Draft EG 201 096-1 V1.1.1 (1997-12)

ETSI Guide

Intelligent Network (IN); Cordless Terminal Mobility (CTM); IN architecture and functionality for the support of CTM; Part 1: CTM phase 1 for single public network case

European Telecommunications Standards Institute

Reference
DEG/NA-061302-1 (a5c90icq.PDF)

Keywords
CTM, IN, network, public,

ETSI Secretariat

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

X.400
c= fr; a=atlas; p=etsi; s=secretariat

Internet
secretariat@etsi.fr
http://www.etsi.fr

Contents

Intellectual Property Rights

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

Pursuant to the ETSI Interim 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 ETR 314 (or the updates on http://www.etsi.fr/ipr) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide (EG) has been produced by ETSI Technical Committee Network Aspects (NA), and is now submitted for the ETSI standards Membership Procedure.

The present document is part 1 of a multi-part EG 201 096 covering Intellligent Network (IN) Cordless Terminal Mobility (CTM); IN Architecture and Functionality for the support of CTM, as identified below:

Part 1: "Intelligent Network (IN) Cordless Terminal Mobility (CTM) IN architecture and functionality for the support of CTM; CTM phase 1 for single network case";

Part 2: "Intellligent Network (IN) Cordless Terminal Mobility (CTM)IN architecture and functionality for the support of CTM; CTM Interworking between Public Intelligent Networks";

Part 3: "Intellligent Network (IN) Cordless Terminal Mobility (CTM)IN architecture and functionality for the support of CTM; CTM Interworking between private networks and public Intelligent Networks".

Introduction

The present document will be produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI). The present document is based on ITU-T CS-1 Q.121X series Intelligent Network Recommendations (Q.1201 through Q.1290 [1]), as given in CCITT COM XI-R 164, 1992, and CS-2 Q.122X series Intelligent Network Recommendations.

1 Scope

This present document describes functional architecture requirements and network procedure for the support of CTM Phase 1 based on IN CS2.

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] CCITT Recommendation Q.1290 (1992): "Glossary of terms used in the definition of Intelligent Networks".

[2] ETS 300 415 (1996): Private Integrated Services Networks (PISN); Terms and Definitions.

[3] CCITT Recommendation Q.1224 (1996): "Distributed Functional Plane for Intelligent Network CS-2".

[4] ES 201 095: "Cordless Terminal Mobility (CTM): numbering and identifing".

[5] CCITT Recommendation Q.1201 (1992): "Principles of Intelligent Network Architecture".

3 Definitions and abbreviations

3.1 Definitions

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

The definitions given in NA-TR 016, draft EN/NA-020039 (see bibliography) and in CCITT Recommendation Q. 1205 (see bibliography) also apply to the present document.

CTM: PT Mobility involves the ability of the PT to be mobile within and between networks. The mobility may be continuous while the PT is accessing and using the telecommunication services offered by the public or private network, and it includes the capability of the networks to keep track of the PT s location throughout the entire network.

CTM Number and CTM ID: As defined in ES 201 095 [4].

FT: A logical group that contains all the processes and procedures on the fixed side of the CTM air interface. An FT may be connected to a Local exchange by one or more Basic Access (BA) or Primary Rate Access (PRA) accesses.

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

Location Area: The radio coverage area in which a PT may receive calls as a result of a single location registration.

scfsl: Indicates a SCF where a SLP devoted to CTM service feature control is active (e.g. the SCF that triggers on a CTM user terminating call request and does access the SDF containing the user profile).

sdfsl: Indicates the SDF where the CTM user profile is stored.

scfmm: Indicates a SCF where a SLP devoted only to mobility control is running (e.g. the CTM user has roamed to a FT under the SCFmm control).

sdfmm: Indicates a SDF where only terminal data are stored.

3.2 Abbreviations

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

ACM	Address Complete Message
ANS	ANSwer
AR	Authentication Request
BA	Basic Access
BCSM	Basic Call State Machine
BCUSM	Basic Call Unrelated State Machine
CCAF	Call Control Agent Function
CCF	Call Control Function
CKEY	enCrypted KEY
CS	Capability Set
CSF	Cell Site Function
CT2	Cordless Telecommunications generation 2
CTM	Cordless Terminal Mobility
CTMid	CTM identity
CUSF	Call Unrelated Service Function
DCK	Derived Chipper Key
DECT	Digital Enhanced Cordless Telecommunications (previously called Digital European Cordless Telecommunications)
FE	Functional Entity
FSM	Finite State Machine
FT	Fixed Termination
IAM	Initial Address Message
IN	Intelligent Network
IPUI	International Portable User Identity
K	secret Key in DECT and CT2
KS	authentication Session Key in DECT
LA	Location Area
LAI	Location Area Identifier
LCI	Local Cell Identifier
LID	Link IDentity
mm	mobility management
PA	Portable Application
PARK	Portable Access Rights Key
PRA	Primary Rate Access
PSTN	Public Switched Telephone Network
PT	Portable Terminal
RAND	a RANDom number issued by the network
RAND_F	a RANDom number issued by the network
RAND_P	a RANDom number issued by a PT
REL	RELease
RES	a RESponse calculated by a PT
RES1	a RESponse calculated by a PT
RES2	a RESponse calculated by the network
RFPI	Radio Fixed Part Identity
RN	Roaming Number
RS	a value used to establish authentication session keys in DECT
SCF	Service Control Function
SCFid	Service Control Function identity
SCP	Service Control Point

SCUAF	Service Control User Agent Function
SDF	Service Data Function
SDP	Service Data Point
sl	service logic
SLPI	Service Logic Program Instance
SPT	Service Profile Transfer
SRF	Specialized Resources Function
SSF	Service Switching Function
SSP	Service Switching Point
TPUI	Temporary Portable User Identity
TRD	Terminal user Registration Data
XRES1	an eXpected RESponse calculated by the network
N°	Number
O&M	Operational and Maintenance
SCFsl	Service Control Function
SLP	Single Link Procedure
IF	InterFace
XRES	X REf. entry Service
LE	Local Exchange
ISUP	ISDN User Part
DP	Distribution Point
EDP	Encrypted Data Processor
CSz	Connected Subaddress z
INAPconnect	IN Application Part Connect

NOTE: For comparison between DECT and CT2 terms see annex 1.

4 CTM service requirements

The CTM Phase 1 service requirements are specified in draft EN/NA-020039 (see bibliography).

NOTE: Document draft EN/NA-020039 (see bibliography) provides the CTM phase 1 service description, subsequent phases are likely to imply further requirements.

4.1 Core requirements

The core service features are listed hereafter.

- Outgoing Call.
- Incoming Call.
- Location Handling.
- Authentication and ciphering.
- Emergency Call.

Requirements for those procedures are contained in draft EN/NA-020039 (see bibliography).

4.2 Optional requirements

The optional service features are listed hereafter.

- Service Profile Modification.
- Service Profile Interrogation.
- Call Forwarding Not Reachable.

– Subscription Registration/Deregistration.

– Location registration Suggest.

– Network Authentication (only for Subscription Registration/Deregistration).

Requirements for those procedures are contained in draft EN/NA-020039 (see bibliography).

5 CTM Phase 1 functional architecture and procedures for the single public network case

This clause identifies CS-2 Functional Architecture required to support the CTM phase 1 service features described in draft EN/NA-020039 (see bibliography) in the case of one single IN-structured public network. The term single is used to pointed out that only one IN network is taken into consideration in this case ad that all the network FEs belong to the same network operator.

The presence of (multiple) service provider(s), which may be in principle different from the network operator, is examined as a particular case(s) of chapter 2.

NOTE: For the wireless access part the terminology and the functional architecture description used in TCR-TR 013 (see bibliography) are used. the access part is shown only for completeness based on DECT/CT-2 radio access, but it is not the intention of this document to specify the radio access part.

5.1 CTM Phase 1 functional model

The following figure provides the CTM phase 1 functional architecture (only the network side of the functional architecture is shown but not the side belonging to the radio interface).

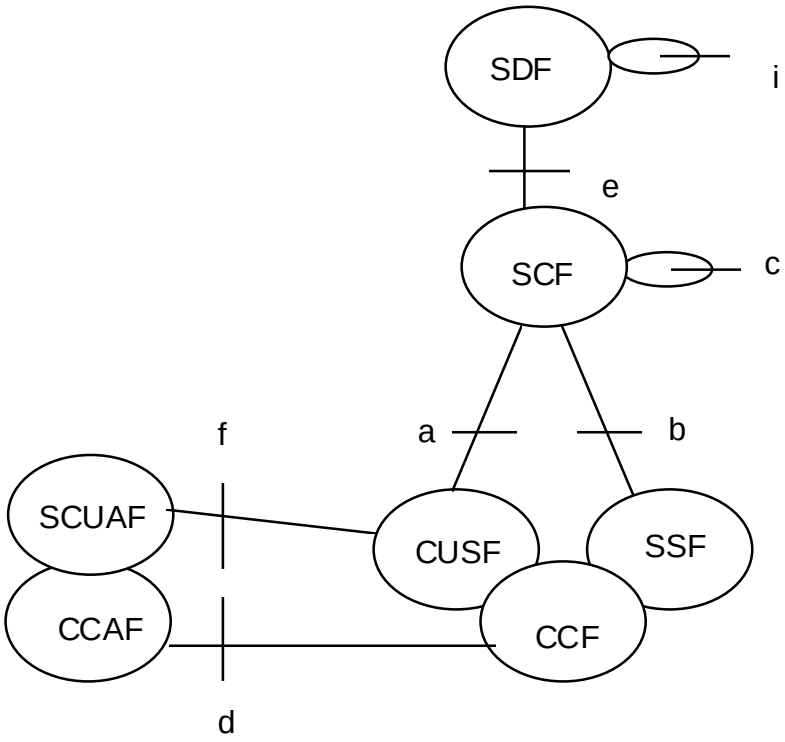


Figure 1: Functional architecture

This functional approach shown in figure 1 indicates ("a", "b" relationship) the need to separate call related versus non call related service functions. Since the description of radio specific cordless access functions (e.g. CT2 or DECT) is outside the scope of this model, SCUAF and Call Control Agent Function (CCAF) Functional Entity (FE) ("d" and "f" relationships) are used to show the functions that map Fixed Termination (FT) on the physical plane. Relationships "b" and "e" are assumed to be CS-1 IN Core INAP. Relationships "a" is assumed to be IN CS-2. Relationship "d" is assumed based on ISDN access (BA or PRA), while relation "f" is assumed to be DSS1+.

Note that figure 1 is applicable in the case of single domain; extension to multiple domains refer to part B and C. The IN CS-2 relationships "c" (SCF-SCF) and "i" (SDF-SDF) are optional in the single network case and they apply to the "end to end" functional model (see annex A clause 2).

As far as physical plane is concerned, Call Unrelated Service Function (CUSF) and Service Switching Function (SSF) can be either located in the same local exchange or can be located separately.

Other CS-1 IN FEs can be used for Cordless Terminal Mobility (CTM) (i.e. Specialized Resources Function (SRF)), but they are not explicitly shown in this document since there is no additional functionality required, compared to CS-1, in order to support CTM.

In the following descriptions, only the additional functionality is defined above CS-1. ETS 300 415 [2].

Service Switching Function (SSF)

As defined in the CS-1.

Moreover the SSF should dynamically associate the access line (to the FT) with the CTM user/terminal identity (e.g. for billing purposes) during the context of the call.

Service Control Function (SCF)

As defined in CS-1 (for incoming and outgoing calls). In addition intra-network CS-2 SCF-SCF service logic co-operation can occur and SCF can initiate interactions with CUSF.

Call unrelated User Service Function (CUSF)

The CUSF is the call Unrelated service function, which, associated with the CCF and the SSF, provides a set of functions, required for call unrelated interactions with a SCUAF. It also provides the set of functions required for interaction between the SCUAF and a SCF. It:

a) establishes, manages and releases the relationship between the instance in the SCUAF and the network for the Call unrelated associated interaction between user/terminal and CTM service processing;

b) recognizes a Call unrelated associated service control triggers and interacts with the SCF;

c) provides the trigger mechanism for non Call unrelated associated interaction to access IN functionality (e.g manages Call unrelated associated interaction events and passes them to the SCF);

d) modifies Call unrelated associated interaction processing functions (in the CUSF) as required to process requests for IN provided service usage under the control of the SCF;

e) it can response to the initiation from the SCF.

Service Control User Agent Function (SCUAF)

The SCUAF is the service control user agent function that provides access for users/terminals. It is the interface between a user/terminal and the call unrelated service functions (CUSF). It:

a) provides for user access, interacting with the user/terminal to establish, maintain, and release, as required, an instance of Call unrelated associated service;

b) access the functions for Call unrelated associated interaction processing in the CUSF, and the service invocation capabilities of the Call unrelated Service Function (CUSF), using service requests (e.g. location registration, attach, etc.) for the invocation of call unrelated associated services;

c) receives indications relating to a call unrelated associated services from the CUSF and relays them to the user/terminal as required;

d) maintains service state information as perceived by this functional entity;

e) (optionally) stores and cancels terminal location data.

Service Data Function (SDF)

As defined in CS-1 Refinements.

Call Control Function (CCF)

As defined in CS-1/Q.71.

Call Control Agent Function (CCAF)

As defined in CS-1 refinements.

5.2 Notations and Assumptions for CTM Phase 1 Procedures

In order to describe the procedures a specific "end to end" functional model is depicted for each case.

The following notations are used:

SCFsl and SCFmm notation

Different types of service logic instances can be running at the same time for the same CTM call, in order to separate the control of (user initiated) IN service features (e.g. CTM Incoming call or CTM Service Profile Interrogation) from the (terminal activated) network set of mechanisms, needed to support mobility features (e.g. Location Update). Therefore each type of service logic could control a distinct type of network events (one example is that Service Control Function (SCFsl) could be invoked because of a specific TDP-R in the O-BCSM while SCFmm could be invoked either because of a TDP-R in the Basic Call Unrelated State Machine (BCUSM) or because of a different TDP-R in the T-BCSM). Therefore SCFsl Single Link Procedure (SLP) and SCFmm SLP can either co-operate each other during the call processing (i.e. during the incoming call procedure) or can act independently (i.e. during a location registration update of an already registered CTM user, SCFmm SLP processing does not affect SCFsl SLP). In order to facilitate the description in the following text this notation is used: SCFmm indicates a SCF where a SLP devoted only to mobility control is running (e.g. the CTM user has roamed to a FT under the SCFmm control); SCFsl indicates a SCF where a SLP devoted to CTM service feature control is active (e.g. the SCF that triggers on a CTM user terminating call request and does access the SDF containing the user profile). Some aspects of this CTM service logic in SCFsl can be related to mobility (e.g. incoming call routing to a registered destination).

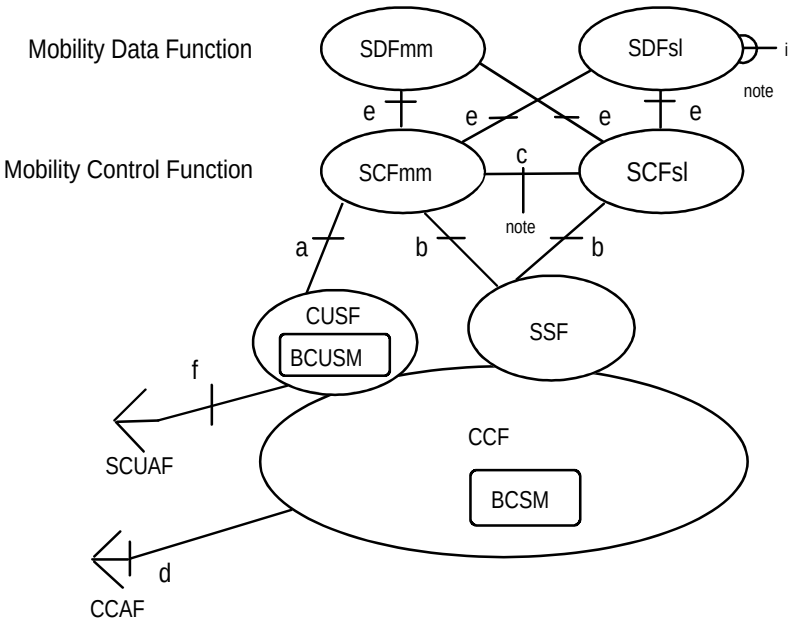
SDFsl and SDFmm notation

In order to be consistent with the previous notation introduced for the SCF case, in the following text the term SDFsl indicates a SDF where both the user profile and terminal data are referred (e.g. message waiting indication , backup number, etc.), while SDFmm indicates a SDF where only terminal data are referred (e.g. location registration and authentication data). In the physical plane the distinction between SDFmm and SDFsl does not assume any physical implementation solution; they can either be merged in a single Service Data Point (SDP) or mapped respectively into a visited SDP and a home SDP, depending on the network topology and network operator specific choices. See Appendix 1 for physical implementation examples.

Relationship between IN FSMs and FEs

BCUSM is used in this model to handle call unrelated terminal mobility associated events, instead of call related outchannel user interaction associated events, as in present CS-2 ITU model. This could imply that the latter type of events can not be handled in CTM phase 1.

When BCSM is engaged for CTM service related events, it can not be available for the invocation of some other IN services.



NOTE: This relationship is a network operator option in the single network case.

Figure 2: Relationship between FEs and FSMs

6 CTM Phase 1 procedures and information flows

This clause displays for each procedures the related functional flows; the mapping of these flows to specific protocol messages is outside the scope of this document.

In the information flows the results parameters associated to a search operation are relative to the procedure in which the search operation has been invoked.

NOTE: The following IFs are based on the following assumptions.

- clause 1

All the different places where authentication might occur are outlined in the Interface (IF) descriptions; the network operator is free to choose any of them.

- clause 2

Terminal mobility data (i.e. terminal id, location area id, etc.) can be optionally stored in the SCUAF. Consequently, if they are present, those data may need to be cancelled. However the SCUAF does not store authentication data (for security reason). These optional flows are inserted in the data deletion procedures.

6.1 Call unrelated procedures/IFs

6.1.1 Terminal authentication and ciphering procedures/IFs

6.1.1.1 Terminal authentication procedures

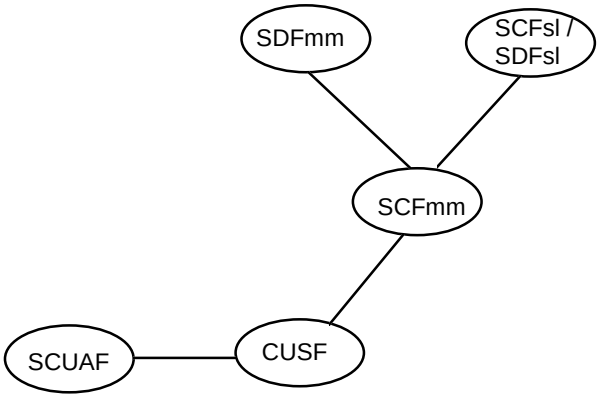


Figure 3: Terminal authentication

Refer to the specific call IFs to determine when it is activated.

NOTE: Secret key (K) is stored only in SDFsl and in the PT, it is not transferred outside the physical network element where it is stored (e.g. SDP).

6.1.1.2 Terminal authentication IFs

This subclause describes the information flows for call unrelated terminal authentication. Two cases are envisaged for DECT, one for CT-2. The description of the storage of the data in the SDFmm is described in a different clause.

6.1.1.2.1 Terminal authentication - case 1: DECT (Rs, Ks) couples previously stored in SDFmm

This case is only applicable with DECT. DECT authentication parameters (Rs, Ks) are already available at SDFmm. The algorithm A12 is in the SCFmm.

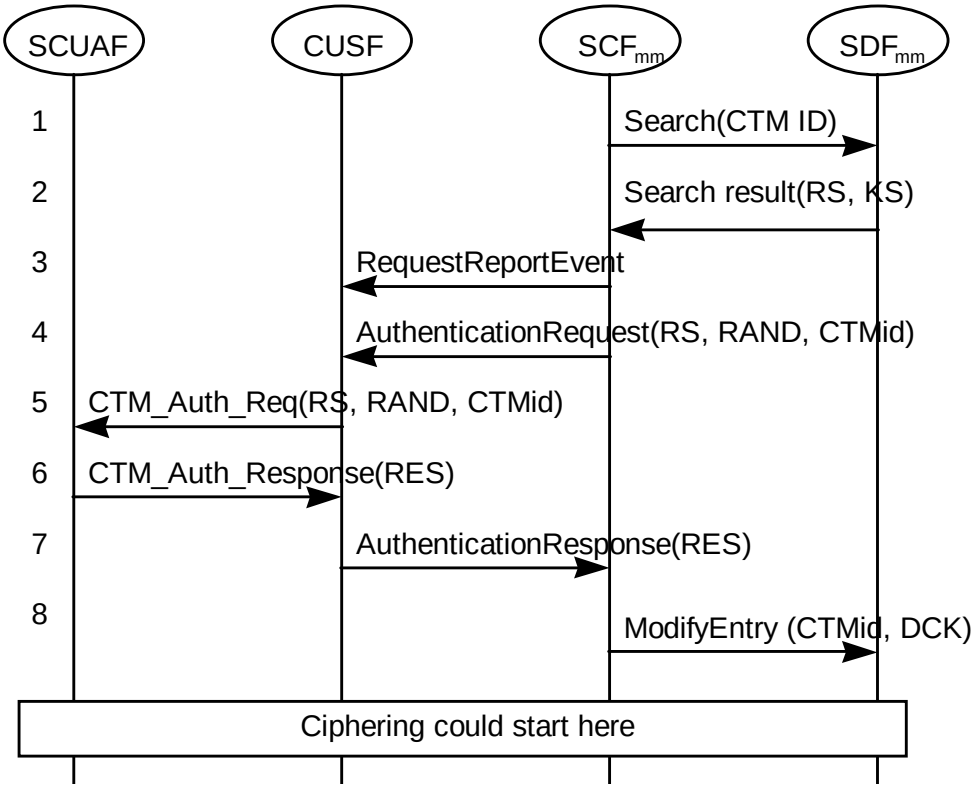


Figure 4: Terminal authentication procedure - case 1

1, 2 SCFmm retrieves from SDFmm the authentication parameters (RS and KS) associated to the CTMid.

3 SCFmm requests to report event, in order to receive back the authentication response from the PT.

4 SCFmm generates a RANDom number issued by the network (RAND) and sends the CTMid, RAND and Rs to CUSF, through a Authentication Request IF.

