Draft EG 201 096-2 V1.1.1 (1997-12)

ETSI Guide

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

European Telecommunications Standards Institute

Reference
DEG/NA-061302-2 (a5ci0icq.PDF)

Keywords
CTM, IN, interworking, 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 5
Foreword 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
3 Definitions and abbreviations 6
3.1 Definitions 6
3.2 Abbreviations 7
4 Requirements and Assumptions 8
4.1 Basic Assumptions for inter-networking case 8
4.2 Relationship at the INAP inter-networking level 8
5 Generic Procedures 9
5.1 Terminal Authentication 9
5.1.1 Terminal Authentication in the Visited Network 9
5.1.1.1 Retrieval and storage of Authentication Parameters 10
5.1.2 Terminal Authentication in the Home Network 10
5.2 Ciphering 11
5.2.1 Ciphering started in the visited network 11
5.2.2 Ciphering started in the Home Network 11
5.3 Location Registration and Data Deletion 11
5.3.1 Location registration with data deletion invoked by the home network 12
5.4 Incoming Call 12
5.4.1 Geographic or portable destination number 12
5.4.2 CTM destination number 13
5.5 Outgoing Call 15
6 Core Features based on SCF-SCF Relation 15
6.1 Terminal Authentication 15
6.1.1 Retrieval and storage of authorization parameters 16
6.1.1.1 Functional architecture 16
6.1.1.2 Information flows 17
6.1.2 Terminal Authentication in the Home Network 18
6.1.2.1 Functional architecture 18
6.1.2.2 Information Flows - Authentication in SCFsl home 19
6.2 Location registration and data deletion 19
6.2.1 Functional architecture 20
6.2.2 Information Flows for Location Registration 21
6.2.3 Information flows for data deletion in the previous visited network 22
6.3 Incoming call (roaming number case) 23
6.3.1 Geographic or portable destination number 23
6.3.1.1 Functional architecture 23
6.3.1.2 Information Flows 23
6.3.2 CTM Destination Number 24
6.3.2.1 Functional architecture 24
6.3.2.2 Information Flows for Incoming Call 24
6.4 Outgoing call 28
6.4.1 Functional architecture 28
6.4.2 Information Flows 28
7 Core Features based on SCF-SDF, SCF-SCF and SDF-SDF Relations 31
7.1 Terminal Authentication 31
7.1.1 Retrieval and storage of authorization parameters 31

7.1.1.1 Functional architecture 31
7.1.1.2 Information flows 32
7.1.2 Terminal Authentication in the Home Network 32
7.1.2.1 Functional architecture 32
7.1.2.2 Information Flows - Authentication in SDFsl home 33
7.2 Location registration and data deletion 33
7.2.1 Functional architecture for Location Registration 34
7.2.2 Information Flows for Location Registration 35
7.2.3 Data deletion in the previous visited network 36
7.2.3.1 Functional architecture for data deletion 36
7.2.3.2 Information Flows for data deletion 37
7.3 Incoming call 37
7.3.1 Geographic or portable destination number 37
7.3.1.1 Functional architecture 38
7.3.1.2 Information Flows 38
7.3.2 CTM destination number - Roaming Number 38
7.3.2.1 Functional architecture (Roaming Number case) 39
7.3.2.2 Information Flows (roaming number case) 40
7.3.3 CTM destination number - Routing Number case 43
7.3.3.1 Functional architecture (Routing Address Case) 43
7.3.3.2 Information Flows for Incoming Call (Routing Address case) 44
7.4 Outgoing call 46
7.4.1 Functional architecture for Outgoing Call 47
7.4.2 Information Flows for Outgoing Call 48

Annex A (informative): List of figures 50

History 51

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 Approval Procedure.

The present document is part 2 of a multi-part EG 201 096 covering Intelligent 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: "Intelligent Network (IN); Cordless Terminal Mobility (CTM), IN architecture and functionality for the support of CTM; CTM Interworking between Public Intelligent Networks";

Part 3: "Intelligent 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

CTM (Cordless Terminal Mobility) requires mobility management functions in the fixed network to allow digital cordless terminals, with a single service registration, to be used to originate and receive calls via any compatible residential, business or public cordless base station [(see DEN/NA 020 039 "Cordless Terminal Mobility (CTM) - Phase1; Service Description")].

The network architecture and functionality to support CTM within a public network is described in EG-NA 61302 part 1 (e.g. ciphering, on-air registration, ...) and between public and private networks is described in EG-NA 61302 part 3.

1 Scope

The present document gives guidance on the network architecture and functionality to support roaming of cordless telephone users between public IN-structured networks and determines the requirements to support CTM across public network boundaries.

The procedures concerned are authentication, location registration, incoming and outgoing call handling and location cancellation when the previously visited network is not the home network.

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.

2.1 Normative references

[1] EN 301 234 (V2.1 onwards): "Example 1".

[2] EG 201 568 (V1.3.5): "Example 2".

[3] EG 201 096-1 (1997) 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".

[4] DEN/NA 020039: "Cordless Terminal Mobililty (CTM) - Phase 1; Service Description".

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-020 039 (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
BA	Basic Access
BCSM	Basic Call State Machine
CCAF	Call Control Agent Function
CCF	Call Control Function
CSz	Connected Subaddress z
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)
DP	Distribution Point
EDP	Encrypted Data Processor
FT	Fixed Termination
IAM	Initial Address Message
IN	Intelligent Network
ISUP	ISDN User Part
LE	Local Exchange
mm	mobility management
N°	Number
O&M	Operational and Maintenance
PRA	Primary Rate Access
PT	Portable Terminal
RAND	a RANDom number issued by the network
RES	a RESponse calculated by a PT
RN	Roaming Number
RS	a value used to establish authentication session keys in DECT
SCF	Service Control Function
SCFsl	Service Control Function
SCP	Service Control Point
SCUAF	Service Control User Agent Function
SDF	Service Data Function
sl	service logic
SLP	Single Link Procedure
SLPI	Service Logic Program Instance
SPT	Service Profile Transfer
SSF	Service Switching Function
XRES	X REf. entry Service
XRES1	an eXpected RESponse calculated by the network

4 Requirements and Assumptions

The procedures concerned are authentication, location registration, incoming and outgoing call handling and location cancellation when the previously visited network is not the home network.

4.1 Basic Assumptions for inter-networking case

In case of a Cordless Terminal Mobility (CTM) user roaming outside of his home network, the following requirements have been identified:

The principle of home's network services has to be supported (see clauses 6 and 7); i.e. the CTM user has to be provided with the services subscribed to his service provider.

Depending upon the capability of the circuit related signalling between Call Control Functions (CCFs) within or between networks, either E.164 routing information or roaming number can be used to route calls to CTM users roaming within that network.

4.2 Relationship at the INAP inter-networking level

The general functional model for CTM support in case of IN inter-networking is shown in figure 1; only the relationships related to the network boundaries are here shown, for the relations used within one network, please refer to EG 201 096-1 [3]:

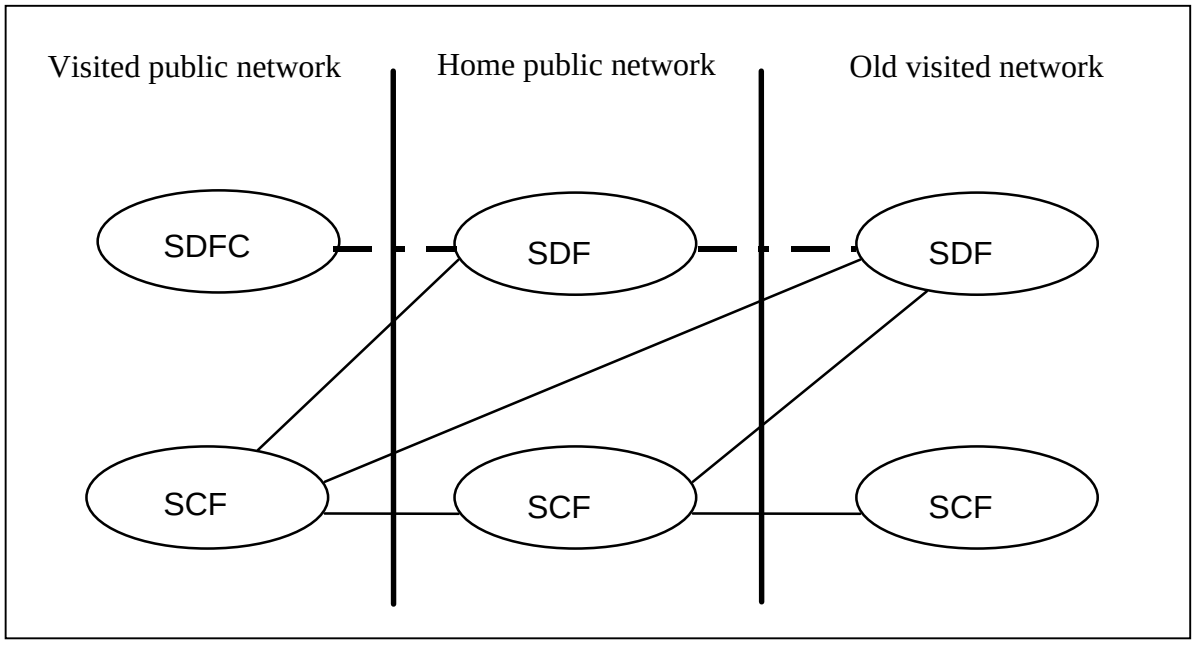


Figure 1: Across networks boundaries relationship

In order to satisfy the requirements identified in the previous clause, the Service Control Function (SCF) relationship has to be supported, limited to the operations required for the CTM provision.

The SCF-SDF relationship can be used to support the CTM, however the SCF-SCF relationship has been identified as appropriate to support home's services when they are selected for the processed call.

The use of SDF-SDF relationship for inter-network Service Profile Transfer (SPT) has to be investigated.

Some problems are envisaged when a CTM user is roaming from network A (old visited) to B (new visited) in case of missed agreements between "old visited" and "new visited" networks; in fact, if the roaming is possible between the home network and network A, and at the same time it's possible between the home network and network B, there is not assurance about roaming and agreement between A and B networks.

5 Generic Procedures

This clause describes the generic procedures for the core features of CTM Phase 1.

5.1 Terminal Authentication

This procedure is split into two independent steps:

- Retrieval and storage of authentication data.
- Authentication of terminal.

For reasons of performance, it may be necessary to maintain sets of authentication parameters in the visited network, retrieving more parameters when the number stored falls below a pre-set threshold.

5.1.1 Terminal Authentication in the Visited Network

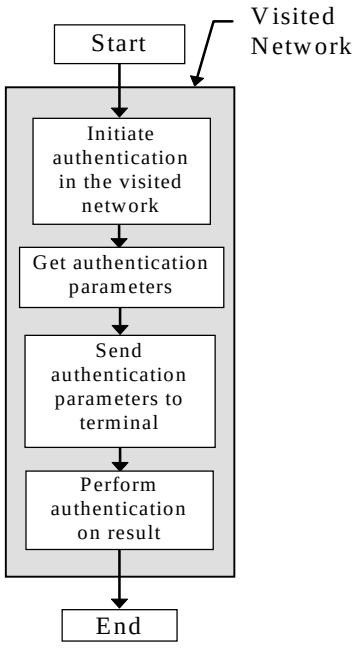


Figure 2: Terminal authentication in the visited network

5.1.1.1 Retrieval and storage of Authentication Parameters

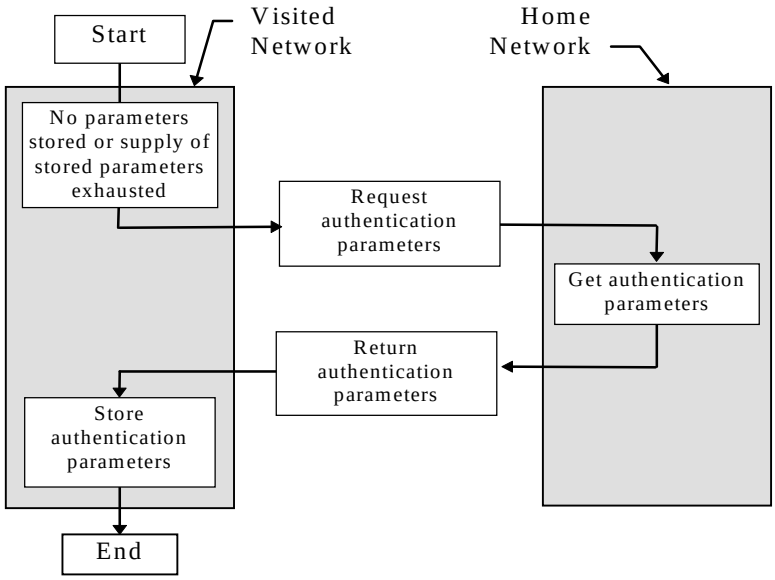


Figure 3: Retrieval and storage of authentication parameters by the visited network

5.1.2 Terminal Authentication in the Home Network

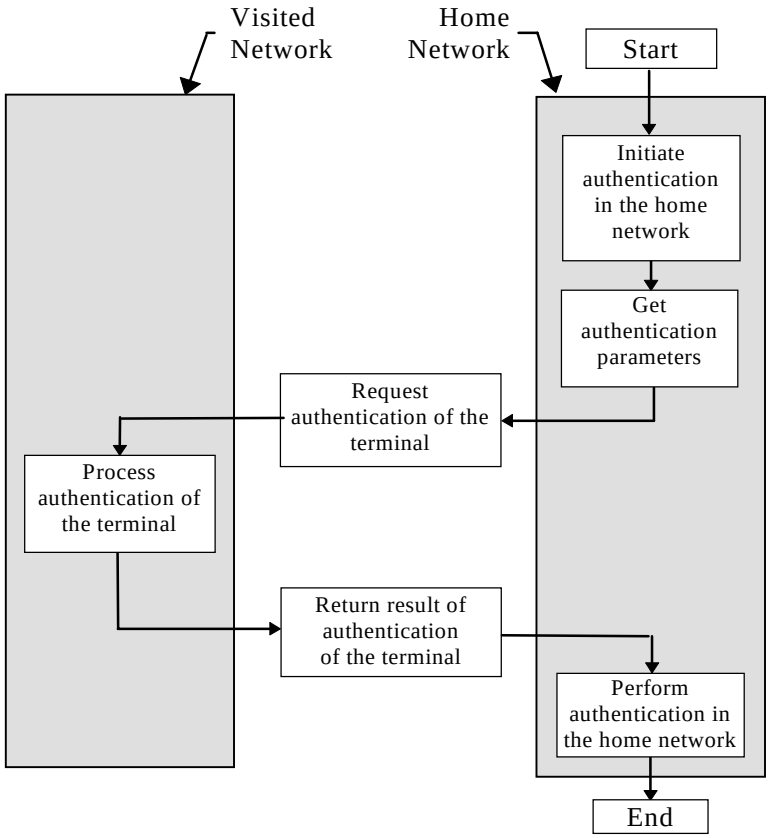


Figure 4: Terminal authentication in the home network

NOTE: If ciphering is to be performed after authentication, then the home network will have to inform the visited network about the result of authentication and the derived ciphering key when needed.

5.2 Ciphering

This procedure uses the ciphering key derived from the authentication process. If ciphering is controlled by the visited network, the ciphering parameter either can be retrieved from the home network together with the authentication parameters or can be locally calculated during the authentication algorithm.

5.2.1 Ciphering started in the visited network

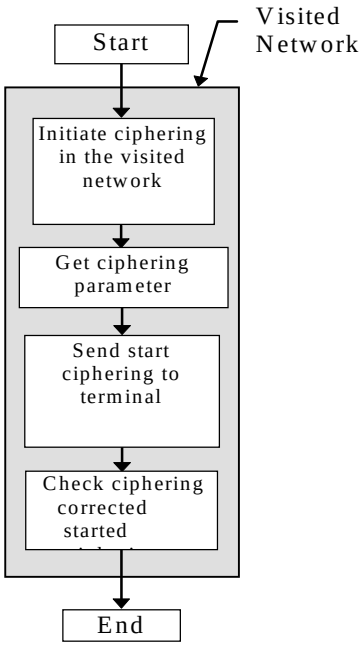


Figure 5: Ciphering started in the visited Network

5.2.2 Ciphering started in the Home Network

The case of ciphering started in the Home Network is not supported.

5.3 Location Registration and Data Deletion

There are two methods that may be used for location registration and data deletion:

- Location registration invoked by the visited network and data deletion invoked by the home network.

