INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.1721

(06/2000)

SERIES Q: SWITCHING AND SIGNALLING
Signalling requirements and protocols for IMT-2000

Information flows for imt-2000 capability set 1

ITU-T Recommendation Q.1721

(Formerly CCITT Recommendation)

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4 AND No. 5	Q.120–Q.249
SPECIFICATIONS OF SIGNALLING SYSTEM No. 6	Q.250–Q.309
SPECIFICATIONS OF SIGNALLING SYSTEM R1	Q.310–Q.399
SPECIFICATIONS OF SIGNALLING SYSTEM R2	Q.400–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	**Q.1700–Q.1799**
BROADBAND ISDN	Q.2000–Q.2999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T RECOMMENDATION Q.1721

INFORMATION FLOWS FOR IMT-2000 CAPABILITY SET 1

Summary

This Recommendation specifies Stage 2 information flow procedures for the support of end-to-end inter-family and inter-system IMT-2000 Capability Set 1 (CS-1) services and network capabilities. The areas covered are mobility management, call and bearer control, services control, and over-the-air authorization services.

Source

ITU-T Recommendation Q.1721 was prepared by ITU-T Study Group 11 (1997-2000) and was approved under the WTSC Resolution 1 procedure on 15 June 2000.

Keywords

CN, CS-1, IMT-2000, LMFh, LMFv, MT, NNI, RAN, UIM, VHE.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Page

Page

Recommendation Q.1721

INFORMATION FLOWS FOR IMT-2000 CAPABILITY SET 1

1 Scope

This Recommendation provides the Stage 2 end-to-end inter-family information flows for IMT-2000 Capability Set 1 (CS-1) services and network capabilities. It is specified according to the Stage 2 methodology described in ITU-T Recommendation Q.65 [1]. Companion ITU-T Recommendations, Q.1701 [2] and Q.1711 [3], form the basis for this Recommendation. Used together, these Recommendations form a Stage 2 description that identifies the functional capability and information flows needed to support the Stage 1 IMT-2000 services and network capabilities.

This Recommendation covers information flows for the UIM to MT interface, the MT to RAN+CN interface, and the CN to CN interface (also known as the NNI.) The information flows described cover the successful cases only. The unsuccessful cases are outside the scope of this Recommendation and are best handled as part of the Stage 3 development. Companion Q-series Recommendations Q.1731, Q.1741 and Q.1751 complement the end-to-end view of Recommendation Q.1721 by addressing interface specific aspects of these interfaces.

This Recommendation does not include Radio Resource Management (RRM), Base Station Management (BSM) or RAN-CN information flows. RRM is covered elsewhere. BSM and RAN-CN information flows are outside the scope of IMT-2000 CS-1 per section 8.1/Q.1701.

The following paragraphs provide a brief overview of the contents of each of the clauses of this Recommendation.

Clauses 2, 3 and 4 provide references, definitions and a list of abbreviations and acronyms relevant to the content of this Recommendation.

Clause 5, "Introduction", provides context for the remainder of this Recommendation. It includes the overall protocol architecture, identification of the functional models used from Recommendation Q.1711, an end-to-end network model, information flow sequence types and the information flow template.

Clause 6, "Mobility Management", describes the information flows for managing authentication, including UIM holder verification, user and network authentication and terminal identification. It then addresses location management, including geographic positioning, subscriber data management, user profile interrogation, identity retrieval, registration management and location data fault recovery.

Clause 7, "Call and Bearer Control", describes basic incoming and outgoing mobile calls, including terminal paging, routing, emergency calls and priority calls.

Clause 8, "Multimedia Call and Bearer Control", describes information flows and procedures for changing a teleservice during a call (switching between voice and data communications), adding and dropping a medium within an existing call, and changing communication configurations by adding and dropping a party in a data call. Access to the Internet is also covered in this clause.

Clause 9, "Virtual Home Environment", provides the information flows for the Direct Home Command (DHC) and Relay Service Control (RSC) methods. (The use of IN to support supplementary services within a network is outside the scope of this Recommendation.)

Clause 10, "Messaging Service Applications", describes short message services, teleservice message broadcast and message waiting notification information flows and procedures.

Clause 11, "Generic Supplementary Service Procedures", provides information flows for a suite of general purpose procedures that may be used by various supplementary services.

Clause 12, "Over-the-Air Service Provisioning", describes information flows for over-the-air service provisioning procedures.

Clause 13, "Definitions of Information Elements", defines what the various information elements used in this Recommendation mean.

Annex A provides a listing of all the common procedure modules used within this Recommendation and the clause number where they are described.

Appendix I, "Q.1721 Coverage of Table 1/Q.1701, Capability Set 1 Requirements", provides linkage between Table 1/Q.1701, the capabilities required of IMT-2000 Capability Set 1 and the contents of this Recommendation.

Appendix II, "A-Key Generation", provides a brief overview of this topic, including the Diffie-Hellman algorithm.

Appendix III, "Bibliography", provides a list of additional references to supplement the specific references listed in clause 2.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently available ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation Q.65 (2000), *The unified functional methodology for the characterization of services and network capabilities including alternative Object Oriented Techniques.*

[2] ITU-T Recommendation Q.1701 (1999), *Framework for IMT-2000 networks.*

[3] ITU-T Recommendation Q.1711 (1999), *Network functional model for IMT-2000.*

[4] ITU-T Recommendation A.3 (1996), *Elaboration and presentation of texts and development of terminology and other means of expression for Recommendations of the ITU Telecommunication Standardization Sector.*

[5] ITU-T Q.1200-series Recommendations, *Intelligent networks.*

[6] ITU-T Recommendation E.164 (1997), *The international public telecommunication numbering plan.*

[7] ITU-T Recommendation E.212 (1988), *Identification Plan for Land Mobile Stations.*

[8] ITU-T Recommendation E.213 (1988), *Telephone and ISDN numbering plan for land mobile stations in public land mobile networks.*

[9] ITU-T Recommendation X.121 (1996), *International numbering plan for public data networks.*

[10] ITU-T Recommendation Q.931 (1998), *ISDN user-network interface layer 3 specification for basic call control.*

[11] ITU-T Recommendation Q.762 (1997), *Signalling System No. 7 – ISDN User Part general functions of messages and signals.*

3 Definitions

This Recommendation defines the following terms:

3.1 anchor core network: In a data session roaming environment, the anchor core network is the network where the data session is initiated and a packet service gateway is assigned to the mobile terminal. The anchor core network may be either the home or the visited network.

3.2 man machine interface: The interaction of the user and network via a subscriber device.

3.3 request indication: The information flow sent from one functional entity to another requesting a specific action. This is referred to as req.ind.

3.4 response confirmation: The information flow sent by the requested functional confirming that the requested action has been successfully completed. This is referred to as resp.conf.

3.5 service application: The provision of services by general purpose capabilities, such as Intelligent Network capabilities as applied at the home location or at a visited location as part of a Virtual Home Environment.

3.6 service control: Functions that set or modify the context, in which basic calls and bearers are established, modified and released.

3.7 subscriber: The user of a mobile terminal who has subscribed to the service.

3.8 supplementary service application: The provision of a specific supplementary service, typically through use of service specific capabilities, whether at the home location or at the visited location as part of a Virtual Home Environment.

3.9 user: The user of a mobile terminal.

3.10 virtual home environment: The provision of a service experience to the subscriber identical to, or as similar as possible to the service environment the subscriber experiences when served at his/her home location.

NOTE 1 – The terms "user" and "subscriber" are used interchangeably in this Recommendation.

NOTE 2 – The home network is synonymous with home core network (CNh).

NOTE 3 – The visited network is synonymous with visited core network (CNv).

Clause 13, "Definitions of Information Elements", defines what the various information elements used in this Recommendation mean.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

A-key	Authentication Key
AC	Authentication Centre
ACSM	Authentication Control State Model
ADDS	Application Data Delivery Service
AMF	Authentication Management Function
AMSC	Anchor Mobile Switching Centre
AMSM	Authentication Management State Model
ARF	Access link Relay Function
AUTH	Authentication Response
BCSM	Basic Call State Model

BS	Base Station
CC	Call Control
CCAF'	Call Control Agent Function (enhanced)
CCF	Call Control Function
CCF'	Call Control Function (enhanced)
CHCNT	Call History Count
CN	Core Network
CNa	Core Network (anchored)
CnCAF	Connection Control Agent Function
CnCF	Connection Control Function
CNdest	Core Network (destination)
CNh	Core Network (home)
CNpv	Core Network (previous visited)
CNs	Core Network (supporting)
CNv	Core Network (visited)
conf.	confirmation
CS	Capability Set
DFP	Distributed Functional Plane
DHC	Direct Home Command
FE	Functional Entity
FEA	Functional Entity Action
FT	Fixed Terminal
GC	Global Challenge/response mechanism
GPCF	Geographic Position Control Function
GPF	Geographic Position Function
ID	Identity
IF	Information Flow
IMT-2000	International Mobile Telecommunications-2000
IMUI	International Mobile User Identity
IN	Intelligent Network
ind.	indication
IP	Internet Protocol
ISP	Internet Service Provider
ITDN	International Temporary Directory Number
LMF	Location Management Function
LMFh	Location Management Function (home)
LMFp	Location Management Function (packet)

LMFv	Location Management Function (visited)
LMSM	Location Management State Model
MCF	Mobile Control Function
MGPF	Mobile Geographic Position Function
MMI	Man Machine Interface
MRTR	Mobile Radio Transmission and Reception
MSC	Mobile Switching Centre
MT	Mobile Terminal
MWN	Message Waiting Notification
NAI	Network Access Identifier
NNI	Network-to-Network Interface
OTASP	Over-the-Air Service Provisioning
PDGN	Packet Data Gateway Node
PDN	Public Data Network
PDSN	Packet Data Serving Node
PIN	Personal Identification Number
PSCAF	Packet Service Control Agent Function
PSCF	Packet Service Control Function
PSGCF	Packet Service Gateway Control Function
QoS	Quality of Service
RACAF	Radio Access Control Agent Function
RAN	Radio Access Network
RAND	Random Number
RANDC	Random Number (Challenge)
RANDG	Random Number (Global)
req.	request
resp.	response
RF	Radio Frequency
RFTR	Radio Frequency Transmission and Reception
RNC	Radio Network Controller
RSC	Relay Service Control
SACF	Service Access Control Function
SCF	Service Control Function
SCP	Service Control Point
SDF	Service Data Function
SDP	Service Data Point
SIBF	System access Information Broadcast Function

SLP	Service Logic Program
SMF	Service Management Function
SMS	Short Message Service
SNCF	Satellite Network Control Function
SPI	Security Parameter Index
SRES	Signature Result
SRF	Specialized Resource Function
SSD	Shared Secret Data
SSF	Service Switching Function
TMB	Teleservice Message Broadcast
TMUI	Temporary Mobile User Identifier
UC	Unique Challenge/response mechanism
UIM	User Identity Module
UIMF	User Identification Management Function
UPT	Universal Personal Telecommunication
USSD	Unstructured Supplementary Service Data
VHE	Virtual Home Environment

5 Introduction

This Recommendation describes the information flows for end-to-end inter-family IMT-2000 procedures, which are necessary for the support of IMT-2000 CS-1 services and network capabilities. The description of information flows contains the list of information elements that are exchanged between the interacting functional entities. In addition, the functional entity actions (FEAs) performed by the receiving entity are also described.

The modelling techniques used in describing the information flows for IMT-2000 procedures are outlined below.

The information flows specified in this Recommendation for the various IMT-2000 services and network capabilities control many aspects of the IMT-2000 network for which signalling and protocol requirements need to be specified. These are as follows:

- Service control, including:
  - multimedia services;
  - Virtual Home Environment (VHE);
  - messaging services; and
  - supplementary services.
- Mobility management and Authentication control.
- Call control.
- Bearer control.

This Recommendation does not address radio resource management.

Common procedure modules are listed in Annex A. These basic modules are reused in a variety of tasks which are composites of these basic procedures and other procedures specific to those tasks.

A fundamental principle that has been applied throughout this Recommendation is "separation of concerns". Strict separation enables both functional and protocol independence for each of the areas addressed, thereby ensuring that each may evolve and provide greater capabilities without requiring that other areas be reworked simultaneously.

Within the framework of IMT-2000 networks, as specified in Recommendation Q.1701, Figure 5.1 captures the boundaries where these separations have been applied to guide the development of IMT-2000 signalling and protocol requirements.

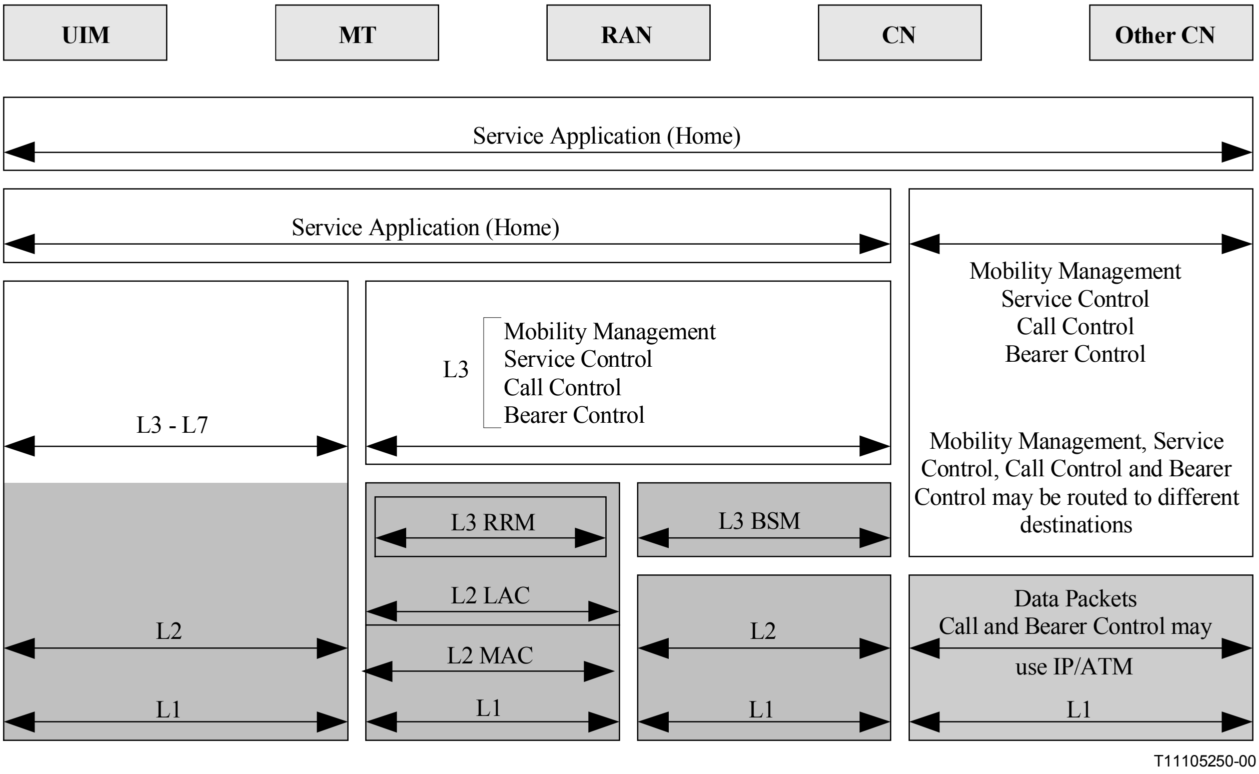


Figure 5-1/Q.1721 – Overall information flows architecture

5.1 Description of information flow modelling techniques

This subclause provides two functional models specified in ITU-T Recommendation Q.1711 [3], namely, "Integrated call control and connection control model" and "Separated call control and connection control model". In addition, this subclause defines an end-to-end subsystem relationship model.

5.1.1 Functional models

Figure 5.1.1-1 is the same as Figure 5-1a/Q.1711 and is an IMT-2000 functional model illustrating an integrated call control and connection control FE. Refer to clause 6/Q.1711 for details.

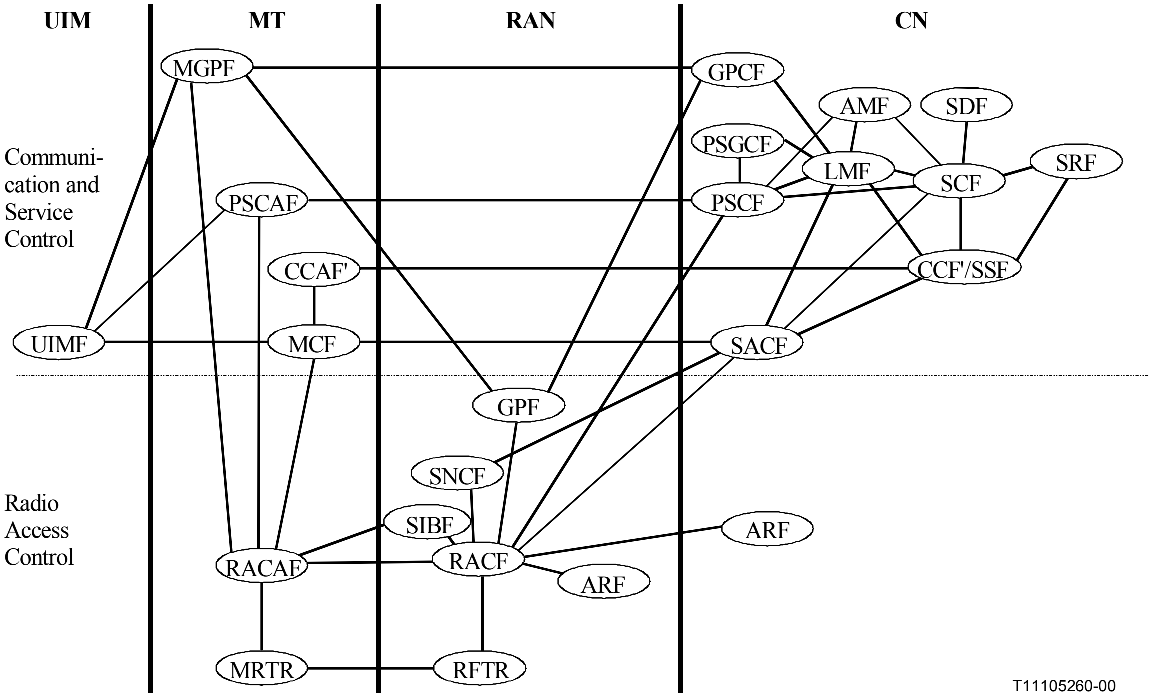


Figure 5.1.1-1/Q.1721 – IMT-2000 functional model (integrated call control and connection control)

Figure 5.1.1-2 is the same as Figure 5-1b/Q.1711 and is an IMT-2000 functional model illustrating separated call control and connection control FEs. Refer to clause 6/Q.1711 for details.

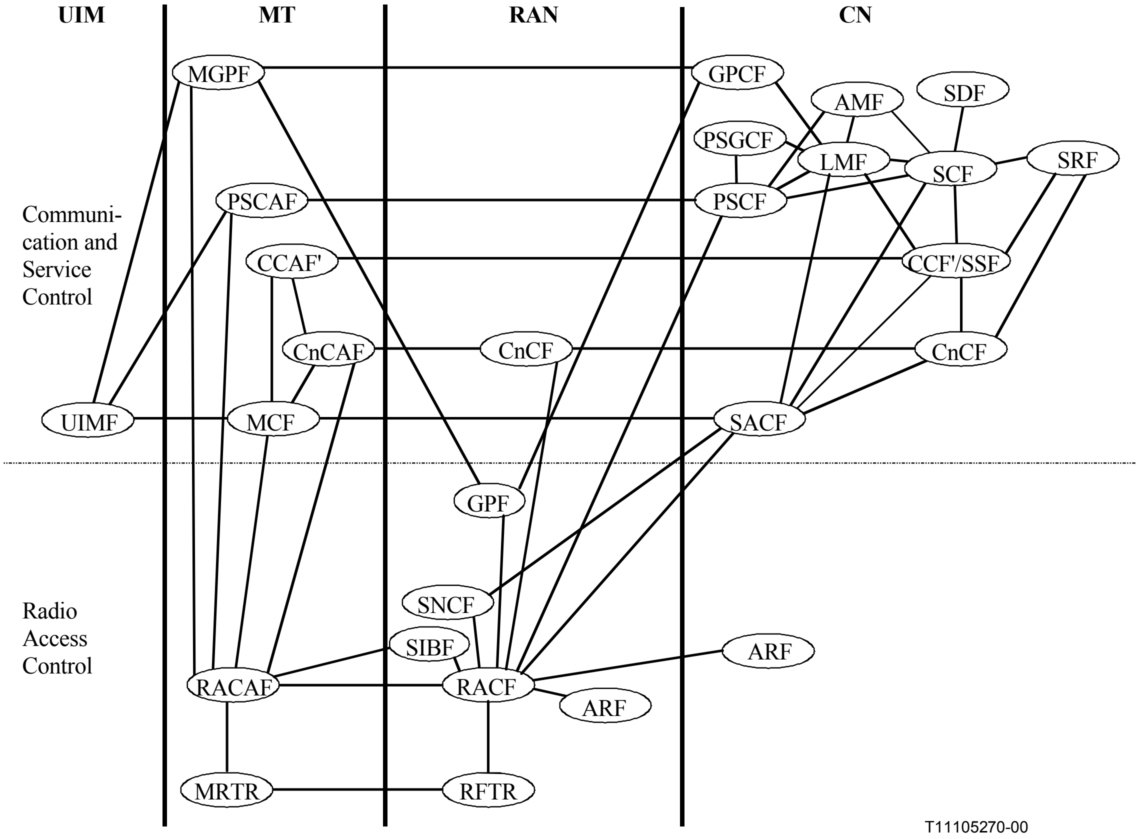
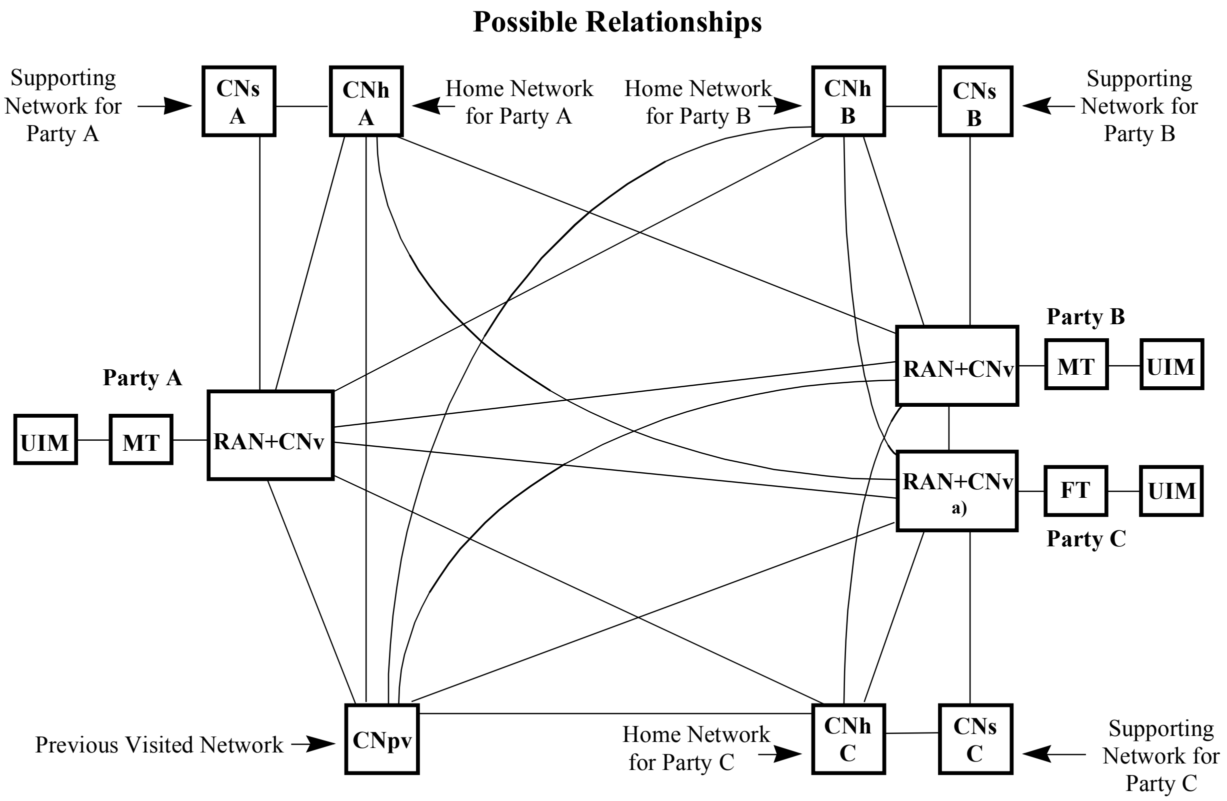


Figure 5.1.1-2/Q.1721 – IMT-2000 functional model (separated call control and connection control)

It should be noted that a mapping of the FEs to the subsystems UIM, MT, RAN and CN, as defined in Q.1701, is also shown in the models to reflect the applicability of the IMT-2000 Family of Systems concept. It should also be noted that the allocation of FEs to the RAN and CN subsystems is preliminary (refer to Q.1711 for more details).

5.1.2 End-to-end subsystem relationship model

The end-to-end functional network relationship model illustrates the network perspective via Functional Subsystems (FS) defined in Q.1701 and Q.1711 (i.e. UIM, MT, RAN and CN) and their associations with multiple users. As illustrated in Figure 5.1.2-1, the end-to-end network model contains three user end points. This is used to illustrate more advanced services such as conference calling, simultaneous establishment of point-to-multipoint bearer services.



T11105280-00

RAN+CN	Visited Radio Access Network + Core Network
UIM	User Identity Module
MT	Mobile Terminal
CNpv	Previous visited Core Network
CNh	Home Core Network
CNs	Supporting Core Network
FT	Fixed Terminal

[a] This Functional Subsystem could be replaced by other network subsystems to illustrate internetworking with other networks such as PSTN, ISDN, etc.

Figure 5.1.2-1/Q.1721 – The IMT-2000 end-to-end subsystem relationship model

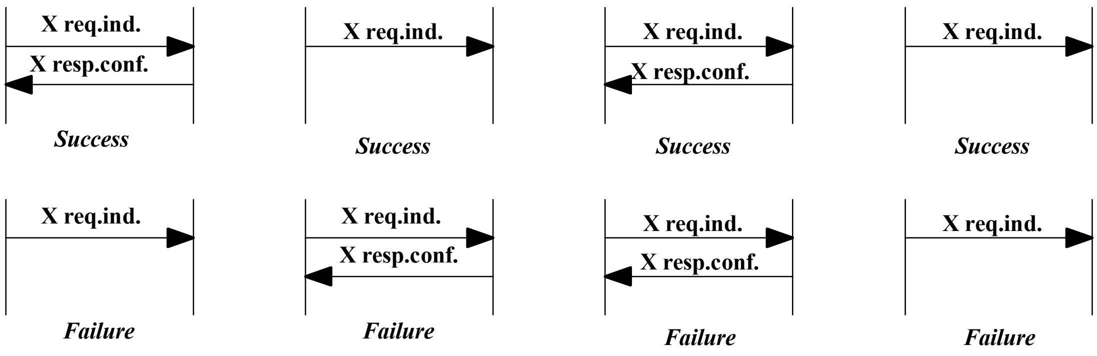
The Core Network may serve in several different roles:

- CNpv = Core Network (previous visited): The network entity that previously was associated with the visited mobile terminal.
- CNh = Core Network (home): where the home Location Management Function (LMFh) and the home Authentication Management Function (AMFh) are located.
- CNs = Core Network (supporting network): where the home Service Control Function (SCFh), home Service Data Function (SDFh) and the home Specialized Resource Function (SRFh) are located.

5.1.3 Information flow sequence type

An information flow consists of two parts: Information Flow Function Name and Flow Sequence Type. Figure 5.1.3-1 illustrates the possible action types.

Flow Sequence Type I (Confirmed Success: Failure is not reported)	**Flow Sequence Type II** (Confirmed Failure: Success is not reported)	**Flow Sequence Type III** (Confirmed Success or Failure: whichever applies is reported)	**Flow Sequence Type IV** (Unconfirmed: neither Success nor Failure is reported)



NOTE – "X" represents Information Flow Function Name, while req.ind. is an example of a type that could be associated with the Information Flow Function Name.

T11105290-00

Figure 5.1.3-1/Q.1721 – Information flow sequence type

The above figure illustrates four types of information flow sequences. Each type describes the specific information flows that constitute that type. The first type is client-server information flow sequence, and the result is a confirmed success, with failure not confirmed. The second type is also client-server information flow sequence, but the result is a confirmed failure, with success not confirmed. The third type is a confirmed notification of either success or failure as applicable. The fourth type is an unconfirmed notification.

The "resp.conf." flow is in response to a previous "req.ind." flow, and as such it carries a unique "Transaction ID" associated with it. This "Transaction ID" is used to tie each pair of "req.ind." and "resp.conf." flows. Therefore, there is no need to repeat any user identification such as IMT-2000 International Mobile User Identity (IMUI) or IMT-2000 International Mobile Directory Number (IMDN) within the "resp.conf." flow.

5.2 Information flow template

This subclause describes the template used in developing the information flow (IF) procedures.

X.Y.Z "Name of procedure (e.g. Terminal location registration)"

In this clause, provide a brief prose description of the service or network capability. "X.Y.Z" is the subclause heading number in Q.1721. This subclause contains a detailed information flow diagram for the service or network capability using the template provided below. See Figure 5.2-1.

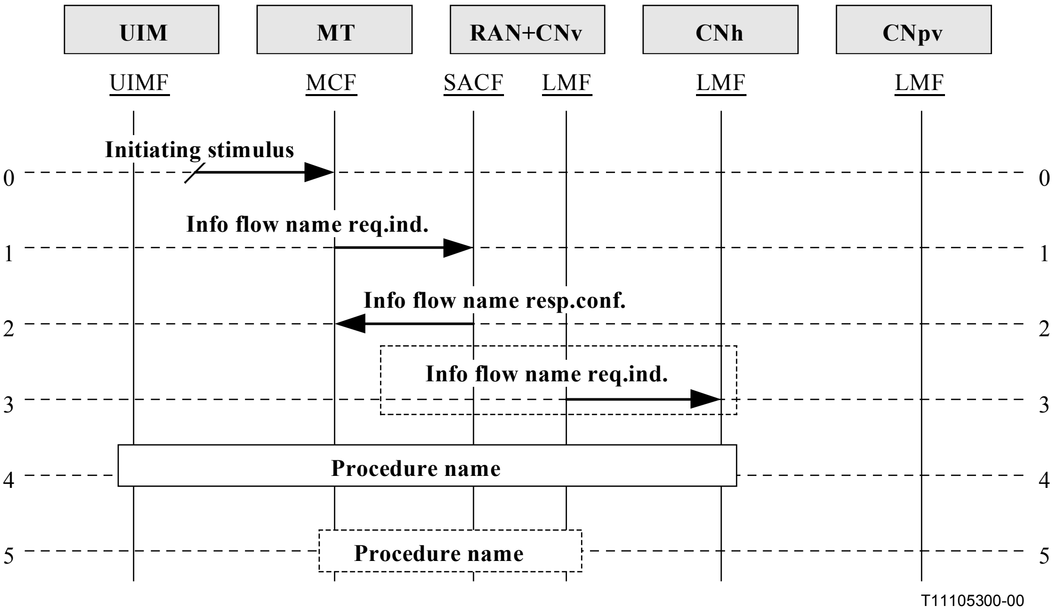


Figure 5.2-1/Q.1721 – The IMT-2000 information flow diagram template

This subclause consists of paragraphs each dedicated to one information flow of the IF diagram. For each information flow, a detailed description is provided on the information flow name, type (e.g. req.ind. or resp.conf.), the information elements within the information flow, whether each IE is mandatory or optional (M/O), in the sequence as shown in the IF diagram. FE actions (FEA) are also provided in this clause. Common actions such as "receiving and analysing a flow" and "generating the next flow" are assumed for each entity that receives a flow and, therefore, not included in the description of FEAs. This subclause format is proposed as follows:

0. **Initial information flow**: *Describe initiating FE Action (FEA) leading to the first IF (Flow #1).*

FEA0	– Describe the action of the FE at the receiving end of this flow.

1. **Information flow #1, flow name, flow sequence type**: *A brief description of the flow and its start and end FEs to be followed by the content of the flow's information elements, as shown in the table below. When an IE is "O", conditions for its inclusion must be specified and response to its presence when received must also be specified, e.g.: include IE #2 when condition xyz occurs. For IFs that are of req.ind. type, indicate whether a response is required based on successful outcome to the received IF, failed outcome, both or neither, e.g. "Response: Success or Failure".*

IF name (Response: Success/Failure/Success or Failure/None)	req.ind.
IE #1 (e.g. Called user identity)	M/O
IE #2	M/O
IE #3	M/O

FEA1	– Description of functional entity action(s) at receiving end of this flow.
NOTE – Describe the conditions of optionality for IEs that are optional.	

2. **Information flow #2, flow name, flow type**: *A brief description of the flow and its start and end FEs to be followed by the content of the flow's information elements as follows. When an IE is "O", conditions for its inclusion must be specified and response to its presence when received must also be specified, e.g.: when IE #6 is received, do wxy. For resp.conf., indication of Response is not applicable.*

IF name	resp.conf.
IE #4	M/O
IE #5	M/O
IE #6	M/O

FEA2	– Description of functional entity action(s) at receiving end of this flow.
NOTE – Describe the conditions of optionality for IEs that are optional.	

3. **Information flow #3, flow name, flow sequence type**: *A brief description of the flow and its start and end FEs to be followed by the content of the flow's information elements, as shown below. When an IE is "O", conditions for its inclusion must be specified and response to its presence when received must also be specified, e.g.: include IE #2 when condition xyz occurs. For IFs that are of req.ind. type, indicate whether a response is required based on successful outcome to the received IF, failed outcome, both or neither, e.g. "Response: Success or Failure".*

IF name (Response: Success/Failure/Success or Failure/None)	req.ind.
IE #1	M/O
IE #2	M/O
IE #3	M/O

FEA3	– Description of functional entity action(s) at receiving end of this flow.
NOTE – Describe the conditions of optionality for IEs that are optional.	

4. **Information flow #4, Procedure name**: *A brief statement about the common procedure that is carried out at this point in the sequence.*

FEA4	– Description of functional entity action(s) at end of this procedure at the FE defined by the specifics of the procedure itself. – If the next procedure is optional as in this template, then include the conditions on when it should or should not be carried out.

5. **Information flow #5, Procedure name**: *A brief statement about the optional common procedure that is carried out at this point in the sequence.*

FEA5	– Description of functional entity action(s) at end of this procedure at the FE defined by the specifics of the procedure itself. – As this completes the procedure illustrated in the template, "No further action" may be indicated.

6 Mobility management

This clause provides the information flows for mobility management related IMT-2000 services and network capabilities.

6.1 Authentication management

6.1.1 UIM holder authorization

This is a feature by which the removable user of the UIM is authorized. This feature only applies when the UIM is used for user association with the IMT-2000 mobile terminals. This is distinct from the "lockout" feature that may be provided by some MT vendors. See Figure 6.1.1-1.

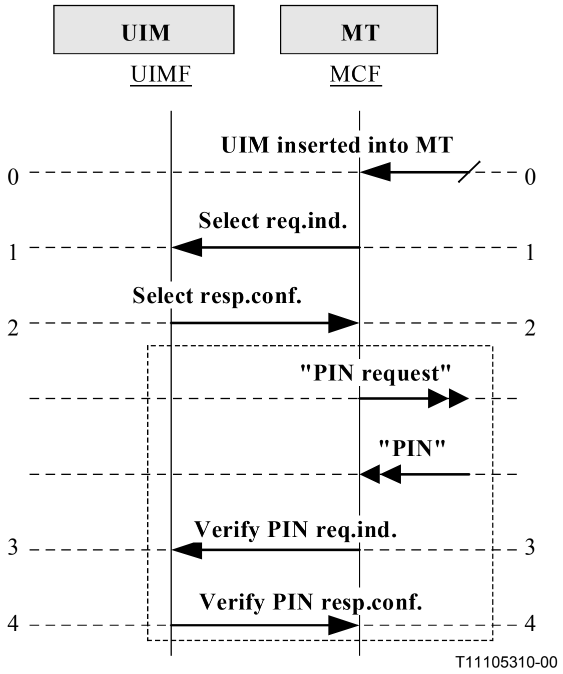


Figure 6.1.1-1/Q.1721 – UIM holder authorization

0. **UIM inserted into MT**: the MT with the UIM inserted is powered-up.

FEA0	– Initiate UIM holder verification procedure.

1. **Select req.ind.**: is used to select the appropriate file(s) in a UIMF.

Select (Response: Success or Failure)	req.ind.
File ID	M

FEA1	– Select appropriate file(s) in the UIMF.

2. **Select resp.conf.**: is the response to the request.

Select	resp.conf.
File ID	M (Note)
PIN Format	M

FEA2	– Interact with user to obtain PIN.
NOTE – Either confirming system or requesting alternate if different.	

3. **Verify PIN req.ind.**: is used to verify PIN.

Verify PIN (Response: Success or Failure)	req.ind.
PIN	M

FEA3	– Compare the user entered PIN with the PIN stored in the UIM.

4. **Verify PIN resp.conf.**: is the response to the request.

Verify PIN	resp.conf.
Result	M

FEA4	– If a successful response is returned then the UIM user is valid and the terminal is authorized.

6.1.2 User authentication

The international mobile user identity (IMUI) authentication process is the verification by the core network that the IMT-2000 MT/UIM identity (IMUI or TMUI) is the one claimed. The authentication is composed of a challenge/response protocol showing knowledge of a secret key, called the Authentication Key (A-key), which is shared between and available only to the IMT-2000 MT/UIM and the Authentication Centre (AC) in the user's home network. The purpose of this authentication security procedure is to protect the network against unauthorized use.

The network may trigger the authentication IMT-2000 process when:

- the subscriber registers in a serving system (including location updates, attached/detached directives); or
- the subscriber originates a call; or
- the subscriber is responding to a page; or
- the subscriber is responding to an SMS page; or
- based on an operator's policies, including management of supplementary services, testing, periodic challenging of a user authentication, Shared Secret Data updates, etc.

If an MT authentication procedure fails then the access to the IMT-2000 network shall be denied, except in case of emergency calls. It should be noted that a service provider may optionally allow this MT access to the network in case the authentication cannot be performed by the serving system and the home LMFh/AMF cannot be reached due to a network overload or failure.

Three different authentication procedures are defined for an IMT-2000 network: two "Unique challenge/response mechanisms (UC)" and the "Global challenge mechanism (GC)" as described below. In the case of inter-system operation between different IMT-2000 family members, the visited system initiates the authentication mechanism according to its capabilities. This implies that a home system shall support the authentication request from the visited system in order to support roaming across IMT-2000 family members.

Two additional security-related procedures are performed after the successful completion of user authentication procedures. The first is the procedure to "start ciphering" and the second is the "TMUI assignment" procedure.

6.1.2.1 Authentication Key

The subscriber's authentication key (A-key) shall be known and stored only in the MT and in the home Authentication Centre (AC). The A-key shall never be transmitted over the air or over the network, and its integrity is essential for an effective authentication process.

6.1.2.2 Unique challenge/response user authentication mechanism based on Triplets Authentication Vectors

The Unique challenge/response user authentication mechanism consists of the following exchange between the visited network and the UIM.

- The visited network transmits a non-predictable random number RAND to the UIM.
- The UIM computes the signature based on the received RAND, using the user authentication algorithm and the user secret authentication key, and transmits the signature result (SRES) to the visited network.
- The visited network checks the signature result.

See Figure 6.1.2.2-1.

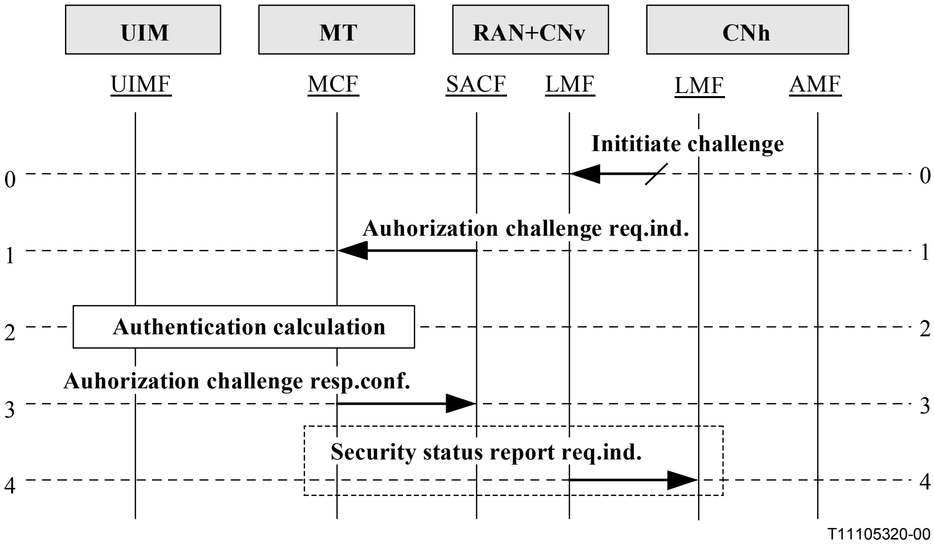

UIM
MT
RAN+CNv
CNh
UIMF
MCF
SACF
LMF
LMF
AMF
Inititiate challenge
Auhorization challenge req.ind.
Authentication calculation
Auhorization challenge resp.conf.
Security status report req.ind.
0
1
2
3
4
T11105320-00

Figure 6.1.2.2-1/Q.1721 – Unique challenge/response user authentication

0. **Initiate challenge request**: the SACF receives an Initiate challenge request. This happens when the LMFv finds that user authentication is needed.

FEA0	– Initiate authentication challenge.
NOTE – The optional Authentication key management procedure is executed to obtain authentication triplets if they are not available. Refer to the Authentication key management procedure for details.	

1. **Authentication challenge req.ind.**: is used to verify the identity of the user.

Authentication challenge (Response: Success or Failure)	req.ind.
Challenge	M

FEA1	– Initiate Authentication calculation.

2. **Authentication**: procedure is performed.

3. **Authentication challenge resp.conf.**: is sent by the MCF to the SACF to convey the result of the authentication calculation.

Authentication challenge	resp.conf.
Challenge Response	M

FEA3	– Determine if a Security status report is needed.

4. **Security status report req.ind.**: is used to send a security status report to the home network (optional).

Security status report (Response: None)	req.ind.
Result	M
IMUI	O (Note)

FEA4	– Analyse security status report.
NOTE – IMUI must be included, if available.	

6.1.2.2.1 Authentication key management

The subscriber authentication key, A-key, is allocated, together with the IMUI, at subscription time.

The A-key is stored on the network side in the Home Network (AMFh), in an Authentication Centre (AC.)

An IMT-2000 network may contain one or more ACs. An AC can be physically integrated with other functions, e.g. with a home Location Register (LMFh.) A subscriber shall be associated with only one AC.

When needed for each MT, the LMFv requests security related information from the AMFh corresponding to the MT. This includes an array of pairs of corresponding RAND and SRES. These pairs are obtained by applying the user authentication algorithm to each RAND and A-key. The pairs are stored in the LMFv as part of the security related information.

For the unique challenge mechanism, authentication triplets may be generated in batches by the AMFh in the Authentication Centre and sent via the LMFh to the LMFv.

See Figure 6.1.2.2-2.

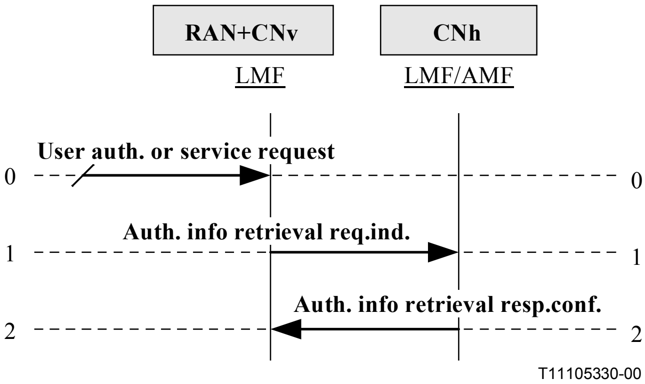

RAN+CNv
CNh
LMF
LMF/AMF
User auth. or service request
0
0
Auth. info retrieval req.ind.
1
1
Auth. info retrieval resp.conf.
2
2
T11105330-00

Figure 6.1.2.2-2/Q.1721 – Authentication key management

0. **User authorization or service request**: the subscriber identity is received, the LMFv checks whether a user authentication is necessary.

FEA0	– If there is not enough authentication information in the LMFv to perform the authentication, an authentication information retrieval request is sent to the LMFh.

1. **Authentication information retrieval req.ind.**: is used to request security information from the LMFh for user authentication.

Authentication information retrieval (Response: Success or Failure)	req.ind.
IMUI	M

FEA1	– Retrieve security information. – Retrieve challenge and response information for authentication.

2. **Authentication information retrieval resp.conf.**: contains the result of Authentication information retrieval req.ind.

Authentication information	resp.conf.
Challenge(s)	M
Challenge Response(s)	M
Result	M
Ciphering Key	O (Note)

FEA2	– Store authentication information.
NOTE – For the triplet-based authentication mechanism, the Ciphering key must be available for some network accesses, e.g. location updates, paging responses, call initiation, etc.	

6.1.2.2.2 Transfer of unused authentication triplets during location update

When a user moves into another LMFv, unused triplets from the previous LMFv may be transferred to the new LMFv. This capability is used only when the authentication is done using TMUI (see Figure 6.2.2).

6.1.2.2.3 Authentication calculation

This procedure is initiated by the MT towards the UIM requesting execution of the authentication calculation algorithm for the purpose of authenticating a user signature.

NOTE – The UIMF holds the authentication key which is used to calculate authentication result. From the security point of view, the authentication key must not be retrieved from outside this functional entity. Therefore, a procedure to request the UIMF to execute an authentication calculation is necessary. This procedure is a common procedure for Unique challenge/response and Global challenge user authentication mechanisms.

See Figure 6.1.2.2-3.

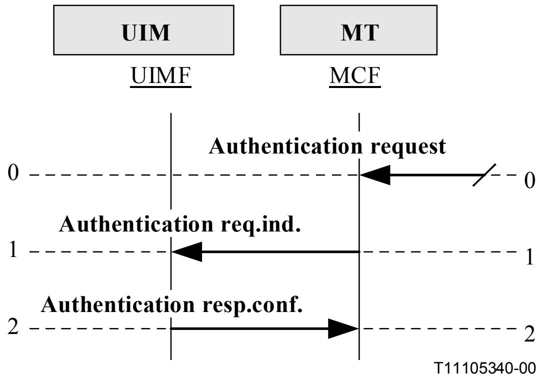


Figure 6.1.2.2-3/Q.1721 – Authentication calculation

0. **Authentication request**: the MCF receives an Authentication request.

FEA0	– Initiate authentication calculation.

1. **Authentication req.ind.**: is used to request the authentication calculation be carried out using the random number and authentication key.

Authentication (Response: Success or Failure)	**req.ind.**
RAND	M

FEA1	– The UIMF calculates the authentication signature using the random number supplied by the MCF and the user authentication key stored in the UIMF.

2. **Authentication resp.conf.**: is used to return the authentication calculation result.

Authentication	**resp.conf.**
Signature result	M
Ciphering key(s)	M

FEA2	– Receive authentication calculation response.

6.1.2.3 Global challenge

A global challenge is the radio interfaces message (RAND) that is broadcast on a common system-wide information channel. Its generation and update frequency are under the control of the network operator, and should be in accordance with good authentication practices.

When attempting a network access or a response to an SMS page, the mobile station has to include its authentication signature. The calculated authentication signature is based on secrets that were distributed during the subscription process. The global challenge response information elements include, but are not limited to, a subscription identifier, a confirmation of the received global challenge (RANDC), an authentication response (AUTH), a value for the parameter CHCNT. The information elements that comprise the response to the network challenge are generally embedded in network access request messages, such as registrations, call originations, call terminations or SMS page responses. Thus, the global challenge mechanism is not utilized as a stand-alone mechanism, but accompanies other network access protocols in order to minimize message traffic on air interface channels. The global challenge procedure also triggers the calculation of the ciphering keys that are then used for encrypting user traffic. See Figure 6.1.2.3-1.

