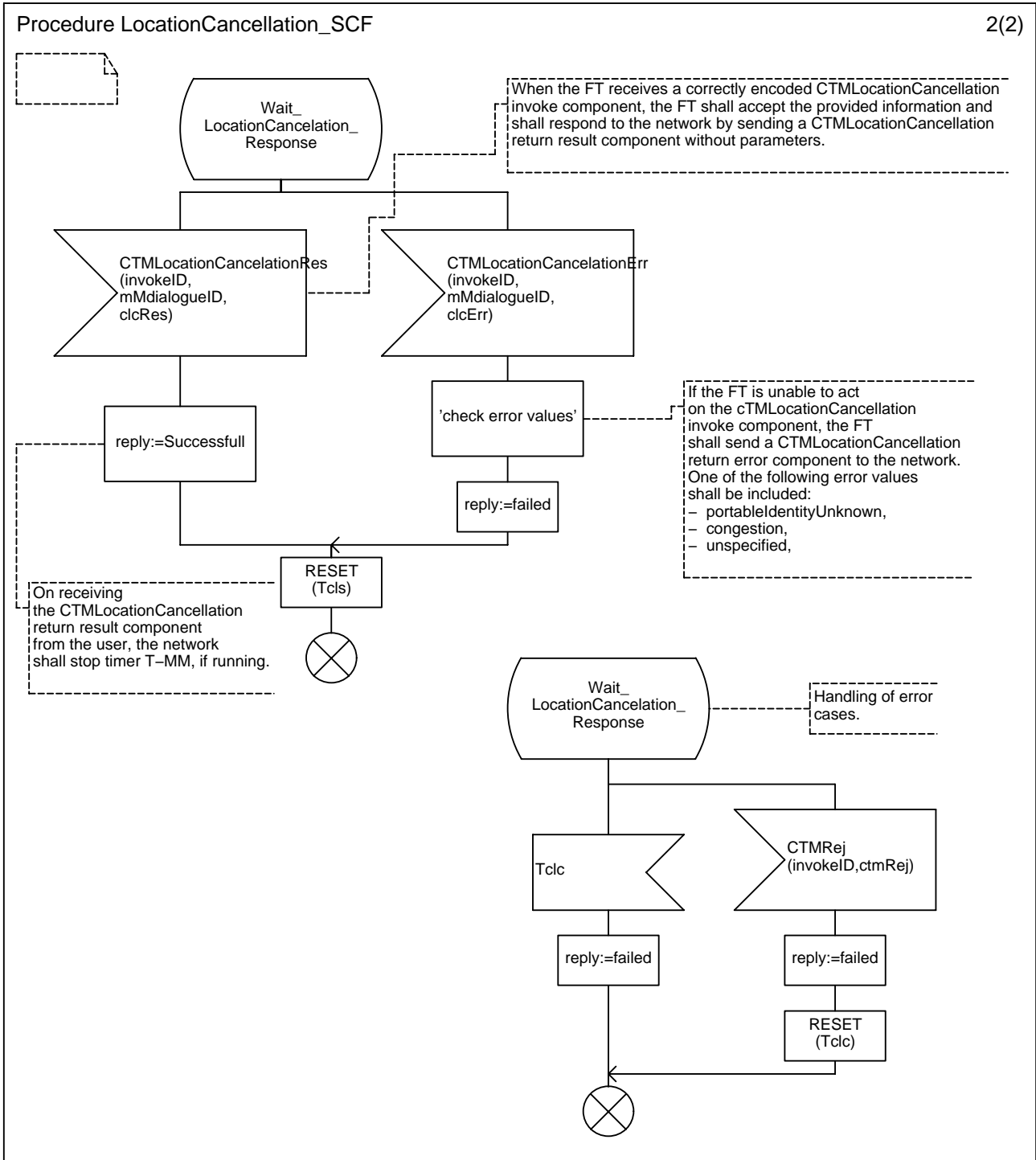


Figure C.60

C.30 Procedure SubscriptionRegistration_SCF

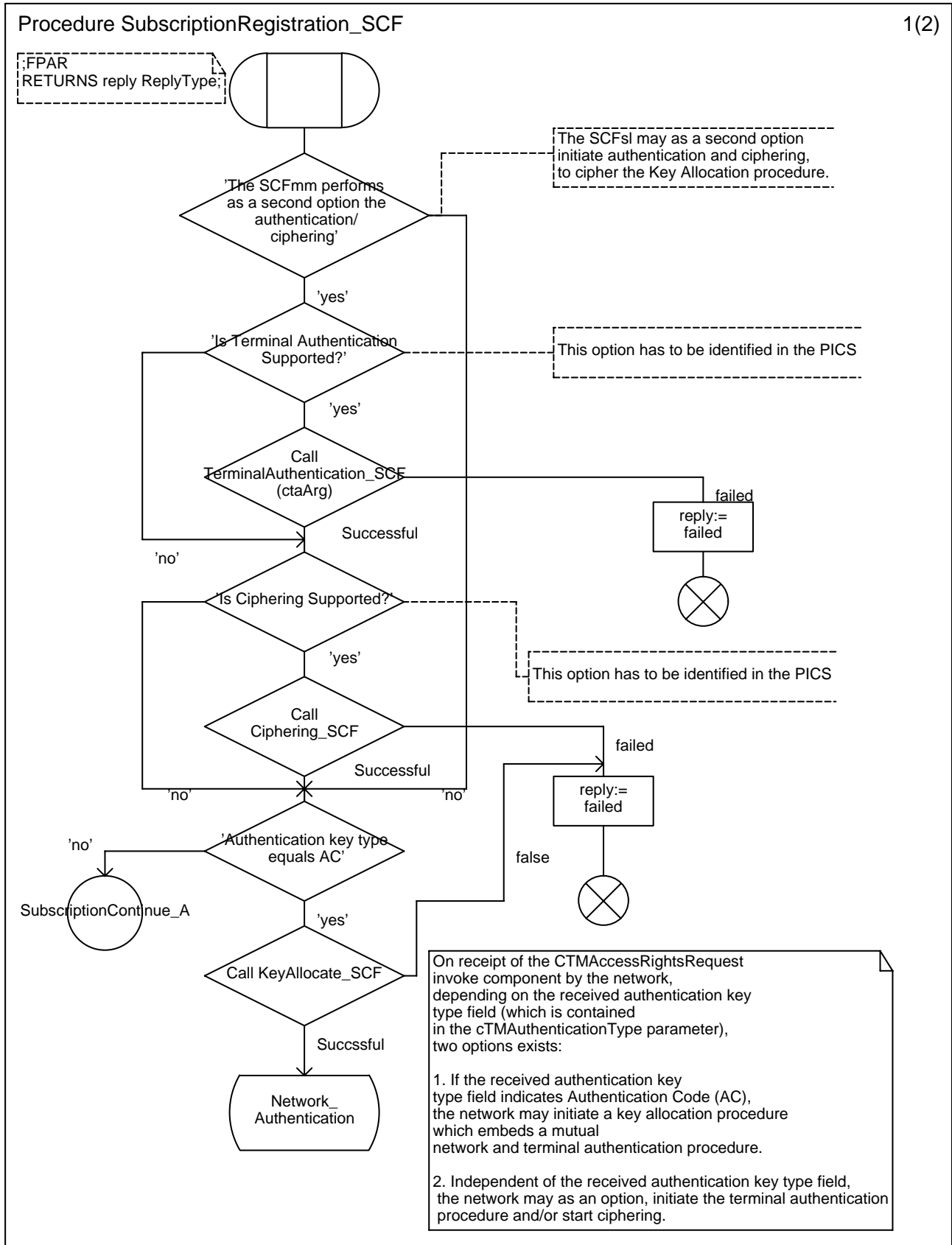


Figure C.61

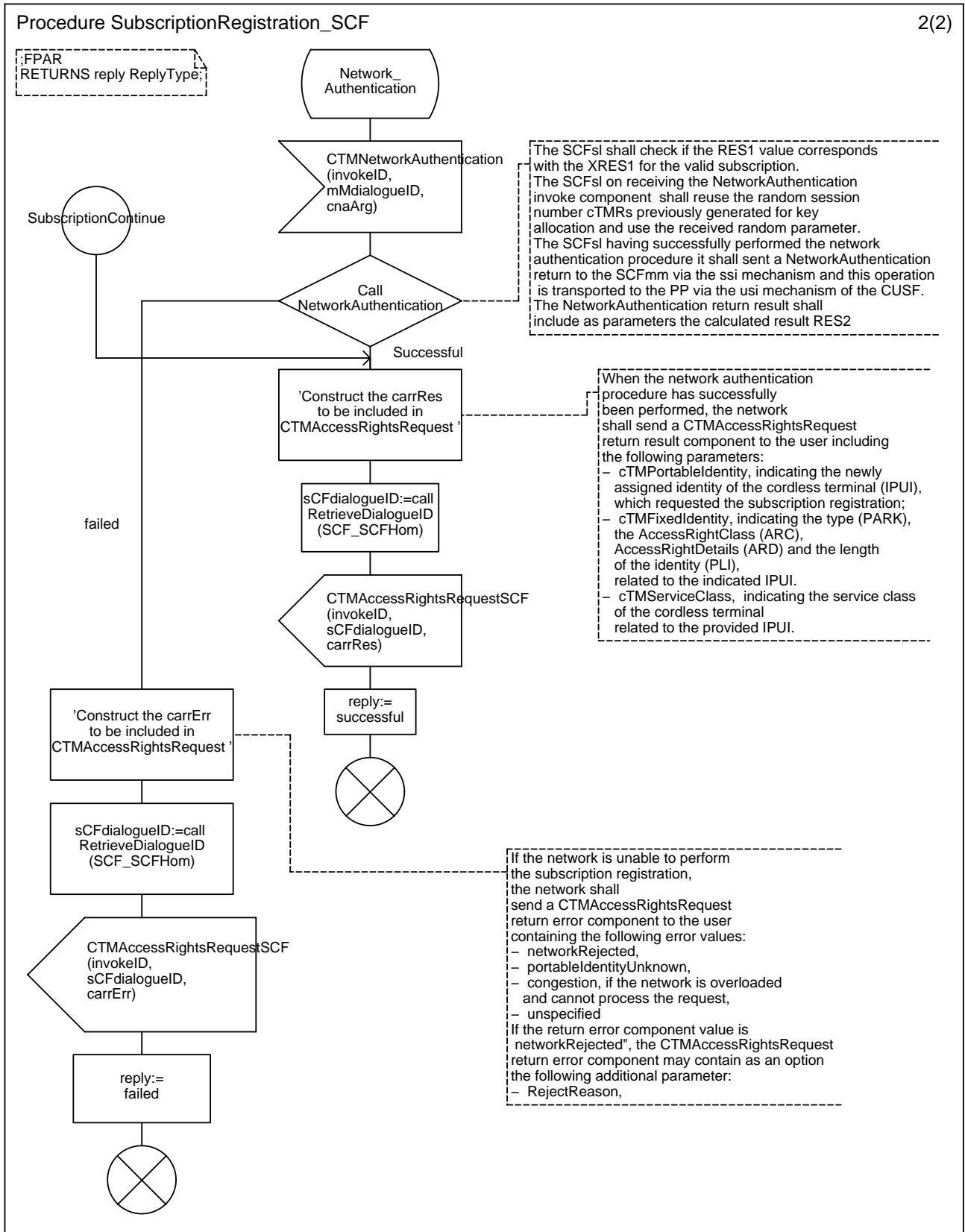


Figure C.62

C.31 Procedure DownloadSecurityData_SCF

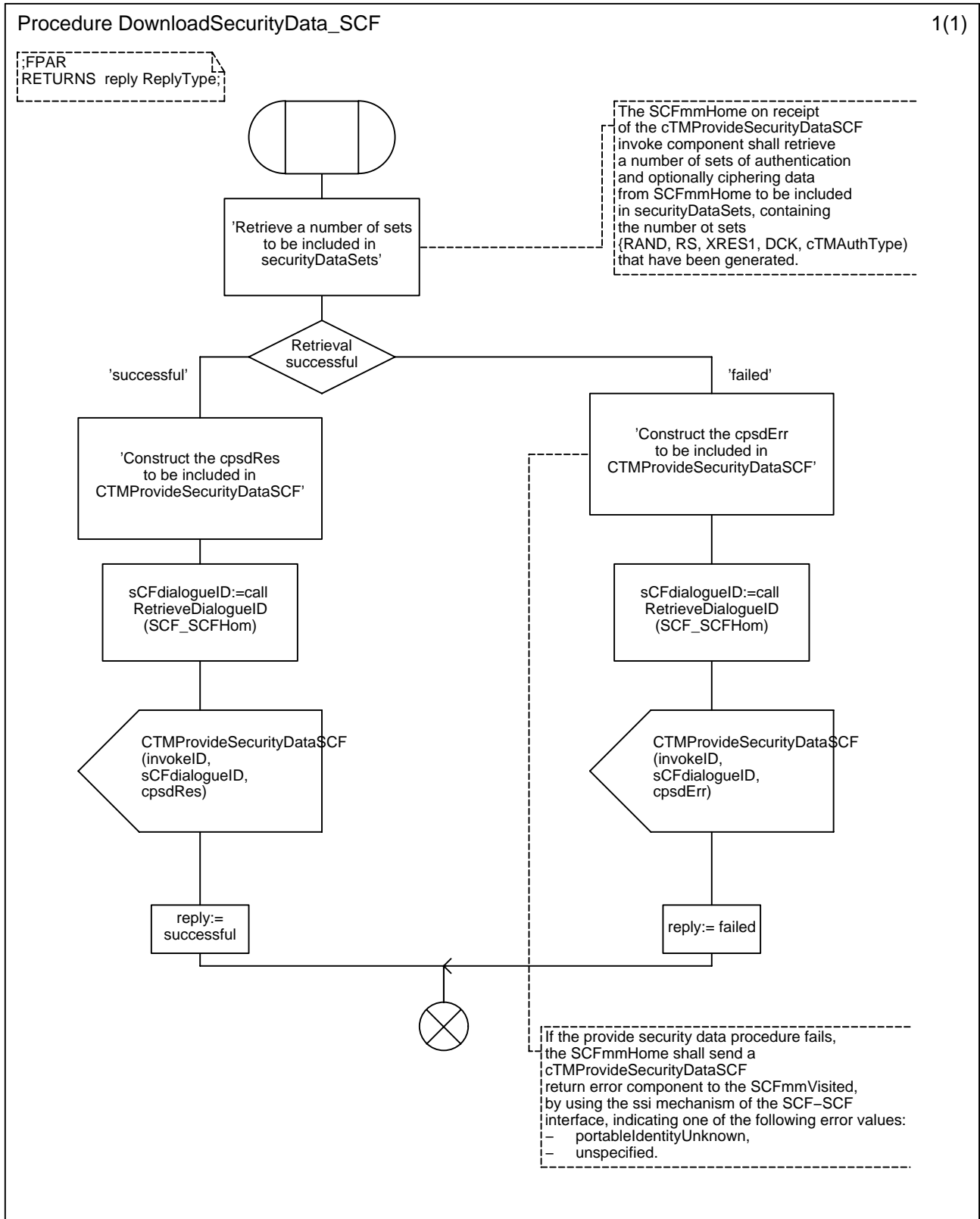


Figure C.63

C.32 Process Type SCFslHomeApplication

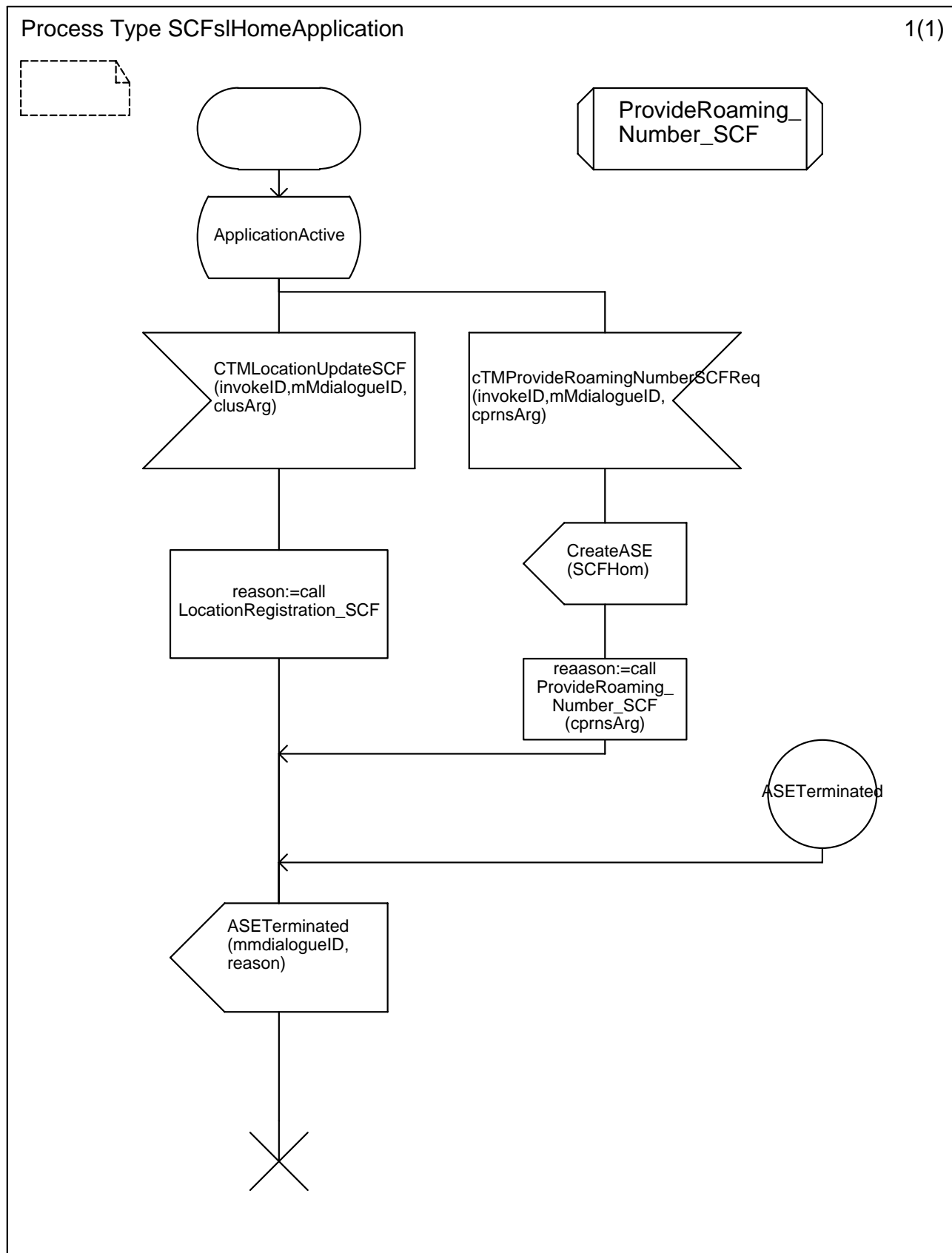