5.3.1 Location registration with data deletion invoked by the home network

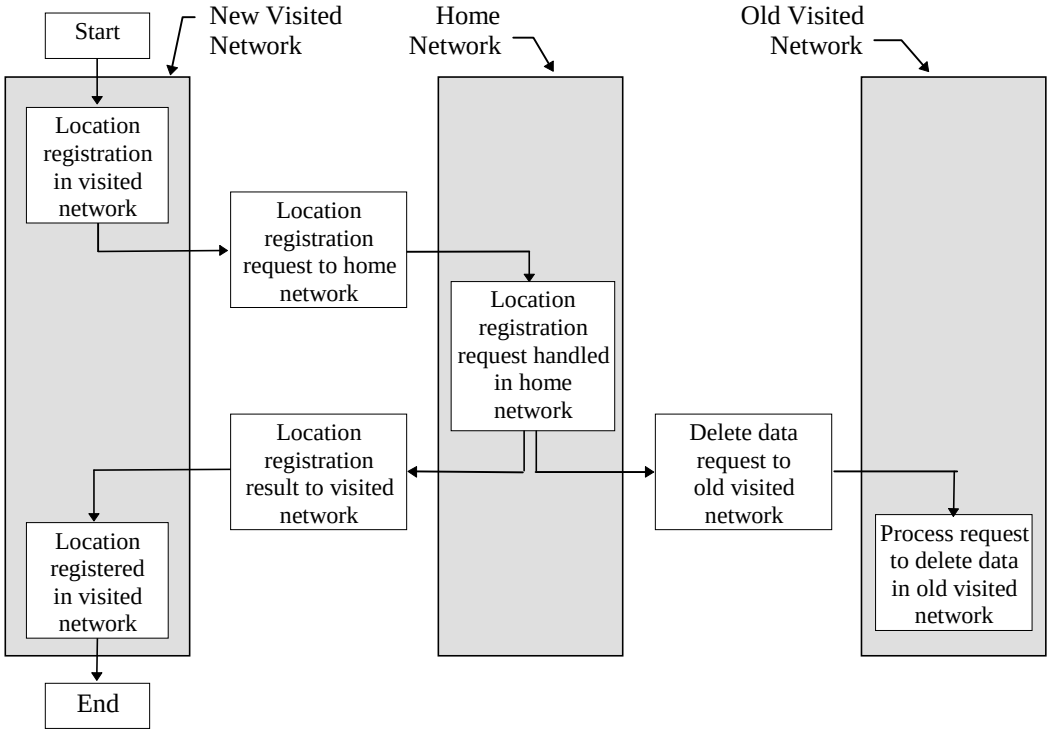


Figure 6: Location registration invoked by the visited network and data deletion invoked by the home network

5.4 Incoming Call

5.4.1 Geographic or portable destination number

It is possible that a geographic E.164 number is used for CTM subscribers, in which case the originating network will not be able to determine that the call is to a CTM customer; it will first route the call to the home network

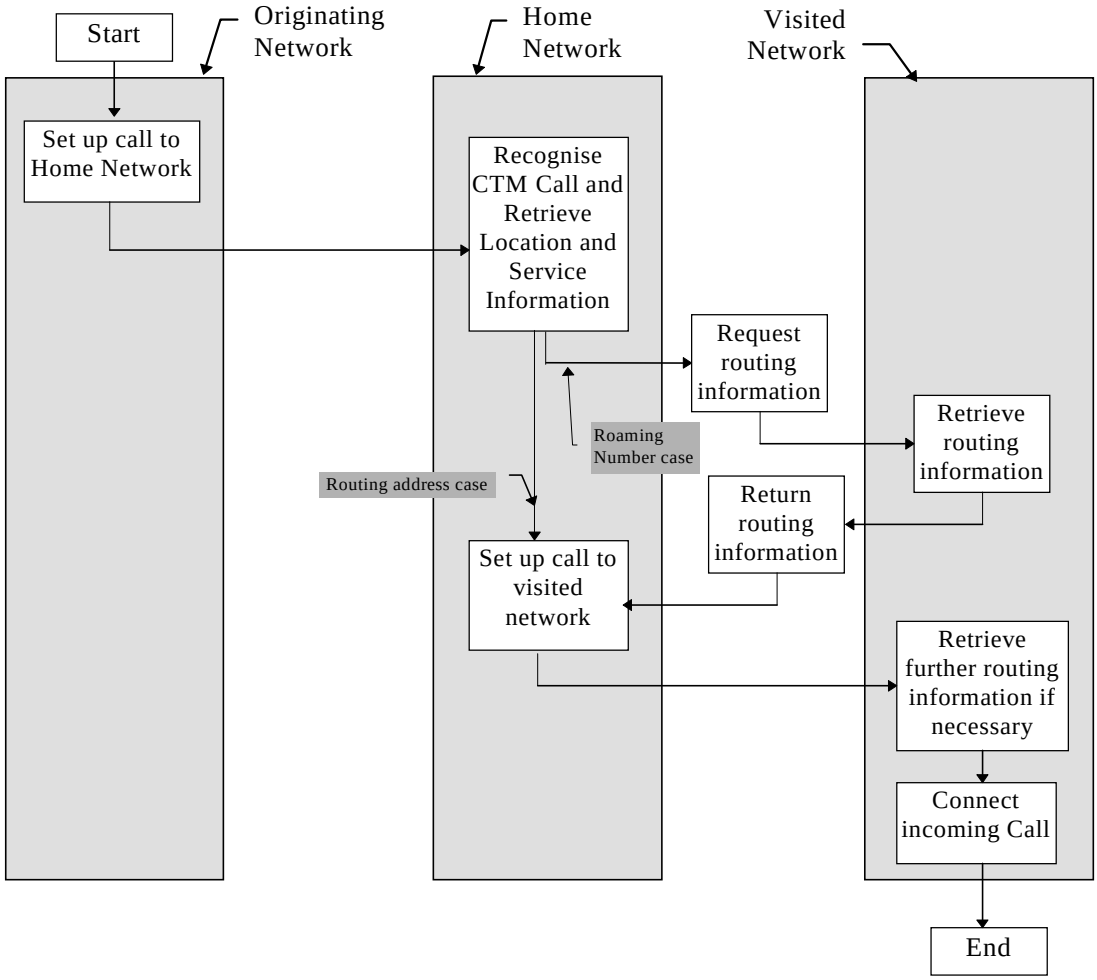


Figure 7: Incoming call to geographic or portable destination number

5.4.2 CTM destination number

It is possible that a non-geographic E.164 CTM Destination number is used for CTM subscribers. This could occur if a European numbering range is dedicated to CTM subscribers and that the subscriber is using a number in that range. The originating network recognizes that the dialled number is a CTM number and may get assistance from the Home Network for routing information and Home Service support.

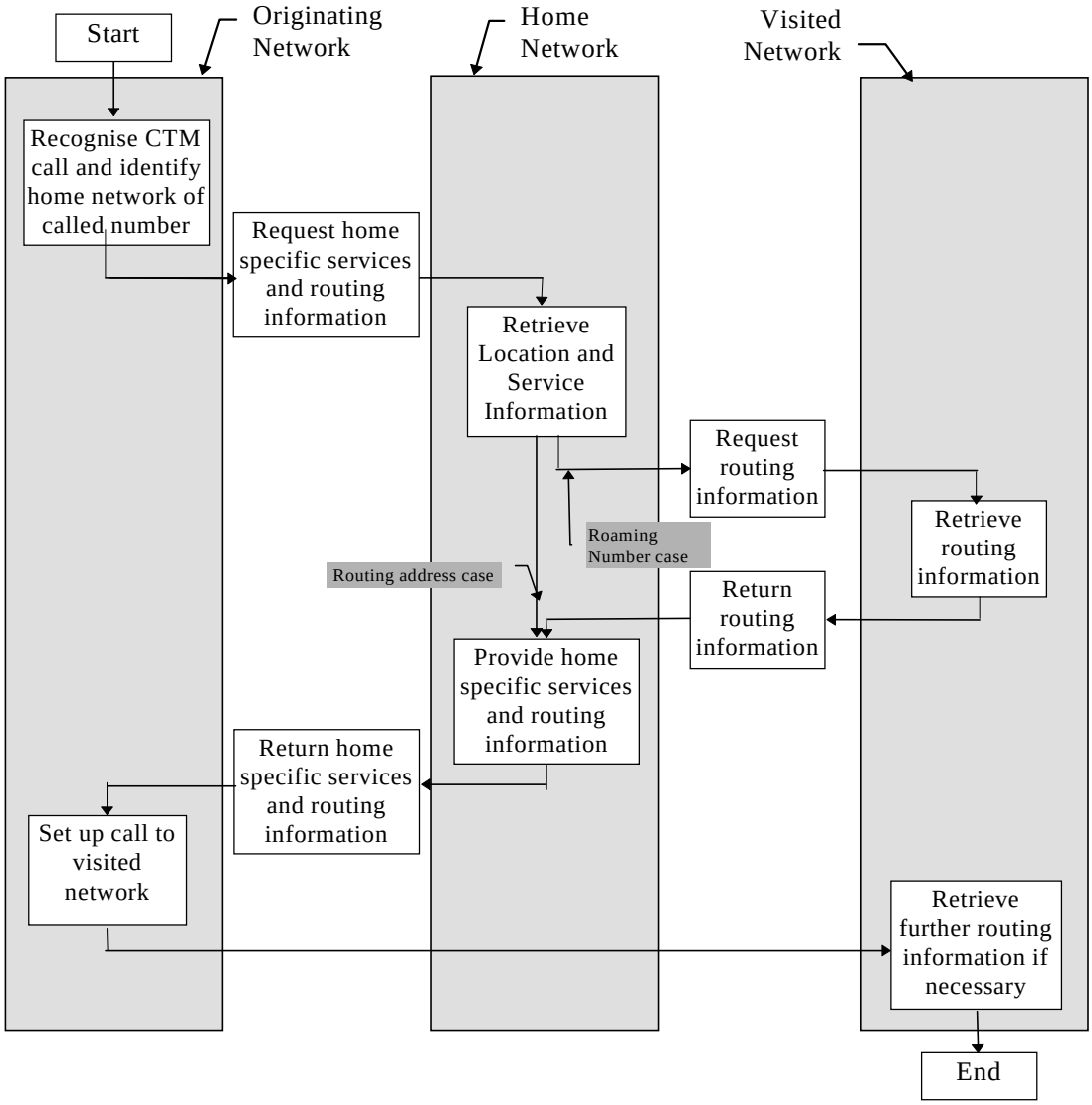


Figure 8: Incoming Call to CTM Number

5.5 Outgoing Call

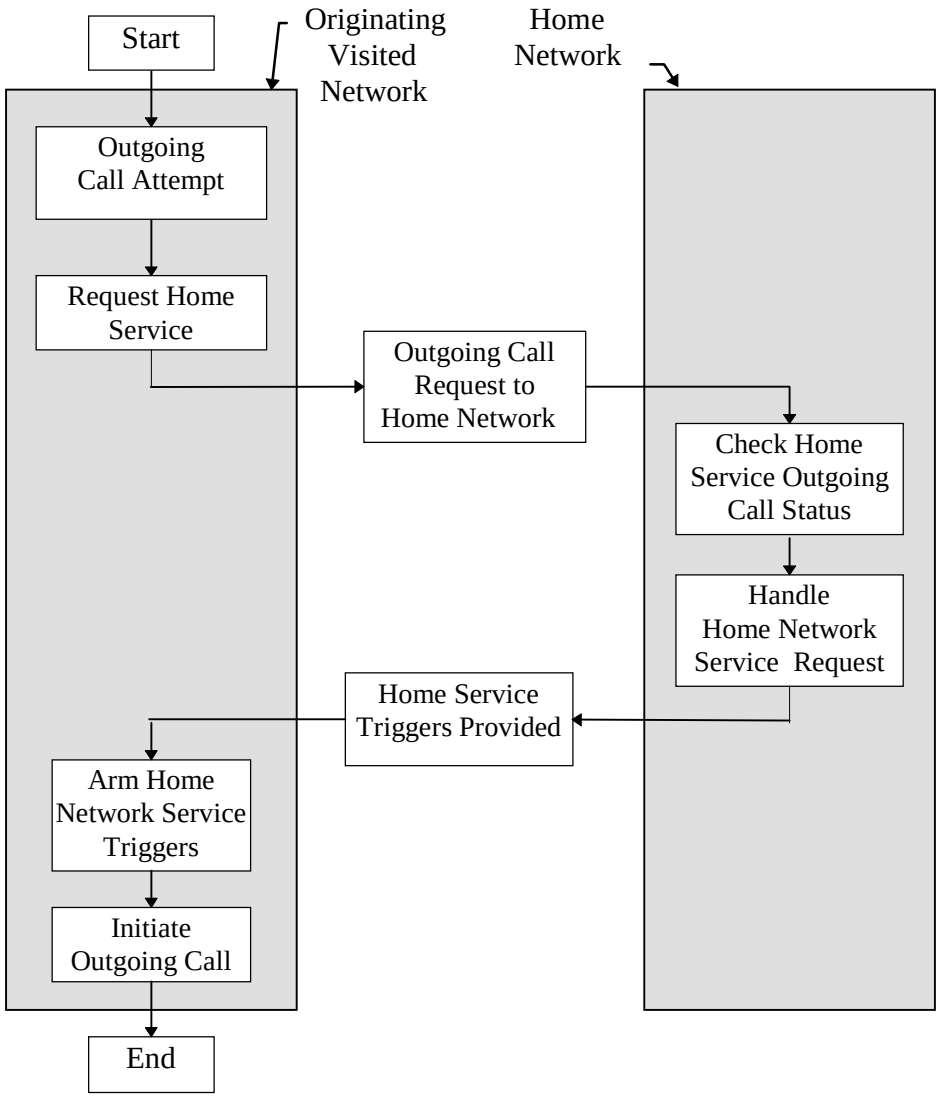


Figure 9: Outgoing Call

6 Core Features based on SCF-SCF Relation

6.1 Terminal Authentication

This subclause provides the functional architecture and information flows for call unrelated terminal authentication which can be performed in either the visited network or in the home network.

When terminal authentication is performed in the visited network, the intra-network procedure described in EG 201 096-1 [3] is followed. When location registration is being performed for the first time in a new visited network, or the supply of authentication parameters falls below a pre-set threshold, authentication parameters are downloaded from the Home Network and stored in the SDFmm.

6.1.1 Retrieval and storage of authorization parameters

During a location registration in a new visited network, or when the supply of authorization parameters falls below a specified limit, a process is initiated to retrieve and store more authorization parameters.

6.1.1.1 Functional architecture

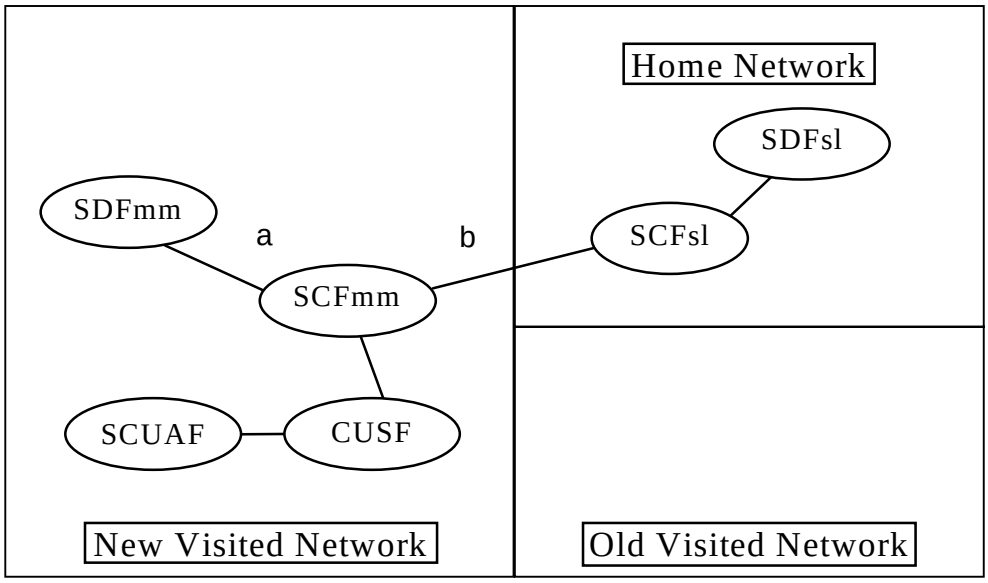


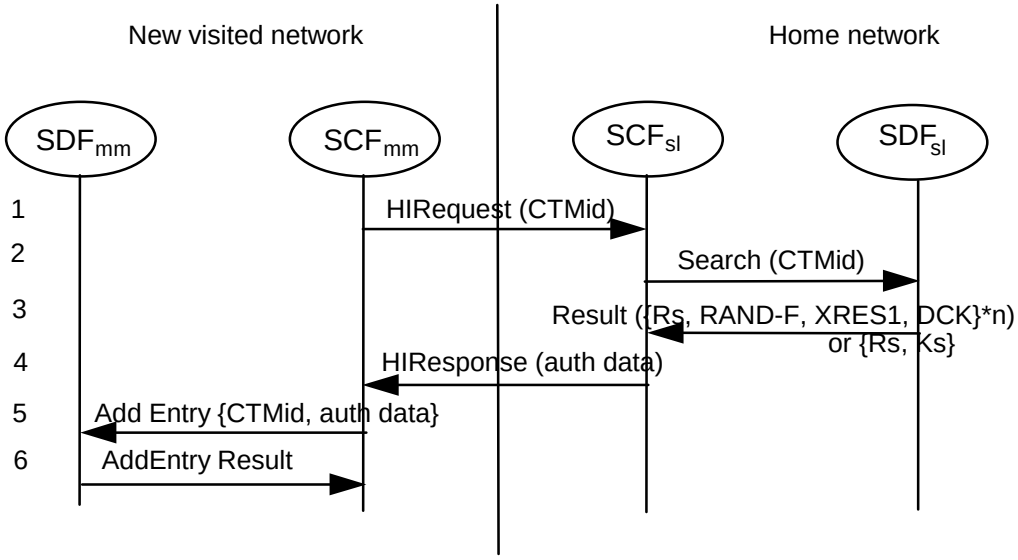
Figure 10: Functional architecture for retrieval and storage of Authentication parameters

In case of authentication performed by the visited network, the following steps are foreseen:

- The SCFmm does not find the authentication data in the SDFmm.
- The SCFmm accesses the Service Control Function (SCFsl) in the home network to retrieve the sets of data necessary to perform authentication.

The information flows shown in figure 11 describe the case where the terminal is registering in the visited network for the first time and the authentication data is not available in the visited network. It is retrieved from the home network and stored in the visited network. The procedure to retrieve and store authentication data is also invoked when the supply of parameters falls below a specified limit.

6.1.1.2 Information flows



NOTE: It has to be discussed if, from a security point of view, authentication data can be stored in the SDFmm of the visited network.

Figure 11: Information Flows for Retrieval and Storage of authorization parameters.

1 The SCFmm visited requests assistance from the home SCFsl to get authentication parameters for the given CTMid terminal.