5 RAND and Rs are relayed to PT via SCUAF.

6 The PT response to the Authentication Request causes SCUAF to send the answer to CUSF through a call unrelated DSS1 message containing the result of authentication (i.e. RES).

7 CUSF sends to SCFmm a Authentication Response IF containing the result of authentication. SCFmm compares the actual response with the expected response, to determine if authentication has succeeded.

8 If ciphering on the air interface is performed and the RESponse calculated by a PT (RES) value provided by the Portable Terminal (PT) is correct then upload Derived Chipper Key (DCK) to the SDFmm.

6.1.1.2.2 Terminal authentication - case 2: DECT triples (RAND, Rs, RES) or CT-2 couples (RAND,RES) previously stored in SDFmm

This case is applicable both with DECT and with CT-2.

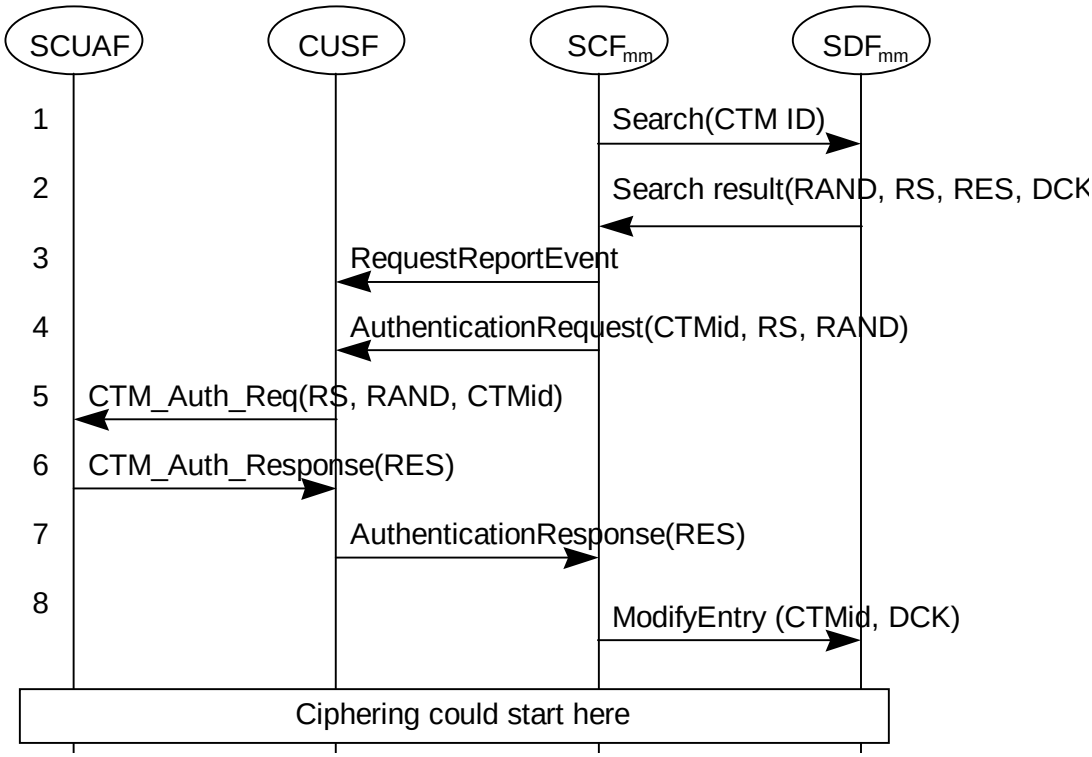


Figure 5: Terminal authentication procedure - case 2

1, 2 SCFmm retrieves from SDFmm the authentication parameters associated to the CTMid. In case of DECT as radio access system, the authentication parameters are composed by RAND, Rs and RES. In case of CT-2 the authentication parameters are composed by RAND and RES. In addition, the Derived Cipher Key (DCK) is retrieved.

3 SCFmm requests to report event, in order to receive back the Authentication Response from the P.

4 In DECT case SCFmm sends the CTM id, RAND and Rs to CUSF. In CT-2 case it sends the CTMid and RAND.

5 The challenge is relayed to PT via SCUAF.

6 The PT response to the authentication request causes SCUAF to send the answer to CUSF through a call unrelated DSS1 message containing the result of authentication (i.e. RES).

7 CUSF sends to SCFmm a Authentication Response message containing the result of authentication. SCFmm compares the actual response with the expected response to determine if authentication has succeeded.

8 If ciphering on the air-interface is performed and the RES value provided by the PT is correct then upload DCK to the SDFmm.

6.1.1.2 Downloading of Authentication Data procedure/IFs

The SCFmm downloads authentication data from the SCFsl/SDFsl into the SDFmm in order to be able to perform terminal authentication.

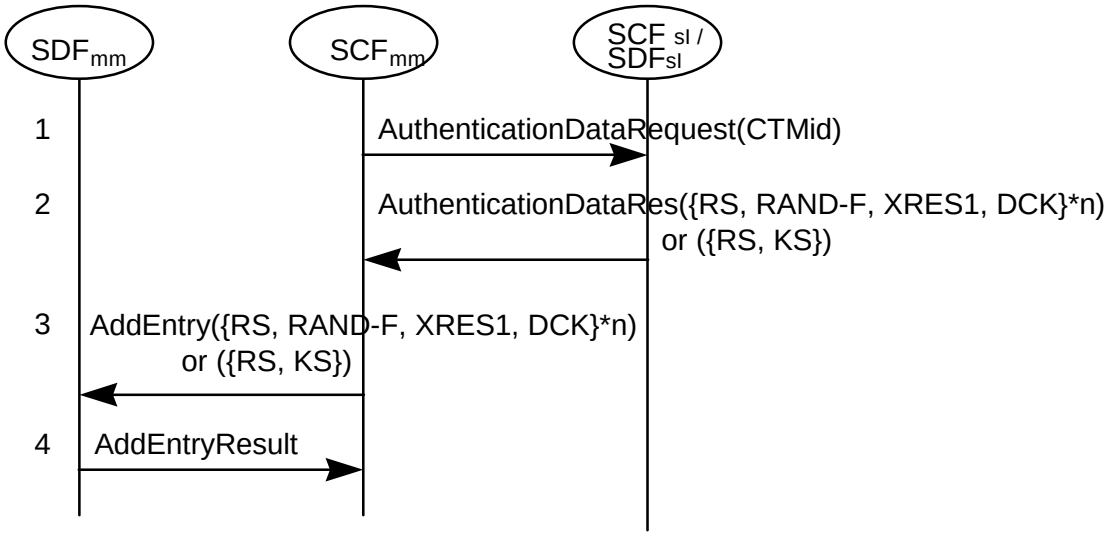


Figure 6: Downloading of authentication Data procedure

1, 2 The SCFmm requests authentication data. In case of DECT, one set of data consists either of a quadruplet (RS, RAND-F, XRES1, DCK) or of a couple (Rs, Ks). In case of CT-2, one set of data consists of a couple (XRES and RAND).

3,4 The SCFmm loads the SDFmm with the received data.

6.1.1.3 Ciphering procedure/IF

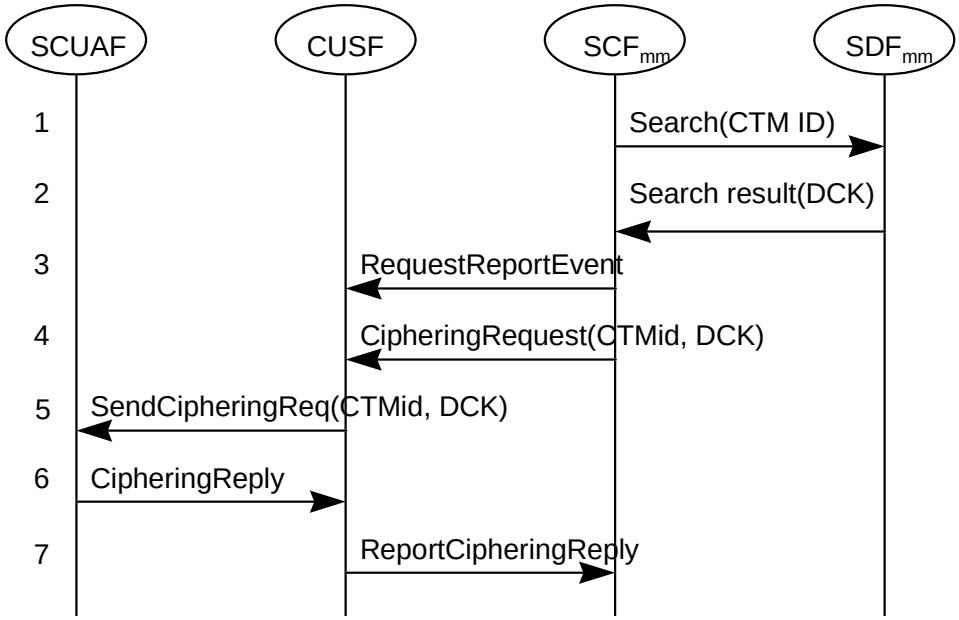


Figure 7: Ciphering procedure

1, 2 The Derived Cipher Key (DCK) obtained during the last successful authentication is retrieved from SDFmm.

3,4,5 SCFmm sends a ciphering request to the PT via the CUSF and SCUAF. The DCK is sent by the SCFmm to the SCUAF via CUSF.

6,7 SCUAF reports the result back to SCFmm via CUSF.

6.1.2 Location registration procedures/IFs

6.1.2.1 Location registration procedures and data deletion

The location registration procedure is used whenever the PT roams in a new Location Area (LA) or when it registers without a previous registration. Several cases are distinguished based on the availability and/or validity of the data stored in the SDFmm.

When the SCUAF sends a non call associated message to the CUSF, the CUSF shall be able to trigger to SCFmm the mobility non call associated request. The SCFmm checks if the PT has been registered before in the SDFmm.

The following cases are possible:

- Case 1: the PT is correctly registered in the SDFmm (see figure 8);
- Case 2: the PT is not yet registered in the SDFmm or the stored data are not valid; depending on the relationship used between SCFmm and service logic (sl) functionalities two scenarios are possible:

  case 2a: use of SCFmm-SDFsl relationship (see figure 9);

– case 2b: use of SCFmm-SCFsl relationship (see figure 10).

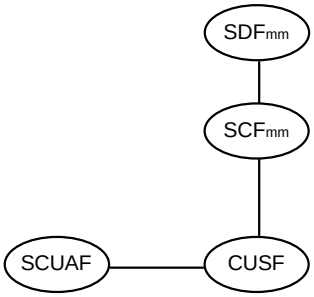


Figure 8: Location registration case 1 (terminal registered in SDFmm): **end to end functional model**

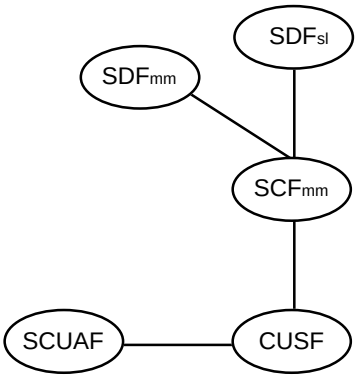


Figure 9: Location registration case 2a (terminal not yet registered in SDFmm; use of SCFmm-SDFsl): end to end functional model

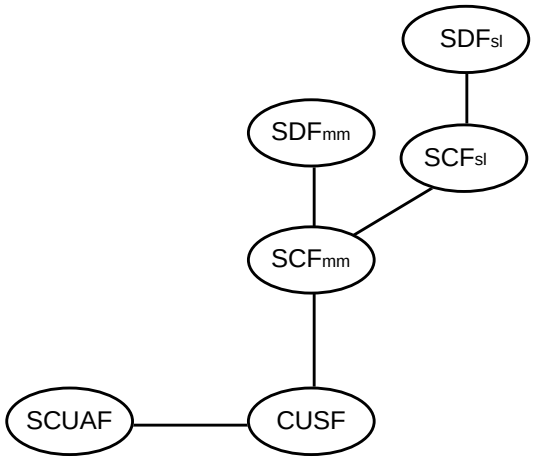


Figure 10: Location registration case 2b (terminal not yet registered in SDFmm; use of SCFmm-SCFsl): end to end functional model

NOTE 1: The use of temporary identities (i.e. TPUI) for registration and paging request is allowed, but it only affects SCUAF.

NOTE 2: One SCFmm can control multiple CUSF. Moreover different SCUAFs can be attached to the same CUSFs.

NOTE 3: For CTM phase 1 a location area is assumed not greater than the coverage area of one FT.

Case 1

If the PT is correctly registered, the SCFmm updates the SDFmm with the FT address. The optional cancellation of data in the old location is a separate procedure.

The location request is acknowledged to the CUSF, which returns the result to SCUAF.

Case 2

When the PT is not registered in SDF_{mm} or the store data are not valid, SCF_{mmnew} stores the FT address and the CTMid in SDF_{mm} SCF_{mm} update location information in SDFsl using SCFmm-SDFsl relationship (case 2a) or SCF_{mm}-SCF_{sl} relationship (case 2b); data deletion procedure can start then (see separate procedure). Prior to updating the location information in SDF_{sl}, $SCF_{mm(new)}$ may download authentication data from SDF_{sl}, perform authentication and ciphering.

6.1.2.2 Location registration IFs

NOTE 1: If chosen by the operator, authentication parameters can be retrieved by SCFmm from SDFsl and stored in SDFmm at any point in time as described in subclause 6.1.1.2.

Case 1

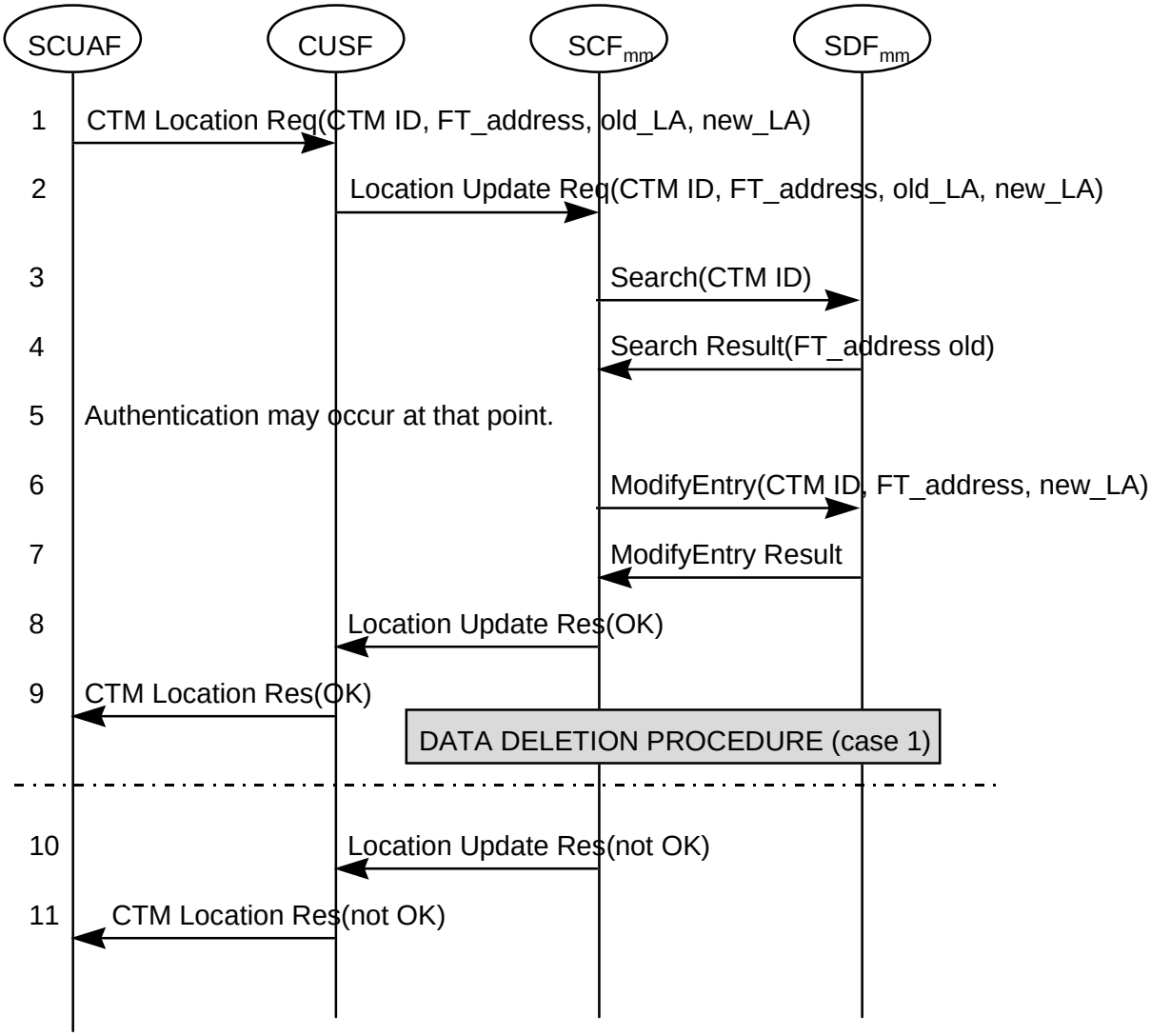


Figure 11: Location registration procedure - case 1 (terminal already registered in SDFmm)

NOTE 2: Data deletion in the same mm area may start in parallel with data modification.

1 SCUAF detects the location registration message and sends a (call unrelated) message to the CUSF including the CTMid of the PT and the FT address.

2 On recognition of a CTM request CUSF sends a call unrelated Location Update Request message to the SCFmm, including the CTMid of the PT and the FT address.

3,4 SCFmm checks if the PT is correctly registered in SDFmm in a Search request including CTMid. On figure 11 the PT is correctly registered and the old FT address is returned in the Search operation.

5 Authentication may occur at this stage. If authentication takes place and it is unsuccessful, go to 10. Data deletion procedure may also start at this stage and can be performed in parallel with data modification.

6,7 SCFmm stores the CTMid and the FT address in SDFmm with an Modify Entry message.

8,9 SCFmm sends back the location registration confirmation to SCUAF via CUSF. At the same time Data Deletion procedure may start.

In case authentication fails:

10,11 SCFmm sends back the location registration negative result to SCUAF via CUSF.

Case 2a

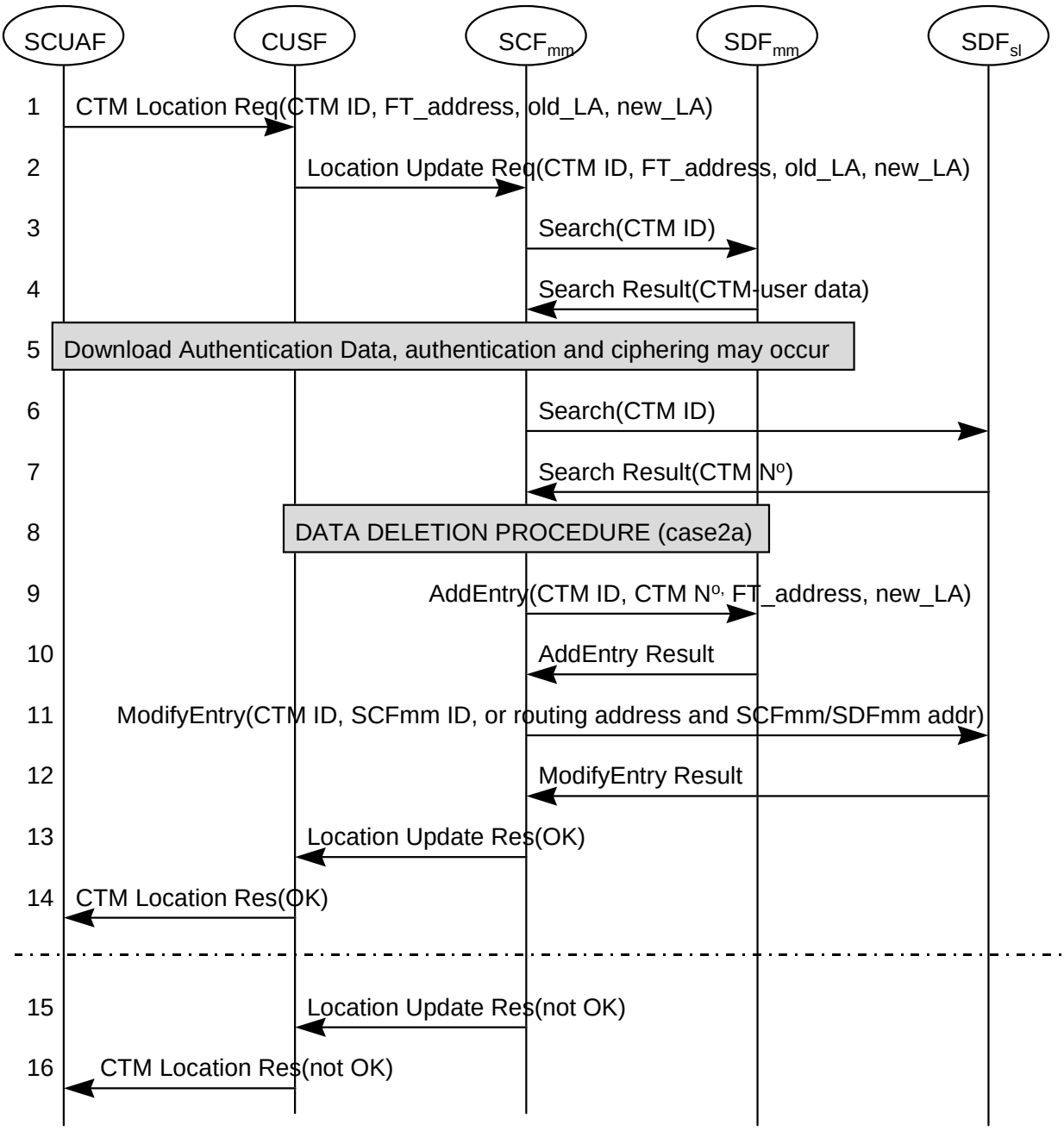


Figure 12: Location registration procedure - case 2a (terminal not registered in SDFmm use of SCFmm-SDFsl).

NOTE 3: Data deletion in the old mm area may start in parallel with data modification in the visited mm area.

1 SCUAF detects the location registration message and sends a (call unrelated) message to the CUSF including the CTMid of the PT and the FT address.

