Draft EG 201 096-3 V1.1.1 (1997-12)

ETSI Guide

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

European Telecommunications Standards Institute

Reference
DEG/NA-061302-3 (a5cr0icq.PDF)

Keywords
CTM, IN, interworking, network, private

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 Approval Procedure.

The present document is part 3 of a multi-part EG 201 096 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

Roaming of users of cordless telephones between private networks and public IN-structured networks result in requirements to support CTM across network boundaries. Procedures concerned are location registration and data deletion, authentication and ciphering, incoming call handling. Outgoing calls are assumed to be handled by the visited network, however, other mechanisms can also be used.

Basic principles are outlined in [1] for ISDN networks and in [2]. Any Intellligent Network (IN)-related aspects above that are to be described herein.

Bilateral commercial agreements between a particular public IN-structured network and a particular private network are assumed for CTM phase 1.

1 Scope

The present document describes inter-networking scenarios and procedures to support roaming of CTM users (public and private) between private networks and public IN-structured networks for CTM phase 1. The same type of procedures are addressed as in part 1.

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] Draft TR/BTC-1007: "Business TeleCommunications (BTC); Cordless Terminal Mobility (CTM); Interworking between Private and Public Networks; General Principles".

[2] TCR TR 021: "Intelligent Network (IN); Interworking between private networks (IN-structured and non IN-structured) and public IN-structured networks".

[3] ETSI ETS 300 415 Add.: "Business TeleCommunications (BTC); Private Integrated Services Networks (PISN); Terms and Definitions".

[4] EN DE/NA 010039: "Cordless Terminal Mobility (CTM) - phase 1; Service Description".

[5] ETR 322: "Intelligent Networks(IN); Vocabulary of terms and abbreviations for CS-1 and CS-2".

[6] EG 201 096-1: "CTM architecture and functionality for the support of CTM; Part 1: Intra-networking".

[7] EG 201 096-2: "CTM architecture and functionality for the support of CTM; Part 2: CTM Interworking between public Intelligent Networks".

3 Definitions, symbols and abbreviations

3.1 Definitions

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

The definitions given in ETS 300 415 [3] and ETR 322 [5], EG 201 096-1 [6], EG 201 096-2 [7] apply to the present document.

3.2 Abbreviations

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

CTM	Cordless Terminal Mobility
CCAF	Call Control Agent Function
CCF	Call Control Function
CUSF	Call Unrelated Service Function
CT2	Cordless Telecommunications generation 2
DECT	Digital Enhanced Cordless Telecommunications
DCK	Derived Cipher Key
FT	Fixed Termination
G-PINX	Gateway PINX
IAF	Intelligent Access Function
IN	Intelligent Network
ISDN	Integrated Services Digital Network
KS	Session Key
PCUSF	Peer Call Unrelated Service Function
PSCF	Peer Service Control Function
PSSF	Peer Service Switching Function
PINX	Private Integrated Network eXchange
PISN	Private Integrated Services Network
PT	Portable Terminal
RAND	RANDom number
REL	RELease
RES	calculated RESponse
RLC	ReLease Complete
RS	a value used to establish authentication session keys in DECT
SCUAF	Service Control User Agent Function
SCF	Service Control Function
SSF	Service Switching Function
SSP	Service Switching Point
DP	
IAM	Initial Address Message
CLI	Calling Line Identity
FIM	Functional Interworking Model
RN	Roaming Number result

4 Requirements

In general, interworking requirements with private networks are identified in [4].

Independent procedures are required for authentication and location handling.

Authentication:

- Authentication of the terminal performed at the home location.
- Authentication of the terminal performed at the visitor location.
- Authentication of the network by the terminal (required for security), which is subject of separate considerations.

The exact time when authentication takes place can vary and is implementation dependent.

The Derived Cipher Key (DCK) needs to be available in the visited network, if encryption is required.

A unique Cordless Teminal Mobility (CTM) identifier is required.

The transfer of user profile during location registration is not considered for CTM phase 1 across network boundaries. For CTM phase 1 it is assumed that any CTM user may make / receive calls in any network with which a roaming agreement exists. Emergency calls are not supported across network boundaries for CTM phase 1.

NOTE 1: The procedure for service profile interrogation / modification are not described herein, the reason being that the method should be left as open as possible and that there is no impact on the ISDN protocol, e.g. DTMF based procedures could be used.

NOTE 2: Subscription registration /deregistration does not apply to this document.

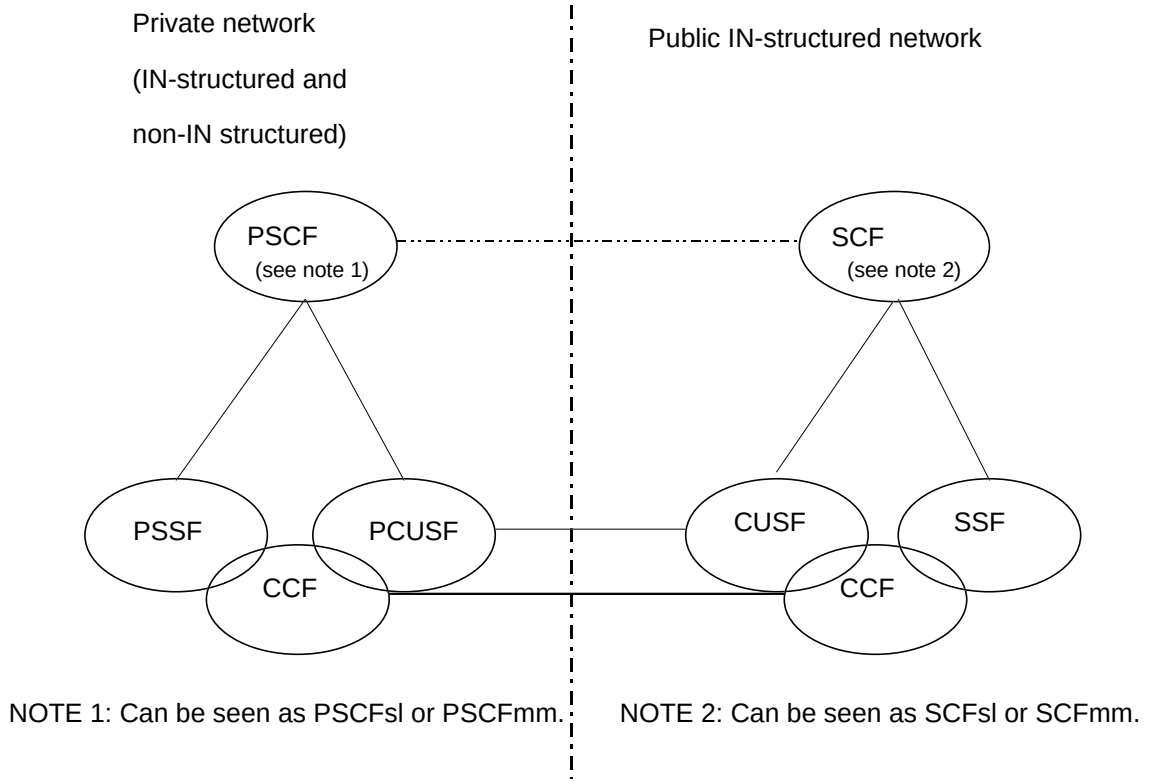
Charging issues, e.g. for an outgoing call of a public CTM user roaming in a private network, where the destination is the public IN or a different private network, are not described in the present document.

Generic mechanisms to identify the access to the SCF via Call Unrelated Service Function (CUSF) are required.

5 Interworking model

From a modelling point of view similar functions as defined in public IN-structured networks can be considered for private networks, but different architectures are found in private networks, e.g. centralized, decentralized, and a number of issues, in particular charging, is different. In non-IN structured private networks, service logic and service data does not have to be separated from basic call processing. For the purpose of describing the interworking between a private network and a public IN-structured network, the relevant functionalities are described in terms of peer functions, which denote functions similar to the corresponding IN functions, denoted with a leading letter 'P'. They do not purport to describe in any way the actual structure of a private network. [2].

The Functional Interworking Model, as shown in figure 1, reflect the functions needed for CTM interworking in its basic form. Non-solid lines indicate logical relationships across network boundaries to be relayed via the gateway functionality CUSF/PCUSF/CCF. There is no direct relationship between Peer Service Control Function (PSCF) and SCF.



PSCF: Peer Service Control Function
SCF: Service Control Function
PSSF: Peer Service Switching Function
SSF: Service Switching Function
PCUSF: Peer Call Unrelated Service Function
CUSF: Call Unrelated Service Function
CCF: Call Control Function

Figure 1: Functional interworking model private network/public IN for CTM

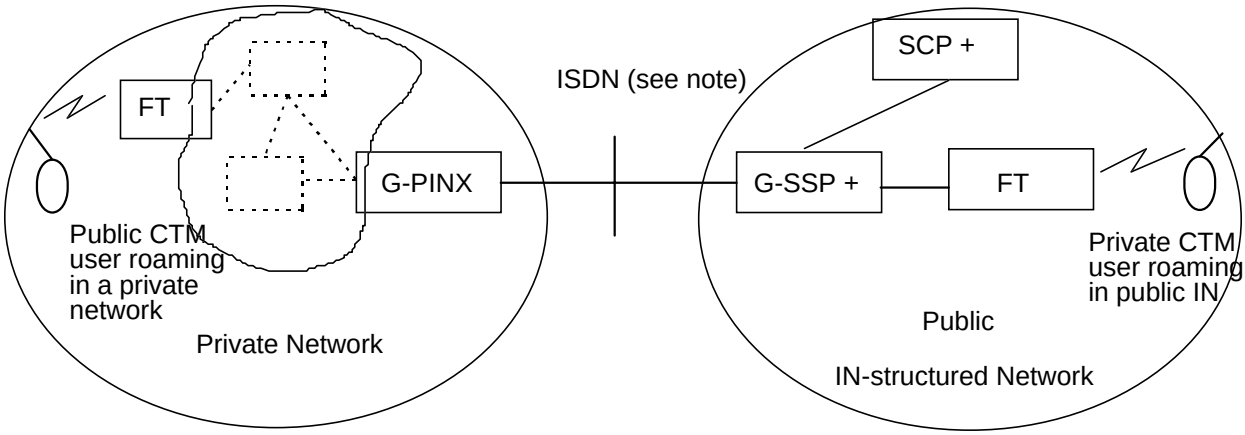
NOTE 1: Two cases can be separated:

- a PINX with no 'intelligence' - a dumb switch - that offers services to a group of users, e.g. has a cluster control functionality. This is covered by part 1 as an intra-network case;
- a PISN with 'intelligence' of an SCF type, therefore called PSCF, that offers services also to public CTM users roaming to that PISN; in this case a roaming agreement is needed between the two networks (symmetrical approach). This is covered by this part 3 as an inter-network case between a private network and a public IN-structured network.