2-3 The home SCFsl requests sets of authentication data. In case of DECT, one set of data consists of RS, RAND-F, eXpected RESponse calculated by the network (XRES1), and Derived Chipper Key (DCK). In case of CT-2, one set of data consists of X REf. entry Service (XRES) and RAND. For DECT, the SCFsl can also receive the (Rs, Ks).

4 The home SCFsl sends the authentication data to the SCFmm in the visited network

5-6 The SCFmm stores the authentication data in the visited SDFmm

6.1.2 Terminal Authentication in the Home Network

6.1.2.1 Functional architecture

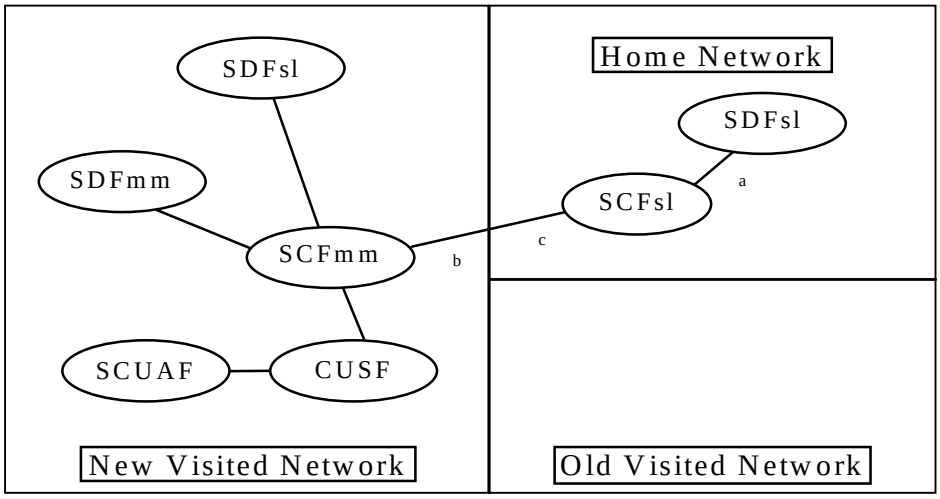


Figure 12: Functional architecture (terminal authentication)

In case of authentication performed by the home network, the following steps are foreseen:

a) the SCFsl in the home network retrieves the authentication data and executes the authentication algorithm;

b) the SCFsl in the home network access the SCFmm in the visited network to request the sending of parameters to portable terminal and the result back;

c) the a RESponse calculated by a PT (RES) is provided from the portable to the SCFsl; this last one will check the value against his result.

6.1.2.2 Information Flows - Authentication in SCFsl home

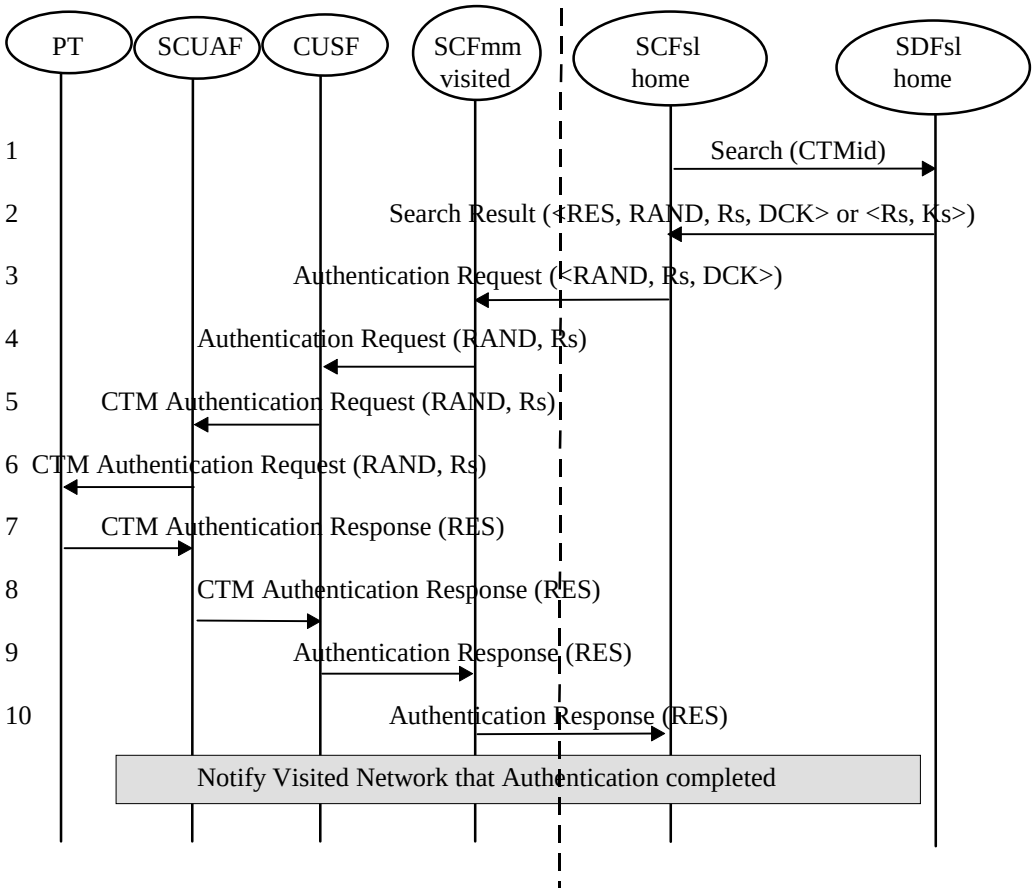


Figure 13: Information Flows (terminal authentication)

1 The SCFsl in the home network requests the SDFsl for authentication data.

2 The SDFsl provides the data needed to the SCFsl.

3 The SCFsl in the home network requests the SCFmm in the visited network to provide the result of the authentication made in the portable part; for this purpose it sends the RAND and Rs values.

4-6 The authentication data are sent from the SCFmm to the portable through the Call Unrelated Service Function (CUSF) and Service Control User Agent Function (SCUAF).

7-9 The portable sends back the result of the authentication (RES) to the SCFmm trough the SCUAF and CUSF.

10 The result is sent to the SCFsl in the home network by the visited SCFmm.

NOTE: The SCFsl home provides the information about the result of the authentication performed (here the authentication is assumed to be successfully completed).

6.2 Location registration and data deletion

The inter-networking location registration procedure is used whenever the Portable Terminal (PT) roams into a new mobility management (mm) area or a new network without a previous registration. For simplicity the procedure description and information flows are split in two sub-procedures:

1. update of CTM user location information (in the visited and home network);
2. data deletion in the previous visited network.

It is assumed hereafter that there are no requirements for agreements between the new visited network and the old visited network.

6.2.1 Functional architecture

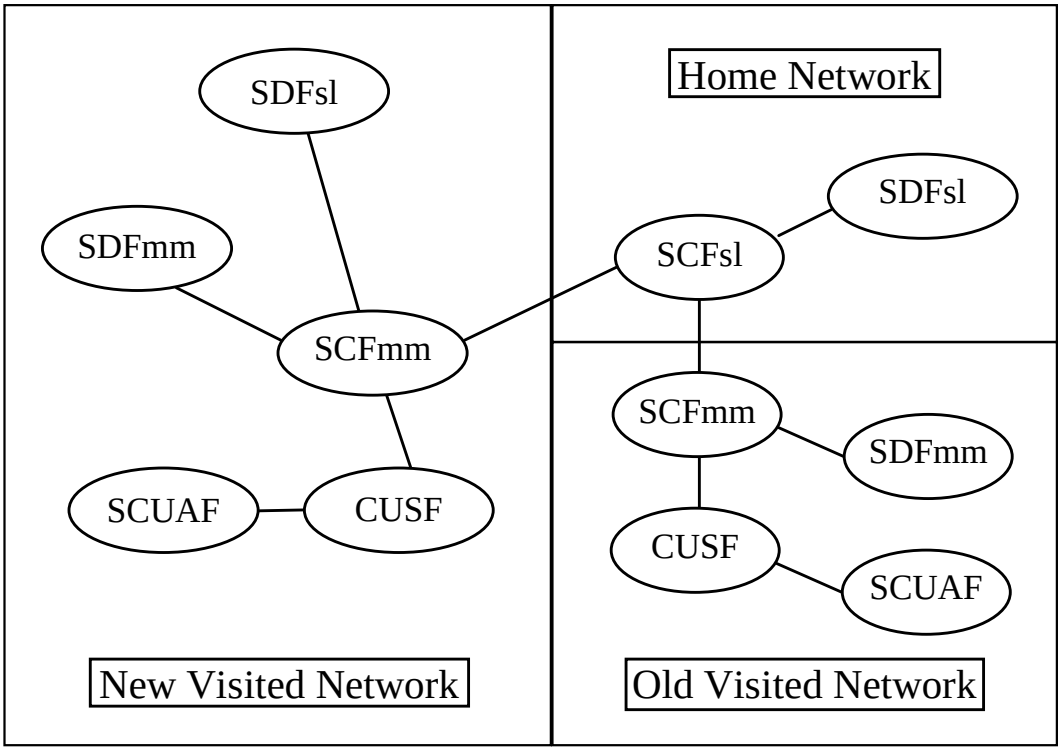


Figure 14: Functional architecture for Location Registration and Data Deletion

6.2.2 Information Flows for Location Registration

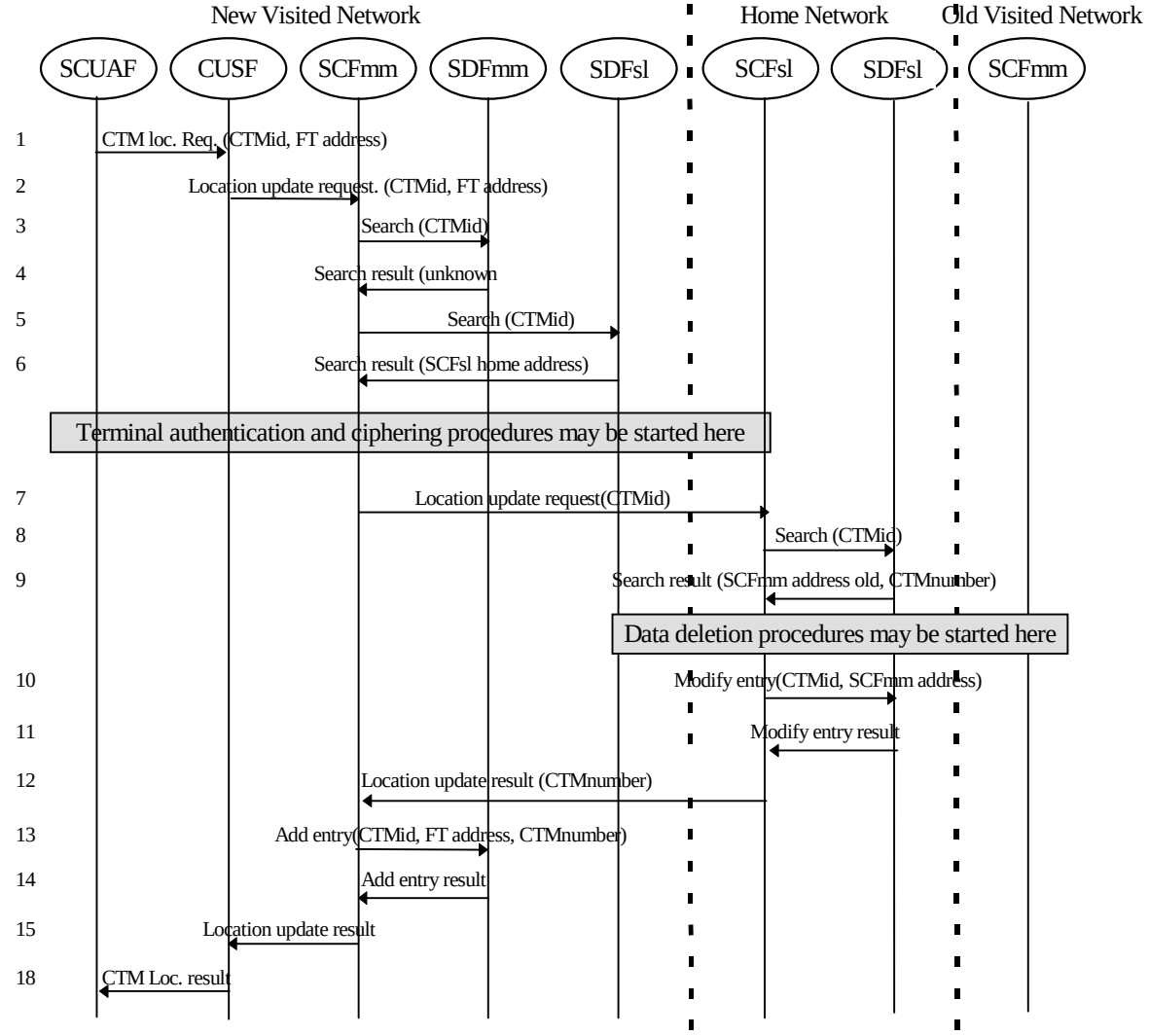


Figure 15: Information Flows for Location Registration

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

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

3 The SCFmm checks if the PT is already registered in SDFmm in a Search request based on the CTMid.

4 The PT is not already registered in the current SDFmm and a negative result is returned in the Search operation.

5-6 The SCFmm accesses the SDFsl in the visited network to retrieve the home SCFsl address and the appropriate information is returned.

7-12 The SCFmm updates the location registration data in home SCFsl. It provides the new SCFmm addresses.

13-14 The SCFmm in the visited network stores the CTMid, the FT address and the CTMnumber in SDFmm with an Add Entry message.

15-16 SCFmm sends back the location registration confirmation to the PT.

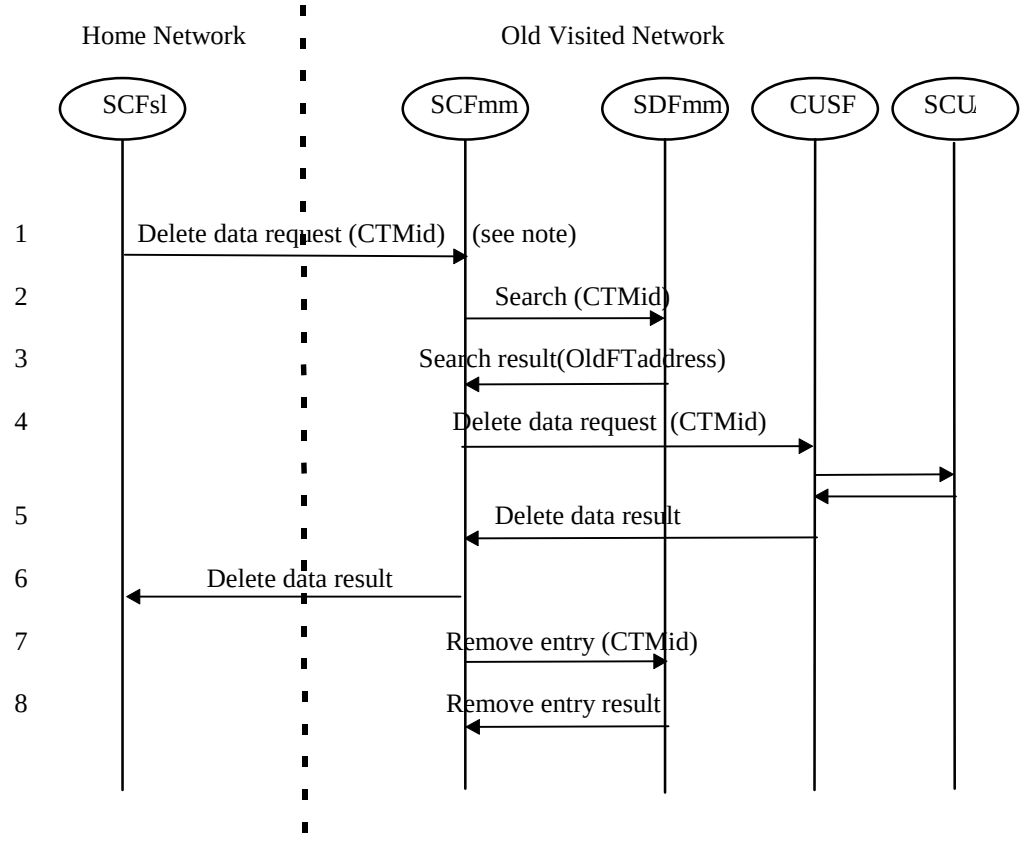
6.2.3 Information flows for data deletion in the previous visited network

This procedure is based on the generic flow for Location Registration with data deletion invoked by the Home Network. When the FT sends a non call associated message to the CUSF using a specific IN service indicator, the CUSF triggers to SCFmm the call unrelated mobility request.

a) The SCFsl in the home network requests the SCFmm in the old visited network to delete data related to CTM user.

b) The SCFmm in the old visited network accesses the SDFmm in the old visited network to delete data previously stored.

c-d) The SCFmm in the old visited network optionally deletes the data in the old SCUAF, via the old CUSF, in case the data have been optionally stored in the SCUAF.



NOTE: If this operation is supported by a TCAP Class 4 operation (result provided o nly in case of error), the flow 6 is not needed.

Figure 16: Information Flows for Data Deletion in Previous Visited Network

1 the SCFsl requests the SCFmm in the old visited network to delete the data concerning the previous CTMid registration.

2-3 the SCFmm in the old visited network requests the FT address for the CTMid and this result is passed back to the old visited SCFmm.

4-5 Optionally, if the data were stored in the SCUAF in the old visited network, the SCFmm requests this local deletion via the CUSF.

6-8 the SCFmm in the old visited network deletes the data stored in the SDFmm and this information is reported to the SCFsl in the home network.