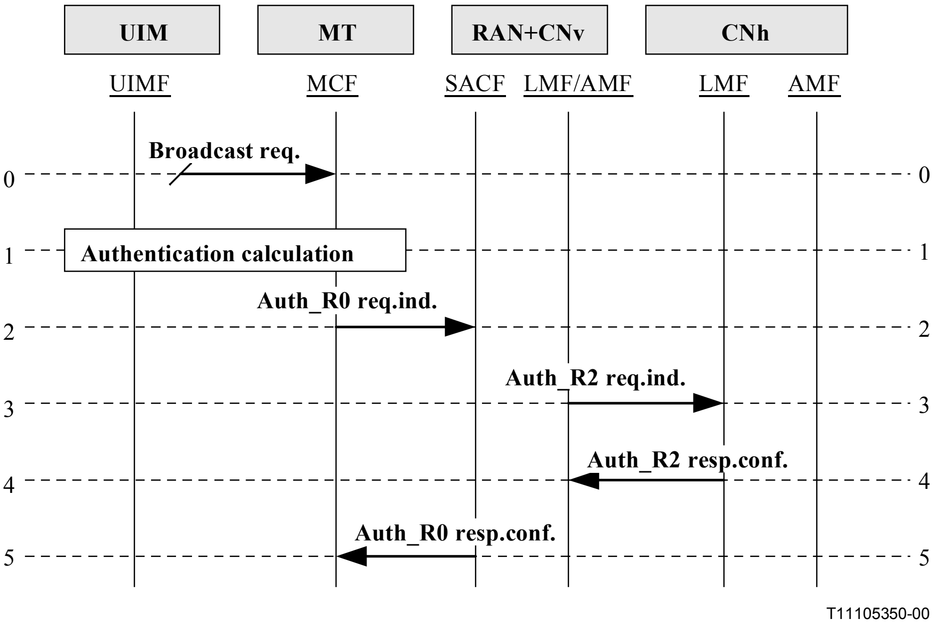


Figure 6.1.2.3-1/Q.1721 – Global challenge user authentication

0. **Broadcast request**: during a system access attempt by the MT, the "global challenge" is read from the system information broadcast channel.

FEA0	– Broadcast "global challenge" is obtained by the mobile station from a common signalling channel, then applied to the authentication algorithm in the UIMF, along with secret user information, to calculate the UIMF's authentication signature (AUTH_R). – Initiate authentication calculation.

1. **Authentication calculation**: is performed.

2. **Auth_R0 req.ind.**: is used as a component of a registration or a service request procedure.

Auth_R0	req.ind.
TMUI	M
Confirmation of RAND (RANDC)	M
AUTH_R	M
CHCNT	M

FEA2	– Verify that Confirmation of RAND (i.e. RANDC) is consistent with global RAND received over the system information channel. – Get user SSD from the serving system LMFv. – If SSD is not available in visited network forward the user authentication response to LMFh, including the full global RAND instead of RANDC. – Perform user authentication procedure. – Calculate applicable ciphering keys.
NOTE – The LMFv supports the global challenge mechanism by participating in the generation and distribution of the global RAND that is broadcast by the serving network on a system-wide information channel. Updates of global RAND are controlled by the serving system.	

3. **Auth_R2 req.ind.**: is used to pass the authentication request to the home network.

Auth_R2 (Response: Success or Failure)	req.ind.
IMUI	M
RANDG	M
AUTH_R	M
CHCNT	M

FEA3	– Calculate applicable ciphering key(s). – Perform user authentication procedure. – Forward confirmation of user validity, along with applicable ciphering key(s), and, under some circumstances, SSD, to LMFv.

4. **Auth_R2 resp.conf.**: is the response providing the security information requested.

Auth_R2	resp.conf.
Result	M
SSD	O (Note 1)
Ciphering Key(s)	O (Note 2)

FEA4	– Forward confirmation of user validity, along with applicable ciphering key(s), and, under some circumstances, SSD, to MCF.
NOTE 1 – If SSD sharing is turned on by the LMFh/AMF, the SSD parameter may be included in this message. NOTE 2 – Returned if available.	

5. **Auth_R0 resp.conf.**: conveys the response to Auth_R0 req.ind. to the MCF.

Auth_R0	resp.conf.
Result	M

FEA5	– Receive a status confirmation from the network as a component of system access attempt.

6.1.2.4 SSD management

6.1.2.4.1 Update of user's shared secret data (SSD update)

In order to minimize network traffic between the serving system and the home AMF, while providing additional protection to the A-key, a secondary authentication key, called Shared Secret Data (SSD), is derived from the subscriber's A-key. The SSD update procedure, by which the MT's SSD is shared with a serving system, may be executed any time at the discretion of the "home" service provider. The SSD update process shall be initiated only after a successful MT authentication. See Figure 6.1.2.4.1-1.

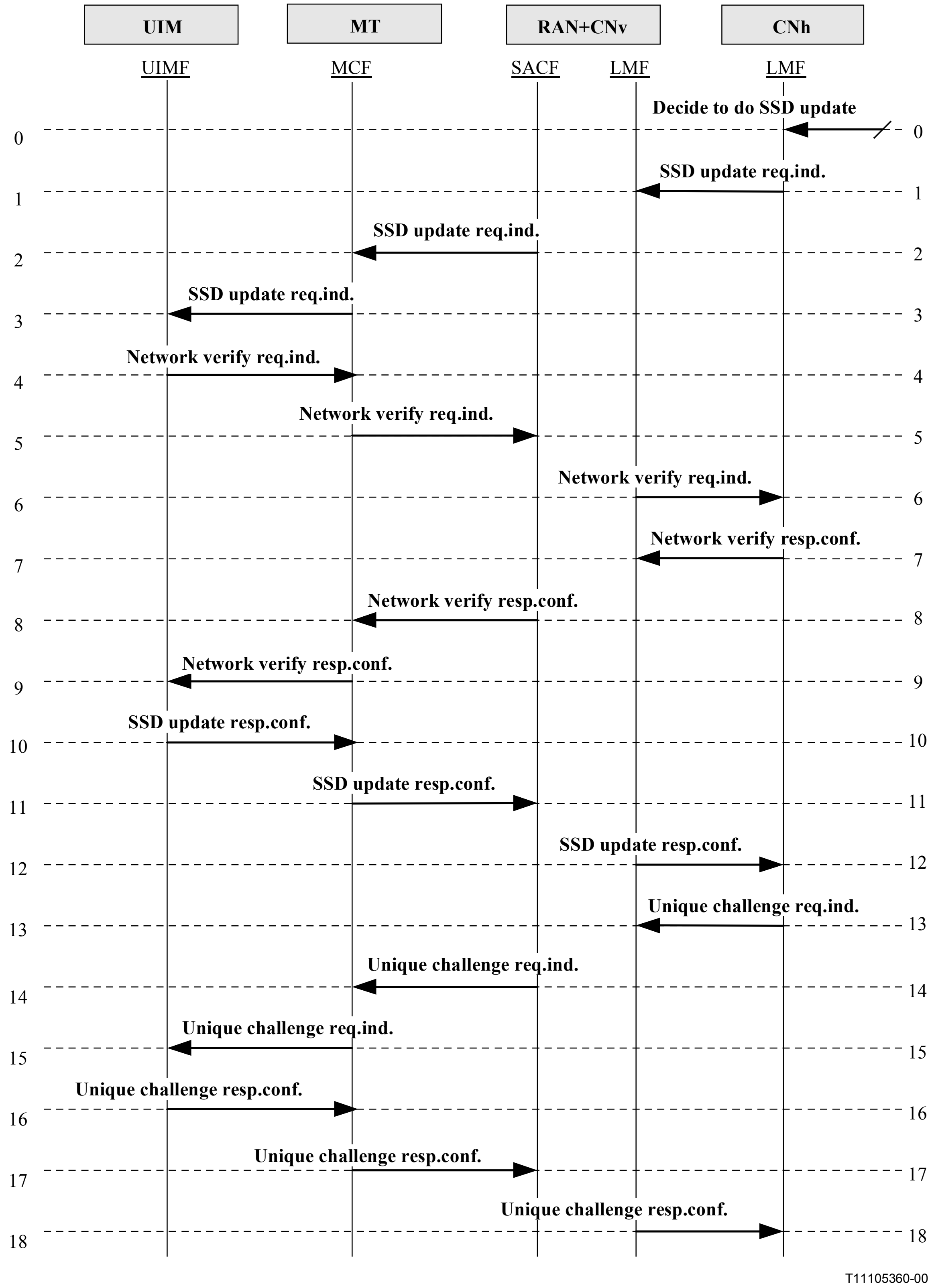


Figure 6.1.2.4.1-1/Q.1721 – SSD update (SSD is not shared)

0. **Decide to do SSD update**: initiates the execution of the SSD update procedure for a selected mobile user in the visited network.

FEA0	– Generate a random number RANDSSD. – Calculate new SSD for mobile user. – Generate RANDU and calculate AUTH_U, using new SSD. – Send SSD update req.ind. to LMFv requesting that the selected mobile user perform an immediate update of his/her SSD.

1. **SSD update req.ind.**: directs the UIMF to update its value of SSD. It is sent from the home system towards the visited system where the mobile user is located. For this procedure to be executed, it is required that the UIM (removable or permanent) be present in the mobile terminal.

SSD update (Response: Success or Failure)	**req.ind.**
IMUI	M
RANDSSD	M
RANDU	M
AUTH_U	M
Ciphering Key(s)	O (Note)

FEA1	– Receive SSD update req.ind. from LMFh, perform IMUI/TMUI translation, and forward it to the MCF.
NOTE – Ciphering Keys are sent if available.	

2. **SSD update req.ind.**: directs the mobile user to update its value of SSD. It is sent from the home system towards the visited system where the mobile user is located. For this procedure to be executed, it is required that the UIM (removable or permanent) be present in the mobile terminal in order to interact with the network.

SSD update (Response: Success or Failure)	**req.ind.**
IMUI	M
RANDSSD	M

FEA2	– Relay SSD update req.ind. from visited network.

3. **SSD update req.ind.**: directs the mobile user to update its value of SSD. It is relayed by the visited system.

SSD update (Response: Success or Failure)	**req.ind.**
IMUI	M
RANDSSD	M

FEA3	– Calculate a new (tentative) SSD. – Generate a random number RANDBS for use in the Network verify IF. – Calculate the expected AUTHBS using the new (tentative) SSD. – Send the Network verify req.ind. to the MCF (to authenticate and verify the network).

4. **Network verify req.ind.**: causes the network to authenticate and verify itself to the mobile. It comes from the UIM.

Network verify (Response: Success or Failure)	req.ind.
TMUI	M
RANDBS	M

FEA4	– Relay Network verify req.ind. from UIMF.

5. **Network verify req.ind.**: is relayed to the visited system by the MCF.

Network verify (Response: Success or Failure)	req.ind.
TMUI	M
RANDBS	M

FEA5	– Perform IMUI/TMUI translation.

6. **Network verify req.ind.**: is relayed by the visited system to the home system for purposes of authenticating the network.

Network verify (Response: Success or Failure)	req.ind.
IMUI	M
RANDBS	M

FEA6	– Generate AUTHBS using new SSD.

7. **Network verify resp.conf.**: is the response from the home network to the Network verify req.ind. information flow.

Network verify	resp.conf.
AUTHBS	M

FEA7	– Perform IMUI/TMUI translation.

8. **Network verify resp.conf.**: is relayed by the visited system.

Network verify	resp.conf.
AUTHBS	M

FEA8	– Relay Network verify resp.conf.

9. **Network verify resp.conf.**: is relayed by the mobile system to the UIM.

Network verify	resp.conf.
AUTHBS	M

FEA9	– Compare received AUTHBS to expected AUTHBS. – Prepare a pass/fail confirmation. – Update memory with new SSD if procedure has been successful.

10. **SSD update resp.conf.**: is the response from the UIM to SSD update req.ind.

SSD update	resp.conf.
Result	M

FEA10	– Relay SSD update resp.conf.

11. **SSD update resp.conf.**: is the response to the SSD update req.ind. information flow.

SSD update	resp.conf.
Result	M

FEA11	– Process confirmation

12. **SSD update resp.conf.**: is the response to the SSD update req.ind. information flow.

SSD update	resp.conf.
Result	M

FEA12	– Prepare to send Unique challenge req.ind. to the mobile user in the visited network.

13. **Unique challenge req.ind.**: enables the network to determine whether (or not) the selected mobile has been able to successfully update its SSD.

Unique challenge (Response: Success or Failure)	req.ind.
IMUI	M
RANDU	M
AUTH_U	M

FEA13	– Perform IMUI/TMUI translation.

14. **Unique challenge req.ind.**: is forwarded from UIMF to MT.

Unique challenge (Response: Success or Failure)	req.ind.
TMUI	M
RANDU	M
AUTH_U	M

FEA14	– Relay Unique challenge req.ind.

15. **Unique challenge req.ind.**: is forwarded to the UIMF.

Unique challenge (Response: Success or Failure)	req.ind.
TMUI	M
RANDU	M
AUTH_U	M

FEA15	– Calculate authentication response AUTH_U using new SSD.

16. **Unique challenge resp.conf.**: is the response to **Unique challenge req.ind.** and contains the authentication response.

Unique challenge	resp.conf.
AUTH_U	M

FEA16	– Relay Unique challenge resp.conf.

17. **Unique challenge resp.conf.**: is forwarded to RAN+CNv.

Unique challenge	resp.conf.
AUTH_U	M

FEA17	– Perform IMUI/TMUI translation.

18. **Unique challenge resp.conf.**: is forwarded to the home network.

Unique challenge	resp.conf.
AUTH_U	M

FEA18	– Update mobile user's data based on status information received. – If status is successful, store the new SSD value for use in future executions of the authentication procedure and allow mobile user to continue with call origination and call termination. Optionally, the SSD can be shared with an LMFv, if permitted by service provider agreements.
NOTE – The LMFh updates the mobile user's data based on status information received. If authentication did not fail, then allow the mobile user to continue with call origination and call termination. In addition, transfer SSD to LMFv if permitted by service provider agreements. If the status is unsuccessful, maintain the current SSD and reattempt to update the SSD of the mobile user in a subsequent transaction.	

6.1.2.4.2 Invoke security sharing

Invoke security sharing is used to invoke the sharing of security information associated with a particular IMT-2000 user.

Scenario:

a) The home system of a subscriber determines that security sharing should be enabled and extends (shares) security information to the visited system.

b) The visited system enables security sharing and responds to the home system indicating success or failure.

See Figure 6.1.2.4.2-1.

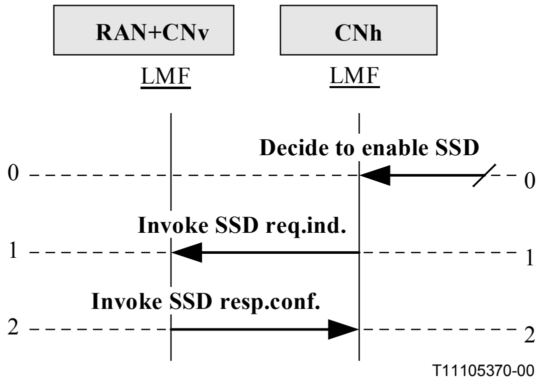


Figure 6.1.2.4.2-1/Q.1721 – Invoke security sharing information flow diagram

0. **Decide to enable SSD**: decide to enable sharing of secret data between home and visited system.

FEA0	– LMFh determines that security sharing should be enabled and sends an Invoke_security_sharing request to the LMFv with the security information to be shared.

1. **Invoke_security_sharing req.ind.**: is used to invoke the sharing of the security information at the visited system.

Invoke_security_sharing (Response: Success or Failure)	req.ind.
IMUI	M
SSD	M

FEA1	– LMFv receives the request, enables security sharing, and returns a success or failure.

2. **Invoke_security_sharing resp.conf.**: is the response to the Invoke_security_sharing req.ind. information flow.

Invoke_security_sharing	resp.conf.
Result	M

6.1.2.4.3 Revoke security sharing

Revoke security sharing is used to revoke the sharing of security information at the visited system.

Scenario:

a) The home system of a subscriber determines that security sharing should be disabled and informs the visited system.

b) The visited system disables security sharing and responds to the home system, with the call history count if available, indicating success or failure.

See Figure 6.1.2.4.3-1.

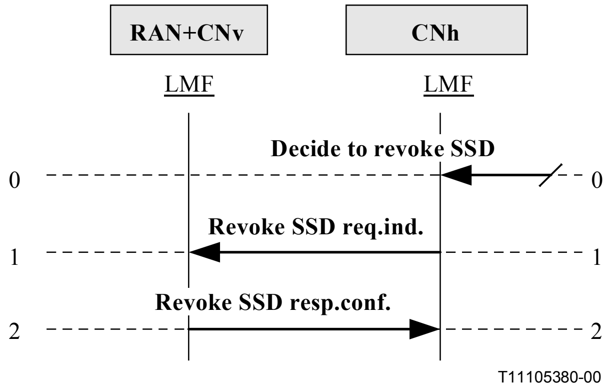


Figure 6.1.2.4.3-1/Q.1721 – Revoke security sharing information flow diagram

0. **Decide to revoke SSD**: decide to enable sharing of secret data between home and visited system.

FEA0	– LMFh determines that security sharing should be disabled and sends a Revoke_security_sharing request to the LMFv.

1. **Revoke_security_sharing req.ind.**: is used to revoke the sharing of the security information at the visited system.

Revoke_security_sharing (Response: Success or Failure)	req.ind.
IMUI	M

FEA1	– LMFv receives the request, disables security sharing and returns a success or failure.

2. **Revoke_security_sharing resp.conf.**: is the response to the Revoke_security_sharing req.ind. information flow.

Revoke_security_sharing	resp.conf.
Result	M
CHCNT	O (Note)
NOTE – CHCNT is returned, if available.	

6.1.2.5 Start ciphering

This procedure provides encryption of the data stream on the radio interface to prevent unauthorized access to the information. Ciphering is initiated in the MT (and LMFv) only after a successful authentication process. See Figure 6.1.2.5-1.

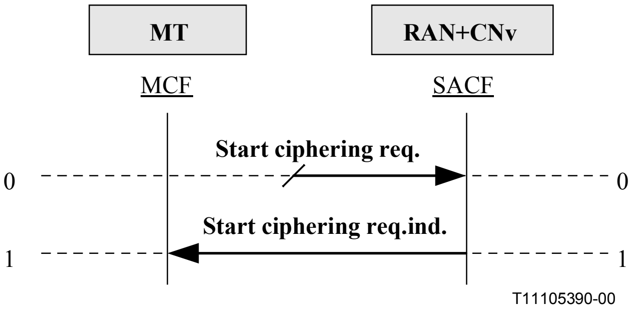


Figure 6.1.2.5-1/Q.1721 – Start ciphering information flow diagram

0. **Start ciphering request**: start ciphering request is received.

1. **Start_ciphering req.ind.**: is used to activate ciphering control over the radio interface.

Start ciphering (Response: None)	req.ind.
None	N/A

FEA1	– Activate ciphering control over the radio interface.

6.1.2.6 TMUI assignment

A TMUI has local significance only in the location area in which the user is registered. Outside that area, it should be accompanied by an appropriate Location Area Identification (LAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the LMFv in which the user is registered.

The TMUI, when available, is normally used to identify the user on the radio access path, for instance in paging requests, location update requests, attach requests, service requests, connection re-establishment requests and detach requests.

This procedure is used to assign and convey the TMUI to the UIM after the network has verified the identify of the user and should be performed after the initiation of ciphering. See Figure 6.1.2.6-1.

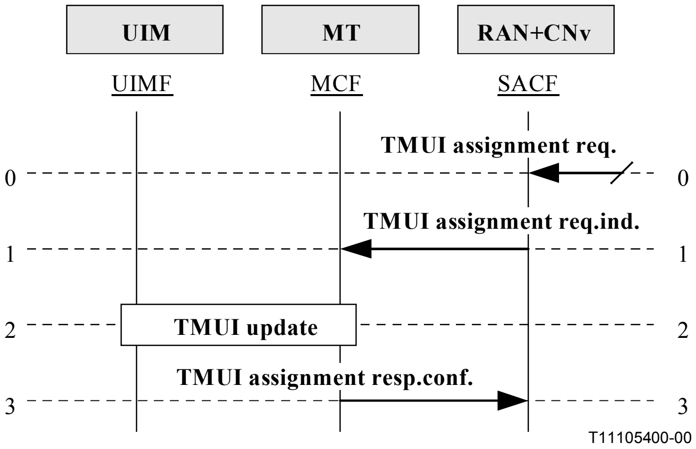


Figure 6.1.2.6-1/Q.1721 – TMUI assignment information flow diagram

0. **TMUI assignment request**: is received.

FEA0	– Retrieve TMUI and TMUI assignment source ID, and optionally TMUI expiration timer. – Send TMUI assignment req.ind.

1. **TMUI_assignment req.ind.**: is used to assign and convey the TMUI to the user after the network has verified the identify of the user.

TMUI_assignment (Response: Success or Failure)	req.ind.
TMUI	M
TMUI assignment source ID	M
TMUI expiration timer	O (Note)

FEA1	– Initiate TMUI update procedure module.
NOTE – Include if other than a default expiration timer value as set by the network is to be used.	

2. **TMUI_assignment resp.conf.**: indicates the TMUI update procedure was executed.

FEA2	– Analyse the result of TMUI update and report it to the visited network.

3. **TMUI_assignment resp.conf.**: is the response to TMUI_assignment req.ind.

TMUI_assignment	resp.conf.
Result	M

FEA3	Note the response. No further action required.

6.1.2.7 Call history count

6.1.2.7.1 Update call history count

The Update call history count procedure is used to update the call history count (CHCNT) in the visited system, mobile terminal and UIM. See Figure 6.1.2.7.1-1.

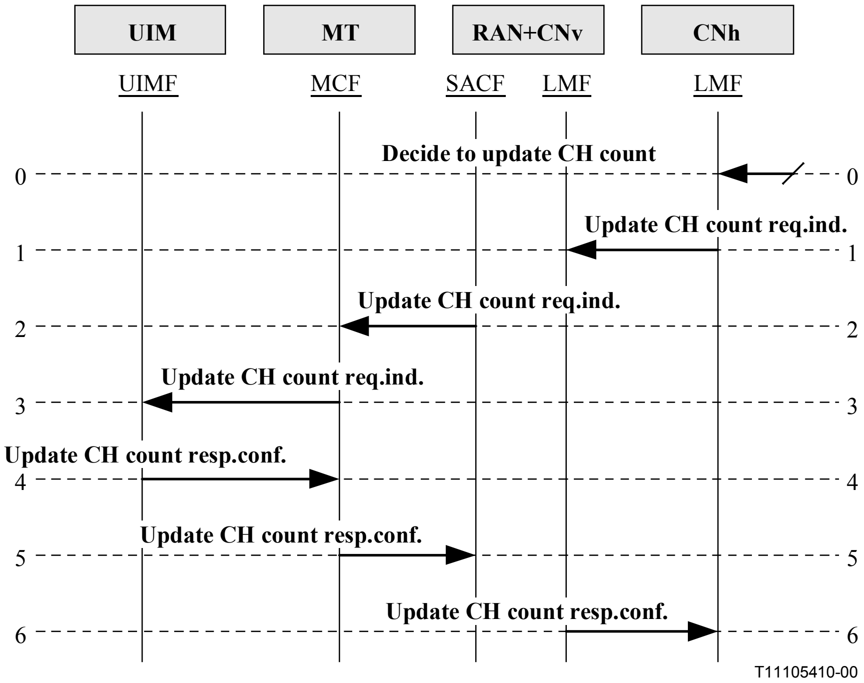


Figure 6.1.2.7.1-1/Q.1721 – Update call history count information flow diagram

0. **Decide to update call history count**: the home system detects the need to update the call history count and sends a request to the visited system to update the call history count.

FEA0	– Retrieve appropriate parameters and initiate Update call history count procedure.

1. **Update_CH_count req.ind.**: is used to request the call history count to be updated in the visited system.

Update_CH_count (Response: Success or Failure)	req.ind.
IMUI	M
Update_CH_count	M

FEA1	– Update call history count data in the visited system.

2. **Update_CH_count req.ind.**: is sent to MCF.

Update_CH_count (Response: Success or Failure)	req.ind.
IMUI	M
Update_CH_count	M

FEA2	– Update call history count data in the mobile terminal.

3. **Update_CH_count req.ind.**: is sent to UIMF.

Update_CH_count (Response: Success or Failure)	req.ind.
IMUI	M
Update_CH_count	M

FEA3	– Update call history count data in the UIM.

4. **Update_CH_count resp.conf.**: is the response to the request from UIMF.

Update_CH_count	resp.conf.
CHCNT	M
Result	M

FEA4	– Relay result to MCF.

5. **Update_CH_count resp.conf.**: is the response to the request from MCF.

Update_CH_count	resp.conf.
CHCNT	M
Result	M

FEA5	– Relay result to SACF in visited system.

6. **Update_CH_count resp.conf.**: is the response to the request from visited system.

Update_CH_count	resp.conf.
CHCNT	O (Note)
Result	M

FEA6	– Relay result to home system.
NOTE – Send CHCNT to home system if needed.	

6.1.2.7.2 Call history count request procedure

When the CHCNT parameter is used, the "home" network needs to query the previously visited network to obtain the current value of CHCNT in order that the current serving network may use it. The current serving network may be the "home" network or another "visited" network. See Figure 6.1.2.7.2-1.

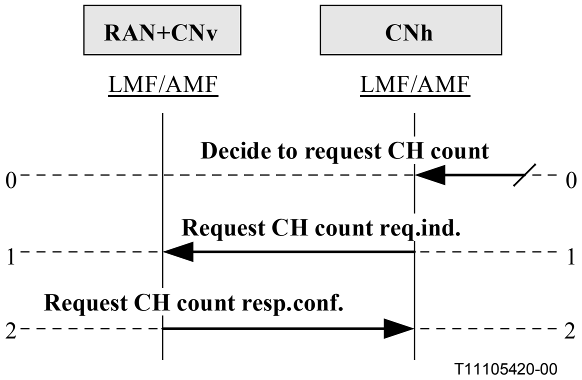

RAN+CNv
CNh
LMF/AMF
LMF/AMF
Decide to request CH count
0
0
Request CH count req.ind.
1
1
Request CH count resp.conf.
2
2
T11105420-00

Figure 6.1.2.7.2-1/Q.1721 – Call history count request information flow diagram

0. **Decide to request call history count**: the home system detects the need to query the previously visited network to obtain the current value of CHCNT in order that the current serving network may use it.

FEA0	– Initiate Call history CHCNT request procedure.

1. **Request_CH_count req.ind.**: is used to request the current value of CHCNT from previously visited network.

Request_CH_count (Response: Success or Failure)	req.ind.
IMUI	M

FEA1	– Access the current value of CHCNT for the user and send to home system.

2. **Request_CH_count resp.conf.**: is the response to the request.

Request_CH_count	resp.conf.
CHCNT	M

FEA2	– Receive CHCNT for the user from previously visited system and store it for later use.

6.1.2.8 Unique Challenge Authentication – RANDU based

The Home HLR/AC as well as the serving system can trigger this type of UC process (if the SSD is shared). A random number is selected by the serving system (RANDU) and an expected authentication response, based on the mobile's SSD, is produced by the authentication algorithm. Upon receiving the challenged (i.e. RANDU), the MT in turn is calculating its own authentication signature using its SSD and the same authentication algorithm. The authentication signature is returned to the serving system (or the AC) where it is checked against the expected one. If they match, the authentication is successful.

The UC process can be optionally used to (re)authenticate an MT, to authenticate supplementary services or as part of the SSD update process. See Figure 6.1.2.8-1.

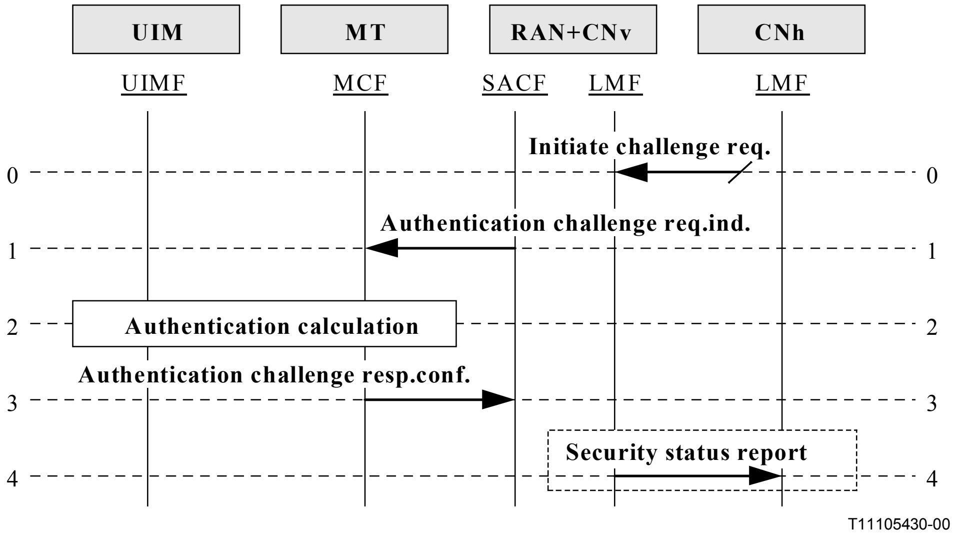

UIM
MT
RAN+CNv
CNh
UIMF
MCF
SACF
LMF
LMF
Initiate challenge req.
Authentication challenge req.ind.
Authentication calculation
Authentication challenge resp.conf.
Security status report
0
1
2
3
4
T11105430-00

Figure 6.1.2.8-1/Q.1721 – Unique challenge/response user authentication (SSD shared)

0. **Initiate challenge request**: the SACF receives an Initiate challenge request after the LMFv is triggered to initiate a UC authentication process.

FEA0	– Initiate authentication challenge. – Generate the challenge – RANDU and send it to the user.

1. **Authentication challenge req.ind.**: is sent to verify the identity of the user.

Authentication challenge (Response: Success or Failure)	req.ind.
RANDU	M

FEA1	– Calculate the expected authentication signature AUTHU.

2. **Authentication calculation**: is executed.

3. **Authentication challenge resp.conf.**: sends the authentication signature based on RANDU.

FEA2	– Receive AUTHU. – Verify the received AUTHU validity.

4. **Security status report req.ind.**: is used to send a security status report to the home network (optional).

Security status report (Response: None)	req.ind.
Result	M
IMUI	O (Note)

FEA5	– Analyse security status report.
NOTE – IMUI must be included, if available.	

6.2 Location management

6.2.1 Subscriber data management

The subscriber data management procedures are used by the LMFh to change or remove certain subscriber data from the subscriber profile in the LMFv if the subscription of one or more basic or supplementary services have been changed or withdrawn. Hence, this can be seen as "stand alone" modification of the subscriber profile in the visited system, i.e. not in conjunction with a location update.

NOTE – The terms "user" and "subscriber" used in this subclause are interchangeable.

Throughout this subclause, it is assumed that the following information items are stored in the subscriber home network/supporting network and are the subject of the subscriber information and profile management activities:

- IMT-2000 mobile directory number (IMDN), e.g. a dialable number;
- IMT-2000 mobile user ID (IMUI);
- international mobile equipment ID (IMEI);
- user/terminal location information;
- basic service data (e.g. subscribed bearer services);
- teleservices (e.g. broadcast and/or group call subscription data);
- security data;
- supplementary services data;
- operator determined features/services (e.g. call barring data);
- subscriber determined features/services (e.g. call screening data);
- roaming restriction data;
- regional subscription data; and
- VHE subscription data.

6.2.1.1 Subscriber profile modification

6.2.1.1.1 Subscriber profile modification, Case 1: Subscriber profile copy

Subscriber profile data have been modified and the modifications have to be reflected in the LMFv. In this case, the "Subscriber profile copy" procedure can be used. This procedure overwrites all exiting values of the parameters by their corresponding new values. See Figure 6.2.1.1-1.

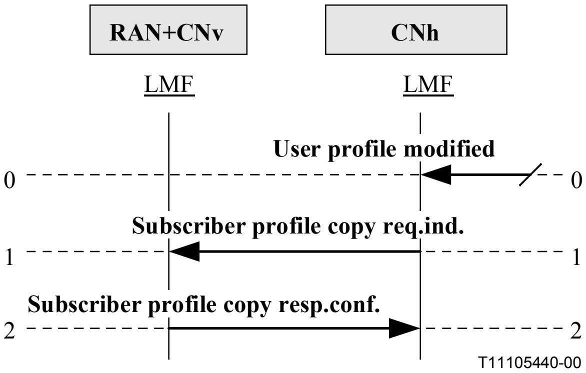

RAN+CNv
CNh
LMF
LMF
User profile modified
0
0
Subscriber profile copy req.ind.
1
1
Subscriber profile copy resp.conf.
2
2
T11105440-00

Figure 6.2.1.1-1/Q.1721 – Subscriber profile modification, Case 1: Subscriber profile copy

0. **User profile modified**: initiates the Subscriber profile copy to the LMFv.

FEA0	– Determine the need to update the user profile residing in the LMF of the visited network.

1. **Subscriber profile copy req.ind.**: is sent from the LMFh to LMFv in the serving network indicating requirements to update one or more elements of the subscriber profile.

Subscriber profile copy (Response: Success)	req.ind.
IMUI	M
User profile	M

FEA1	– Identifies the IMT-2000 user in question. – Updates the user profile.

2. **Subscriber profile copy resp.conf.**: is sent from the LMFv in the serving network to the LMFh in the user's home network. It is to inform the LMFh of the profile update results.

Subscriber profile copy	resp.conf.
Result	M

FEA2	– Note the completion of the Subscriber profile update procedure.

6.2.1.1.2 Subscriber profile modification, Case 2: Delete user data

The subscription of one or more basic or supplementary services has been withdrawn. This procedure is used to indicate the specific services that have been withdrawn and the specific data to be deleted. See Figure 6.2.1.1-2.

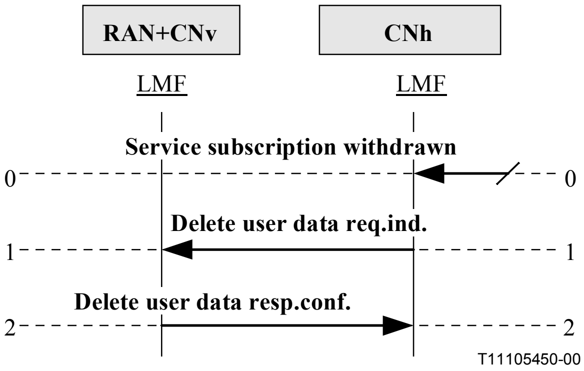

RAN+CNv
CNh
LMF
LMF
Service subscription withdrawn
0
0
Delete user data req.ind.
1
1
Delete user data resp.conf.
2
2
T11105450-00

Figure 6.2.1.1-2/Q.1721 – Subscriber profile modification, Case 2: Delete user data

0. **Service subscription withdrawn**: is a request to delete a specific service subscription from the list of subscribed services.

FEA0	– Determine the need to delete one or more basic or supplementary services from the user profile residing in the LMF of the visited network.

1. **Delete user data req.ind.**: is used to delete specific user data.

Delete user data (Response: Success)	req.ind.
IMUI	M
Deleted user data	M

FEA1	– Identify the concerned IMT-2000 user. – Delete the user data indicated in the Delete user data req.ind.

2. **Delete user data resp.conf.**: confirms the request.

Delete user data	resp.conf.
Result	M

FEA2	– Note the completion of the Delete user data procedure.

6.2.1.1.3 Subscriber profile modification, Case 3: Subscriber profile removal

The authentication algorithm or authentication key of the subscriber has been changed or the modification of the subscriber profile affects the subscriber's permission to roam in its current area. In this case, the subscriber profile should be removed entirely from the visited network and, therefore, the "Subscriber profile removal" procedure is used. See Figure 6.2.1.1-3.

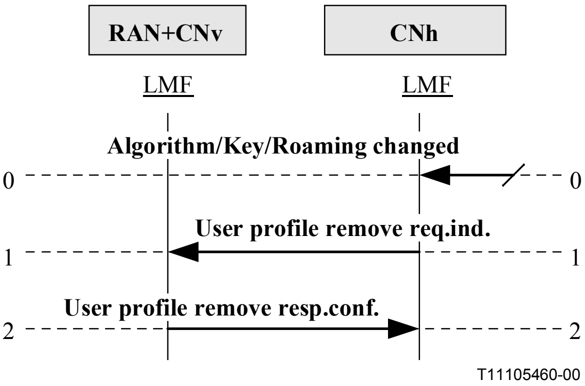

RAN+CNv
CNh
LMF
LMF
Algorithm/Key/Roaming changed
0
0
User profile remove req.ind.
1
1
User profile remove resp.conf.
2
2
T11105460-00

Figure 6.2.1.1-3/Q.1721 – Subscriber profile modification, Case 3: Subscriber profile removal

0. **Algorithm/Key/Roaming changed**: initiates removal of the subscriber profile from the LMFv.

FEA0	– Initiate User profile removal.

1. **User profile remove req.ind.**: is used to request removal of the user profile.

User profile remove (Response: Success)	req.ind.
IMUI	M

FEA1	– Identify the concerned IMT-2000 user. – Remove the user profile of the identified user.

2. **User profile remove resp.conf.**: is returned to confirm the actions taken by the LMFv.

User profile remove	resp.conf.
Result	M

FEA2	– Note the completion of the user profile removal procedure.

6.2.1.2 Location information interrogation

The location information interrogation procedure may be invoked in the following cases:

Case 1: the most current version of the user location information residing in the LMFv is the subject of interrogation by the LMFh; and

Case 2: a supporting network interrogates the home network for location information. Case 1 may be implemented independently or as a nested procedure within Case 2.

6.2.1.2.1 Location information interrogation by LMF

This procedure is for the LMFh to interrogate the LMFv for the user information. Upon receiving a request for the user location information, the LMFh may request for the latest/most current location information (e.g. the status and location of the user) from the serving network. See Figure 6.2.1.2-1.

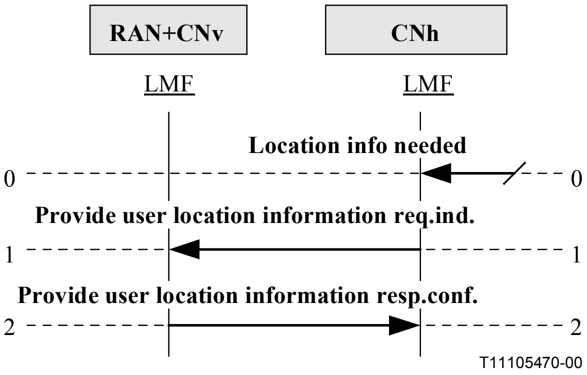

RAN+CNv
CNh
LMF
LMF
Location info needed
0
0
Provide user location information req.ind.
1
1
Provide user location information resp.conf.
2
2
T11105470-00

Figure 6.2.1.2-1/Q.1721 – User information interrogation by LMFh

0. **Location info needed**: initiates the request for user location information interrogation.

FEA0	– Determine the need to acquire current user information in order to perform a mobility management procedure (e.g. Terminal registration), or simply in an updating/relaying mode, to respond to a request for the information.

1. **Provide user location information req.ind.**: is sent from the LMFh to the LMFv to request that user information (e.g. state and location information) be given.

Provide user location information (Response: Success or Failure)	req.ind.
Requested information	M
IMUI	O (Note)
IMDN	O (Note)

FEA1	– Identifies the concerned IMT-2000 user. – Retrieves the requested user information.
NOTE – Either IMUI or IMDN must be provided.	

2. **Provide user location information resp.conf.**: is sent from the LMFv to the LMFh providing the requested user information (e.g. state and location information).

Provide user information	resp.conf.
Location information	O (Note)
User state	O (Note)

FEA2	– Note the completion of the Provide User Information procedure.
NOTE – This IE should be provided if it is requested and available.	

6.2.1.2.2 User information interrogation by SCF

This procedure enables the SCF to obtain the user information (e.g. state of the terminal and its location information) residing in the LMFh. The information is used in support of the IN based services to the user. See Figure 6.2.1.2-2.

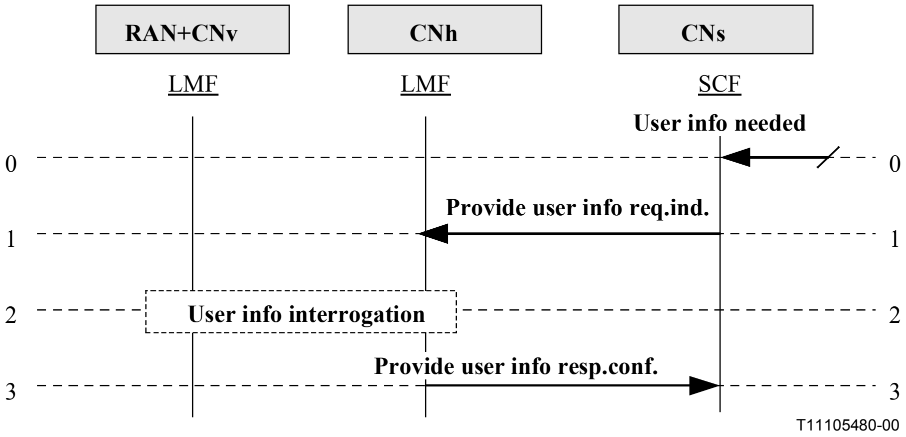


Figure 6.2.1.2-2/Q.1721 – User location information interrogation by SCF

0. **User info needed**: initiates the request for user information interrogation.

FEA0	– Determine the need to acquire user information in order to provide an IN based service.

1. **Provide user information req.ind.**: is sent from the SCF in the supporting network to LMFh to request the user information.

Provide user information (Response: Success or Failure)	req.ind.
Requested information	M
IMUI	O (Note)
IMDN	O (Note)

FEA1	– Identifies the concerned IMT-2000 user. – Retrieves the requested user information. If the user information is not available, it requests the information from the LMFv by performing the User info interrogation procedure.
NOTE – Either the IMUI or the IMDN must be provided.	

2. **User info interrogation**: is performed if required.

3. **Provide user information resp.conf.**: is the response from the LMFh to the SCF providing the requested user information.

Provide user information	resp.conf.
Location information	M
Terminal status	M

FEA3	– Utilize the information received in the SLP that has been executed.

6.2.1.3 Subscriber profile transfer

This procedure is invoked when an IMT-2000 user attempts to register in a visited network. This procedure is required as a common module for transferring the subscriber profile from the LMFh to the LMFv when a user roams into a serving network outside its home network. See Figure 6.2.1.3-1.

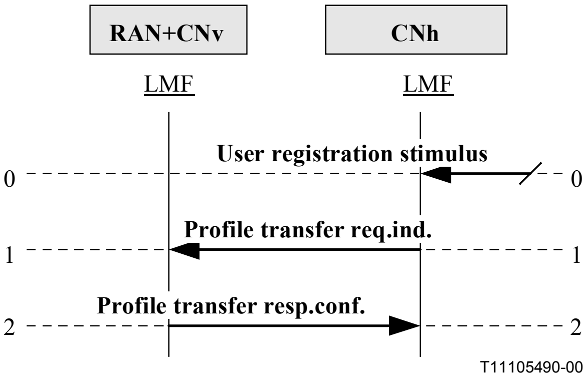

RAN+CNv
CNh
LMF
LMF
User registration stimulus
Profile transfer req.ind.
Profile transfer resp.conf.
0
0
1
1
2
2
T11105490-00

Figure 6.2.1.3-1/Q.1721 – Subscriber profile transfer

0. **User registration stimulus**: initiates this procedure.

FEA0	– Determine that the user profile is needed to support a user in a visiting user.

1. **Profile transfer req.ind.**: is sent from the LMFh to the LMFv to provide the profile for the roaming user.

Profile transfer (Response: Success)	req.ind.
IMUI	M
Subscriber profile	M

FEA1	– Identifies the IMT-2000 user in question and stores the profile.

2. **Profile transfer resp.conf.**: is the response from the LMFv to the LMFh confirming the update of the user service profile with data provided by the LMFh.

Profile transfer	resp.conf.
Result	M

FEA2	– Note successful profile transfer.

6.2.2 Identity retrieval – user

6.2.2.1 Identity retrieval and update

The UIMF retains TMUI, LAI and the IMT-2000 user's IMUI. For call origination, call termination, terminal location update, etc., the mobile terminal needs to retrieve IMUI, TMUI and the LAI information. For terminal location update, the mobile terminal needs to update TMUI and LAI.

Five information flow diagrams for identity retrieval and update are described, namely:

- IMUI inquiry;
- TMUI inquiry;
- LAI inquiry;
- TMUI update;
- LAI update.

6.2.2.1.1 IMUI inquiry

See Figure 6.2.2.1-1.

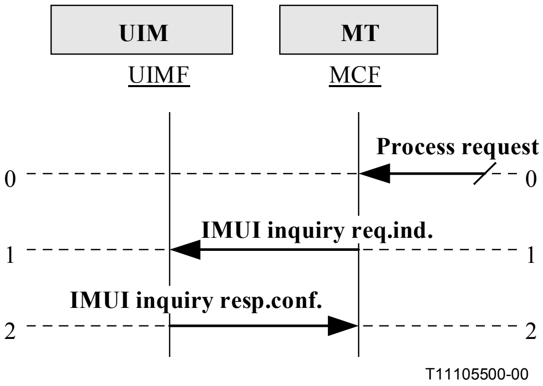


Figure 6.2.2.1-1/Q.1721 – IMUI inquiry

0. **Process request**: is the stimulus for the IMUI inquiry received by the MCF.

FEA0	– Initiate the IMUI inquiry procedure.

1. **IMUI inquiry req.ind.**: is sent from the MCF to the UIMF to retrieve the IMUI of the subscriber.

IMUI inquiry (Response: Success or Failure)	req.ind.
None	N/A

FEA1	– Retrieve the IMUI of the subscriber.

2. **IMUI inquiry resp.conf.**: is the response to the request.

IMUI inquiry	resp.conf.
IMUI	M

FEA2	– Record the IMUI.

6.2.2.1.2 TMUI inquiry

See Figure 6.2.2.1-2.

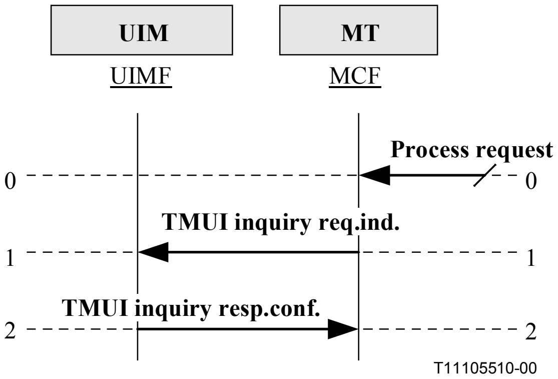


Figure 6.2.2.1-2/Q.1721 – TMUI inquiry

0. **Process request**: received by the MCF initiates the TMUI inquiry.

FEA0	– Initiate the TMUI inquiry procedure.

1. **TMUI inquiry req.ind.**: is sent from the MCF to the UIMF to retrieve the TMUI of the subscriber.

TMUI inquiry (Response: Success or Failure)	req.ind.
None	N/A

FEA1	– Retrieve the TMUI of the subscriber.

2. **TMUI inquiry resp.conf.**: is the response to the request.

IMUI inquiry	resp.conf.
TMUI	M
TMUI assignment source ID	M

FEA2	– Record the TMUI and the TMUI assignment source ID.

6.2.2.1.3 LAI inquiry

See Figure 6.2.2.1-3.

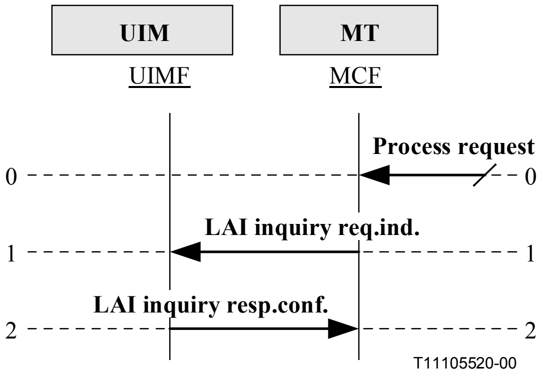


Figure 6.2.2.1-3/Q.1721 – LAI inquiry

0. **Process request**: received by the MCF, is the stimulus for the LAI inquiry.

FEA0	– Initiate the LAI inquiry procedure.

1. **LAI inquiry req.ind.**: is sent from the MCF to the UIMF to retrieve the LAI of the subscriber.

LAI inquiry (Response: Success or Failure)	req.ind.
None	N/A

FEA1	– Retrieve the LAI of the subscriber.

2. **LAI inquiry resp.conf.**: is the response to the request.

LAI inquiry	resp.conf.
LAI	M

FEA2	– Record the LAI.

6.2.2.1.4 TMUI update

See Figure 6.2.2.1-4.