NOTE 2: The PSCF-SCF relationship may be related to:

- the SCF-SCF relationship, as modelled for part 2;
- the Intelligent Access Function - Service Control Function (IAF-SCF) relationship, as modelled in ITU-T WP4/11 for interworking with private networks.

The functional interworking model allows for various physical implementations. An example physical interworking model, which is based on [1], uses a gateway in each network, the interface being an appropriate enhanced ISDN interface (see figure 2). For the private network, a black box approach is used.



G-SSP+: SSP enhanced with mobility management functions (SSF, CCF, CUSF)

SCP+: SCP enhanced with mobility management functions (SCFmm, SDFmm, SCFsl, SDFsl)

Note: The symmetric requirements need to be supported by an appropriate enhanced ISDN protocol.The use of this symmetric protocol in a particular instance depends on the roaming agreement. The roaming agreement can either be in only one direction, i.e. from public to private networks or from private to public networks, or in both directions (see NA1 'CTM Phase 1 Service Description', see [4]).

Figure 2: Physical interworking model private networks / public IN CTM (example)

The gateway in each network has to perform the necessary mapping between the appropriate enhanced ISDN protocol used at the interface between the networks and the protocol used inside each network. The appropriate enhanced ISDN interface could, for example, reflect a T+ reference point.

6 Scenarios

The following scenarios for CTM interworking are identified ([1] and [4]):

- Public CTM user roaming into a private network, and a previously visited network was another private network.
- Private CTM user roaming into a public IN-structured network, and a previously visited network was a private network (note, that the case of a previously visited network being a public network is excluded).

7 Procedures

The information flows that need to be supported across network boundaries are described herein. It is assumed that an appropriate enhanced ISDN interface is used for the transport of these information flows.

The information flows that reside inside the public IN-structured network, apart from those required to be relayed via the CUSF to the Peer Call Unrelated Service Function (PCUSF), correspond to those given in part 1, however, limited to those necessary to understand the procedures, i.e. not all the options listed in part 1 are reproduced as well as not all information flows.

The parameters included in the terminal authentication procedures apply to Digital Enhanced Cordless Telecommunications (DECT) terminals (RS, RAND). For Cordless Telecommunications generation 2 (CT2) terminals only one parameter (RAND) is required.

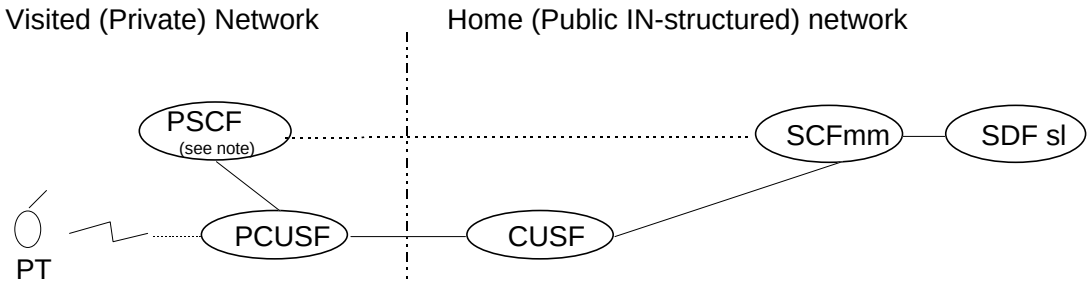
7.1 Public CTM user roaming into a private network, and a previously visited network was another private network (Scenario A)

7.1.1 Authentication and Ciphering

Authentication of the terminal may be performed in the visited (private) or the home (public IN-structured) network.

The visited network is responsible for ciphering. The ciphering parameter can either be retrieved from the home network together with the authentication parameters, or can be locally calculated during execution of the authentication algorithm.

7.1.1.1 Authentication when performed in the visited (private) network



NOTE: Can be seen as PSCF mm.

Figure 3: End-to-end functional interworking model for scenario A. Authentication in the visited (private) network

If the visited (private) network performs authentication of a public CTM user who roams in that private network, the authentication parameters have to be provided by the public IN-structured network via the CUSF.

Two alternatives exist:

- either the Session Key (RS, KS) is provided by the home (public IN-structured) network, and the visited (private) network calculates the result, using the KS received from the home network and the RANDom number (RAND) created, and compares this calculated result (RES) with the RES received from the Portable Terminal (PT) (a);

- or the calculation result (RES) is provided by the home (public IN-structured) network, and the visited (private) network only compares the RES received from the home network with the RES received from the PT (b).

a) The home network (public IN) provides the RS and KS across network boundaries

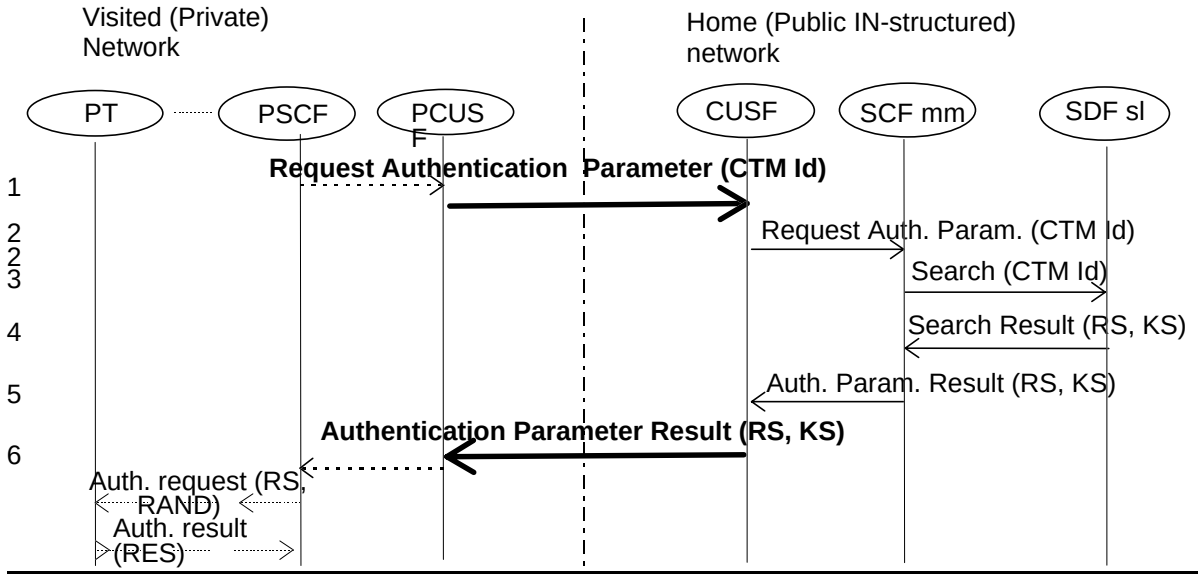


Figure 4: Scenario A: Terminal authentication in the visited (private) network

NOTE: To use this alternative, encryption on the line interface (between the networks) is recommended to cope with security requirements.

1,2 The visited (private) network requests authentication parameters from the public IN-structured network, providing the CTM Id (PSCF via PCUSF to CUSF, which is relayed to the SCFmm).

5,6 The SCFmm return the parameters (RS, KS) to the visited (private) network, relayed via the CUSF.

The visited (private) network then performs authentication of the public CTM user by calculating the result, using the KS received from the home network and the RANDom number (RAND) created for the authentication request towards the PT, and compares this RES with the result parameter (RES) obtained from the PT. The visited network uses KS and RS to derive the cipher key, if it is necessary to encrypt the radio link.

b) The home network (public IN) provides the RS, RAND and RES across network boundaries.

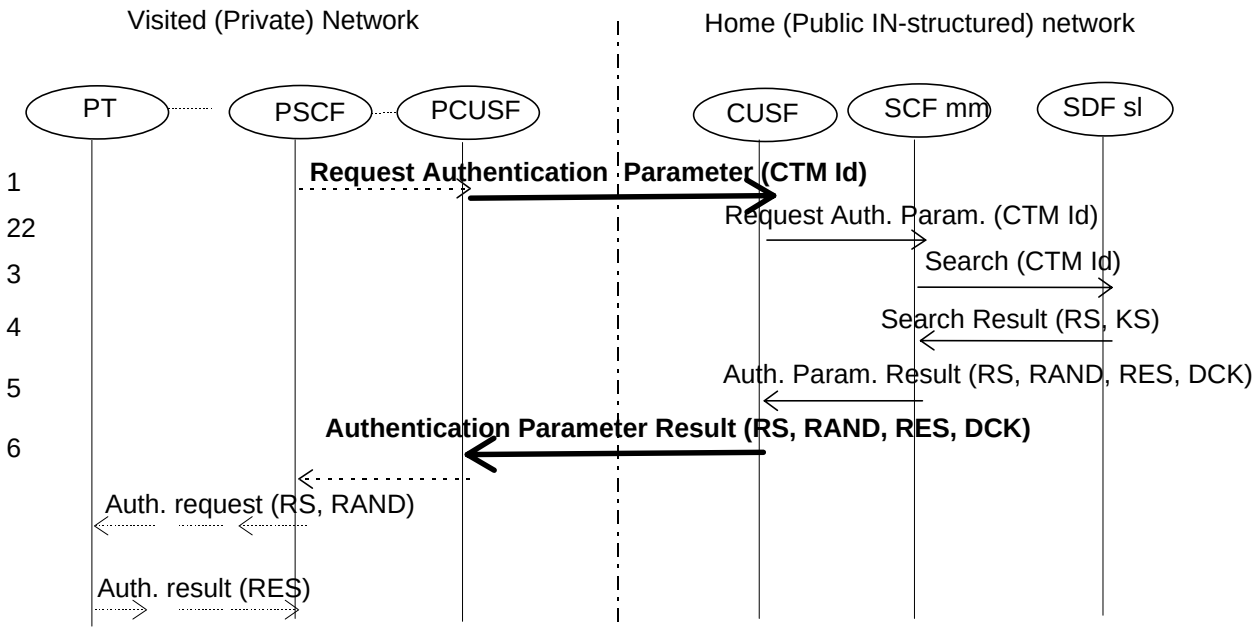


Figure 5: Scenario A: Terminal authentication in the visited (private) network- case b