6.3 Incoming call (roaming number case)

For the handling of incoming calls towards a CTM user a roaming number is used to route the call towards the terminating network and the related Service Switching Point (SSFt) under which the CTM user is currently located; the roaming number is therefore a temporary identifier assigned by the intelligent network to route the incoming calls: when the call arrives to the SSFt the precise location of the CTM user (i.e. the FT address) is then identified accessing the local SDFmm.

6.3.1 Geographic or portable destination number

The originating network will not be able to determine that the call is to a CTM customer and must first route the incoming call to the Home network.

6.3.1.1 Functional architecture

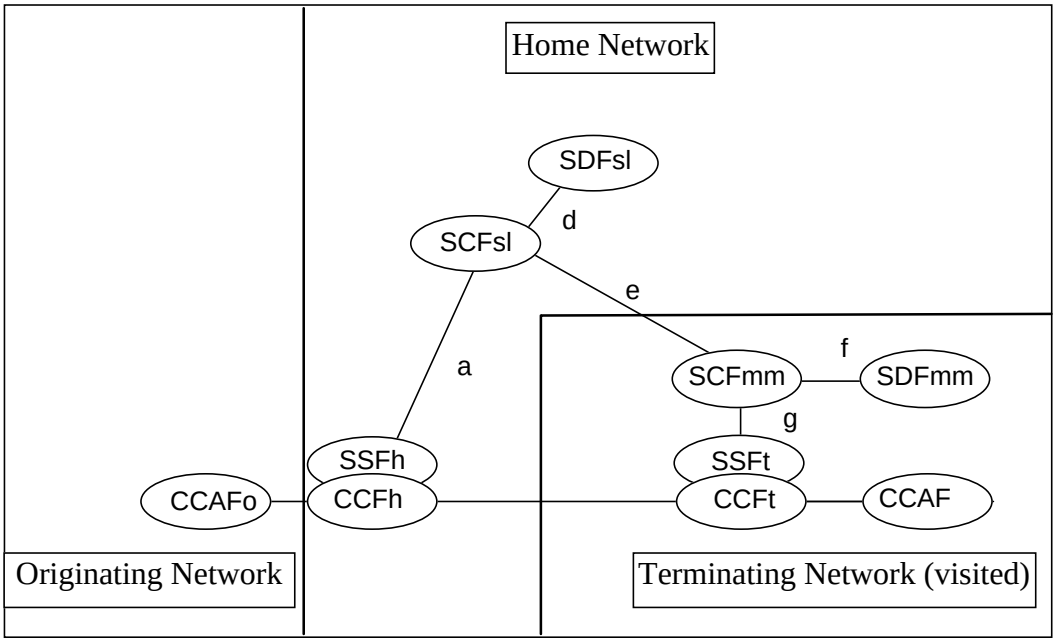


Figure 17: Functional architecture for Incoming Call (geographic number)

6.3.1.2 Information Flows

In this configuration, the information flows are a sub-case of the ones described below for the CTM Destination number case: originating and home networks are the same (home) networks, except the Call Control Agent Function (CCAF).

6.3.2 CTM Destination Number

The originating network is able to determine that the call is to a CTM customer.

6.3.2.1 Functional architecture

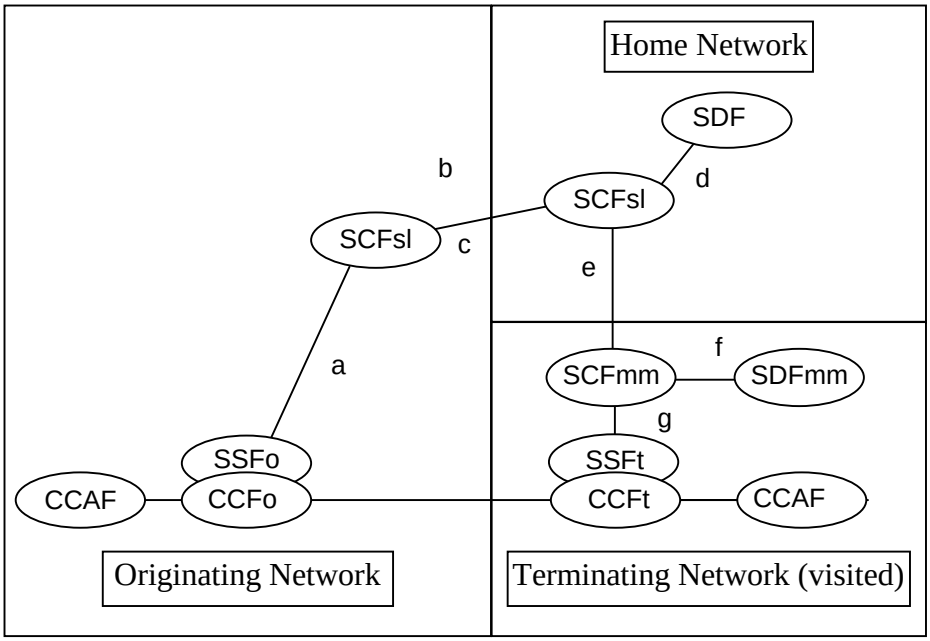


Figure 18: Functional architecture for Incoming Call (CTM destination number)

When a originating party dials the CTM number, the call is routed towards the nearest SSF, if the dialled number enables any triggering.

- The SSFo triggers the originating SCFsl.
- The SCFsl in the originating network recognizes the CTM user as belonging to another network and optionally checks the SDFsl in the home network if the home services are subscribed.
- The SCFsl interrogates the SCFsl in the home network to obtain the roaming number of CTM user.
- The SCFsl in the home network interrogates the SDFsl and retrieves the SCFmm address related to the current CTM user location.
- The SCFsl interrogates the SCFmm to obtain the roaming number.
- The SCFmm interrogates the SDFmm and provides back the roaming number; this information will be passed through the network till the SSFo. If the SSFt is not located in the LE the convey of roaming number within ISUP is needed.
- When the incoming call is offered to the visited network, the SSFt interrogates the SCFmm in order to get the FT address and the CTMid.

NOTE**:** In case of both incoming and outgoing calls, the SCFsl in the home network can instruct the SCFsl in the originating network to continue with the call when no special service logic is required to be invoked.

At any time during the call, the originating SCFsl can request assistance from the home SCFsl as soon as home specific services requests are detected".

6.3.2.2 Information Flows for Incoming Call

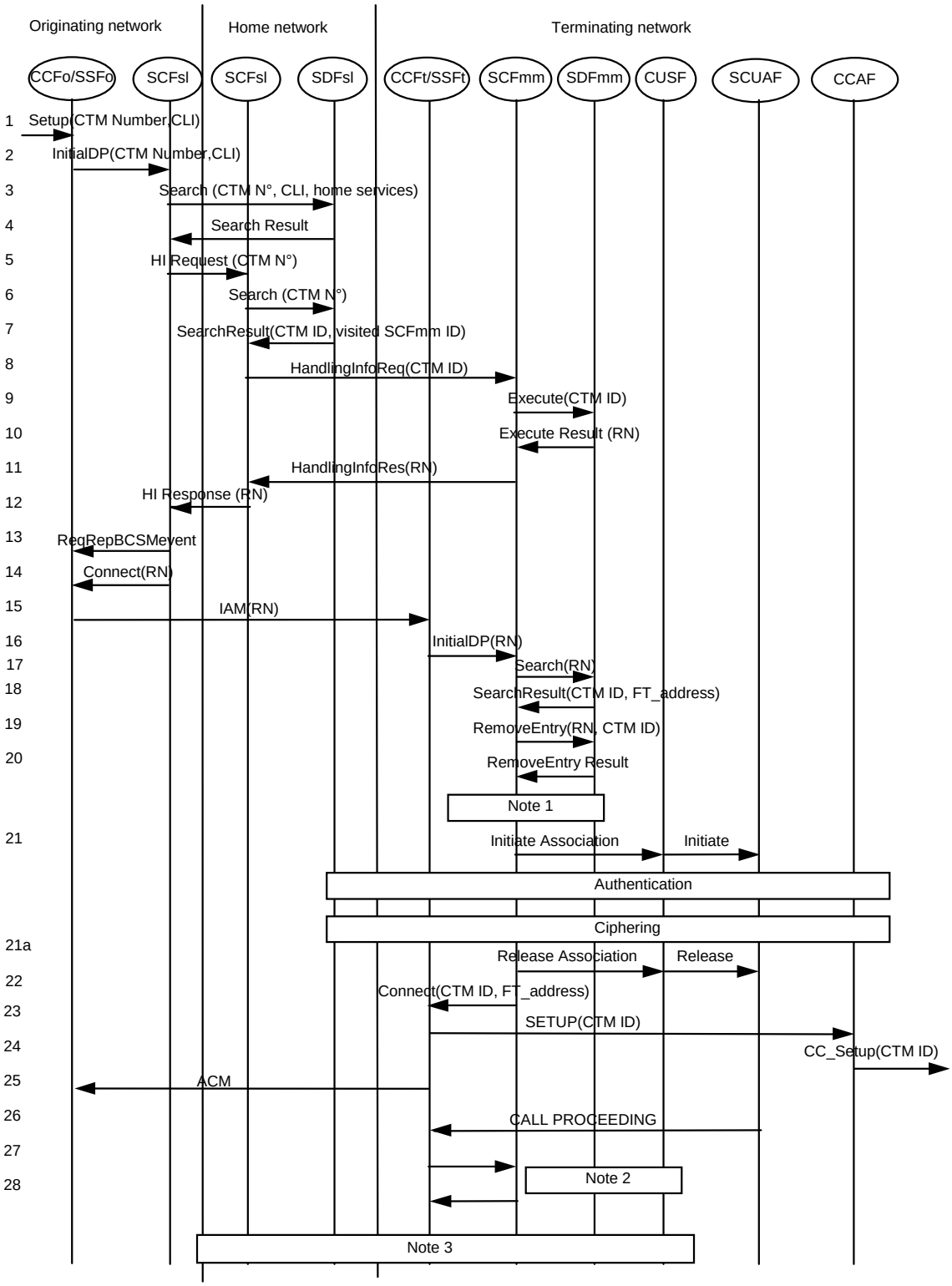


Figure 19: Information Flows for Incoming call, 1 of 2

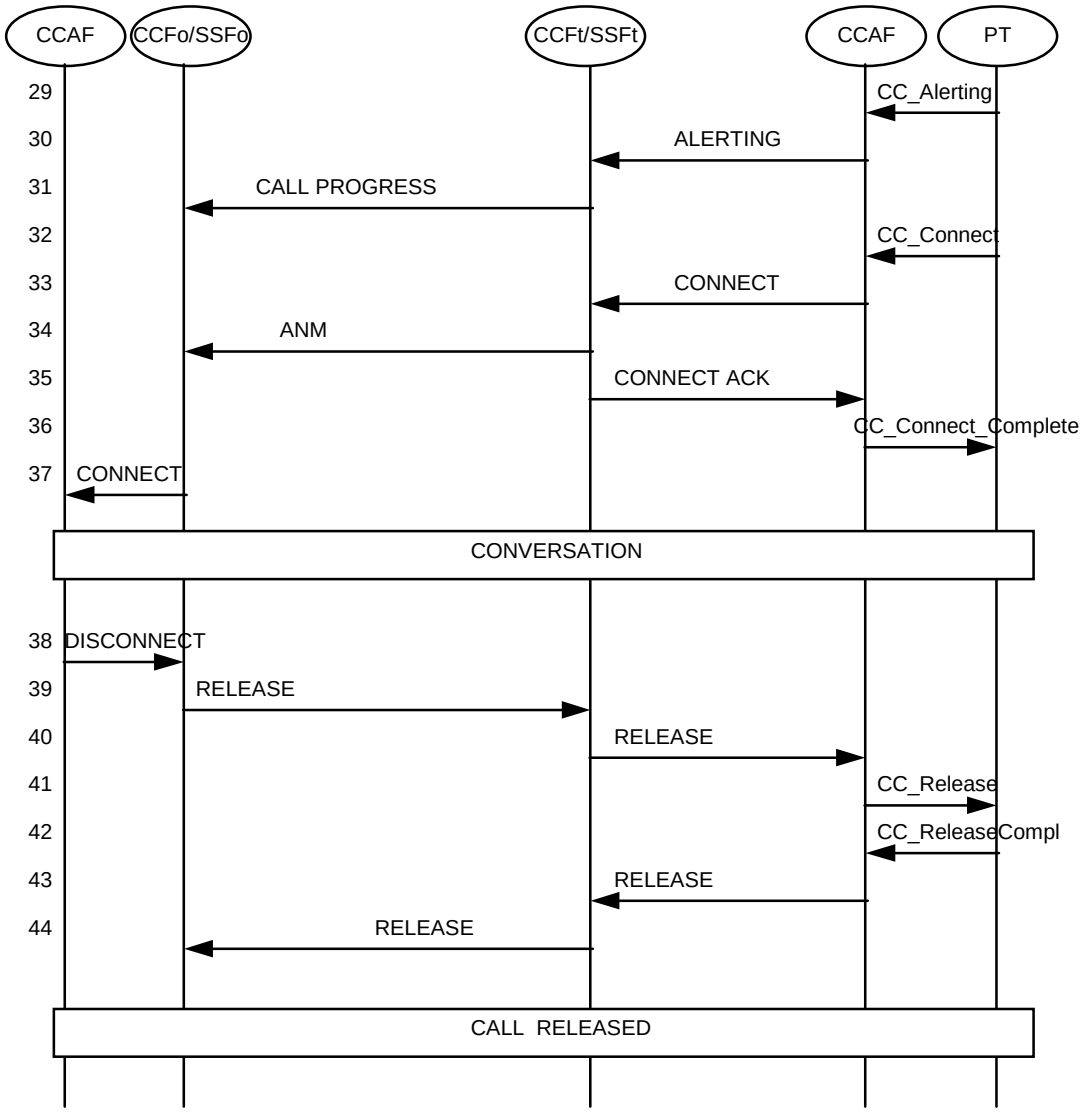


Figure 20: Information Flows for Incoming call, 2 of 2

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's choice.

NOTE 3: Optionally, SSFt triggers the terminating SCFsl to check for terminating services in the service profile in the SDFsl and possible need for supporting home specific services on the terminating side.

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

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

3, 4 The SCFsl in the originating network requests information on home specific services to the SDFslhome. The response to the query to the SDFsl home could be made of a mark in the profile of the SCFh address and of the criteria (e.g. detection points) for which this SCFh should be called (corresponding to specific services not

covered by the ETSI service description). The mark indicates that assistance service may be needed and that the stored criteria should be looked at.

In the same time, the service profile is checked.

5 the originating SCFsl request assistance from the home SCFsl in order to get a roaming number.

6, 7 The home SCFsl queries the home SDFsl in order to get the address of the visited SCFmm.

8 The home SCFsl requests assistance from the visited SCFmm to provide a Roaming Number (RN); SCFsl sends a Handing Information Request to SCFmm.

9, 10 Based on this request, the visited 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.

11 SCFmm responds to the home SCFsl with the allocated RN of the PT. To do that, SCFmm, sends a Handling Information Response message, inserting RN in the "destinationRouting Address" IE.

12 The RN is passed from the home SCFsl tothe originating SCFsl.

13, 14 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.

15 CCF/SSFo routes the call to the CCF/SSFt and provides the RN in an Initial Address Message (IAM) message.

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

17-20 The SCFmm interrogates the SDFmm to get the CTM identity (CTMid) and FT address; SCFmm also releases the roaming number and deletes it from SDFmm.

In the event of no authentication data in SDFmm, SCFmm retrieves them from home SDFsl and store them in SDFmm.

If authentication data are present in SDFmm, in DECT case they can be either (Rs, Ks) or (RANDom number issued by the network(RAND), Rs, RES). If data are present in SDFmm in CT-2 case they can only be (RAND, RES).

21 The SCFmm initiates an association with the CUSF. Authentication and ciphering may start then.

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

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

24 The FT sets up the call to the PT.

25 The CCFt/SSFt sends an early Address Complete Message (ACM) to the originating side to stop network timers.

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

27,28 Some correlation may be needed between call processing and authentication result from the terminating SCFmm. (Operator's choice).

29-37 Normal call set up procedure.

38-44 Release phase, initiated from called party.

NOTE: If no Initial DP is received by SCFmm a logic timeout in the Single Link Procedure (SLP) causes SCFmm to delallocate and delete RN in SDFmm.

6.4 Outgoing call

The inter-networking outgoing call procedure is used whenever a PT that is roaming in a visited network initiates an outgoing call. It is assumed that location registration of the visiting PT with the home network has preceded the outgoing call attempt.

NOTE: "Check home service outgoing call status" checks whether barring applies to the outgoing call attempt.

6.4.1 Functional architecture

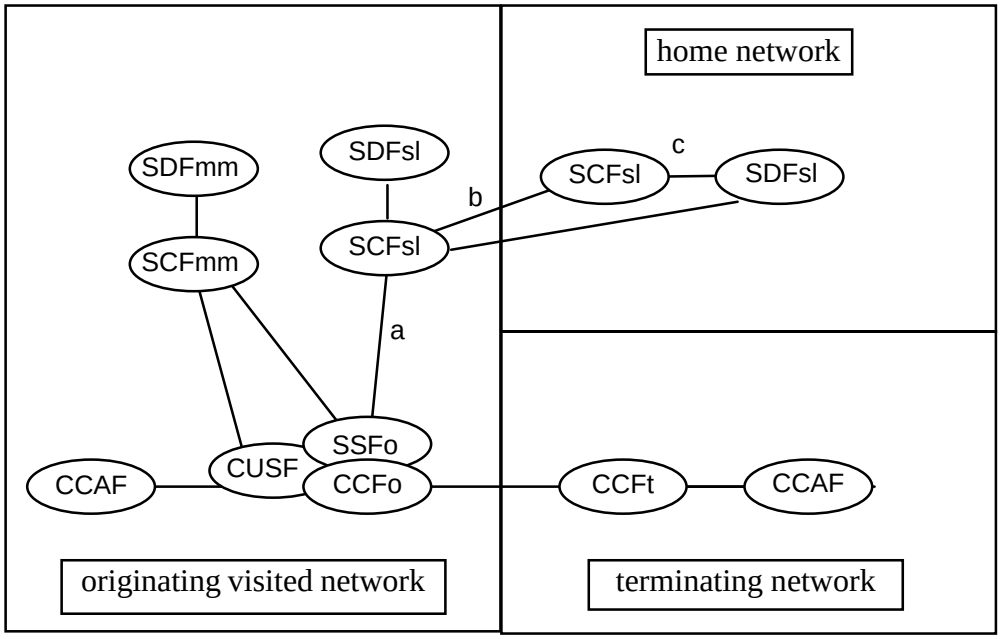


Figure 21: Functional architecture for Outgoing Call

When the CTM user makes an outgoing call, this is triggered by the SSF at the originating side; the following actions will be performed:

a) after authentication and ciphering by the the SCFmm, the SSF triggers the SCFsl in the originating network;

b) for the purpose of supporting home based services the SCFsl in the originating network accesses the SDFsl in the home network. The service profile is checked in the same time. This check can also be processed through the SCFsl-SCFsl interface.