2 On recognition of a CTM request CUSF sends a call unrelated Location Update Request message to the SCFmm, including the CTMid of the PT and the FT address.

3,4 SCFmm requests SDFmm to return data about the CTM user. If the CTM user is not registered in SDFmm, SDFmm informs SCFmm about "CTM user not registered".

5 SCFmm may at this stage perform the download of authentication data followed by terminal authentication and ciphering (see separate procedure). If authentication takes place and it is unsuccessful, go to 15.

6,7 Based on the data returned from SCFmm, SCFmm will ask to the SDFsl with a Search request whether the CTM ID is registered with the network. If not then continue in line 15. In positive case the CTM N° is returned in order to be stored in SDFmm.

8 Data deletion procedure may start at this stage and can be performed in parallel with data modification.

9,10 SCFmm stores the CTMid, the CTM N°, the FT address and the new LA in SDFmm with an Add Entry message. (note that a ModifyEntry message may also be used).

11,12 SCFmm updates location registration data in SDFsl. It inserts the new SCFmm ID, if roaming number method will apply for incoming call. The routing address and SCFmm/SDFmm address are stored instead of the SCFmm ID when routing number method is used.

13,14 SCFmm sends back the location registration confirmation to SCUAF via CUSF.

In case authentication fails:

15,16 SCFmm sends back the location registration negative result to SCUAF via CUSF.

Case 2b

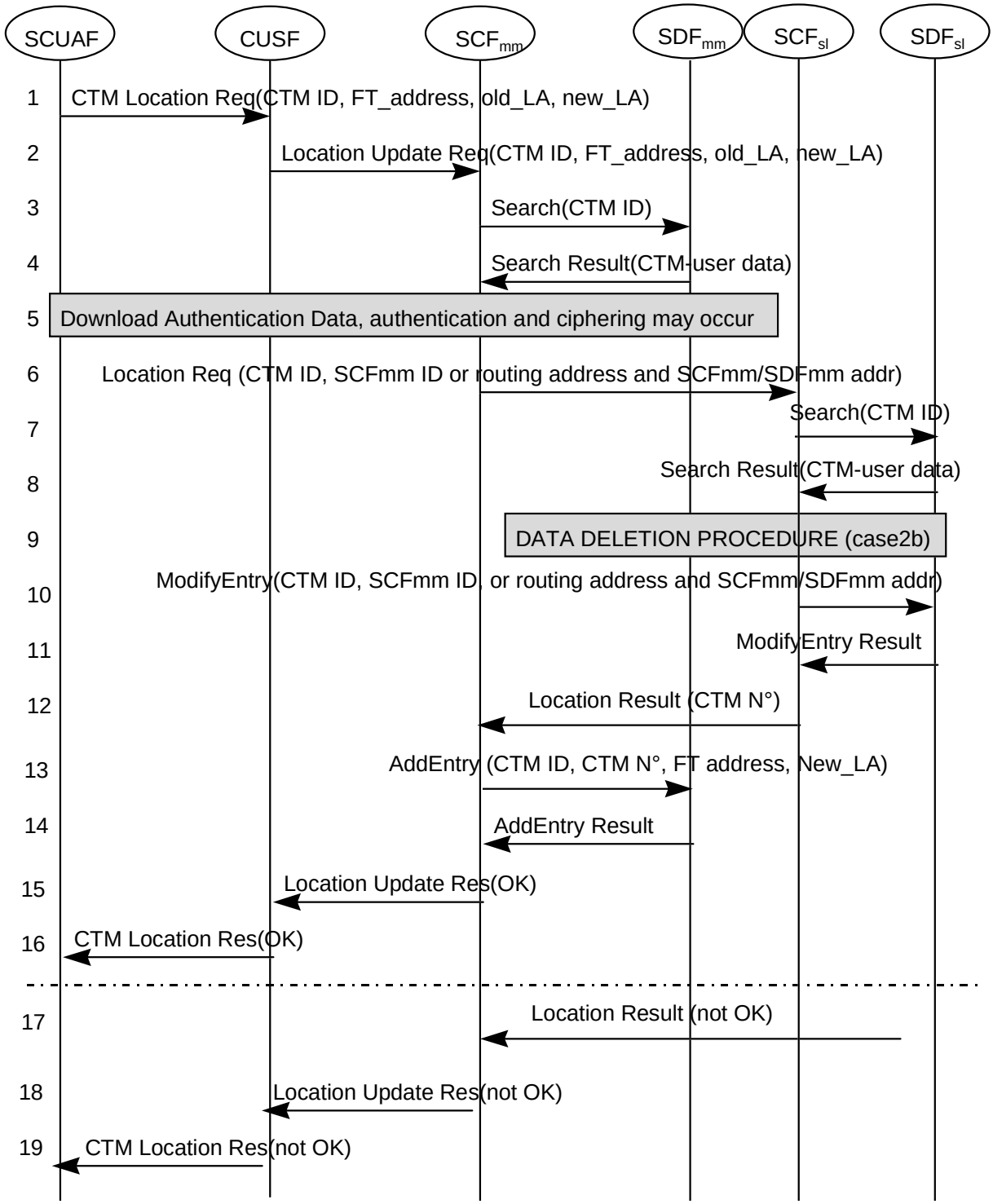


Figure 13: Location registration procedure - case 2b (terminal not registered in SDFmm use of SCFmm-SCFsl).

NOTE 4: Data deletion in the old mm area may start in parallel with data modification in the visited mm area.

1 SCUAF detects the location registration message and sends a (call unrelated) message to the CUSF including the CTMid of the PT and the FT address.

2 On recognition of a CTM request CUSF sends a call unrelated Update Location Request message to the SCFmm, including the CTMid of the PT and the FT address.

3,4 SCFmm requests SDFmm to return data about the CTM user. If the CTM user is not registered in SDFmm, SDFmm informs SCFmm about "CTM user not registered".

5 SCFmm may at this stage perform the download of authentication data followed by terminal authentication and ciphering (see separate procedure). If authentication takes place and it is unsuccessful, go to 18.

6 Based on the data returned from SCFmm, SCFmm will inform SCFsl that the CTM user is roaming in SCFmm domain.

7,8 SCFsl asks to the SDFsl with a Search request whether the CTM ID is registered with the network. If not then continue in line 17. In positive case the CTM user data are returned, in particular the CTM Number is returned in order to be sent back to SCFmm.

9 Data deletion procedure may start at this stage and can be performed in parallel with data modification.

10,11 If the CTM user is allowed to roam in the domain controlled by SCFmm, SCFsl updates location registration data in SDFsl. It inserts the new SCFmm ID, if roaming number method will apply for incoming call. The routing address and SCFmm/SDFmm address are stored instead of the SCFmm ID when routing number method is used.

12 SCFsl informs SCFmm that the location registration is accepted.

13,14 SCFmm stores the CTM N°, the FT address and the new Location Area in SDFmm with an Add Entry message (note that a ModifyEntry message may also be used).

15,16 SCFmm sends back the location registration confirmation to SCUAF via CUSF.

In case the user is not allowed to roam in the SCFmm domain:

17 SCFsl sends back a location registration negative result to SCFmm, the flows continue as in line 18.

If authentication fails:

18,19 SCFmm sends back the location registration negative result to SCUAF via CUSF.

6.1.3 Data deletion procedure

Case 1

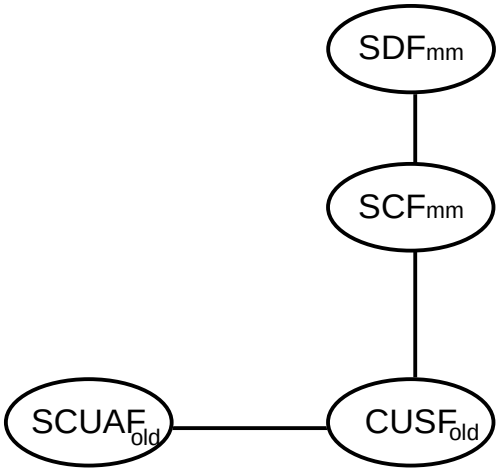


Figure 14: Data deletion procedure - case 1 - end to end functional model

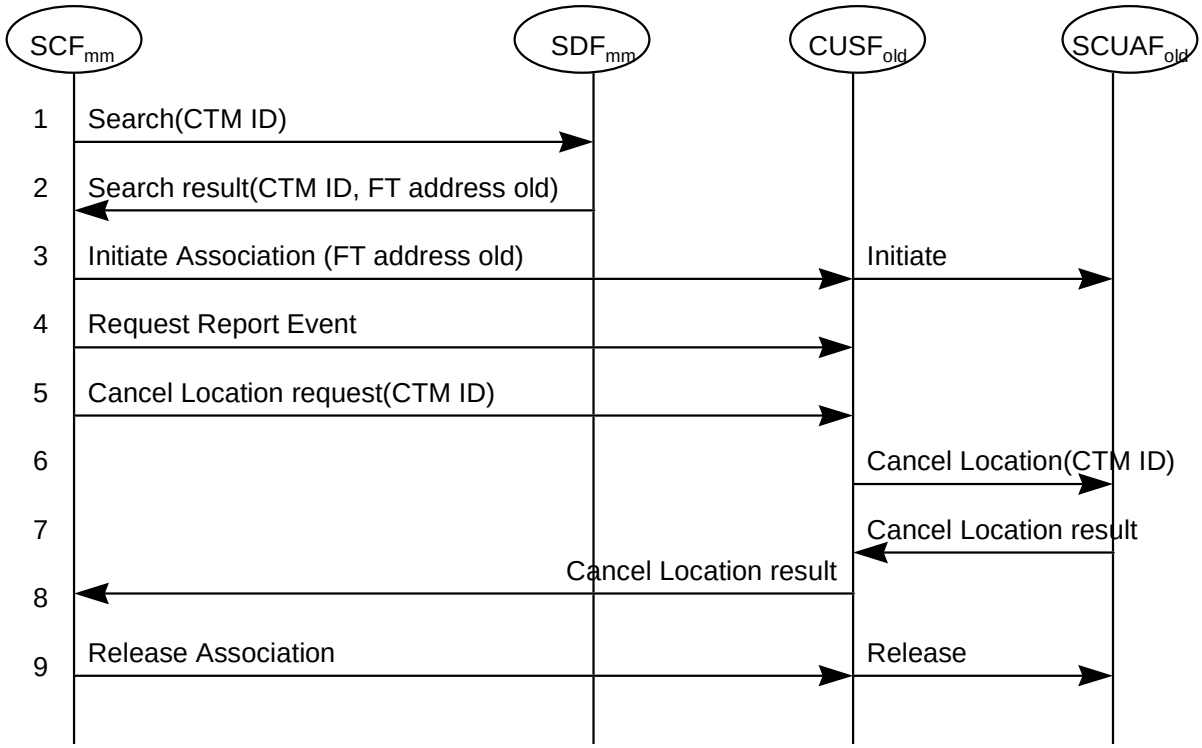


Figure 15: Data deletion procedure - case 1

1,2 SCFmm retrieves from SDFmm the address of old FT.

3 SCFmm initiate a new call unrelated dialogue towards SCUAFold via CUSFold.

4,5,6 SCFmm requests to cancel terminal data from old SCUAF by sending a Cancel Location Message containing the CTMid through the old CUSF. The SCFmm request also a confirmation of the cancel location.

7,8 After the cancellation the SCUAFold sends the confirmation to the SCFmm.

9 The SCFmm release the association.

NOTE 5: Timers or resource management may be used to delete location information in the FT, if needed (operator's choice).

Case 2a (SCFmm controlled)

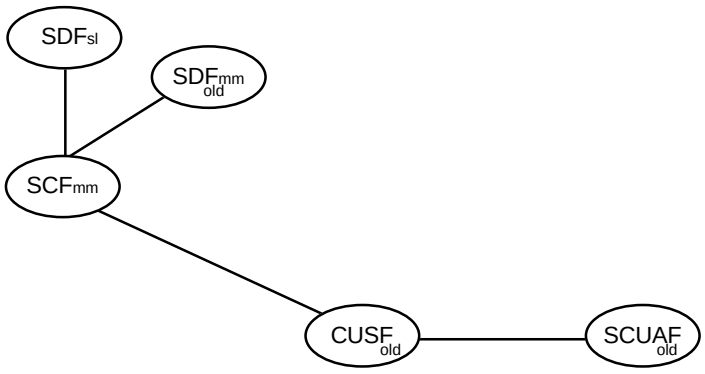


Figure 16: Data deletion procedure - case 2a - end to end functional model

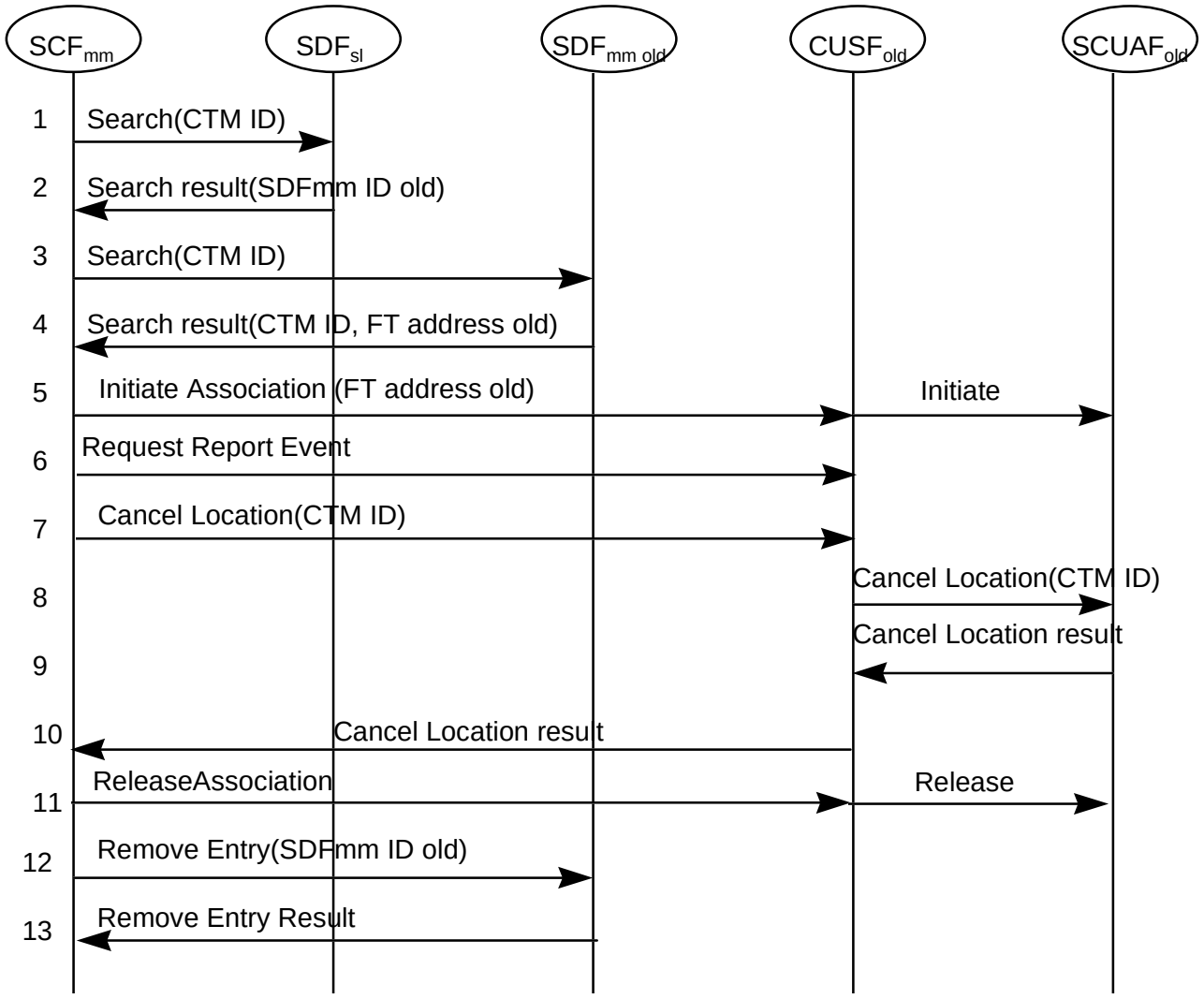


Figure 17: Data deletion procedure - case 2a

1,2 SCFmm retrieves from SDFsl the address of SDFmm old.

3,4 SCFmm retrieves from old SDFmm the address of old FT.

5 SCFmm initiate a new call unrelated dialogue towards SCUAFold via CUSFold.

6,7,8 SCFmm requests to cancel terminal data from old SCUAF by sending a Cancel Location Message containing the CTMid through the old CUSF. The SCFmm request also a confirmation of the cancel location.

9,10 After the cancellation the SCUAFold sends the confirmation to the SCFmm.

11 SCFmm release the association towards SCFAFold.

12,13 SCFmm removes from SDFmm old all the data associated to the CTMid.

NOTE 1: Timers or resource management may be used to delete location information in the FT, if needed (operator's choice).

Case 2b (SCFsl controlled):

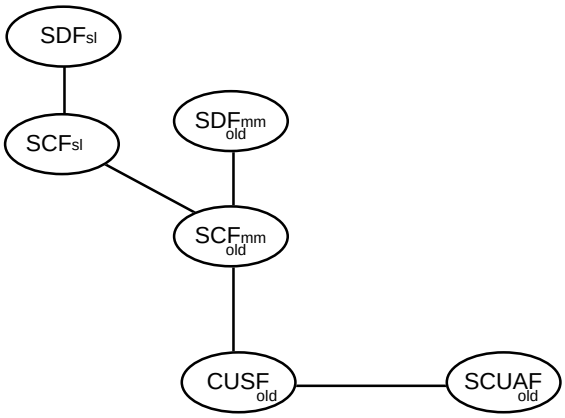


Figure 18: Data deletion procedure - case 2b - end to end functional model

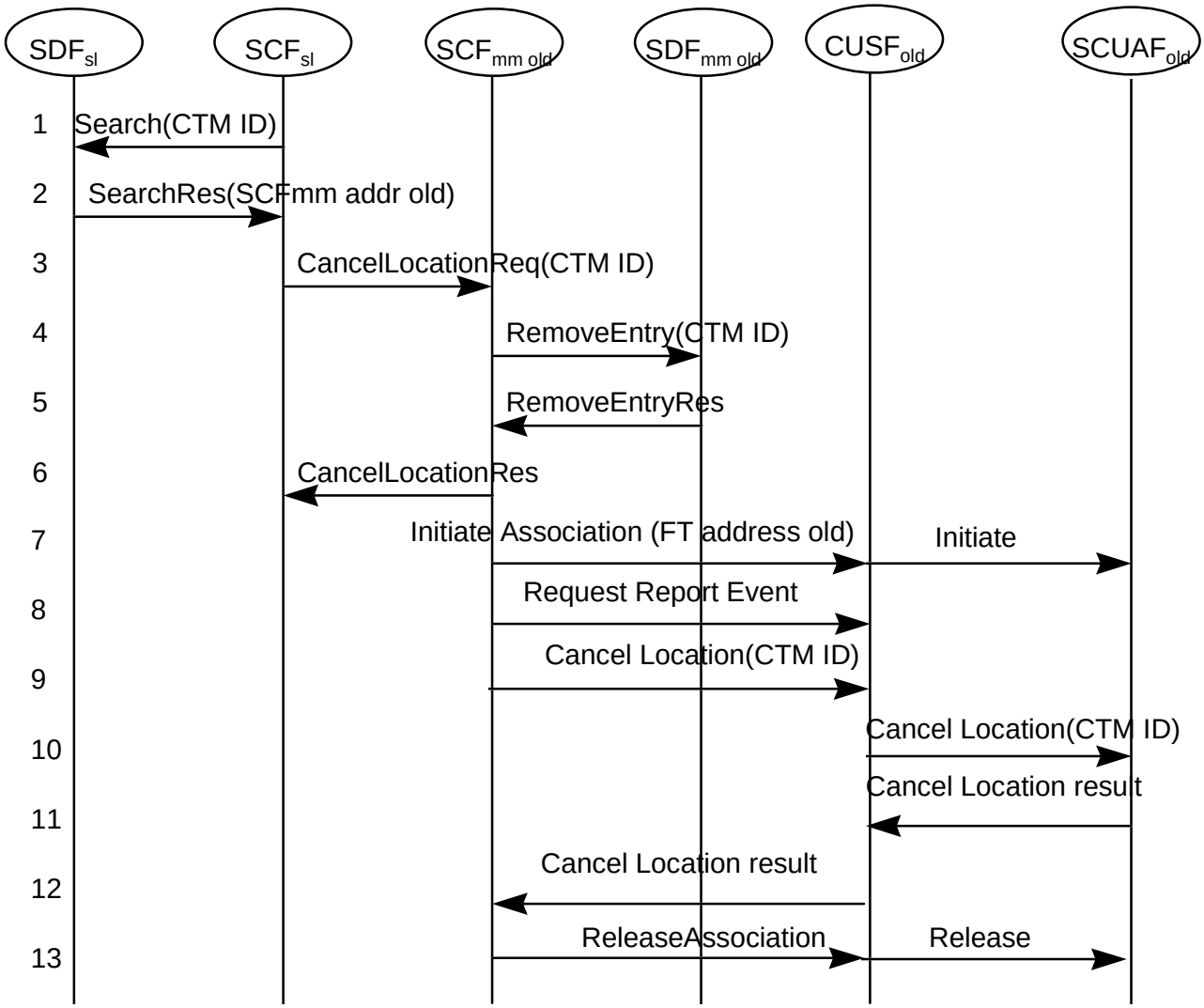


Figure 19: Data deletion procedure - case 2b

1,2 SCFsl retrieves from SDFsl the address of SCFmm old.

3 SCFsl requests from SCFmm old to cancel the location information of the CTM user.

4,5,6 SCFmm old removes the entry from the SDFmm old, and reports the result back to SCFsl.

7 SCFmm old initiate a new call unrelated dialogue towards SCUAFold via CUSFold.

8,9,10 SCFmm old requests to cancel terminal data from old SCUAF by sending a Cancel Location Message containing the CTMid through the old CUSF. The SCFmm request also a confirmation of the cancel location.

11,12 After the cancellation the SCUAFold sends the confirmation to the SCFmm old.

13 SCFmm old release the association.

NOTE 2: Timers or resource management may be used to delete location information in the FT, if needed (operator's choice).