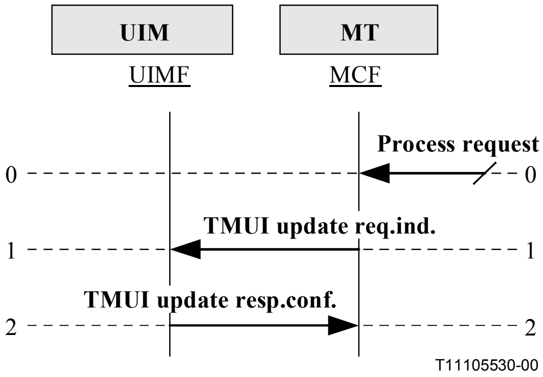


Figure 6.2.2.1-4/Q.1721 – TMUI update

0. **Process request**: stimulus for the TMUI update is received by MCF.

FEA0	– Initiate the TMUI update procedure.

1. **TMUI update req.ind.**: is sent from the MCF to the UIMF to update the TMUI for the subscriber.

TMUI update (Response: Success or Failure)	req.ind.
TMUI	M
TMUI assignment source ID	M

FEA1	– Update TMUI for the subscriber and record the TMUI assignment source ID.

2. **TMUI update resp.conf.**: is the response to the request.

TMUI update	resp.conf.
None	N/A

FEA2	– Note successful completion.

6.2.2.1.5 LAI update

See Figure 6.2.2.1-5.

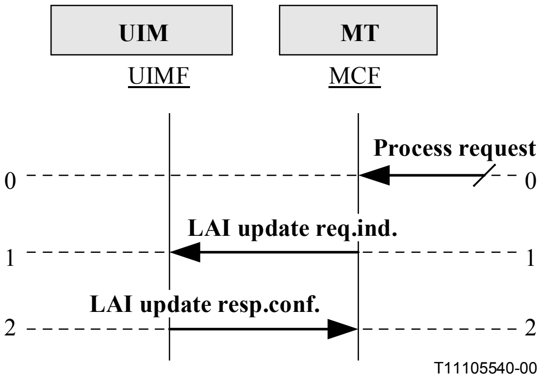


Figure 6.2.2.1-5/Q.1721 – LAI update

0. **Process request**: stimulus for the LAI update is received by MCF.

FEA0	– Send request to UIMF to update LAI.

1. **LAI update req.ind.**: is sent from the MCF to the UIMF to update LAI of the subscriber.

LAI update (Response: Success or Failure)	req.ind.
LAI	M

FEA1	– Update the LAI of the subscriber.

2. **LAI update resp.conf.**: is the response to the request.

LAI update	resp.conf.
None	N/A

FEA2	– Note successful completion.

6.2.2.2 User ID retrieval

This procedure is used to convert the TMUI to the IMUI of the user. The newly visited network initiates this procedure when the network receives the TMUI, or a set of TMUI, and the TMUI assignment source ID as user ID from the mobile side.

For Terminal location registration and update, there are two cases:

- Case 1: TMUI has been assigned by newly visited LMF (see 6.2.2.1.2).
- Case 2: TMUI has been assigned by another LMF different from newly visited LMF (this subclause).

If the newly visited network cannot retrieve the IMUI successfully (e.g. loses the TMUI), then the newly visited network attempts to retrieve the IMT-2000 user's IMUI from the UIMF (see 6.2.2.1.1). See Figure 6.2.2.2-1.

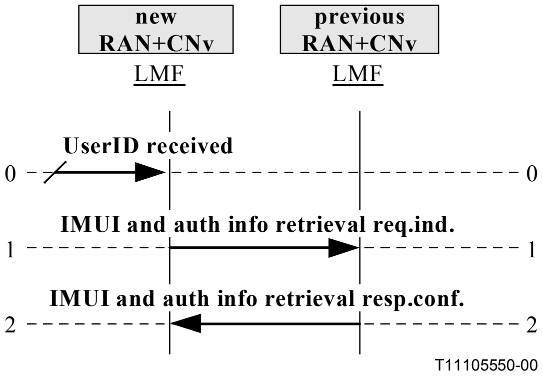

new
RAN+CNv
LMF
previous
RAN+CNv
LMF
0
UserID received
0
1
IMUI and auth info retrieval req.ind.
1
2
IMUI and auth info retrieval resp.conf.
2
T11105550-00

Figure 6.2.2.2-1/Q.1721 – IMUI and Authentication info retrieval information flow diagram

0. **UserID received**: received by the newly visited LMF initiates this procedure.

FEA0	For Case 1: – Retrieve the IMUI of the requesting IMT-2000 user with the TMUI. For Case 2: – Identify the LMF by which the TMUI is assigned with the TMUI assignment source ID.

1. **IMUI and authentication info retrieval req.ind.**: is used to retrieve the IMUI with the TMUI. This information flow is sent to the LMF in the previous visited network.

IMUI and authentication info retrieval (Response: Success or Failure)	req.ind.
TMUI	M
TMUI assignment source ID	M

FEA1	– Retrieve the IMUI and unused authentication triplets of the requesting IMT-2000 user with the TMUI.

2. **IMUI retrieval resp.conf.**: is the response to the request.

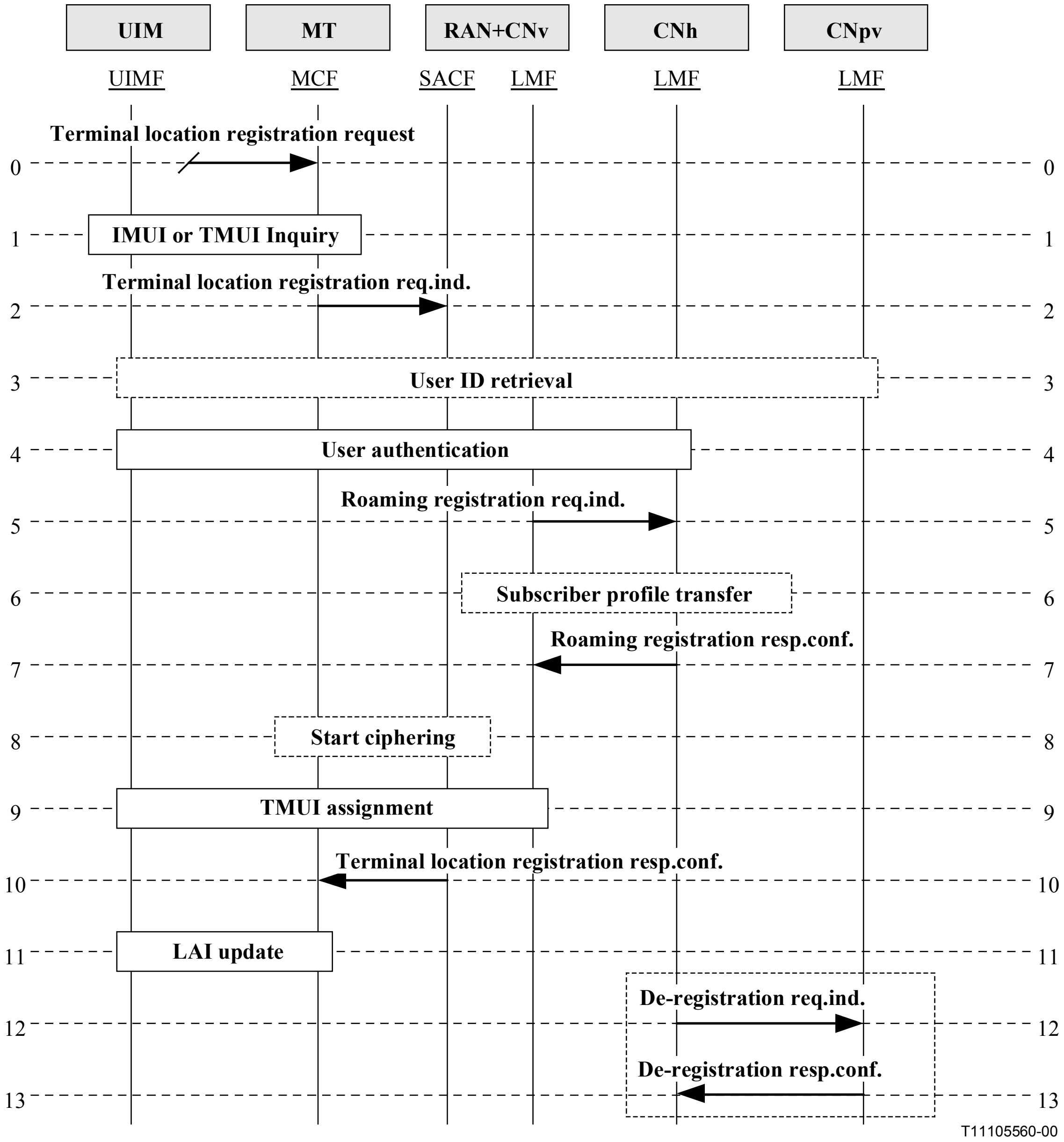
IMUI and authentication info retrieval	resp.conf.
IMUI	M
Result	M
Challenge(s)	O (Note 1)
Challenge Response(s)	O (Note 1)
Ciphering Key(s)	O (Note 2)

FEA2	– Confirm completion of IMUI retrieval.
NOTE 1 – Included if authentication is to be carried out. NOTE 2 – Returned if available.	

6.2.3 Registration management

6.2.3.1 Terminal location registration

This feature is used when an IMT-2000 user notifies the system on his location. This procedure enables the location area information of the IMT-2000 user to be registered in the visited network. A Terminal location registration procedure is carried out when no previous location details are known about the user when he first appears in a network domain. During this procedure, all the information on the user is erased in the previously visited network. Updating of the location area information may occur after network or terminal failure. See Figure 6.2.3.1-1.


UIM
MT
RAN+CNv
CNh
CNpv
UIMF
MCF
SACF
LMF
LMF
LMF
Terminal location registration request
IMUI or TMUI Inquiry
Terminal location registration req.ind.
User ID retrieval
User authentication
Roaming registration req.ind.
Subscriber profile transfer
Roaming registration resp.conf.
Start ciphering
TMUI assignment
Terminal location registration resp.conf.
LAI update
De-registration req.ind.
De-registration resp.conf.
0
1
2
3
4
5
6
7
8
9
10
11
12
13
T11105560-00

NOTE – IFs 12 and 13 may occur any time after IF 5 and are independent of IFs 8 through 11 inclusive.

Figure 6.2.3.1-1/Q.1721 – Terminal location registration

0. **Terminal location registration request**: is initiated when the MT is powered-up and attempts to register in the network using the information broadcast by that network.

FEA0	– Obtain the user identity.

1. **IMUI or TMUI inquiry**: is used to obtain the IMUI or TMUI as appropriate.

2. **Terminal location registration req.ind.**: is used to register the location area information of the mobile terminal to the network.

Terminal location registration (Response: Success or Failure)	req.ind.
UserID	M (Note 1)
TC Info	O (Note 2)
AUTH_R	O (Note 3)
Confirmation of RANDG	O (Note 3)
CHCNT	O (Note 3)

FEA2	– Initiate User ID retrieval procedure to retrieve the IMUI, if the TMUI is used.
NOTE 1 – Either IMUI or TMUI as available. NOTE 2 – If available, sent to indicate the services that the terminal can support. NOTE 3 – If the global challenge (random number) is used in the broadcast information for authentication purposes, authentication data is sent.	

3. **User ID retrieval**: is executed if required.

4. **User authentication**: is executed.

5. **Roaming registration req.ind.**: is used to update the LMFv address in the home network.

Roaming registration (Response: Success or Failure)	req.ind.
IMUI	M
LMFv address	M

FEA5	– Identify the requesting IMT-2000 user. – Update the LMFv address. – Identify the LMFv address of the previously visited network, if applicable. – Initiate User Profile Update if required.

6. **Subscriber profile transfer**: is executed if required.

7. **Roaming registration resp.conf.**: is the confirmation to Roaming Registration req.ind.

Roaming registration	resp.conf.
Result	M

FEA7	– Confirm completion of roaming registration for the IMT-2000 user. – Identify Location area and TC info. – Store Location area and TC info for the IMT-2000 user. – Invoke TMUI update procedure for the IMT-2000 user.

8. **Start ciphering**: is executed if appropriate.

9. **TMUI assignment**: is executed.

FEA9	– Analyse the result of TMUI update procedure.
NOTE – TMUI update procedure module is separated from user authentication procedure module in order to assign TMUI after user profile is created in the newly visited network.	

10. **Terminal location registration resp.conf.**: is the confirmation of Terminal location registration req.ind.

Terminal location registration	resp.conf.
Result	M

FEA10	– Memorize Location area identifier of current location in the MT.

11. **LAI update**: is executed to update the Location Area Identifier in the UIM.

12. **De-registration req.ind.**: is optionally used to de-register the user from the previously visited network.

De-registration (Response: Success or Failure)	req.ind.
IMUI	M

FEA12	– Identify the requesting IMT-2000 user. – Remove user profile of the requesting IMT-2000 user. – Formulate and send De-registration resp.conf.

13. **De-registration resp.conf.**: is the confirmation of De-registration req.ind.

De-registration	resp.conf.
Result	M

FEA8	– Identify the newly visited network.

6.2.3.2 Terminal location updating

This feature is used when an IMT-2000 user who roams within the same network domain notifies the system on his new location area. This new location area information is then registered in the visited network. Updating of such location area information may also occur after a network or terminal failure. See Figure 6.2.3.2-1.

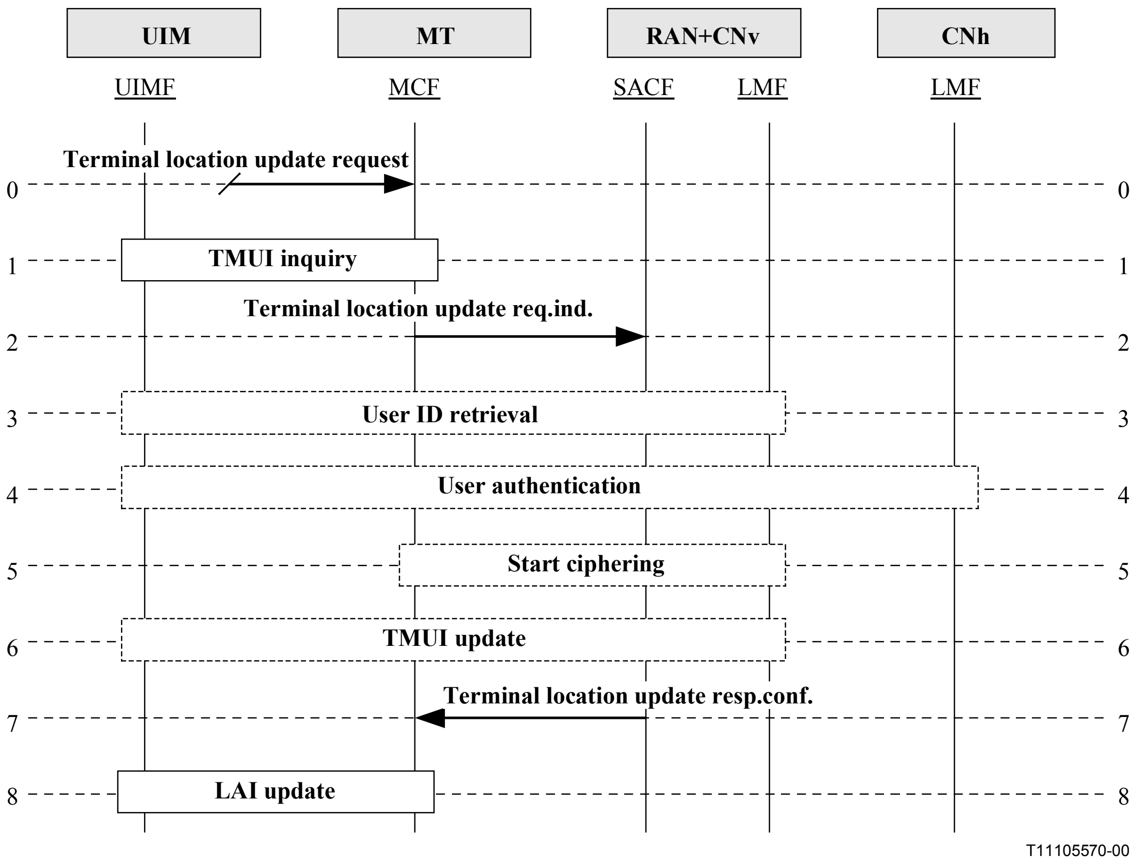


Figure 6.2.3.2-1/Q.1721 – Terminal location updating

0. **Terminal location update request**: request is initiated by the visited network.

FEA0	– Initiate TMUI inquiry procedure to retrieve the TMUI.

1. **TMUI inquiry**: is executed.

2. **Terminal location update req.ind.**: is sent from the MCF to the LMFv.

Terminal location update (Response: Success or Failure)	req.ind.
TMUI	M
TMUI sourceID	M
AUTH_R	O (Note 1)
Confirmation of RANDG	O (Note 1)
CHCNT	O (Note 2)
Terminal Status	O (Note 3)
TC info	O (Note 3)

FEA2	– Initiate User ID retrieval procedure, if TMUI and TMUI assignment source ID are used as the IMT-2000 user ID in the Terminal location update request.
NOTE 1 – Included if authentication is to be carried out. NOTE 2 – Included if Call History Count is available. NOTE 3 – Provided if available.	

3. **User ID retrieval**: is executed to identify the requesting IMT-2000 user, if needed.

4. **User authentication**: is executed if the User ID retrieval procedure was executed.

5. **Start ciphering**: is executed if the user authentication procedure was executed.

6. **TMUI update**: is executed following the above two procedures if they were executed.

7. **Terminal location update resp.conf.**: is the confirmation to Terminal location update req.ind.

Terminal location update	**resp.conf.**
Result	M

FEA7	– Record the LAI. – Initiate the LAI update procedure.

8. **LAI update**: procedure is executed.

6.2.3.3 Detach

The terminal explicitly notifies the serving network that it will not be reachable (e.g. switching off or do not disturb), using this procedure.

In certain situations (e.g. following a period of inactivity) the visited network may decide to notify the LMFh that the user is not reachable, so that for example any request for routing information for mobile terminating calls will be treated accordingly.

This capability may also be used in other implicit cases (e.g. battery discharge or radio signal deterioration). See Figure 6.2.3.3-1.

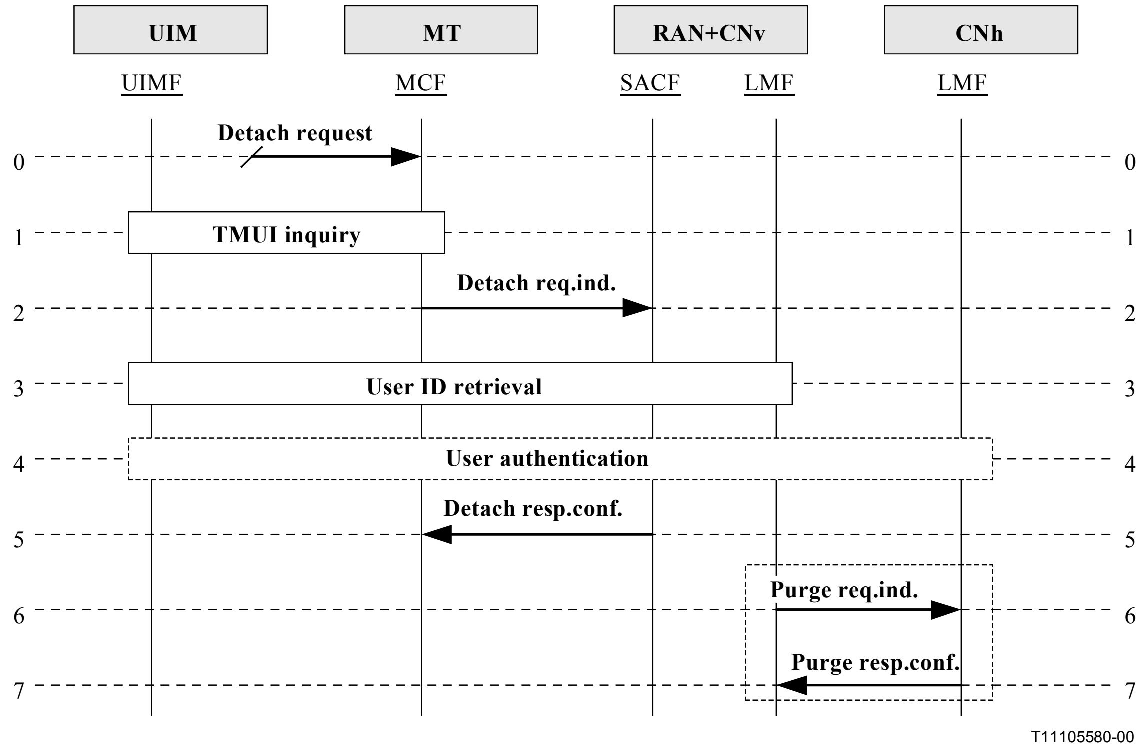


Figure 6.2.3.3-1/Q.1721 – Detach

0. **Detach request**: is the stimulus, initiates the Detach procedure.

FEA0	– Initiate TMUI inquiry procedure to retrieve the TMUI.

1. **TMUI inquiry**: procedure is executed.

2. **Detach req.ind.**: is used by the terminal to notify the serving network that it is going to be unreachable.

Detach (Response: Success or Failure)	req.ind.
UserID	M (Note)

FEA2	– Initiate User ID retrieval procedure, if TMUI and TMUI assignment source ID are used as the IMT-2000 User ID in the Detach request.
NOTE – TMUI should be used instead of IMUI as the IMT-2000 User ID to keep the identity of the user confidential.	

3. **User ID retrieval**: procedure is executed.

4. **User authentication procedure**: is executed, if necessary.

5. **Detach resp.conf.**: is the confirmation of the Detach req.ind.

Detach	resp.conf.
Result	M

FEA5	– Note that the Detach procedure is complete.

6. **Purge req.ind.**: is used by the serving network to notify the home network that the terminal is unreachable.

Purge (Response: Success or Failure)	req.ind.
IMUI	M
LMFv address	O

FEA6	– Mark the IMT-2000 user as not reachable in the notifying network.

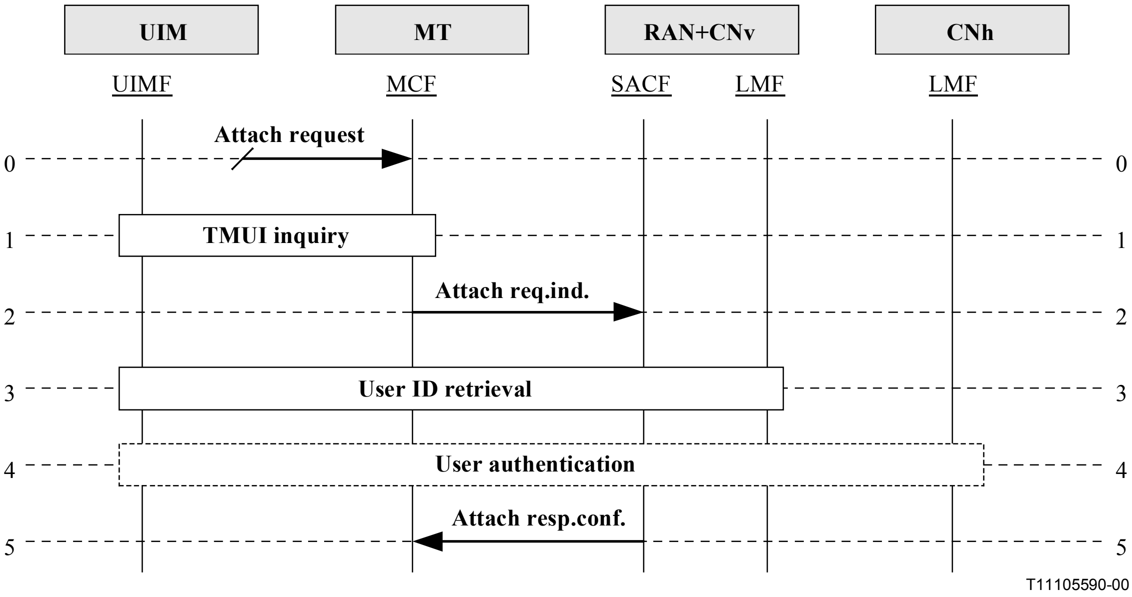
7. **Purge resp.conf.**: is the confirmation to Purge req.ind.

Purge	resp.conf.
Result	M

FEA7	– Decide whether the subscriber record has to be deleted from the LMFv.

6.2.3.4 Attach

See Figure 6.2.3.4-1.



NOTE – If the Attach procedure fails, the MT should interpret this as a need to do the Terminal Location Registration procedure.

Figure 6.2.3.4-1/Q.1721 – Attach

0. **Attach request**: initiates the Attach procedure.

FEA0	– Initiate TMUI inquiry procedure to retrieve the TMUI.

1. **TMUI inquiry**: is executed.

2. **Attach req.ind.**: is used by the terminal to notify the serving network that the MT is reachable.

Attach (Response: Success or Failure)	req.ind.
TMUI	M

FEA0	– Initiate User ID retrieval procedure.

3. **User ID retrieval**: is executed.

4. **User authentication**: is executed, if necessary as a result of the above procedure.

FEA4	– Based on a short message state info in the LMFv (e.g. short message transfer failure because terminal is unreachable), the short message notification procedure will start (not shown in the figure). – If LMFv has the flag set to show that the home system's roaming data is unreliable, the location update will be executed (not shown in the figure). – Acknowledge the Attach req.ind.

5. **Attach resp.conf.**: is the confirmation of the Attach req.ind.

Attach	resp.conf.
Result	M

FEA 5	– MT continues normal operation.

6.2.4 Location data fault recovery

This category of procedures deals with recovery after fault situation. The purpose is to make sure that data stored in different nodes is consistent. In this category three procedures apply:

- Unreliable roamer data.
- Check supplementary service data indication.
- Restore LMF data.

6.2.4.1 Unreliable roamer data

Unreliable roamer data is used to inform a Visited System that the Home System's roaming mobile terminal data is unreliable (e.g. due to a system failure). See Figure 6.2.4.1-1.

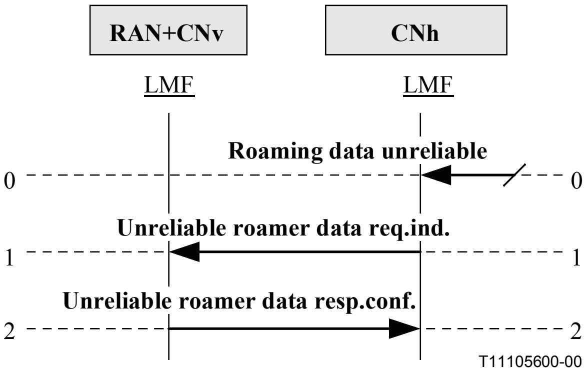

RAN+CNv
CNh
LMF
LMF
Roaming data unreliable
0
0
Unreliable roamer data req.ind.
1
1
Unreliable roamer data resp.conf.
2
2
T11105600-00

Figure 6.2.4.1-1/Q.1721 – Unreliable roamer data

0. **Roaming data unreliable**: indicates that roamer data is unreliable and initiates notification of other systems.

FEA0	– LMFh prepares to inform other system(s) that it has experienced a failure which renders its roaming data unreliable.

1. **Unreliable roamer data req.ind.**: is sent from LMFh to LMF(s) in other system(s).

Unreliable roamer data (Response: Success or Failure)	req.ind.
Home network ID	M

FEA1	– The LMFv removes all records of the subscribers associated with the LMFh sending the message.

2. **Unreliable roamer data resp.conf.**: is the response to the request.

Unreliable roamer	resp.conf.
Result	M

FEA2	– Note the acknowledgement.

6.2.4.2 Check supplementary service data indication

The Check supplementary service data feature is used by the LMFh to indicate to the mobile user that supplementary service data might be altered due to the restart. On receipt from the LMFh, the LMFv forwards this indication to SACF which in turn forwards this indication to the MCF. See Figure 6.2.4.2-1.

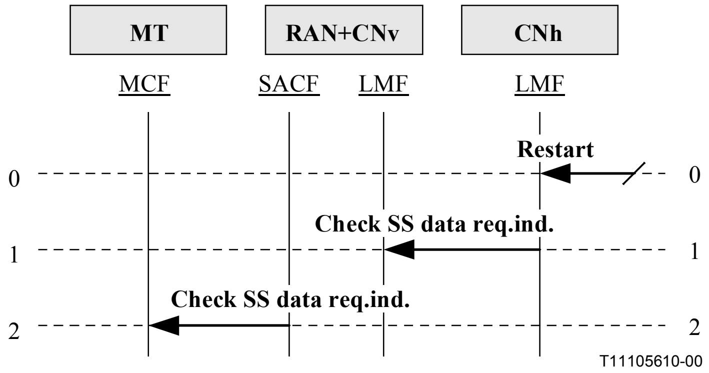


Figure 6.2.4.2-1/Q.1721 – Check supplementary service data indication

0. **Restart**: is the stimulus, initiates the Check SS data procedure.

FEA0	– Determine that a restart has occurred and that the mobile should be informed of possible changes to the SS data.

1. **Check SS data req.ind.**: is sent from LMFh to LMFv.

Check SS data (Response: None)	**req.ind.**
None	N/A

FEA1	– Forward Check SS data req.ind.

2. **Check SS data req.ind.**: is sent from SACF to MCF.

Check SS data (Response: None)	**req.ind.**
None	N/A

FEA2	– The terminal should indicate to the user that SS info should be verified.

6.2.4.3 Restore LMF data

The Restore LMF data feature is used to indicate to the LMFh that it has received a Provide roaming number operation for an unknown IMUI or for a known IMUI with the indicator "Confirmed by HLR" set to "Not confirmed". The service is used to update the Location number (i.e. LAI and LMFv address) in the LMFh, if provided, and to request the LMFh to send all subscriber profile data to the LMFv. See Figure 6.2.4.3-1.

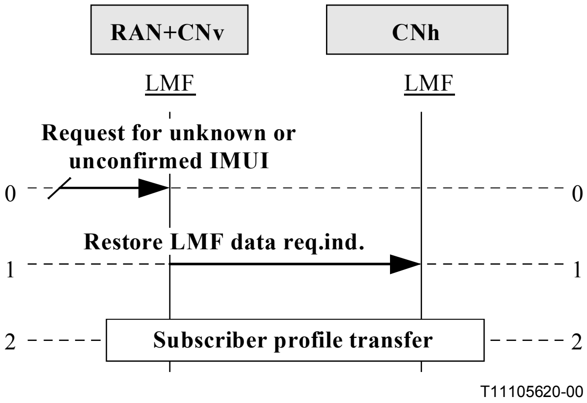

RAN+CNv
CNh
LMF
LMF
Request for unknown or unconfirmed IMUI
0
0
Restore LMF data req.ind.
1
1
2
Subscriber profile transfer
2
T11105620-00

Figure 6.2.4.3-1/Q.1721 – Restore LMF data

0. **Request for unknown or unconfirmed IMUI**: initiates the Restore LMF data procedure.

FEA0	– Determine that a roaming number was requested for an unknown IMUI or for an IMUI that needs confirmation from the LMFh.

1. **Restore LMF data req.ind.**: is sent from the LMFv to the LMFh.

Restore LMF data (Response: Success or Failure)	req.ind.
IMUI	M
LAI	M

FEA1	– Execute the subscriber profile transfer procedure.

2. **Subscriber profile transfer**: is executed to complete the restoration process.

7 Basic call and bearer control

This clause provides the information flows for Basic call and bearer control for IMT-2000 systems, for setting up and tearing down voice calls using circuit switched or packet based bearers.

Basic call and bearer control encompasses IFs for:

- Mobile outgoing call;
- Terminal paging;
- Call routing;
- Mobile incoming call;
- Mobile call release;
- Emergency call; and
- Priority Call.

7.1 Mobile outgoing call

The Mobile outgoing call procedure involves a mobile subscriber originating a call in the idle state (initial call) or in the busy state (additional call). Before the call is established, the visited network validates the calling party and may invoke services based on the origination attempt. This procedure is either local to the serving network or uses the VHE network capability.

7.1.1 Initial mobile outgoing call

The Initial mobile outgoing call procedure is used when the user originates a call in the idle state. See Figure 7.1.1-1.

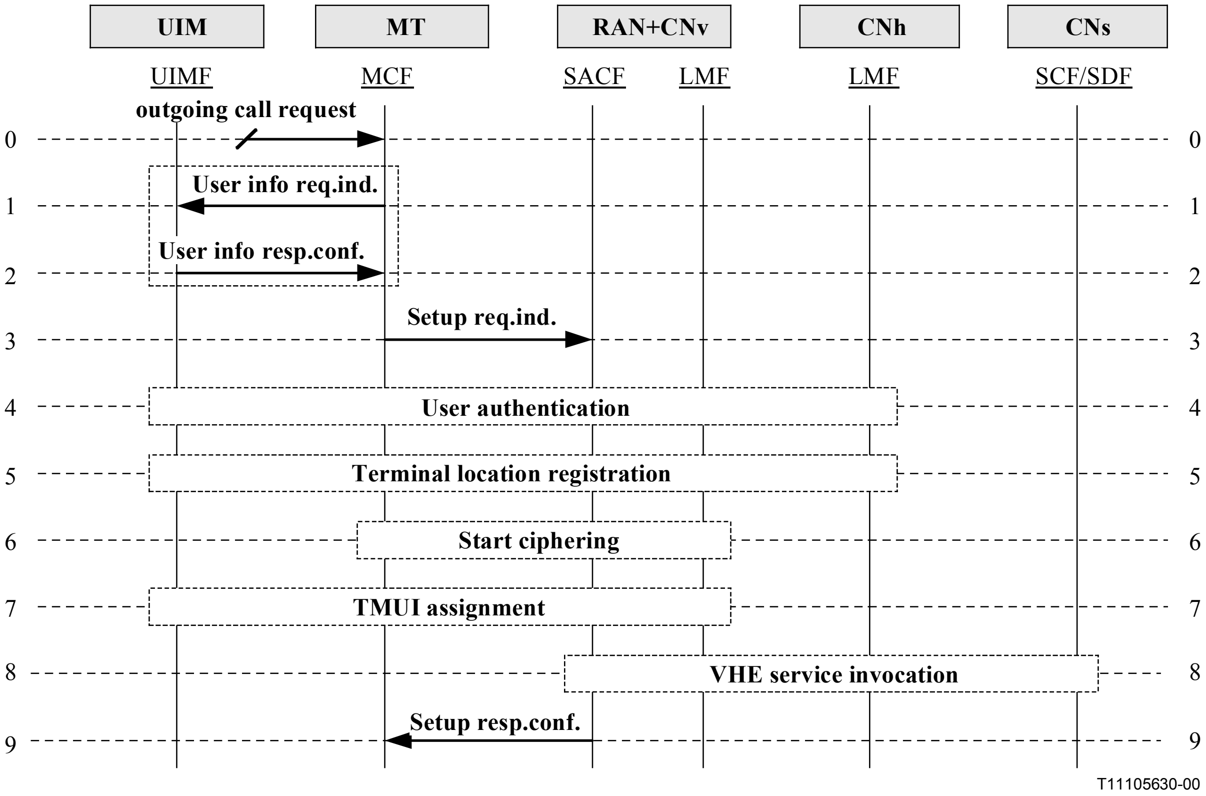


Figure 7.1.1-1/Q.1721 – Initial mobile outgoing call information flow diagram

0. **Outgoing call request**: the mobile subscriber initiates an outgoing (mobile originated) call in the idle state.

FEA0	– The MT may interact with the subscriber to accumulate information. It may invoke service logic (e.g. speed dialling list).

1. **User info req.ind.**: the MCF optionally queries the UIMF for further information/instructions.

User info (Response: Success or Failure)	req.ind.
UIM information request	M

FEA1	– Optionally, invoke local (e.g. UIM based) service logic. – Collect requested information.

2. **User info resp.conf.**: the UIMF returns the requested user information to the MCF.

User info	resp.conf.
UIM information response	M

FEA2	Initiate call setup and bearer request.

3. **Setup req.ind.**: the MCF proceeds to set up the call, and requests the SACF in the serving network to allocate a bearer channel.

Setup (Response: Success or Failure)	req.ind.
UserID	M (Note 1)
Called Number	M
Calling Number	M
Service Identifier	M
Billing ID	O (Note 2)
Bearer Capability	O (Note 3)
QoS	O (Note 4)
AUTH_R	O (Note 5)
RANDC	O (Note 5)
CHCNT	O (Note 5)
IMEI	O (Note 5)
AUTHKEYS	O (Note 6)
SRES	O (Note 7)

FEA3	– Optionally, invoke and await completion of User authentication. – Optionally, invoke and await completion of Terminal location registration. – Optionally, invoke and await completion of Start ciphering. – Set up the call and bearer channel.

NOTE 1 – Include either IMUI or TMUI as available. TMUI is recommended for over-the-air security.

NOTE 2 – Include if required by the home service provider.

NOTE 3 – Include to indicate the capability of the bearer channel.

NOTE 4 – Include to indicate desired quality of service.

NOTE 5 – Include to provide authentication related information only for SSD based systems.

NOTE 6 – Include to provide authentication related information only for non-SSD based systems.

NOTE 7 – Include to provide the signature result.

4. **User authentication**: if authentication is required for this call attempt, it is performed.

5. **Terminal location registration**: if the MT is not registered in the visited network, terminal location registration is performed.

6. **Start ciphering**: if ciphering is required for this call attempt, it is initiated.

7. **TMUI assignment**: if a TMUI needs to be assigned, it can be done any time after ciphering has been initiated.

8. **VHE service invocation**: based on the subscriber profile, the visited network may invoke IN service logic. This may occur at any defined and active trigger detection point.

9. **Setup resp.conf.**: the SACF in the visited network reports the successful completion of call and bearer channel setup.

Setup	**resp.conf.**
Bearer ID	M

FEA9	Complete call setup on selected bearer.

7.1.2 Additional mobile outgoing call

The mobile outgoing additional call involves a mobile subscriber originating a second call while already on a call, i.e. a three-way call. The procedure is performed similarly to mobile outgoing calls.

7.2 Terminal paging

The Terminal paging procedure is used to page a mobile terminal. See Figure 7.2-1.

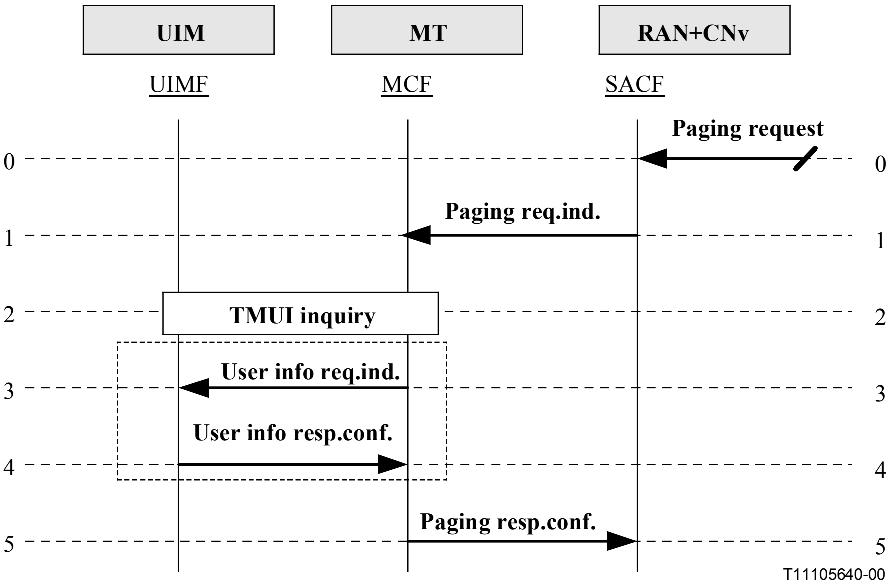


Figure 7.2-1/Q.1721 – Terminal paging

0. **Paging request**: a mobile incoming call results in a page request at the visited network.

FEA0	– The visited network forwards the page request to the MCF.

1. **Paging req.ind.**: the visited network attempts to page the mobile terminal.

Paging (Response: Success or Failure)	**req.ind.**
TMUI	M

FEA1	– Prepare to perform TMUI inquiry.

2. **TMUI inquiry**: the MCF retrieves the TMUI from the UIMF, compares it to the received TMUI from the visited network and determines that the page request is meant for this mobile terminal.

3. **User info req.ind.**: optionally the MCF queries the UIMF for further information/instructions.

User info (Response: Success or Failure)	req.ind.
Termination treatment request	O (Note)

FEA3	Instruct the MCF to respond to the page.
NOTE – Include to request page response instructions from UIMF.	

4. **User info resp.conf.**: the UIMF returns the requested information to the MCF.

User info	resp.conf.
Termination treatment info	O (Note)

FEA4	– Prepare to respond to the page.
NOTE – Include to indicate type of call termination treatment to be applied.	

5. **Paging resp.conf.**: the MCF responds to the page.

Paging	resp.conf.
None	(Note)

FEA5	– None
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

7.3 Network call routing

This subclause addresses end-to-end information flows for inter-family (or inter-network) IMT-2000 call routing operations. Routing a call within an IMT-2000 family member system is considered an intra-family operation and is not addressed here.

The Call routing procedure is used to get an address (e.g. roaming number) from the network element of the visited network where the user is located in order to route a terminating call. The address is dynamically linked to the identity of the user.

Routing information data is needed by the interrogating networks for requesting a "Call Setup" to the visited network of the called party. The term "Routing Information" is used here to represent all the information data that is needed to identify the visited network and the user's terminal location.

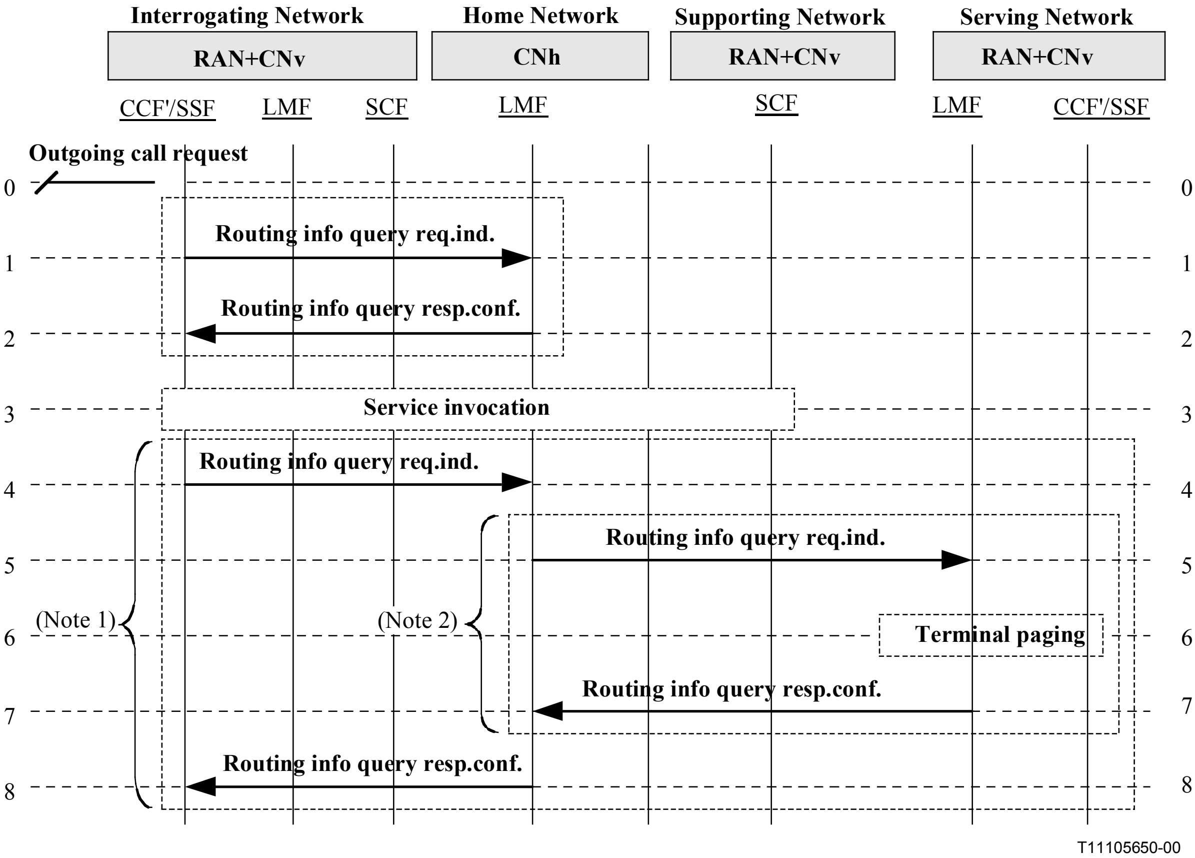
Routing Information query can be executed directly between networks. When either the originating network or the intermediate network is the interrogating network, the query for routing information is sent directly to the home network without routing the call (Call setup request) to the home network. However, the execution depends on the bilateral agreement between networks. When neither the originating network nor the intermediate network are capable of interrogation, the call is routed to the home network and the first query is invoked there. In all these cases, there is only one "interrogating network", either the originating, the intermediate or the home network.

The call routing procedure uses a chain interrogation scheme by which the interrogating network obtains updated routing information (e.g. DN, IP Address) directly from the called party's home network. Furthermore, the chain query scheme is defined as the procedure by which the interrogating network queries for routing information to the called party's home network, and then the home network queries the visited network for the updated called party's routing information.

The following assumptions are made related to this Call routing information flow:

- The "Interrogating Network" could either be the originating, an intermediate, or a supporting network.
- Query for "Routing Information" is sent in a chain scheme from the interrogating network to the called party's home network, and after receiving the information, the call setup request is sent to the called party's visited network.
- The Paging execution in the called party's visited network may be carried out any time after receiving a request for routing information.

See Figure 7.3.1.



NOTE 1 – This service control relationship could be invoked multiple times.
NOTE 2 – These IFs may not be required if the LMFh already has routing information.

Figure 7.3-1/Q.1721 – Call routing

0. **Outgoing call request**: a mobile outgoing call request is received.

FEA0	– The interrogating network initiates routing query procedures.

1. **Routing info query req.ind.**: optionally invoked by the CCF'/SSF of the interrogating network, this flow is used to obtain from the LMFh the routing address of the supporting network if service control is to be performed.

Routing info query (Response: Success or Failure)	req.ind.
Called number	M

FEA1	– Retrieve called party's supporting network's routing address.

2. **Routing info query resp.conf.**: this flow is used to inform the interrogating network of the called party's supporting network's routing address. The supporting network's routing address may (optionally) be used to invoke the called party's IN service features (e.g. Call Screening, Call Barring).

Routing info query	resp.conf.
Routing address (for called party's supporting network)	M

FEA2	Optionally perform IN service invocation procedure.
NOTE 1 – There may be additional service control interactions within the "Service Control Relationship" (schematically shown by the shaded square) encompassing the "Service Logic Invocation" information flows. The Service Control Relationship may end after the first service logic interaction or it may continue until the call is routed. NOTE 2 – Service invocation can be from SSF in the interrogating network to SCF in the home network (possibly relayed via SCF in the interrogating network), or from the LMF in the home network. NOTE 3 – In case service invocation is invoked from the interrogating network, information obtained from the home network in response to the routing information query will contain instruction to the serving network for the service invocation. NOTE 4 – Service invocation can result in different scenarios, like call diversion to, for example, a fixed line, user interaction with an SRF, or other scenarios. This figure depicts only the simple call termination towards the mobile subscriber.	

3. **IN service invocation**: this procedure may be optionally invoked.

4. **Routing info query req.ind.**[1]: invoked by the CCF'/SSF of the interrogating network this flow is used to inquire the routing information (e.g. ITDN for the called party) from the LMF of the called party's home network.

Routing info query (Response: Success or Failure)	req.ind.
Called number	M

FEA4	– Identify called user. – Forward the query to the serving/visited network in order to obtain a routing number (e.g. ITDN).

[1] Conditional, if service invocation from the interrogating network.

5. **Routing info query req.ind.**: this flow is used to forward the query to the LMF in the serving network to obtain the routing number (e.g. ITDN) of the user. It may (optionally) be used to invoke the service logic to page the terminal.

Routing info query (Response: Success or Failure)	req.ind.
IMUI	M
Called number	O

FEA5	– Identify Called user. – Paging procedure (Optional Flows). – Assign a routing number (e.g. ITDN) for the called user.

6. **Terminal paging.**: this procedure is optionally performed, if necessary.

7. **Routing info query resp.conf.**: this flow is used to transfer the routing number (e.g. ITDN) of the called user to the user's home network LMF.

Routing info query	resp.conf.
Routing number of called party (e.g. ITDN)	M

FEA7	– Forward routing number (e.g. ITDN).

8. **Routing info query resp.conf.**: this flow is used to transfer the routing address/number of the called user and may also be used to transfer the result of paging (if executed).

Routing info query	resp.conf.
Routing number of called party (e.g. ITDN)	M

FEA8	– Uses the routing number (e.g. ITDN) to route the call (e.g. via the PSTN) to the serving network.