At any time during the call, the originating SCFsl can request assistance from the home SCFsl as soon as home specific services requests are detected.

6.4.2 Information Flows

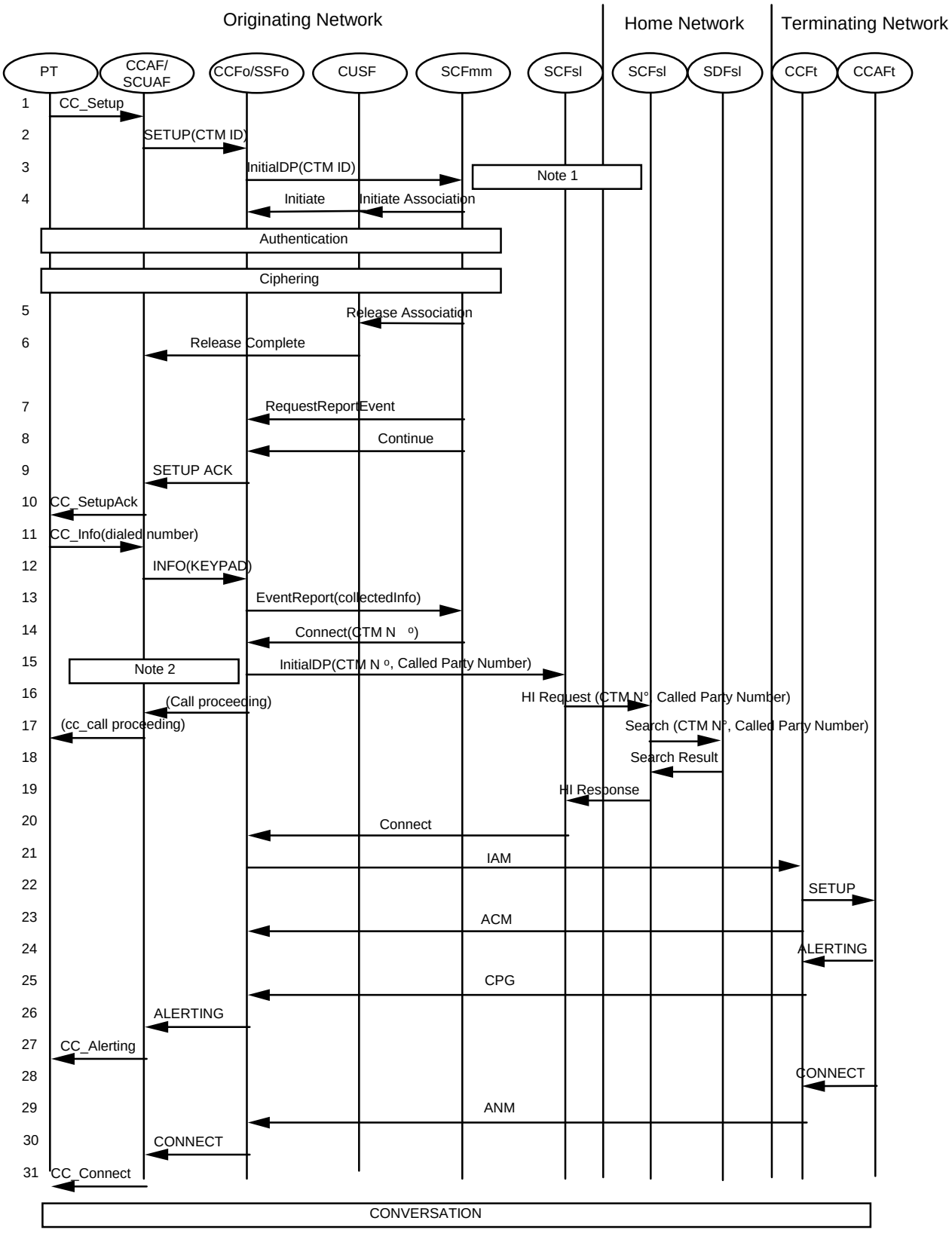


Figure 22: Information Flows for Outgoing Call (establishment of the call by the PT)

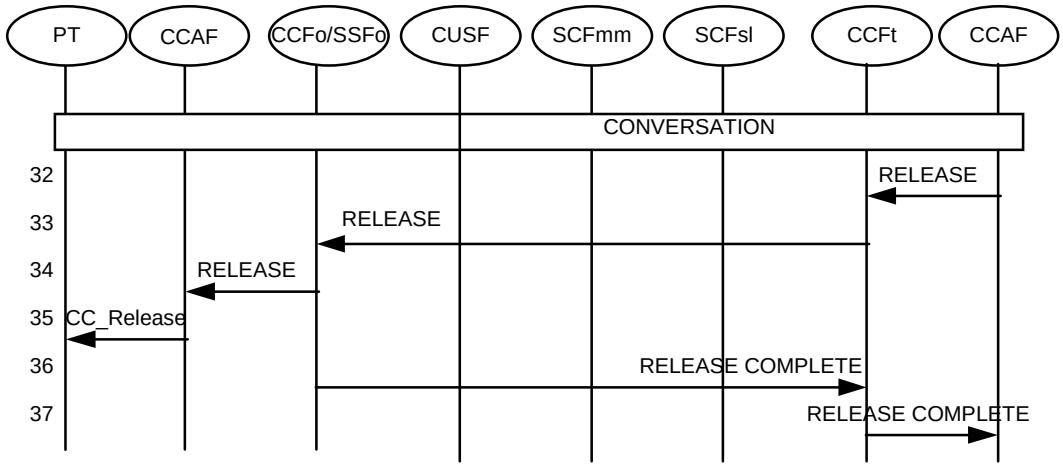


Figure 23: Information Flows for Outgoing Call (Release of the call bu the network)

NOTE 1: Authentication and ciphering may be processed in parallel with call setup. If processed in sequence then it could be necessary to restart the setup timer in FT and PT.

NOTE 2: If it is an emergency call then the authentication result is ignored and the call continues without SCFsl triggering (flows 16 to 19).

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.

Note: if the call can not be triggered in CCFo/SSFo, it is routed to the CCF/SSF to which the CTM user's subscription is associated and where triggering occurs.

4 SCFmm initiates an association with CUSF. Authentication and ciphering may start here.

5,6 The call unrelated association is released.

7 SCFmm request the report of the collected information event.

8 SCFmm orders the CCFo/SSFo to continue call setup.

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 a Connect inorder to identify the calling CTM User.

15 The SSFo triggers the SCFsl to ask for services.

16-19 SCFsl request assistance from the home SCFsl to check the service profile (e.g. restrictions on called party number) and get information on the support of home specific services.

20 The originating SCFsl orders CCFo/SSFo to route the call (based on the called party number).

21-31 CCFo/SSFo routes the call accordingly and receives backward signaling. The connection is established.

32- 37 Release phase; here initiated from called party.

7 Core Features based on SCF-SDF, SCF-SCF and SDF-SDF Relations

7.1 Terminal Authentication

This subclause provides the functional architecture and information flows for call unrelated terminal authentication which can be performed in either the visited network or in the home network.

Terminal authentication is performed in the visited network following the intra-network procedure described in EG NA61302 -1. When location registration is being performed for the first time in a new visited network, or the supply of authentication parameters falls below a pre-set threshold, authentication parameters are downloaded from the Home Network and stored in the SDFmm.

7.1.1 Retrieval and storage of authorization parameters

During a location registration in a new visited network, or when the supply of authorization parameters falls below a specified limit, a process is initiated to retrieve and store more authorization parameters.

7.1.1.1 Functional architecture

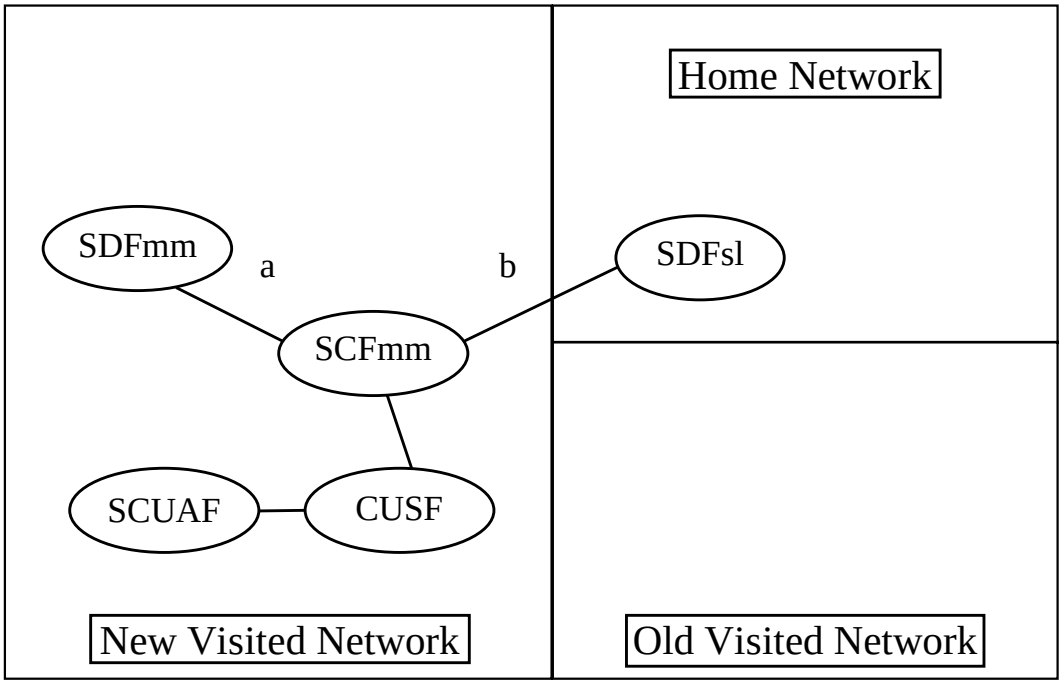


Figure 24: Functional architecture(retrieval and storage of authorization parameters)

In case of authentication performed by the visited network, the following steps are foreseen:

a) the SCFmm does not find the authentication data in the SDFmm;

b) the SCFmm accesses the SDFsl in the home network to retrieve the sets ofdata needed and performs authentication.

In this case of call unrelated terminal authentication for DECT, two cases are actually envizaged, depending on the operations invoked on the SCFmm-SDFsl (home) interface: in fact, in case of use of a Search operation, the authentication data retrieved include the fixed values Rs and Ks, while in case of use of Execute operation, the authentication data include RES, Rs and RAND values.

7.1.1.2 Information flows

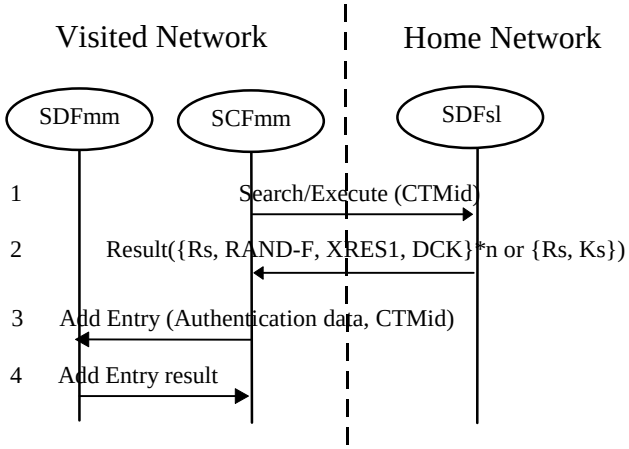


Figure 25: Information Flows for retrieval and storage of authorization parameters

NOTE: It has to be discussed if, from a security point of view, authentication data can be stored in the SDFmm of the visited network.

1 The SCFmm visited requests sets of authentication data. In case of DECT, one set of data consists of RS, RAND-F, XRES1, and DCK. In case of CT-2, one set of data consists of XRES and RAND. For DECT, the SCFsl can also receive the (Rs, Ks).

2 The home SDFsl sends back the authentication data to the SCFmm in the visited network.

3-4 The SCFmm stores the authentication data in the visited SDFmm.

7.1.2 Terminal Authentication in the Home Network

This subclause provides the functional architecture and information flows for call unrelated terminal authentication which can be performed in either the visited network or in the home network.

7.1.2.1 Functional architecture

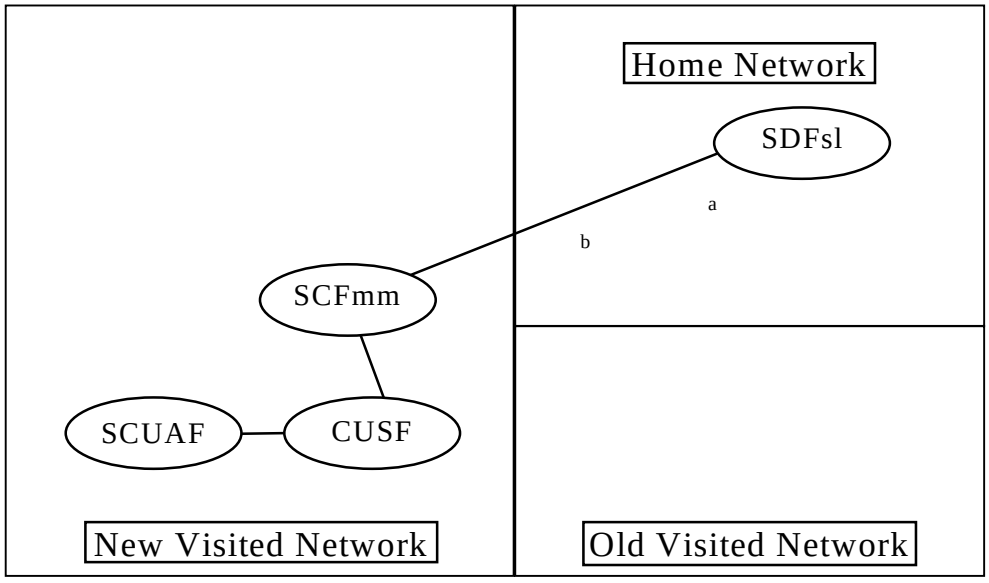


Figure 26: Functional architecture (Terminal Authentication)

In case of authentication performed by the home network, the following steps are foreseen:

a) the visited SCFmm provides SDFsl home with the authentication parameters;

b) the authentication algorithm is processed by the home network and the result sent back to the visited network.

7.1.2.2 Information Flows - Authentication in SDFsl home

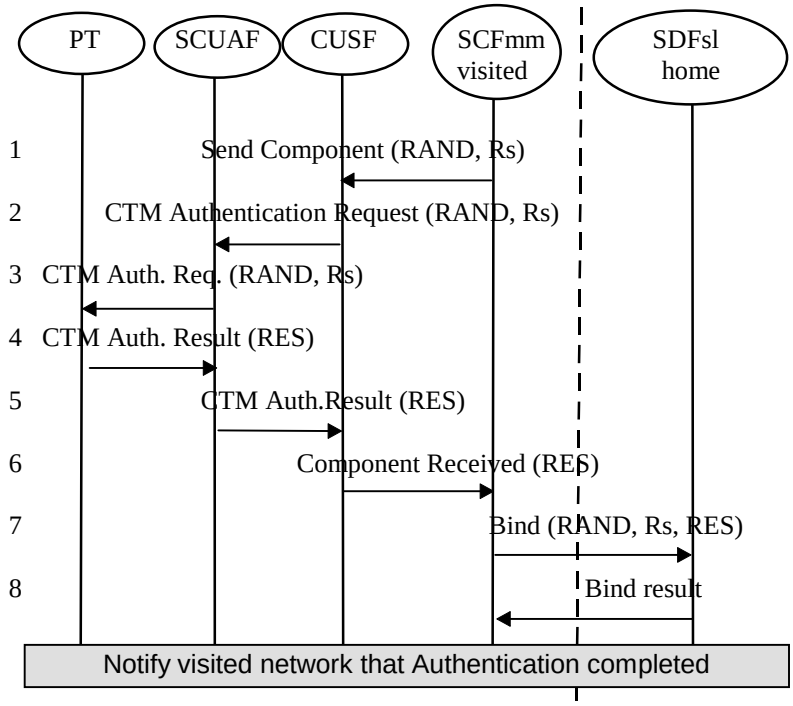


Figure 27: Information Flows (Terminal Authentication)

1-3 The authentication data are sent from the SCFmm to the portable through the CUSF and SCUAF

4-6 The portable sends back the result of the authentication (RES) to the SCFmm trough the SCUAF and CUSF

7-8 The Bind operation is invoked in case of authentication performed by the SDFsl in the home network

NOTE: The SCFsl provides the information about the result of the authentication performed (here the authentication is assumed to be successfully completed).