6.1.4 Network Authentication Procedure/IFs

The network authentication included in GAP may be invoked by the terminal in relation with a Subscription Registration/Deregistration procedure therefore the information flows for this procedure are included in the following subclauses 6.1.5 and 6.1.6.

6.1.5 Subscription Registration Procedure/IFs

6.1.5.1 Subscription Registration Procedure

The subscription registration procedure is used to load the PT over the air with certain identities, and to make the PT known to the network. The PT can use the data to gain access to the network and to make calls, and to recognize the system to receive calls. The network can use the information to validate service requests from the PT, and to route calls to valid PTs.

The location where the PT can perform the procedure may be restricted to certain location areas. A PT can start the procedure only if bit A44 is "on" among the data broadcasting by the FT. Since the activation/deactivation of this bit is a FT management procedure it's description is out of the scope of this document. For security and performance reasons, the time when a given user can perform subscription registration may be restricted.

NOTE: The IPUI-N stored in the terminal in case of DECT is provided by the manufacturer, not by the operator.

The procedure applies only to the intra-network case.

Case 1: Based on SCFmm-SCFsl relationship

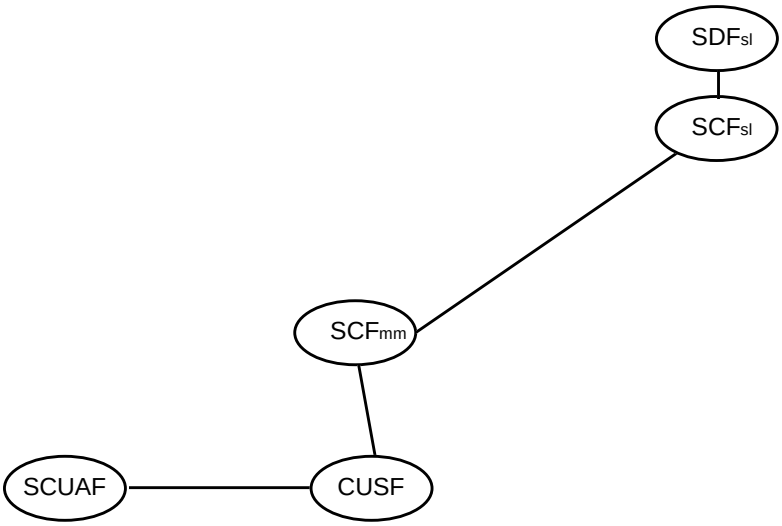


Figure 20: Subscription registration: end to end functional model (Case 1: SCFmm-SCFsl rel.)

When the SCUAF sends a call unrelated message to the CUSF, the CUSF triggers a call unrelated request to the SCFmm. The SCFmm then requests authentication parameters from the SCFsl. A default SCFsl is chosen since no information has been received from the SCUAF that identifies the PT. The SCFsl retrieves authentication parameters from the SDFsl and sends the parameters to the SCFmm, which forwards them to the PT via CUSF and SCUAF. The PT response, which includes a request for network authentication, is relayed back to the SCFmm. The SCFmm sends the PT response and the network authentication request to the SCFsl.

The response from the PT is used to identify the subscriber. Since the authentication parameters cannot be calculated from the response, the network shall calculate a list with all responses together with the corresponding CTM IDs, store it in the SDFsl, and then use the received response to lookup the CTM subscriber record in the list. However, the response may be in some rare cases ambiguous, i.e., two different sets of authentication parameters may result in the same response. If this is the case then the network has to calculate a new challenge using different authentication parameters.

After the subscriber record could unambiguously be found, the SCFsl calculates the response to the network authentication request and sends it together with the identities to the SCFmm. The SCFmm forwards the network response to the PT via the CUSF and SCUAF. At that stage, a call unrelated terminal authentication may be performed. Finally, the SCFmm forwards the requested identities to the PT.

For security reasons the RAND-F, RS pair used for subscription registration should be changed from time to time. The changing of security parameters should, however, not affect ongoing registration procedures.

Case 2: Based on SCFmm-SDFsl relationship

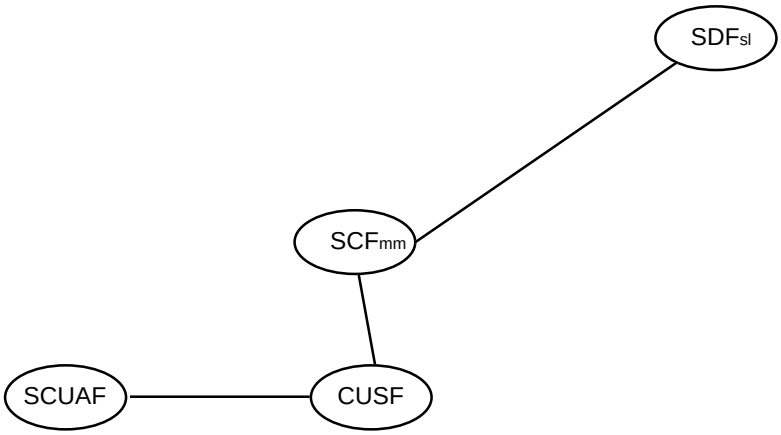


Figure 21: Subscription registration: end to end functional model (Case 2: SCFmm-SDFsl rel.)

When the SCUAF sends a call unrelated message to the CUSF, the CUSF triggers a call unrelated request to the SCFmm. The SCFmm then requests authentication parameters from the SDFsl. A default SDFsl is chosen since no information has been received from the SCUAF that identifies the PT. The SDFsl sends the parameters to the SCFmm, which forwards them to the PT via CUSF and SCUAF. The PT response, which includes a request for network authentication, is relayed back to the SCFmm. The SCFmm then asks the SDFsl to search for the subscriber record.

The response from the PT is used to identify the subscriber. Since the authentication parameters cannot be calculated from the response, the network shall calculate a list with all responses together with the corresponding CTM IDs, store it in the SDFsl, and then use the received response to lookup the CTM subscriber record in the list. However, the response may be in some rare cases ambiguous, i.e., two different sets of authentication parameters may result in the same response. If this is the case then the network has to calculate a new challenge using different authentication parameters.

After the subscriber record could unambiguously be found, the CTM ID, the Portable Access Rights Key (PARK) and the KS' is sent to the SCFmm. The SCFmm calculates the response to the network authentication request. The SCFmm sends the network response to the PT via the CUSF and SCUAF. At that stage, a call unrelated terminal authentication may be performed. Finally, the SCFmm forwards the requested identities to the PT.

For security reasons the RAND-F, RS pair used for subscription registration should be changed from time to time. The changing of security parameters should, however, not affect ongoing registration procedures.

6.1.5.2 Subscription Registration IFs

Case 1: Based on SCFmm-SCFsl relationship

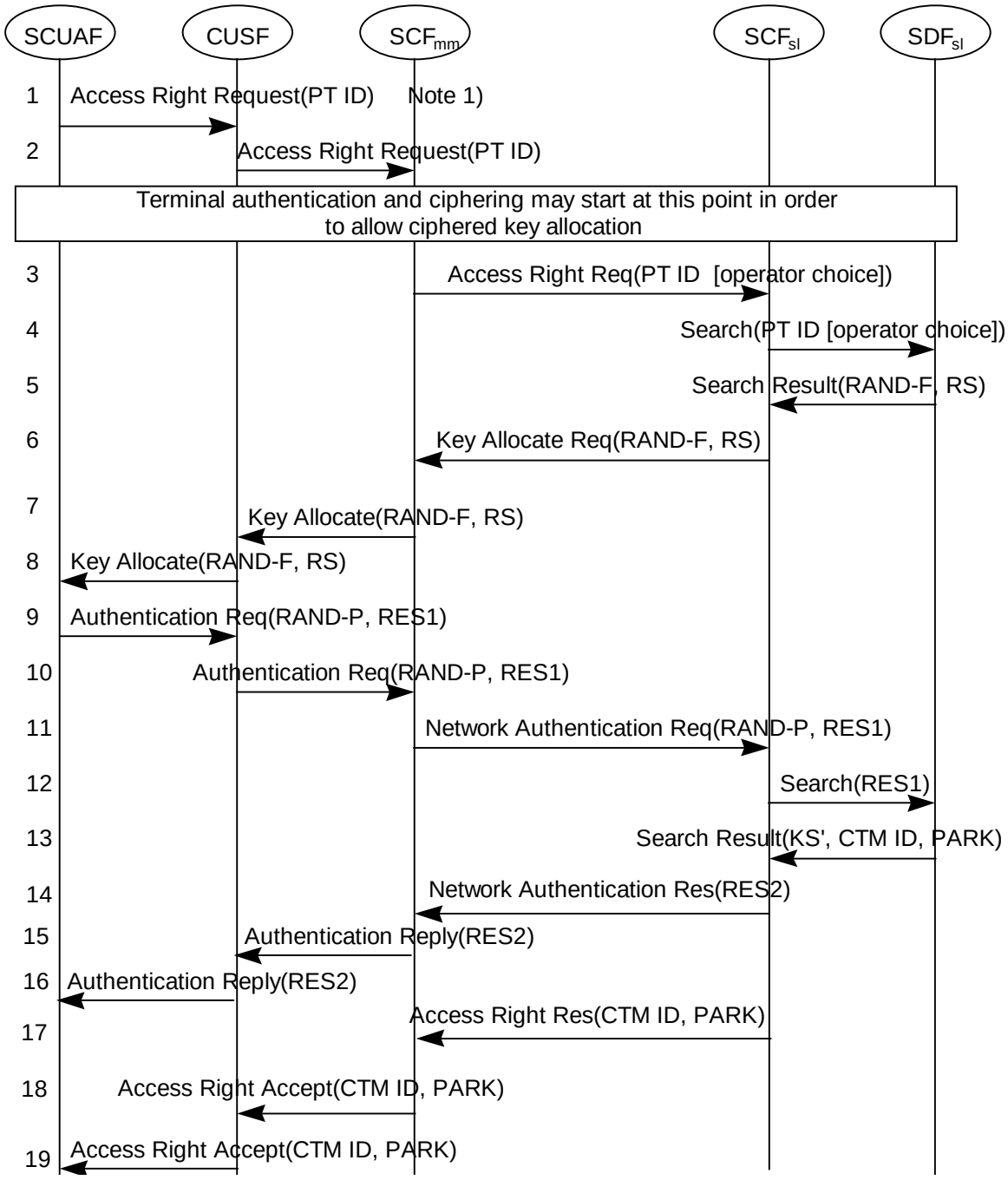


Figure 22: Subscription Registration procedure (Case 1: SCFmm-SCFsl relationship)

1 The SCUAF detects a request for access rights and sends a message to the CUSF. The message contains a portable ID.

NOTE 1: The portable ID is a default IPUI (IPUI-N) if no CTM ID is stored in the portable, otherwise it is the CTM ID. See DECT specifications for details.

2 The CUSF forwards the request to the SCFmm.

NOTE 2: Authentication and ciphering may be initiated by SCFmm at this point. The option to have these procedure initiated by SCFsl (between flows 5 and 6) is an operator choice.

3 The SCFmm selects a pre-defined SCFsl to perform access right request.

4,5,6 The SCFsl retrieves a pair RAND-F, RS from the SDFsl and sends it to the SCFmm. The RAND-F, RS pair has been stored before in the SDFsl.

7,8 The SCFmm sends the challenge to the PT via CUSF and SCUAF.

9,10 The response from the PT contains a request for network authentication and a RAND-P. The SCUAF sends the request to the SCFmm.

11 The SCFmm requests network authentication to the SCFsl.

12,13 The SCFsl retrieves the identities (CTM ID, PARK) and the KS' from the SDFsl using the received response RES1 as a search key. The SDFsl has a table with all expected responses that could be calculated from the given RAND-F, RS pair. For performance reasons, this table can be calculated in advance and be used for every subscription registration during a certain time period. In this case, the RAND-F, RS pair would be identical for all registrations performed in that time window. The SDFsl returns all records that match the search key. If the RES1 is ambiguous (i.e., more than one record is returned) then the SCFsl generates a new RAND-F, which may be used only for the ongoing subscription registration. The SCFsl calculates the expected responses for the ambiguous sets with the new RAND-F. If there is still an ambiguity then the SCFsl will generate new RAND-Fs till any ambiguity is removed. The IF continues at line 6.

14 The SCFsl calculates the response RES2 using algorithm A22 and the KS' received from the SDFsl and sends it to the SCFmm.

15,16 The SCFmm sends a reply with the RES2 to the authentication request of the PT via CUSF and SCUAF.

17-19 Before the network accepts the access right request the network may perform a terminal authentication procedure. If it fails then the access right request is rejected. When the SCFsl accepts the access right request then it sends the identities (PARK, CTM ID) to the terminal.

NOTE 3: In case that the RES1 cannot be found by the SDFsl the access right request and the network authentication is rejected.

Case 2: Based on SCFmm-SDFsl relationship

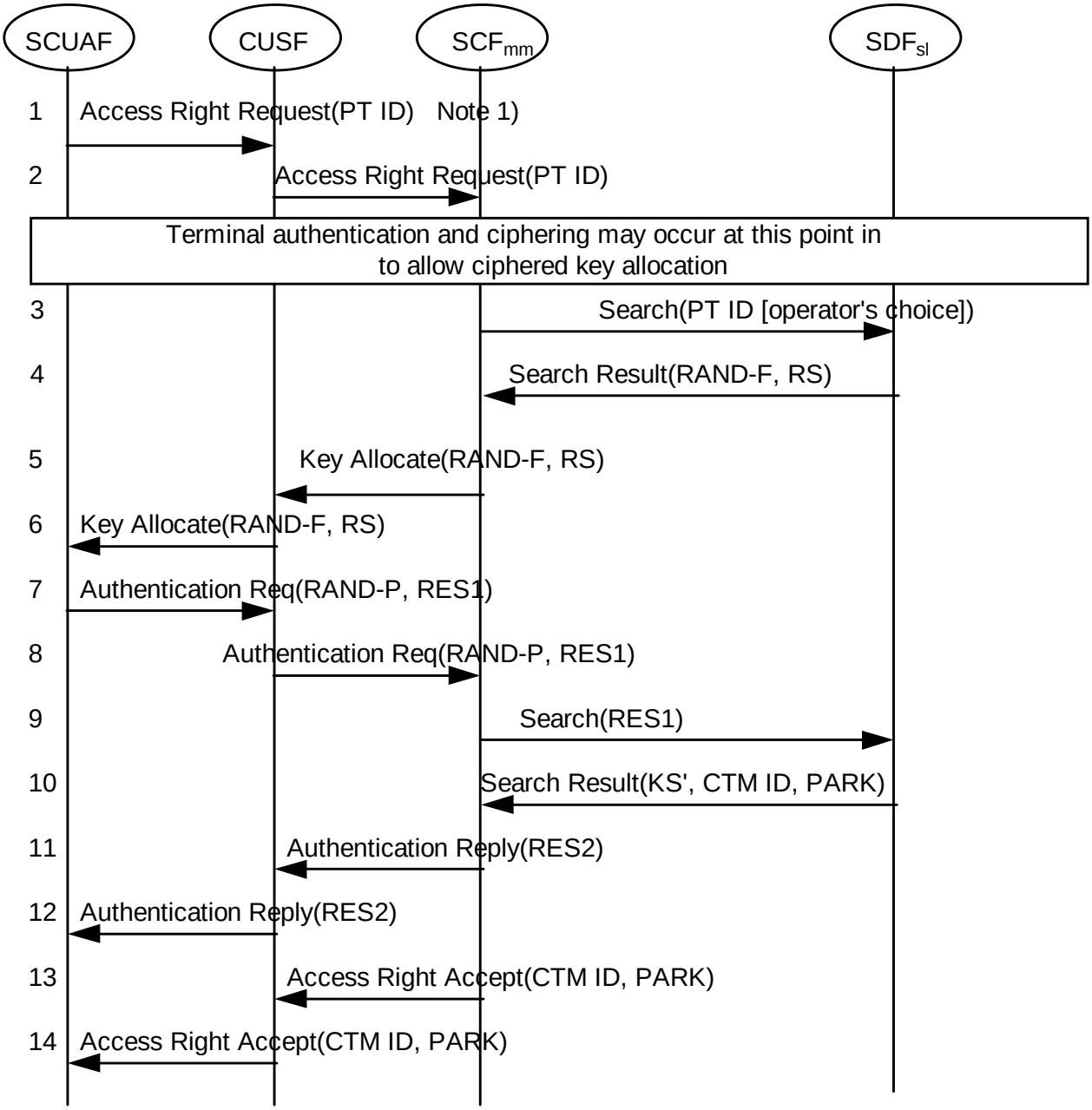


Figure 23: Subscription Registration procedure (Case 2: SCFmm-SDFsl relationship)

1 The SCUAF detects a request for access rights and sends a message to the CUSF. The message contains a portable ID.

NOTE 4: The portable ID is a default IPUI (IPUI-N) if no CTM ID is stored in the portable, otherwise it is the CTM ID. See DECT specifications for details.

2 The CUSF forwards the request to the SCFmm.

3 The SCFmm selects a pre-defined SDFsl to send a search to.

4 The SDFsl retrieves a pair RAND-F, RS and sends it to the SCFmm. The RAND-F, RS pair has been stored before in the SDFsl.

5,6 The SCFmm sends the challenge to the PT via CUSF and SCUAF.

7,8 The response from the PT contains a request for network authentication and a RAND-P. The SCUAF sends the request to the SCFmm.

9 The SCFmm sends a search to the SDFsl using the terminal response RES1 as a search key.

10 The SDFsl retrieves the identities (CTM ID, PARK) and the KS'. The SDFsl has a table with all expected responses XRES1 that could be calculated from the given RAND-F, RS pair. For performance reasons, this table can be calculated in advance and be used for every subscription registration during a certain time period. In this case, the RAND-F, RS pair would be identical for all registrations performed in that time window. The SDFsl returns all records that match the search key. If the RES1 is ambiguous (i.e., more than one record is returned) then the SCFmm generates a new RAND-F, which may be used only for the ongoing subscription registration. The SCFmm calculates the expected responses for the ambiguous sets with the new RAND-F. If there is still an ambiguity then the SCFmm will generate new RAND-Fs till any ambiguity is removed. The IF continues at line 6.

11,12 The SCFmm calculates the response RES2 using algorithm A22 and the KS' received from the SDFsl, and sends a reply with the RES2 to the authentication request of the PT via CUSF and SCUAF.

13,14 Before the network accepts the access right request the network may perform a terminal authentication procedure. If it fails then the access right request is rejected. When the SCFmm accepts the access right request then it sends the identities (PARK, CTM ID) to the terminal.

10-14 In case that the RES1 cannot be found by the SDFsl the access right request and the network authentication is rejected. The SCFsl sends a handling information result to the SCFmm. The SCFmm then sends a authentication reject message to the PT via SCUAF and CUSF. It also sends an access right reject message to the PT via CUSF and SCUAF.

6.1.6 Subscription Deregistration procedure/IFs

6.1.6.1 Subscription Deregistration procedure

The subscription deregistration procedure is used to terminate the access right of a PT, to remove the identities over-the-air from the PT, and to remove all entries from the network databases.

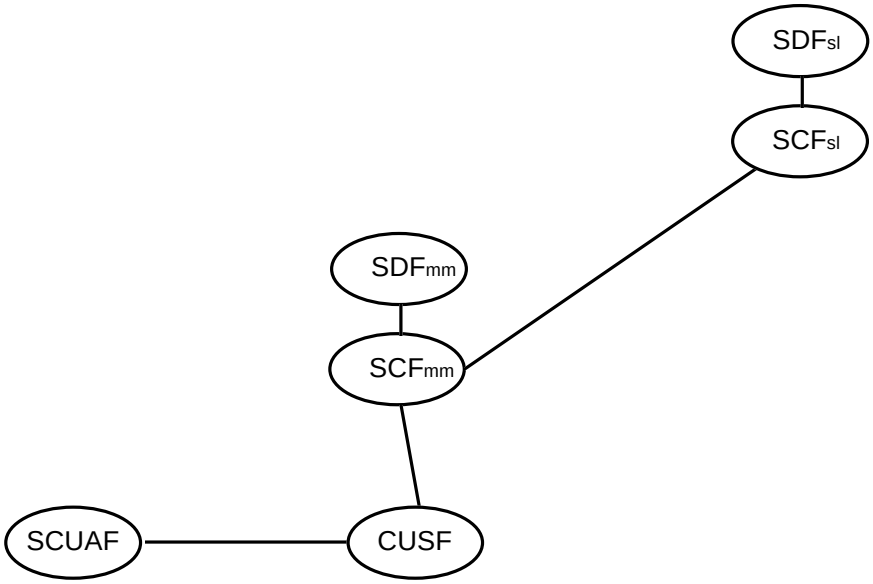


Figure 24: Subscription Deregistration - end to end functional model.

The procedure is initiated by the SCFsl when an indication is found in the service logic during normal CTM procedures. It supplies the SCFmm with the PT identities that are necessary for the over-the-air access right termination procedure. The SCFmm then requests the PT via CUSF and SCUAF to terminate the access right. Before the PT accepts the request it will requests the network to authenticate itself. The SCFmm handles the network authentication requesting the necessary parameters from the SDFmm. After successful authentication the PT accepts the access right terminate request. The SCFmm then removes the subscriber's entry from the SDFmm and informs the SCFsl of the result of the deregistration request. The SCFsl then removes the subscription record from the SDFsl.