7.4 Mobile incoming call

The mobile incoming call procedure is used to terminate a call to a mobile terminal in the idle state.

Assuming that the call is optimally routed (the interrogating network is not the home network):

- for basic services the call is routed from the serving network to the destination through call control signalling, using the roaming number previously retrieved;
- for advanced services the VHE applies.

7.4.1 Initial mobile incoming call

See Figure 7.4.1-1.

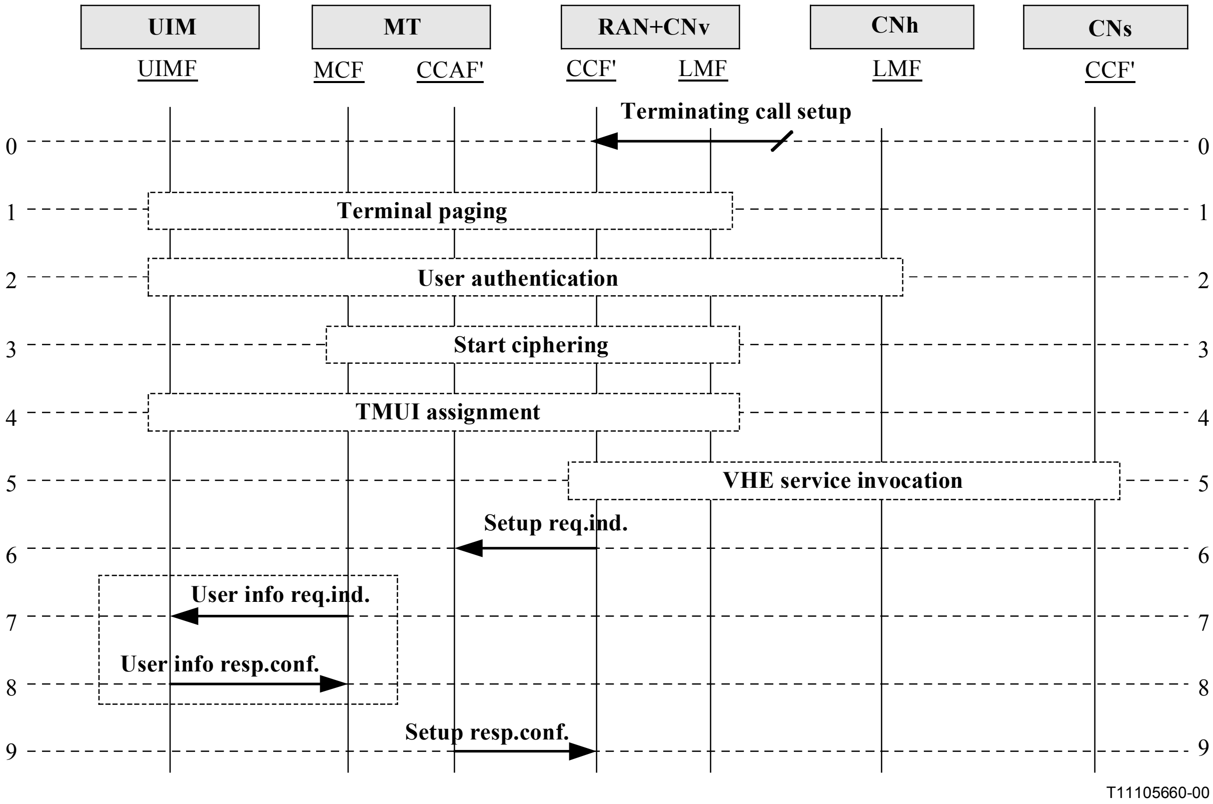


Figure 7.4.1-1/Q.1721 – Mobile incoming call

0. **Terminating call setup**: a call arrives at the serving system for a mobile subscriber in the idle state.

FEA0	– Before establishing the call, the visited network validates the called party and may invoke services based on the termination attempt.

1. **Terminal paging**: the serving system may attempt to page the MT at this time. Paging may have occurred earlier during the routing stage or may not be necessary if the MT is already on another call.

2. **User authentication**: if authentication is required for this call attempt, it is performed.

3. **Start ciphering**: if ciphering is required for this call attempt, it is initiated.

4. **TMUI assignment**: if a TMUI needs to be assigned, it can be done any time after ciphering has been initiated.

5. **VHE service invocation**: based on the subscriber profile, the visited network may invoke IN service logic. This may occur at any defined and active trigger detection point.

6. **Setup req.ind.**: the CCF' proceeds to set up the call.

Setup (Response: Success or Failure)	req.ind.
UserID	M (Note)
Calling Number (IMDN)	M

FEA6	– Optionally, invoke and await completion of User info procedure. – Set up the call and bearer channel.
NOTE – Include either IMUI or TMUI as available. TMUI is recommended for over-the-air security.	

7. **User info req.ind.**: optionally, the MCF queries the UIMF for further information/instructions.

User info (Response: Success or Failure)	req.ind.
Termination treatment request	O (Note)

FEA7	– Instruct the MCF to accept the call.
NOTE – Include to request call treatment instructions from UIMF.	

8. **User info resp.conf.**: the UIMF returns the requested information to the MCF.

User info	resp.conf.
Termination treatment info	O (Note)

FEA8	– Apply the indicated call termination treatment.
NOTE – Include to indicate type of call termination treatment to be applied.	

9. **Setup resp.conf.**: the CCAF' reports the successful completion of call and bearer channel setup.

Setup	resp.conf.
None	(Note)

FEA9	– None.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

7.4.2 Additional mobile incoming call

The mobile incoming additional call involves a mobile subscriber receiving a second call while already on a call, i.e. a three-way call. The procedure is performed similarly to mobile incoming calls, with the exception that paging will not be needed when adding the third party.

7.5 Mobile call release

7.5.1 Normal release: mobile initiated

See Figure 7.5.1-1.

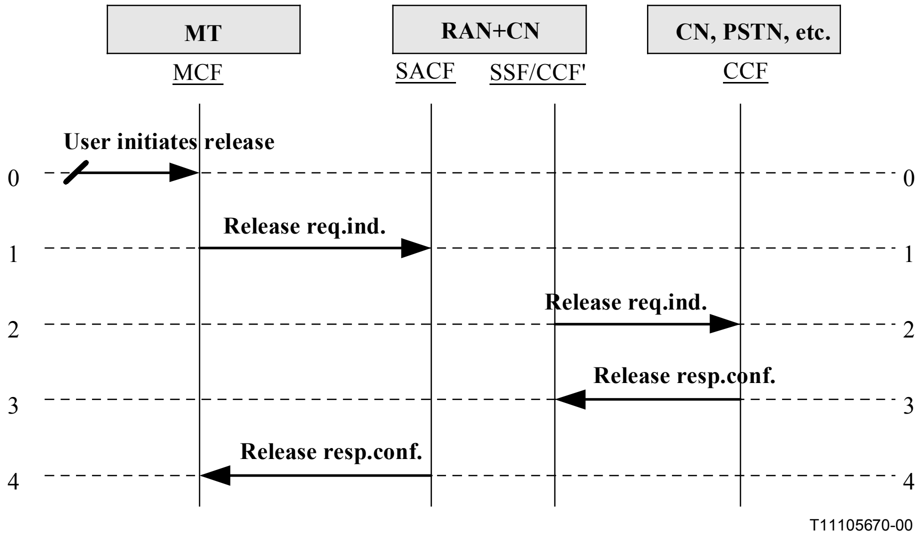


Figure 7.5.1-1/Q.1721 – Mobile initiated normal release

0. **User initiates release**: the mobile subscriber releases the call.

FEA0	– The MT makes a release request.

1. **Release req.ind.**: MCF sends a release request to the SACF.

Release (Response: Success or Failure)	req.ind.
TMUI	M

FEA1	– Prepare to forward the release request to the originating network.

2. **Release req.ind.**: the SSF/CCF' in the visited network forwards the release request to the CCF in the originating network.

Release (Response: Success or Failure)	req.ind.
TMUI	M

FEA2	– Release resources associated with this call.

3. **Release resp.conf.**: the CCF in the originating network returns an acknowledgement of successful call release to the SSF/CCF' in the visited network.

Release	resp.conf.
None	(Note)

FEA3	– Prepare to forward the release response to the visited network.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

4. **Release resp.conf.**: the SACF in the visited network forwards the acknowledgement of successful call release to the MCF.

Release	resp.conf.
None	(Note)

FEA4	– Release resources associated with this call.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

7.5.2 Normal release: network initiated

See Figure 7.5.2-1.

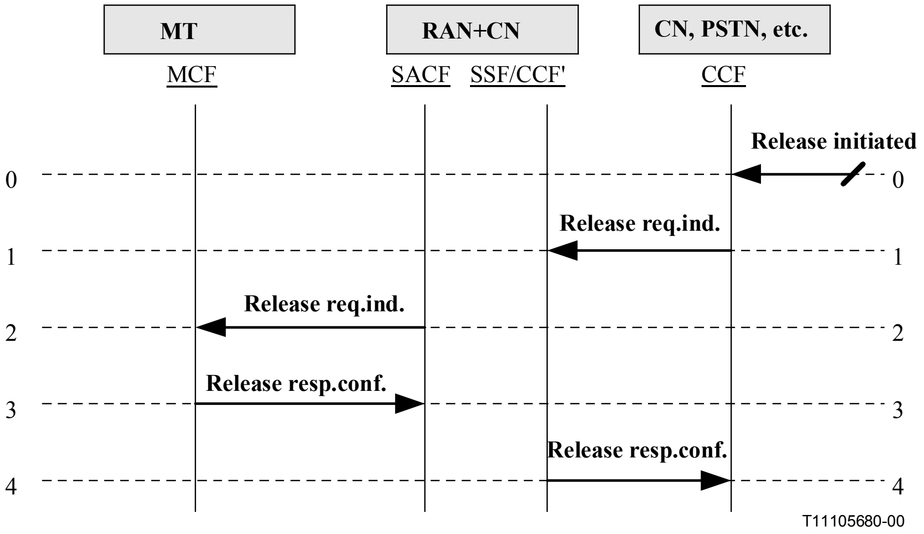


Figure 7.5.2-1/Q.1721 – Network initiated normal release: call information flow diagram

0. **Release initiated**: either the network autonomously initiates release or it receives a release request from a user in the network (e.g. wireline/non-mobile subscriber).

FEA0	– The network prepares to make a release request to the visited network.

1. **Release req.ind.**: CCF sends a release request to the SSF/CCF'.

Release (Response: Success or Failure)	req.ind.
TMUI	M

FEA1	– Prepare to forward the release request to the mobile terminal.

2. **Release req.ind.**: the SACF in the visited network forwards the release request to the MCF.

Release (Response: Success or Failure)	req.ind.
TMUI	M

FEA2	– Release resources associated with this call.

3. **Release resp.conf.**: the MCF returns an acknowledgement of successful call release to the SACF in the visited network.

Release	resp.conf.
None	(Note)

FEA3	– Prepare to forward the release response to the originating network.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

4. **Release resp.conf.**: the SACF in the visited network forwards the acknowledgement of successful call release to the originating network.

Release	resp.conf.
None	(Note)

FEA4	– Release resources associated with this call.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

7.6 Emergency calls

7.6.1 Emergency call origination

Emergency calls should bypass normal authentication and location registration processing. Emergency calls may not require the presence of a UIM in the MT.

The emergency call origination procedure is performed similarly to a mobile outgoing call with the exception that the procedures for User Authentication, Terminal Location Registration, Start Ciphering, TMUI Assignment will not need to be performed. Additionally the serving network receives the call request and attempts to set up the call once a routing number is available. The serving network may invoke VHE service at any defined and active trigger detection point. For an emergency call, this may include a translation of an emergency number into a local or regional number. Also, the geographic position of the MT may be determined at any time after the serving network receives the Setup request. Geographic position determination may occur before any VHE services are invoked.

7.6.2 Emergency call release: network initiated

The emergency call release – network initiated – procedure is performed similarly to call release – network initiated. In an emergency call, when the Public Safety Answering Point (PSAP) releases the call, the complete path to the user will be released.

7.6.3 Emergency call release: mobile initiated

The emergency call release – mobile initiated – procedure is performed similarly to call release – mobile initiated. The resources may be held when the calling user requests the call release and communication of the emergency call is suspended. This procedure is optional and the normal call release procedure (i.e. release of the complete path to the user) may also be applied. If the resources are held and the user originates the call setup afterwards, the suspended emergency call is resumed.

7.7 Priority calls

Priority calling allows a subscriber to have priority access to voice or traffic channels on call origination. This feature permits a subscriber to obtain priority access to voice or traffic channels by queueing these subscribers' originating calls when channels are not available. When a channel becomes available, the queued subscriber is served on a first come first served and a priority basis. The subscriber is assigned one of *n* priority levels at subscription time (where *n* has a minimum and a maximum). Priority levels are defined as 1, 2, 3, … , *n*, with 1 being the highest priority level and *n* being the lowest priority level. The priority level is carried in the Subscriber Profile and is used within the RAN+CN to assign radio channels.

8 Multimedia call and bearer control

This clause covers the information flows for establishing and controlling of multimedia calls, multi-party calls, and packet data services calls including establishing access to Internet services. This clause contains two groups of services: teleservices and access to Internet services.

8.1 Teleservice change

Teleservice change procedure enables an IMT-2000 user to change the service during a call (e.g. switching from voice to data communication and vice versa) which may lead to a change of the access link to be used. From the network-to-network interface perspective, the teleservice change is to modify the bearer to allow for the bearer capability to support the change in the service type. Changes in teleservices may be initiated by either the originating user or the terminating user. However, an end-to-end (mobile-to-mobile) information flow for the teleservice change will cover both cases as shown in Figure 8.1-1.

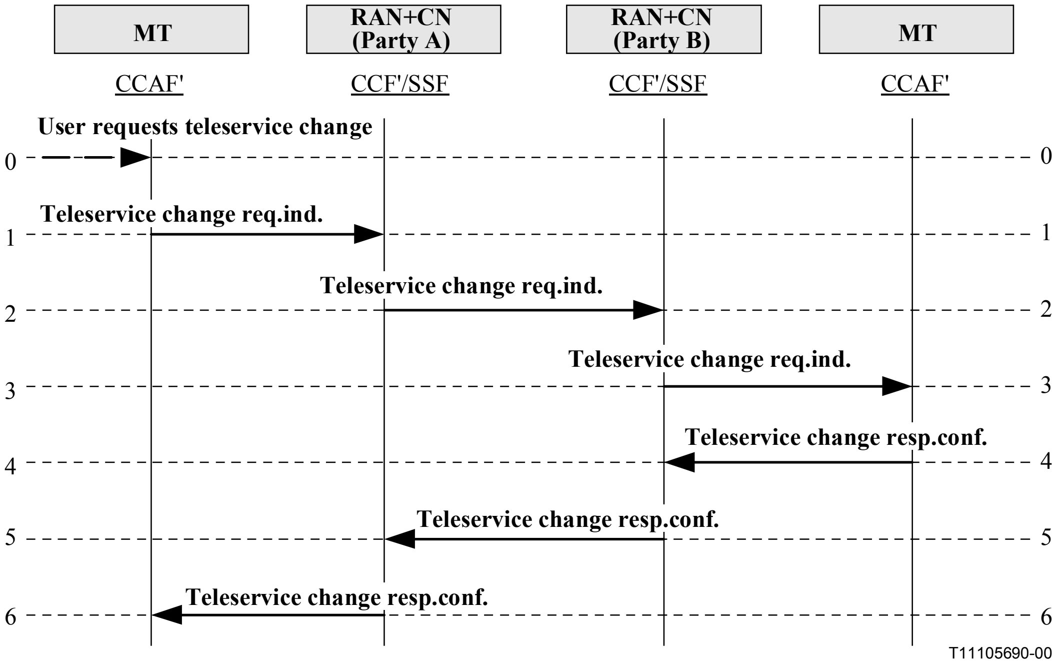

MT
RAN+CN (Party A)
RAN+CN (Party B)
MT
CCAF'
CCF'/SSF
CCF'/SSF
CCAF'
0 User requests teleservice change 0
1 Teleservice change req.ind. 1
2 Teleservice change req.ind. 2
3 Teleservice change req.ind. 3
4 Teleservice change resp.conf. 4
5 Teleservice change resp.conf. 5
6 Teleservice change resp.conf. 6
T11105690-00

Figure 8.1-1/Q.1721 – Teleservice change

0. **User requests teleservice change**: the user requests teleservice (access link) change.

FEA0	– Request for change in the connection.

1. **Teleservice change req.ind.**: is used to request establishment of a connection.

Teleservice change (Report: Success/Failure)	**req.ind.**
Call ID	M
Teleservice type	M

FEA1	– Interact with radio resource management to adjust the access link as requested. – Send request for teleservice change to inform other call party(ies).

2. **Teleservice change req.ind.**: is issued by the CCF'/SSF to make the teleservice change request.

Teleservice change (Report: Success/Failure)	**req.ind.**
Call ID	M
Teleservice type	M

FEA2	– Send teleservice change request.

3. **Teleservice change req.ind.**: is to request Party B network for teleservice change.

Teleservice change (Response: Success or Failure)	**req.ind.**
Call ID	M
Teleservice type	M

FEA3	– Interact with radio resource management for the access link adjustment. – Respond to confirm teleservice (access link) change.

4. **Teleservice change resp.conf.**: is issued by the CCAF' to respond to the teleservice change request.

Teleservice change	**resp.conf.**
Result	M

FEA4	Respond to Party A network to confirm connection establishment for the teleservice change.

5. **Teleservice change resp.conf.**: is used to confirm that the connection has been established.

Teleservice change	**resp.conf.**
Result	M

FEA5	Connect with the new access link.

6. **Teleservice change resp.conf.**: is used to confirm that the connection has been established.

Teleservice change	resp.conf.
Result	M

FEA6	None.

8.2 Add media during a call (mobile user originating)

The purpose of this procedure is to add a media component to an active call. It is supposed that the adding of the media component is related to an allocation into the call of a new bearer dedicated to support it. See Figure 8.2-1.

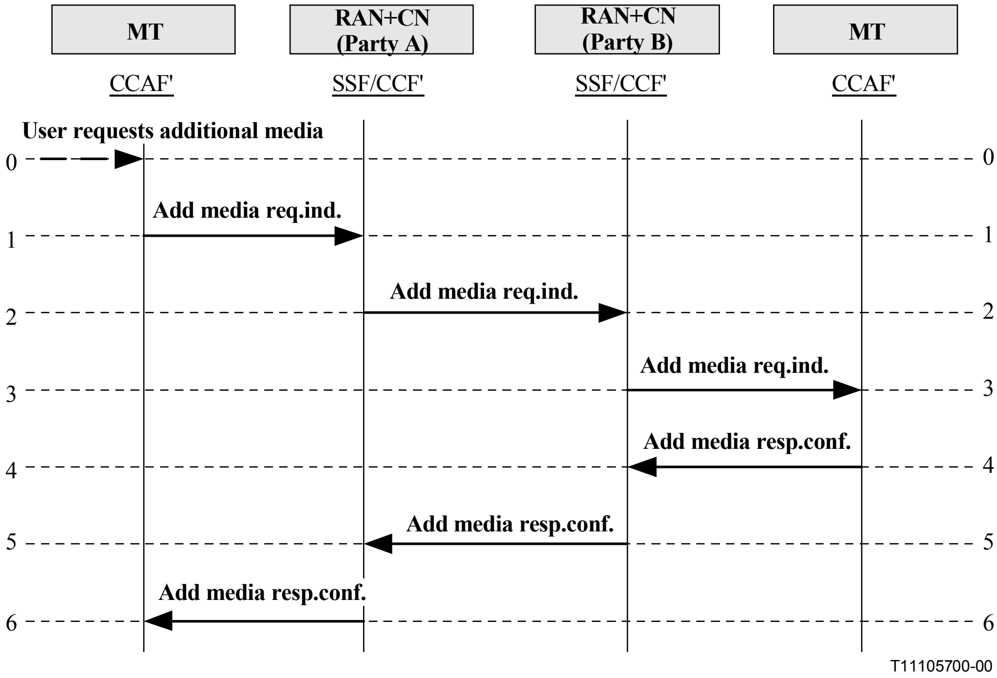


Figure 8.2-1/Q.1721 – Add media to a call (mobile originating)

0. **User requests additional media**: the mobile user wishes to add a media component. It specifies which supplementary service is wanted.

FEA0	– Request for an additional medium. – Send request for connection of access link.

1. **Add media req.ind.**: is to transport the information that the user wishes to add a media component to the active call. It specifies which supplementary teleservice is wanted.

Add media (Response: Success or Failure)	req.ind.
Call ID	M
Medium type	M

FEA1	– Check for service authorization of Party A (internal operation). Request downstream for "Add media".

2. **Add media req.ind.**: is to request for an additional media component to the active call.

Add media (Response: Success or Failure)	req.ind.
Call ID	M
Medium type	M

FEA2	– Check for service authorization of Party B (internal). – Send request for connection of access link.

3. **Add media req.ind.**: is to transport the information that the user wishes to add a media component to the active call. It specifies which supplementary teleservice is wanted.

Add media (Response: Success or Failure)	req.ind.
Call ID	M
Medium type	M

FEA3	– Check for service authorization. – Send request for connection of access link.

4. **Add media resp.conf.**: is to inform that actions are being taken for add media request.

Add media	resp.conf.
Result	M

FEA4	– Relay response.

5. **Add media resp.conf.**: is to inform that actions are being taken for add media request.

Add media	resp.conf.
Result	M

FEA5	– Relay response.

6. **Add media resp.conf.**: is to inform that actions are being taken for add media request.

Add media	resp.conf.
Result	M

FEA6	– Request for the establishment of bearer channel.

8.3 Drop media from an active call

This procedure aims to remove a media component from an active call. It can either be user decided or network decided (if needed resources are no more available and if it concerns a "low class" call). First case is shown here. See Figure 8.3-1.

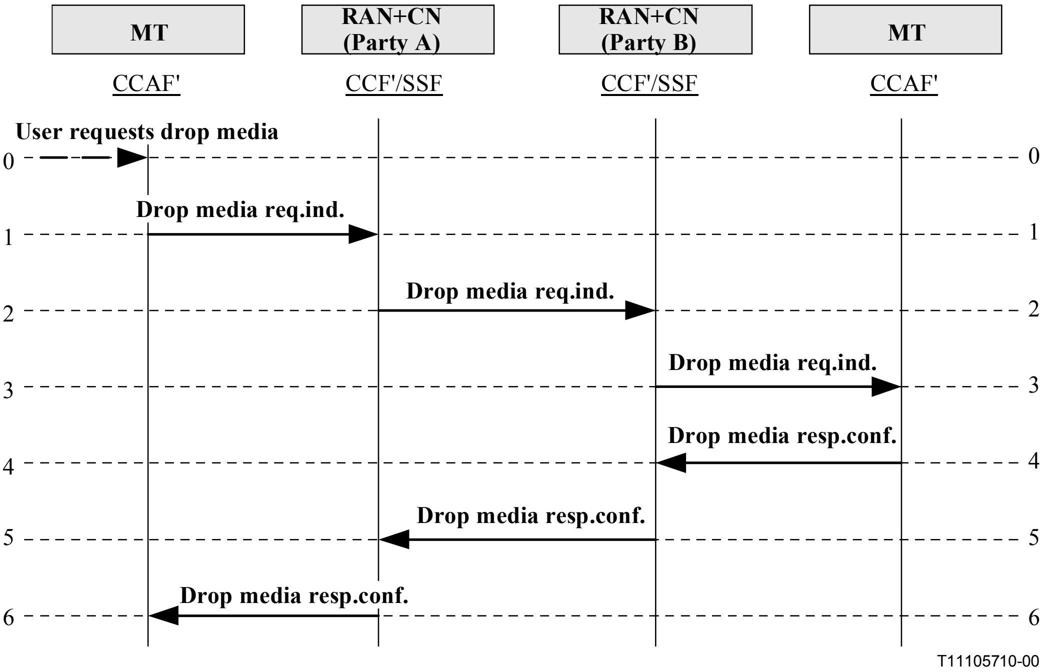


Figure 8.3-1/Q.1721 – Drop media from a multimedia call (mobile originating)

0. **User requests drop media**: is the request from the user to remove a media component.

FEA0	– Send a request for dropping the media component from the corresponding call control entity in the network.

1. **Drop media req.ind.**: is used to request the "drop media" operation.

Drop media (Response: Success or Failure)	req.ind.
Call ID	M
Media ID	M

FEA1	– Identifies the call and the corresponding medium to be dropped. – Forward the "drop media" request to the distant call control entity, Party B's serving network.

2. **Drop media req.ind.**: is to forward the "drop media" request to the core network of other call party to modify the call (removing the concerned bearer) in the part under their responsibility.

Drop media (Response: Success or Failure)	req.ind.
Call ID	M
Media ID	M

FEA2	– Identifies the call and the corresponding medium to be dropped. – Send a request to drop the medium to the access network. – Drop the corresponding media component.

3. **Drop media req.ind.**: is to forward the "drop media" request to the access network to modify the call by removing the medium under its control.

Drop media (Response: Success or Failure)	req.ind.
Call ID	M
Media ID	M

FEA3	– Identifies the call and the corresponding medium to be dropped. – Interact with the radio resource management elements. – Drop the corresponding media component.

4. **Drop media resp.conf.**: is to confirm that both the remote access network and the core network have correctly removed the media component and its related bearer(s).

Drop media	resp.conf.
Result	M

FEA4	– Drop media component and its associated bearer.

5. **Drop media resp.conf.**: is to confirm that both the remote access network and the core network have correctly removed the media component and its related bearer(s).

Drop media	resp.conf.
Result	M

FEA5	– Drop media component and its associated bearer.

6. **Drop media resp.conf.**: is to forward the result to the originating call control FE.

Drop media	resp.conf.
Result	M

FEA6	– Request release of the media associated bearers.

8.4 Point-to-multipoint call

8.4.1 Party addition (mobile-to-mobile)

In a two-party call, each party can request the addition of another party to the call. Party A will become the root of the type 1 network connection (i.e. point-to-point connection) requesting that a new mobile Party C be added to the call. The old type 1 network connection will become a type 2 network connection (i.e. point-to-multipoint connection) with both root and leaf parties being present in the configuration. The request for the "add_party" operation also requires that a "teleservice change" or "notification" procedure be carried out for the call in progress between parties on the call. This subclause addresses both root and leaf initiated party addition procedures.

8.4.1.1 Party addition (root initiated)

Figure 8.4.1-1 shows the information flow diagram for a root initiated party addition. Party C is added to the call already under way between Party A and Party B. For the new party, Party C, in the destination visited network, a mobile incoming call procedure is applied as part of the "connection establishment" common procedure.

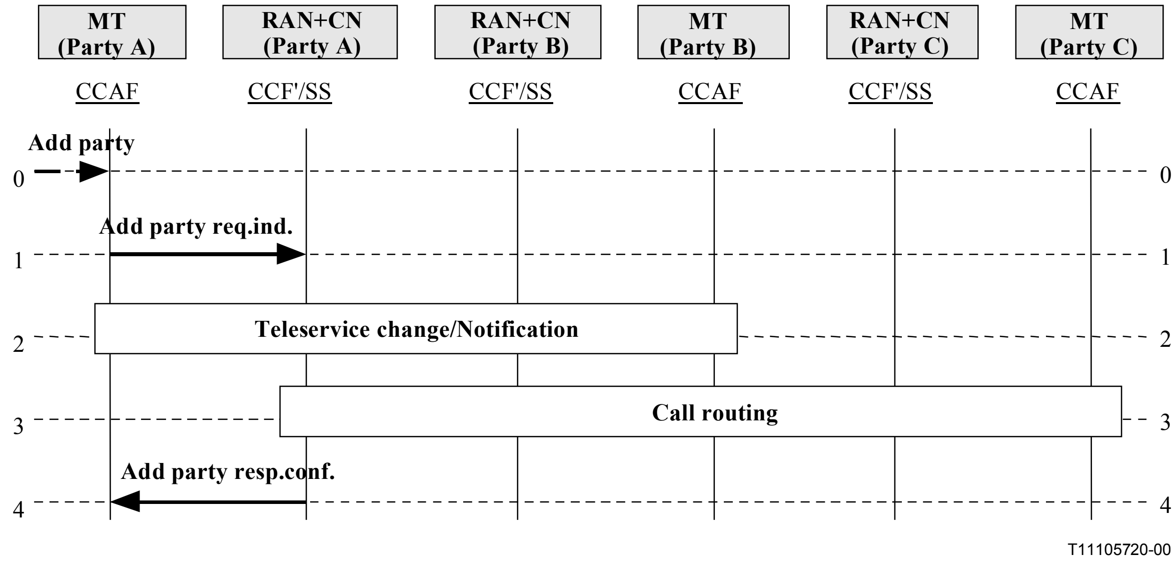


Figure 8.4.1-1/Q.1721 – Party addition (root initiated)

0. **Add party**: is initiated by the user Party A to add another party, Party C, to an ongoing call with Party B.

FEA0	– Send add party request. – A teleservice change request is made for the parties involved in the call.

1. **Add party req.ind.**: is to initiate the addition of a party to an existing connection.

Add party (Report: Success or Failure)	req.ind.
Call ID	M
Called number	M
End point reference	M

FEA1	– Identify the user to be added. – Select and reserve outgoing resources. – Send setup request to initiate call and connection establishment.

2. **Teleservice change/Notification**: is to request change of the service (e.g. from point-to-point to point-to-multipoint) and process addition of access link (if needed).

FEA2	– Request change of service (e.g. from point-to-multipoint to point-to-point).

3. **Call routing**: is used to request establishment of a call to be followed by a bearer connection.

4. **Add party resp.conf.**: is used to acknowledge that the add party request was successful.

Add party	resp.conf.
Call ID	M
End point reference	M

FEA4	– Send add party confirmation. – Request establishment of bearer channel(s).

8.4.1.2 Party addition (leaf initiated)

Figure 8.4.1-2 shows the information flow diagram for a leaf initiated party addition. Party D is to be added by Party C to the call that is already under way between Party A, Party B and Party C. Party C notifies the root party, Party A, for adding Party D to the call. From this point on, the root party CN takes over and performs a "party addition (root initiated)" procedure.

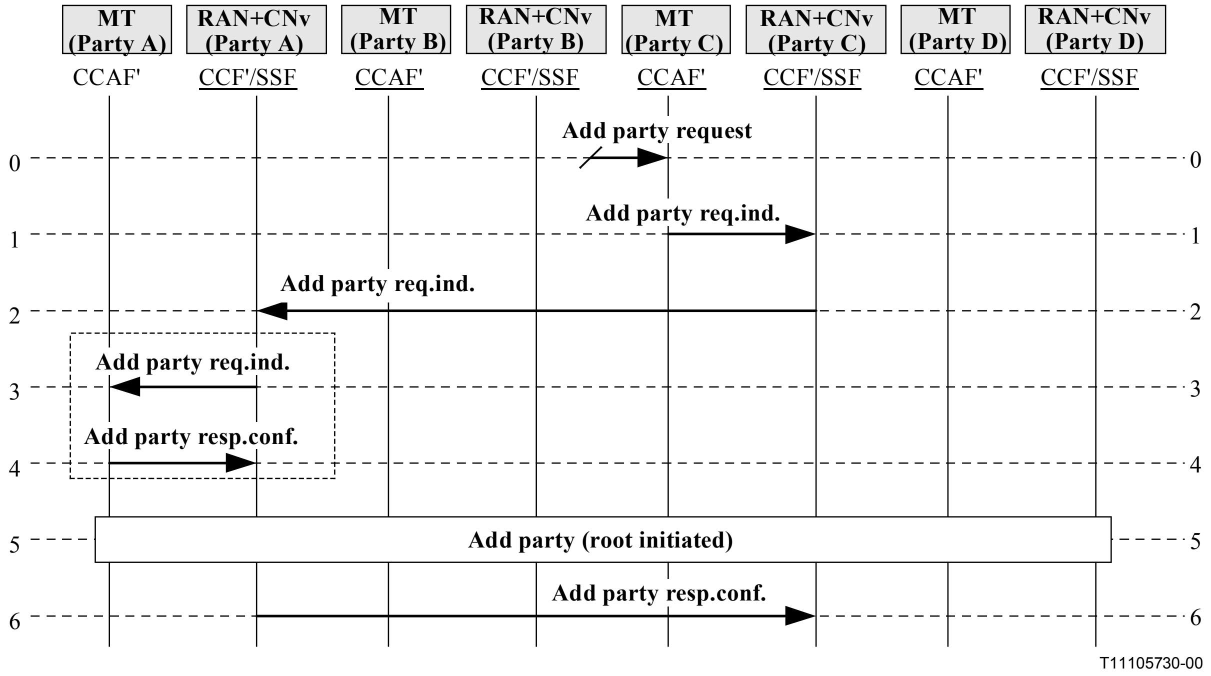


Figure 8.4.1-2/Q.1721 – Party addition (leaf initiated)

The information flows, information elements and functional entity actions related to this procedure are described below in the same order as the flows are shown in Figure 8.4.1-2.

0. **Add party request**: is initiated by the user Party C to add another party, Party D, to an active call with Parties A and B.

1. **Add party req.ind.**: is to initiate the addition of a party to an existing connection.

Add party (Report: Success or Failure)	req.ind.
Call ID	M
Called number	M

FEA1	– Send an add party request to the root party. – Select and reserve outgoing resources.

2. **Add party req.ind.**: is to initiate the addition of a party to an existing connection.

Add party (Report: Success or Failure)	req.ind.
Call ID	M
Called number	M
End point reference	M

FEA2	– Identify the new party to be added. – Notify all call parties (except the requesting party) of the party addition. – Select and reserve outgoing resources. – Send setup request to initiate call and connection establishment. – Provide end point reference.

3. **Add party req.ind.**: (optional) is to initiate the addition of a party to an existing connection.

Add party (Response: Neither Success nor Failure)	req.ind.
Call ID	M
Called number	M
End point reference	M

FEA3	– Identify the new party to be added. – Acknowledge the request to add party. – Initiate the add party procedure.

4. **Add party resp.conf.**: is used to acknowledge the add party request.

Add party	resp.conf.
Result	M

FEA4	– None.

5. **Party Addition (root initiated)**: is used to request addition of a party by the root party of an ongoing call.

6. **Add party resp.conf.**: is used to acknowledge that the add party request was successful.

Add party	**resp.conf.**
Result	M

FEA6	– None.

8.4.2 Party dropping

A leaf party may be dropped from an existing point-to-multipoint connection by a request from either the root party or the leaf party itself.

8.4.2.1 Party dropping (root party initiated)

The root party (Party A) may request that a leaf party (Party C) be dropped from the connection. In this procedure, the resources between Party C and the core network are released normally by trigger of the core network. See Figure 8.4.2-1.

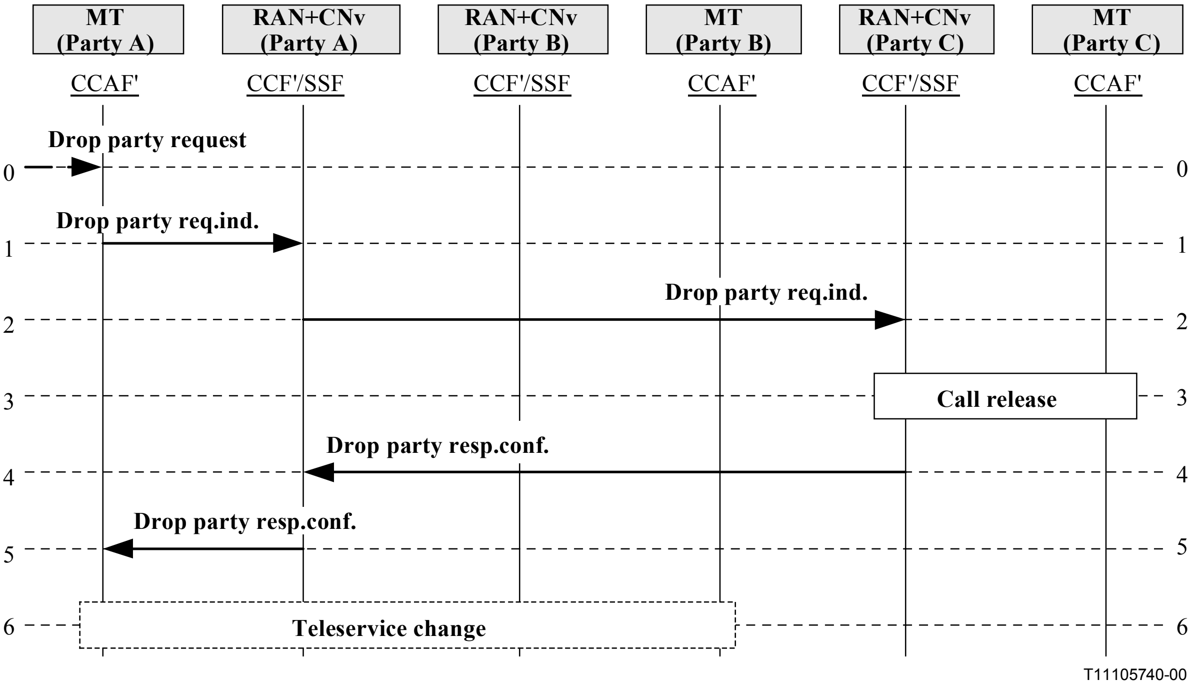


Figure 8.4.2-1/Q.1721 – Party dropping (root party initiated)

0. **Drop party request**: is the user's request to drop a call party.

FEA0	– Identify the party to be dropped. – Verify the states of all other leaf parties associated with the connection, if necessary.

1. **Drop party req.ind.**: is to initiate the detachment of a party from an existing connection.

Drop party (Response: Success or Failure)	req.ind.
Call ID	M
End point reference	M
Cause	M

FEA1	– Identify the requesting user. – Acknowledge that the requesting user is root. – Identify the party to be dropped. – Verify the states of all other leaf parties associated with this connection.

2. **Drop party req.ind.**: is to initiate the detachment of a party from an existing connection.

Drop party (Response: Success or Failure)	req.ind.
Call ID	M
End point reference	M
Cause	M

FEA1	– Identify the requesting user. – Acknowledge that the requesting user is root. – Identify the party to be dropped. – Verify the states of all other leaf parties associated with this connection. – Initiate Release call procedure.

3. **Release call**: (network initiated) procedure is used to request the drop of a party from the call.

FEA3	– Send drop party/release call response.

4. **Drop party resp.conf.**: is used to notify that the drop party request was successful.

Drop party	resp.conf.
Cause	O (Note)

FEA4	– Relay drop party confirmation response.
NOTE – Send information on the cause of release of the party if available.	

5. **Drop party resp.conf.**: is used to notify that the drop party request was successful.

Drop party	resp.conf.
Cause	O (Note)

FEA5	– Send drop party confirmation.
NOTE – Send information on the cause of release of the party if available.	

6. **Teleservice change**: procedure is a request for the possible change of teleservice for Party A and Party B, changing from point-to-multipoint to point-to-point.

FEA6	– Request change of service (e.g. from point-to-multipoint to point-to-point).

8.4.2.2 Party dropping (a leaf party initiated)

On receipt of release request from a leaf party to be dropped (Party C), core network notifies the root party (Party A) that the leaf party has dropped by sending drop party request. See Figure 8.4.2-2.

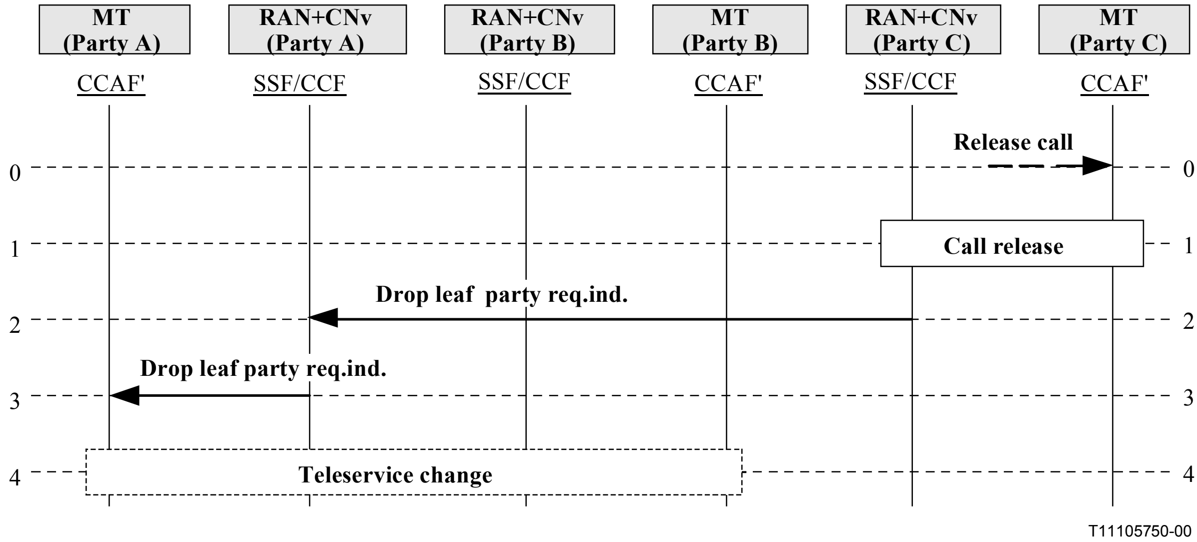


Figure 8.4.2-2/Q.1721 – Party dropping (a leaf party initiated)

0. **Call release**: is initiated from a leaf party requesting to be dropped from the call/connection.

FEA0	– Start mobile call release procedure. – Identify the leaf party (requesting party) to be dropped. – Send a drop party request to the root party's network.

1. **Call release**: procedure is to release the call between the dropping leaf party and the remaining parties in the call.

FEA1	– Send a drop party request to the root party's mobile terminal.

2. **Drop party req.ind.**: is sent to notify the detachment of a leaf party from an existing connection.

Drop party (Response: Neither Success nor Failure)	req.ind.
Call ID	M
End point reference	M
Cause	M

FEA2	– Identify the detached leaf party based on end point reference. – Verify the states of all other leaf parties associated with the connection, if necessary. – Send drop party indication.

3. **Drop party req.ind.**: is sent to notify the detachment of a leaf party from an existing connection.

Drop party (Response: Neither Success nor Failure)	req.ind.
Call ID	M
End point reference	M
Cause	M

FEA3	– Identify the detached leaf party based on end point reference. – Verify the states of all other leaf parties associated with the connection, if necessary. – Send drop party indication.

4. **Teleservice change**: (optional) is to process a change of teleservices for the remaining parties in the call.

FEA4	– Request change of service (e.g. from point-to-multipoint to point to-point).

8.5 Access to Internet services

The access to Internet services enables a roaming IMT-2000 subscriber to initiate a data service session in a visited Core Network (CN). Once the data service session has been established, the subscriber will be able to roam into the next visited CN without any interruption in the data service session. When starting a data service session, the subscriber's mobile terminal may have one or several public IP addresses, that was permanently allocated to it by the home CN, or a public IP address (one or several) may be dynamically allocated to it by the home CN or by the visited CN. The routing context in the IMT-2000 network will be established when the session is initiated and it will be updated whenever the mobile terminal roams into the next visited CN.

The procedures described in this subclause are mandatory when roaming between IMT-2000 networks with different core network architectures (i.e. from different IMT-2000 family members). Roaming between networks implemented using the same family member may use family-member specific procedures.

8.5.1 Packet data service session establishment

To access packet data services, the roaming mobile terminal will register with the visiting IMT-2000 network by employing common authentication and terminal registration procedures, and requesting access to packet data facilities. The mobile terminal will register for use of packet data resources upon gaining access to packet data facilities. The IMT-2000 architecture will allow for separation of LMF (and associated AMF) capabilities that pertain to access facilities and LMFp (and associated AMFp) capabilities that pertain to the packet data services.

Figure 8.5.1-1 shows the information flow diagram for this procedure. Steps 4-7 may be repeated in order to support multiple data sessions from the same mobile terminal.

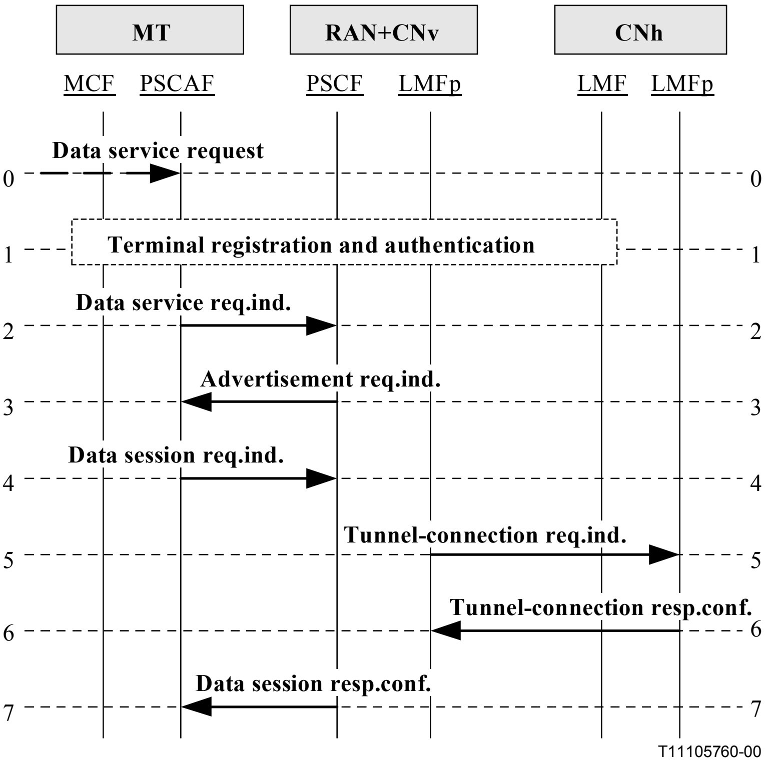


Figure 8.5.1-1/Q.1721 – Packet data session establishment

0. **Data service request**: the user initiates a packet data service session.

FEA0	– Request establishment of a data service session, preceded by terminal registration and authentication.

1. **Terminal registration and authentication**: is required if not already done.

2. **Data service req.ind.**: is to initiate a data service session in the visited network by requesting the service.

Data service (Response: Neither Success nor Failure)	req.ind.
User ID	M
Service type (data)	M

FEA2	– Employs the link layer procedure to establish an access link to be followed by "advertisement" request.

3. **Advertisement req.ind.**: is for the flow to the terminal to request establishment of a data session when a new network access identifier (NAI) is detected.

Advertisement (Response: Neither Success nor Failure)	req.ind.
IP address (PSCF)	M
IP address (PSCF-Public)	M (Note)
Challenge value	M
NAI (PSCF)	M

FEA3	– Respond to the advertisement with a Data Session request if it detects a new PSCF NAI. – Specify a well-known UDP port and the IP address of the PSCF as a destination for this information.
NOTE – This IP address is the address of the foreign agent (e.g. it is used as the tunnel termination point seen from the PSGCF).	

4. **Data session req.ind.**: is sent from the PSCAF to the PSCF in the visited network over the established access link to request the establishment of a new data session[2].

Data session (Response: Success or Failure)	req.ind.
Session ID	O (Note 1)
NAI (MT)	M
NAI (PSCFpv)	M
IP address (MT)	O (Note 2)
IP address (PSCF Public)	M
Service discriminator	O (Note 3)
Challenge value (from PSCF)	M
Challenge response	M
Encapsulation method	M
Data session lifetime	M

FEA4	– Determine address of LMFp based on service discriminator. – Request the establishment of a tunnel-connection for this data session. – May reduce the proposed data session lifetime before forwarding this information to the LMFp.
NOTE 1 – If it is a case of multiple session. NOTE 2 – Static assignment if the IP address is static and permanent, else dynamic assignment. NOTE 3 – The LMFp may need the service discriminator for authorization purposes.	

5. **Tunnel-connection req.ind.**: is from the visited LMFp to the mobile terminal's home LMFp to authenticate and authorize the visiting mobile terminal to use the packet data services in the visited network.

Tunnel-connection (Response: Success or Failure)	req.ind.
NAI (MT)	M
NAI (PSCFpv)	M
NAI (PSCFv)	M
IP address (MT)	O (Note 1)
IP address (PSCF Public)	M
Service discriminator	O (Note 2)
Challenge value (from PSCF)	M

[2] Not to confuse the mobile terminal "Registration" procedure with the registration to establish data session, the name "Data Session" was chosen to this flow.