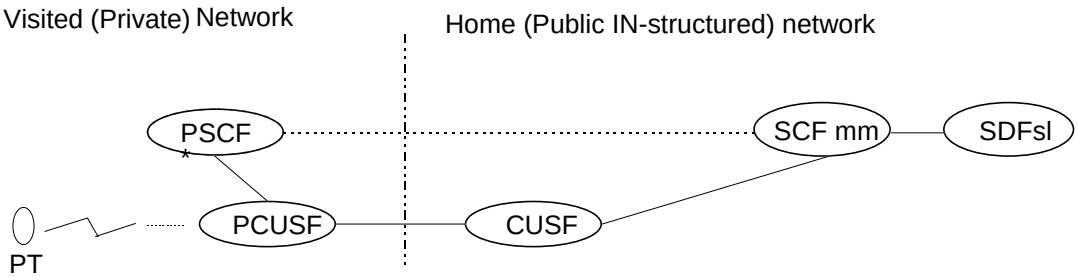
1,2 The visited (private) network requests authentication parameters from the public IN-structured network providing the CTM Id (PSCF via PCUSF to CUSF, which is relayed to the SCFmm).

5,6 The SCF mm return the parameters (RS, RAND and RES) to the visited (private) network, relayed via the CUSF. The DCK is transmitted to allow encryption of the air interface in the visited network, and may be stored in the visited network to be used for subsequent ciphering.

The visited (private) network then performs authentication of the public CTM user by comparing the RES received from the home network with the result parameter (RES) obtained from the PT.

7.1.1.2 Authentication when performed in the home (public IN-structured) network

If the home (public IN-structured) network performs authentication of a public CTM user who roams in a private network, the Authentication Request is sent across network boundaries, providing the RS and RAND. The RES given in the Authentication Response from the visited (private) network is compared with the result obtained from calculation performed in the home (public IN-structured) network.



NOTE: Can be seen as PSCFmm.

Figure 6: End-to-end functional interworking model for Scenario A. Authentication in the home (public IN-structured) network

If the home (public IN-structured) network performs authentication of a public CTM user who roams in a private network, the Authentication Request is sent across network boundaries, providing the RS and RAND. The RES given in the Authentication Response from the visited (private) network is compared with the result obtained from calculation performed in the home (public IN-structured) network.

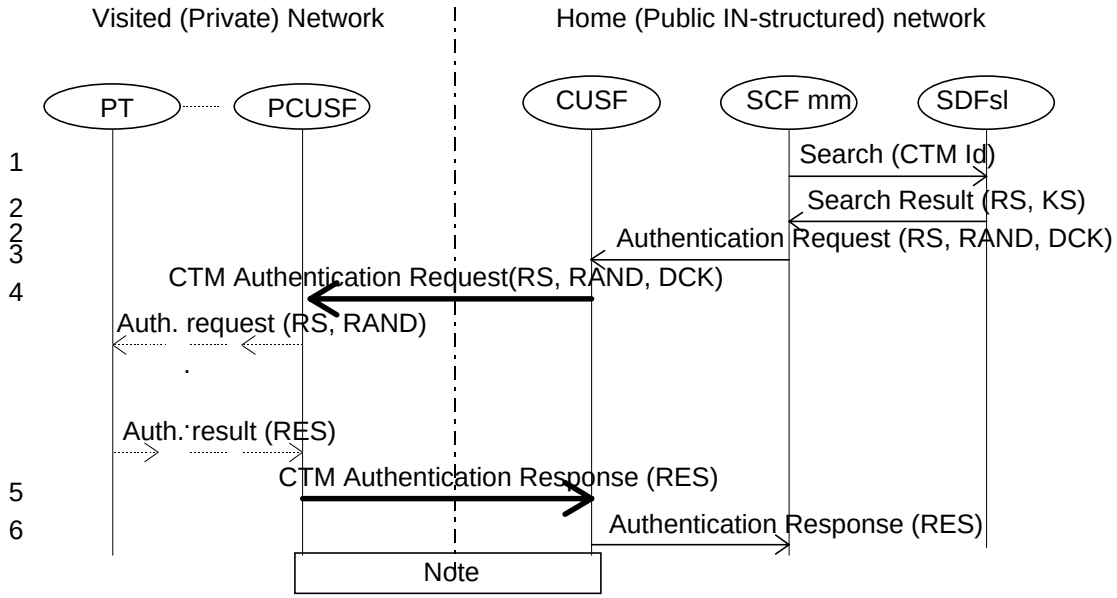
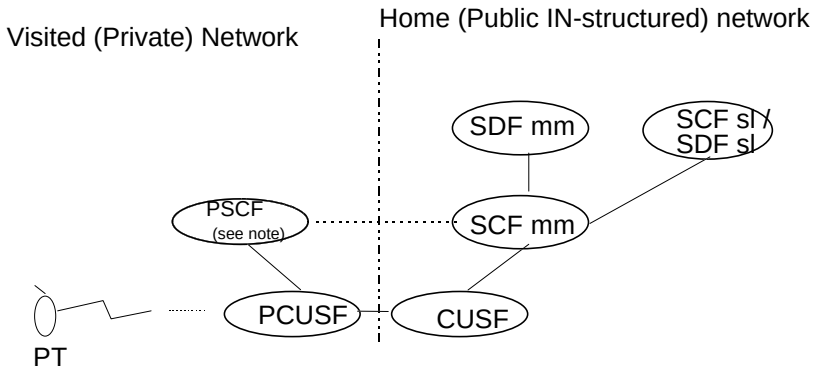


Figure 7: Scenario A: Terminal authentication in the home (public IN-structured) network



NOTE: Can be seen as SCFmm.

Figure 8: End-to-end functional interworking model for scenario A - Location Registration

NOTE: The visited network is advised that authentication was successful as a precondition to apply ciphering.

3,4 The home (public-IN structured) network computes an Authentication Request in the SCFmm, including the RS and a RANDom number (RAND), and sends it to the visited (private) network (PSCF) via CUSF/PCUSF. The DCK is transmitted to allow encryption of the air interface in the visited network, and is stored in the visited network if authentication is confirmed.

The request is forwarded within the visited (private) network to the public CTM user, via the visited private network node. The Authentication Response from the public CTM user, which contains the authentication result (RES) is passed back to the PCUSF.

5,6 The Authentication Response, including the RES, is sent across network boundaries to the home (public IN-structured) network, and is relayed by the CUSF to the SCFmm.

The home (public-IN structured) network (SCFmm) performs the authentication of the public CTM user by comparing the RES received from the visited (private) network with the RES calculated (using the KS and RAND).

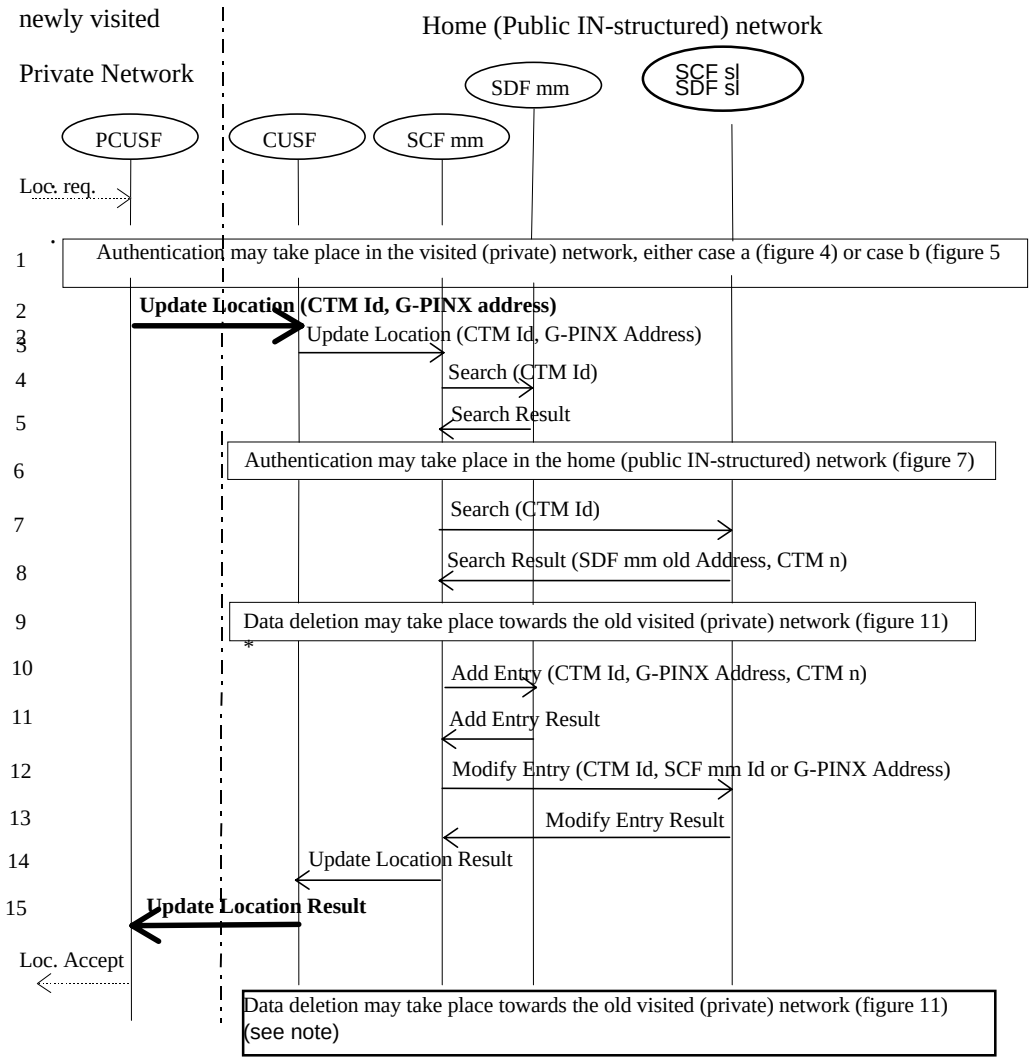
7.1.2 Location Registration and Data Deletion

The procedures described assume that the public CTM user is not already registered in the visited (private) network, and the previously visited network was another private network. Since in this case, the previously visited network is different

from the home (public IN-structured) network, also data deletion procedures (Cancel Location) towards the previously visited network are required.