6.1.6.2 Subscription Deregistration IFs

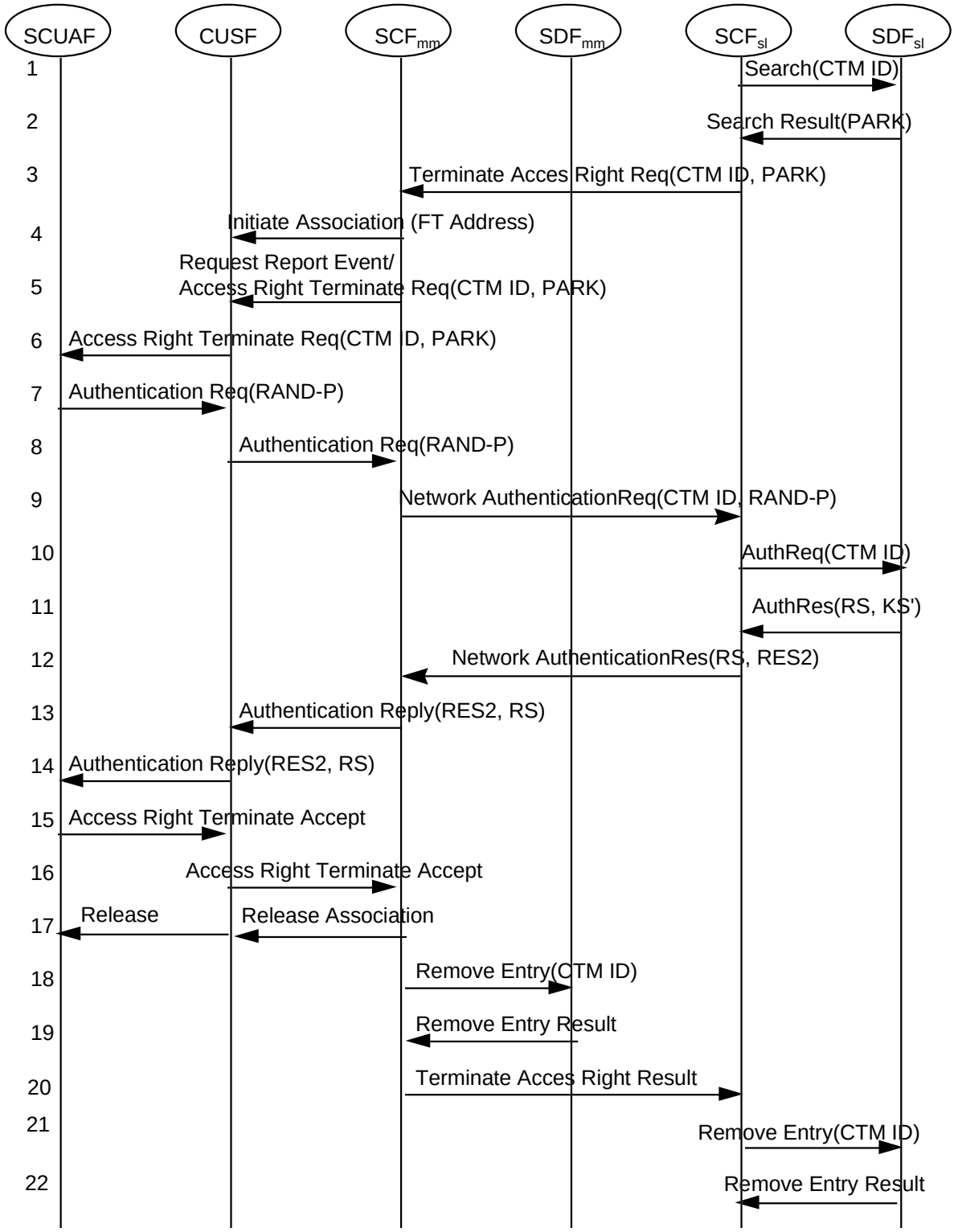


Figure 25: Subscription Deregistration procedure

1,2 The SCFsl retrieves the PARK from the SDFsl.

3 The SCFsl requests to the SCFmm to terminate access right. The message contains the CTM ID and the PARK of the PT.

4,5,6 The SCFmm requests the termination of access right from the PT via CUSF and SCUAF. If the PT is not reachable then the SCFmm removes the subscriber's record from the SDFmm, and will inform the SCFsl with a handling information result. The SCFsl will mark the subscriber in the SDFsl and upon a location registration attempt, the SCFsl starts the subscription deregistration anew.

7,8 The PT requests network authentication. A message containing a random number RAND-P is sent to the SCFmm via SCUAF and CUSF.

9 The SCFmm requests from the SCFsl the necessary authentication data (RS, RES) to answer the PT authentication request. It sends the RAND-P to the SCFsl.

10,11,12 The SCFsl retrieves from SDFsl the RS and KS' and performs the authentication algorithm. It sends the RS and RES2 in a response to the SCFmm.

13,14 The SCFmm sends the response to the PT via CUSF and SCUAF.

15,16 The PT accepts or rejects the access right terminate request. The SCUAF then sends a message to the CUSF, which forwards it to the SCFmm.

17 The SCFmm release the association with the SCUAF.

18,19 The SCFmm removes the subscriber's record from the SDFmm.

20 The SCFmm reports the result of the terminate access right request to the SCFsl.

21,22 The SCFsl removes the subscription record from the SDFsl.

6.1.7 Subscription Registration and Deregistration via O&M

The network operator can perform the subscription registration and deregistration via an O&M system. These procedures are not in the scope of the present document and are therefore not described.

6.1.8 Location Registration Suggest Procedure/IFs

6.1.8.1 Location Registration Suggest Procedure

In some cases the SCFmm invokes the procedure and asks the terminal to register.

6.1.8.2 Location Registration Suggest IFs

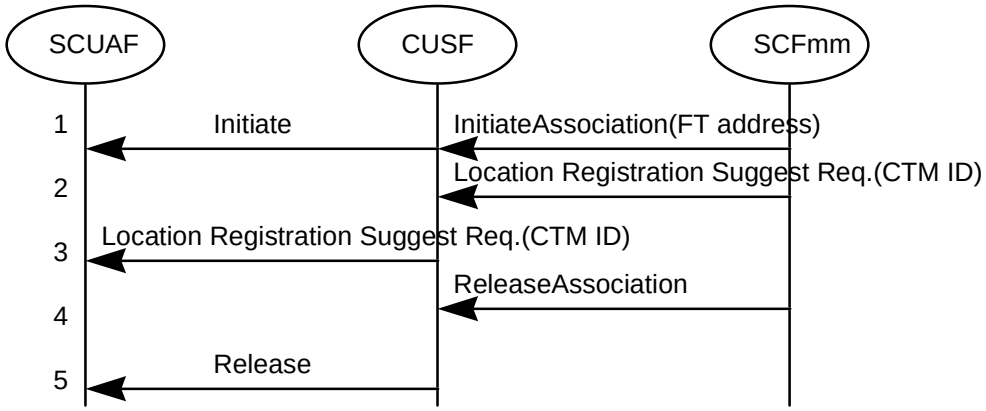


Figure 26: Location registration suggest procedure

1 A new association is created for the FT.

2,3 The SCFmm sends a call unrelated Location Registration Suggest request containing the CTM ID to the terminal via CUSF and SCUAF. The locate suggest message is provided to the terminal without paging if radio link already established, otherwise preceded by paging. If the message is successfully delivered to the terminal, the PT may afterwards initiate a location registration procedure. If the message is not delivered to the terminal, e.g. for paging failure, a location registration suggest error may be returned to the network.

4,5 The association is released by SCFmm.

6.2 Call related procedures/IFs

6.2.1 CTM incoming call procedures/IFs

6.2.1.1 CTM incoming call procedures

For authentication refer to subclause 6.1.1

Case 1: roaming number case

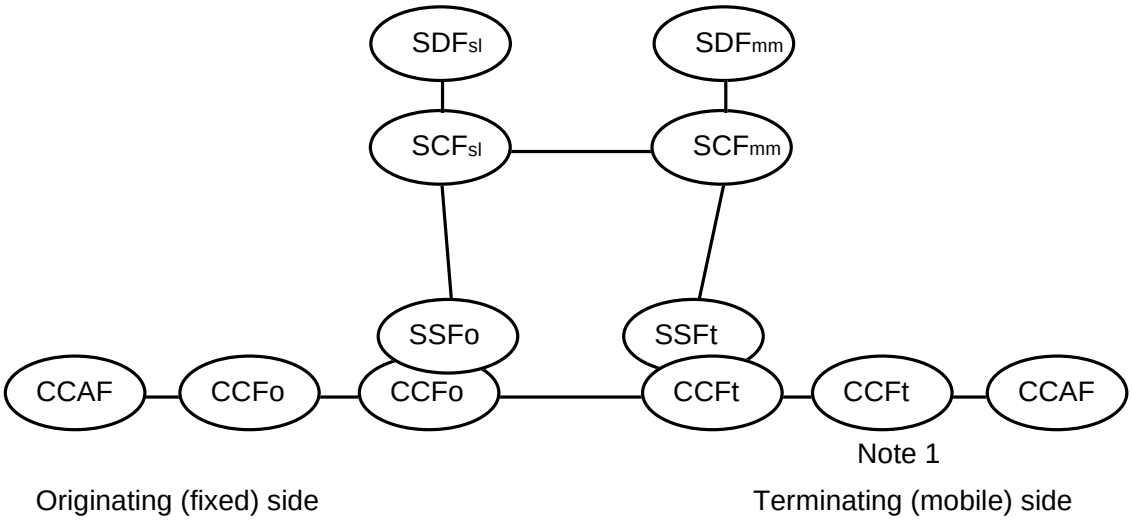


Figure 27: PT terminating call case 1

An originating party dials the directory number of a mobile terminal (CTM number). If the CTM number is a non-geographical IN number then the call will be routed to the nearest SSF of the calling party. If the CTM number is a geographical number then the call will be routed to the SSF nearest to the Local Exchange (LE) that is associated with the CTM user's subscription (home SSF). The SSF will trigger the SCFsl. SCF_{sl} retrieves the address of the visited SCF_{mm} from SDF_{sl}

With the obtained SCF_{mm} address, SCF_{sl} requests SCF_{mm} for a roaming number. SCF_{mm} checks if the subscriber is registered and reachable (in SDF_{mm}), selects a roaming number and returns this to SCF_{sl}. SCF_{sl} instructs originating SSF to route the call with the obtained number (i.e. INAP CONNECT) to the visited CCF/SSF, where the call is triggered. Visited SSF queries SCFmm (one shot rule) in order to get the FT address and the CTM identity. SCFmm releases the roaming number. and asks visited CCF/SSF to route the call toward the identified CCAF. CCAF pages the PT.

NOTE 1: This CCF can be optionally present, depending on the network topology.

Case 2: routing number case

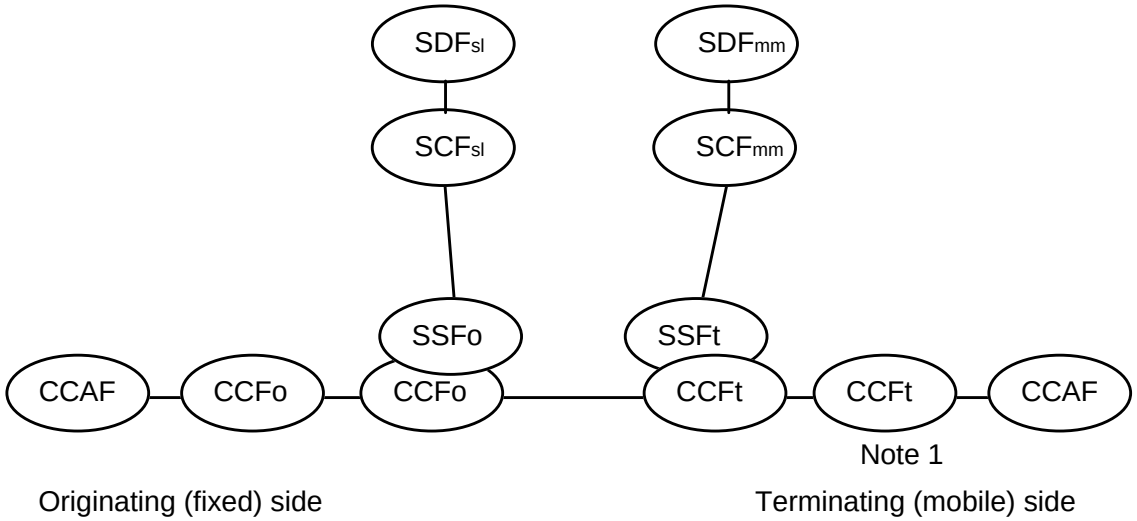


Figure 28: PT incoming call case 2

An originating party dials a directory number of a mobile terminal (CTM number). If the CTM number is a non-geographical IN number then the call will be routed to the nearest SSF of the calling party. If the CTM number is a geographical number then the call will be routed to the SSF nearest to the LE that is associated with the CTM user's subscription (home SSF). The SSF will trigger the SCFsl. SCF_{sl} retrieves CTMid and a routing address (e.g. SSFt address) from SDFsl. . With the obtained data, SCF_{sl} instructs originating SSFo to route the call to the SSFt. The SCFmm asks the visited SSF/CCF to route the call towards the identified FT. FT pages the PT.

NOTE 2: This CCF can be optionally present, depending on the network topology.

6.2.1.2 CTM Incoming call IFs

This subclause describes the information flows for incoming call. Procedures are based on the following assumptions**:**

(**clause 4**) The information flows reported refers to the case when CTM number is a non-geographical number so that the call is routed to the nearest CCFo/SSFo (originating). The reported information flows could be extended to cover the case when the CTM number is a geographical number, so that the call is first routed with the appropriate ISDN User Part (ISUP) message to the CCFh/SSFh (home), where the incoming call to a CTM number is recognized.

(**clause 5**) Since authentication procedure processing could cause expiration of timer Tssf, Reset Timer IF will be used, if appropriate, even this is not explicitly shown in the following pictures.

6.2.1.2.1 Incoming call Method 1: roaming number case

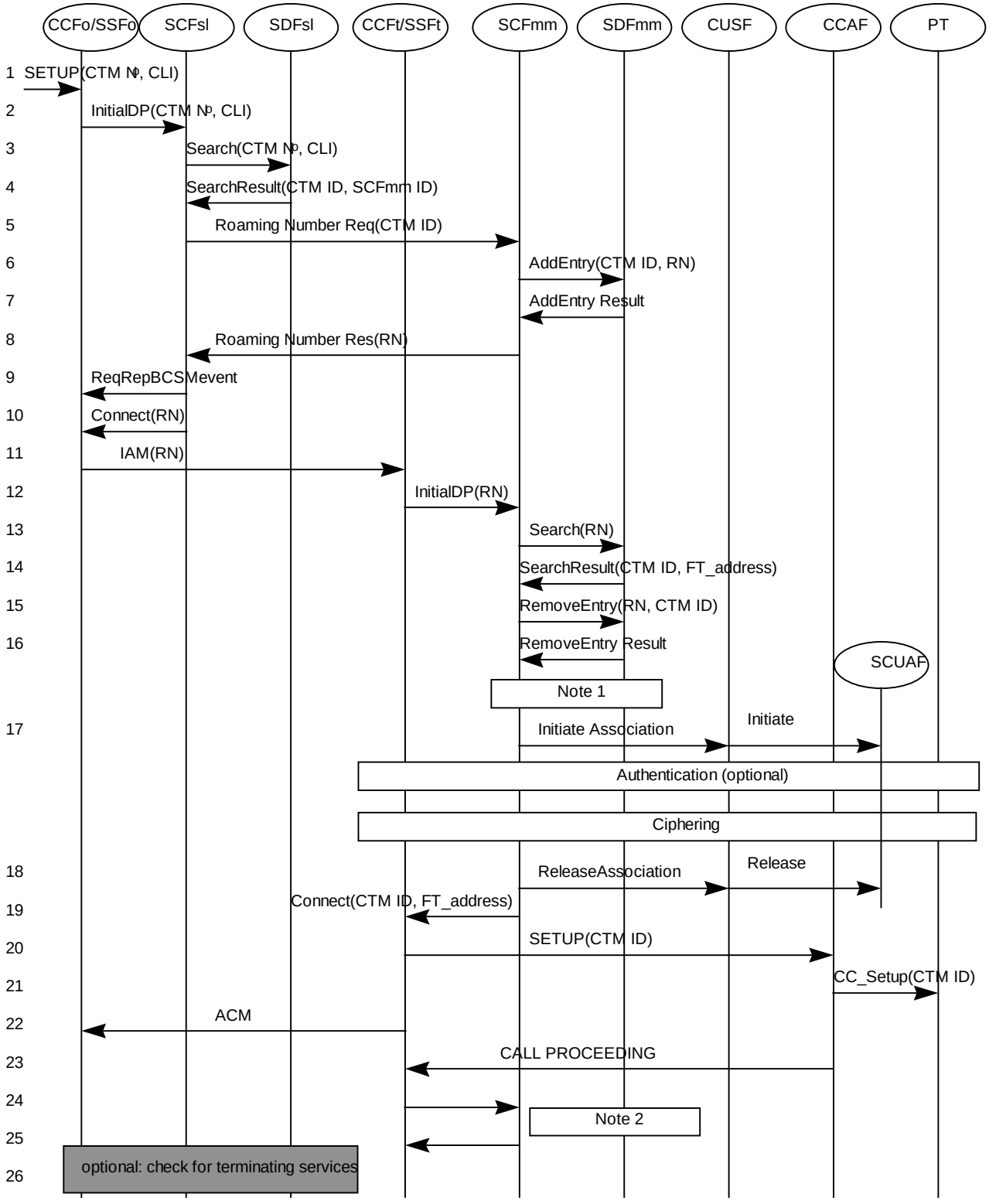


Figure 29: Incoming call case 1, 1 of 2

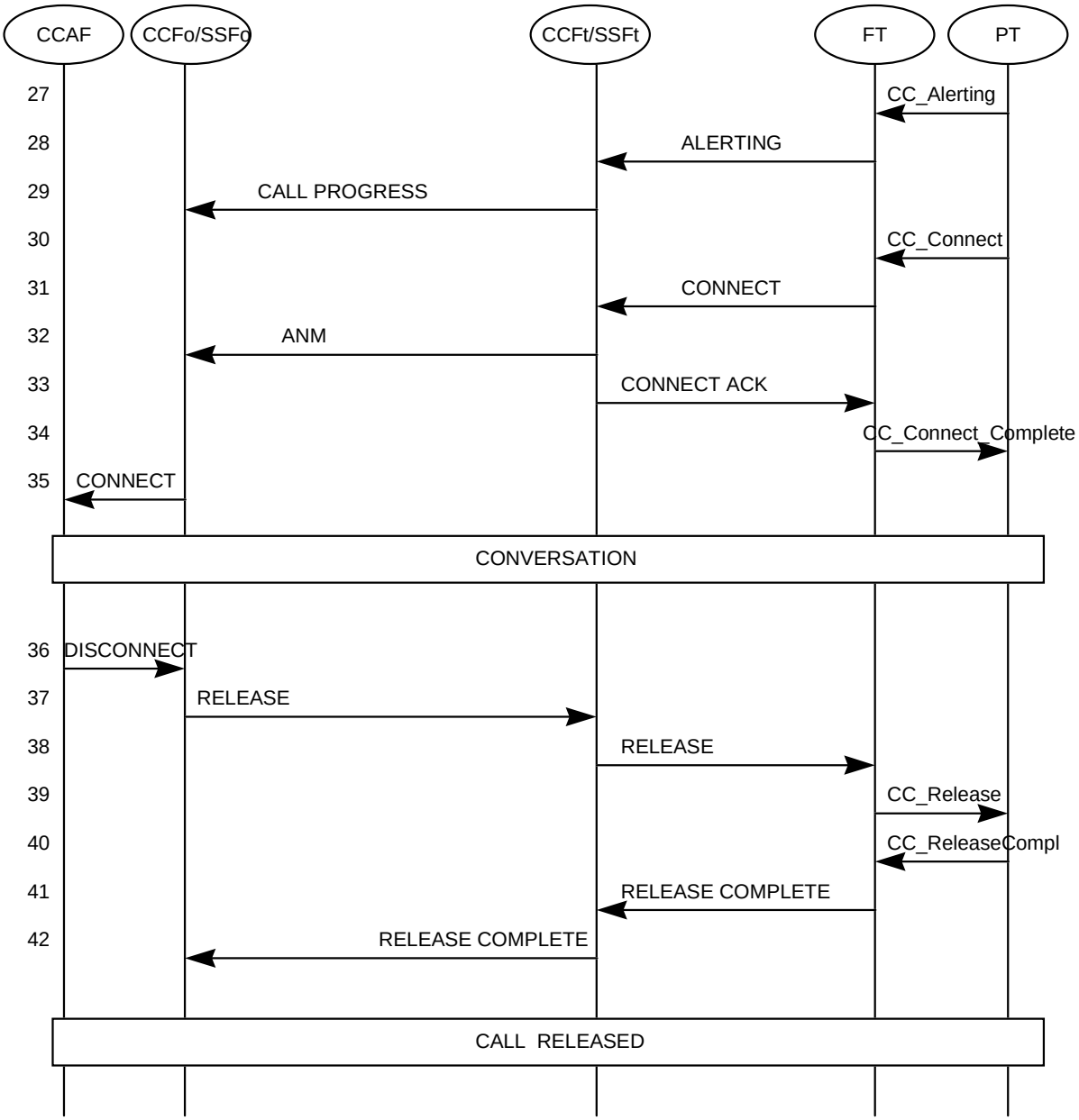


Figure 30: Incoming call case 1, 2 of 2

NOTE 1: The use of the "execute" operation to allocate the roaming number is for further study.

NOTE 2: An intermediate CCF, located between CCF/SSFt and CCAF could be involved in this procedure. If so the CTMid may be conveyed to CCAF through the generic number parameter.

NOTE 3: - Authentication and ciphering may be processed in parallel with call set up.

- Paging is performed with the first message arriving at the FT (authentication, call set up).

- If in parallel call proceeding is used to stop the call set up timer.

- If in sequence a new paging may be requested if the radio link is not maintained; in this case the message 'CC_SETUP' is not ciphered.

NOTE 4: Correlation may be needed between call processing and authentication result from the SCFmm (Operator choice).

1 The calling user sends a Setup message, containing the CTM number (called CTM N°) of the called PT, to the CCF/SSFo.

2 The trigger Distribution Point (DP) is recognized by the CCF/SSFo, which, on recognition of CTM N°, sends a InitialDP message, containing the CTM N° and the Calling Line Identity, to the appropriate SCFsl.The DPT criteria are on a per service base. The way used to route the query to the SCFsl is network operator dependant.

3 The SCFsl interrogates the particular SDFsl that contains the CTM user profile, to get the routing information of the PT.

4 The SDFsl responds with the related CTMid and the identity of the SCFmm, where the PT is currently registered. The action to be taken when no SCFmmid is available is a network operator choice. For instance the call could be routed to a diversion not reachable number, if the latter is available; otherwise the call could be cleared with appropriate announcement.

5 SCFsl establishes a relationship with SCFmm and requests the SCFmm to provide a Roaming Number (RN) of the PT, identified by the CTMid. To do that, SCFsl sends a Handing Information Request to SCFmm.