Tunnel-connection (Response: Success or Failure)	req.ind.
Challenge response	M
Encapsulation method	M
Data session lifetime	M

FEA5	– Determine PSGCF based on service discriminator. – Authenticate the mobile terminal by using the challenge value, challenge response and the secret that it shares with its mobile terminal. – May allocate an IP address to the mobile terminal or it may decide that the PSGCF should allocate this address. As requested by the tunnel-connection req.ind., the PSGCF may be dynamically allocated, or it may have been already statically pre-allocated to the mobile terminal. – If the PSGCF is dynamically allocated, then the home LMFp may either allocate it in the home network or the home LMFp may decide that the visited network should allocate the PSGCF. – May also generate a set of security keys and security parameter indices (SPIs) that will be distributed to the mobile terminal, visited PSCF, and PSGCF to support encryption and security associations between these entities. – Employ the shared secrets it shares with the PSCAF, home PSGCF and the visited LMFp. – May also reduce the proposed data session lifetime before forwarding this information to its PSGCF or the visited LMFp. – Return the tunnel-connection response to the visited LMFp indicating that the PSGCF in the visited network should be allocated.
NOTE 1 – Static IP address assignment if the IP address is static and permanent, else dynamic assignment. NOTE 2 – The LMFp may need the service discriminator for authorization purpose.	

6. **Tunnel-connection resp.conf.**: is sent from the mobile terminal's home LMFp to the visited LMFp to authorize the packet data service for the mobile terminal in the visited network.

Information elements	resp.conf.
Result (PSGCF allocation indication)	M
IP address (PSGCF public)	M
IP address (MT) included if assigned by home network	O (Note)
Data session lifetime	M
Security information	M

FEA6	– Respond to confirm the establishment of the tunnel connection. – Send result for establishment of the data session.
NOTE – IP address may not be required if no new assignment by the home network has taken place.	

7. **Data session resp.conf.**: is a response to a request for establishment of a new data session.

Registration	resp.conf.
Session ID	O (Note)
Result (success or fail)	M
IP address (PSGCF public)	M
IP address (MT)	M
Security information	M
Session lifetime	M

FEA7	Continues with the data session, no further action needed.
NOTE – If supplied by PSCAF in flow 4.	

8.5.2 Roaming during an established packet data session

When roaming into the next visited network, a PSGCF in the anchor network has already been assigned to the mobile terminal. The anchor network may be either the home network or the visited network where the data session was initiated. The mobile terminal may register with the next visiting network by employing common authentication and terminal registration procedures. By invoking the radio resource management (RRM) procedure, the mobile terminal will establish an access link with the PSCF in the next visited network. Since the advertised PSCF NAI address is different than the current one, the PSCAF will start a new "packet data service session establishment" procedure as shown in Figure 8.5.2-1.

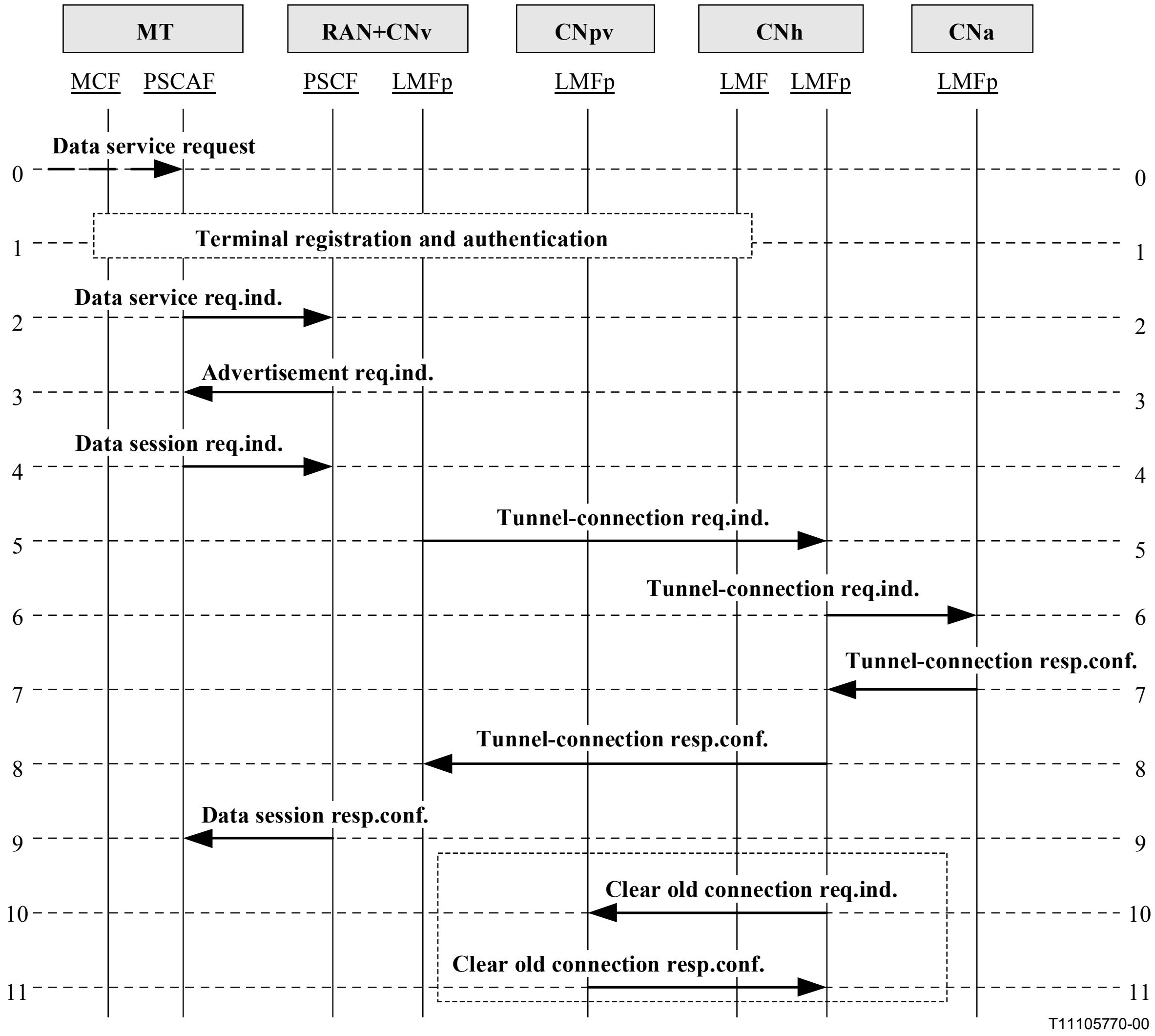

MT
RAN+CNv
CNpv
CNh
CNa
MCF
PSCAF
PSCF
LMFp
LMFp
LMF
LMFp
LMFp
Data service request
Terminal registration and authentication
Data service req.ind.
Advertisement req.ind.
Data session req.ind.
Tunnel-connection req.ind.
Tunnel-connection req.ind.
Tunnel-connection resp.conf.
Tunnel-connection resp.conf.
Data session resp.conf.
Clear old connection req.ind.
Clear old connection resp.conf.
0
1
2
3
4
5
6
7
8
9
10
11
T11105770-00

Figure 8.5.2-1/Q.1721 – Roaming during an established data session

This information flow diagram is similar to the information flow diagram of 8.5.1 up to the "tunnel connection" operation where the flow is forwarded (from the home network) to the anchor network. In addition, the "clear old connection" operation must be performed once the new connection is established.

0. **Data service request**: is the trigger to register for the mobile terminal during an established packet data session.

FEA0	– Initiate terminal authentication and registration if required.

1. **Terminal registration and authentication**: is for the mobile terminal to register with the visited network before requesting packet data service.

FEA1	– Request a data service session establishment.

2. **Data service req.ind.**: the mobile terminal initiates a data service session in the visited network.

Data service (Response: Neither Success nor Failure)	req.ind.
User ID	M
Service type (data)	M

FEA2	– Request for access link setup to be followed by the "Advertisement" operation request to the terminal.

3 **Advertisement req.ind.**: is sent to the terminal to request establishment of a data session when a new NAI is detected.

Advertisement (Report: Neither Success nor Failure)	req.ind.
IP address (PSCFv)	M
IP address (PSCFv – Public)	M
Challenge value (PSCFv)	M
NAI (PSCFv)	M

FEA3	– Respond to the advertisement with a registration if it detects a new PSCF NAI. – Specify a well-known UDP port and the IP address of the visited PSCF as a destination for this information. – Specify a UDP port that should be used by the visited PSCF when returning the reply information to the PSCAF.

4. **Data session req.ind.**: is sent from the PSCAF to the PSCF in the visited network over the established access link to request the establishment of a new tunnel-connection for the existing data session.

Registration (Response: Success or Failure)	req.ind.
Session ID	O (Note 1)
NAI (MT)	M
NAI (PSCFpv)	M
IP address (MT)	M
IP address (PSCFv Public)	M
Service discriminator	M (Note 2)
IP address (PSGCF Public)	M
Challenge value (PSCFv)	M
Challenge response	M
Encapsulation method	M
Data session lifetime	M

FEA4	– Communicate with its LMFp to request the establishment of a new tunnel-connection with the anchor PSGCF for the existing data session. – Store locally all information that has been supplied to it by the PSCAF in the Registration req.ind. and bind this information to the access link and the IMSI if it was supplied during the access link establishment. – May reduce the proposed data session lifetime before forwarding this information to its LMFp. – Assign a transaction identifier to this transaction. Subsequently, it will forward the information obtained from the Registration req.ind. to its LMFp. A security association between the next visiting PSCF and its LMFp will have been previously arranged. – Store the session ID.
NOTE 1 – If supplied by PSCAF in flow 4. NOTE 2 – The service discriminator, as it is used in 8.4.1, is not used here as the session is already active in the PSGCF. Consequently, the LMFp does not select the PSGCF. However, the LMFp may need the service discriminator for authorization purposes.	

5. **Tunnel-connection req.ind.**: is sent from the Visited LMFp to the mobile terminal's home LMFp to authenticate and authorize the visiting mobile terminal and establish a new tunnel-connection between the Visited PSCF and the PSGCF. Based on the previous NAI information, the visited LMFp will determine that the previous PSCF is in a different network. The mobile terminal's NAI will be used to locate its home LMFp. A security association between the visited LMFp and the home LMFp should exist before any information can be exchanged between these two entities. The visited LMFp forwards this information with the information that was included in the original registration req.ind. to the home LMFp.

Tunnel connection (Report: Success or Failure)	**req.ind.**
NAI (MT)	M
NAI (PSCFpv)	M
NAI (PSCFv)	M
IP address (MT)	M
IP address (PSCFv Public)	M
Service discriminator	M
IP address (PSGCF Public)	M
Challenge value (from PSCFv)	M
Challenge response	M
Encapsulation Method	M
Data session lifetime	M

FEA5	– Authenticate the mobile terminal by using the Challenge Value, Challenge Response and the secret it shares with its mobile terminal. – Detect that this is an established packet data session and it will know whether the anchor network is the home network or the visited network where the session was initiated. – May decide to use the existing security keys and Security Parameter Indices (SPIs) that were allocated to the previous PSCF or it may generate new values for these parameters. – When passing the security keys and SPIs to the PSCAF, anchor PSGCF, anchor LMFp, and the Visited LMFp, the home LMFp will employ the shared secrets it shares with these entities. – When the anchor network is not the home network, the home LMFp will forward the tunnel-connection req.ind. to the anchor LMFp in the visited network where the session was initiated. – For the case where the PSGCF is in the home network, a request is sent from the home LMFp to its PSGCF in the home network to request the establishment of a new tunnel-connection between the visited PSCF and the home PSGCF.

6. **Tunnel-connection req.ind.**: is sent from the home LMFp to the anchor LMFp to request the establishment of a new tunnel-connection between the anchor PSGCF and the visited PSCF. The home LMFp has recorded the NAI of anchor LMFp when the data session was initiated.

Tunnel connection (Response: Success or Failure)	req.ind.
NAI (MT)	M
IP address (MT)	M
IP address (PSCFv Public)	M
IP address (PSGCF Public)	M
Encapsulation method	M
Remaining data session lifetime	M
Security keys and SPI	M
Data session lifetime	M

FEA6	– Detect that this is an established data session. – Forward a request to its PSGCF to request the establishment of a new tunnel-connection between the visited PSCF and the anchor PSGCF.

7. **Tunnel-connection resp.conf.**: is sent from the anchor LMFp to the home LMFp to indicate whether the request to establish a new tunnel-connection between the visited PSCF and the anchor PSGCF has been accepted or rejected.

Tunnel connection	resp.conf.
Result (PSGCF allocation indication)	M
IP address (PSGCF public)	M
IP address (MT)	M
Data session lifetime	M

FEA7	– Respond to confirm authorization of establishing the new data session. – Optionally, request previously visited network to remove the old connection, "clear old connection" operation.

8. **Tunnel-connection resp.conf.**: is sent from the mobile terminal's home LMFp to the visited LMFp to authorize the packet data service for the mobile terminal in the visited network and indicate whether a new tunnel-connection with the anchor PSGCF has been established.

Tunnel connection	resp.conf.
Result (PSGCF allocation indication)	M
IP address (PSGCF public)	M
IP address (MT)	M
Data session lifetime	M
Security keys and SPI	M

FEA8	– Informs the Visited PSCF whether a new tunnel-connection has been established.

9. **Data session resp.conf.**: is sent from the Visited PSCF to the PSCAF in response to the Registration req.ind. requesting the establishment of a new tunnel-connection. This information is sent over the established access link.

Data session	resp.conf.
Result (PSGCF allocation indication)	M
IP address (PSGCF public)	M
IP address (MT)	M
Security keys and SPI	M
Data session lifetime	M
Session ID	O (Note)

FEA9	– No action required.
NOTE – If supplied by PSCAF.	

10. **Clear old connection req.ind.**: (optional) is for the home LMFp to inform the previously visited LMFp to clear all local information that pertains to the old tunnel-connection with the anchor PSGCF. This IF is independent of IF 9.

Clear old connection (Response: Neither Success nor Failure)	req.ind.
NAI (MT)	M
IP address (MT)	M
NAI (PSCFpv)	M
IP address (PSGCF-Public)	M

FEA11	– Respond to confirm removal of the old connection.

11. **Clear old connection resp.conf.**: (optional) is for the previously visited LMFp to send confirmation information to the home LMFp indicating that the old tunnel-connection has been cleared.

Clear old connection	resp.conf.
Result	M

FEA11	– No action required.

8.5.3 Packet data service session termination

8.5.3.1 Mobile terminal initiated session termination

Either the terminal or the network may decide to terminate an active packet data session. This subclause describes the terminal initiated de-registration information flow procedure. Figure 8.5.3-1 shows the information flow diagram for this procedure. Steps 2-4 may be repeated in order to support multiple data sessions from the same mobile terminal.

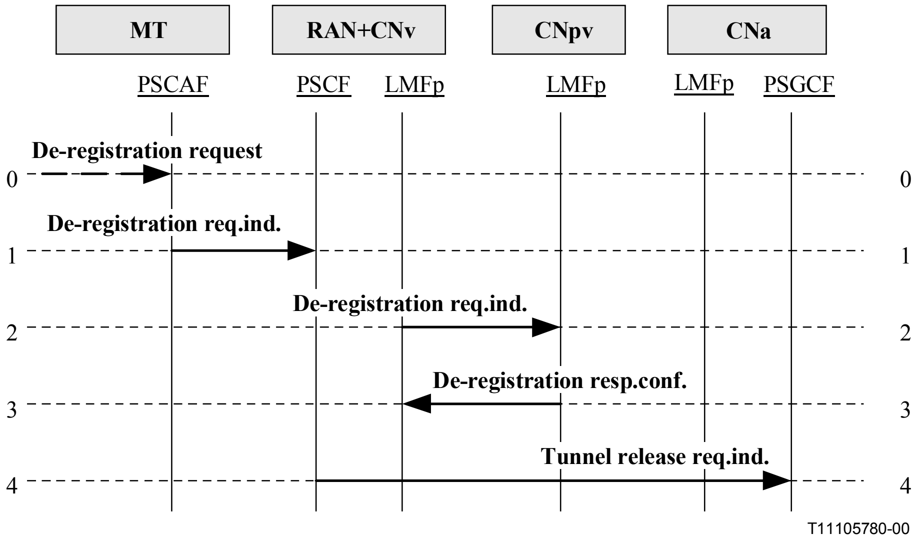


Figure 8.5.3-1/Q.1721 – Terminal initiated packet data session termination

0. **De-registration request**: is to initiate a packet data service de-registration.

FEA0	– Request termination of the active packet data session.

1. **De-registration req.ind.**: is from the mobile terminal to inform the IMT-2000 network of its request to de-register from the active packet data service session.

De-registration (no response expected)	req.ind.
User identification (IMUI or TMUI)	M
IP address (PSGCF – Public)	M
IP address (PSCFv – Public)	M
NAI (PSCFv)	M
IP address (MT)	M
NAI (MT)	M
Data session lifetime	M

FEA1	– The visited LMFp updates its database as appropriate. – The visited LMFp notifies the home LMFp.

2. **De-registration req.ind.**: is from the visited LMFp sending the de-registration req.ind. to the home LMFp to indicate that the terminal is no longer reachable in the visited system.

De-registration (Response: Success/Failure)	req.ind.
IP address (PSGCF – Public)	M
IP address (PSCFv – Public)	M
NAI (PSCFv)	M
IP address (MT)	M
NAI (MT)	M
Data session lifetime	M
Session source address	O (Note)

FEA2	– The home LMFp updates its database as appropriate. – The home LMFp responds to the visited LMFp.
NOTE – In the case of multiple sessions, the PSCFv must associate the resp.conf. signal with the corresponding req.ind. signal using source address information.	

3. **De-registration resp.conf.**: is from the home LMFp acknowledging the request to de-register the terminal.

De-registration	resp.conf.
IP address (MT)	M
NAI (MT)	M
Session source address	O (Note)

FEA3	The visited system initiates tunnel release to the gateway PSCF.
NOTE – In the case of multiple sessions, the PSCFv must associate the resp.conf. signal with the corresponding req.ind. signal using source address information.	

4. **Tunnel release req.ind.**: is from the serving PSCF notifying the anchor PSGCF to release the tunnel to the visited network.

Tunnel release (Response: Neither Success nor Failure)	req.ind.
IP address (PSGCF – Public)	M
IP address (PSCFv – Public)	M
NAI (PSCFv)	M
IP address (MT)	M
NAI (MT)	M
Data session lifetime	M

FEA4	– The PSGCF in the anchor network notifies its local LMFp that it is no longer serving as gateway to the de-registered terminal. – The anchor LMFp updates its database as appropriate.

8.5.3.2 Network initiated session termination

Either the terminal or the network may decide to terminate an active packet data session. This subclause describes the network initiated de-registration information flow procedure. Figure 8.5.3-2 shows the information flow diagram for this procedure. Steps 2-4 may be repeated in order to support multiple data sessions from the same mobile terminal.

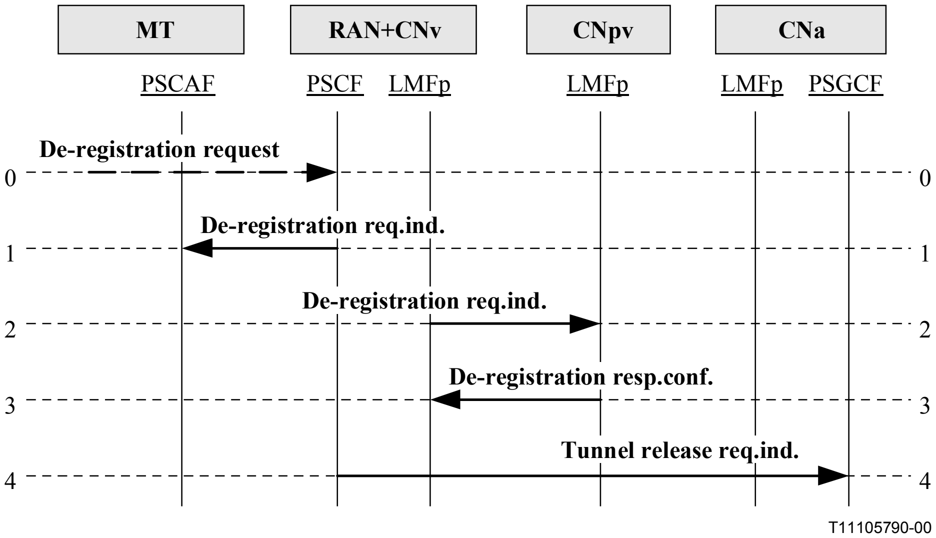


Figure 8.5.3-2/Q.1721 – Network initiated packet data session termination

0. **De-registration request**: the network initiates a packet data service de-registration.

FEA0	– Notify terminal (PSCAF) for de-registration.

1. **De-registration req.ind.**: is to inform the terminal of the network's intent to de-register the terminal from the active packet data service session.

De-registration (Response: Neither Success nor Failure)	req.ind.
User identification (IMUI or TMUI)	M

FEA1	– The terminal prepares to release the access link.

2. **De-registration req.ind.**: sends the de-registration request to the home LMFp to indicate that the terminal is no longer reachable in the visited system.

De-registration (Report Success/Failure)	req.ind.
IP address (PSGCFv – Public)	M
IP address (PSCFv – Public)	M
NAI (PSCFv)	M
IP address (MT)	M
NAI (MT)	M
Data session lifetime	M
Session source address	O (Note)

FEA2	– The home LMFp updates its database as appropriate. – The home LMFp responds to the visited LMFp.
NOTE – For multiple sessions, the PSCFv must associate the response signal with the corresponding req.ind. signal using source address information.	

3. **De-registration resp.conf.**: is for the home LMFp to acknowledge the request to de-register the terminal.

De-registration	resp.conf.
IP address (MT)	M
NAI (MT)	M
Session source address	O (Note)

FEA3	– The visited system initiates tunnel release to the gateway PSCF.
NOTE – For multiple sessions, the PSCFv must associate the response signal with the corresponding request signal using source address information.	

4. **Tunnel release req.ind.**: the serving PSCF notifies the anchor PSGCF to release the tunnel to the visited network.

Tunnel release (no response expected)	req.ind.
IP address (PSGCFv – Public)	M
IP address (PSCFv – Public)	M
NAI (PSCFv)	M
IP address (MT)	M
NAI (MT)	M
Data session lifetime	M

FEA4	– The PSGCF in the anchor network notifies its local LMFp that it is no longer serving as gateway to the de-registered terminal. – The anchor LMFp updates its database as appropriate.

9 Virtual Home Environment

Service invocation in the IMT-2000 system may occur at any time during call processing. It may also occur, either in conjunction with or independent of a call, in relation to mobility management processing, or for authentication processing. Services are offered according to information contained in the subscriber service profile. The subscriber service profile lists subscribed standard basic and supplementary services as well as triggers and associated information (e.g. trigger criteria, associated service logic address, etc.) for VHE-based customized services. Visited IMT-2000 networks are not expected to offer customized services (i.e. customized services offered by home network operators/service providers.) However, the VHE capability and procedures enable the serving network to make these services available to visiting users.

In the VHE concept, service provisioning and network operation may be separated, allowing services to be offered by networks other than those providing the home network's call processing capabilities. In some cases, service logic may be accessed in a separate supporting network. In other cases, the home network provides the service logic and therefore acts as the supporting network.

In the following description (subclauses 9.1 and 9.2), the supporting network is the network where the service logic is located and executed (marked as CNs). The serving or visited network is the network where the user is roaming when the service execution is requested (marked as CNv). The home network (marked as CNh) is where the home Location Management Function (LMFh) and the home Authentication Management Function (AMFh) are located. The CNs and the CNh may be the same network.

Recommendations Q.1701 and Q.1711 identify two VHE realization scenarios for IMT-2000 CS-1. They are the "Direct Home Command" scenario addressed in 9.1 and the "Relay Service Control" scenario addressed in 9.2.

9.1 "Direct Home Command"

In the "Direct Home Command" VHE scenario, the supporting network provides service logic to a visited network serving the roaming subscriber to support that subscriber's VHE-based services. Service logic in the supporting network is invoked via the IN triggering capability of the visited network. Pre-arrangement between the supporting and the visited networks may be needed for screening trigger invocations.

9.1.1 High level "Direct Home Command" service procedure

In an end-to-end IF scheme, this procedure consists of four components: call origination, VHE service logic invocation, call routing, and call connect (in the case of call-related services; similar VHE service procedures apply to call-unrelated scenarios). This subclause addresses the information flows for the VHE service logic invocation part, and treats the information flows for the other three parts as common procedures within the context of the end-to-end information flows.

The following assumptions are made related to VHE service logic invocation information flows:

- In this scenario, pre-arrangement between the supporting and the home networks, or between the supporting and the visited networks, is needed for screening trigger invocations.
- The serving/visited network has IN capability for triggering the required service logic.

Figure 9.1.1-1 presents a high-level overview information flow (IF) diagram for the "Direct Home Command" VHE scenario. The following points should be noted with respect to this figure:

- for call-related services, it includes only the call origination side of the flows from a calling party; similar interaction could occur from a terminating call to a called party;
- other means of initiating service logic not related to calls, such as from mobility management or authentication management, behave in the same way, although the messaging is from a different FE in the "RAN+CNh or v" (see 9.1.3 and 9.1.4);

- the case of a notification to service logic is a subset of Figure 9.1.1-1 (i.e. flow 2 would not be required); and
- the figure is greatly simplified in that it does not illustrate the full range of service logic interaction supported by IN, e.g. it does not reflect an extended interaction with service logic (which may continue until the call is released), user interaction controlled by service logic, etc.

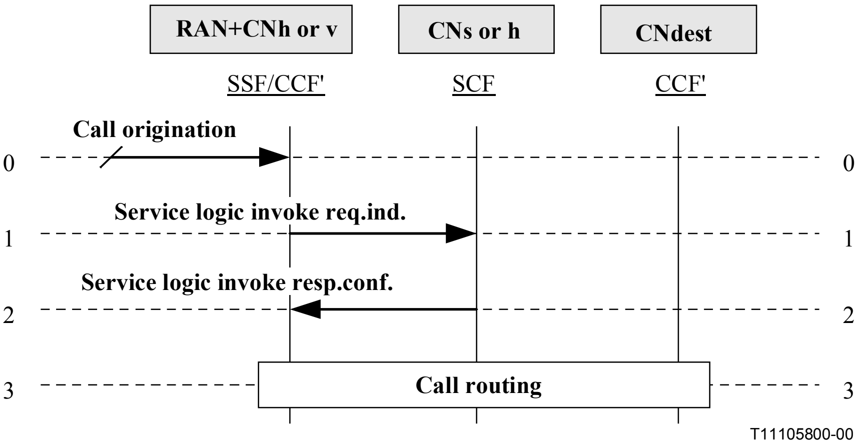


Figure 9.1.1-1/Q.1721 – High-level call related "Direct Home Command"

0. **Call origination**: a subscriber originates a call. The information obtained from the home network at registration will contain information for the serving network to support VHE service invocation[3].

FEA0	– Continue call processing until an armed trigger is encountered at a TDP, and the criteria for the armed trigger are met.

1. **Service logic invoke req.ind.**: is used to invoke service logic at the SCF associated with the trigger whose criteria were met. It conveys information about the subscriber, the state of the call and the trigger condition encountered.

Service logic invoke (Response: Success or Failure)	req.ind.
Information elements in a service logic initiating IF	Per [5]
IMUI	M

FEA1	– Execute service logic.

2. **Service logic invoke resp.conf.**: provides the call processing instruction which service logic wishes the invoking entity to perform.

Service logic invoke	resp.conf.
Information elements in a service logic responding IF	Per [5]

FEA2	– Execute call processing instruction if possible.

[3] This information is included in user profile information obtained during MT registration. This avoids the need to obtain this information as part of call origination.

3. **Call routing**: is employed to continue call processing and to connect the call to the destination network, if that is the appropriate action based on the information in the Service Logic Invoke resp.conf.

Service logic for VHE-based customized services using the "Direct Home Command" is provided by the user's home network or a supporting network (which may be the home network). For the generalized VHE scenario, it is assumed services are provided by a supporting network.

This subclause above provides a high-level simplified end-to-end IF for the "Direct Home Command" (DHC) procedure. The invocation of the VHE-based service triggering capability may occur for two classes of services:

- **Call-related service invocation** occurs during call processing (e.g. call origination, call termination or mid-call). At the FE level, this scenario invokes service logic in the SCF of the supporting network via the triggering capability of the CCF'/SSF in the visited network.
- **Call-unrelated service invocation** occurs for mobility management events[4], or authentication events. At the FE level, this scenario invokes service logic in the SCF of the supporting network by a query from the LMF or a query from the AMF.

9.1.2 "Direct Home Command" – Call related services

This subclause expands upon the "VHE service invocation" component for the NNI and addresses the signalling requirements for the DHC scenario for services invoked by an SSF/CCF' in the visited network. It is assumed that the SSF/CCF' has the capability to trigger the required SCF service logic residing in the supporting network.

Subclause 7.2.2.5/Q.1711 describes an IMT-2000 functional model for interconnections across the NNI between a home network, a supporting network and a visited network. These interconnections are required for invocation of service logic in the supporting network.

Figure 9.1.2-1 presents the DHC scenario of the VHE information flow diagram. The figure is simplified in that it does not illustrate the full range of service logic interaction supported by IN as noted in 9.1.1 above. The "VHE service invocation" procedure may end after the first "Specialized Resource Assist" or it may continue until the call-related service is complete.

This subclause describes triggering in relation to call origination. Triggers may also occur during call termination or mid-call.

[4] Mobility management processing may occur in conjunction with a call or separate from any call event.

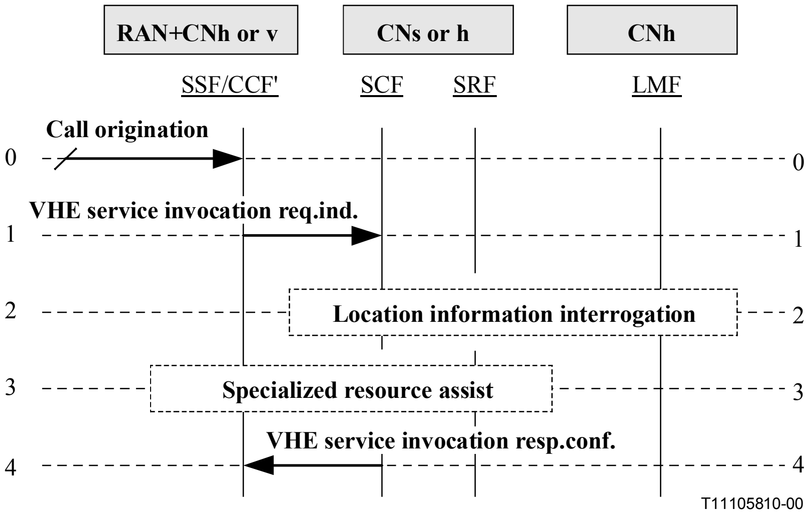

RAN+CNh or v
CNs or h
CNh
SSF/CCF'
SCF
SRF
LMF
Call origination
0
VHE service invocation req.ind.
1
2
Location information interrogation
3
Specialized resource assist
VHE service invocation resp.conf.
4
T11105810-00

Figure 9.1.2-1/Q.1721 – Detailed call related "Direct Home Command"

0. **Call origination**: the calling party originates a call in a visited network. The information obtained from the home network at registration includes triggers and associated criteria and other parameters for visited network support of VHE-based services.

FEA0	– An armed trigger in the SSF/CCF' BCSM is encountered and its criteria are met.

1. **VHE service invocation req.ind.**: is used to invoke the VHE-based service logic of the supporting SCF.

VHE service invocation (Response: Success or Failure)	req.ind.
Information elements in a service logic initiating IF	Per [5]
IMUI	M
MS capability	O (Note 1)
MS Location information	O (Note 2)

FEA1	– Identify the user. – Retrieve user service data from the subscriber VHE service profile (e.g. SDF). – If required, formulate and send a request for MS location and state information to the LMF in the home network.
NOTE 1 – MS capability is included based on trigger criteria. NOTE 2 – MS location information is included if it is available.	

2. **Location information interrogation**: is used to request information on the called user's location if it is required by service logic and it was not included in the first information flow.

3. **Specialized resource assist**: if needed, is initiated by service logic at the SCF to obtain access to the SRF's specialized resources (e.g. play announcement and/or digit collection) in conjunction with the SSF/CCF'. This procedure uses INAP procedures as defined in Recommendation Q.1238.

4. **VHE service invocation resp.conf.**: transfers VHE-based service instructions to the VHE-based service invocation initiating entity.

VHE service invocation	resp.conf.
Information elements in a service logic responding IF	Per [5]

FEA4	– Continue processing the call per the instruction received from the SCF, if possible.

9.1.3 "Direct Home Command" – LMF invoked services

Subclause 7.2.2.5/Q.1711 describes an IMT-2000 functional model for interconnections across the NNI between a home or a visited network and a supporting network. These interconnections are required for invocation of service logic in the supporting network triggered from the LMF.

Figure 9.1.3-1 provides the LMF invoked VHE DHC scenario information flow diagram.

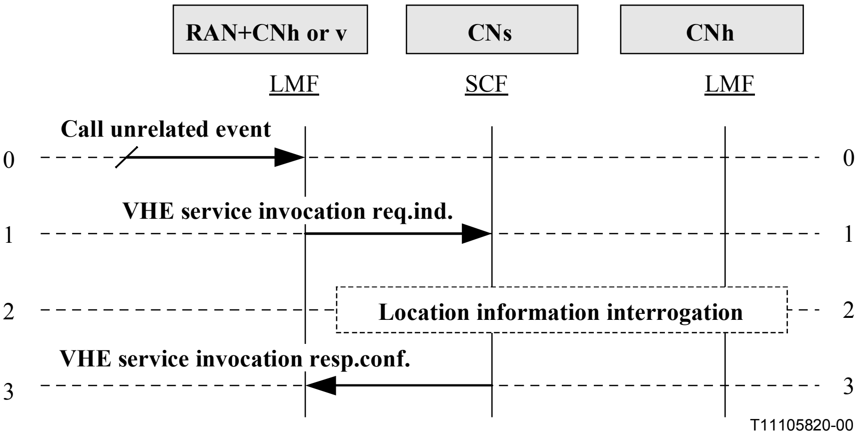

RAN+CNh or v
CNs
CNh
LMF
SCF
LMF
Call unrelated event
VHE service invocation req.ind.
Location information interrogation
VHE service invocation resp.conf.
0
1
2
3
0
1
2
3
T11105820-00

Figure 9.1.3-1/Q.1721 – LMF "Direct Home Command"

0. **Call unrelated event**: the mobility management process utilizes information obtained from the home network at registration. This information includes triggers and associated criteria and other parameters for visited network support of LMF invoked VHE-based services.

FEA0	– An armed trigger is encountered at a TDP in the LMF state model, and the criteria for the armed trigger are met.

1. **VHE service invocation req.ind.**: is used to invoke VHE-based service logic at the supporting SCF.

VHE service invocation (Response: Success or Failure)	req.ind.
Service key	M
Event type	M
IMUI	M
MS capability	O (Note 1)
MS location information	O (Note 2)

FEA1	– Identify user. – Retrieve user data from the subscriber VHE service profile (e.g. SDF). – If required, formulate and send a request for MS location and state information to the LMF in the home network.
NOTE 1 – MS capability is included based on trigger criteria. NOTE 2 – MS location information is included if it is available.	

2. **Location information interrogation**: is used to request information on the called user's location if it is required by service logic and it was not included in the first information flow.

3. **VHE service invocation resp.conf.**: transfers VHE-based service instruction to the VHE-based service invocation initiating entity.

VHE service invocation	resp.conf.
VHE service instruction	M

FEA2	– Continue processing the location registration procedure per the instruction received from the SCF.

9.1.4 "Direct Home Command" – AMF invoked services

Subclause 7.2.2.5/Q.1711 describes an IMT-2000 functional model for interconnections across the NNI between a home or a visited network and a supporting network. These interconnections are required for invocation of the service logic in the supporting network triggered from the AMF.

Figure 9.1.4-1 presents the AMF invoked VHE DHC scenario information flow diagram.

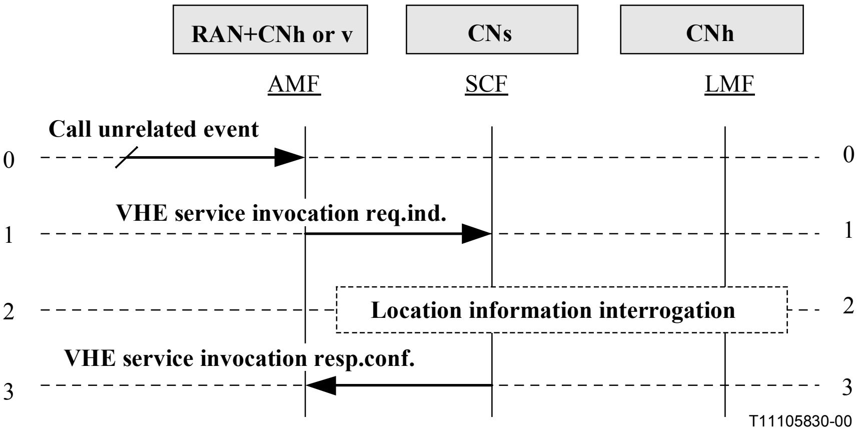

RAN+CNh or v
CNs
CNh
AMF
SCF
LMF
Call unrelated event
VHE service invocation req.ind.
Location information interrogation
VHE service invocation resp.conf.
0
1
2
3
0
1
2
3
T11105830-00

Figure 9.1.4-1/Q.1721 – AMF "Direct Home Command"

0. **Authentication management event**: initiates the authentication management process. The information available includes triggers and associated criteria and other parameters for support of AMF invoked VHE-based services.

FEA0	– An armed trigger is encountered at a TDP in the AMF state model, and the criteria for the armed trigger are met.

1. **VHE service invocation req.ind.**: is used to invoke VHE service logic at the supporting SCF.

VHE service invocation (Response: Success or Failure)	**req.ind.**
IMUI	M
Service key	M
Event type	M
MS location information	O (Note)

FEA1	– Identify user. – Retrieve user data from the subscriber VHE service profile (e.g. SDF). – If required, formulate and send a request for MS location and state information to the LMF in the home network.
NOTE – MS location information is included if it is available.	

2. **Location information interrogation**: is used to request information on the called user's location if it is required by service logic and it was not included in the first information flow.

3. **VHE service invocation resp.conf.**: is used to send VHE service instructions from the SCF in the supporting network to the requesting AMF.

VHE service invocation	**Resp.conf.**
VHE service instruction	M

FEA2	– Continue processing the authentication procedure per the instruction received from the SCF.

9.2 "Relay Service Control"

The VHE "Relay Service Control" (RSC) scenario is the invocation of service logic that resides in the SCF of a supporting (or home) network by the SCF of a serving network (either a home or visited network).

In VHE RSC, service logic is distributed between the supporting network and the visited network to support a roaming subscriber's VHE-based services.

When the serving network is the same as the supporting network, VHE RSC is IN-based service invocation for which well-established procedures exist. When the serving network is not a supporting network, then VHE RSC can apply. For VHE RSC, it is always assumed that the serving and the supporting networks are two different networks interworking through an NNI protocol.

In the serving network, events of interest may be reported by the CCF'/SSF, LMF or AMF to the SCF. The triggers in the invoking FEs may be armed by information from the subscriber's profile or by a concurrent service provisioning process. The invoked SCFv (of the serving network) will query the SCF (of the supporting network) for service control support[5].

[5] Figures 7-7/Q.1711 and 7-8/Q.1711 show the interconnections across the NNI that can be used for this event reporting.

Service logic for VHE-based services using RSC is provided by the user's home network or a supporting network. For the generalized VHE scenario, it is assumed services are provided by a supporting network.

It is assumed that pre-arrangements are made for cooperation and coordination between the serving and supporting networks for VHE RSC. The extent of the cooperation may vary from a partial (shared) to a full relay of service control program[6].

Similar to VHE "Direct Home Command," services for the RSC scenario may be call-related or call unrelated.

9.2.1 "Relay Service Control" service procedure

This procedure calls for the invocation of service logic via the SCFv to the SCFs for service control support. Pre-arrangement between the supporting and the visited networks may consist of the relay of security/screening capabilities, service logic execution program subroutines, or wholly executable programs.

Subclause 7.2.2.5/Q.1711 describes an IMT-2000 functional model for interconnections across the NNI between a home network, a supporting network and a visited network. These interconnections are required for invocation of the service command/logic in the supporting network.

In an end-to-end IF scheme, this procedure consists of four components: initial stimulus, VHE service invocation, VHE handling information and completion of initial procedure. This subclause addresses the information flows for the VHE service logic invocation and VHE handling information parts and treats the information flows for the other three parts as common procedures within the context of the end-to-end information flows.

Figure 9.2.1-1 is the information flow diagram for the VHE "Relay Service Control" scenario. It is assumed that the SSF/CCF', LMF or AMF, upon matching trigger criteria, has the capability to send a message to the required SCF within the serving network, and that the serving SCF has the capability to request assistance from the supporting SCF. The following points should be noted with respect to this figure:

- the case of a notification to service logic is a subset of Figure 9.2.1-1 (i.e. flows 2 and 3 would not be required); and
- the figure is greatly simplified in that it does not illustrate the full range of service logic interaction supported by IN, e.g. it does not reflect an extended interaction with service logic (which may continue until the call is released), user interaction controlled by service logic, etc.

[6] Relay of Security or Screening Capability for Fraud/Abuse control procedures may also be executed by a Service Logic Program (SLP) at an SCF.

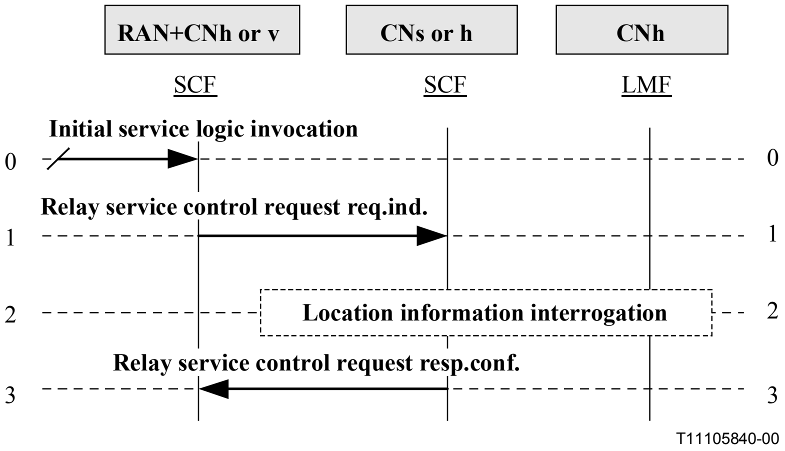

RAN+CNh or v
CNs or h
CNh
SCF
SCF
LMF
Initial service logic invocation
0
0
Relay service control request req.ind.
1
1
2
Location information interrogation
2
Relay service control request resp.conf.
3
3
T11105840-00

Figure 9.2.1-1/Q.1721 – "Relay Service Control" high level

0. **Initial service logic invocation**: invokes service logic at the SCF associated with the trigger whose criteria were met. It conveys information about the subscriber, the state of the call process (invoked from SSF/CCF'), or the state of mobility management (invoked from the LMF) or the state of the authentication process (invoked from AMF) and the trigger condition encountered.

FEA0	– Identify user's supporting network. – Check bilateral agreement for the RSC scheme. – Invoke the SCFs (of the supporting network) for the user's VHE service logic program (SLP).

1. **Relay service control req.ind.**: is used by the controlling SCF to send a request to the supporting SCF, or for requesting the supporting SCF to perform predefined actions.

Relay service control (Response: Success or Failure)	**req.ind.**
Service key	M
Event type	M
IMUI	M
MS Capability	O (Note 1)
MS Location Information	O (Note 2)

FEA1	– Identify User and its Service ID. – Identify requested SLP. – If required, formulate and send a request for MS location and state information to the LMF in the home network. – Check restrictions (using IMUI, MS Location, etc.)
NOTE 1 – MS capability is included based on trigger criteria. NOTE 2 – MT location information is sent if available.	

2. **Location information interrogation**: is used to request information on the called user's location if it is required by service logic and it was not included in the first information flow.

3. **Relay service control resp.conf.**: is used to forward to the controlling SCF the requested information to enable the call to proceed.

Relay service control	req.ind.
Relayed service logic	M

FEA2	– Execute relayed service logic.

10 Messaging services applications

The point-to-point short message service (SMS) provides a means of sending text messages to and from IMT-2000 mobile terminals. The provision of SMS makes use of a message centre (MC), which acts as a store and forward centre for short messages.

Two different point-to-point services have been defined: mobile originated and mobile terminated. Mobile originated messages will be transported from an MT to a message centre. These may be destined for other mobile users, or for subscribers in the fixed network. Mobile terminated messages will be transported from a message centre to an MT. These may be input to the message centre by other mobile users (via a mobile originated short message) or by a variety of other sources, e.g. speech, telex or facsimile.

The point-to-multipoint teleservice message broadcast (TMB) provides a method to manage and deliver teleservice messages for broadcast over the radio interface to IMT-2000 mobile terminals. TMB messages are broadcast to defined geographical areas known as cell broadcast areas. These areas may comprise one or more cells, or may comprise the whole network for a certain service provider. Individual TMB messages will be assigned their own geographical coverage areas by mutual agreement between the information provider and the network operator.

10.1 Short message service (SMS)

10.1.1 SMS notification transfer

The SMS notification procedure is used for alerting the message centre. The procedure starts when the mobile terminal is active (after a short message transfer has failed because the mobile terminal was previously not reachable), or when the mobile terminal has indicated that it now has memory capacity to accept a short message.

10.1.1.1 MT is active

See Figure 10.1.1.1-1.

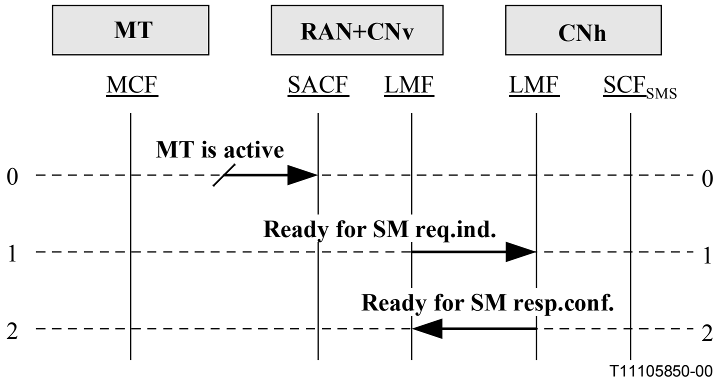


Figure 10.1.1.1-1/Q.1721 – SMS notification transfer (MT is active)

0. **MT is active**: when the MT is active, e.g. the MT made a service request, had a call origination or paging response. Optionally, user authentication may have occurred.

FEA0	– When the MT is present, LMFv will change the relevant database and inform the LMFh.

1. **Ready for SM req.ind.**: informs the LMFh that the MT is ready to accept short messages.

Ready for SM (Response: Success)	req.ind.
IMUI	M
Alert reason	M

FEA1	– Inform the visited network that the SM ready request has been received.

2. **Ready for SM resp.conf.**: acknowledges the receipt of the short message request.

Ready for SM	resp.conf.
User error	O (Note)
Provider error	O (Note)

FEA2	– Concludes the SMS notification transfer.
NOTE – Only required if an error situation has occurred.	

10.1.1.2 Memory capacity available

See Figure 10.1.1.2-1.

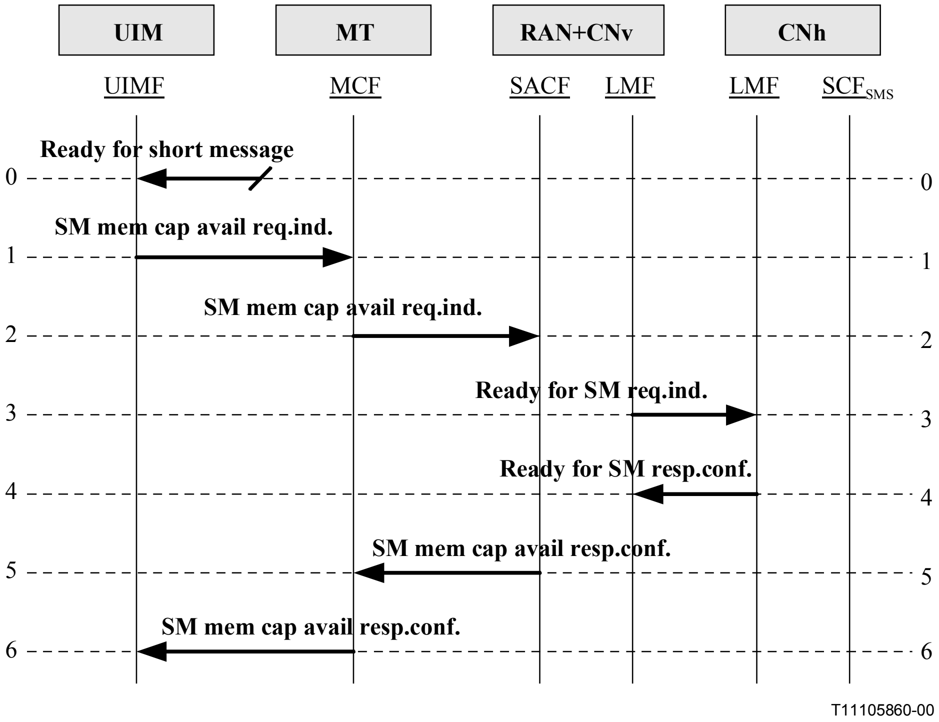


Figure 10.1.1.2-1/Q.1721 – SMS notification transfer (memory capacity available)

0. **Ready for short message**: is the initial stimulus where the mobile terminal has made a service request. Optionally, user authentication may have occurred.