7.2 Location registration and data deletion

The inter-networking location registration procedure is used whenever the PT roams in a new mm area or in a new visited network without a previous registration.

The approach to location registration and data deletion described in this section are for the case where the Service Control Point (SCP) in the visited network is the controlling element and there is a requirement for agreement between the old visited and new visited network operators for deletion of obsolete location data. In this case, the request to delete Location Registration data is generated by the New-Visited Network and passed directly to the Old-Visited network without the intervention of the Home Network.

Iin the following subclauses the Service profile transfer during location registration is not yet addressed (this feature if used will require a SDFsl-SDFsl interface).

7.2.1 Functional architecture for Location Registration

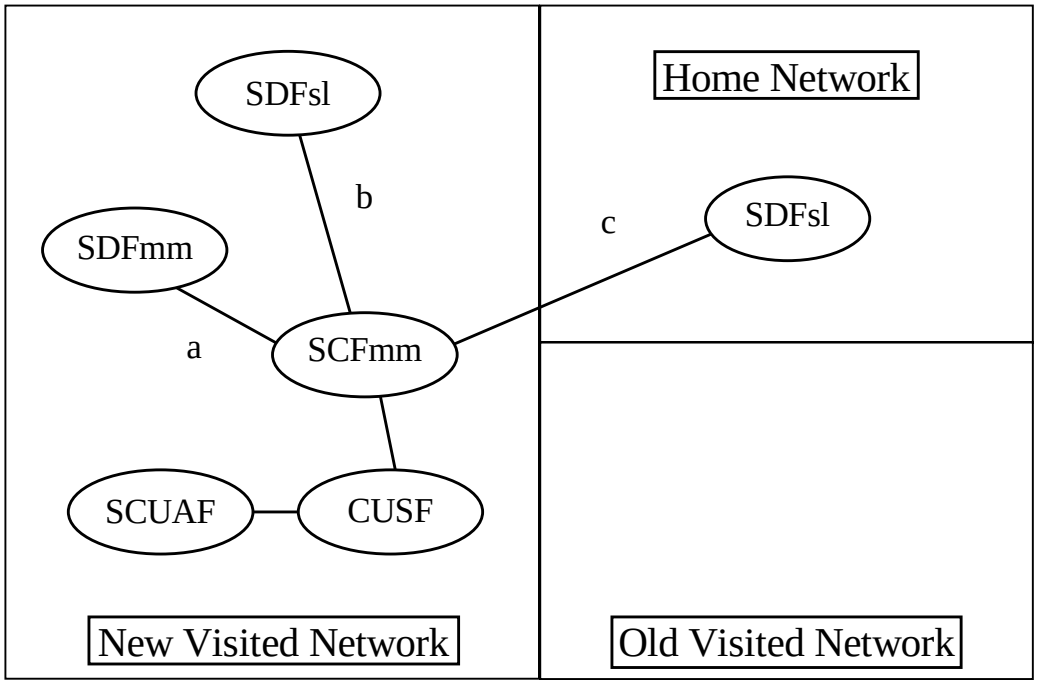


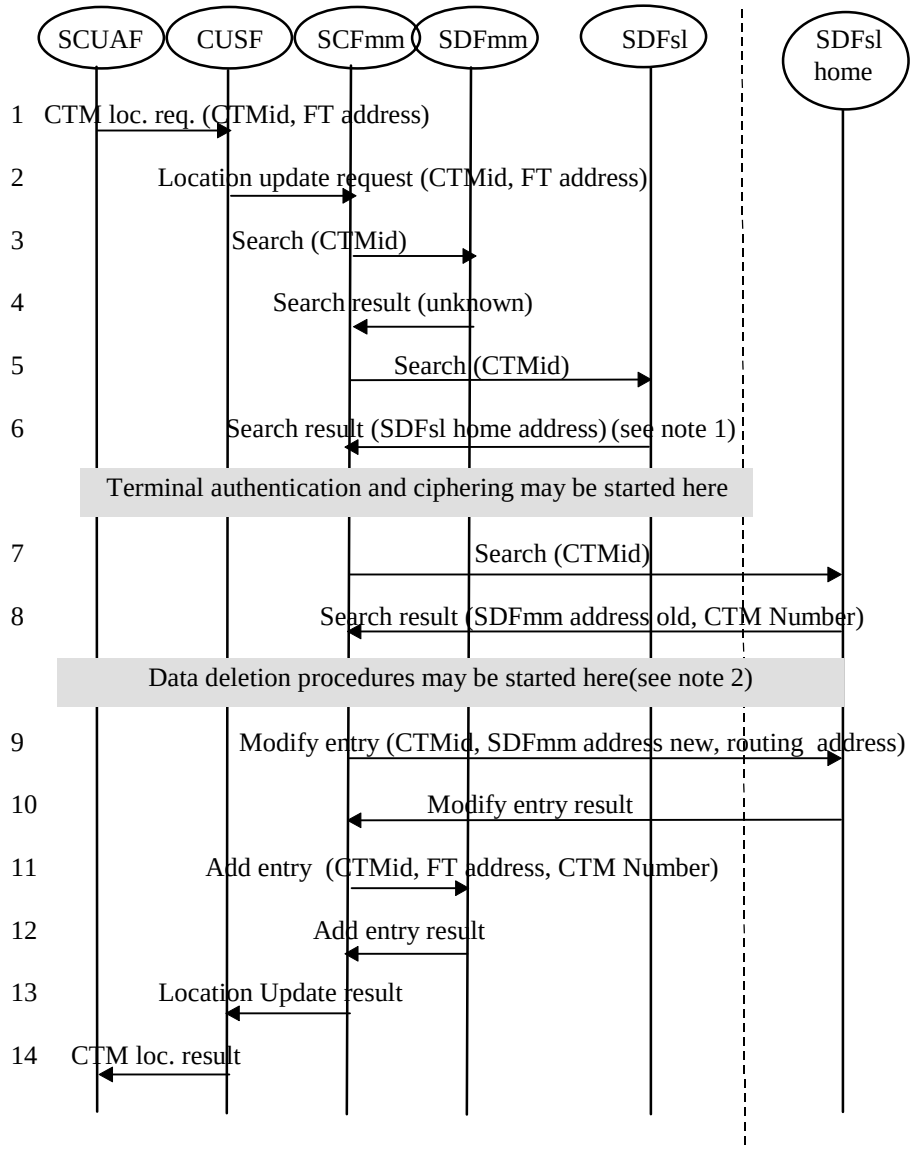
Figure 28: Functional architecture (Location Registration)

a) The SCFmm in the visited network looks for the terminal data in the local SDFmm.

b) If the location registration is performed for the first time, the SCFmm has to ask the SDFsl in the same network about the home network addresses to be used to get information about the new CTM user.

c) The SCFmm in the visited network provides to the SDFsl in the home network the new location information of the CTM user.

7.2.2 Information Flows for Location Registration



NOTE 1: It has to be clarified if the CTM id can include information about the routing towards the relevant SDF; in this case the SDF/SCF addresses are not needed.
NOTE 2: Data deletion in the old network can start in parallel with data modification in the visited network.

Figure 29: Information Flows (Location Registration)

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 CUSF sends a call unrelated Update_Location Request message to the SCFmm, including the CTMid of the PT and the FT address.

3 SCFmm checks if the PT is already registered in SDFmm in a Search request including CTMid. Depending on the result there are two cases (lines 4a or 4b).

4 The PT is not already registered in the current SDFmm and a negative result is returned in the Search operation.

5-6 The SCFmm accesses the SDFsl in the visited network to retrieve the home SDFsl address.

7-8 The SCFmm accesses the SDFsl in the home network to retrieve the SDFmm address of the previous visited network and the CTM Number.

9-10 The SCFmm updates location registration data in home SDFsl. It inserts the new SDFmm address, if roaming number method will apply for incoming call. The routing address is stored instead of the SDFmm address when the routing address method is used.

11-12 SCFmm stores the CTMid, the CTM Number and the FT address in SDFmm with an Add Entry message.

13-14 SCFmm sends back the location registration confirmation to the PT.

NOTE: The SCFsl provides the information about the result of the authentication performed (here the authentication is assumed to be successfully completed).

7.2.3 Data deletion in the previous visited network

The following figure shows the main relationships identified for data deletion across network boundaries; the different possibilities identified in figure 5 are detailed in the three cases analysed in this subclause.

7.2.3.1 Functional architecture for data deletion

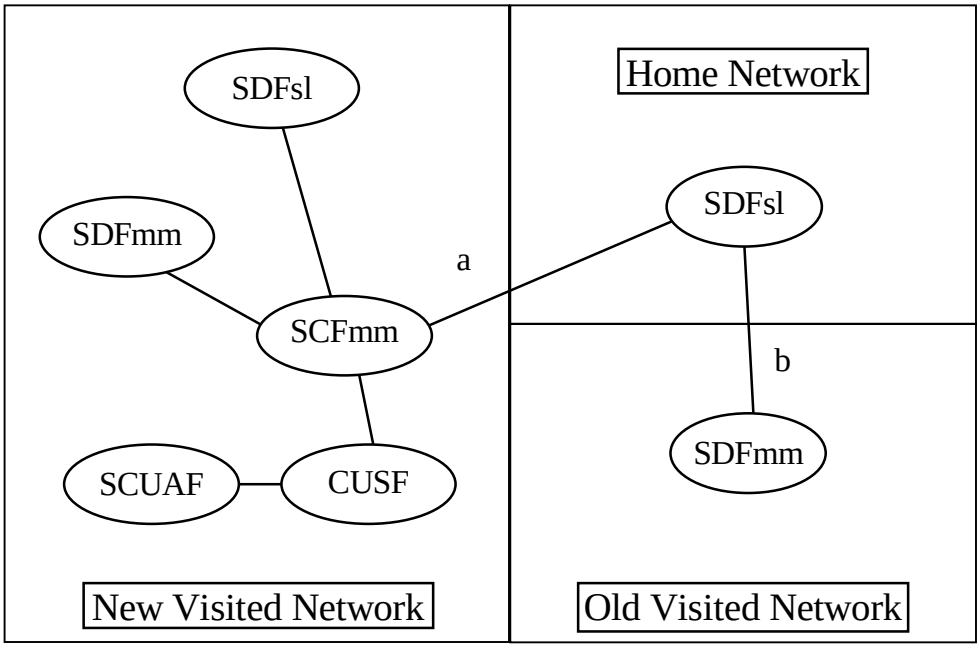


Figure 30: Functional architecture (no agreement between new and old networks)

When the FT sends a non call associated message to the CUSF using a specific IN service indicator, the CUSF triggers to SCFmm the call unrelated mobility request.

a) the SCFmm asks the SDFsl in the home network process location data deletion in the old visited SDFmm. No confirmation is expected from the new visited network;

b) location data deletion is done via the SDF-SDF relationship.

7.2.3.2 Information Flows for data deletion

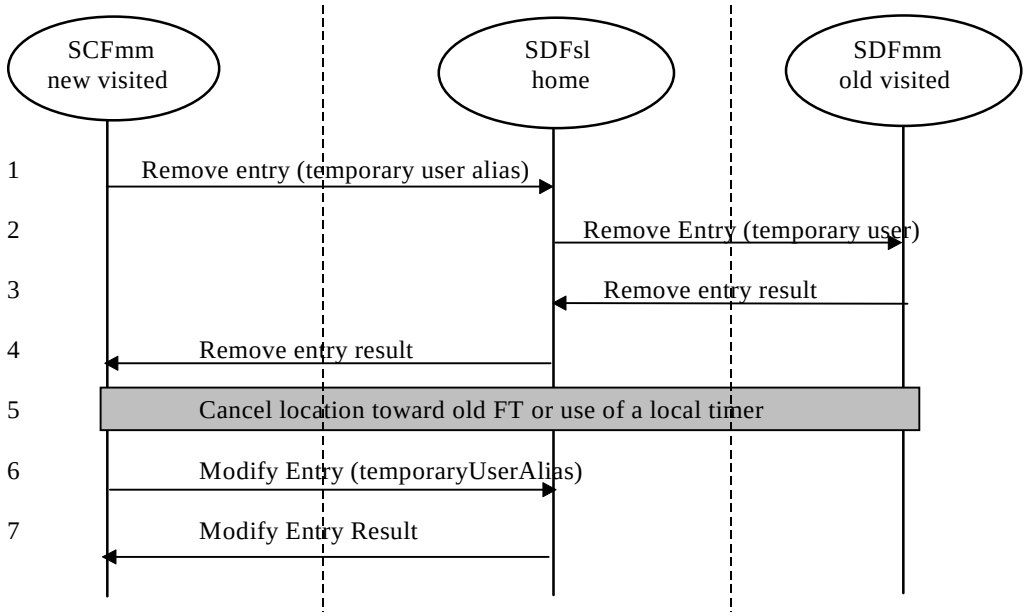


Figure 31: Information flows (no agreement between new and old visited networks)

1 The new SCFmm sends a "Remove Entry" operation to the SDFsl in the home network, with the following arguments:

object: The destination number of the entry of class temporaryUserAlias stored in the SDFsl;

servicecontrol: dontDereferenceAliases=FALSE.

2-3 The SDFsl dereferences the received DN to the DN contained in the aliasedEntryName attribute of the alias entry. The request is then chained to the old visited network using fixed knowledge references based on the analysis of the initial levels of the DN (e.g. country code, service provider code)

4 The result of Remove Entry is provided to SCFmm in the new visited network.

5 In the case when location data are stored in the SCUAF, the SCFmm optionally cancels terminal data from old SCUAF (if included in the agreements) or the data will be deleted on the basis of a local timer expiring.

6-7 The SCFmm modifies the aliasedEntryName of the alias entry by replacing the current value by the DN of the temporary entry created in the new SDFmm (dontDereferenceAliases=TRUE).

7.3 Incoming call

7.3.1 Geographic or portable destination number

The originating network will not be able to determine that the call is to a CTM customer and must first route the incoming call to the Home network.

7.3.1.1 Functional architecture

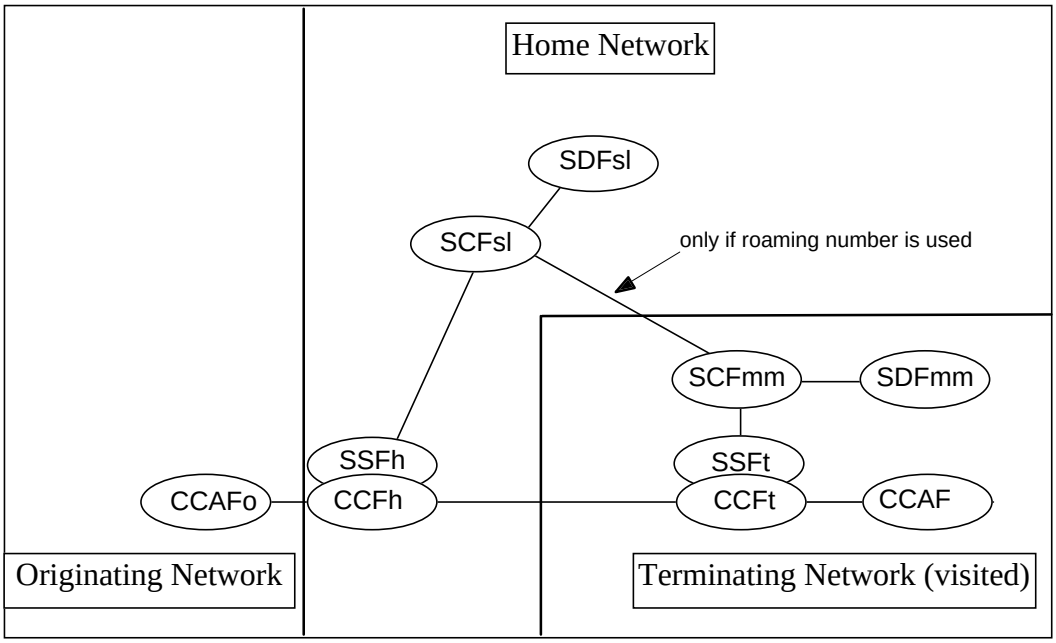


Figure 32: Functional architecture for Incoming Call (geographic number)

7.3.1.2 Information Flows

In this configuration, the information flows are a sub-case of the ones described in subclause 7.3.2 for the CTM Destination number case: originating and home networks are the same (home) networks, except the CCAFo.

7.3.2 CTM destination number - Roaming Number

The example described here is based on the Generic information flow for an Incoming Call to a CTM user.

For the handling of incoming calls towards a CTM user, two cases have been envisaged from the network perspective:

- The use of a roaming number to route the call towards the terminating network and the related SSFt under which the CTM user is currently located; the roaming number is therefore a temporary identifier assigned by the intelligent network to route the incoming calls: when the call arrives to the SSFt the precise location of the CTM user (i.e. the FT address) is then identified accessing the local SDFmm.

- The use of CTM Number and routing address to route the incoming call towards the terminating network; in this case these information are retrieved before to route the call through the network boundary and have to be carried on the access/network protocols conform to White Book specifications.