6,7 Based on this request, the SCFmm allocates the RN and inserts it in the terminal data profile in the SDFmm. This RN belongs to the numbering set of the CCF/SSF to which the CCAF, where the terminal is roaming, is linked to.

8 SCFmm responds to the SCFsl with the allocated RN of the PT. To do that, SCFmm, sends a Handling Information Result message, inserting RN in the "destination Routing Address" IE.

9,10 SCFsl answers to the CCF/SSFo InitialDP, providing the allocated RN, placed in the destinationRoutingAddress IE of the Connect operation.

Eventually, SCFsl asks the CCF/SSFo to report for appropriate Basic Call State Machine (BCSM) events (i.e. 'Route select failure', 'O_no_answer', O_Called_Party_busy) to provide appropriate treatment on not reachable situations.

11 CCF/SSFo routes the call to the CCF/SSFt and provides the RN in an IAM message.

12 CCF/SSFt recognizes the trigger DP (CS-2 "single service interaction " DP processing rule) and sends an InitialDP message to the SCFmm.

13-16 The SCFmm interrogates the SDFmm to get the CTMid and FT address; SCFmm also releases the roaming number and deletes it from SDFmm.

17 The SCFmm initiates an association with the SCUAF via the CUSF providing the FT address. Authentication and ciphering may start then. In the event of no authentication data in SDFmm, SCFmm retrieves them from SDFsl and store them in SDFmm.

18 The SCFmm release the non call related association with the SCUAF.

19 The SCFmm instructs the CCFt/SSFt to route the call to the given FT address.

20 The CCFt sets up a call to the FT providing also the CTM ID.

21 The FT sets up the call to the PT.

22 The CCFt/SSFt sends an early address complete message to the originating side to stop network timers.

23 FT sends a call proceeding to the CCFt/SSFt.

24,25 Correlation between call processing and authentication result from the SCFmm may be optionally performed here.

26 Optionally, SSFt checks the SCFsl for terminating services.

27-35 Normal call set up procedure.

36-42 Release phase, initiated from called party.

NOTE 5: If no Initial DP is received by SCFmm a logic timeout in the SLP causes SCFmm to deallocate and delete RN in SDFmm.

NOTE 6: This procedure has been moved in the new subclause 6.2.1.2.3.

6.2.1.2.2 Incoming call Method 2

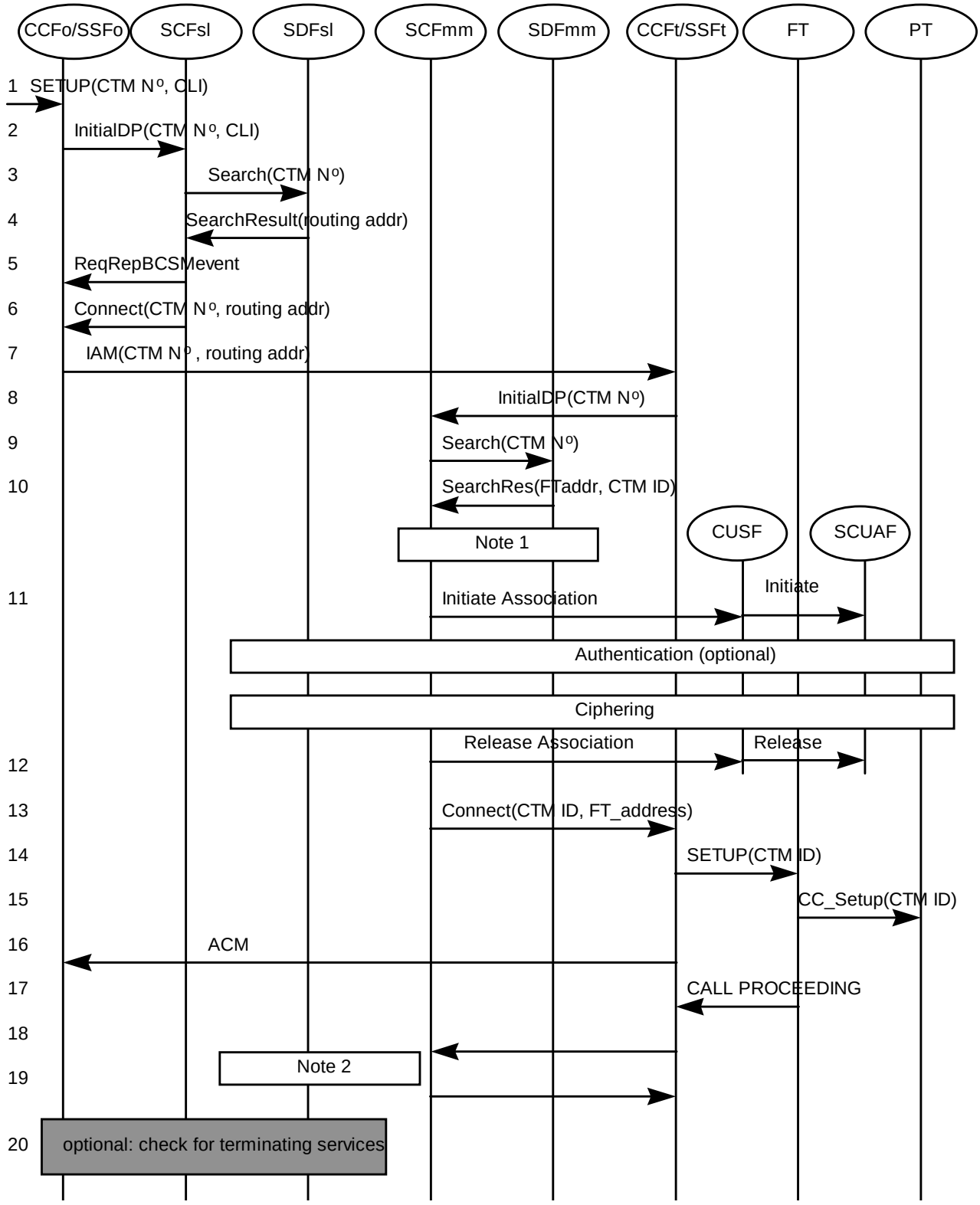


Figure 31: Incoming call - case 2 - 1 of 2

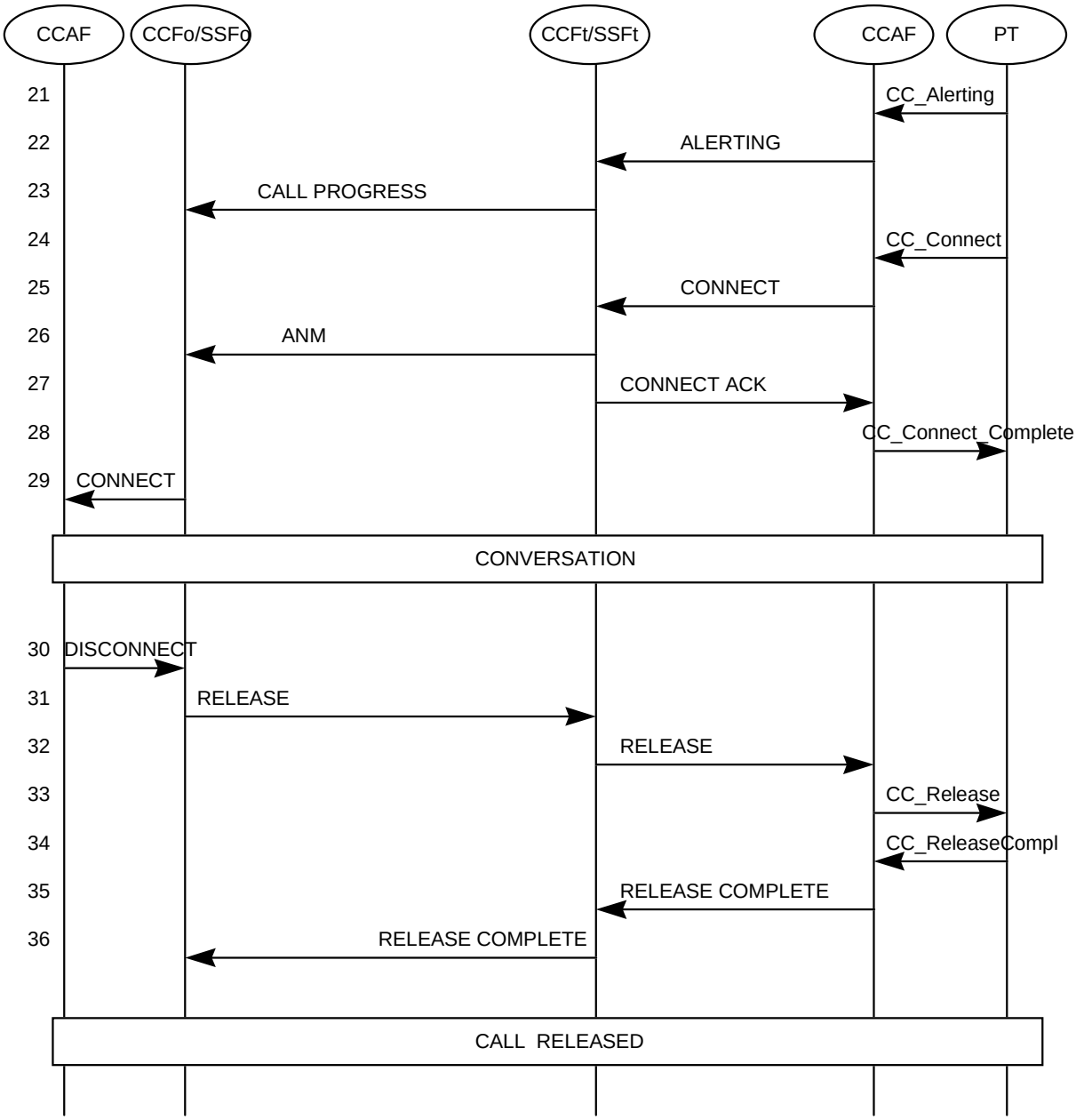


Figure 32: Incoming call - case 2 - 2 of 2

NOTE 1: - Authentication and ciphering may be processed in parallel with call set up.

- Paging is performed with the first message arriving at the FT (authentication, call set up).

- If in parallel call proceeding is used to stop the call set up timer.

- If in sequence a new paging may be requested if the radio link is not maintained.

NOTE 2: Correlation may be needed between call processing and authentication result from the SCFmm (operator choice).

1 The calling party sends a set-up message, including the called number (CTM number) and its identity (CLI).

2 The SSFo recognizes the request as an incoming CTM call and sends an InitialDP to the SCFsl.

3,4 SCFsl retrieves from SDFsl the routing address.

5 SCFsl orders SSFo to suspend call processing at given detection points.

6 SCFsl orders SSFo to set up the call. The CTM number and the routing address are included in the Connect operation.

7 CCFo/SSFo routes the call to CCFt/SSFt.

8 The SSF triggers the SCFmm to retrieve the CTM ID and FT address from SDFmm.

9,10 SCFmm retrieves CTM ID and FT address from SDFmm.

11 SCFmm initiates a call unrelated dialogue with SCUAF via CUSF by providing FT address. Authentication and ciphering may start then.

12 The SCFmm release the call unrelated association.

13 The SCFmm requests the CCFt/SSFt to setup the call to the FT. The CTM ID and FT address are included in the Connect message.

14,15 CCFt sets up the call to the PT via FT providing the CTMid.

16 CCFt sends an early Address Complete Message (ACM) to the originating side to stop network timer.

17 FT sends Call Proceeding message to the CCFt/SSFt.

18,19 Correlation may be performed between call processing and authentication result from the SCFmm (operator choice).

20 Optionally, SSFt checks the SCFsl for terminating services.

21-29 Normal call set up procedure.

30-36 Release phase, here initiated from the mobile party.

6.2.1.2.3 Incoming call released for authentication failure

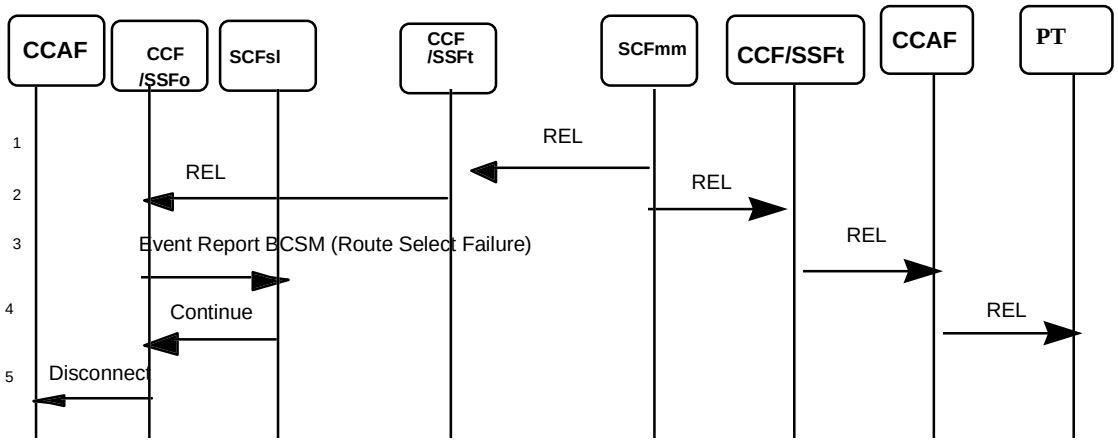


Figure 33: Incoming call case 1, authentication failure case

1,2 After SCFmm realizes that authentication is failed, it instruct CCF/SSFt to release the call.

3 Call release E-DP Route Select Failure is reported to SCFsl.

4 SCFsl instructs call processing to continue.

5 The connection is released.

6.2.2 CTM outgoing calls procedures/IFs

6.2.2.1 CTM outgoing calls procedures

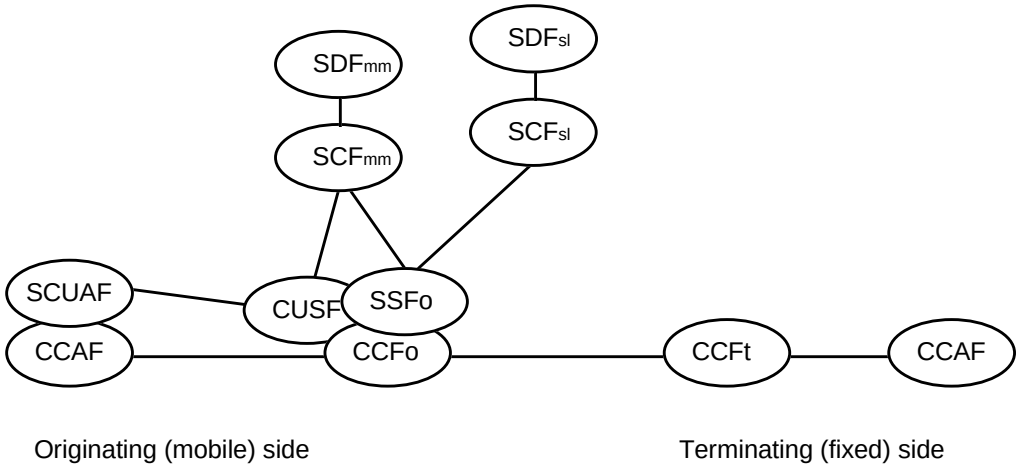


Figure 34: PT originating call

When the PT makes an outgoing call, the CCAF routes the call to the nearest CCF/SSF that triggers (e.g. on the access line) and involves SCFsl. SCFsl retrieves from SDFsl the CTM user profile and instructs CCF/SSF to handle the call.

6.2.2.2 CTM outgoing calls Ifs

This subclause describes the information flow for outgoing call. It is based on the following assumption:

(**clause 6**) clause 5 applies also to the following IFs.

NOTE 1: The outgoing call procedure was preceded by a location registration procedure.

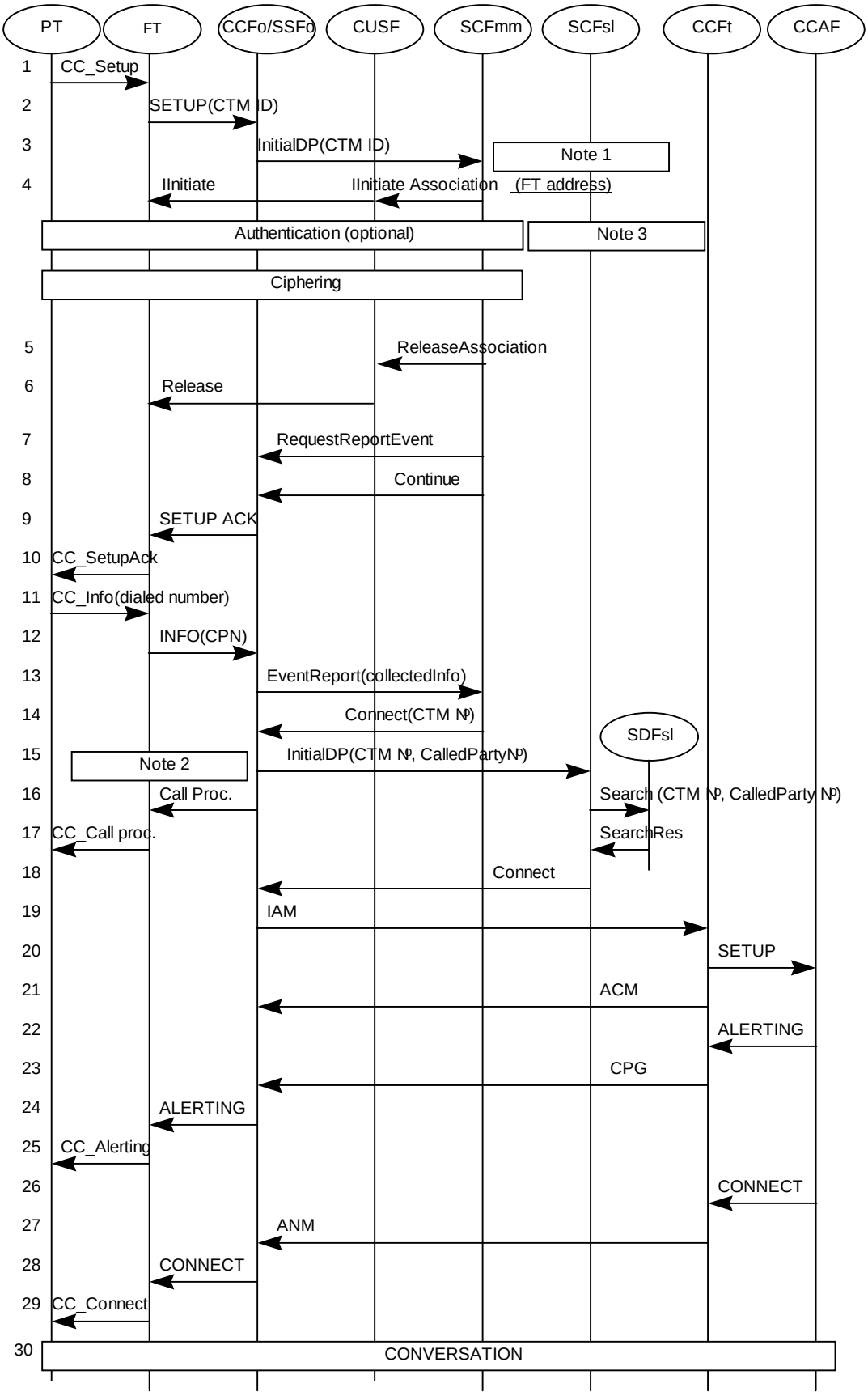


Figure 35: Outgoing call - 1 of 2

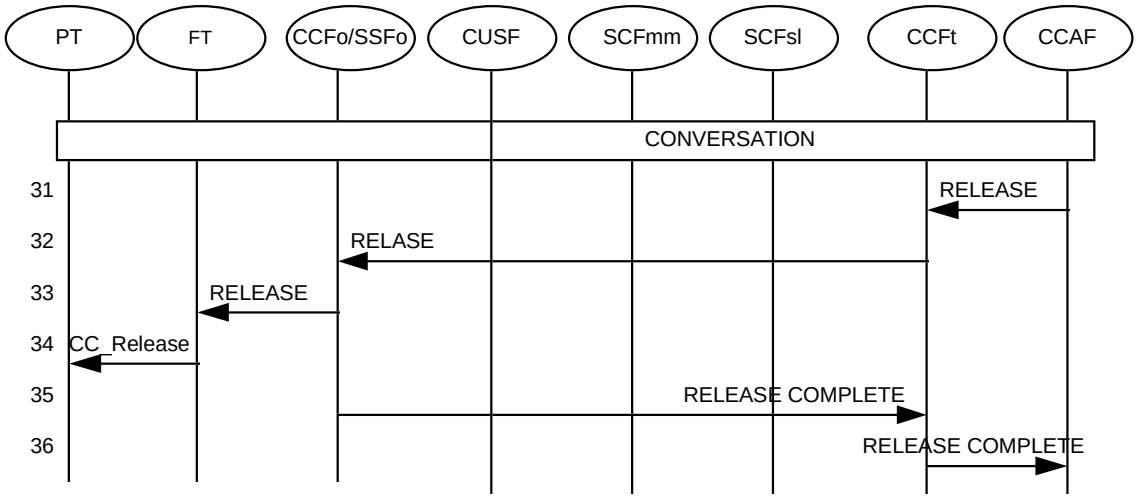


Figure 36: Outgoing call - 2 of 2

NOTE 2: Authentication and ciphering may be processed in parallel with call setup (correlation between call processing and authentication may be performed as operator choice). If processed in sequence then it could be necessary to restart the setup timer in FT and PT.

NOTE 3: If it is an emergency call then the authentication result is ignored and the call continues without SCFsl triggering (flows 16 to 19).

NOTE 4: Ciphering may be initiated without authentication using a previously stored DCK.

1,2 The PT initiates a call, identifying itself (CTM). FT sends a set-up message to the CCFo/SSFo, including CTMid of the calling PT.

3 The CCFo/SSFo recognizes the request as an outgoing CTM call and sends an InitialDP to the SCFmm.

4 SCFmm initiates a call unrelated association with SCUAF via CUSF by providing the FT address. Authentication and ciphering may start then.

5,6 The call unrelated association is released by the SCFmm.

7 SCFmm request the report of the collected information event.

8 SCFmm orders the CCFo/SSFo to continue call setup. If the SETUP ACK is sent earlier, some digits of the called party number could not be ciphered.

9-12 The Setup message is acknowledged and the dialled digits are received.