FEA0	– When the UIMF has the possibility to handle short messages and has made available memory capacity, it informs MCF.

1. **SM memory capacity available req.ind.**: informs the MCF in the MT that it has memory available to accept short messages.

SM memory capacity available (Response: Success)	req.ind.
TMUI or IMUI	M (Note)

FEA1	– Relay the request to serving network.
NOTE – TMUI should be used if it is available.	

2. **SM memory capacity available req.ind.**: informs the visited network that the MT is ready to accept short messages.

SM memory capacity available (Response: Success)	req.ind.
TMUI or IMUI	M (Note)

FEA2	– Prepare to inform the home network that the requesting subscriber is ready to accept short messages.
NOTE – TMUI should be used if it is available.	

3. **Ready for SM req.ind.**: informs the LMFh that the MT is ready to accept short messages.

Ready for SM (Response: Success)	req.ind.
IMUI	M
Alert reason	M

FEA3	– Inform the visited network that the SM ready request has been received.

4. **Ready for SM resp.conf.**: acknowledges the receipt of the short message request.

Ready for SM	resp.conf.
User error	O (Note)
Provider error	O (Note)

FEA4	– Relay acknowledgement to MCF.
NOTE – Only required if an error situation has occurred.	

5. **SM memory capacity available resp.conf.**: sends from visited network to confirmed.

SM memory capacity available	resp.conf.
None	(Note)

FEA5	– Relay acknowledgement to UIMF.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

6. **SM memory capacity available resp.conf.**: sends a confirmation to UIMF.

SM memory capacity available	resp.conf.
None	(Note)

FEA6	– No action required.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

10.1.2 Mobile originated short message

The mobile terminal sends the short message to the CCF'/SACF in the visiting network. The CCF'/SACF interrogates the LMFv to retrieve the MS ISDN address and forward the message to the interworking CCF'/SSF node in the destination network. The CCF'/SSF nodes sends the short message to the message centre. An E.164 number in the destination network numbering plan to which the message centre is connected addresses the message centre from the mobile. The E.164 number is stored in the UIM.

10.1.2.1 Mobile originated short message (on a traffic channel)

This procedure is invoked when an IMT-2000 user sends a point-to-point short message and a call is already in progress. See Figure 10.1.2.1-1.

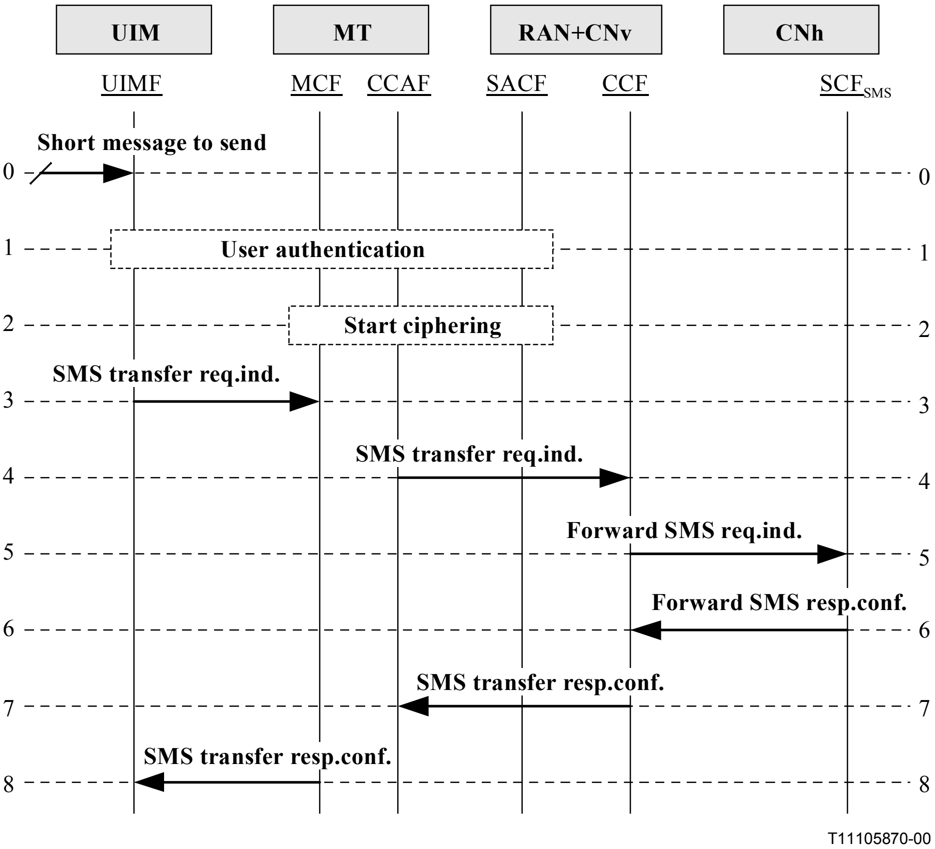


Figure 10.1.2.1-1/Q.1721 – Mobile originated short message (on a traffic channel)

0. **Short message to send**: is the initial stimulus where the subscriber submits a short message to the MT to send to a recipient.

FEA0	– The mobile terminal makes a short message request.

1. **User authentication**: optionally, user authentication procedure may be invoked.

2. **Start ciphering**: optionally, ciphering procedure may be initiated.

3. **SMS transfer req.ind.**: transfer short message to MCF.

SMS transfer (Response: Success)	**req.ind.**
TMUI or IMUI	M (Note)
Called number	M
Message centre address	M
Message	M

FEA3	– Forward the information to the CCAF.
NOTE – TMUI should be used if it is available.	

4. **SMS transfer req.ind.**: is used to send the message to CNv.

SMS transfer (Response: Success)	**req.ind.**
< Same information elements as in information flow 3 >	< See IF 3 >

FEA4	– Forward the information to the short message centre in the CNh.

5. **Forward SMS req.ind.**: transfer the message to short message centre in CNh.

Forward SMS (Response: Success)	**req.ind.**
< Same information elements as in information flow 3 >	< See IF 3 >

FEA5	– Formulates a delivery report to send back to the CNv.

6. **Forward SMS resp.conf.**: acknowledgement received to the message.

Forward SMS	**resp.conf.**
None	(Note)

FEA6	– Forwards the delivery report to the CCAF.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

7. **SMS transfer resp.conf.**: acknowledgement received to the message.

SMS transfer	**resp.conf.**
None	(Note)

FEA7	– Forwards the delivery report to the MCF.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

8. **SMS transfer resp.conf.**: acknowledgement received to the message.

SMS transfer	resp.conf.
None	(Note)

FEA8	– Informs the subscriber whether or not the message was successfully delivered.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

10.1.2.2 Mobile originated short message (on a control channel)

See Figure 10.1.2.2-1.

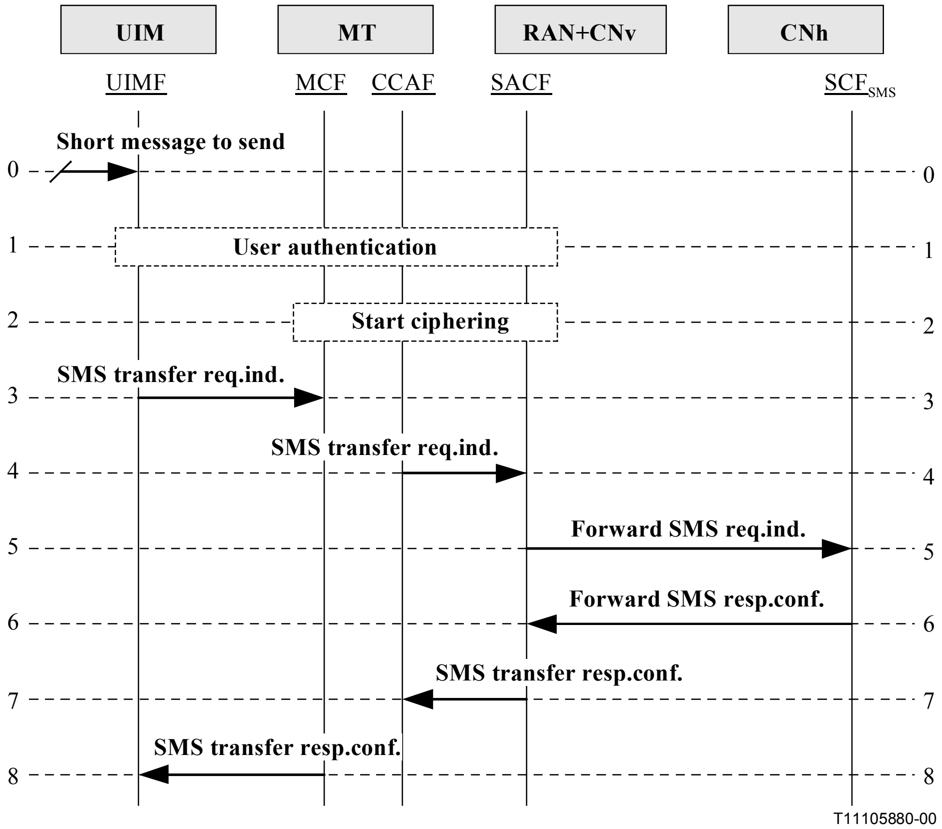


Figure 10.1.2.2-1/Q.1721 – Mobile originated short message (on a control channel)

0. **Short message to send**: is the initial stimulus where the subscriber submits a short message to the MT to send to a recipient.

FEA0	– The mobile terminal makes a short message request.

1. **User authentication**: optionally, the User authentication procedure may be invoked.

2. **Start ciphering**: optionally, the ciphering procedure may be initiated.

3. **SMS transfer req.ind.**: transfers a short message to the MCF.

SMS transfer (Response: Success)	req.ind.
TMUI or IMUI	M (Note)
Called number	M
Message centre address	M
Message	M

FEA3	– Forwards the information to the CCAF.
NOTE – TMUI should be used if it is available.	

4. **SMS transfer req.ind.**: is used to send the message to the CNv.

SMS transfer (Response: Success)	req.ind.
< Same information elements as in information flow 3 >	< See IF 3 >

FEA4	– Forwards the information to the short message centre in the CNh.

5. **Forward SMS req.ind.**: transfers the message to SCF in CNh.

Forward SMS (Response: Success)	req.ind.
< Same information elements as in information flow 3 >	< See IF 3 >

FEA5	– Formulates a delivery report to send back to the CNv.

6. **Forward SMS resp.conf.**: acknowledges receipt of the message.

Forward SMS	resp.conf.
None	(Note)

FEA6	– Forwards the delivery report to the CCAF.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

7. **SMS transfer resp.conf.**: acknowledgement received to the message.

SMS transfer	resp.conf.
None	(Note)

FEA7	– Forwards the delivery report to the MCF.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

8. **SMS transfer resp.conf.**: acknowledgement received to the message.

SMS transfer	resp.conf.
None	(Note)

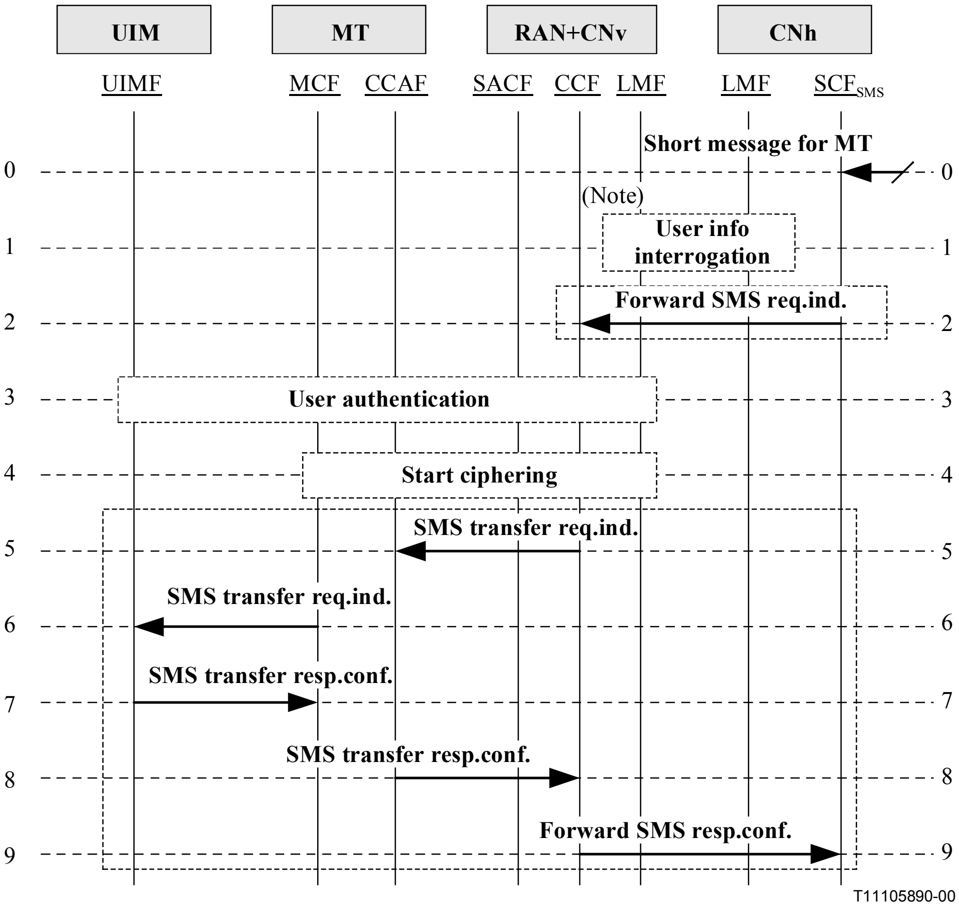
FEA8	– Informs the subscriber whether or not the message was successfully delivered.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

10.1.3 Mobile terminated short message

The message centre sends the short message to the CCF'/SACF in the subscriber's home network. The CCF'/SACF interrogates the LMFh to retrieve routing information necessary to forward the short message, and then sends the message to the relevant CCF'/SACF in the visiting network, transiting other networks if necessary. The CCF'/SACF then sends the short message to the MT.

10.1.3.1 Mobile terminated short message on a traffic channel

See Figure 10.1.3.1-1.



NOTE – The SCF$_{SMS}$ may optionally query the LMFh for location information if the mobile is known to be reachable and has available memory capacity. "User info interrogation" being optional leads to the subsequent information flows being optional.

Figure 10.1.3.1-1/Q.1721 – Mobile terminated short message (on a traffic channel)

0. **Short message for MT**: a short message is submitted at the subscriber's home system message centre for delivery to the subscriber's MT.

FEA0	– Initiate the user info interrogations procedure to obtain information needed to deliver the message.

1. **User information interrogation**: the LMFh queries the LMFv for the current location and state of the subscriber to whom the short message is destined. The LMFv determines the current location and state of the MT and responds to the LMFh with this information.

2. **Forward SMS req.ind.**: transfers the short message to CCF identified in step 1.

Forward SMS (Response: Success)	req.ind.
IMUI	M
Calling number	M
Message centre address	M
Message	M

FEA2	– Transfers the message to the CCAF in the MT.

3. **User authentication**: optionally, the User authentication procedure may be invoked.

4. **Start ciphering**: optionally, the Ciphering procedure may be initiated.

5. **SMS transfer req.ind.**: transfers the message to the mobile terminal.

SMS transfer (Response: Success)	req.ind.
< Same information elements as in information flow 2 >	< See IF 2 >

FEA5	– Forwards the information to the MCF.

6. **SMS transfer req.ind.**: transfers the message to UIM.

SMS transfer (Response: Success)	req.ind.
< Same information elements as in information flow 2 >	< See IF 2 >

FEA6	– Displays the short message to the user or notifies user of SM. – Initiates a delivery report to send back to the CNh.

7. **SMS transfer resp.conf.**: acknowledges receipt of the message.

SMS transfer	resp.conf.
None	(Note)

FEA7	– Forwards the acknowledgement to the CCAF.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

8. **SMS transfer resp.conf.**: acknowledgement received to the message.

SMS transfer	resp.conf.
None	(Note)

FEA8	– Transfers the acknowledgement to the SCF in the CNh.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

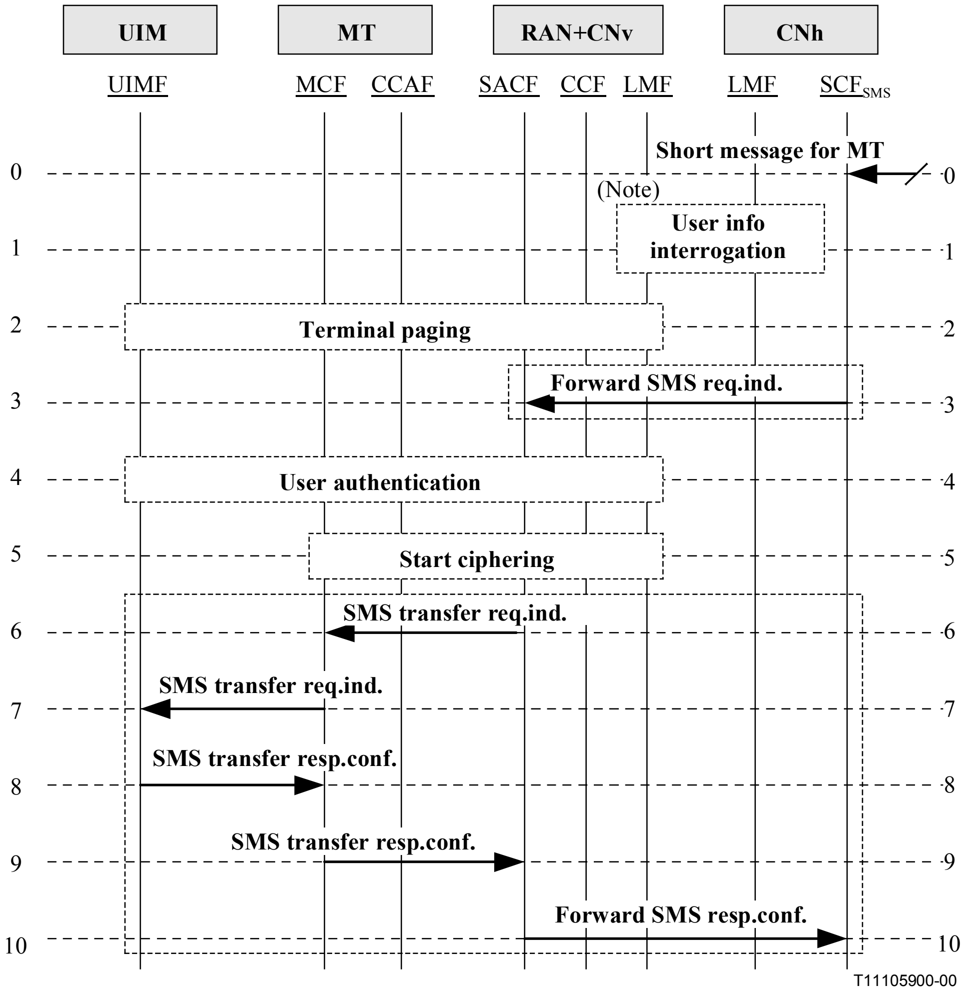
9. **Forward SMS resp.conf.**: acknowledges receipt of the message.

Forward SMS	resp.conf.
None	(Note)

FEA9	– Marks the message as successfully delivered.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

10.1.3.2 Mobile terminated short message on a control channel

See Figure 10.1.3.2-1.



NOTE – The SCF$_{SMS}$ may optionally query the LMFh for location information if the mobile is known to be reachable and has available memory capacity. "User info interrogation" being optional leads to the subsequent information flows being optional.

Figure 10.1.3.2-1/Q.1721 – Mobile terminated short message (on a control channel)

0. **Short message for MT**: a short message is submitted at the subscriber's home system message centre for delivery to the subscriber's MT.

FEA0	– Initiate the user info interrogations procedure to obtain information needed to deliver the message.

1. **User information interrogation**: the LMFh queries the LMFv for the current location and state of the subscriber to whom the short message is destined. The LMFv determines the current location and state of the MT and responds to the LMFh with this information.

2. **Terminal paging**: optionally, paging procedure may be done to further pinpoint the location of the mobile terminal.

3. **Forward SMS req.ind.**: transfers the short message to the SACF in the CNv.

Forward SMS (Response: Success)	req.ind.
IMUI	M
Calling number	M
Message centre address	M
Message	M

FEA3	– Transfers the message to the MCF in the MT.

4. **User authentication**: optionally, the User authentication procedure may be invoked.

5. **Start ciphering**: optionally, the Ciphering procedure may be initiated.

6. **SMS transfer req.ind.**: transfer the message to the mobile terminal.

SMS transfer (Response: Success)	req.ind.
< Same information elements as in information flow 3 >	< See IF 3 >

FEA6	– Transfers the message to the UIMF.

7. **SMS transfer req.ind.**: transfers the message to UIM.

SMS transfer (Response: Success)	req.ind.
< Same information elements as in information flow 3 >	< See IF 3 >

FEA7	– Displays the short message to the user or notifies user of SM. – Initiates a delivery report to send back to the CNh.

8. **SMS transfer resp.conf.**: acknowledges receipt of the message.

SMS transfer	resp.conf.
None	(Note)

FEA8	– Forwards the acknowledgement to the SACF.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

9. **SMS transfer resp.conf.**: acknowledges receipt of the message.

SMS transfer	resp.conf.
None	(Note)

FEA9	– Transfers the acknowledgement to the SCF in the CNh.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

10. **Forward SMS resp.conf.**: acknowledges receipt of the message.

Forward SMS	**resp.conf**.
None	(Note)

FEA10	– Marks the message as successfully delivered.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

10.2 Teleservice message broadcast (TMB)

This subclause provides information flows for Teleservice Message Broadcast (TMB) which provides a method to manage and deliver teleservice text messages for broadcast over the radio interface to IMT-2000 mobile terminals. Examples of areas where teleservice text messages can be used are pertaining to emergencies, administrative announcements, advertisements, subscribed-to services, etc. The broadcast may be done over a prescribed zone (i.e. over a whole or partial SACF in a CN). The broadcast may be done under home-system based periodicity control or under visited-system based periodicity control. Other attributes such as broadcast language, priority, etc., also characterize the broadcast. Teleservice message broadcasts are unacknowledged (i.e. the mobile is not expected to respond when it receives a broadcast message).

TMB happens periodically in the following ways:

NOTE – The **periodicity** consists of a **start time**, a **repetition rate** and a **duration**.

Option A: Visited-System Based Periodicity Control – The periodicity of the broadcast of teleservice messages is under the control of the visited system. The teleservice message to be broadcast is deposited by a "client" at the message centre (the SCF_{SMS} in the home system) which then transfers it to one or more CNvs. The SACFs in the CNvs then store and begin the broadcast of the message at regular intervals and for the prescribed duration, in accordance with the periodicity that is specified. The SACFs in the CNvs store the message until the completion of the broadcast (i.e. until the end of the broadcast period). The SACFs may prematurely curtail broadcasting the message when and if directed by the SCF_{SMS}.

Option B: Home-System Based Periodicity Control – The periodicity of the broadcast of teleservice messages is under the control of the home system. The teleservice message to be broadcast is deposited by a "client" at the message centre (the SCF in the home system) which then transfers it to one or more CNvs. The SACFs in the CNvs then immediately broadcast the message. Here, the SACFs do not need to store the message. However, if the client had desired rebroadcast at regular intervals and for some duration, the home (SCF_{SMS}) can re-send the message to the CNvs for rebroadcast. In this scenario, the SCF_{SMS} in the CNh has the responsibility of retaining the message until the completion of the broadcast (i.e. until the end of the broadcast period).

Both options are illustrated in the Figure 10.2-1.

Also, the SCF sends the teleservice message broadcast payload and associated IEs to all the SACFs in the CNvs that are part of the prescribed broadcast zone. However, for simplicity only one SACF is shown in the Figure 10.2-1.

Typically, Option A is used for high repetition rate broadcasts (e.g. every two minutes,) over a short duration (e.g. for three hours).

Typically, Option B is used for low repetition rate broadcasts (e.g. every six hours) over a long duration (e.g. for seven days).

It is an operator's decision: Option A tends to utilize greater system resources (memory) while Option B tends to utilize greater signalling link resources (higher occupancy).

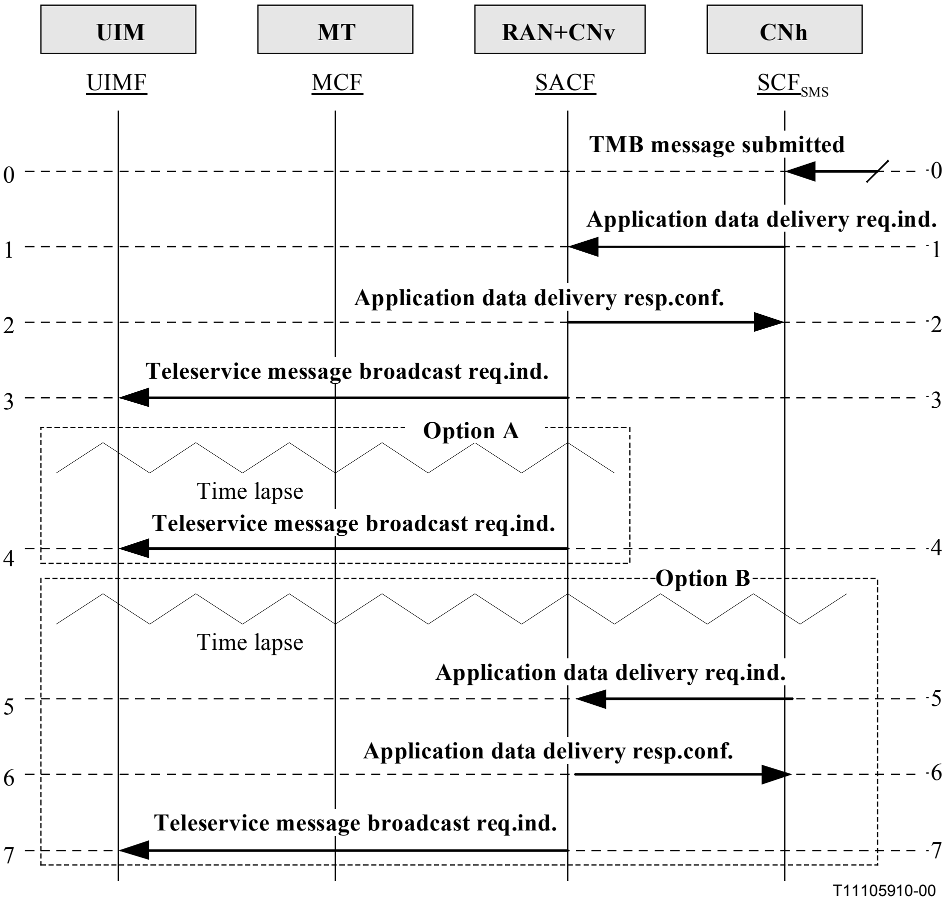

UIM
MT
RAN+CNv
CNh
UIMF
MCF
SACF
SCF_{SMS}
TMB message submitted
Application data delivery req.ind.
Application data delivery resp.conf.
Teleservice message broadcast req.ind.
Option A
Time lapse
Teleservice message broadcast req.ind.
Option B
Time lapse
Application data delivery req.ind.
Application data delivery resp.conf.
Teleservice message broadcast req.ind.
0
1
2
3
4
5
6
7
T11105910-00

Figure 10.2-1/Q.1721 – Teleservice message broadcast

0. **TMB message submitted**: this is the initial stimulus where a "client" submits a message to be broadcast using teleservice message broadcast. The request includes the actual broadcast payload, the originator's address, the broadcast category, broadcast message type, broadcast message status, broadcast message priority, broadcast periodicity, broadcast service group, broadcast zone identifier and the preferred language for broadcast.

FEA0	– Initiates Option A (Visited-System Based Periodicity Control) or Option B (Home-System Periodicity Control) in accordance with the TMB requests.

1. **Application data delivery req.ind.**: is from the SCF in the home network to all the SACFs which control the prescribed broadcast zone.

Application data delivery (Response: Success)	req.ind.
Originator address	M
Payload	M
Category	M
Message type	M
Message status	M
Zone identifier	O (Note 1)

Application data delivery (Response: Success)	req.ind.
Periodicity	O (Note 2)
Message priority	O (Note 3)
Service group	O (Note 4)
Preferred language	O (Note 5)

FEA1	– Acknowledge the application data delivery request. – Initiates to send teleservice message broadcast in the visiting network.
NOTE 1 – Include to specify broadcast zones. Absence of IE means broadcast over whole SACF. NOTE 2 – Include for Visited-System Based Periodicity control if absent, send the message once only. NOTE 3 – Include to indicate normal (default), interactive, urgent or emergency broadcast. NOTE 4 – Include to indicate target MT audience (operator defined). NOTE 5 – Include to indicate the language that the message is written in. Used for filtering.	

2. **Application data delivery resp.conf.**: acknowledges receipt of the application data delivery requests.

Application data delivery	resp.conf.
None	(Note)

FEA2	– No action required if Option A is selected. – Wait for timer expiry if Option B is selected.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

3. **Teleservice message broadcast req.ind.**: passes the message to UIMF.

Teleservice message broadcast (Response: None)	req.ind.
Originator address	M
Payload	M
Category	M
Message type	M
Message status	M
Message priority	O (Note 1)
Service group	O (Note 2)
Preferred language	O (Note 3)

FEA3	– Display the message to the user in accordance with the parameters as received.
NOTE 1 – Include to indicate normal (default), interactive, urgent or emergency broadcast. NOTE 2 – Include to indicate target MT audience (operator defined). NOTE 3 – Include to indicate the language that the message is written in. Used for filtering.	

Step 4 is a repeat of information flow 3, and applies only in the case of Option A, where the visited system controls the periodicity. The IEs and the FEA are the same as in information flow 3. This step is repeated in accordance with the prescribed periodicity.

Steps 5, 6 and 7 are the same as information flows 1, 2 and 3 except the Periodicity is not included in information flow 5. They apply only in the case of Option B where the home system controls the periodicity. These steps are repeated in accordance with the prescribed periodicity.

10.3 Message waiting notification (MWN)

10.3.1 MWN information flows

This scenario shows the information flow related to message waiting notification (MWN) for IMT-2000 systems in a global roaming situation. Message waiting notification is a feature whereby enrolled subscribers are notified when pending voice, fax, e-mail and other types of messages have been deposited in their messaging systems and are available for retrieval. See Figure 10.3.1-1.

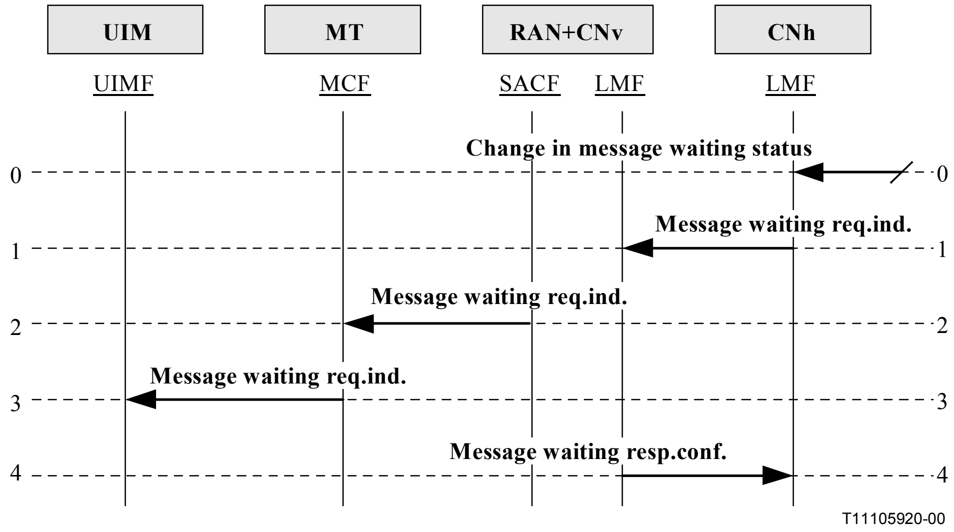


Figure 10.3.1-1/Q.1721 – Message waiting notification

0. **Change in message waiting status**: this is the initial stimulus where a messaging system, fax or e-mail server or similar entity reports a change in the MT's voice, fax, e-mail or other message status to the LMFh.

FEA0	– Change the message waiting status.

1. **Message waiting req.ind.**: for each type of message (voice, fax, e-mail, etc.) a separate req.ind. may be sent. Alternatively, using constructor parameters, information on more than one type of message may be bundled and sent in one req.ind. This scenario illustrates the former mechanism.

Message waiting (Response: Success)	req.ind.
IMUI	M
Message waiting indicator	M (Note 1)
Message waiting type	O (Note 2)
Message priority	O (Note 3)
Messages pending count	O (Note 4)
Preferred language	O (Note 5)

FEA1	– Relay the contents to the SACF so that they can be sent to the MCF.
NOTE 1 – Can have two values "Yes" or "No". NOTE 2 – Indicates whether the messages are voice, fax, e-mail or other. NOTE 3 – Include to indicate normal (default), interactive, urgent or emergency broadcast. NOTE 4 – Indicates the number of pending messages. NOTE 5 – Indicates the language to be used if a notification announcement is made.	

2. **Message waiting req.ind.**: transfers information about the messages waiting to the MCF.

Message waiting (Response: Success)	req.ind.
< Same information elements as in information flow 1 >	< See IF 1 >

FEA2	– Relay the contents to the UIMF.

3. **Message waiting req.ind.**: transfers the message waiting notification to UIMF.

Message waiting notification (Response: Success)	req.ind.
< Same information elements as in information flow 1 >	< See IF 1 >

FEA3	– Use the received information to provide the specified type of notification to the user.

4. **Message waiting resp.conf.**: acknowledgement for message waiting notification.

Message waiting notification	resp.conf.
None	(Note)

FEA6	– No action is required.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

11 Supplementary service procedures

The following features may not be applicable to all IMT-2000 family members.

These stand-alone procedures are used to control the supplementary services (SS) of a user. They are initiated by the user[7], normally by pressing keys on the mobile terminal.

The following supplementary service procedures are described:

- Get password.
- Register password.
- Register SS.
- Erase SS.

[7] The "get password" and "unstructured supplementary service notify" procedures are initiated by the HLR (LMFh), but they are triggered by other supplementary service control procedures previously initiated by the user.

- Activate SS.
- Deactivate SS.
- Interrogate SS.
- Invoke SS.
- Process unstructured SS request.
- Unstructured SS request.
- Unstructured SS notify.
- SS invocation notification.

11.1 Get password

This procedure is initiated by the home network to request a password from the user, when the home network receives a request from the user for a supplementary service control operation that requires a password. This procedure can be used in combination with any of the other supplementary service control procedures, but it will not be shown explicitly in all of them. See Figure 11.1-1.

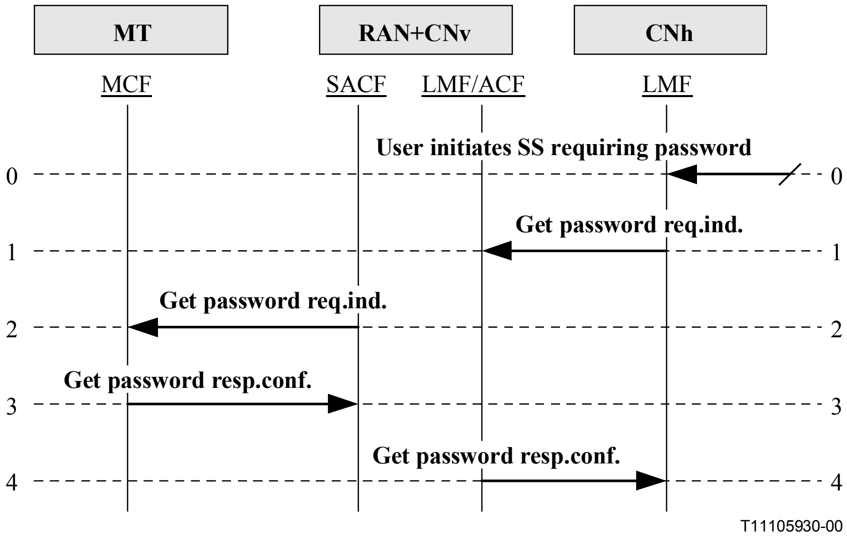


Figure 11.1-1/Q.1721 – Get password

0. **User initiates SS requiring password**: the LMFh receives a user initiated SS requiring password.

FEA0	– Detect the need to request a password from the user in response to an initiated SS procedure. – Prepare and send a Get password req.ind. to LMF in the visiting network.

1. **Get password req.ind.**: is used to request the user to provide a password.

Get password (Response: Success or Failure)	req.ind.
Guidance information	M

FEA1	– Relay the Get password req.ind. to SACF.

2. **Get password req.ind.**: is used to request the user to provide a password via the MMI.

Get password (Response: Success or Failure)	req.ind.
Guidance information	M

FEA2	– Interpret the guidance information element and display the relevant information to the user via the MMI. – Receive the password from the user via the MMI. – Prepare and send a Get Password resp.conf. to SACF, possibly using multiple messages, e.g. for DTMF emulation.

3. **Get password resp.conf.**: send the current password and result to the SACF.

Get password	resp.conf.
Current password	M
Result	M

FEA3	– Relay the Get password resp.conf. to LMFv. – Prepare and send a Get password resp.conf. to the LMFh, possibly using multiple messages, e.g. for DTMF emulation.

4. **Get password resp.conf.**: send the current password and result to the LMFh.

Get password	resp.conf.
Current password	M
Result	M

FEA4	– Confirmed password reviewed.

11.2 Register password

This procedure is initiated by the home network to request the old password from the user. When the home network receives the old password, a request will be sent to the user to request the new password. The home network will request one additional time the user to confirm the new password. See Figure 11.2-1

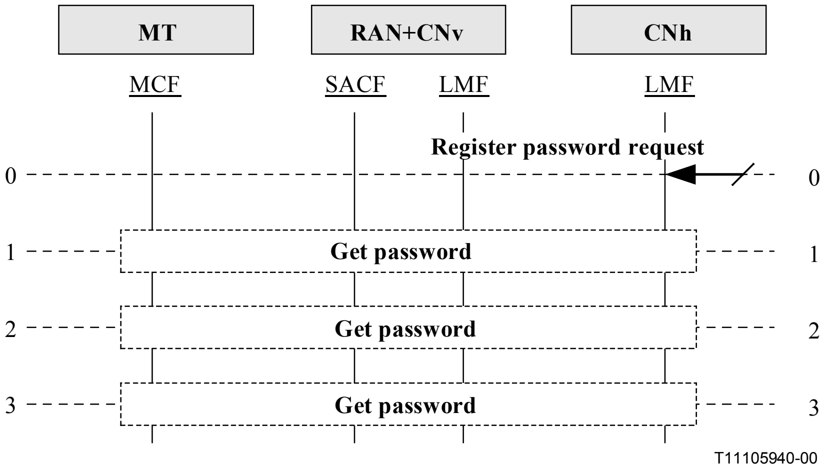


Figure 11.2-1/Q.1721 – Register password

0. **Register password request**: the user requests to change the password for a supplementary service.

1. **Get password**: the LMFh requests the old password from the user.

2. **Get password**: the LMFh requests the user to give the new password.

3. **Get password**: the LMFh requests the user to give the new password one more time for confirmation.

11.3 Register SS

This procedure is used to register data related to a supplementary service in the home network. See Figure 11.3-1.

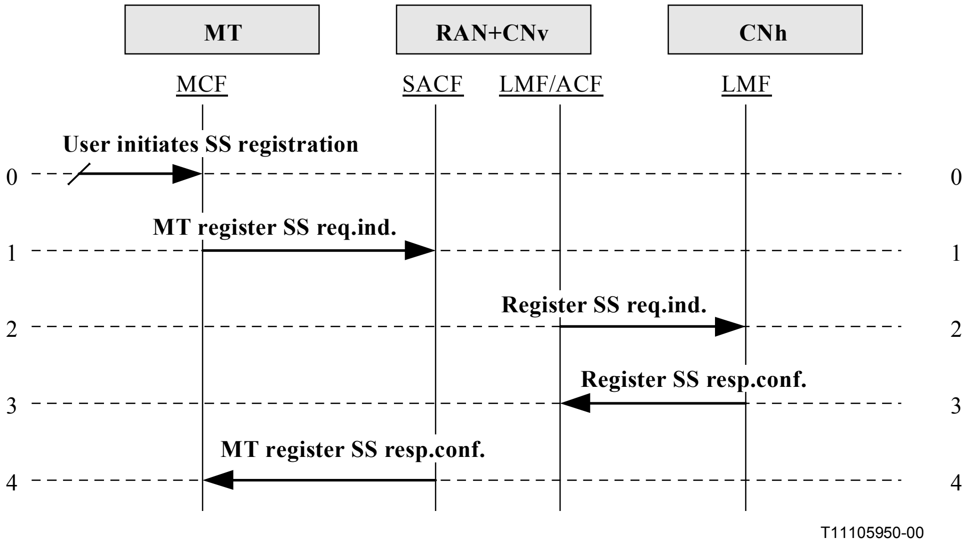


Figure 11.3-1/Q.1721 – Register SS

0. **User initiates SS registration**: the MCF receives a user initiated SS registration.

FEA0	– Detect user initiated SS control procedure via the MMI to request a registration of a supplementary service. – Prepare and send the received information to SACF.

1. **MT register SS req.ind.**: is used to request to register a supplementary service.

MT register SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	M

FEA1	– Prepare and send Register SS req.ind. to LMFv.

2. **Register SS req.ind.**: is used to request the LMFh to register a supplementary service.

Register SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	M

FEA2	– Identify the concerned supplementary service. – Store the received SS data according to the command. – Prepare and send a Register SS resp.conf. to LMFv.

3. **Register SS resp.conf.**: is used to send a response back to the user to inform about the result of the registration.

Register SS (Response: Success or Failure)	resp.conf.
Result	M

FEA3	– Relay the information to SACF. – Prepare and send an MT register SS resp.conf. from SACF.

4. **MT register SS resp.conf.**: sends the result of the registration of supplementary service to the user.

MT register SS	resp.conf.
Result	M

FEA4	– Acknowledge to the user that the related data for the supplementary service has been stored in LMFh.

11.4 Erase SS

This procedure is initiated by the user to delete information stored against a particular service by a previous registration in the home network. See Figure 11.4-1.

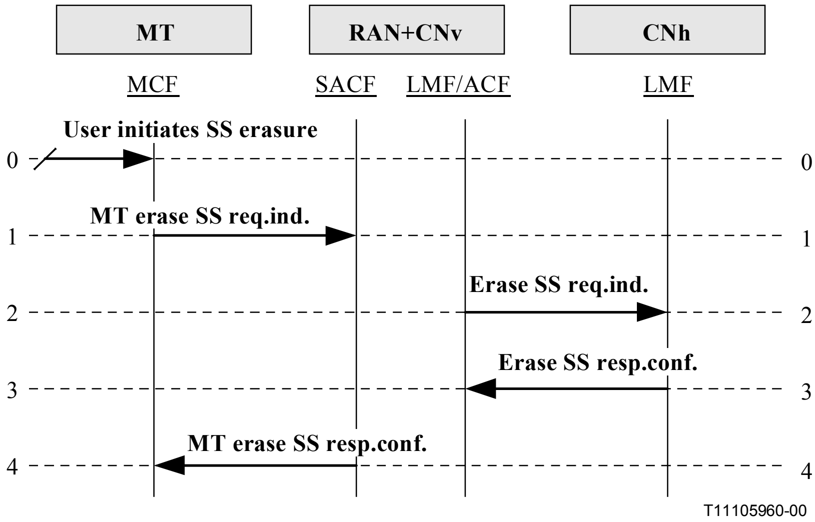


Figure 11.4-1/Q.1721 – Erasure of SS

0. **User initiates SS erasure**: the MCF receives a user initiated SS Erasure.

FEA0	– Detect user initiated SS control procedure via the MMI to request an erasure of a supplementary service. – Prepare and send the received information to SACF.

1. **MT erase SS req.ind.**: is used to request to erase a supplementary service.

MT erase SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	O (Note)

FEA1	– Request to erase SS data.
NOTE – Only requested for such supplementary services which have data.	

2. **Erase SS req.ind.**: is used to request the LMFh to erase a supplementary service.

Erase SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	O (Note)

FEA2	– Identify the concerned supplementary service. – Erase SS data according to the command.
NOTE – Only requested for such supplementary services which have data.	

3. **Erase SS resp.conf.**: is used to send a response back to the user to inform about the result of the erasure.

Erase SS (Response: Success or Failure)	resp.conf.
Result	M

FEA3	– Relay the information to SACF.

4. **MT erase SS resp.conf.**: sends the result of the erasure of supplementary service to the user.

MT Erase SS	resp.conf.
Result	M

FEA4	– No action required.

11.5 Activate SS

This procedure is used to enable a process to run as and when required by the service concerned, resulting in the active phase. Some services can be either "operative" or "quiesent" (not operative) during the active phase according to whether or not the system would be able to invoke or use the service. The information is stored in the home network and for some relevant services is stored in the serving network as well. See Figure 11.5-1.

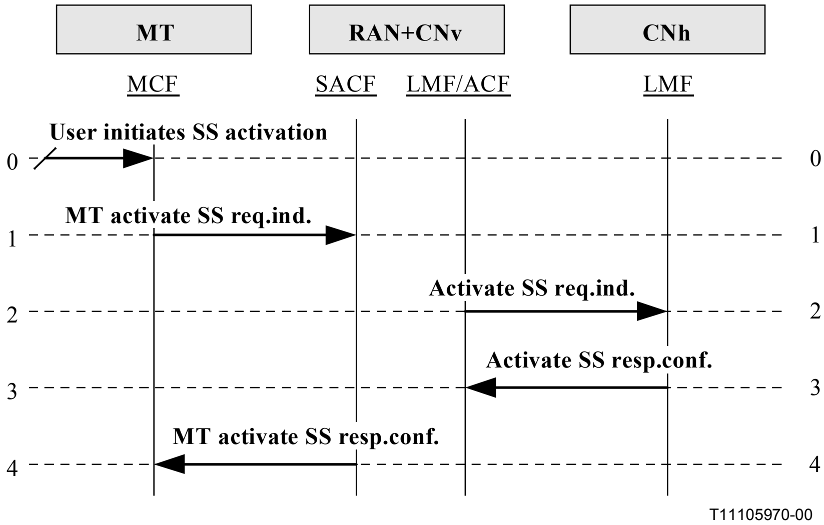


Figure 11.5-1/Q.1721 – Activation of SS

0. **User initiates SS activation**: the MCF receives a user initiated SS Activation.

FEA0	– Detect user initiated SS control procedure via the MMI to request an activation of a supplementary service. – Prepare and send the received information to SACF.

1. **MT activate SS req.ind.**: is used to request to activate a supplementary service.

MT activate SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	O (Note)

FEA1	Request to activate SS.
NOTE – Only requested for such supplementary services which have data.	

2. **Activate SS req.ind.**: is used to request the LMFh to activate a supplementary service.

Activate SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	O (Note)

FEA2	– Identify the concerned supplementary service. – Activate SS data according to the command.
NOTE – Only request for such supplementary services which have data.	

3. **Activate SS resp.conf.**: is used to send a response back to the user to inform about the result of the activation.

Activate SS (Response: Success or Failure)	resp.conf.
Result	M

FEA3	– Relay the information to SACF.

4. **MT activate SS resp.conf.**: sends the result of the activation of supplementary service to the user.

MT activate SS	resp.conf.
Result	M

FEA4	– No action required.

11.6 Deactivate SS

This procedure is initiated by the user, to terminate the process started at the activation. The information will be stored in the home network and for some relevant services it will be stored in the serving network as well. See Figure 11.6-1.