7.1.2.1 Location Registration

The visited (private) network appears to the public IN-structured network as a single visited area.



NOTE: Could also be performed in parallel to location updating.

Figure 9: Location registration, public CTM user roaming in a private network

The public CTM user performs a location registration to the visited (private) network. In the case assumed the CTM user (CTM Id) is unknown to the private network.

1 If the visited (private) network performs authentication of the public CTM user who roams in the private network, the PSCF via PCUSF requests the public (IN-structured) network to provide the authentication parameters (see Authentication, subclause 7.1.1.1, case a (figure 4) or case b (figure 5)).

2 The visited (private) network sends a location registration request across network boundaries, including the CTM Id and the Gateway PINX (G-PINX) address.

3 The CUSF forwards the location registration request to the SCFmm, including the CTM Id plus the G-PINX address.

4,5 The SCFmm checks if the CTM user is already registered in the Service Data Function (SDF mm). In the case assumed here, he is not yet registered.

6 If the home (public IN-structured) network performs authentication of the public CTM user who roams in the private network, it sends an Authentication Request to the private network (see Authentication, subclause 7.1.1.2 (figure 7)).

7, 8 The home (public-IN structured) network (SCFmm) retrieves the CTM number and information about the previously visited location from the SCFsl/SDFsl, which is assumed to be another private network. The result returned includes the SDFmm old Address.

9 Data deletion towards the old visited (private) network may take place (figure 11). Alternatively, the data deletion procedure could also be performed after (or in parallel to) the updating of the location.

10,11 The G-PINX address and CTM number needs to be stored in the SDF mm.

12,13 The home (public IN-structured) network (SCFmm) stores the parameters to reach the new visited (private) network (SCFmm Id or G-PTNX address) in the SCFsl/SDFsl.

14,15 The location registration procedure is confirmed (SCFmm-CUSF information flow chain to PSCF via PCUSF).

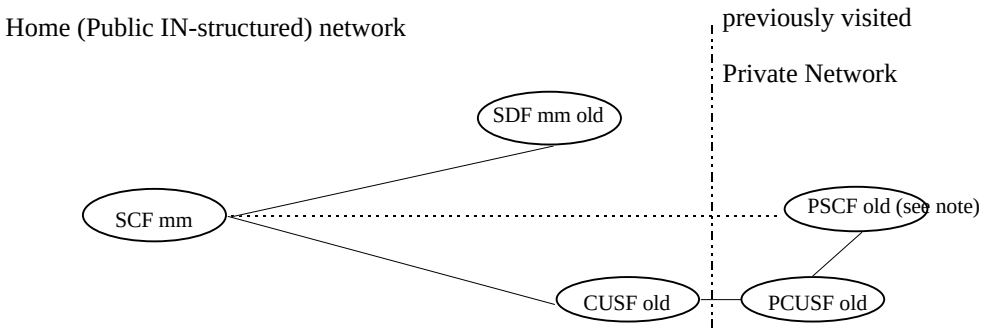
As an alternative, the Update Location procedure may be combined with Authentication in the visited network. In that case, the authentication parameters would be returned within the Update Location Result.

7.1.2.2 Data Deletion

It is assumed that there is no agreement between the previously visited (private) network and the currently visited (private) network to delete data. In the case shown deletion of location registration information in the previously visited (private) network is initiated from the home (public IN-structured) network.

NOTE: If the previously visited network was the home (IN-structured) network, the data deletion procedure is subject of part 1.

If the previously visited network was another public IN-structured network, the data deletion procedure is subject of part 2.



NOTE: Can be seen as SCFmm.

Figure 10: End-to-end functional interworking model for Scenario A - Data Deletion

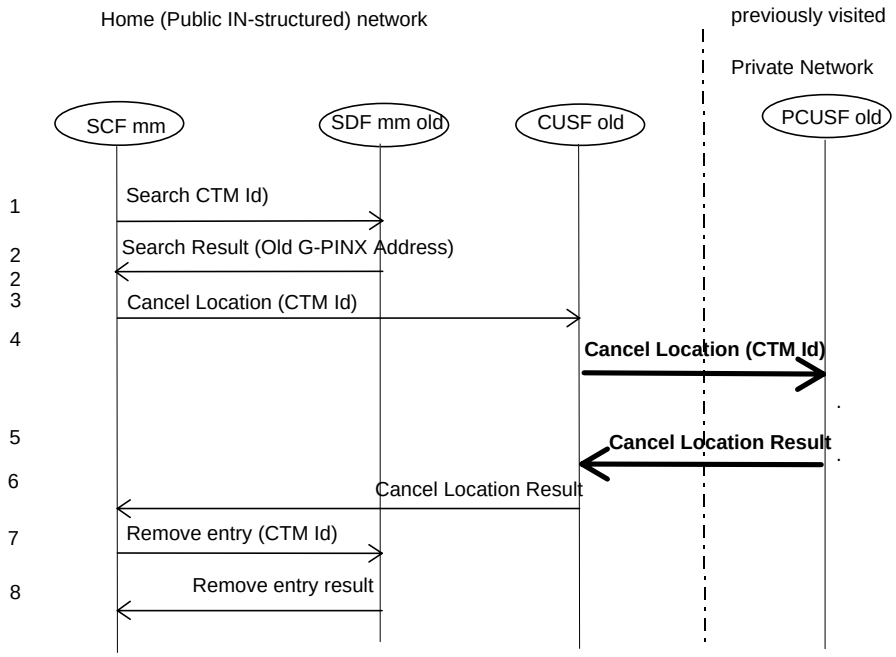


Figure 11: Data Deletion, public CTM user roaming in a private network

1,2 The SCF mm derives information from the SDF mm old about the previously visited (private) network.

3,4 A cancel location request is forwarded from the SCF mm to the previously visited (private) network (PCUSF old) via CUSF old.

.. * The previously visited (private) network removes the entry of the public CTM user who previously roamed in that private network from its databases.

5,6 A confirmation of the deletion procedure is sent from the previously visited (private) network (PCUSF old) to the home (public IN-structured) network (CUSF old), relayed back to SCF mm.

7,8 The SCF mm orders the SDF mm old to delete all information about the previous location of the CTM user.

7.1.3 Incoming Call

A call for a public CTM user who roams in a private network will be routed to the nearest public (IN-structured) network node (SSP). Via an SSF-SCFsl-SDFsl-SCFmm-SDFmm (case 1) or SSF-SCFsl-SDFsl-SDFmm (case 2) information flow chain the visited (private) network address will be determined. The SSF/CCF then sends a Setup information flow to the private network, including the CTM Id. The private network uses its mobile call handling procedures to send the call to the visited node and finally to the public CTM user roaming in that private network. Authentication may take place at various points, most likely after the page response has been received from the PT. Ciphering is performed in the visited network using the DCK obtained during terminal authentication. For CTM phase 1 it is assumed that a public CTM user may receive calls when roaming to a private network with which a roaming agreement exists.

Case 1: Roaming number case

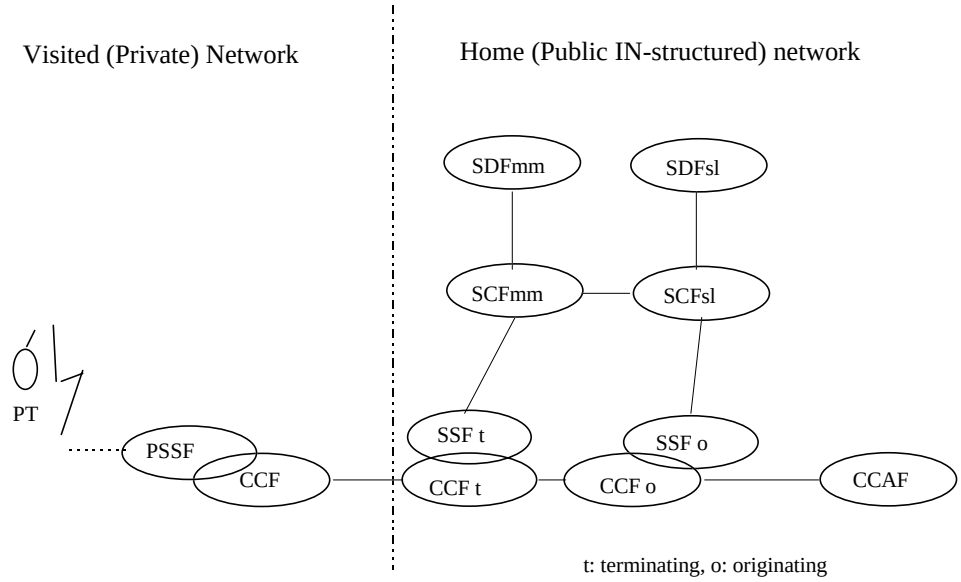


Figure 12: End-to-end functional interworking model for Scenario A - Incoming call, case 1