13 The collected information is sent in an EventReport message to SCFmm.

14 SCFmm sends the CTM number to CCFo/SSFo in order to identify the calling CTM user.

15 The CTM number triggers an initial detection point in SSFo to SCFsl to ask for services.

16-17 SCFsl queries the SDFsl to check the service profile (e.g. restriction on called party Num).

18 If no restriction applies the SCFmm instruct the CCFo/SSF0 to continue the call.

19-30 CCFo/SSFo routes the call accordingly and receives backward signaling. The connection is established.

31-36 Release phase; here initiated from called party.

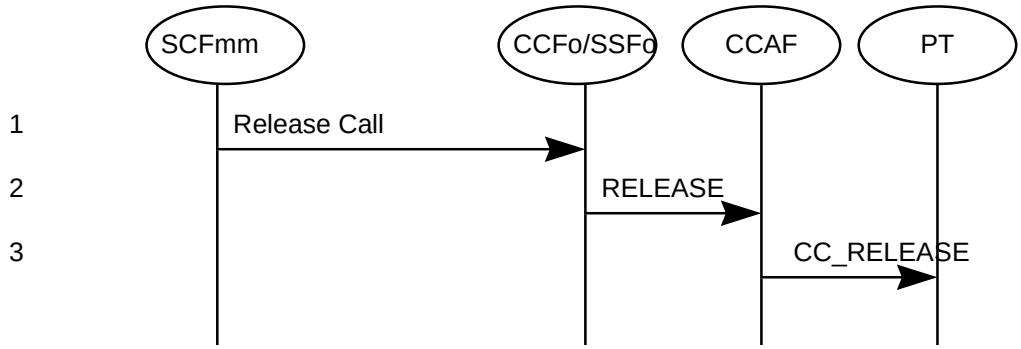


Figure 37: Outgoing call, authentication failure case

1 If authentication fails and the call is not an emergency call, SCFmm orders CCF/SSFo to release call.

2-3 Call release is propagated back to the PT.

6.2.2.3 CTM outgoing calls procedures with Service Profile Transfer capability

Within the intra-network case (single public network) Service Profile Transfer (SPT) is *an optional* capability that allows to *differentiate CTM features among different subscriptions*. This functionality provides the visited side information related the type of features subscribed by the user (e.g. message waiting indication delivery). Done in conjunction with the first location registration procedure in the visited side, it save queries toward the SDFhome for each subsequent situation when this type of check might be required (subsequent location registrations, outgoing calls, etc.).

Moreover it specifically gives the means to solve *interactions between supplementary services* (e.g. clip, clir, colp, colr, call waiting, call hold, etc.) *versus CTM service features*. This interactions are very likely, since from the market perspective a CTM user might/should be a fixed network subscriber (with all his/her Supplementary Services) with an additional cordless mobility capability.

To provide this functionality a network operator can adopt (optionally) the SDFsl-SDFsl relationship, even in CTM phase 1, and to shadow *service profile data* to the visited level. In this case at visited side both a SDFmm and SDFsl are involved, the same apply for SCFmm and SCFsl. At home side only SDFsl and SCFsl are involved. Anyway, the instance of SCFsl SLP at visited side does not need to be as complex as the one in the home side.

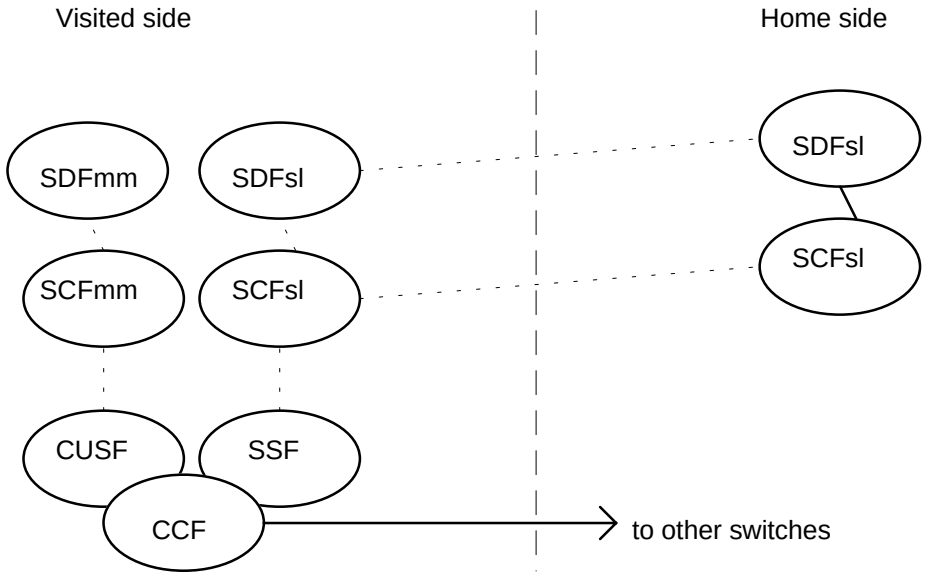


Figure 38: CTM outgoing calls procedures with Service Profile Transfer capability

6.2.3 CTM to CTM call

A CTM to CTM call would be a combination of CTM outgoing call and CTM incoming call.

6.2.4 CTM Emergency call procedures/IFs

The emergency call procedure description is included in the outgoing call procedure description.

6.2.5 Service Profile interrogation/modification

These procedures have been left open by NA1; for this reason they are no investigated here; a possibility is to use a DTMF signalling, without impact on DSS1.

6.2.6 Call Forwarding on Not Reachable

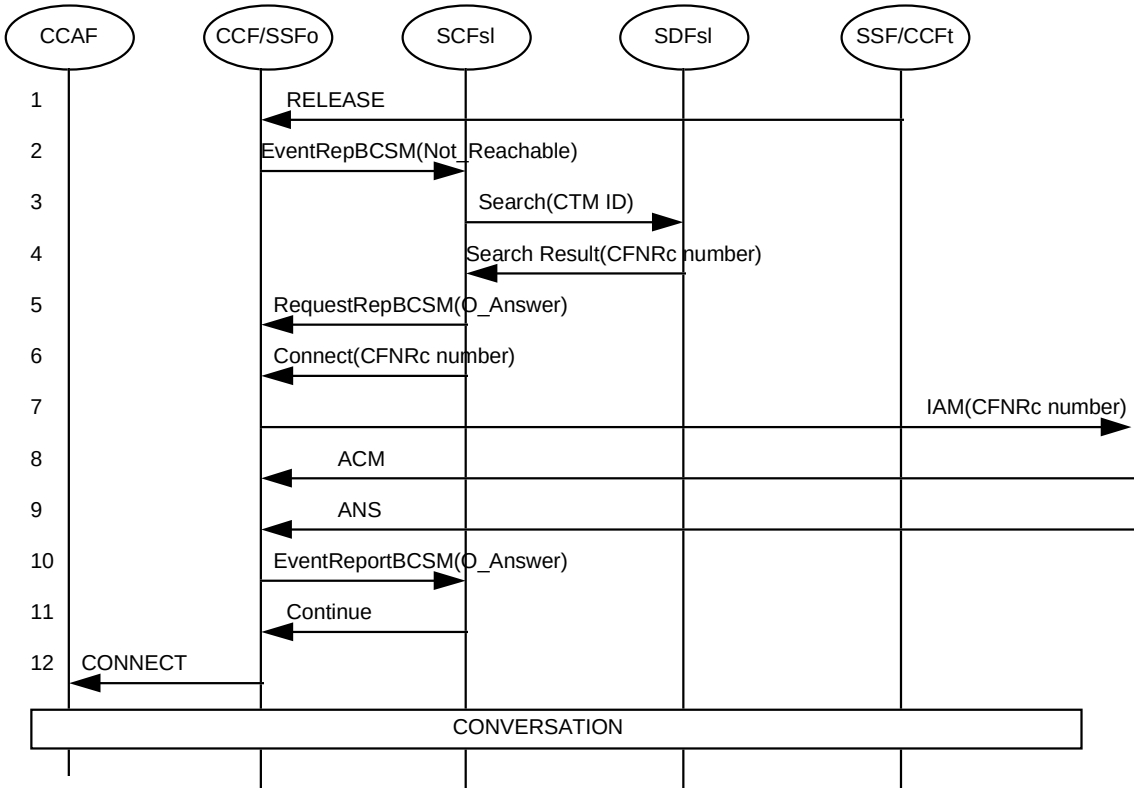


Figure 39: Incoming call, CFNR case

1 CCF/SSFt realizes that user has not answered and release the call back to CCF.

2 CCF/SSFo reports appropriate Encrypted Data Processor (EDP) (Not Reachable) to SCFsl.

3,4 SCFsl retrieves from SDFsl the routing number.

5,6 SCFsl instructs to route the call towards the new destination and arms an E-DP on O_ANSwer.

7,8,9 CCF/SSFo routes the call to new destination and receives the answer message.

10 CCF/SSFo reports SCFsl the O_Answer EDP.

11 SCFsl instructs the CCF/SSFo to complete the path through the access.

12 The connection is established and conversation takes place.

Annex A (informative): Mapping Between CTM Generic TERMS AND DECT/CT-2 TERMS

The aim of the CTM service is to operate over the two European air interface DECT and CT2. Therefore, generic CTM terms are used to describe CTM identities and information elements. The following table proposes generic terms and their mapping on DECT and CT2 terms, which are functionally equivalent.

	Generic CTM term	Dect term	CT2 term
PP Identities	CTMid	part of IPUI	TRD
	CTM Access Right	PARK	LID
	CTM Temporary Id	TPUI	-
FP Identities	CTM base identity	RFPI	LID, LAI, LCI
Authentication Elements	RAND	RAND	RAND
	RS	RS	-
	RES	RES	CKEY
	ZAP	ZAP	ZAP
	DCK	DCK	-

The following table proposes generic messages and their corresponding messages in DECT and CT2, which are functionally equivalent.

ACTIVITIES	Generic messages	DECT GAP Messages	CT2 Messages
Location Registration	CTM Locate Request	LOCATE_REQ	FA (class, value)
	CTM Locate Response	LOCATE_ACCEPT/REJECT	FI (class, value, state parameter)
			LR-PARAMS
Paging	CTM Paging Request	LCE-Req-Page	Polling

(continued)

ACTIVITIES	Generic messages	DECT GAP Messages	CT2 Messages
	CTM Paging Response	LCE-Page-Resp	ID-OK
Incoming Call Setup	CTM call set up	CC-SETUP	FI (class, value, state parameter)
	CTM Connection	CC-CONNECT	CC
Outgoing Call Setup	CTM Call Setup	CC-SETUP	FA (class, value)/ TERM-CAP
	CTM Alerting	CC-ALERTING	-
	CTM Connection	CC-CONNECT	CC
Authentication	CTM Authentication Req	AUTH-REQ	AUTH-REQ
	CTM Authentication Response	AUTH-REP	AUTH-RES
Ciphering	CTM ciphering req	CIPHER_REQ	-
	CTM cipher reply	---	-
Information	CTM Info	CC Info	Keypad
Com. release from the PP	CTM Release Req	CC-RELEASE	FA (class, value)
	CTM Release confirmation	CC-RELEASE-COM	INIT
Com. release from the FP	CTM Release Req	CC-RELEASE	INIT

(continued)

(concluded)

ACTIVITIES	Generic messages	DECT GAP Messages	CT2 Messages
	CTM Release confirmation	CC-RELEASE-COM	Ack
Access Rights	CTM Access rights Request	ACCESS_RIGHTS_REQ	
	CTM Access rights Response	ACCESS_RIGHTS_ACCEPT	TRD_ALLOC
		ACCESS_RIGHTS_REJECT	-
Key Allocation	CTM Key Allocation	KEY_ALLOCATE	KEY-ALLOC

Annex B (informative): Examples Of The Mapping Of FEs Into Physical Elements For CTM

NOTE: Only external relationships are shown, i.e., relationships between FEs residing in different PEs.

CASE 1: Link between home Service Control Point (SCP) and visited SCP, SDPs separated from SCPs.

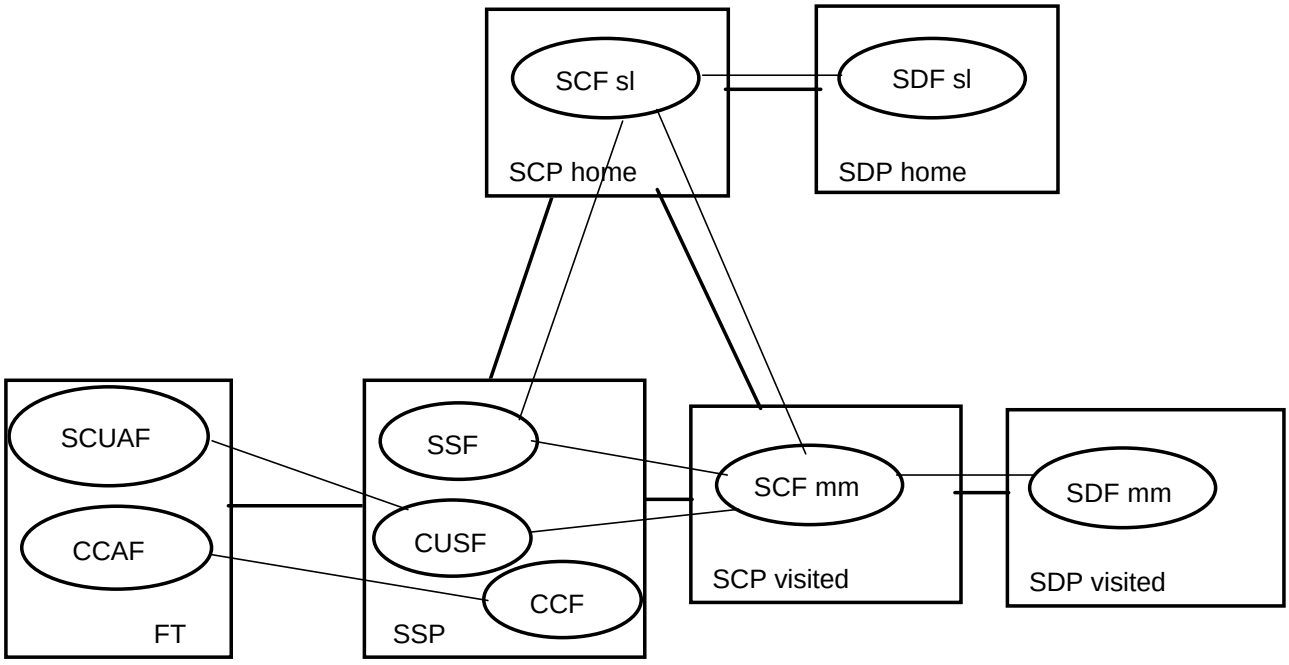


Figure 40: Physical scenario case 1

CASE 2: Link between visited SCP and home SCP; no separate SDPs.

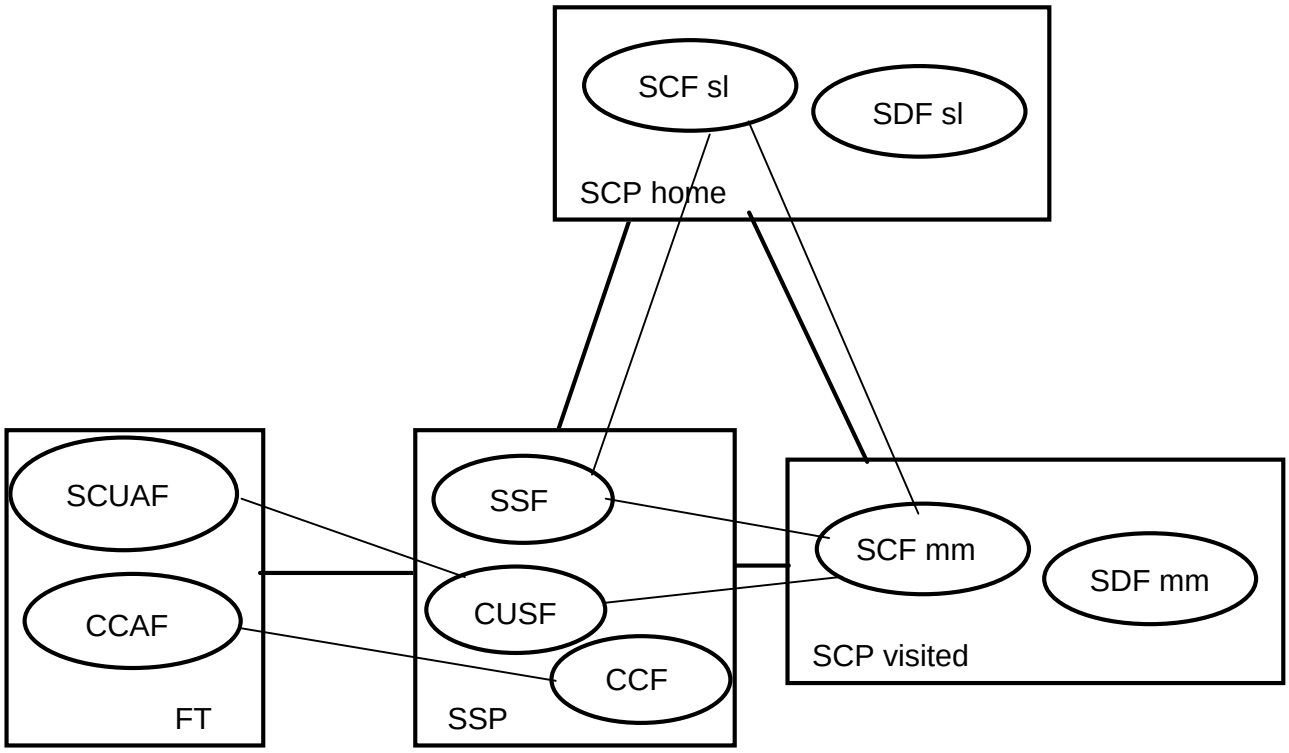


Figure 41: Physical scenario case 2

CASE 3: Visited SSP with SCFmm/SDFmm capabilities.

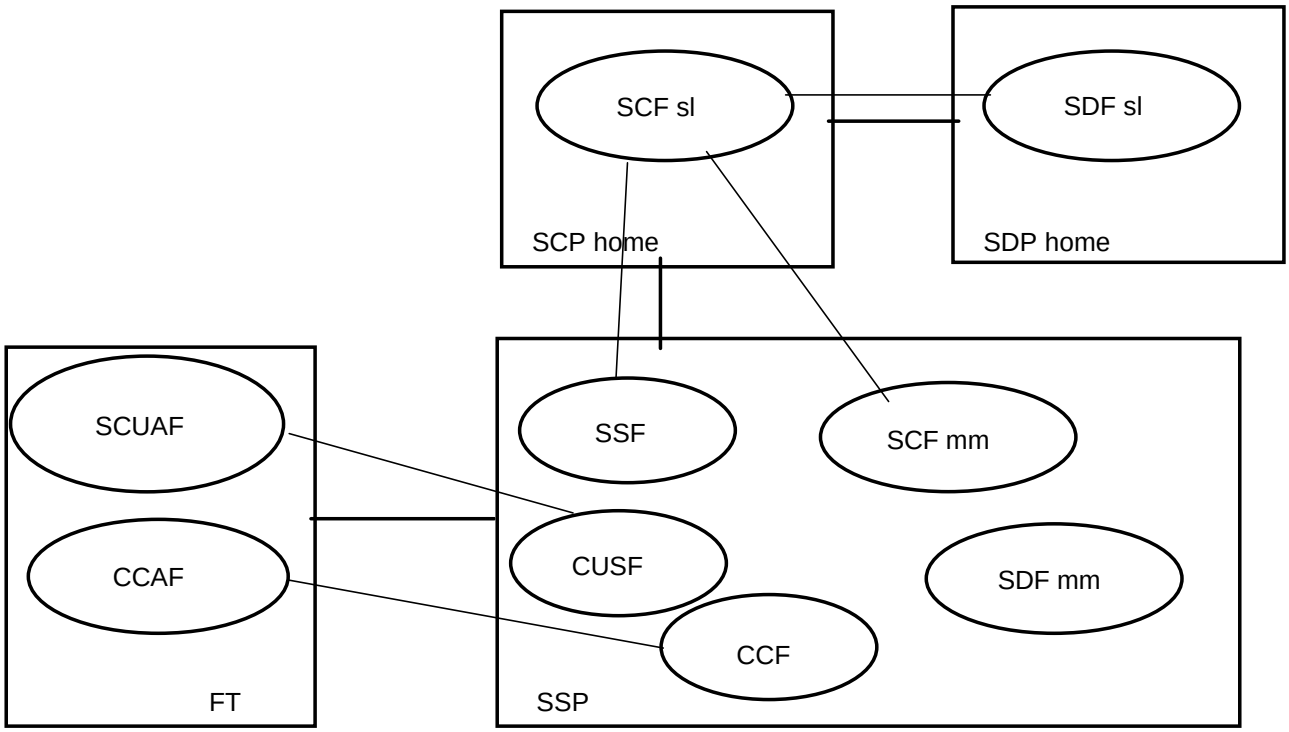


Figure 42: Physical scenario case 3

CASE 4: SCP with SCFmm, SCFsl, SDFsl and SDFmm capabilities.