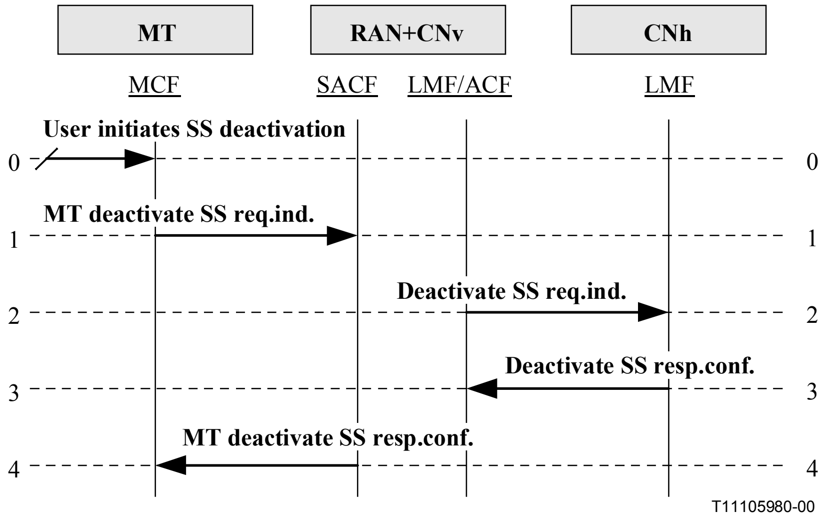


Figure 11.6-1/Q.1721 – Deactivation of SS

0. **User initiates SS deactivation**: the MCF receives a user initiated SS deactivation.

FEA0	– Detect user initiated SS control procedure via the MMI to request a deactivation of a supplementary service. – Prepare and send the received information to SACF.

1. **MT deactivate SS req.ind.**: is used to request to deactivate a supplementary service.

MT deactivate SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	O (Note)

FEA1	Request to deactivate SS.
NOTE – Only requested for such supplementary services which have data.	

2. **Deactivate SS req.ind.**: is used to request the LMFh to deactivate a supplementary service.

Deactivate SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	O (Note)

FEA2	– Identify the concerned supplementary service. – Deactivate SS data according to the command.
NOTE – Only requested for such supplementary services which have data.	

3. **Deactivate SS resp.conf.**: is used to send a response back to the user to inform about the result of the deactivation.

Deactivate SS (Response: Success or Failure)	resp.conf.
Result	M

FEA3	– Relay the information to SACF.

4. **MT deactivate SS resp.conf.**: sends the result of the deactivation of supplementary service to the user.

MT deactivate SS	resp.conf.
Result	M

FEA4	– No action required.

11.7 Interrogate SS

This procedure is initiated by the user to provide information about a specific supplementary service. The information is fetched from the home network. See Figure 11.7-1.

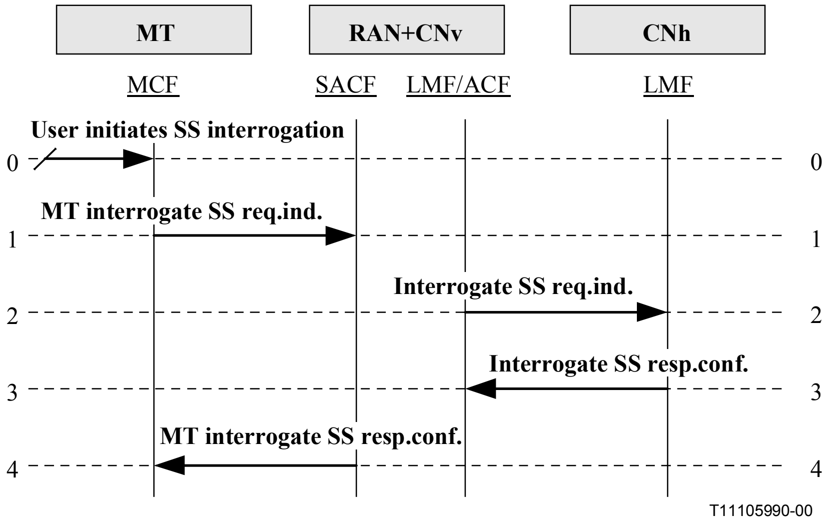

MT
RAN+CNv
CNh
MCF
SACF
LMF/ACF
LMF
User initiates SS interrogation
MT interrogate SS req.ind.
Interrogate SS req.ind.
Interrogate SS resp.conf.
MT interrogate SS resp.conf.
0
1
2
3
4
0
1
2
3
4
T11105990-00

Figure 11.7-1/Q.1721 – Interrogation of SS

0. **User initiates SS interrogation**: the MCF receives a user initiated SS interrogation.

FEA0	– Detect user initiated SS control procedure via the MMI to request an interrogation of a supplementary service. – Prepare and send the received information to SACF.

1. **MT interrogate SS req.ind.**: is used to request to retrieve information related to a supplementary service.

MT interrogate SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	O (Note)

FEA1	– Request to interrogate SS data.
NOTE – Only requested for such supplementary services which have data.	

2. **Interrogate SS req.ind.**: is used to request the LMFh if necessary to retrieve information related to a supplementary service.

Interrogate SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	O (Note)

FEA2	– Identify the concerned supplementary service. – Interrogate SS data according to the command.
NOTE – Only requested for such supplementary services which have data.	

3. **Interrogate SS resp.conf.**: is used to send a response back to the user to inform about the result of the interrogation.

Interrogate SS (Response: Success or Failure)	resp.conf.
Result	M

FEA3	– Relay the information to SACF.

4. **MT interrogate SS resp.conf.**: sends the result of the retrieved information of supplementary service to the user.

MT interrogate SS	resp.conf.
Result	M

FEA4	– No action required.

11.8 Invoke SS

This procedure is initiated by the user. The procedure is used to check the subscriber's subscription to a given supplementary service in the serving network. See Figure 11.8-1.

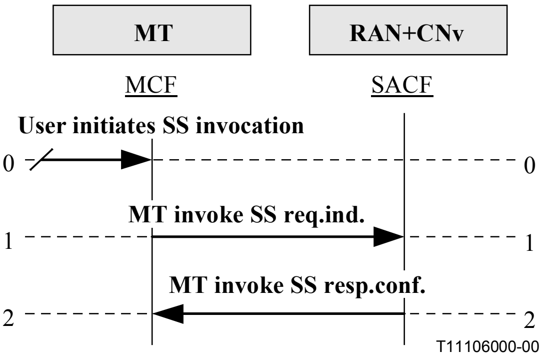


Figure 11.8-1/Q.1721 – Invocation of SS

0. **User initiates SS invocation**: the MCF receives a user initiated SS Invocation.

FEA0	– Detect user initiated SS control procedure via the MMI to request an invocation of a supplementary service. – Prepare and send the received information to SACF.

1. **MT invoke SS req.ind.**: is used to request to check the subscriber's subscription to a given supplementary service (e.g. call hold or multi-party) in LMFv, in connection with in-call invocation of that supplementary service, i.e. after the call setup phase is finished.

MT invoke SS (Response: Success or Failure)	req.ind.
SS code	M
SS data	O (Note)

FEA1	– Identify the concerned supplementary service. – Checked the subscriber's subscription according to the received information. – Prepare and send information to SACF.
NOTE – Only requested for such supplementary services which have data.	

2. **MT invoke SS resp.conf.**: sends the result of the checked subscriber's subscription information of supplementary service to the user.

MT interrogate SS	resp.conf.
Result	M

FEA2	– Present the result for the user.

11.9 Process unstructured SS request

This procedure is used to relay information in order to allow unstructured supplementary service operation. The received network entity passes the data received in the request to the application handling unstructured supplementary service application and waits for response from the application. See Figure 11.9-1.

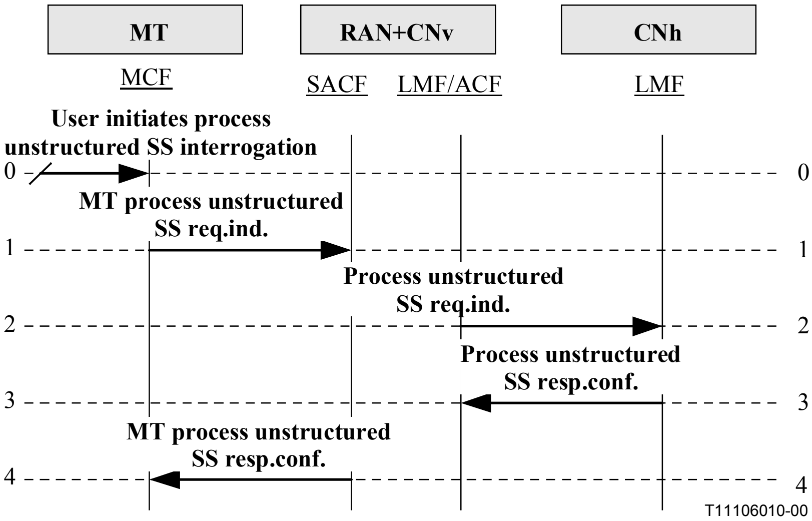

MT
RAN+CNv
CNh
MCF
SACF
LMF/ACF
LMF
User initiates process unstructured SS interrogation
MT process unstructured SS req.ind.
Process unstructured SS req.ind.
Process unstructured SS resp.conf.
MT process unstructured SS resp.conf.
0
1
2
3
4
T11106010-00

Figure 11.9-1/Q.1721 – Process unstructured SS request

0. **User initiates process unstructured SS request**: the MCF receives a user initiated process unstructured SS request.

FEA0	– Detect user initiated SS control procedure via the MMI to request a process unstructured request of a supplementary service. – Prepare and send the received information to SACF.

1. **MT process unstructured SS req.ind.**: is used to request to allow unstructured supplementary service operation.

MT process unstructured SS (Response: Success or Failure)	req.ind.
USSD data coding scheme	M
USSD string	M

FEA1	– Request to Process unstructured SS data.

2. **Process unstructured SS req.ind.**: is used to request the LMFh to process the USSD request.

Process unstructured SS (Response: Success or Failure)	req.ind.
USSD data coding scheme	M
USSD string	M

FEA2	– Perform one or more of the following functions as required by service logic. – Set up or release speech channels. – Pass the request to another network entity (unchanged or changed). – Pass a different USSD request to another network entity. – Request further information from the user.

3. **Process unstructured SS resp.conf.**: is used to send a response back to the user to inform about the result of the process unstructured SS request.

Process unstructured SS (Response: Success or Failure)	resp.conf.
USSD data coding scheme	O (Note 1)
USSD string	O (Note 2)
Result	O (Note 3)

FEA3	Relay the information to SACF.
NOTE 1 – If this IE is present, then the USSD String IE has to be present. NOTE 2 – If this IE is present, then the USSD Data Coding Scheme IE has to be present. NOTE 3 – Only used if an error situation has occurred.	

4. **MT process unstructured SS resp.conf.**: sends the result of the retrieved information of supplementary service to the user.

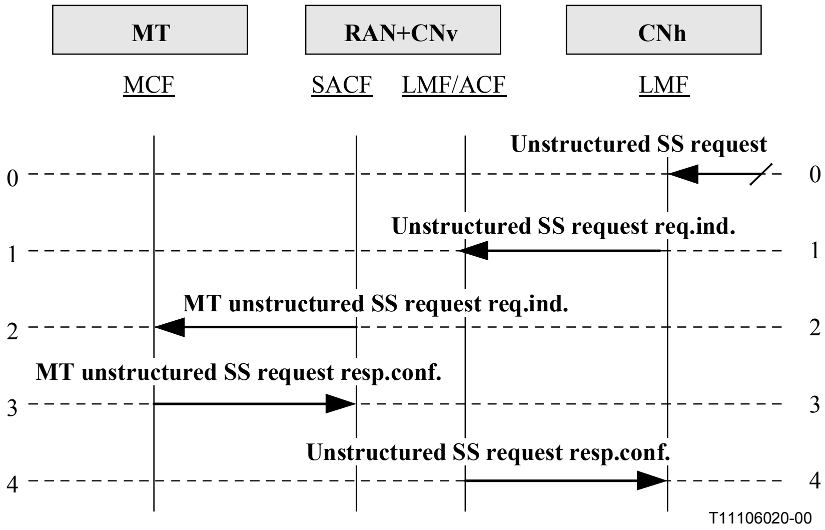
MT process unstructured SS	resp.conf.
USSD data coding scheme	O (Note 1)
USSD string	O (Note 2)
Result	O (Note 3)

FEA4	– Confirmation about allowing unstructured supplementary service operation to be used.
NOTE 1 – If this IE is present, then the USSD String IE has to be present. NOTE 2 – If this IE is present, then the USSD Data Coding Scheme IE has to be present. NOTE 3 – Only used if an error situation has occurred.	

11.10 Unstructured SS request

This procedure is used by the invoking entity, when information is required from the mobile user, in connection with unstructured supplementary service handling.

In some circumstances the SCFh may generate (or receive) an unstructured SS request towards (or from) the LMFh. This is likely to occur when an operator specific service, which is provided by the home SCF, requires a dialogue with the mobile user. This dialogue may be user initiated or SCF service initiated. The unstructured supplementary service data provides a transparent transport mechanism which enables this mobile user/service dialogue to take place. See Figure 11.10-1.



MT
RAN+CNv
CNh
MCF
SACF
LMF/ACF
LMF
Unstructured SS request
Unstructured SS request req.ind.
MT unstructured SS request req.ind.
MT unstructured SS request resp.conf.
Unstructured SS request resp.conf.
0
1
2
3
4
T11106020-00

Figure 11.10-1/Q.1721 – Unstructured SS request

0. **Unstructured SS request**: the invoking entity requires information from the mobile user.

FEA0	– Prepare and send Unstructured SS Request req.ind. to LMFv.

1. **Unstructured SS request req.ind.**: is used to request information from the mobile user.

Unstructured SS request (Response: Success or Failure)	req.ind.
USSD data coding scheme	M
USSD string	M
Alerting pattern	O (Note)

FEA1	– Prepare and send Unstructured SS request req.ind. to SACF.
NOTE – Will be present if received in connect operation from SCFh, otherwise will be absent.	

2. **MT unstructured SS request req.ind.**: is used to request the mobile user.

MT unstructured SS request (Response: Success or Failure)	req.ind.
USSD data coding scheme	M
USSD string	M
Alerting pattern	O (Note)

FEA2	– Prepare and send an MT unstructured SS request resp.conf. to SACF.
NOTE – Will be present if received in connect operation from SCFh, otherwise will be absent.	

3. **MT unstructured SS request resp.conf.**: is used to send a response back to the LMFh via SACF and LMFv about the result of the request.

MT unstructured SS request (Response: Success or Failure)	resp.conf.
USSD data coding scheme	O (Note 1)
USSD string	O (Note 2)
Result	O (Note 3)

FEA3	– Prepare and send an MT unstructured SS request resp.conf. to LMFv.
NOTE 1 – If this IE is present, then the USSD string IE has to be present. NOTE 2 – If this IE is present, then the USSD data coding scheme IE has to be present. NOTE 3 – Only used if an error situation has occurred.	

4. **Unstructured SS request resp.conf.**: sends the result of the retrieved information from the mobile user.

Unstructured SS request	resp.conf.
USSD data coding scheme	O (Note 1)
USSD string	O (Note 2)
Result	O (Note 3)

FEA4	– The required information has been fetched from the user.
NOTE 1 – If this IE is present, then the USSD string IE has to be present. NOTE 2 – If this IE is present, then the USSD data coding scheme IE has to be present. NOTE 3 – Only used if an error situation has occurred.	

11.11 Unstructured SS notify

This procedure is used by the invoking entity, when required a notification to be sent to the mobile user, in connection with unstructured supplementary service handling.

In some circumstances the SCFh may generate (or receive) an unstructured SS notification request towards (or from) the LMFh. This is likely to occur when an operator specific service, which is provided by the home SCF, requires a dialogue with the mobile user. This dialogue may be user initiated or SCF service initiated. The unstructured supplementary service data provides a transparent transport mechanism which enables this mobile user/service dialogue to take place. See Figure 11.11-1.

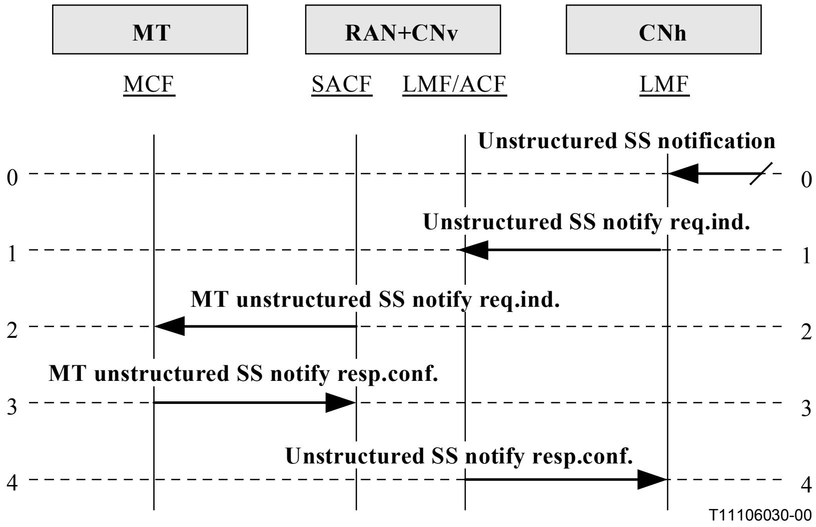

MT
RAN+CNv
CNh
MCF
SACF
LMF/ACF
LMF
Unstructured SS notification
0
Unstructured SS notify req.ind.
1
MT unstructured SS notify req.ind.
2
MT unstructured SS notify resp.conf.
3
Unstructured SS notify resp.conf.
4
T11106030-00

Figure 11.11-1/Q.1721 – Unstructured SS notification

0. **Unstructured SS notification**: indicates that a notification is to be sent to the mobile user.

FEA0	– Send an unstructured SS notify request to the LMFv.

1. **Unstructured SS notify req.ind.**: is used to send information to the mobile user.

Unstructured SS notify (Response: Success or Failure)	req.ind.
USSD data coding scheme	M
USSD string	M
Alerting pattern	O (Note)

FEA1	– Send an unstructured SS notify request to the SACF.
NOTE – Will be present if received in connect operation from SCFh, otherwise will be absent.	

2. **MT unstructured SS notify req.ind.**: is used to send information to the mobile user.

MT unstructured SS notify (Response: Success or Failure)	req.ind.
USSD data coding scheme	M
USSD string	M
Alerting pattern	O (Note)

FEA2	– Send an MT Unstructured SS Notify response to the SACF.
NOTE – Will be present if received in connect operation from SCFh, otherwise will be absent.	

3. **MT unstructured SS notify resp.conf.**: is used to send a response back to the LMFh via SACF and LMFv about the result of the request.

MT unstructured SS notify (Response: Success or Failure)	resp.conf.
Result	O (Note)

FEA3	– Send an MT Unstructured SS Notify response to the SACF.
NOTE – Only used if an error situation has occurred.	

4. **Unstructured SS notify resp.conf.**: sends the result of the retrieved information from the mobile user.

Unstructured SS notify	resp.conf.
Result	O (Note)

FEA4	– Confirm that the retrieved information has been received.
NOTE – Only used if an error situation has occurred.	

11.12 SS invocation notification

This procedure is used between the SACF and the SCF at invocation of certain supplementary services by the user. The services are explicit call transfer, call deflection and multi-party service. The SACF checks whether the criteria for sending a notification is fulfilled. If this is the case a notification is sent to the home SCF. If the notification criteria is not fulfilled, the processing of the particular supplementary service continues unchanged and no notification is sent. See Figure 11.12-1.

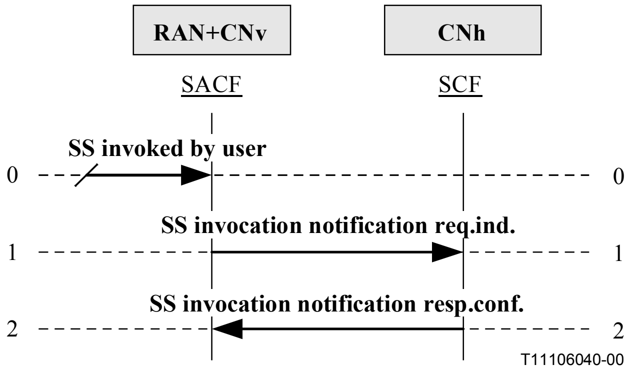

RAN+CNv
CNh
SACF
SCF
SS invoked by user
0
0
SS invocation notification req.ind.
1
1
SS invocation notification resp.conf.
2
2
T11106040-00

Figure 11.12-1/Q.1721 – Invocation notification

0. **SS invoked by user**: the SACF receives a user initiated SS invocation.

FEA0	– Detect invocation of a certain supplementary service. – Prepare and send an SS Invocation Notification req.ind. to SCF.

1. **SS invocation notification req.ind.**: is used when a subscriber invokes a certain supplementary service.

SS invocation notification (Response: Success or Failure)	req.ind.
MS ISDN	M
IMUI	M
SS-Event	M
SS-Data	O (Note)

FEA1	– If the information received is understood, prepare and send a positive acknowledgement SS invocation notification resp.conf. – If the information received is not understood, prepare and send a negative acknowledgement SS invocation notification resp.conf.
NOTE – Not all supplementary services contain data.	

2. **SS invocation notification resp.conf.**: sends the result of the invocation notification back to SACF.

SS invocation notification	resp.conf.
Result	M

FEA2	– Confirm the completion of the SS invocation notification procedure.

12 Over-the-air services

The following feature may not be applicable to all IMT-2000 family members.

12.1 Over-the-air service provisioning (OTASP)

This clause provides information flow diagrams for one of the Over-the-Air (OTA) services called Over-the-Air Service Provisioning (OTASP) for IMT-2000 systems.

12.2 Overview

The OTASP feature meets a need of the IMT-2000 based wireless industry to enable and expedite, in a secure manner, the process by which potential IMT-2000 service subscribers can activate (i.e. become authorized for) new wireless service(s). In addition, current subscribers can request changes in their existing service without third party intervention. An integral component of this process is the over-the-air functionality in the CNh.

One of the primary objectives of OTASP is the ability to provide a secure authentication key to a UIM to facilitate authentication. Authentication is the process by which information is exchanged between a UIM and the network for the purpose of confirming and validating the identity of the UIM.

The OTASP feature incorporates a cryptographic Authentication Key Generation procedure. This procedure allows the network to exchange Authentication Key parameters with a UIM. These parameters are used to generate the A-key. The Authentication Key Generation procedure enhances security for the subscriber (i.e. voice and data ciphering can be enabled to allow for the secure transfer of a new subscriber's credit/financial and IMUI information). It reduces the potential for fraudulent use of the IMT-2000 telecommunication service.

12.3 Description

OTASP information flows illustrate the following logical progression of events:

- **Invocation of activation with desired service provider**: Where an "attachment" occurs between the serving CNv and the over-the-air functionality (modelled in the SCF and depicted in the information flows as SCF_{OTA}) in the desired service provider's CN, and a correlation between the voice path (user to Customer Representative (CR), or a Voice Response Unit (VRU), at the Customer Service Centre (CSC)) and the data path (between the UIM and the over-the-air functionality) is established. The mobile terminal performs the initial system access based on a preferred system selection list that is pre-loaded within the UIMF. The user dials the prescribed OTASP digits to initiate the activation process. The visited network will need to be able to recognize and process the received digits from the mobile terminal in order to initiate the OTASP session. Based on the digits, the visited network will need to recognize that this is an OTASP origination and route the call appropriately to the CSC. This special handling of the received digits will require a bilateral business agreement between the home and visited systems, which is outside the scope of this Recommendation.
- **A-key generation**: Where the Authentication Key is separately generated in the AMF and the UIMF. The A-key is then used for ciphering and security during the OTASP process.
- **Re-authentication for voice and signalling ciphering**: This process computes and transfers ciphering information to the CNv to invoke ciphering of user plane (voice) and control plane (signalling messages) data prior to the exchange over the air of sensitive financial and provisioning information.
- **Transfer of OTASP data**: Where the actual provisioning information is transferred between the home network and the UIM.

12.4 Over-the-air service provisioning information flows

12.4.1 Invocation of activation with desired service provider

A potential subscriber ("user") wants to have an IMT-2000 mobile terminal activated in a desired service provider's network (the "home" network), while in another network (the "visited" network). This information flow shows the first step in OTASP called the "attachment" process whereby the user's voice call is correlated with the data path end the necessary information is downloaded to the UIM. The user's voice call origination is redirected from the visited network to a Customer Representative (CR – a human) or a Voice Response Unit (VRU – a machine), at the Customer Service Centre (CSC) in the home network. The visited network assigns a Temporary Reference Number (TRN) for voice and data path correlation. The TRN pool is administered via bilateral agreements between partnering service providers in order to maintain uniqueness of TRNs used in each visited network. The home network assigns an "activation" IMUI that is used during the activation process. See Figure 12.4-1.

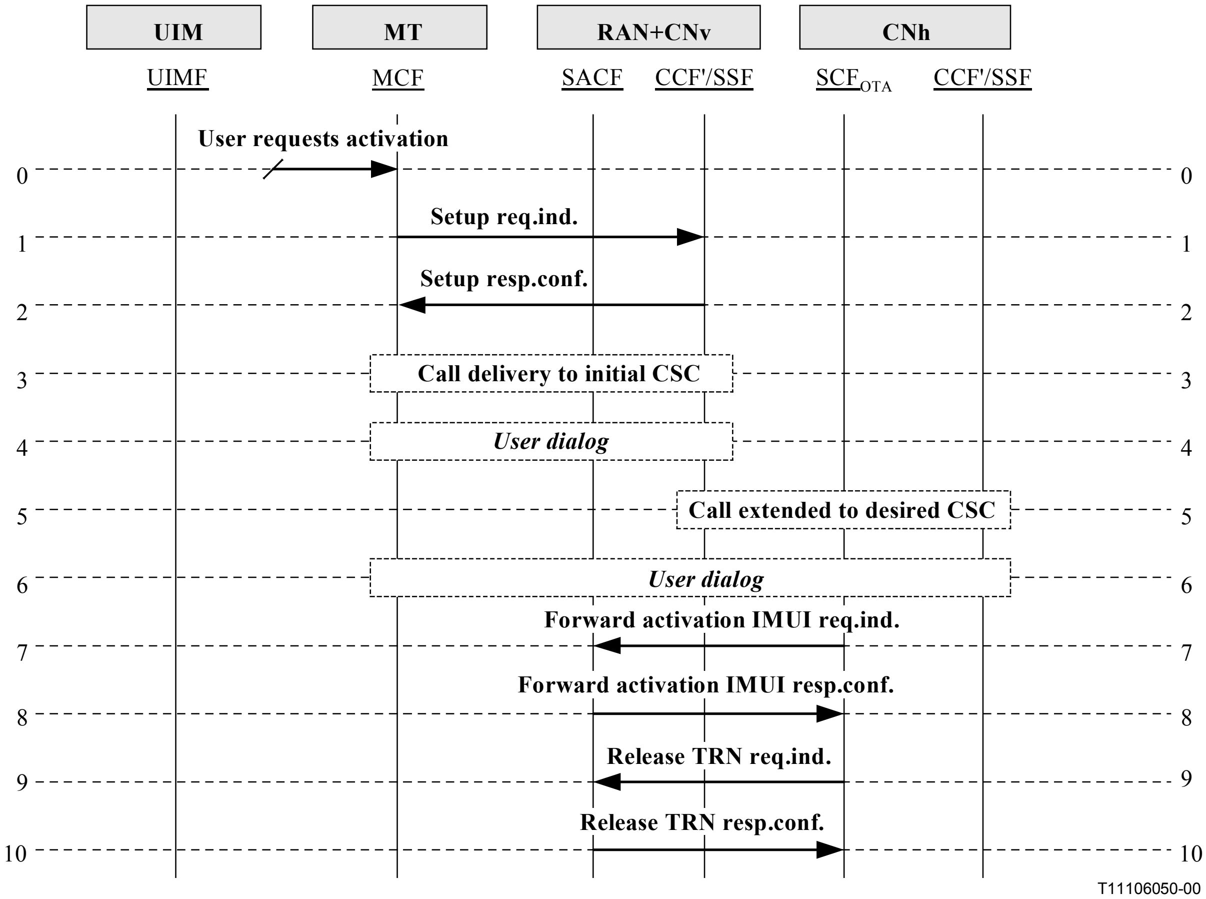


Figure 12.4-1/Q.1721 – Invocation of activation with desired service provider information flow diagram

0. **User requests activation**: is the initial stimulus where the user desires activation but happens to be on a system other than the system of choice.

FEA0	– The user initiates the process by making an OTASP call origination, i.e. by dialling the appropriate digits for activation (for e.g. a local Feature Service Code and directory number, as advertised or per the package instructions with the mobile terminal). – The MCF requests a bearer channel to establish the call to the local CSC.

1. **Setup req.ind.**: is from the MCF to the CCF'/SSF in the CNv. Upon receiving the OTASP call origination digits that the user had entered, the MCF sends the dialled digits to the CCF'/SSF in the CNv.

Setup (Response: Success)	req.ind.
Initial IMUI (INIT_IMUI)	M (Note)

FEA1	– Upon receiving the digits string and recognizing the local Feature Service Code as an OTASP attempt, the CNv may bypass or may perform normal network access authorization or subscriber validation and authentication prior to proceeding. Irrespective of the outcome of this procedure, the CNv connects the voice call to a local CSC (Customer Service Centre). – The CCF'/SSF allocates a unique TRN (Temporary Reference Number) for this OTASP session. – The CNv transfers the TRN to the CSC during call setup. Note that the TRN may be sent as a Calling Number or a Called Number based on the signalling schemes used. – The CCF'/SSF grants a bearer channel to carry the call.
NOTE – INIT_IMUI is the IMUI placed in the UIM at manufacture time. It is short-lived and is replaced by the Newly Assigned IMUI (NEW_IMUI) that is granted by the CNh, prior to the conclusion of the OTASP session.	

2. **Setup resp.conf.**: is from the CCF'/SSF to the MCF.

Setup	**resp.conf.**
Bearer ID	M

FEA2	– The MCF acquires the granted bearer channel and proceeds with completing the call.

3. **Call delivery to initial CSC**: the call connection between the user and the CSC associated with the CNv is made.

4. **Dialogue between user and initial CSC's CR or VRU**: a customer representative or a voice response unit at the CNv's CSC begins a dialogue with the user.

FEA4	– The customer representative or a voice response unit at the CSC determines that the user desires to have the MT activated on another CN, which would then become the user's home CN (CNh). – Since a business agreement exists between the operator of the CNv and the CNh, the CSC initiates a call re-route to the CSC in the desired CNh. – The initial CSC may make use of an internal look-up table to obtain the address of the desired CSC to re-route the call. No dialling number will be allowed from the user to avoid fraud.

5. **Call extended to desired CSC**: the customer representative or a voice response unit at the CSC obtains information from the user regarding the system that he/she desires to be connected to.

FEA5	– The CSC customer representative or a voice response unit then extends the voice call to another CSC (assuming that business agreements for such a transfer exist) that is associated with the desired service provider (operator). – Forwards the TRN to the new CSC.

6. **Dialogue between user and desired CSC's CR or VRU**: a customer representative or a voice response unit at the desired CSC begins a dialogue with the user.

FEA6	– The CSC then contacts the desired over-the-air functionality to activate service provisioning via the SCF_{OTA}.

7. **Forward activation IMUI req.ind.**: is from the SCF_{OTA} in the home network to the SACF in the visited network. The CSC representative causes the SCF_{OTA} to initiate this flow. The CNh is able to determine the routing address of the CNv from the TRN previously provided. This flow requests the SACF to attach to the CNh for this OTASP session. The CNh also assigns an "activation" IMUI to be used only during this OTASP session.

Forward activation IMUI (Response: Success)	req.ind.
Activation IMUI (ACT_IMUI)	M (Note 1)
Temporary reference number (TRN)	M (Note 2)
Action code (ACTCODE)	M (Note 3)

FEA7	– The CNv associates the call in question with the CNh, and thus a correlation between the voice path and the signalling path is established.
NOTE 1 – The ACT_IMUI is only used for this OTASP session. NOTE 2 – The TRN is used to associate the CNh with this OTASP call. NOTE 3 – The ACTCODE instructs the SACF to attach to this CNh for this call.	

8. **Forward activation IMUI resp.conf.**: is from the SACF in the visited network to the SCF_{OTA} in the home network.

Forward activation IMUI	resp.conf.
INIT_IMUI	M (Note 1)
CNv identity (CNv ID)	M (Note 2)
CNv authentication capabilities (CNv_AUTHCAP)	M (Note 3)
Authorization denied (AUTHDEN)	O (Note 4)

FEA8	– The CNh informs the CSC that the attachment with the CNv has been accomplished. – The CSC informs the CNh that it should direct the CNv to release the TRN.
NOTE 1 – The INIT_IMUI is received from the UIM at call setup and used for A-key Generation. NOTE 2 – The CNv ID is needed to route messages back to the CNv later in the OTASP process. NOTE 3 – The CNv_AUTHCAP informs the CNh about the CNv's authentication capabilities, used for Re-Authentication. NOTE 4 – Include the AUTHDEN if this UIM had previously (in Step 2) been denied network access authorization or failed subscriber validation and authentication.	

9. **Release TRN req.ind.**: is from the SCF_{OTA} in the home network to the SACF in the visited network. The CSC representative causes the SCF_{OTA} to initiate this flow. Since the attachment of the mobile terminal to the desired system (CSC and CNh) has completed successfully, the TRN is no longer needed, and the CNh decides to release the TRN (a potentially limited resource) so that it can be reused.

Release TRN (Response: Success)	req.ind.
ACT_IMUI	M
ACTCODE	M (Note)

FEA9	– The SACF in the CNv releases the TRN, thus permitting it to be reused for another OTASP session.
NOTE – The ACTCODE instructs the SACF to release the TRN.	

10. **Release TRN resp.conf.**: is from the SACF in the visited network to the SCF_{OTA} in the home network.

Release TRN	resp.conf.
None	(Note)

FEA10	– The SACF acknowledges the instruction after having released the TRN. – This concludes the attachment process.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

12.4.2 A-key generation

Prior to activating the user's IMT-2000 mobile terminal, secure voice and data paths have to be established. This is done by generating identical authentication keys (A-key) separately in the network (LMF) and the UIM (UIMF), using a public encryption method (such as the Diffie-Hellman algorithm; see Appendix II for a description). The A-key (never sent over the air) is then used to produce the necessary masks needed to establish voice and data ciphering. This information flow shows how the A-key is generated for IMT-2000 OTASP. See Figure 12.4-2.

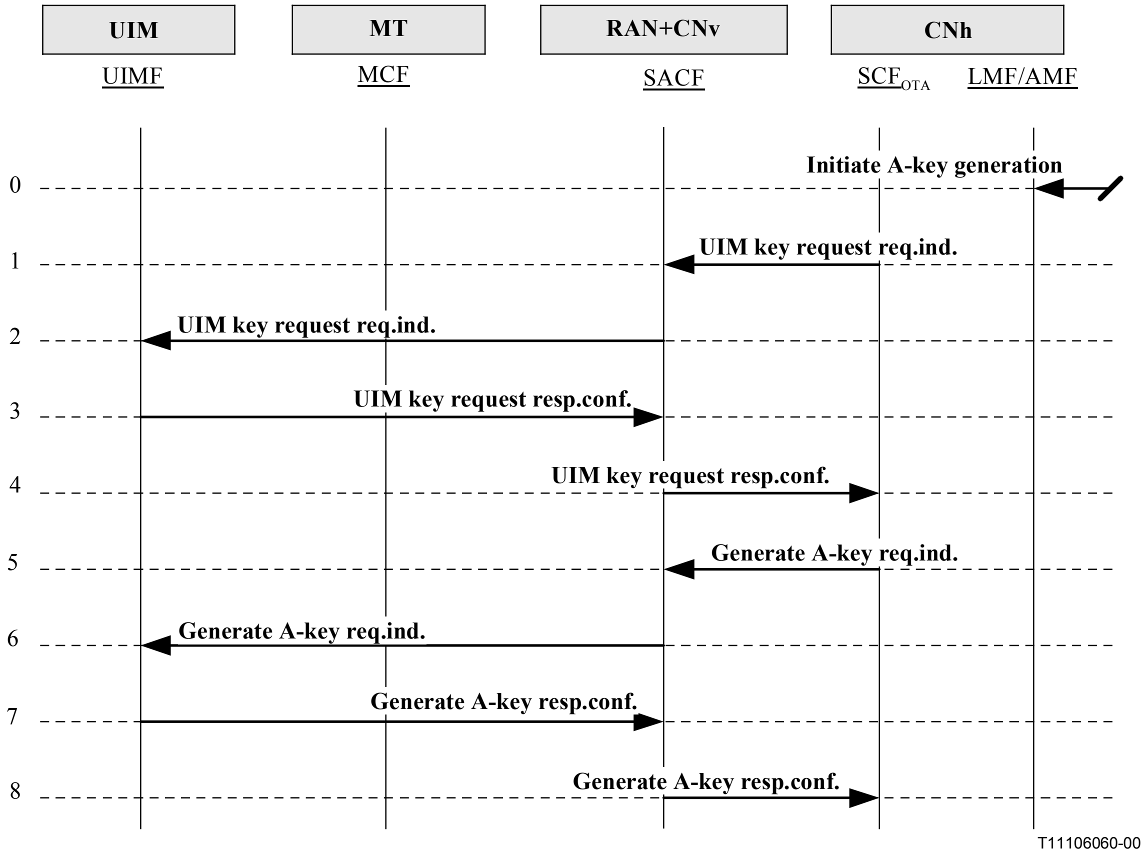


Figure 12.4-2/Q.1721 – A-key generation information flow diagram

0. **Initiate A-key generation process**: is the initial stimulus where the CSC initiates the authentication key generation procedure.

FEA0	– The CSC initiates the A-key Generation process. – The over-the-air functionality sends the LMFh a request, which includes the authentication key protocol version, corresponding to the UIM's A-key generation capabilities[8], the UIM's IMUI, and the activation IMUI. – The LMFh responds by returning the authentication key protocol version it will use, and public keys called Modulus Value (N*) and Primitive Value (g*). It also includes the CN Key Value (Y*), which the over the air functionality stores.

1. **UIM key request req.ind.**: is from the SCF_{OTA} in the home network to the SACF in the visited network. The CSC representative causes the SCF_{OTA} to initiate this flow. It includes the authentication key protocol version and the public keys. The over-the-air functionality stores the CN Key Value, and does not send it to the SACF.

[8] The Diffie-Hellman algorithm is modelled here, since it is publicly available for use, and is scalable, allowing for various combinations of exponents and public encryption values (modulus and primitive) to be used to meet the degree of security desired by the operator.

UIM key request (Response: Success)	req.ind.
Authentication key protocol version (AKEYPV)	M (Note)
Modulus value (MODVAL)	M
Primitive value (PRIMVAL)	M

FEA1	– The SACF in the CNv relays the contents so that they can be sent over the radio interface.
NOTE – The AKEYPV provides the authentication key protocol version corresponding to the specific combination of the Modulus Value (N*), the Primitive Value (g*) and the Exponent (y*), which the CNh (and the UIM) will use, as desired by the operator.	

2. **UIM key request req.ind.**: is from the SACF in the visited network to the UIMF via the MCF. The SACF merely forwards the contents it had received in Step 1 from the over-the-air functionality, to the UIMF.

UIM key request (Response: Success)	req.ind.
Authentication key protocol version (AKEYPV)	M
Modulus value (MODVAL)	M
Primitive value (PRIMVAL)	M

FEA2	– The UIMF successfully computes the UIM Key value (X*) based on the received public key values: MODVAL and PRIMVAL, and the Exponent, as specified by the authentication key protocol version.

3. **UIM key request resp.conf.**: This flow is from the UIMF (via the MCF) to the SACF in the visited network. The UIMF successfully computes the UIM Key Value and indicates this fact to the SACF in the CNv.

UIM key request	resp.conf.
Result	M (Note)

FEA3	– The SACF in the CNv relays the contents to the over-the-air functionality.
NOTE – The Result indicates that the UIMF has successfully computed the UIM Key Value.	

4. **UIM key request resp.conf.**: is from the SACF in the visited network to the SCF_{OTA} in the home network. The SACF merely forwards the contents it had received in Step 3 from the UIMF, to the over-the-air functionality.

UIM key request	resp.conf.
Result	M

FEA4	– The over-the-air functionality in the CNh computes the CN Key Value.

5. **Generate A-key req.ind.**: is from the SCF_{OTA} in the home network to the SACF in the visited network. The CSC representative causes the SCF_{OTA} to initiate this flow. The over-the-air functionality includes the CN Key Value (Y*) that the over-the-air functionality had stored in Step 1.

Generate A-key (Response: Success)	req.ind.
CN key value (CNKEY)	M

FEA5	– The SACF in the CNv relays the contents so that they can be sent over the radio interface.

6. **Generate A-key req.ind.**: is from the SACF in the visited network to the UIMF (via the MCF). The SACF merely forwards the contents it had received in Step 5 from the over-the-air functionality, to the UIMF.

Generate A-key (Response: Success)	req.ind.
CNKEY	M

FEA6	– The UIMF successfully computes the Authentication Key using the CNKEY, MODVAL and the same Exponent it had used when computing the UIM Key Value.

7. **Generate A-key resp.conf.**: is from the UIMF (via the MCF) to the SACF in the visited network. The UIMF has successfully computed the A-key Value and indicates this fact to the SACF in the CNv. It sends the computed UIM Key Value to the SACF, but not the A-key Value (which is never sent over the air).

Generate A-key	resp.conf.
Result	M (Note)
UIM key value (UIMKEY)	M

FEA7	– The SACF relays the contents to the over-the-air functionality.
NOTE – The Result indicates that the UIMF has successfully computed the A-key Value.	

8. **Generate A-key resp.conf.**: this flow is from the SACF in the visited network to the SCF_{OTA} in the home network. The SACF merely forwards the contents it had received in Step 7 from the UIMF, to the over-the-air functionality.

Generate A-key	resp.conf.
Result	M
UIMKEY	M

FEA8	– The over-the-air functionality directs the LMFh to generate the A-key also, using the received UIMKEY, the MODVAL and the same Exponent used in Step 1 to compute the CNKEY. – Thus both the UIM and the CNh generate identical A-keys.

12.4.3 Re-authentication for voice and signalling ciphering

This scenario describes UIM re-authentication for the purpose of computing and sending encryption parameters to the CNv. These parameters are used to invoke signalling message encryption and voice privacy, respectively, over the air interface. See Figure 12.4-3.

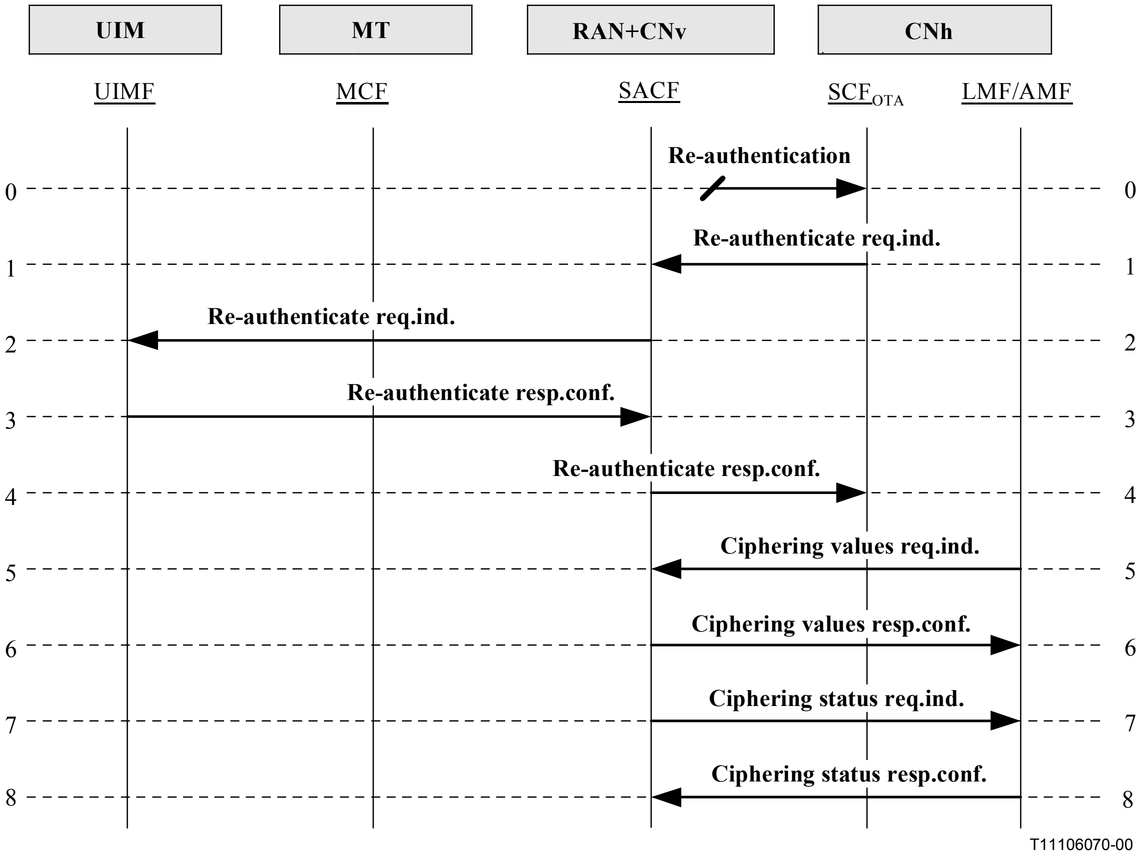

UIM
MT
RAN+CNv
CNh
UIMF
MCF
SACF
SCF$_{OTA}$
LMF/AMF
0 Re-authentication
1 Re-authenticate req.ind.
2 Re-authenticate req.ind.
3 Re-authenticate resp.conf.
4 Re-authenticate resp.conf.
5 Ciphering values req.ind.
6 Ciphering values resp.conf.
7 Ciphering status req.ind.
8 Ciphering status resp.conf.
T11106070-00

Figure 12.4-3/Q.1721 – Re-Authentication for voice and signalling ciphering information flow diagram

0. **Re-authentication**: is the initial stimulus where the CSC initiates the re-authentication procedure.

FEA0	– The CSC initiates the re-authentication process. – It determines that ciphering is needed over the radio interface. – The over-the-air functionality generates a Random challenge value (RAND) and sends it to the SACF.

1. **Re-authenticate req.ind.**: is from the SCF$_{OTA}$ in the home network to the SACF in the visited network. The CSC representative causes the SCF$_{OTA}$ to initiate this flow. The over-the-air functionality generates a Random Challenge Value (RAND) and sends it to the SACF. The purpose is to authenticate the UIM (again, as it were) following A-key generation, to ensure that the correct UIM is still involved in the OTASP process, prior to turning on ciphering.

Re-authenticate (Response: Success)	req.ind.
Random challenge value (RAND)	M (Note)

FEA1	– The SACF in the CNv relays the contents to the UIMF via the MCF.
NOTE – The RAND is used by the UIMF to respond with a corresponding result that will allow the CNh to determine that the UIM has re-authenticated correctly.	

2. **Re-authenticate req.ind.**: is from the SACF in the visited network to the UIMF (via the MCF). The SACF merely forwards the contents it had received in Step 1 from the over-the-air functionality, to the UIMF.

Re-authenticate (Response: Success)	req.ind.
RAND	M

FEA2	– The UIMF successfully computes a corresponding response that indicates it has re-authenticated correctly.

3. **Re-authenticate resp.conf.**: is from the UIMF (via the MCF) to the SACF in the visited network. The UIMF performs re-authentication and computes a corresponding Random Challenge Response (RANDC) value based on the received RAND, its own IMUI and other attributes. The computation may be based on an algorithm understood exclusively by the UIMF and the CNh.

Re-authenticate	resp.conf.
Random challenge response (RANDC)	M

FEA3	– The SACF in the CNv relays the contents to the over-the-air functionality via the SCF_{OTA}.

4. **Re-authenticate resp.conf.**: is from the SACF to the SCF_{OTA} in the visited network.

Re-authenticate	resp.conf.
RANDC	M

FEA4	– The over-the-air functionality forwards the information to the LMFh, along with the RAND value. – The LMFh independently computes a RANDC using the algorithm as in Step 3. – The LMFh compares it with the received RANDC. – The LMFh determines that the UIM has been re-authenticated correctly. – The LMFh then initiates the generation of ciphering related values.

5. **Ciphering values req.ind.**: is from the LMFh in the home network to the SACF in the visited network. Having determined that the UIM has been correctly re-authenticated, the LMFh computes the ciphering values and sends them to the SACF.

Ciphering values (Response: Success)	req.ind.
CNv identity (CNv ID)	M (Note 1)
Control plane cipher key (CPCKEY)	M (Note 2)
User plane cipher key (UPCKEY)	M (Note 3)

FEA5	– The SACF in the CNv uses the CPCKEY and UPCKEY to turn on ciphering.
NOTE 1 – The CNv ID is used to route the Ciphering Values req.ind. to the correct SACF. NOTE 2 – This is used to turn on ciphering of control plane information such as signalling messages. NOTE 3 – This is used to turn on ciphering of user plane information such as voice.	