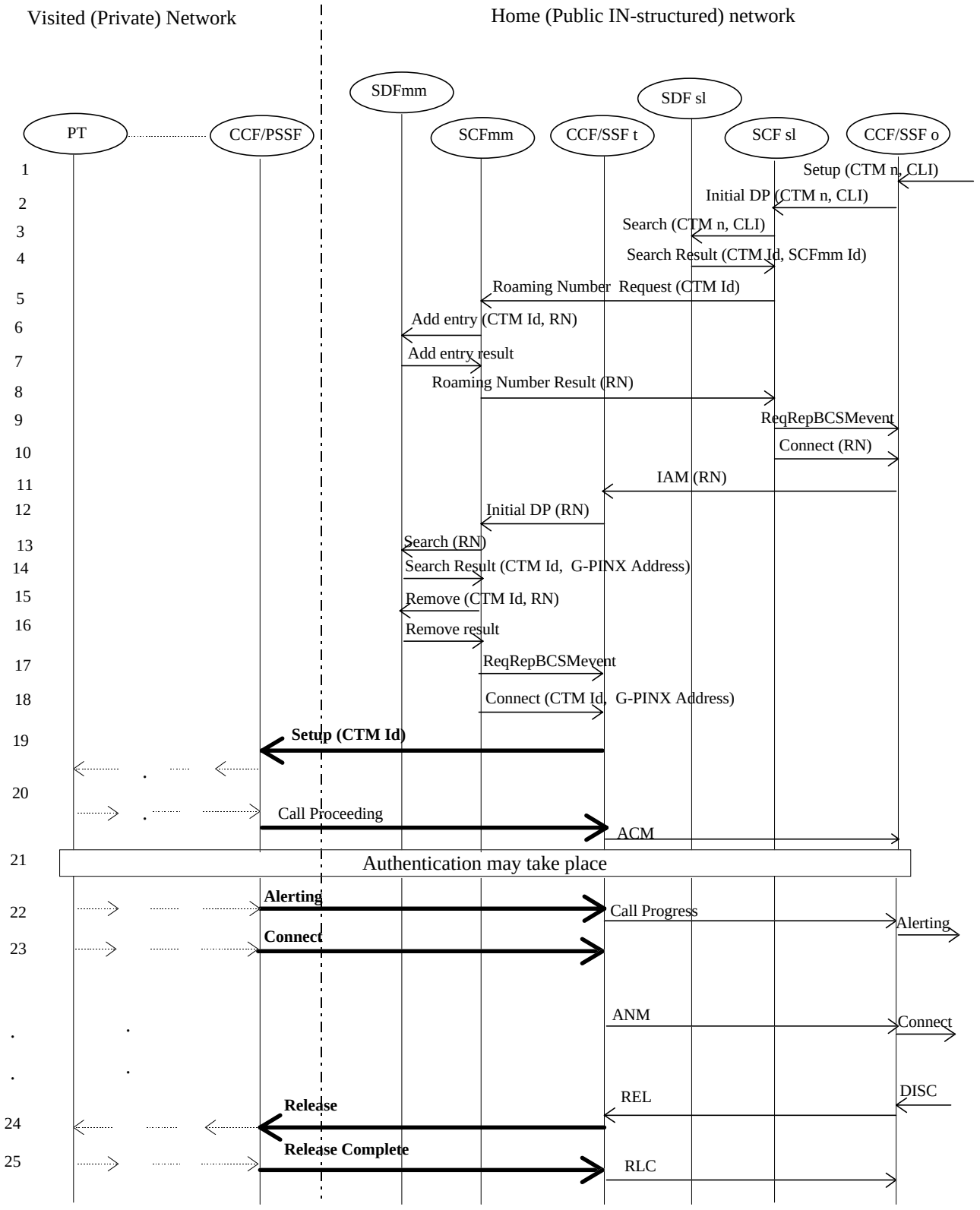


Figure 13: Scenario A: Public CTM user roaming in a private network - Incoming call, case

1 Calling user sends a Setup information flow which contains the CTM number of the called public CTM user who roams in a private network, plus the Calling Line Identity (CLI).

2 An Initial DP message is sent to the SCFsl.

3-4 Interrogation with the SDFsl provides the SCFmm Id where information is stored of the visited (private) network location.

5-8 The appropriate SCFmm is requested to provide a Roaming Number (RN).

9-10 The SCFsl requests the CCF/SSF originating to connect the calling user. The SCFsl further requests the receipt of event reports, i.e. 'Route_Select_Failure', 'O_No_Answer', 'O_Called_Party_Busy', to provide appropriate treatment on not reachable situations.

11 The call is routed to the terminating CCF/SSF using the IAM containing the roaming number.

12-18 Via an CCF/SSFt-SCFmm-SDFmm information flow chain the G-PINX address is determined.

19 A Setup information flow is sent across network boundaries to the G-PINX (CCF/PSSF functionality), including the CTM Id.

.. Within the visited (private) network mobile call handling procedures occur to forward the call to the destination network node, to perform paging, and continue the setup procedure towards the PT. 'Call Proceeding' is returned to the CCF/SSFt.

21 It is assumed that authentication is performed after successfully paging the PT, however, may also be performed at other points.

22..25 'Alerting' will be returned, followed by 'Connect'. At the end of the call, 'RELease' confirmed by 'RELease Complete' will be transported via the networks involved.

Case 2: Routing Number Case

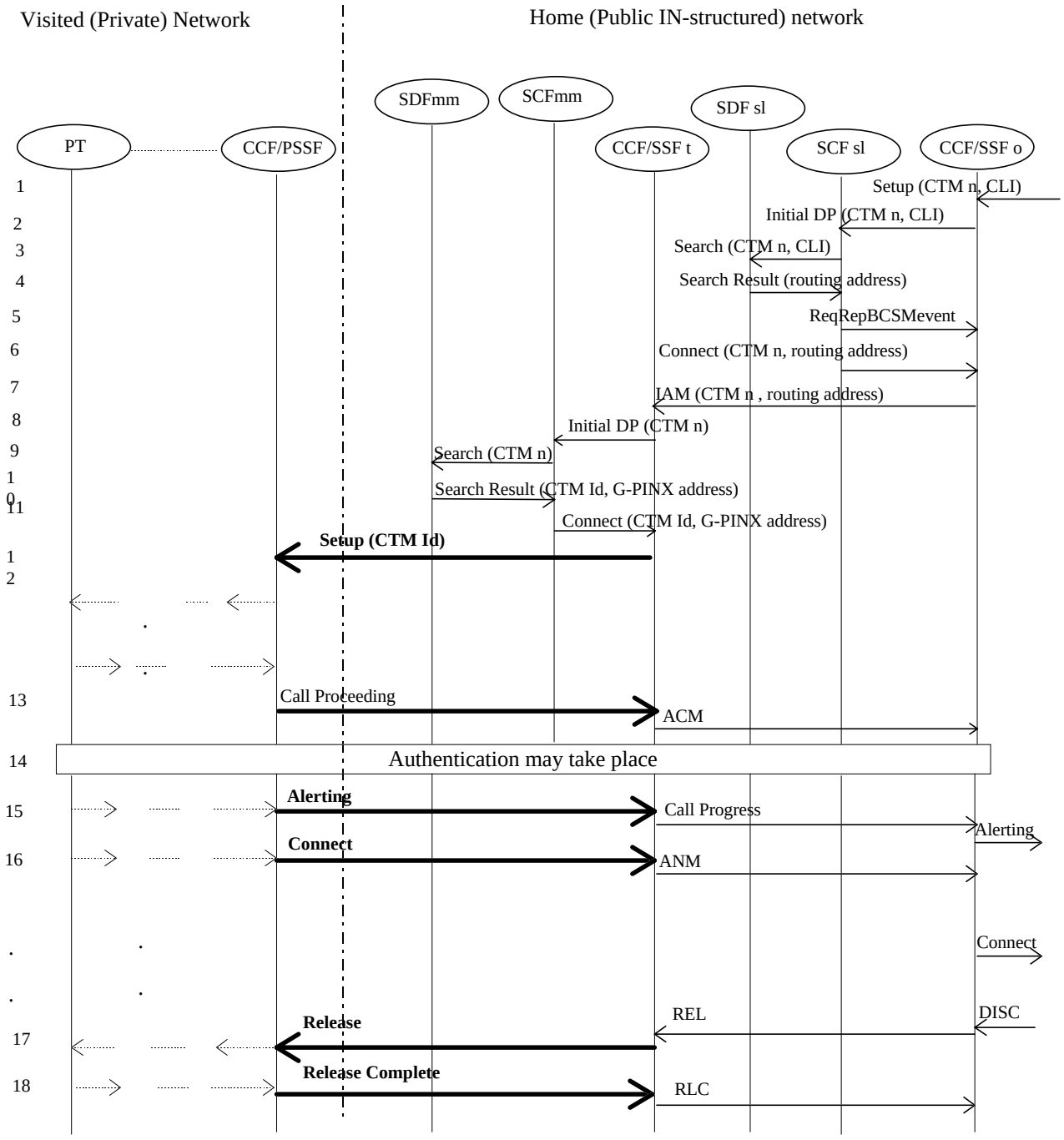


Figure 15: Public CTM user roaming in a private network - Incoming call, case 2

1-4 As in case 1, except that the information returned to the SCFsl is the routing address.

5-11 The SCFsl orders SSFo to set up the call, which then is routed to the CCF/SSFt. After retrieval of the CTM Id and the G-PINX address, call set up is continued as in case 1.

12-18 Call set-up procedures continue as in case 1.

7.1.4 OutgoingCall

Case 1: No use of home network services

A call from a public CTM user who roams in a private network may be forwarded by the private network to a destination (in a private or public network). The visited (private) network can handle the call without involving the home (public IN-structured) network. This also avoids the problem of tromboning, which could occur, if the home (public IN-structured) network was involved in routing outgoing calls. Authentication within the visited (private) network would be

required before doing so (see Authentication, subclause 7.1.1.1, case a (figure 4) or case b (figure 5)). Ciphering is performed in the visited network, using the DCK obtained during terminal authentication.

Some other mechanisms could also be used. For CTM phase 1 it is assumed that a public CTM user may make calls when roaming to a private network with which a roaming agreement exists.

Case 2: Use of home network services

Alternatively, a call from a public CTM user who roams in a private network may be routed via the home network. Authentication within the home (public IN-structured) network would be required (see Authentication, subclause 7.1.1.2). Ciphering is performed in the visited network, using the DCK obtained during terminal authentication.

7.2 Private CTM user roaming into a public IN-structured network, and a previously visited network was a private network (Scenario B)

NOTE: The VPN case may need separate considerations, or may be covered by this subclause, choosing the option that Authentication is performed in the visited (IN-structured) network. Different from the authentication procedures shown in subclause 7.2.1.1, the authentication data are already available in the network. Therefore, authentication can start without requesting the private network for authentication parameters (i.e. information flows 4-11 only apply in figures 17 and 18. In addition, the information has to be passed back to the SDFsl).