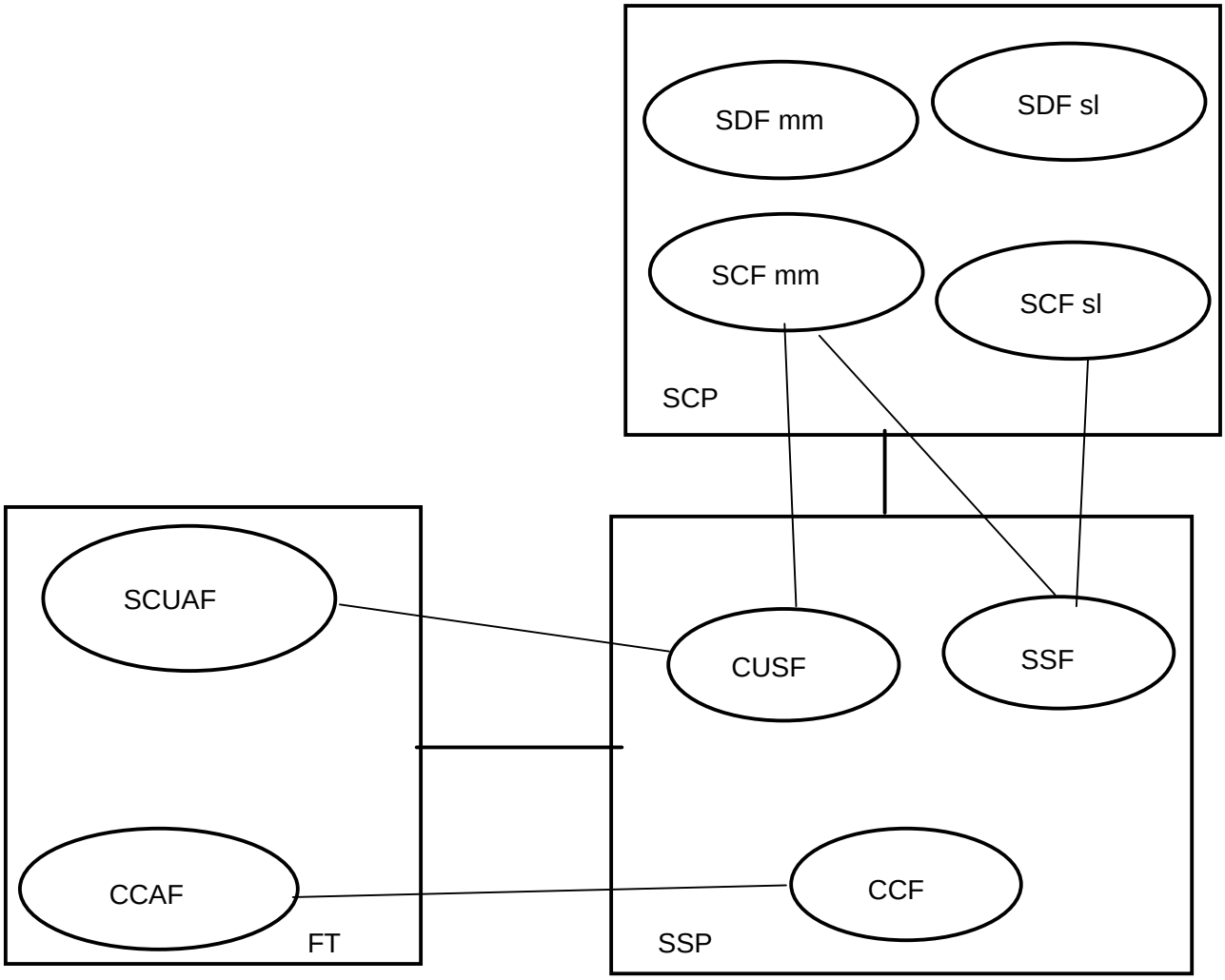


Figure 43: Physical scenario case 4

CASE 5: Visited SSP with SCFmm capabilities and FT with SDFmm capabilities.

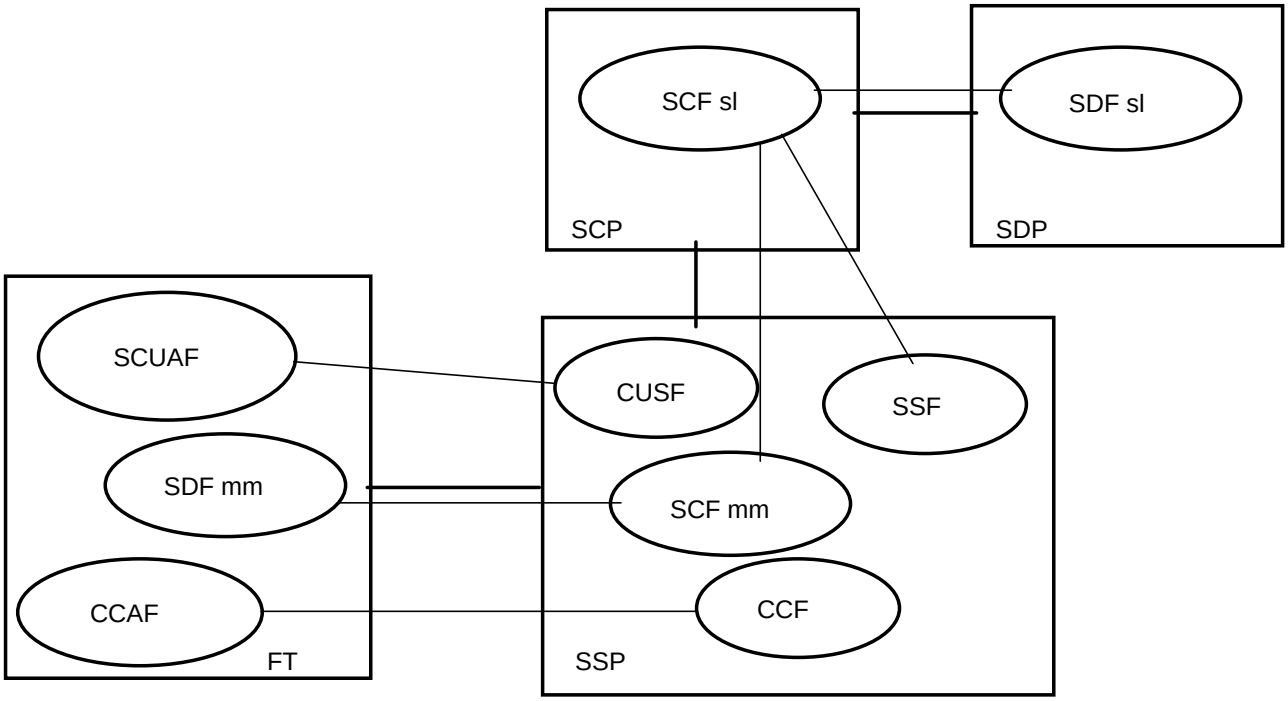


Figure 44: Physical scenario case 5

CASE 6: Home SCP with SDFsl capabilities and visited SCP with SDFmm capabilities.

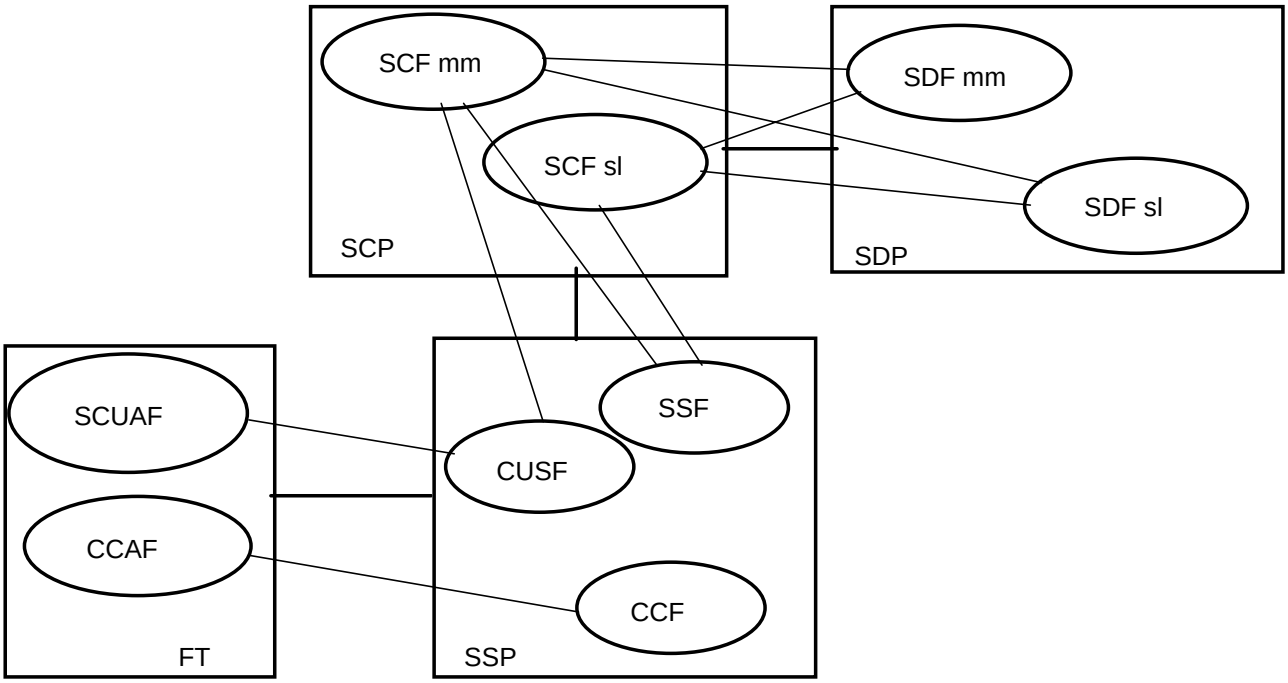


Figure 45: Physical scenario case 6

CASE 7: Home SCP, home SDP home and visited SDP.

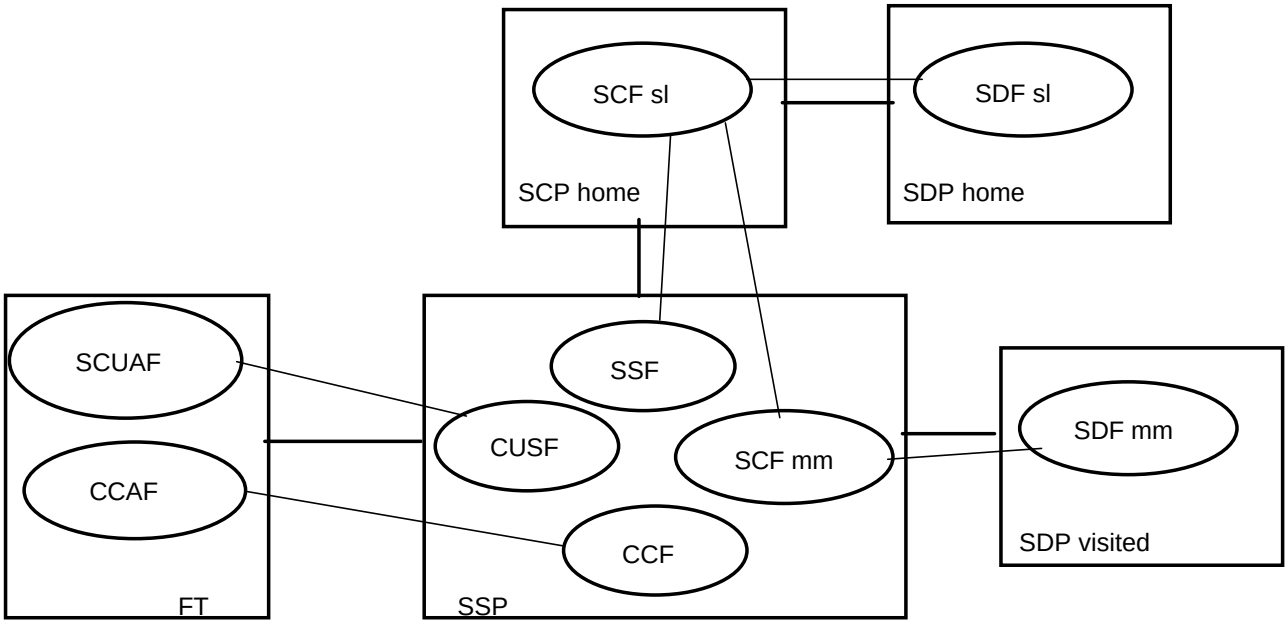


Figure 46: Physical scenario case 7

CASE 8: Visited SSP (with SCFmm/SDFmm capabilities) and home SCP.

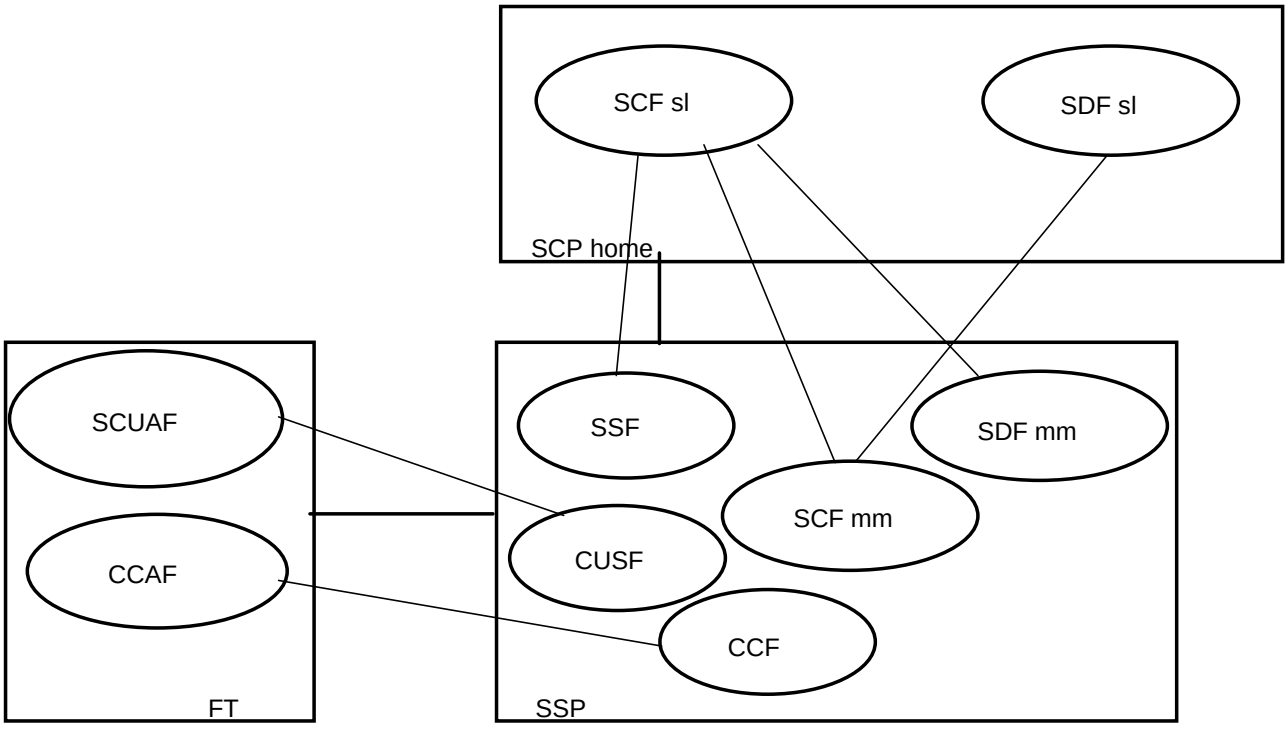


Figure 47: Physical scenario case 8

CASE 9: Visited SSP (with SCFmm, SDFmm and SDFsl capabilities) and home SDP.

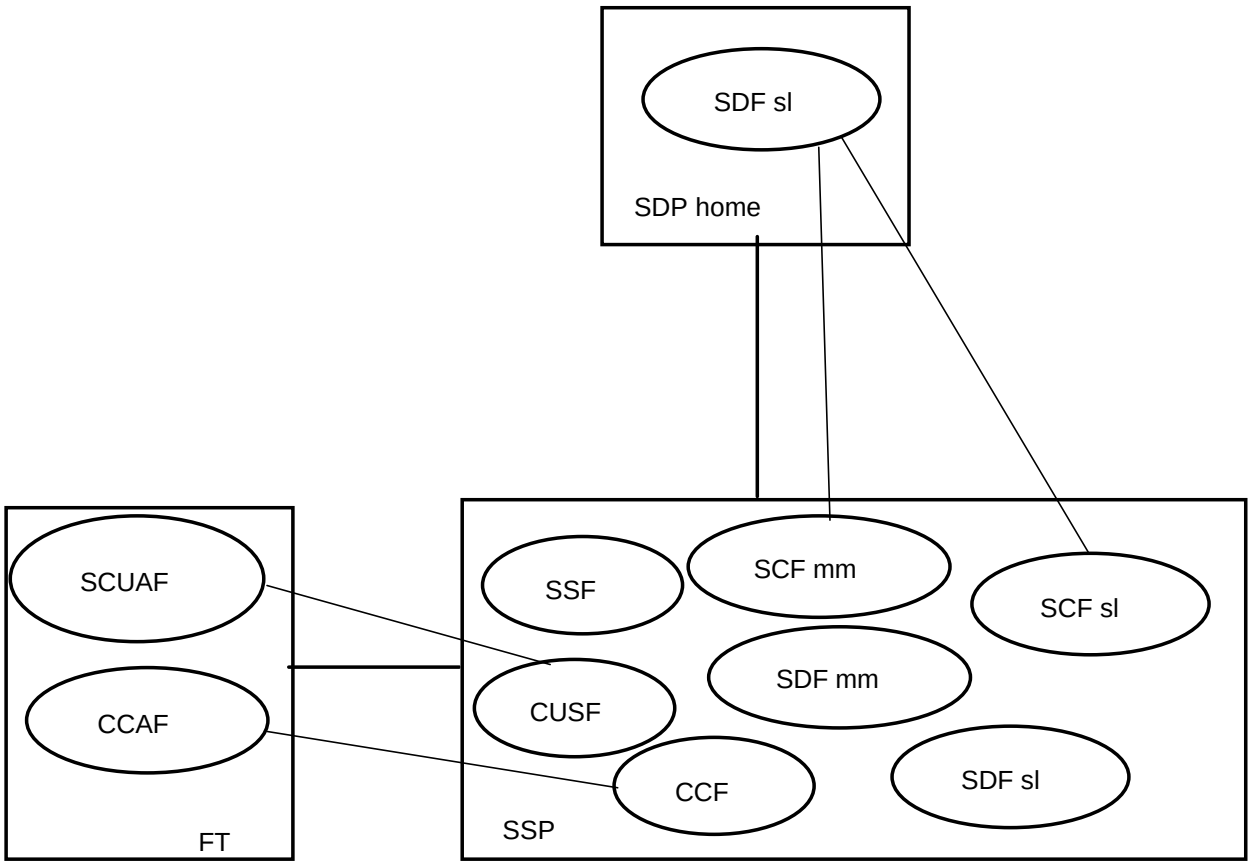
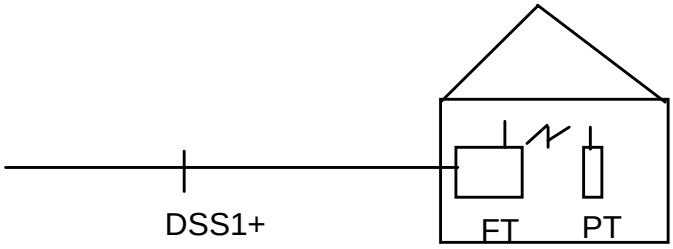


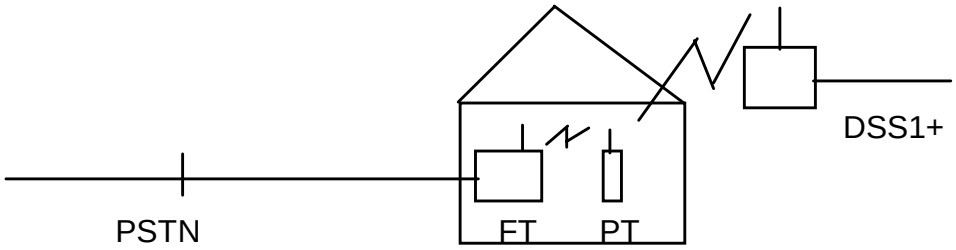
Figure 48

Case 10: PT in the own residential environment.

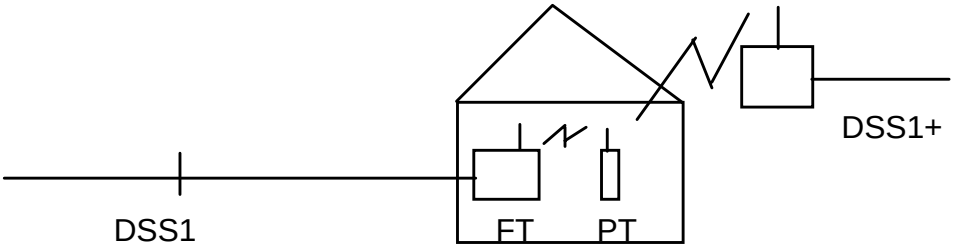
The following cases are currently envisaged and described in the following picture. Case 10.1 does not imply additional requirement, compared to the public environment case. Case 10.2 requires interworking with PSTN access and in this scenario, as an operator option, DTMF user procedures will be used to activate user home registration. Case 10.3 requires interworking with ISDN network using DSS1 without enhancement, in this scenario, as an operation option, DTMF procedure or mechanisms such as call forwarding on not reachable may be used to activate user home registration.



Case 10.1: domestic device behaves like a public FT



Case 10.2: domestic device does not behave like a public FT (PSTN access)



Case 10.3: domestic device does not behave like a public FT (ISDN access)

Figure 49: Different physical scenarios related to the residential environment

Annex C (informative): Bibliography

The following material, though not specifically referenced in the body of the present document, gives supporting information.

- CCITT Recommendation Q.1205 (1992): "Intelligent Network Physical Plane Architecture".
- CCITT Recommendation Q.1211 (1992): "Introduction to Intelligent Network CS-1".
- CCITT Recommendation Q.1214 (1995): "Revised Distributed Functional Plane for Intelligent Network CS-1".
- CCITT Recommendation Q.1215 (1992): "Physical Plane for Intelligent Network CS-1".
- CCITT Recommendation Q.1218 (1995): "Interface Recommendations for Intelligent Network CS-1".
- NA-TR 016 (1993): "Network Aspects. Intelligent Network CS-2 targeted telecommunications services".
- TCR-TR 027 (1995): "Network Aspects. Intelligent Network. Vocabulary of terms and abbreviations".
- ETS 300 374-1 Core INAP.
- TCR-TR NA-60801: "IN management requirements and capabilities for CS-2".
- Draft DEN/NA-020039: "CTM Phase 1 Service Description".
- TCR-TR 013 (1993): Network Aspects (NA); Network Support of PT Mobility.
- ETS 300 175-X series (1992): "Digital European Cordless Telecommunications (DECT)".
- ETS 300 444, "Digital European Cordless Telecommunications (DECT) Generic Access Profile (GAP)".
- ETS 300 131 Second edition (1994): "CAI/CT2 specifications".
- Eg 201 027 (1997): "Mobility Interworking between private and public networks".
- NA-TR 021: "Interworking between private networks (IN-structured and non IN-structured) and public IN-structured networks".

History

Document history				
V1.1.1	December 1997	Membership Approval Procedure	MV 9808:	1997-12-23 to 1998-02-20