6. **Ciphering values resp.conf.**: is from the SACF in the visited network to the LMFh in the home network.

Ciphering values	resp.conf.
None	(Note)

FEA6	The LMFh in the CNh has indication that the ciphering values have successfully reached the SACF.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

7. **Ciphering status req.ind.**: this flow is from the SACF in the visited network to the LMFh in the home network. User plane ciphering (voice) or control plane ciphering (signalling messages) or both get turned on over the radio interface.

Ciphering status (Response: Success)	req.ind.
Control plane ciphering report (CPCRPT)	M (Note 1)
User plane ciphering report (UPCRPT)	M (Note 2)

FEA7	– The LMFh in the CNh has information regarding the current status of ciphering over the radio interface.
NOTE 1 – This informs whether or not control plane ciphering has turned on. NOTE 2 – This informs whether or not user plane ciphering has turned on.	

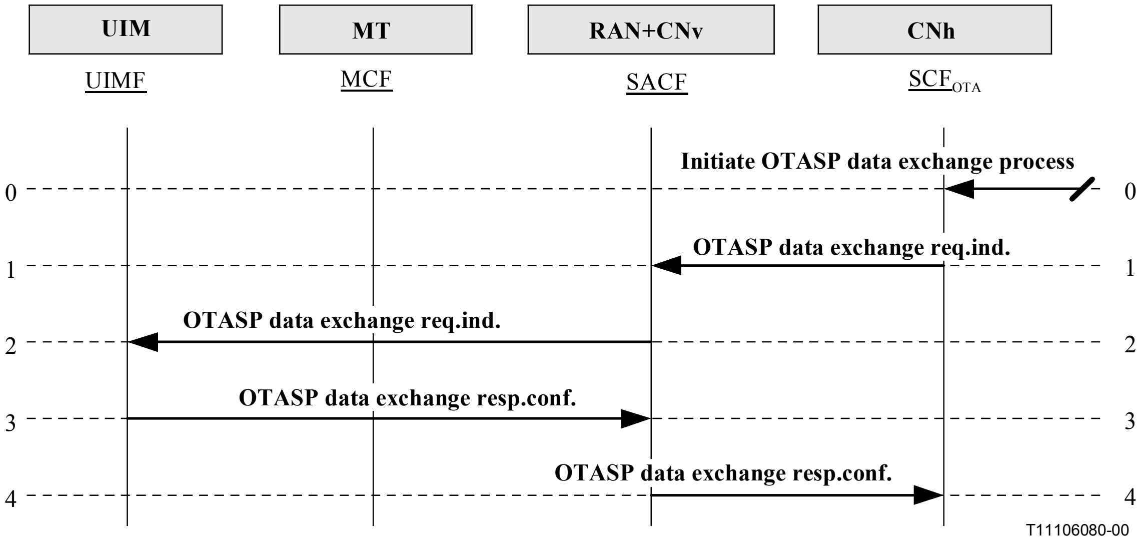
8. **Ciphering status resp.conf.**: this flow is from the SACF in the visited network to the LMFh in the home network. The LMFh forwards this information to the over-the-air functionality which then provides an indication to the CSC representative in the CNh if it is now safe to exchange sensitive user data over the air.

Ciphering status	resp.conf.
None	(Note)

FEA8	– The LMFh in the CNh forwards this information to the over-the-air functionality. – This indicates to the CSC if it is now safe to exchange data over the air. – Hence, the CSC and the subscriber exchange sensitive (financial, etc.) information. – This concludes the re-authentication process.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.	

12.4.4 Transfer of OTASP data

This scenario describes the exchange of OTASP Data Messages which carry the actual activation related information, between the over-the-air functionality in the CNh, and the UIMF via the MCF and the SACF in the CNv. This is typically done after ciphering has been turned on. See Figure 12.4-4.



UIM
MT
RAN+CNv
CNh
UIMF
MCF
SACF
SCF$_{OTA}$
Initiate OTASP data exchange process
OTASP data exchange req.ind.
OTASP data exchange req.ind.
OTASP data exchange resp.conf.
OTASP data exchange resp.conf.
0
1
2
3
4
T11106080-00

Figure 12.4-4/Q.1721 – OTASP data exchange information flow diagram

0. **Initiate OTASP data exchange process**: is the initial stimulus where the CSC representative causes the SCF$_{OTA}$ to initiate the OTASP Data Exchange procedure.

FEA0	– The CSC initiates the OTASP Data Exchange process. – Having confirmed that ciphering is present over the radio interface, it prompts the over-the-air functionality to send OTASP related data to the SACF in the CNv. – This includes the Newly Assigned IMUI for downloading into the UIMF and other supplementary service related information.

1. **OTASP data exchange req.ind.**: is from the SCF_{OTA} in the home network to the SACF in the visited network.

OTASP data exchange (Response: Success)	req.ind.
Newly assigned IMUI (NEW_IMUI)	M (Note 1)
ACTCODE	M (Note 2)

FEA1	– The SACF in the CNv relays the contents to the UIMF via the MCF. – The SACF also releases any resources when the OTASP session is completed.

NOTE 1 – The NEW_IMUI is the permanent identity assigned and committed into the user's UIM.

NOTE 2 – Depending on the data exchange case, the ACTCODE can variously instruct the:

- SACF to send the NEW_IMUI to the UIMF;
- UIMF to commit the NEW_IMUI to its permanent memory;
- UIM to re-register the user after the NEW_IMUI has been committed to its permanent memory;
- SACF and UIMF to release resources after completing the OTASP tasks.

2. **OTASP data exchange req.ind.**: this flow is from the SACF in the visited network to the UIMF (via the MCF).

OTASP data exchange (Response: Success)	req.ind.
Newly assigned IMUI (NEW_IMUI)	M

FEA2	– The UIMF replaces the ACT_IMUI with the NEW_IMUI. – It commits the NEW_IMUI to permanent memory. – It uses the Terminal Registration Procedure to re-register the user.

3. **OTASP data exchange resp.conf.**: this flow is from the UIMF (via the MCF) to the SACF in the visited network.

OTASP data exchange	resp.conf.
None	(Note)

FEA3	– The SACF forwards the OTASP Data Exchange resp.conf. on to the over-the-air functionality.

NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success.

4. **OTASP data exchange resp.conf.**: this flow is from the SACF in the visited network to the SCF_{OTA} in the home network.

OTASP data exchange	resp.conf.
None	(Note)

FEA4	– The over-the-air functionality informs the CSC that the OTASP Data Exchange concluded successfully.
NOTE – The response confirmation is empty. Merely its presence is sufficient to indicate success. This successfully completes the OTASP session. At this point the MT and UIM are activated and the subscriber can receive service.	

13 Definitions of information elements

13.1 action code (ACTCODE): Specifies the nature of the action to be performed by the designated functional entity. For example, in OTASP, the action code is used by the SCF in the home network to instruct the SACF in the serving network to:

- Attach to the home network during a particular OTASP session.
- Release a TRN, thus permitting the TRN to be reused for another OTASP session.
- Send the newly assigned IMUI to the UIM.
- Commit the new IMUI to the UIM's permanent memory.
- Re-register the user after the new IMUI has been committed within the UIM.
- Release resources at the CNv at the conclusion of the OTASP session.

13.2 activation IMUI (ACT_IMUI): Is a temporary IMUI assigned by the SCF in the home network, that is used only for the duration of a particular OTASP session. It is eventually replaced by the newly assigned IMUI.

13.3 alert reason: Indicates the reason why the message service centre is alerted. It can take one of the following values:

- MT present.
- Memory available.

13.4 alerting pattern: An indication that can be used by the MT to alert the user in a specific manner in case of mobile terminating traffic (switched call or unstructured supplementary data). This indication can be an alerting level or an alerting category.

13.5 authorization denied (AUTHDEN): Indicates that a UIM had previously been denied network access authorization or failed subscriber validation and authentication.

13.6 authentication key (A-key): Is a security related value used in voice/data and signalling message ciphering. It is never sent over the radio interface. It may be established at both the CNh and UIM by OTASP procedures, or it may be programmed into the UIM by service provider specified methods.

13.7 authentication key protocol version (AKEYPV): Indicates the specific combination (as desired by the home operator) of modulus value "N", the primitive value "g" and the exponent "y", which the CNh and the UIM will be using during an OTASP authentication key generation process. (See Appendix II.)

13.8 AUTHBS: An authentication response generated by the network in response to a random challenge sent by the UIM during an "Update SSD" procedure.

13.9 AUTH_R: An authentication response to SSD-based global challenge.

13.10 AUTH_U: An authentication response to an SSD-based unique challenge.

13.11 bearer capability: Indicates a requested ISDN bearer service to be provided by the network. (See ITU-T Recommendation Q.931 [10].)

13.12 bearer ID: Is used to specify the bearer (e.g. channel number).

13.13 billing ID: Is used to identify the billing plan (tariff, account owner, etc.) associated with the call.

13.14 called number: Identifies the called party of a call. (See ITU-T Recommendation Q.931 [10].)

13.15 call history count (CHCNT): A counter held and maintained in the network and the UIM. This counter may be updated by either the home or visited network, and serves as a detector of possible "cloned" UIMs.

13.16 call ID: Indicates the identity of a call in a signalling transfer point.

13.17 calling number: Identifies the origin of a call. (See ITU-T Recommendation Q.931 [10].)

13.18 calling user ID: Identifies the calling party of a call.

13.19 category: Provides an indication of the specific subject matter (e.g. emergency, system operator announcement, news, advertisement, sports, etc.) carried in the payload being sent to a user or users (e.g. SMS or teleservice broadcast messaging).

13.20 challenge (or RANDU): A random unique challenge generated by the network to authenticate the UIM.

13.21 challenge response: A UIM-computed authentication response to the network-initiated random unique challenge. Also, known as SRES (Signature result) in some systems.

13.22 challenge response value: It is a value generated by the mobile terminal (PSCAF) using the challenge value and the secret data that it shares with its home network (LMFp/AMFp).

13.23 challenge value: It is a random value generated by the visited network to be used for authentication of the visited mobile terminal.

13.24 ciphering key(s): Secret key(s) used for encipherment of radio interface traffic.

13.25 CNv authentication capabilities (CNv_AUTHCAP): Provides information regarding a visited/serving network's authentication capabilities; for example used in re-authentication during an OTASP session.

13.26 CNv identity (CNvID): Provides the identity of the visited/serving network for routing purposes. For example, in OTASP, it is provided by a CNv to the CNh, so that the CNh may use it later during an OTASP session to route messages to the CNv.

13.27 CN key value (CNKEY): Is a number "Y" generated by the home network (i.e. in the LMFh) which is sent to the visited network and on to the UIM, for the generation of the authentication key during an OTASP session. It is computed as:

$$Y = g^{y} \text{ Mod } N$$

13.28 confirmation of RANDG: A form of RAND sent by the MCF, consistent with specific radio interfaces.

13.29 connected line ID: Identifies the connected party of a call.

13.30 control plane cipher key (CPCKEY): Contains the key to be used for ciphering of appropriate data fields within signalling messages sent in both directions over the radio interface. It is computed at the CNh. Its presence also instructs the serving/visited network to turn on control plane ciphering.

13.31 control plane ciphering report (CPCRPT): Is sent by a visited/serving network to the home network to indicate whether or not control plane ciphering has been turned on.

13.32 current password: The password used by a user for supplementary service control.

13.33 data session lifetime: It is the duration of time allocated to the tunnel-connection of a data session. It is determined and/or extended by the PSCAF when requesting establishment of a new data session. A tunnel-connection is cleared when its lifetime expires.

13.34 deleted user data: Describes the user profile data to be deleted in the subscriber data management procedures. It may include:

- a list of basic services;
- a list of supplementary services (in the form of supplementary codes);
- supplementary services data;
- VHE subscription data;
- broadcast and/or group call subscription data.

13.35 encapsulation method: It is a user plane scheme to prevent out-of-sequence delivery of users' packet data units across the tunnel-connection. The choice of encapsulation method is suggested by PSACF when sending a request for establishment/re-establishment of a data session to the LMFp of the visited network.

13.36 end point reference (point): It is the routing address/number of the user (i.e. ITDN), the party, to be added to or dropped from a multi-party call.

13.37 expected quality: This information element is used to report the expected quality of a radio bearer, which the network may allocate to the mobile terminal, based on the measurement result.

13.38 feature information: Feature code, visited system capabilities, current visited system action.

13.39 guidance information: Refers to the guidance information given to a user who is requested to provide a password supplementary service control. The following information may be given:

- "Enter password": This is used to prompt the user for his/her current password.
- "Enter new password": This is used to prompt the user for a new password during registration of a new password.
- "Enter new password again": This is used to prompt the user to re-enter the new password during registration of a new password.

13.40 high layer compatibility: Provides a means for the remote user to check compatibility. (See ITU-T Recommendation Q.931 [10].)

13.41 LMFh address: A routable address to a home location management function, e.g. the ISDN number of the HLR.

13.42 IMT-2000 mobile directory number (IMDN): A dialable number that uniquely identifies an IMT-2000 user and is used to place, or forward, a call to that user, or to identify a user upon call origination.

NOTE – E.164 MS ISDN Number may be applied for this.

13.43 international mobile user identity (IMUI): Is used to address a mobile terminal and identify the mobile user uniquely to a service provision function.

13.44 information transfer capability: Indicates the type of the bearer capability requested by the calling party (e.g. speech). (See ITU-T Recommendation Q.931 [10].)

13.45 international temporary directory number (ITDN): An E.164 number which carries a dialable, routable number that a called party is assigned in and by a visited system for a short duration to facilitate call routing, while roaming globally.

13.46 initial IMUI (INIT_IMUI): Is the original IMUI that is placed in the UIM at time of manufacture and is used during the OTASP authentication key generation process. It is short-lived and is replaced by the newly assigned IMUI that is granted by the home network, prior to the conclusion of an OTASP session.

13.47 interference level: This information element is used to report the interference level as a part of a measurement report.

13.48 IP address (X): IP address of the entity X (e.g. PSCAF, PSCF and PSGCF). It is used as the tunnel termination point.

13.49 location area identity (LAI): Identifies the area in which the mobile terminal is located in the visited network.

13.50 LMFv address: A routable address to a visited location management function, e.g. the ISDN number of the VLR.

13.51 location information: Indicates the location of the mobile user as accurately as possible with the available information. This could be, for example, cell ID, location area ID, VLR address, or some kind of geographical information.

13.52 low layer compatibility: Provides a means which should be used for compatibility checking by an addressed entity (e.g. a remote user or an interworking unit or a high-layer function network node addressed by the calling user). (See ITU-T Recommendation Q.931 [10].)

13.53 media ID: It is used to identify/select a media type.

13.54 media type: Is referred to a specific service transport medium. The word media is referred to a set of bearers allocated to support a variety of generic services such as voice, data, image and video.

13.55 measurement condition: This information element is used to instruct the mobile terminal on the condition on which the measurement is performed. Information such as repetition interval is included.

13.56 message: This parameter contains the SMS message.

13.57 message centre address: Represents the E.164 address of a SMS message centre.

13.58 message notification type: Indicates the manner in which to notify the user (e.g. audible, visual, vibratory, combinations of these, or other).

13.59 messages pending count: Indicates the number of messages that are awaiting retrieval by the user.

13.60 message priority: Provides in increasing order, an indication of the level of priority (e.g. normal, interactive, urgent, emergency) of a message (e.g. SMS or teleservice broadcast).

13.61 message status: Provides an indication of whether a message is new, a replacement, or a deletion of an existing message (e.g. SMS or teleservice broadcast) with the same identification (see Message type).

13.62 message type: Provides an identification for a message (e.g. SMS or teleservice broadcast) within a serving network.

13.63 message waiting indicator: Indicates if it is a message that is waiting or not.

13.64 message waiting type: Indicates whether the pending messages are voice, fax, e-mail or other.

13.65 modulus value (MODVAL): Is a number "N" generated by the home network (i.e. in the LMFh) which is sent to the visited network and on to the UIM, for the generation of the authentication key during an OTASP session. Its length is set by the operator (e.g. 512 bits, 768 bits, etc.) and the larger the number the greater the security provided during the authentication key generation process.

13.66 MS ISDN: Refers to one of the ISDN numbers assigned to a mobile subscriber in accordance with ITU-T Recommendation E.213 [8].

13.67 network access identifier (NAI): A string that uniquely identifies the FE, in this case the PSCF.

13.68 newly assigned IMUI (New_IMUI): Is the permanent identity assigned by the home network (LMFh) to the UIM of a new subscriber, and is committed within the UIM at the conclusion of an OTASP session where it replaces the Activation IMUI.

13.69 number of measured calls: This information element is used to instruct the mobile terminal on the maximum number of surrounding cells of which measurement should be performed if radio condition allows.

13.70 operation result: Provides the outcome of the operation such as operation rejected (e.g. invalid operation), operation accepted and completed, or operation accepted and not completed (e.g. error).

13.71 originator address: Is the address of the original message sender (e.g. in SMS or teleservice broadcast). Typical formats include BCD Digits, IA5 encoding and IP address variants.

13.72 payload: Is any text carried (e.g. by SMS or teleservice broadcast) for display or other use by a recipient entity. It is meaningful only to the protocol end points, and is interpreted by a teleservice identifier.

13.73 periodicity: Provides an indication of the start time, duration and repetition rate with which a message (e.g. SMS or teleservice broadcast) needs to be delivered to recipient(s).

13.74 pilot channel reception level: This information element is used to report the reception level of a pilot channel as a part of a measurement report.

13.75 personal identification number (PIN): A number used in the verification of a user's claimed identity, used here to unlock the UIM. Assigned by the service provider at time of service provisioning.

13.76 preferred language indicator: Indicates the language of choice of a recipient of a voice announcement or a text message (e.g. when notifying a user of pending messages that require retrieval, providing a roamer greeting, displaying a short message).

13.77 primitive value (PRIMVAL): Is a number "g" set by the home network (i.e. in the LMFh) which is sent to the visited network and on to the UIM, for the generation of the authentication key during an OTASP session. Its length is set by the operator and the larger the number the greater the security provided during the authentication key generation process.

13.78 power control info.: Is used to instruct the mobile terminal on the initial power level it should set for the allocated radio bearer.

13.79 provider error: Indicates a protocol related type of error:

– duplicated invoke ID;

– not supported service;

– mistyped parameter;

- resource limitation;
- initiating release, i.e. the peer has already initiated release of the dialogue and the service has to be released;
- unexpected response from the peer;
- service completion failure;
- no response from the peer;
- invalid response received.

13.80 quality of service (QoS): Is used to specify the required quality of service such as bit error rate.

13.81 RANDBS: A random challenge sent by the MCF to validate the network in SSD-based systems.

13.82 RANDG: A global random challenge (random number) broadcast over the system information channel. It is used in SSD-based systems in conjunction with SSD and other parameters, as appropriate, to authenticate the user.

13.83 RANDSSD: A random number sent to the UIM, for use in the SSD update process.

13.84 RANDU: A random unique challenge used to authenticate the user of the terminal in SSD-based systems. (May be generated by the visited network when SSD is shared.)

13.85 remaining session lifetime: Computed by the home LMFp using the original session lifetime, it is sent to the anchor LMFp during an established data session.

13.86 remote action: Tone or announcement to play.

13.87 requested information: Indicates type of information requested, e.g. location information, user state, or both.

13.88 radio frequency info.: Is used to specify the information of the radio frequency which is allocated to the mobile terminal.

13.89 reverse link info.: Is used to specify the information of the reverse radio link which is allocated to the mobile terminal.

13.90 result: Is used to indicate success or failure of a requested procedure.

13.91 routing address: Is used for routing to the terminating visited/serving/supporting network.

13.92 security key: Generated by LMFp, it is sent to the mobile terminal, visited PSCF, and PSGCF for support of encryption and security association between these entities.

13.93 security parameter index: Generated by LMFp, it is sent to the mobile terminal, visited PSCF, and PSGCF for support of encryption and security association between these entities.

13.94 selection: Specifies the data that is to be retrieved from the SDF.

13.95 service address information: Is used by the SCF to select the correct application.

13.96 service discriminator: It is an indicator used by the home LMFp to determine the PSGCF and to indicate to the mobile terminal which network to connect to (e.g. specific ISP, specific corporate network, generic internet access). It also indicates whether or not access is preferred to be through a PSGCF in the visited or in the home network.

13.97 service ID: Identifies the service type for which the user wants to register (possible service types are: telephone, fax, videotex, data, etc.).

13.98 service group: Provides information that identifies the target mobile station audience intended for receiving SMS or teleservice broadcast service. It is "free form", in that its format is determined and understood only by the protocol end points (e.g. for teleservice broadcast, the end points would be the message centre and the mobiles).

13.99 service type: It is referred to the types of service when the establishment of a packet data session is requested (e.g. voice and data).

13.100 session ID: Supplied by PSCAF (when an "advertisement" request is received), it is to remove ambiguity from the response to the MT in a later stage of a "data session establishment/ re-establishment" procedure. It is a unique identifier of each packet data session in a multiple sessions environment.

13.101 session source address: In a multiple sessions case, it is the address information of a session (i.e. Session ID), used to associate the "de-registration" response signal with the session to be terminated.

13.102 SS-data: Contains additional information related to supplementary service invocation. Depending on the service invoked it can contain the following information:

– A list with all called party numbers involved.

– The called party number involved.

13.103 shared secret data (SSD): A quantity derived from the A-key for use in authenticating the subscriber in both the "home" and "roaming" environments, in SSD-systems. The SSD is partitioned into two distinct subsets, SSD-A and SSD-B, used for authentication response and encryption key generation, respectively.

13.104 SS-event: Indicates the supplementary service for which an invocation notification is sent towards the SCF. It can indicate one of the following services:

– Explicit call transfer.

– Call deflection.

– Multi-party call.

13.105 SS code: Indicates one supplementary service or a set of supplementary services.

13.106 SS data: A general information element including data used by different supplementary services, e.g. call forwarding information or call barring information.

13.107 target CCF ID: Is used to indicate the CCF in which the access bearer is to be established.

13.108 TC Info.: Is the terminal capability information which determines the services that the terminal can support.

13.109 teleservice type: Refers to services such as messaging, speech, facsimile, paging, etc.

13.110 temporary reference number (TRN): Is assigned by the SCF in the home network and is used to correlate the voice connection (between the user's mobile and the Customer Service Centre) with the data connection (between the serving network and home network), during an OTASP session.

13.111 terminal status: Identifies the status of the mobile terminal and its user (i.e. MT active or inactive, service granted, operator determined barring, etc.).

13.112 termination treatment info: Is used to provide information regarding how a particular termination attempt should be dealt with (e.g. respond to a page).

13.113 termination treatment request: Is used to query about how a particular termination attempt should be dealt with (e.g. whether or not a page be responded to).

13.114 temporary mobile user ID (TMUI): Is used both to address a mobile terminal and to identify an IMT-2000 user. It is allocated and used by the visited network temporarily to preserve anonymity.

13.115 TMUI assignment source ID: Is used to identify an LMFv which assigned the TMUI.

13.116 TMUI expiration timer: Is used together with TMUI in order to provide enhanced user confidentiality.

13.117 transit network selection: Indicates the transit network(s) requested to be used in the call. (See ITU-T Recommendation Q.762 [11].)

13.118 UIM info request: Refers to the information requested from the UIM to provide the following:

- called number associated with speed (abbreviated) dialling number;
- specific authentication related information;
- specific subscriber related information;
- specific address related information.

13.119 UIM info response: Contains the UIM information requested.

13.120 UIM key value (UIMKEY): Is a number "X" generated by UIM and sent to the home network (i.e. in the LMFh), via the visited network, during an OTASP authentication key generation process. It is computed as:

$$X = g^{x} \text{ Mod } N$$

13.121 user error: Indicates that an error has occurred during handling with short message service.

13.122 user information rate: Is used to indicate the actual user information rate which is transmitted over the radio bearer and the terrestrial channel. It may also indicate the rate adaptation in the case the user information rate and the bearer capability of the radio bearer are not the same.

13.123 user plane cipher key (UPCKEY): Contains the key to be used for ciphering of voice/data sent in both directions over the radio interface. Its presence also instructs the serving/visited network to turn on user plane ciphering.

13.124 user plane ciphering report (UPCRPT): Is sent by a visited/serving network to the home network to indicate whether or not user plane ciphering has been turned on.

13.125 user profile: Is the data that specifies the subscribed services, and authentication related data for the IMT-2000 user. In addition, it may include the following attributes:

- Broadcast and/or group call subscription data (if applicable);
- IMT-2000 Mobile directory number (IMDN), e.g. a dialable number;
- IMT-2000 Mobile user ID (IMUI);
- IMT-2000 Temporary mobile user ID (TMUI);
- terminal state;
- user/terminal location information;
- basic service data (e.g. subscribed bearer services);
- teleservices (e.g. broadcast and/or group call subscription data);
- supplementary services data;
- operator determined features/services (e.g. Call barring data);
- subscriber determined features/services (e.g. Call screening data);
- roaming restriction data;
- regional subscription data; and
- VHE Subscription Data.

13.126 USSD data coding scheme: Contains the information of the alphabet and the language used for the unstructured information in an unstructured supplementary service data operation.

13.127 USSD string: Contains a string of unstructured information in an unstructured supplementary service data operation. The mobile user or the network either sends the string.

13.128 zone identifier: Provides an indication of the geographical area (e.g. whole RANs or portions of a RAN within a serving network, or to the whole serving network) over which a message should be broadcast, as in the case of teleservice broadcast messaging. It is "free form", in that its format is determined and understood only by the protocol end points (e.g. for teleservice broadcast, the end points would be the message centre and the serving network).

ANNEX A

List of common procedure modules used in this Recommendation

Name of common procedure	Clause No.	Procedure used in
Authentication calculation	6.1.2.2.3	User authentication
Call Release	7.5	Party dropping (root party initiated and leaf initiated)
Call routing	7.3	VHE "Direct Home Command", Party addition (root party initiated)
Get password	11.1	Register password
IMT-2000 user ID retrieval	6.2.2	Terminal location update
LAI update	6.2.2.1.5	Terminal location registration, Terminal location update
Location update		Terminal location registration
Mobile call release	7.5	Party dropping
Mobile incoming call	7.4	Party addition
Specialized resource assist	IN procedure	VHE "Direct Home Command"
Start ciphering	6.1.2.5	Terminal location registration, Terminal location update, Initial mobile outgoing call, Initial mobile incoming call, Mobile originated short message, Mobile terminated short message
Subscriber profile transfer	6.2.1.3	Restore LMF data
Terminal location registration	6.2.3.1	Initial mobile outgoing call, Packet data session
Terminal paging	7.2	Initial mobile incoming call, Mobile terminating short message
TMUI assignment	6.1.2.6	Terminal location registration, Terminal location update, Initial mobile outgoing call, Initial mobile incoming call
TMUI inquiry	6.2.2.1.1	Terminal location update, Detach, Terminal paging, Attach
TMUI update	6.2.2.1.4	TMUI assignment
User authentication	6.1.2	Terminal location registration, Terminal location update, Detach, Initial mobile outgoing call, Initial mobile incoming call, Mobile originated short message, Mobile terminated short message, Attach

Name of common procedure	Clause No.	Procedure used in
User ID retrieval	6.2.2.2	Terminal location registration, Detach, Attach
User info interrogation	6.2.1.2	User information interrogation, Mobile terminated short message
VHE service invocation	9	Initial mobile outgoing call, Call routing, Initial mobile incoming call

APPENDIX I

Q.1721 Coverage of Table 1/Q.1701, Capability Set 1 Requirements

This appendix uses Table 1/Q.1701 copied verbatim from Q.1701. A third column is added to indicate whether Q.1721 covers the identified capability.

The entries in the third column should be interpreted as follows:

Entry	Interpretation
Not Applicable	This capability is of a type that specific information flows are not associated with it.
Yes	This capability is supported by the information flows described in the indicated clause.
No	This capability is not supported by information flows in Q.1721. Reasons are given.
Partial	This capability is partially supported by the information flows described in the indicated clause. Those aspects not supported are indicated together with reasons.

Table I.1/Q.1721 – Capability Set 1 for IMT-2000

Category	Capabilities	Coverage
A) Existing Capability	1 Widely used existing 2nd generation core fixed and mobile services and capabilities, possibly enhanced	1 Not Applicable
B) Long-Term Objectives	1 Support network capabilities that are a distinct improvement over widely used 2G (second generation) wireless networks system capabilities in the areas of voice, data, messaging, image and multimedia, including: 1.1 Enhanced roaming 1.2 Increased data rates 1.3 Multimedia and Internet wireless services	1 Not Applicable. The capabilities needed to support these enhancements are further addressed later in the table.
C) Bearer Capability	1 For terrestrial access: 1.1 At least 144 kbit/s in vehicular radio environment, BER ≤ 10^{-6}, both for circuit and packet services 1.2 At least 384 kbit/s in outdoor to indoor and pedestrian radio environments, BER ≤ 10^{-6}, both for circuit and packet services	1 Yes. Subclause 7.1

Table I.1/Q.1721 – Capability Set 1 for IMT-2000 *(continued)*

Category	Capabilities	Coverage
	1.3 At least 2048 kbit/s in indoor office radio environment, BER ≤ 10^{-6}, both for circuit and packet services	
	2 Range of QoS with independent negotiation: 2.1 Real time/non-real time 2.2 Delay characteristics 2.3 Maximum acceptable Bit Error Rate 2.4 Bit rate/throughput	2 Yes. Subclause 7.1
	3 Support of packet services (both on the radio interface and on the fixed interfaces)	3 Yes. Subclause 8.4
	4 For the satellite access interface: 4.1 The data rates from any one user of the satellite component of IMT-2000 may be expected to range from 9.6 kbit/s up to 144 kbit/s, depending on operating environment and type of terminal	4 Yes. Subclause 7.1
	5 Communication configurations: 5.1 PTP: Point-to-point service bidirectional (Connection Type 1) 5.2 PTM: Point-to-multipoint service (Connection Type 2) 5.2.1 Broadcast 5.2.2 Multicast Capabilities 5.2.2.1 Pre-assigned, i.e. root selected at call setup	5 Yes. Clauses 7 and 8
	6 Communication types: 6.1 CLNS: Connectionless network service 6.2 CONS: Connection-oriented network service	6 Yes. Bearer Capability
	7 Symmetry of access links: 7.1 Symmetric (equal bit rates upstream and downstream) 7.2 Asymmetric (unequal bit rates upstream and downstream)	7 Yes. Bearer Capability
	8 Fixed and variable bit rate traffic	8 Yes. Bearer Capability
	9 Bearer interworking procedures: 9.1 Bearer connection adaptation/conversion 9.2 Bearer, Service component and Teleservice 9.2.1 Mapping 9.2.2 Negotiation 9.2.3 Fallback procedures	9 Not explicitly addressed

Table I.1/Q.1721 – Capability Set 1 for IMT-2000 ***(continued)***

Category	Capabilities	Coverage
D) Access Network Capability – General	1 Support for packet services including: 1.1 Negotiable bit rate of delivery (peak and mean throughput) 1.2 Negotiable delay tolerance 1.3 Negotiable reliability classes (determines the probability of data loss, out of sequence delivery, duplicate delivery and corrupted data)	1 Yes. Clause 8
	2 Support of: 2.1 Constant bit rate with timing: connection-oriented 2.2 Variable bit rate with timing: connection-oriented 2.3 Variable bit rate without timing: connectionless 2.4 Variable bit rate without timing: connection-oriented 2.5 Efficient link layer recovery	2 Yes, Clauses 7, 8; QoS
	3 Radio Resource Control Capabilities: 3.1 Radio channel and Radio environment monitoring and supervision 3.1.1Radio channel quality monitoring 3.1.2Macro diversity monitoring 3.2 Radio resources allocation, deallocation 3.3 Radio-Frequency power Control and setting	3 No. Radio resource management
	4 Support of FWA applications with ISDN-like functionality	4 Not specifically addressed
E) Core Network Capability – General	1 Support of: 1.1 Constant bit rate with timing: connection-oriented 1.2 Variable bit rate with timing: connection-oriented 1.3 Variable bit rate without timing: connectionless 1.4 Variable bit rate without timing: connection-oriented	1 Yes. Clauses 7, 8. QoS and Bearer Capability
	2 Support of both circuit and packet communications for handling voice, data and video simultaneously	2 Yes. Clauses 7 and 8

Table I.1/Q.1721 – Capability Set 1 for IMT-2000 *(continued)*

Category	Capabilities	Coverage
	3 Interworking: 3.1 With ISDN: support of ISDN "like" services at 56 kbit/s, 64 kbit/s, 128 kbit/s, and 144 kbit/s (including D-Channel) 3.2 With B-ISDN CS-2.1 3.3 With X.25 PDN: support PAD access bearer at rates of 300, 1200, 2400, 4800, and 9600 bit/s. Support X.25 packet mode bearer at rates of 2400, 4800, and 9600 bit/s 3.4 With IP networks for user-initiated and network-initiated contexts 3.5 With PSTN (voice, fax, and data via modem)	3 Not explicitly addressed
	4 Mobility: 4.1 Terminal Mobility 4.2 Personal Mobility 4.3 Service Mobility (e.g. Virtual Home Environment)	4 Yes. Clause 6
	5 Internet and Data Applications: 5.1 IMT-2000 shall provide interworking with IP networks (including intranet, IPv4 and IPv6) 5.2 IMT-2000 may provide stand-alone Internet-type services	5 Yes. Subclause 8.5
	6 Global (worldwide) roaming and service interoperability between IMT-2000 Family Members	6 Yes. Clause 6 for roaming and Clause 9 for VHE services
	7 Core Network Transport Capabilities: 7.1 Support of packet-switched and circuit-switched operation 7.2 Support of evolved family member network architecture (PDH/SDH/ATM) 7.3 Support of open interfaces to IN Servers, Dedicated Service Providers Servers	7 Yes. Clauses 7 and 8
F) Network Capabilities – Call Control	1 Separation of call and bearer channel/connection control	1 Yes. Clause 7
	2 Single address/name/directory for a user, to facilitate service transportability. This does not preclude multiple subscriber numbers	2 Not explicitly addressed
	3 Support of IN CS-1/2 to enable access to IN based services	3 Yes. Clause 9
	4 Provision of mobility-enhanced BCSM functionality	4 Yes. Clause 9

Table I.1/Q.1721 – Capability Set 1 for IMT-2000 ***(continued)***

Category	Capabilities	Coverage
	5 Multiple simultaneous calls per terminal or directory number 6 Multimedia mail store and forward 7 Multimedia Calls (see Broadband Signalling Capability Sets 1 and 2.1, including add/drop connection for point-to-point communication configurations, and add/drop party) 8 Call internetworking procedures: 8.1 Belonging to different IMT-2000 Networks (IMT-2000 Family Members internetworking) 8.2 Belonging to IMT-2000 Networks and to Fixed Networks (PSTN, PSDN, (IP)INTERNET, (B)ISDN) 9 Emergency Call: 9.1 Identification of emergency call 9.2 Emergency call handling 9.3 Emergency caller location 10 Priority Call: 10.1 Identification of priority call 10.2 Priority call handling 11 Geographic positioning of a terminal/user: 11.1 Geographic position determination 11.2 Geographic position notification 11.3 User control over subscribed location service information, including the capability to prevent inadvertent disabling of mandatory service location functionality 12 Independence of connection characteristics for multi-connection calls	5 Not explicitly addressed 6 No. Function of an MM FE. 7 Yes. Clause 8 8 Not explicitly addressed 9 Yes. Section 7.6 10 Yes. Section 7.7 11 Yes. Subclause 6.2 12 Yes. Subclause 8.4
G) Network Capabilities – Security Procedures	1 User authentication and ciphering for both circuit and packet modes 2 Terminal identification including the ability to detect stolen and non-type approved terminals 3 User-network mutual authentication 4 Support of service dependent authentication and ciphering mechanisms 5 Control of misuse of a network, i.e. prevent fraudulent use by an unauthorized user or by an authorized user exceeding his authority 6 Ciphering on the radio interface (user and control information) 7 Lawful interception (as applicable per national regulatory requirements)	1 Yes. Subclause 6.1.2 2 Not explicitly addressed 3 Yes. Subclause 6.1.2 4 Not explicitly addressed 5 Not explicitly addressed 6 No. Radio interface matter 7 Not explicitly addressed

Table I.1/Q.1721 – Capability Set 1 for IMT-2000 *(continued)*

Category	Capabilities	Coverage
	8 Privacy of user and subscriber related data (including user identity)	8 Management topic
	9 Privacy of billing data	9 Management topic
	10 Privacy of user messages	10 Management topic
	11 Authentication mechanism negotiation between user, serving and home networks	11 Not explicitly addressed
	12 Event reporting and event limitation to support fraud prevention	12 AMF internal function
H) Network Capabilities – Resource Allocation	1 Allocation based on negotiated QoS	1 Not explicitly addressed
	2 Overload controls	2 Not explicitly addressed
	3 Spectrum-efficient support for mixed services configurations (e.g. low bit rate/high bit rate, real-time/non-real-time services)	3 Radio interface matter
	4 Route optimization at call setup and during a call	4 Not explicitly addressed
I) Network Capabilities – Numbering and Addressing	1 Support of numbering and addressing portability	1 Not explicitly addressed
	2 Identification, Addressing and Numbering Plan:	2 Not explicitly addressed
	2.1 Identity Management	
	2.1.1 Terminal	
	2.1.2 International Mobile User	
	2.1.3 Subscriber ISDN	
	2.1.4 Multicast Group	
	2.2 Support of existing and advanced Addressing and Numbering Plans, including:	
	2.2.1 Recommendation E.164	
	2.2.2 Recommendation E.212	
	2.2.3 Recommendation E.213	
	2.2.4 Recommendation X.121	
	2.2.5 NSAP (Network Service Access Point)	
	2.2.6 IPv4/v6	
	2.2.7 E-mail and Internet type addresses	
	2.2.8 Other mechanisms, e.g. calling by name	
	2.3 Address encapsulation and mapping	
	2.4 Support of Recommendation E.214 (Land Mobile Global Title) addressing	
J) Network Capabilities – Charging and Accounting	These items reflect the choices identified for IMT-2000 charging and accounting.	
	1 Standardized billing and charging user profiles	1 See M.3210
	2 Standardized event reporting and usage detail recording:	2 See M.3210
	2.1 Call detail recording	

Table I.1/Q.1721 – Capability Set 1 for IMT-2000 *(continued)*

Category	Capabilities	Coverage
	2.2 Charging information generation for: 2.2.1 Circuit-switched calls 2.2.2 Packet data transmission sessions 2.2.3 Services realized exclusively by exchanging signalling information 2.2.4 Data transmission on the transparent UIM-Home Network channel	
	3 New charging mechanisms (e.g. volume (number of packets or bytes including by source/destination address pair), QoS, time, etc.)	3 See M.3210
	4 Real-time charging	4 See M.3210
	5 Flexible charging/billing mechanisms: 5.1 User notification of charges before, during and after significant events 5.2 Quasi-real time transmission of usage data records	5 No. Significant unresolved issues in internetwork business arrangements, tariff sharing, currency conversion, accuracy, etc.
	6 Third-party charging (e.g. charging to other parties during multi-party calls)	6 See M.3210
	7 Prepaid billing	7 No: serving network matter
	8 Location-dependent billing and charging	8 See M.3210
	9 Real-time access to billing information	9 See M.3210
K) Network Capabilities – Roaming	1 Interoperability and roaming among IMT-2000 family of systems using a single subscription	1 Yes. Clause 6
	2 Ability to supplement mobility management with IN-type service logic	2 Yes. Clause 9
	3 Ability to supplement authentication control with IN-type service logic. This capability does not include generation of authentication parameters (e.g. triplets)	3 Yes. Clause 9
	4 Mobility and global roaming: 4.1 Location management, including automatic update 4.2 User Registration, Update and Cancellation 4.3 Service Monitoring Registration, Update, Activation, Deactivation and Cancellation 4.4 User Profile Database management and control 4.5 Security and Authentication Database management and control	4 Yes. Clause 6

Table I.1/Q.1721 – Capability Set 1 for IMT-2000 *(continued)*

Category	Capabilities	Coverage
L) Network Capabilities – Service Portability	1 The serving system should be able to enable support of a roaming user's services based on the user profile information 2 Seamless (i.e. transparent to users) service portability with other IMT-2000 networks independent of environment technologies (e.g. cellular, cordless, satellite) 3 Support of Virtual Home Environment to enable a user to be offered the same service experience when roaming as when in the home network, for operator specific services: 3.1 Direct home command 3.2 Relay service control 4 Support of UPT 5 Support of Service profile management 6 Support of standardized supplementary services	1 Yes. Clause 9 2 Yes. Clause 9 3 Yes. Clause 9 4 Not explicitly addressed 5 Yes. Clause 12 6 Yes. Clause 11
M) Network Services/ Features – Handover	1 Intra-Family Member handover is supported 1.1 Support for Hierarchical Cell Structure 1.1.1 Call transfer and handover across cell layers 1.1.2 Location management within multiple cell layers	1 Intra-family matter
N) Network Services/ Features – Service Provisioning	1 Over-the-air service provisioning: 1.1 Support for both voice and data services 1.2 Uploadable and downloadable (e.g. service parameters) 1.3 Support for security and authentication	1 Yes. Clause 12
O) Network Services/ Features – Quality of Service	1 Based on subscription 2 QoS negotiation during service invocation 3 QoS re-negotiation during a service session (e.g. call) 4 QoS of multimedia services as good as on wired access (depending on bearer service classes) 5 Speech quality equivalent to wireline 6 Meet minimum delay requirements (affects signalling timers, etc.)	1 Yes 2 Yes. Clause 7 3 Yes. Subclause 8.1 4 Radio interface matter 5 Radio interface matter 6 Not explicitly addressed
P) Network Services/ Features – Supplemental Support	1 Cordless Telephone Access 2 Virtual private networks 3 Operator support services 4 IP-based services 5 Satellite access: considerations for long link delay, limited power, and bandwidth management 6 Media transparency (i.e. user data delivered unchanged)	1 Not explicitly addressed 2 Not explicitly addressed 3 Not explicitly addressed 4 Yes. Clause 8 5 Not explicitly addressed 6 Not explicitly addressed

Table I.1/Q.1721 – Capability Set 1 for IMT-2000 *(concluded)*

Category	Capabilities	Coverage
Q) Network Services/ Features – Terminals and User Identity Modules (UIM)	1 Network model to support: 1.1 Network with uploading and downloading of user profiles, data information, etc., to support UIM functionality via functional communication channels 1.2 Software configurable terminals, for operational flexibility (e.g. to support pro-active applications) 1.3 Flexible enough to support future enhancements in software-defined radios, for operational flexibility	1 Yes. Clause 12
	2 Mobiles and UIM with downloading capabilities over the air for data and applications. Appropriate procedures should set in place to protect sensitive and confidential information transferred over the air	2 Yes. Clause 12
	3 Multiple calls on a single terminal	3 Not explicitly addressed
	4 Support terminal roaming with removable or integrated UIM and provide information needed from UIM to associate a subscriber with the MT and to personalize the MT	4 Yes. Clause 6
	5 Personal mobility based on a UIM separate from the terminal (IC card)	5 Not explicitly addressed
	6 Multiple registration of one user on several terminals for different services	6 Not explicitly addressed
R) Network Capabilities – Packet Transfer Control	1 Registration/Authentication	1 Yes. Clause 6
	2 Address Assignment: 2.1 Static 2.2 Dynamic	2 Not explicitly addressed
	3 Sleep mode to support battery power conservation	3 Radio interface matter
	4 Optimal packet routing	4 Not explicitly addressed
	5 Multi-protocol support	5 Not explicitly addressed
	6 Data compression	6 Not explicitly addressed
	7 Internetworking (e.g. tunnelling, mobile-IP support)	7 Yes. Clause 8
	8 Location Identification	8 Yes. Clause 6
	9 Load Balancing across RF channels	9 Radio interface matter
	10 Multiple simultaneous address registrations (e.g. IP addresses) on a single terminal	10 Not explicitly addressed
	11 Priority access (for registration and data transfer)	11 Yes. Subclause 7.7
	12 Multimedia sessions	12 Yes. Clause 8

APPENDIX II

A-key generation

II.1 Introduction

Generation of the A-key is supported in OTASP using the public key encryption method. An example of such a method is the Diffie-Hellman public key encryption method, described here. Diffie-Hellman offers certain advantages in that it is publicly available and also scalable, i.e. the various values used in this algorithm may be set by the operator for achieving the desired level of security. The MS and the network establish which set of values is supported for A-key generation, prior to the actual A-key generation process.

II.2 A-key Generation using the Diffie-Hellman Algorithm

In the Diffie-Hellman scheme, the A-key is generated in both the UIMF and the LMFh/AMF using information that is shared between both entities. The LMFh/AMF generates values for a public modulus N and primitive g. The LMFh/AMF generates a secret key, y, which is at least a 160-bit random number. The LMFh/AMF sends to the UIMF: N, g, and Y, where:

$$Y = g^y \text{ Mod } N$$

The UIMF, upon receipt of N, g, and Y, generates a secret key, x, which is at least a 160-bit random number, computes and sends X to the LMFh/AMF, where:

$$X = g^x \text{ Mod } N$$

The A-key in the UIMF is computed as the least significant 64 bits of:

$$Y^x \bmod N = (g^y)^x \bmod N$$

The LMFh/AMF computes the same A-key value as the least significant 64 bits of:

$$X^y \bmod N = (g^x)^y \bmod N$$

After the successful generation of the A-key, the LMFh/AMF and the UIMF exchange confirmations. UIMF generation of x, and LMFh/AMF generation of N, g and y are beyond the scope of this Recommendation. Requirements and properties for generation of these numbers may be obtained from current, publicly available cryptographic literature.

APPENDIX III

Bibliography

The following references are not explicitly used in the body of this Recommendation but provide additional useful background and related information.

[1] ITU-T Recommendation M.3100 (1995), *Generic network information model.*

[2] ITU-R Recommendation M.687-2 (1997), *International Mobile Telecommunications-2000 (IMT-2000).*

[3] ITU-R Recommendation M.816-1 (1997), *Framework for services supported on International Mobile Telecommunications-2000 (IMT-2000).*

[4] ITU-R Recommendation M.817 (1992), *International Mobile Telecommunications-2000. Network architectures.*

[5] ITU-R Recommendation M.818-1 (1993), *Satellite operation within International Mobile Telecommunications-2000 (IMT-2000).*

[6] ITU-R Recommendation M.819-2 (1997), *International Mobile Telecommunications-2000 (IMT-2000) for developing countries*.

[7] ITU-R Recommendation M.1034-1 (1997), *Requirements for the radio interface(s) for International Mobile Telecommunications-2000 (IMT-2000).*

[8] ITU-R Recommendation M.1035 (1993), *Framework for the radio interface(s) and radio sub-system functionality for International Mobile Telecommunications-2000 (IMT-2000).*

[9] ITU-R Recommendation M.1078 (1993), *Security principles for International Mobile Telecommunications-2000 (IMT-2000).*

[10] ITU-R Recommendation M.1167 (1995), *Framework for the satellite component of International Mobile Telecommunications-2000 (IMT-2000).*

[11] ITU-R Recommendation M.1168 (1995), *Framework of International Mobile Telecommunications-2000 (IMT-2000).*

[12] ITU-R Recommendation M.1223 (1997), *Evaluation of security mechanisms for IMT-2000.*

[13] ITU-R Recommendation ITU-R M.1224 (1997), *Vocabulary of terms for International Mobile Telecommunications-2000 (IMT-2000).*

[14] ITU-T Recommendation F.115 (1995), Service objectives and principles for future public land mobile telecommunication systems.

[15] ITU-T Recommendation F.116 (2000), *Service features and operational provisions in IMT-2000.*

[16] ITU-T Recommendation F.700 (2000), *Framework Recommendation for multimedia services.*

[17] ITU-T Recommendation I.211 (1993), *B-ISDN service aspects.*

[18] ITU-T Recommendation I.374 (1993), *Framework Recommendation on "Network capabilities to support multimedia services". (Withdrawn in 1998 – replaced by I.375.1 and I.375.2.)*

[19] ITU-T Recommendation Q.1001 (1988), *General aspects of public land mobile networks.*

[20] ITU-T Recommendation Q.1290 (1998), *Glossary of terms used in the definition of intelligent networks.*

[21] ITU-R Recommendation M.1311 (1997), *Framework for modularity and radiocommonality within IMT-2000.*

[22] ITU-T Recommendation E.214 (1988), *Structure of the land mobile global title for the signalling connection control part (SCCP).*

[23] ITU-R Recommendation M.1457 (2000), *Detailed specifications of the radio interfaces of International Mobile Telecommunications-2000 (IMT-2000).*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

Geneva, 2001