7.3.2.1 Functional architecture (Roaming Number case)

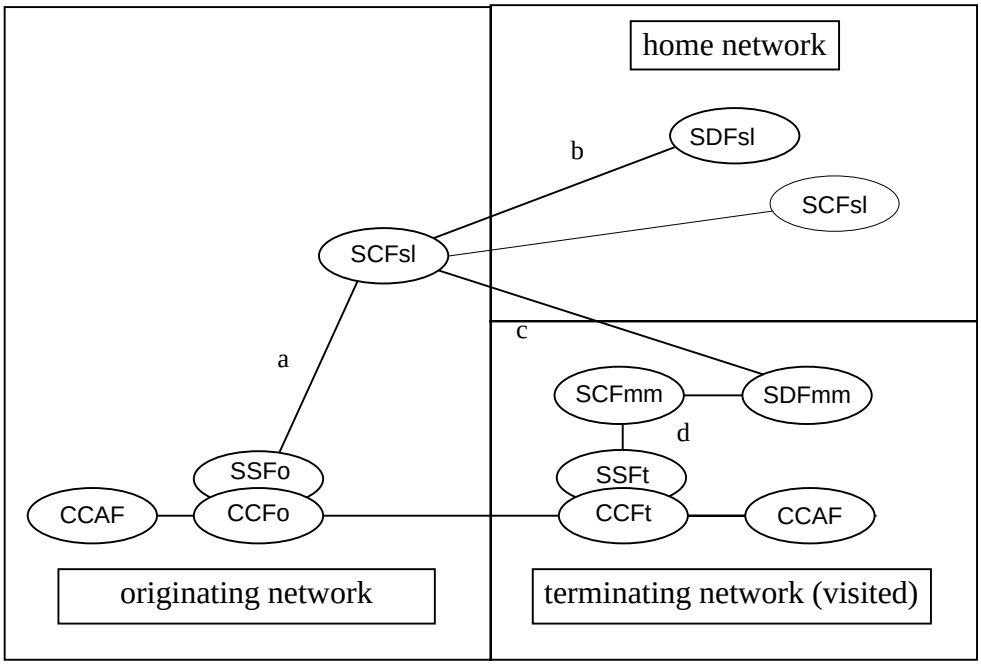


Figure 33: Functional architecture (roaming number case)

When a originating party dials the CTM number, the call is routed towards the nearest SSF, if the dialled number enables any triggering.

a) The SSFo triggers the originating SCFsl.

b) The SCFsl in the originating network recognizes the CTM user as belonging to another network and optionally checks the SDFsl in the home network if the home services are subscribed. The SCFsl retrieves the address of the visited SDFmm.

c) The SCFsl interrogates the SDFmm in the visited network to obtain the roaming number of CTM user. This information will be passed through the network to the SSFo. If the SSFt is not located in the LE, ISUP is needed to convey of roaming number within the network.

d) When the incoming call is offered to the visited network, the SSFt interrogates the SCFmm in order to get the roaming number.

At any time during the call, the originating SCFsl can request assistance from the home SCFsl as soon as home specific services request are detected.

7.3.2.2 Information Flows (roaming number case)

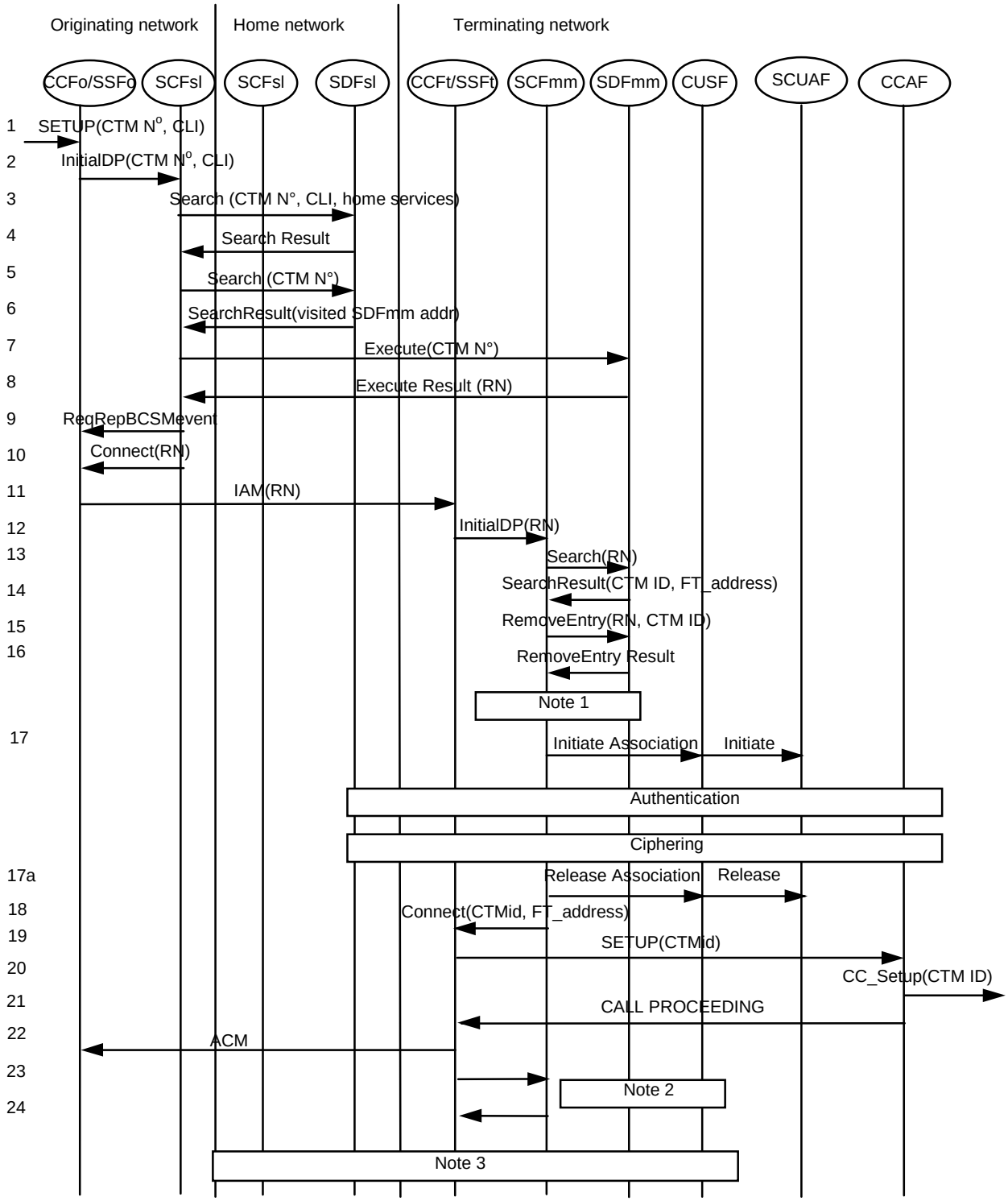


Figure 34: Information Flows for Incoming call (1 of 2)

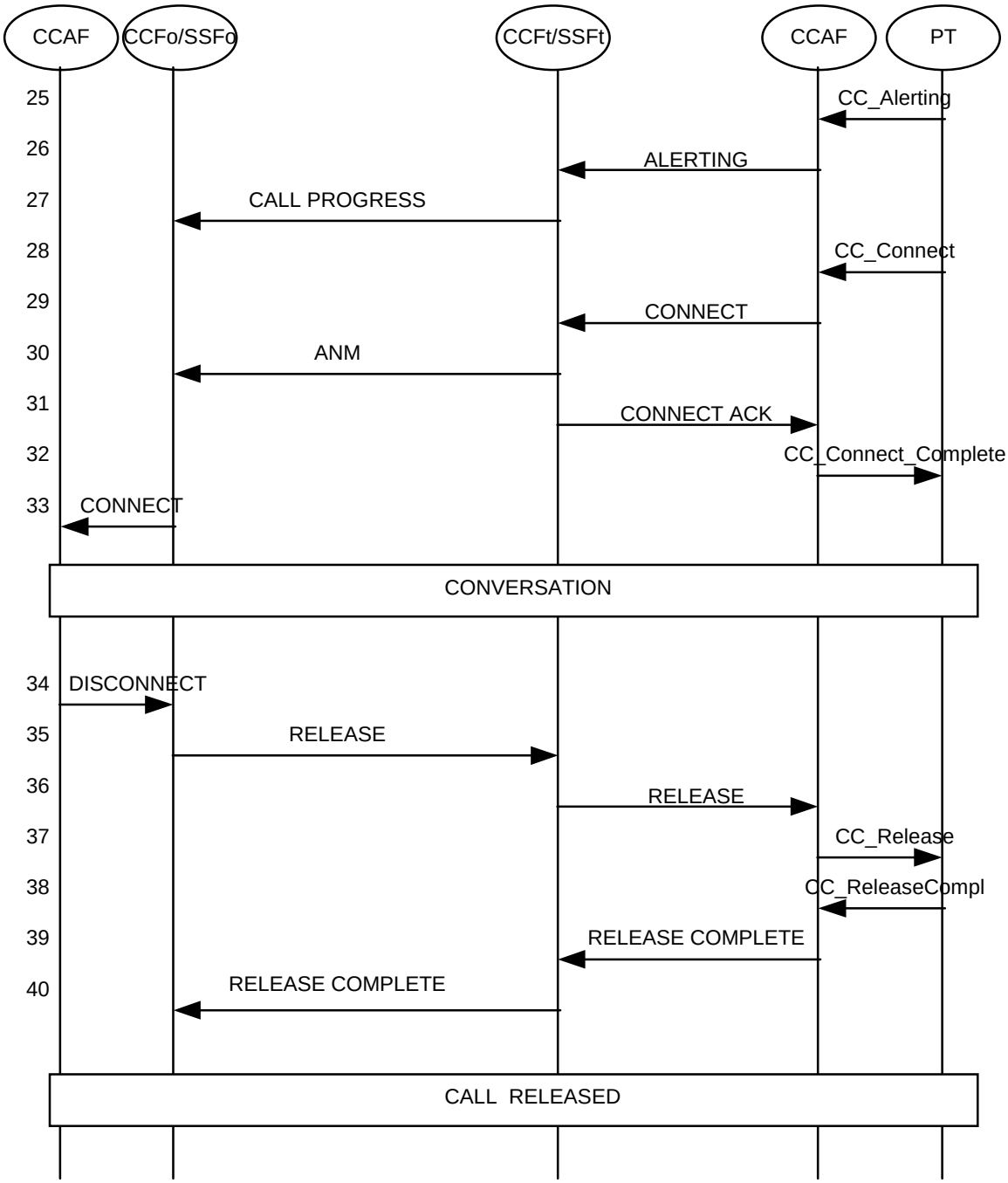


Figure 34: Information Flows for Incoming call (2 of 2)

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's choice).

NOTE 3: Optionally, SSFt triggers the terminating SCFsl to check for terminating services in the service profile in the SDFsl and possible need for supporting home specific services on the terminating side.

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 DP is recognized by the CCF/SSFo which,on recognition of a CTM N°, sends a InitialDP message, containing the CTM N° and the Calling Line Identity, to the appropriate SCFsl.[1]

3, 4 The SCFsl in the originating network requests information on home specific services to the SDFslhome. The response to the query to the SDFsl home could be made of a mark in the profile of the SCFh address and of the criteria (e.g. detection points) for which this SCFh should be called (corresponding to specific services not covered by the ETSI service description). The mark indicates that assistance service may be needed and that the stored criteria should be looked at.

In the same time, the service profile is checked.

5; 6 The originating SCFsl queries the home SDFsl in order to get the address of the visited SDFmm.

7, 8 The originating SCFsl queries the visited SDFmm to get a roaming number for the user; the visited SDFmm 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.

9, 10 The originating 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 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.

In the event of no authentication data in SDFmm, SCFmm retrieves them from home SDFsl and store them in SDFmm.

If authentication data are present in SDFmm, in DECT case they can be either (Rs, Ks) or (RAND, Rs, RES). If data are present in SDFmm in CT-2 case they can only be (RAND, RES).

17 The SCFmm initiates an association with the CUSF. Authentication and ciphering may start then.

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

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

20 The FT sets up the call to the PT.

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

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

23,24 Some correlation may be needed between call processing and authentication result from the terminating SCFmm (Operator's choice).

25-33 Normal call set up procedure.

34-40 Release phase, initiated from called party.

NOTE: If no InitialDP is received by SCFmm a logic time-out in the SLP causes SCFmm to de-allocate and delete RN in SDFmm.

7.3.3 CTM destination number - Routing Number case

7.3.3.1 Functional architecture (Routing Address Case)

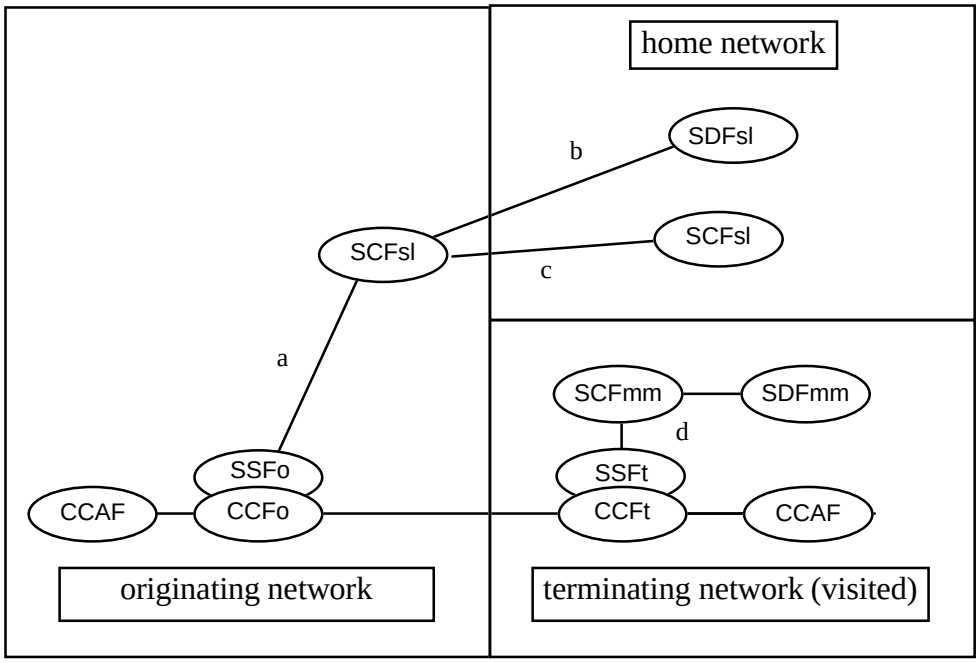


Figure 35: Functional architecture (routing address case)

When a calling user makes a call towards a CTM user, this is triggered in the originating network, if IN capabilities are available. In this case the following actions are performed:

a) the SSF in the originating network triggers the SCFsl;

b) the SCFsl in the originating network queries the SDFsl in the home network to retrieve the routing address, check service profile and get information on home specific services;

c) At any time during the call, the originating SCFsl can request assistance from the home SCFsl as soon as home specific services request a re detected;

d) the SCFmm in the terminating network queries the SDFmm in order to retrieve CTMid and FTaddress.

7.3.3.2 Information Flows for Incoming Call (Routing Address case)

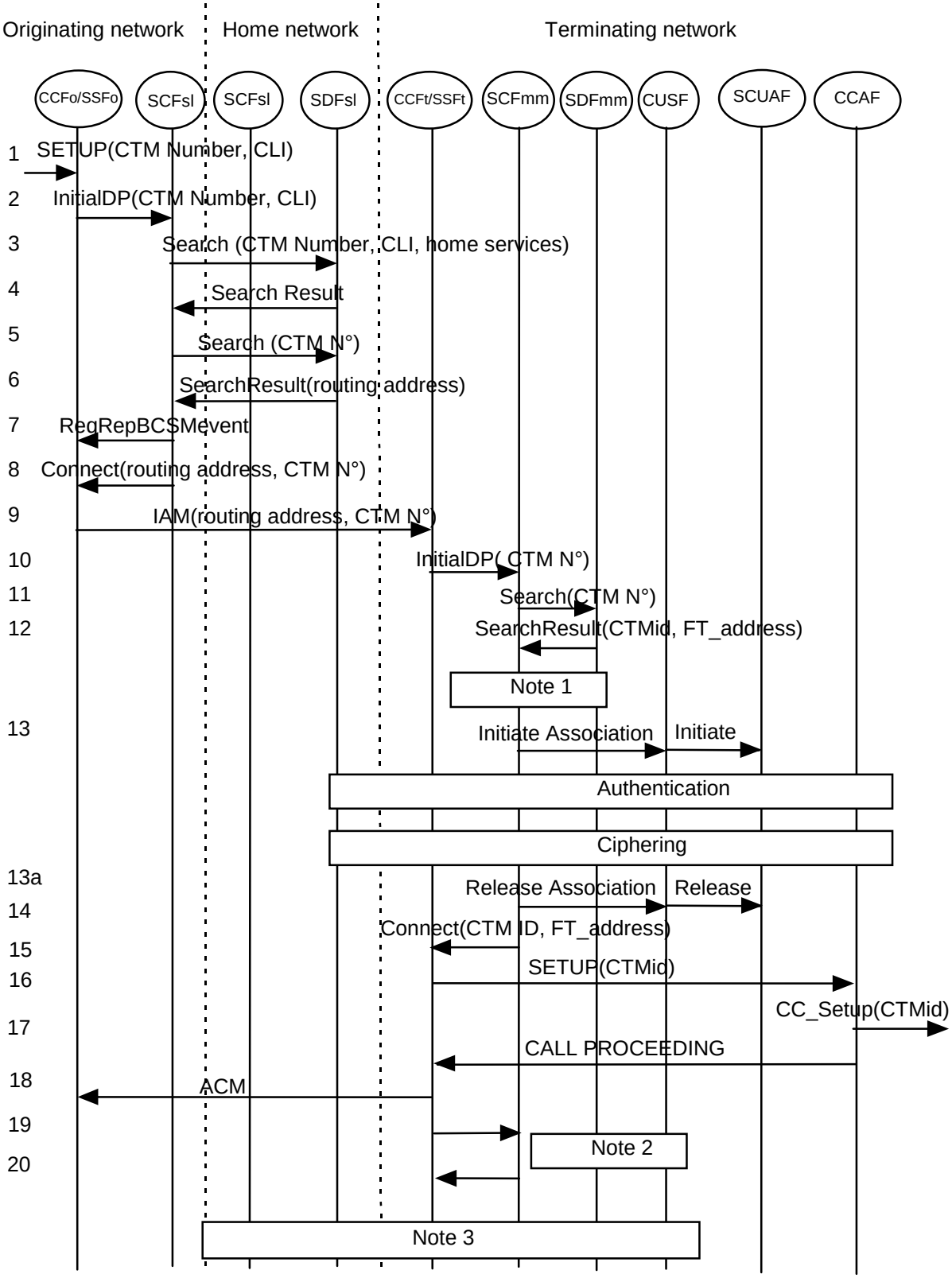


Figure 36: Information Flows (Routing address case), (1 of 2)