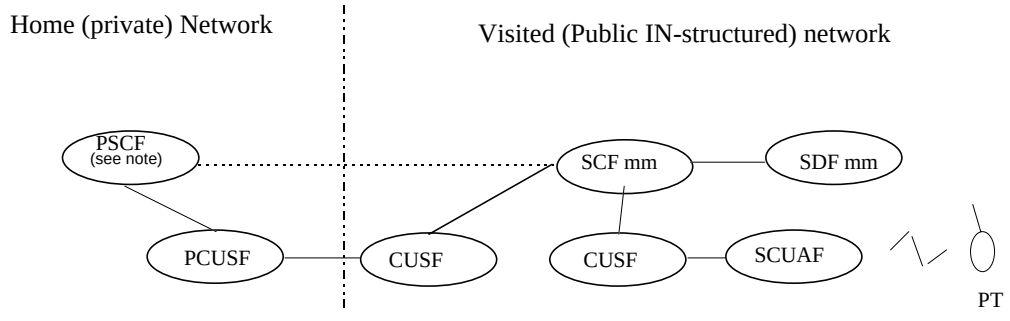
7.2.1 Authentication

Authentication of the terminal may be performed in the visited (public IN-structured) or the home (private) network.

The visited network is responsible for ciphering. The ciphering parameter can either be retrieved from the home network together with the authentication parameters, or can be locally calculated during execution of the authentication algorithm.

7.2.1.1 Authentication when performed in the visited (public IN-structured) network

If the visited (public IN-structured) network performs authentication of a private CTM user who roams in that public network, the authentication parameters have to be provided by the private network via the PSCF.



NOTE: Can be seen as PSCF sl.

Figure 16: End-to-end functional interworking model for Scenario B - Authentication is the visited (public IN - structured) network

The CUSF close to the gateway is not necessarily the CUSF where the Service Control User Agent Function (SCUAF) is attached to.

Two alternatives exist:

- either the session key (RS, KS) is provided by the home (private) network, and the visited (public IN-structured) network calculates the result, using the KS received from the home network and the RANDom number (RAND) created, and compares this calculated result (RES) with the RES received from the PT (a);

- or the calculation result (RES) is provided by the home (private) network, and the visited (public IN-structured) network only compares the RES received from the home network with the RES received from the PT (b).

a) The home (private) network provides the RS and KS across network boundaries.

NOTE: To use this alternative, encryption on the line interface (between the networks) is recommended to cope with security requirements.

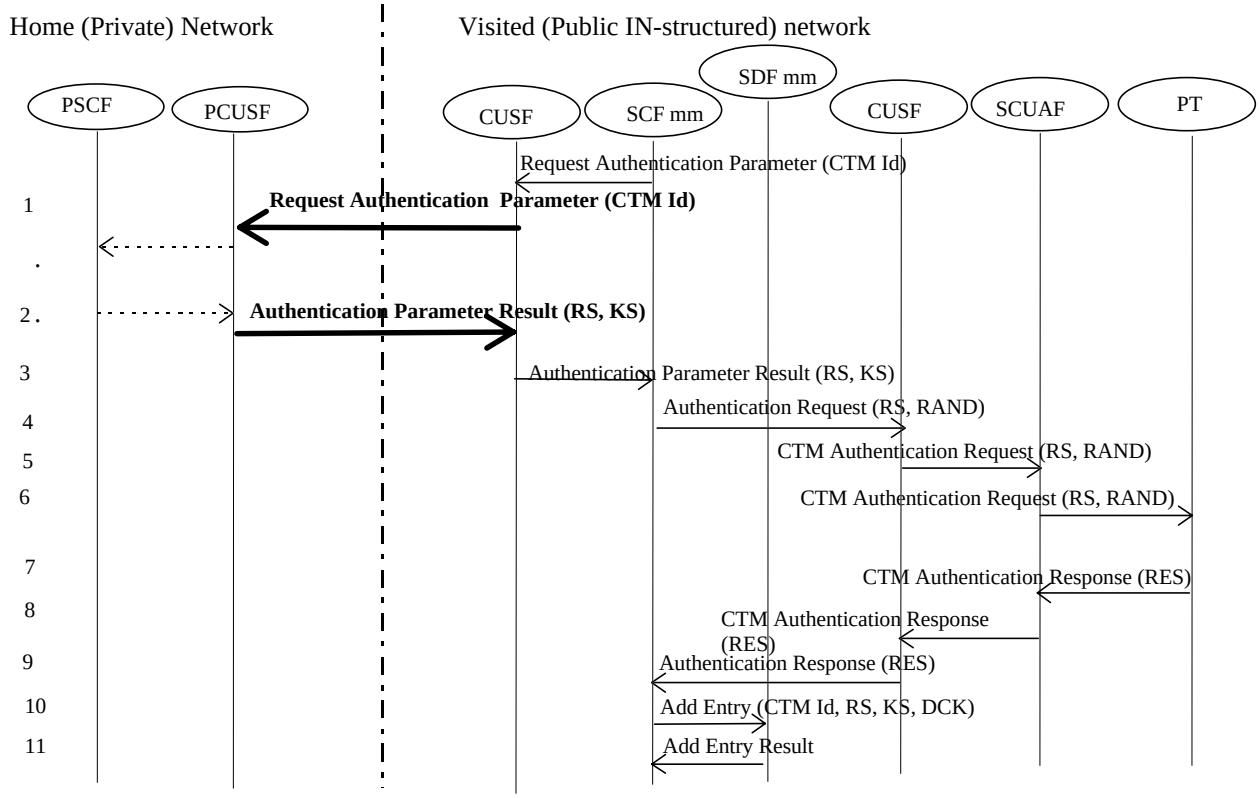


Figure 17: Terminal authentication in the visited (public IN-structured) network - case a

1 The visited (public IN-structured) network requests authentication parameters from the private network, providing the CTM Id (visited SCFmm via CUSF to PSCF via PCUSF).

2 The PSCF returns the parameters (RS, KS) to the visited (public IN-structured) network (via PCUSF to CUSF). The visited network uses KS and RS to derive the cipher key, if it is necessary to encrypt the radio link.

3 The CUSF relays this information flow to the visited SCFmm.

4-6 An authentication request is forwarded to the CUSF to which the SCUAF is attached to; this CUSF relays this message to the PT via SCUAF.

7-9 The response containing the RES is passed back from the PT to the CUSF via SCUAF, and the CUSF relays this message to the visited SCFmm.

10,11 The authentication parameters are stored in the SDFmm.

The visited (public IN-structured) network (visited SCFmm) then performs authentication of the private CTM user by calculating the result, using the KS received from the home network and the RANDom number (RAND) created for the authentication request towards the PT, and compares this RES with the result parameter (RES) obtained from the PT.

b) The home (private) network provides the RS, RAND and RES across network boundaries.

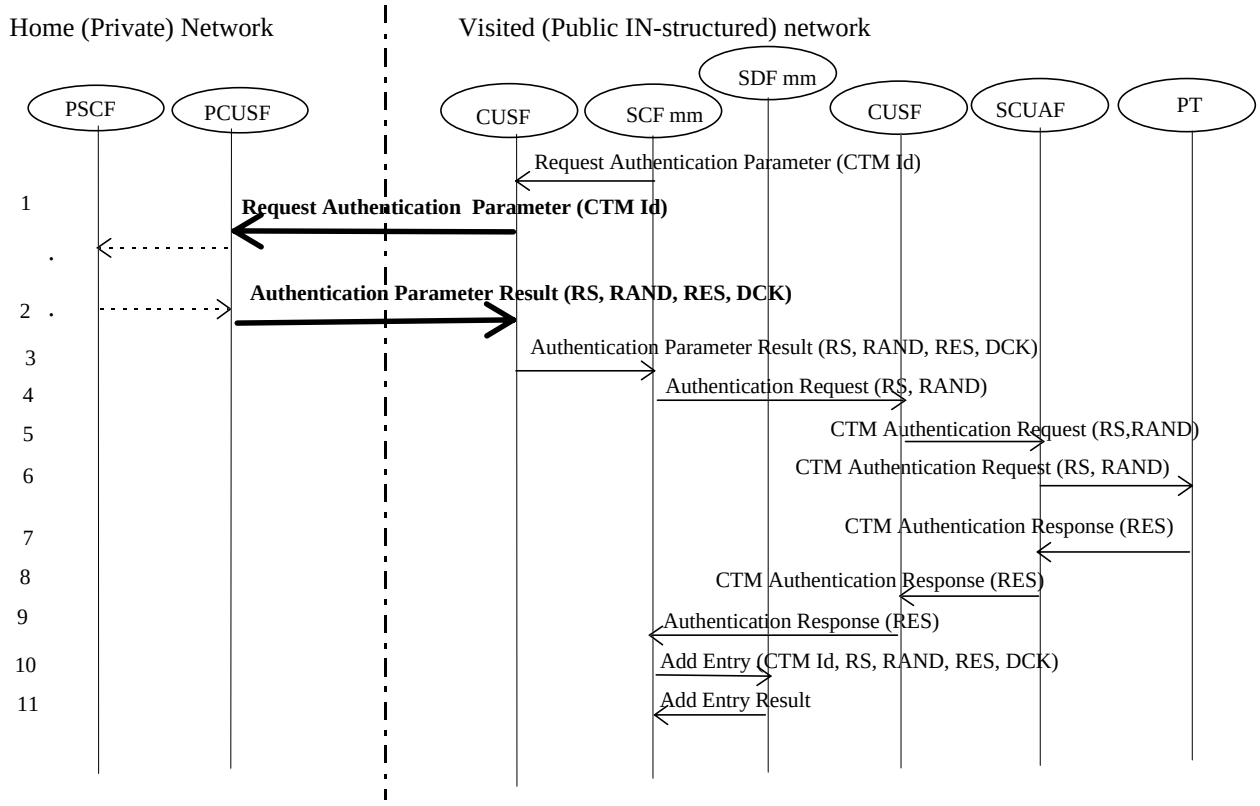


Figure 18: Terminal authentication in the visited (public IN-structured) network - case b

1 The visited (public IN-structured) network requests authentication parameters from the private network, providing the CTM Id (visited SCFmm via CUSF to PSCF via PCUSF).

2 The PSCF returns the parameters (RS, RAND and RES) to the visited (public IN-structured) network (via PCUSF to CUSF). The DCK is transmitted to allow encryption of the air interface in the visited network, and may be stored in the visited network to be used for subsequent ciphering.