Figure C.64

C.33 Procedure ProvideRoamingNumber_SCF

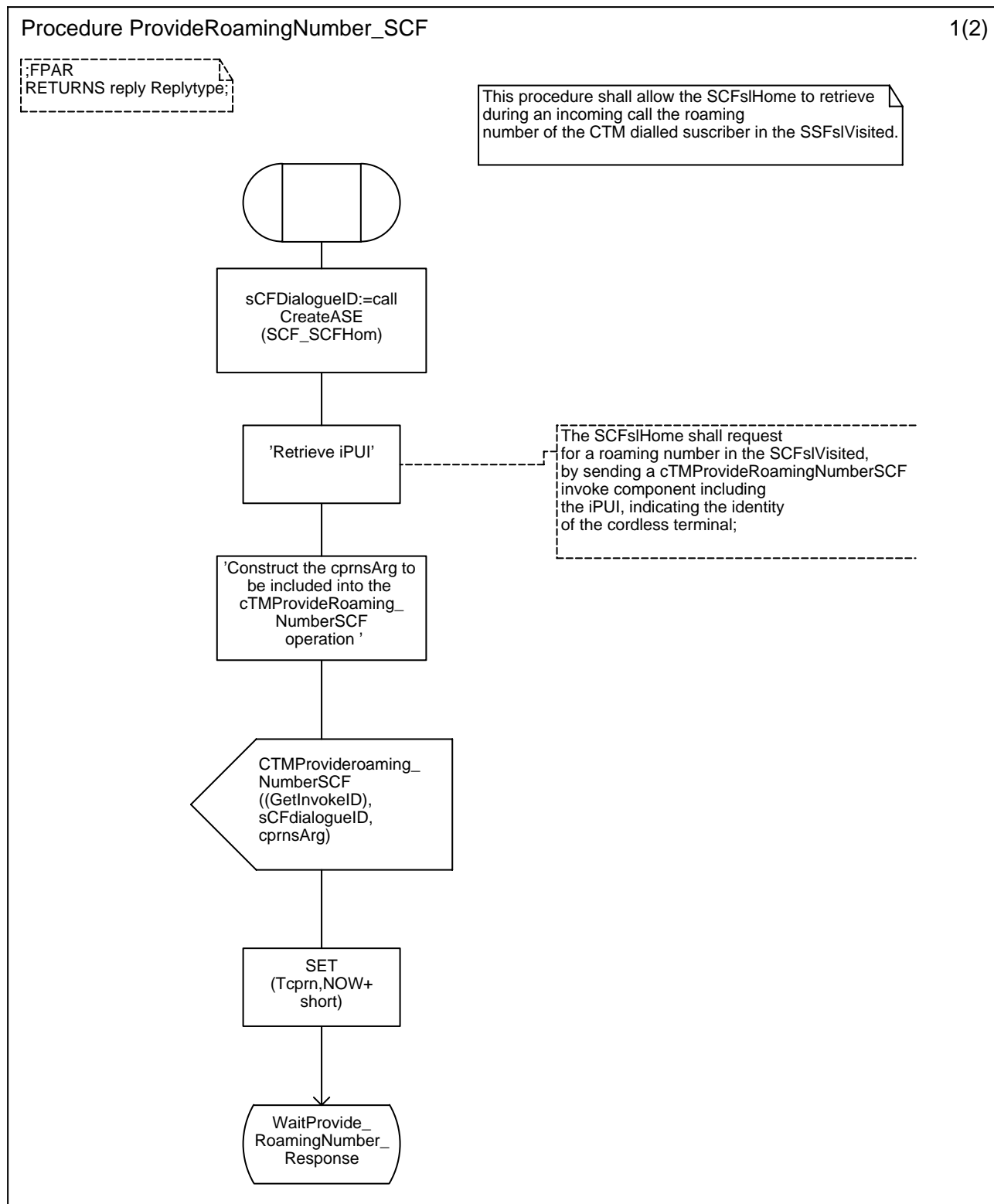


Figure C.65

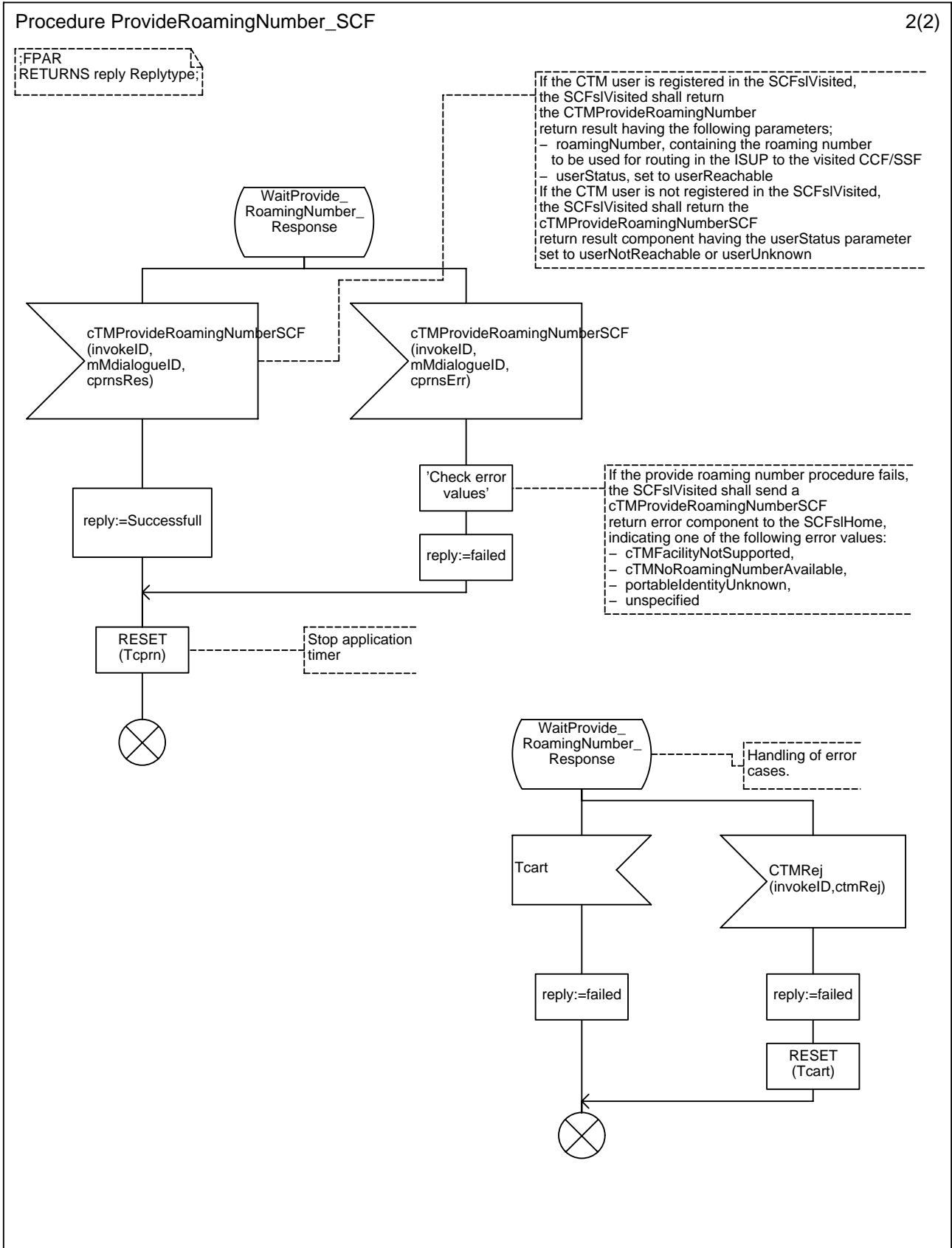


Figure C.66

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 I.112 (1993): "Vocabulary of terms for ISDN".
- CCITT Recommendation I.130 (1988): "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".