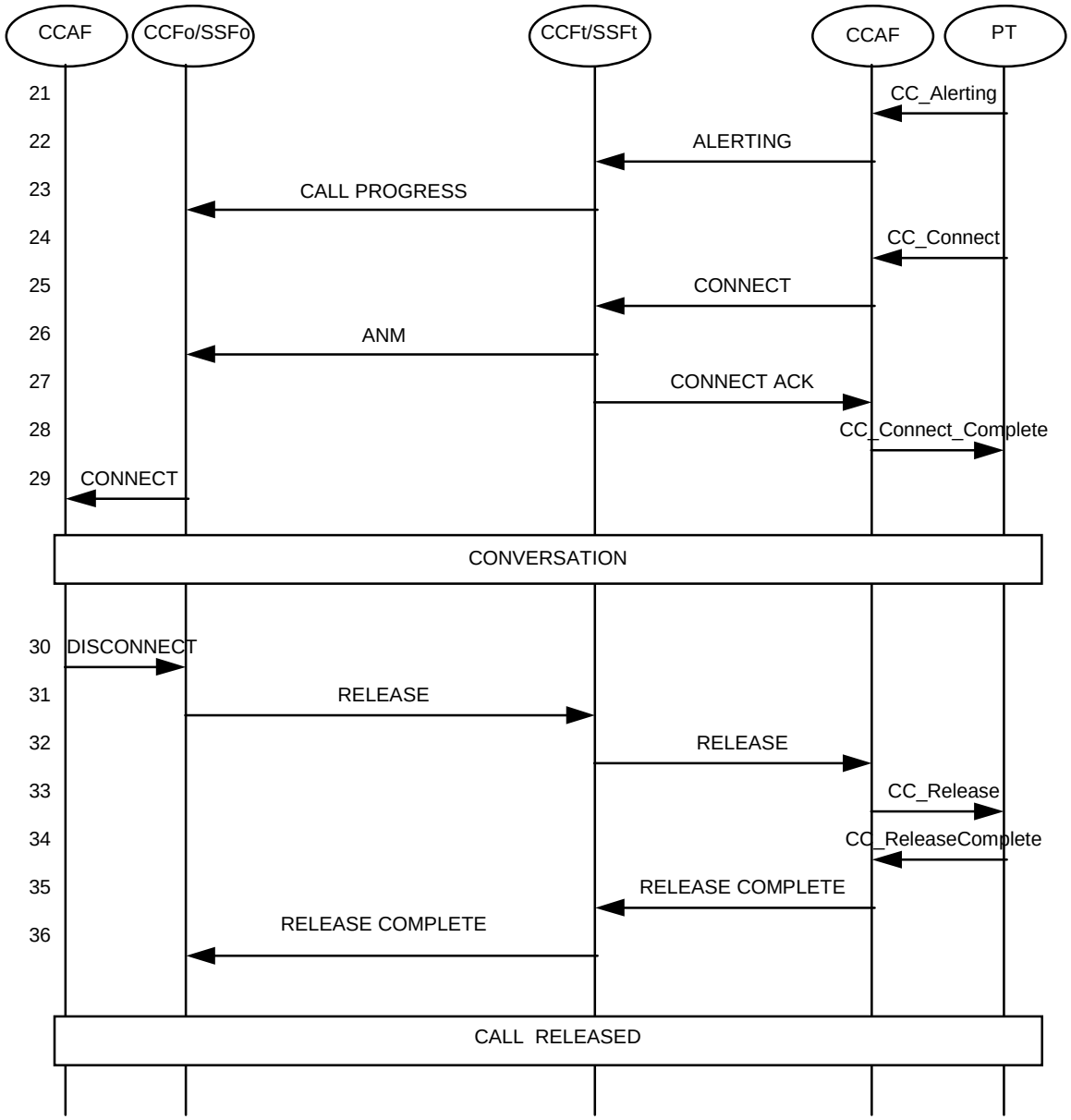


Figure 36: Information Flows (Routing address case) (2 of 2)

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's choice).

NOTE 3: Optionally, SSFt triggers the terminating SCFsl to check for terminating services in the service profile in the SDFsl and possible need for supporting home specific services on the terminating side.

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. The TDP criteria are on a per service base. The way used to route the query to the SCFsl is network dependant.

3, 4 The SCFsl in the originating network requests information on home specific services to the SDFslhome. The

response to the query to the SDFsl home could be made of a mark in the profile of the SCFh address and of the criteria (e.g. detection points) for which this SCFh should be called (corresponding to specific services not covered by the ETSI service description). The mark indicates that assistance service may be needed and that the stored criteria should be looked at.
In the same time, the service profile is checked.

5, 6 The originating SCFsl retrieves from home SDFsl the routing address.

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

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

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

10 The SSFt triggers the terminating/visited SCFmm to retrieve the CTM ID and FT address from SDFmm.

11, 12 SCFmm retrieves CTM ID and FT address from SDFmm

13 SCFmm initiates a call unrelated association with CUSF. Authentication and ciphering may start here.

14 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.

15,16 CCFt sets up the call to the PT via FT, providing also the CTMid.

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

18 The CCF/SSFt sends an early Adress Complete Message to the originating side to stop network timers.

19-20 Optionally, SSFt triggers the SCFsl to check for terminating services in the service profile.

21-29 Normal call set up procedure.

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

7.4 Outgoing call

The inter-networking outgoing call procedure is used whenever a PT that is roaming in a visited network initiates an outgoing call. It is assumed that location registration of the visiting PT with the home network has preceded the outgoing call attempt.

NOTE: "Check home service outgoing call status" checks whether barring applies to the outgoing call attempt.

7.4.1 Functional architecture for Outgoing Call

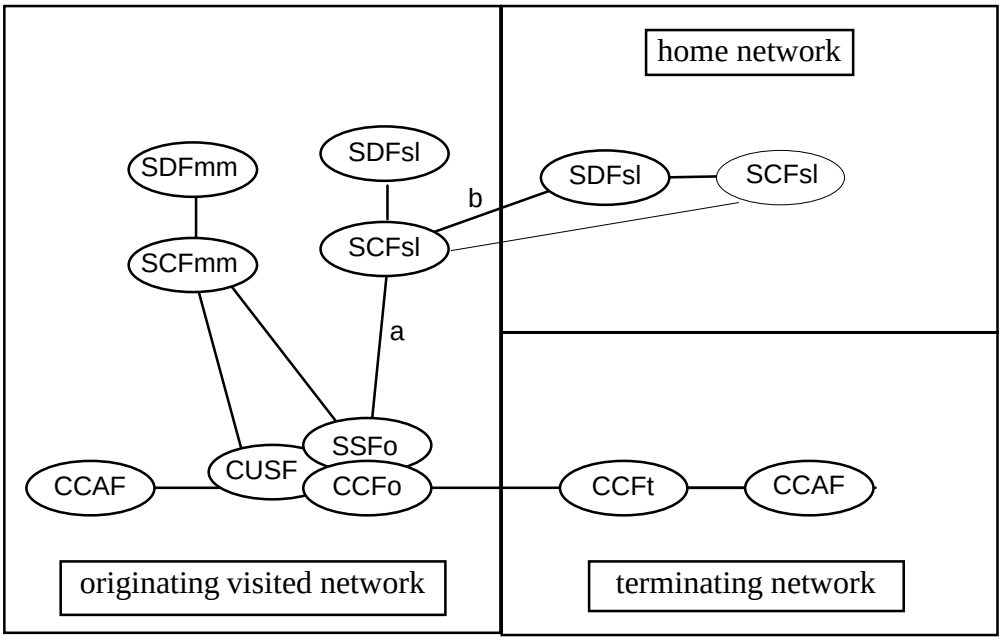


Figure 37: Functional architecture for outgoing call

When the CTM user makes an outgoing call, this is triggered by the SSF at the originating side; the following actions will be performed:

a) after authentication and ciphering by the the SCFmm, the SSF triggers the SCFsl in the originating network;

b) for the purpose of supporting home based services the SCFsl in the originating network accesses the SDFsl in the home network. The service profile is checked in the same time.

At any time during the call, the originating SCFsl can request assistance from the home SCFsl as soon as home specific services requests are detected.

7.4.2 Information Flows for Outgoing Call

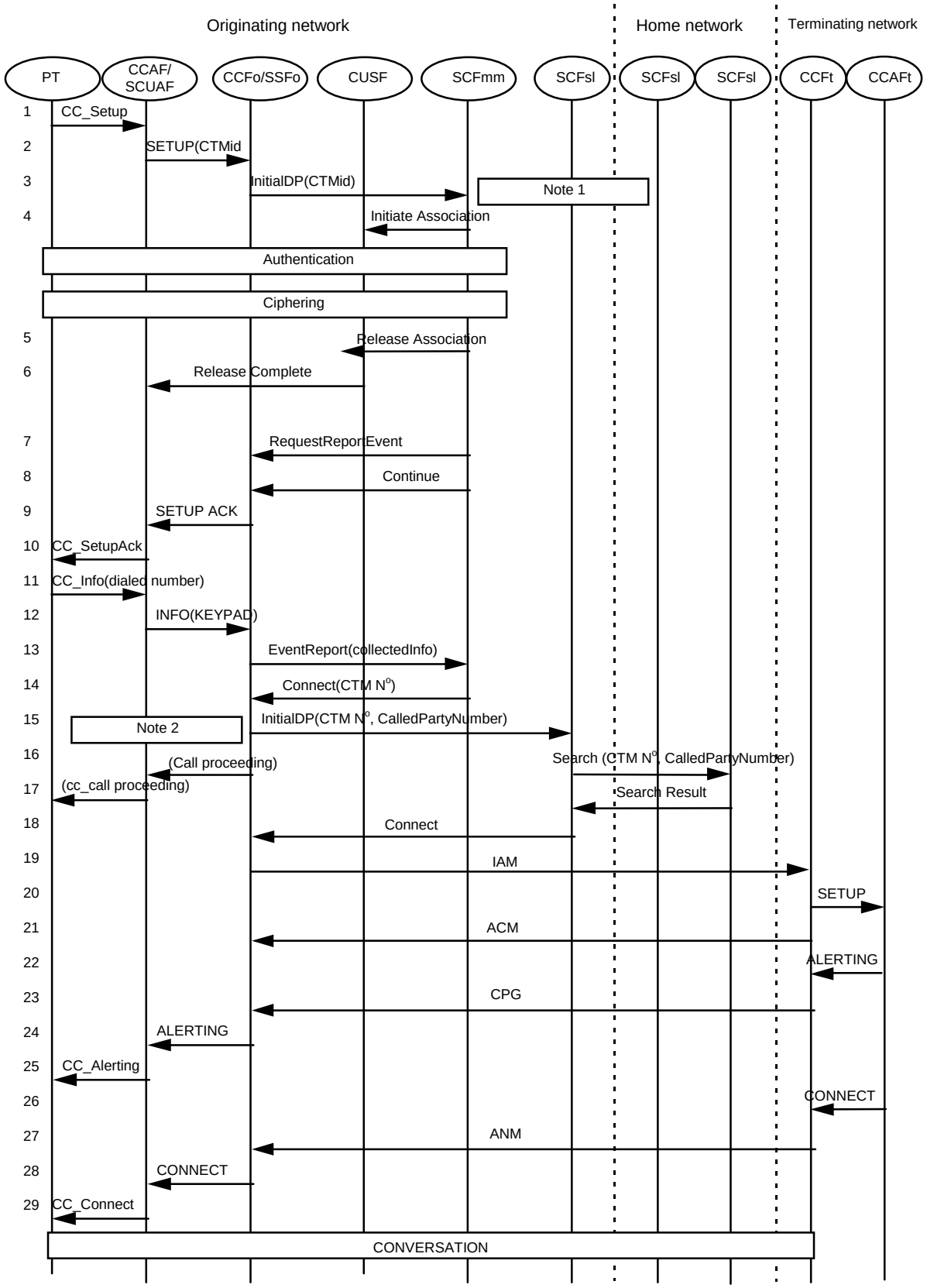


Figure 38: Information Flows for outgoing call, (1 of 2)

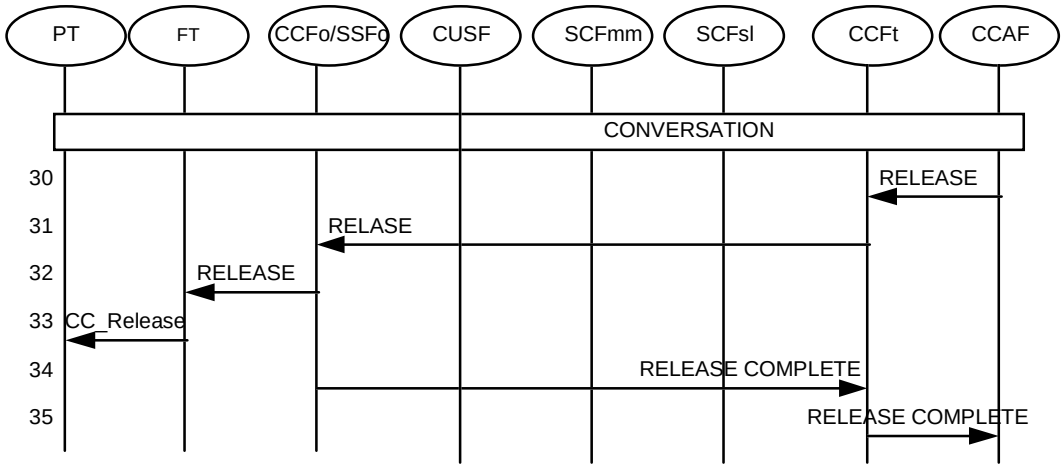


Figure 38: Information Flows for outgoing call, (2 of 2)

NOTE 1: Authentication and ciphering may be processed in parallel with call setup. If processed in sequence then it could be necessary to restart the setup timer in FT and PT.

NOTE 2: If it is an emergency call then the authentication result is ignored and the call continues without SCFsl triggering (flows 16 to 19).

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

Note: if the call cannot be triggered in CCFo/SSFo, it is routed to the CCF/SSF to which the CTM user's subscription is associated and where triggering occurs.

4 SCFmm initiates an association with CUSF. Authentication and ciphering may start here.

5,6 The call unrelated association is released.

7 SCFmm request the report of the collected information event.

8 SCFmm orders the CCFo/SSFo to continue call setup.

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 a Connect inorder to identify the calling CTM User.

15 The SSFo triggers the SCFsl to ask for services.

16-17 The originating SCFsl queries the home SDFsl to check the service profile (e.g. restrictions on called party N°) and get information on the support of home specific services.

18 the originating SCFsl orders CCFo/SSFo to route the call (based on the called party number).

19-29 CCFo/SSFo routes the call accordingly and receives backward signalling. The connection is established.

30- 35 Release phase; here initiated from called party.

Annex A (informative): List of figures

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

Figure 1: Across networks boundaries relationship 8
Figure 2: Terminal authentication in the visited network 9
Figure 3: Retrieval and storage of authentication parameters by the visited network 10
Figure 4: Terminal authentication in the home network 10
Figure 5: Ciphering started in the visited Network 11
Figure 6: Location registration invoked by the visited network and data deletion invoked by the home network 12
Figure 7: Incoming call to geographic or portable destination number 13
Figure 8: Incoming Call to CTM Number 14
Figure 9: Outgoing Call 15
Figure 10: Functional architecture for retrieval and storage of Authentication parameters 16
Figure 11: Information Flows for Retrieval and Storage of authorization parameters. 17
Figure 12: Functional architecture (terminal authentication) 17
Figure 13: Information Flows (terminal authentication) 18
Figure 14: Functional architecture for Location Registration and Data Deletion 19
Figure 15: Information Flows for Location Registration 20
Figure 16: Information Flows for Data Deletion in Previous Visited Network 21
Figure 17: Functional architecture for Incoming Call (geographic number) 22
Figure 18: Functional architecture for Incoming Call (CTM destination number) 22
Figure 19: Information Flows for Incoming call, 1 of 2 24
Figure 20: Information Flows for Incoming call, 2 of 2 25
Figure 21: Functional architecture for Outgoing Call 27
Figure 22: Information Flows for Outgoing Call, 1 of 2. 28
Figure 23: Information Flows for Outgoing Call, 2 of 2. 29
Figure 24: Functional architecture(retrieval and storage of authorization parameters) 31
Figure 25: Information Flows for retrieval and storage of authorization parameters 32
Figure 26: Functional architecture (Terminal Authentication) 32
Figure 27: Information Flows (Terminal Authentication) 33
Figure 28: Functional architecture (Location Registration) 34
Figure 29: Information Flows (Location Registration) 35
Figure 30: Functional architecture (no agreement between new and old networks) 36
Figure 31: Information flows (no agreement between new and old visited networks) 37
Figure 32: Functional architecture for Incoming Call (geographic number) 38
Figure 33: Functional architecture (roaming number case) 39
Figure 34: Information Flows for Incoming call 1 of 2 40
Figure 34: Information Flows for Incoming call 2 of 2 41
Figure 35: Functional architecture (routing address case) 43
Figure 36: Information Flows (Routing address case), 1 of 2. 44
Figure 36: Information Flows (Routing address case) 2 of 2. 45
Figure 37: Functional architecture for outgoing call 47
Figure 38: Information Flows for outgoing call, 1 of 2. 48
Figure 38: Information Flows for outgoing call, 2 of 2. 49

History

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