3 The CUSF relays this information flow to the visited SCFmm.

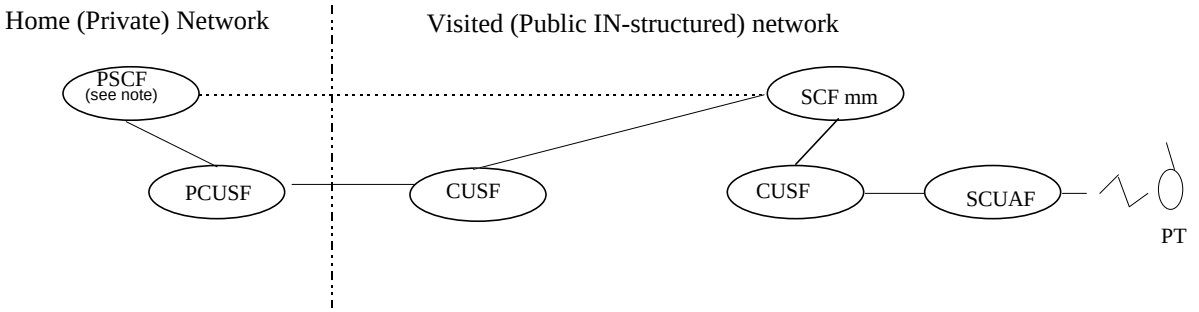
4-8 The RES is stored by the visited SCFmm in the SDFmm, and an Authentication Request is forwarded to the CUSF which relays this request to the PT via SCUAF.

The visited (public IN-structured) network (visited SCFmm) then performs authentication of the private CTM user by comparing the RES received from the home (private) network (2) with the result parameter obtained from the PT.

9-11 The response containing the RES is passed back from the PT to the CUSF via SCUAF, and the CUSF relays this response to the visited SCFmm.

7.2.1.2 Authentication when performed in the home (private) network

If the home (private) network performs authentication of a private CTM user who roams in a public IN-structured network, the Authentication Request is sent across network boundaries, providing the RS and RAND. The RES given in the Authentication Response from the visited (public IN-structured) network is compared with the result obtained from calculation performed in the home (private) network.



NOTE: Can be seen as SCF sl.

Figure 19: End-to-end functional interworking model for Scenario B - Authentication in the home (private) network

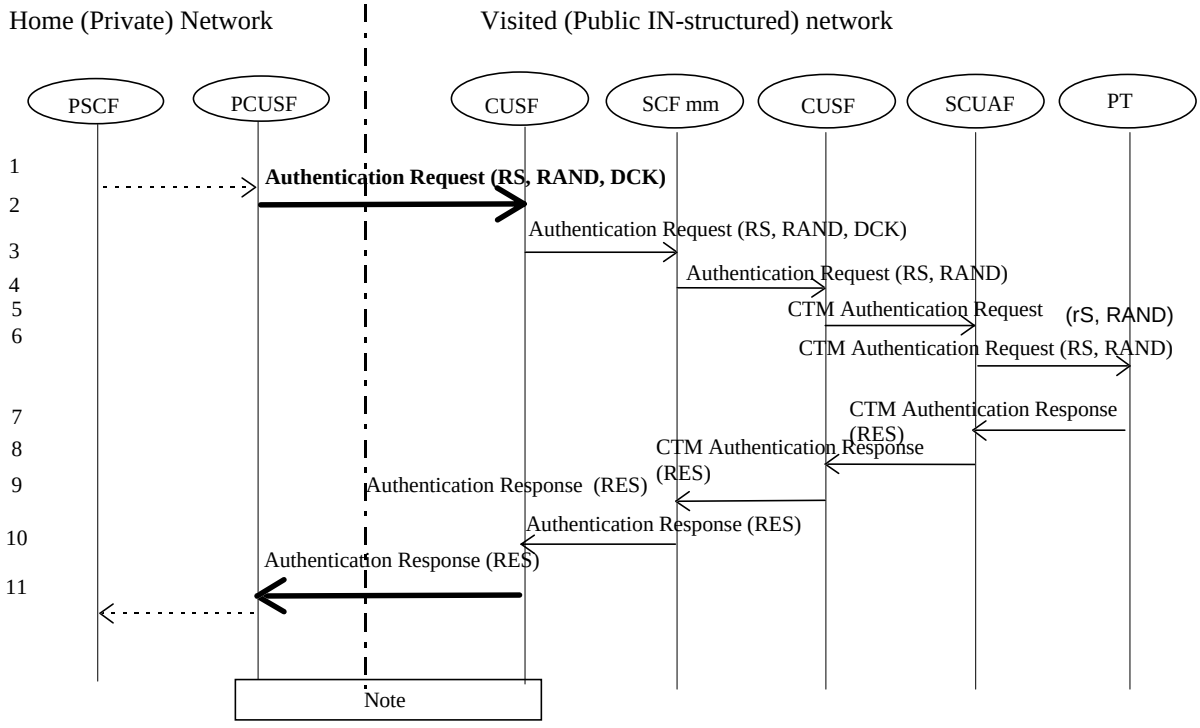


Figure 20: Terminal authentication in the home (private) network

NOTE: The visited network is advised that authentication was successful as a precondition to apply ciphering.

1 The home (private) network sends an Authentication Request to the visited (public IN-structured) network (PSCF to CUSF via PCUSF), including the RS and a RANDom number (RAND). The DCK is transmitted to allow encryption of the air interface in the visited network, and is stored in the visited network if authentication is confirmed.

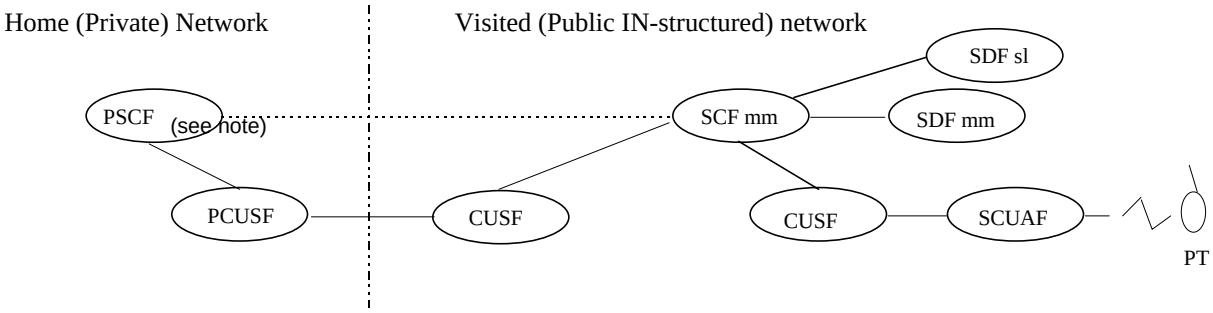
2-6 The CUSF forwards the request to the PT via visited SCFmm, CUSF and SCUAF.

7-10 The Authentication Response, including the RES, is sent back from the PT to the CUSF at the gateway (via SCUAF, visited CUSF, visited SCFmm).

11 The Authentication Response, including the RES, is sent across network boundaries to the home (private) network (PSCF via PCUSF).

The home (private) network performs the authentication of the private CTM user who roams in the public IN-structured network by comparing the RES received from the visited (public IN-structured) network with the RES calculated (using the KS and RAND).

7.2.2 Location Registration



NOTE: Can be seen as PSCF sl.

Figure 21: End-to-end functional interworking model for Scenario B - Location Registration

The procedure described assumes that the private CTM user is not already registered in the visited (public IN-structured) network, and the previously visited network was a private network (either the same or a different private network). If the previously visited network was a different private network, location deregistration procedures (Cancel Location) towards this previously visited network would be required. (Since the approach for private networks is a 'black box' approach, this is not shown in the following figure).

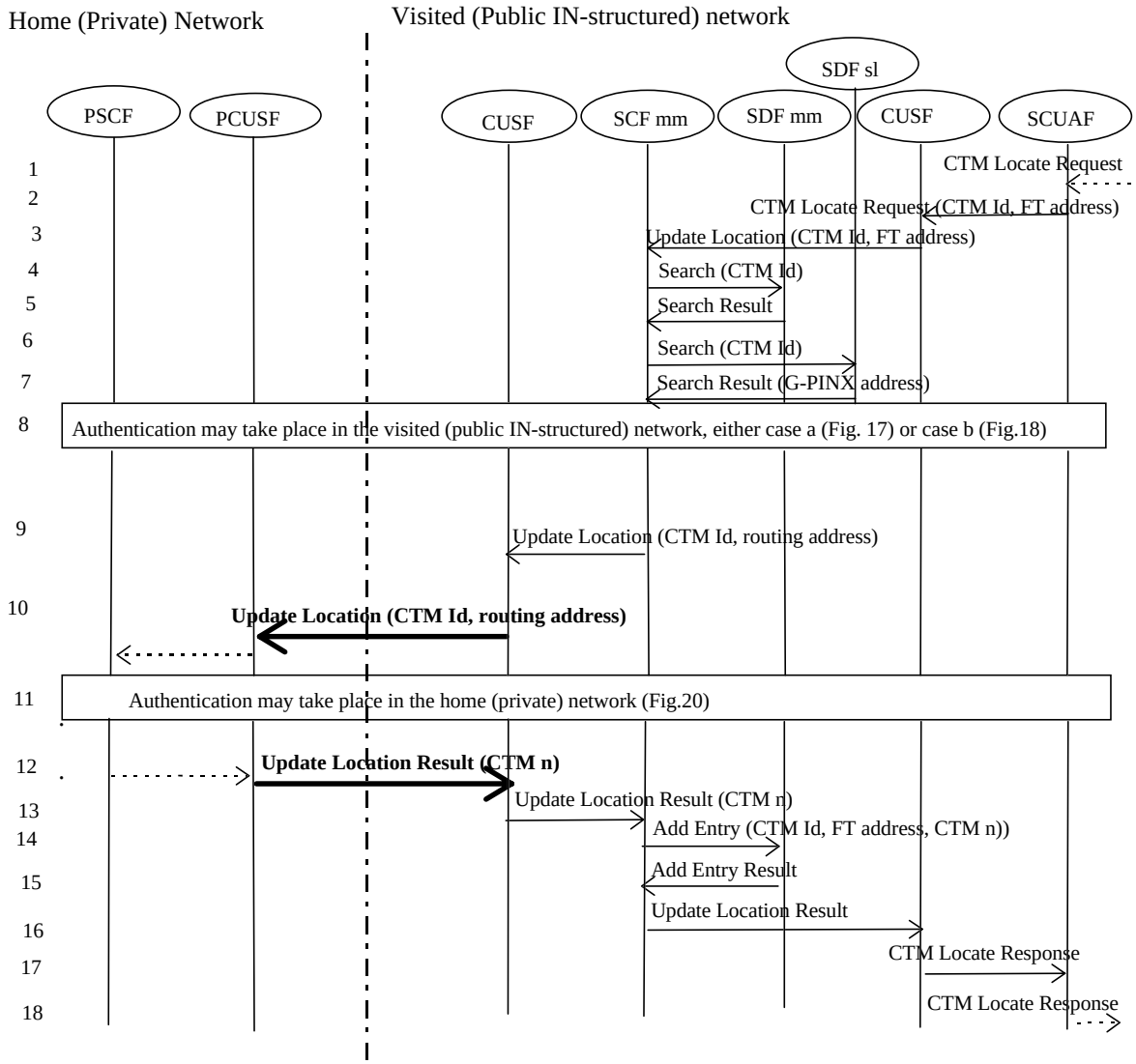


Figure 22: Location registration, private CTM user roaming in a public IN-structured network