- ITU-T Recommendation I.210 (1993): "Principles of telecommunication services supported by an ISDN and the means to describe them".
- ITU-T Recommendation I.221 (1993): "Common specific characteristics of services".
- CCITT Recommendation Q.9 (1988): "Vocabulary of switching and signalling terms".
- CCITT Recommendation X.219 (1988): "Remote Operations: Model, notation and service definition".
- ITU-T Recommendation X.680 (1994): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".
- ITU-T Recommendation Z.100: "CCITT Specification and description language (SDL)".
- EG 201 096-1: "Intelligent Network (IN); Cordless Terminal Mobility (CTM); IN architecture and functionality for the support of CTM".
- EG 201 096-2: "Intelligent Network (IN); Cordless Terminal Mobility (CTM); IN architecture and functionality for the support of CTM; Part 2: CTM interworking between public Intelligent Networks".
- EG 201 096-3: "Intelligent Network (IN); Cordless Terminal Mobility (CTM); IN architecture and functionality for the support of CTM; Part 3: CTM interworking between private networks and public Intelligent Network".
- EN 301 175 (V1.1): "Cordless Terminal Mobility (CTM), Phase 1; Service description".
- ETS 300 175-5 (1995): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer".
- ETS 300 175-6 (1995): "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing".
- 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".
- EN 300 444 (V1.2): "Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)".
- ETS 300 787 (1997): "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".
- ETS 300 788 (1997): "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".

History

Document history				
V1.1.1	January 1998	Public Enquiry	PE 9820:	1998-01-16 to 1998-05-15
V1.1.3	June 1999	Vote	V 9935:	1999-06-14 to 1999-08-27
V1.1.4	September 1999	Publication		