1-7 The private CTM user performs a location registration to the visited (public IN-structured) network. In the case assumed the CTM user (CTM Id) is unknown to the public network. The SCUAF passes the location request to the CUSF, and the CUSF request the SCFmm to update the location.

8 If the visited (public IN-structured) network performs authentication of the private CTM user who roams in the public network, the visited SCFmm via CUSF requests the private network to provide the authentication parameters (see Authentication, subclause 7.2.1.1, case a (figure 17) or case b (figure 18)).

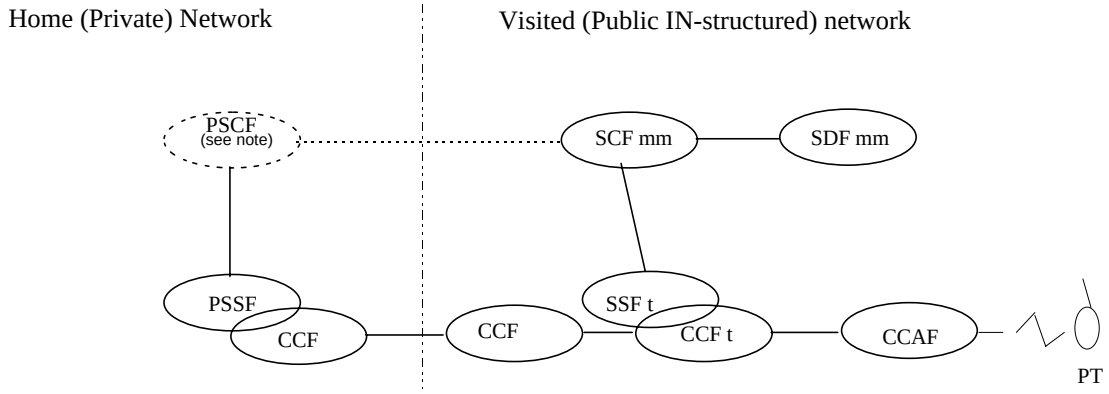
9,10 The visited (public IN-structured) network (visited SCFmm) sends an Update Location Request via CUSF across network boundaries, including the CTM Id, and a routing address.

11 If the home (private) network performs authentication of the private CTM user who roams in the public network, it sends an Authentication Request to the public network (see Authentication, subclause 7.2.1.2 (figure 20)).

.. The home (private) network stores the parameters received from the visited (public IN-structured) network, retrieves information about the previously visited location, and performs the cancel location procedures to remove the entry from the databases.

12-18 The location registration procedure is confirmed to the visited (public IN-structured) network (visited SCFmm via CUSF), including the CTM number, and the response is passed from the CUSF to the PT via SCUAF. The CTM Id, CTM number and Fixed Termination (FT) address are stored in the SDFmm.

7.2.3 Incoming Call



NOTE: Can be seen as PSCF sl.

Figure 23: End-to-end functional interworking model for Scenario B, incoming call

A call for a private CTM user (identified by a PISN number) who roams in a public IN-structured network will be routed to the private network. The private network uses its mobile call handling procedures to forward the call to the private network gateway. A Setup request is then sent across network boundaries, including the parameters (CTM Id) . As soon as the CCF/SSFt receives the setup request, the procedures within IN-structured networks apply. Ciphering is performed in the visited network, using the DCK obtained during terminal authentication. For CTM phase 1 it is assumed that a private CTM user may receive calls when roaming to a public IN-structured network with which a roaming agreement exists.

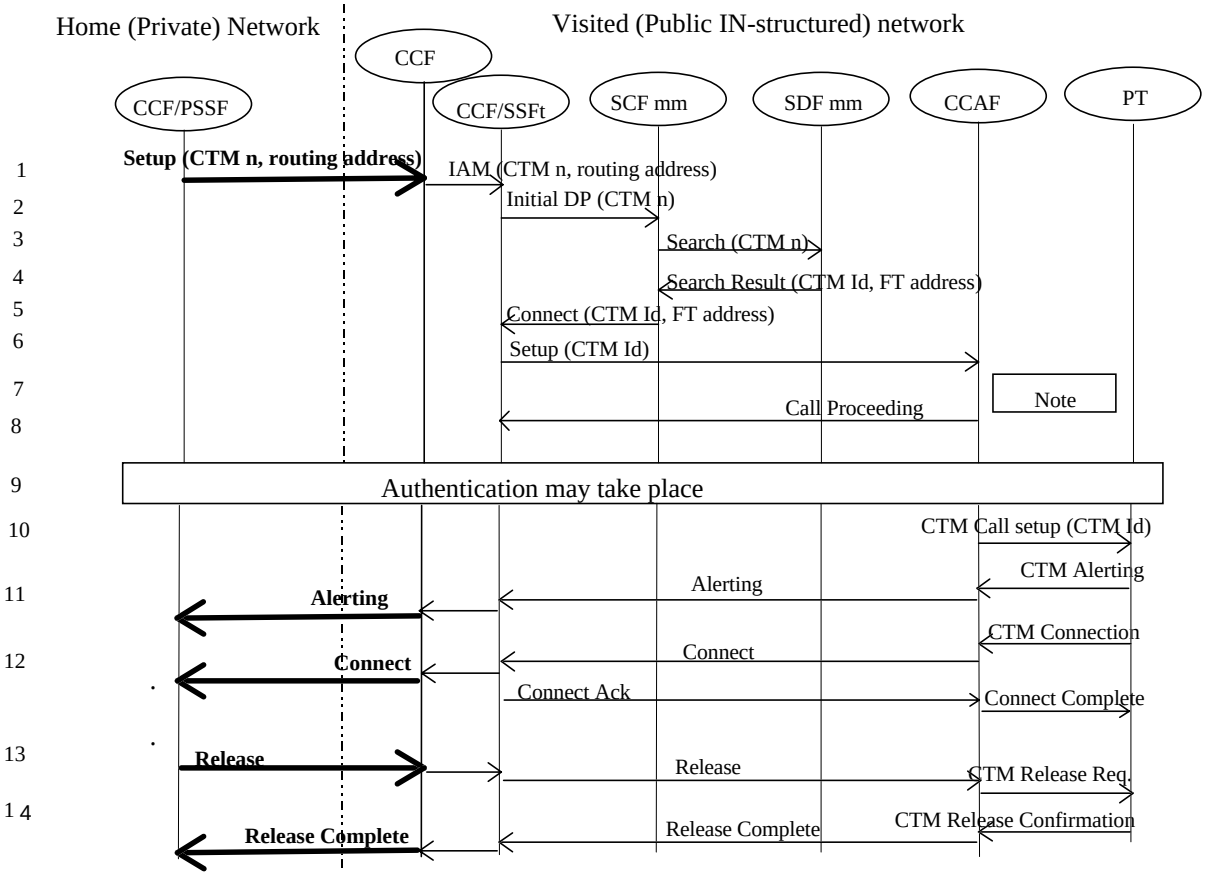


Figure 24: Scenario B: Private CTM user roaming in a public IN network - Incoming call

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

1 The home (private) network (CCF/PSSF of gateway) sends the Setup information flow, continued with an IAM, which contains the CTM number and routing address to the CCF/SSF in the area where the private CTM user is currently registered.

2-5 An Initial DP is sent to the SCF mm, followed by a search/response pair of information flows to/from the SDFmm to identify the user and the current location. The SCFmm then requests the CCF/SSF to continue call set up.

6-8 A Setup information flow including the CTM Id is forwarded to the appropriate FT, which pages the private CTM user who is currently roaming to a public IN-structured network.

9 It is assumed that authentication is performed after successfully paging the PT, however, may also be performed at other points.

10-14 Call set up to the PT is continued. 'Alerting' will be returned, followed by 'Connect'. At the end of the call 'RELease' confirmed by 'RELease Complete' will be transported via the networks involved.

Comment: Two cases can be envisaged: the setup is continued independently from the authentication completion, or the SCF mm requests the setup after successful authentication.

7.2.4 Outgoing Call

Case 1: No use of home network services

A call from a private CTM user who roams in a public IN-structured network may be forwarded by the public network to a destination (in a public or private network). The visited (public IN-structured) network can handle the call without routing to the home (private) network. Authentication within the visited (public IN-structured) network would be required (see Authentication, subclause 7.2.1.1, case a (figure 17) or case b (figure 18) before doing so. Ciphering is performed in the visited network, using the DCK obtained during terminal authentication. For CTM phase 1 it is assumed that a private CTM user may make calls when roaming to a public IN-structured network with which a roaming agreement exists.

Some other mechanisms could also be used.

Case 2: Use of home network services

Alternatively, a call from a private CTM user who roams in a public IN-structured network may be routed via the home network. Authentication within the home (private) network would be required (see Authentication, subclause 7.2.1.2). Ciphering is performed in the visited network, using the DCK obtained during terminal authentication.

History

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