UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Q.1721

(06/2000)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Q: CONMUTACIÓN Y SEÑALIZACIÓN

Requisitos y protocolos de señalización para IMT-2000

Flujos de información para el conjunto de capacidades 1 de IMT-2000

Recomendación UIT-T Q.1721

(Anteriormente Recomendación del CCITT)

RECOMENDACIONES UIT-T DE LA SERIE Q

CONMUTACIÓN Y SEÑALIZACIÓN

SEÑALIZACIÓN EN EL SERVICIO MANUAL INTERNACIONAL	Q.1–Q.3
EXPLOTACIÓN INTERNACIONAL SEMIAUTOMÁTICA Y AUTOMÁTICA	Q.4–Q.59
FUNCIONES Y FLUJOS DE INFORMACIÓN PARA SERVICIOS DE LA RDSI	Q.60–Q.99
CLÁUSULAS APLICABLES A TODOS LOS SISTEMAS NORMALIZADOS DEL UIT-T	Q.100–Q.119
ESPECIFICACIONES DE LOS SISTEMAS DE SEÑALIZACIÓN N.° 4 Y N.° 5	Q.120–Q.249
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.° 6	Q.250–Q.309
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN R1	Q.310–399
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN R2	Q.400–Q.499
CENTRALES DIGITALES	Q.500–Q.599
INTERFUNCIONAMIENTO DE LOS SISTEMAS DE SEÑALIZACIÓN	Q.600–Q.699
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.º 7	Q.700–Q.849
SISTEMA DE SEÑALIZACIÓN DIGITAL DE ABONADO N.º 1	Q.850–Q.999
RED MÓVIL TERRESTRE PÚBLICA	Q.1000–Q.1099
INTERFUNCIONAMIENTO CON SISTEMAS MÓVILES POR SATÉLITE	Q.1100–Q.1199
RED INTELIGENTE	Q.1200–Q.1699
REQUISITOS Y PROTOCOLOS DE SEÑALIZACIÓN PARA IMT-2000	**Q.1700–Q.1799**
RED DIGITAL DE SERVICIOS INTEGRADOS DE BANDA ANCHA (RDSI-BA)	Q.2000–Q.2099

Para más información, véase la Lista de Recomendaciones del UIT-T.

RECOMENDACIÓN UIT-T Q.1721

FLUJOS DE INFORMACIÓN PARA EL CONJUNTO DE CAPACIDADES 1 DE IMT-2000

Resumen

En esta Recomendación se especifican los procedimientos asociados a los flujos de información de la etapa 2 para soportar las capacidades de red y de servicios del conjunto de capacidades 1 (CS-1) de IMT-2000 extremo a extremo entre sistemas y entre familias. Abarca los aspectos relativos a gestión de la movilidad, control de llamada y de portador, control de servicio y servicios de autorización por medios radioeléctricos.

Orígenes

La Recomendación UIT-T Q.1721 ha sido preparada por la Comisión de Estudio 11 (1997-2000) del UIT-T y fue aprobada por el procedimiento de la Resolución 1 de la CMNT el 15 de junio de 2000.

Palabras clave

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

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Conferencia Mundial de Normalización de las Telecomunicaciones (CMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la CMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Página

Recomendación Q.1721

FLUJOS DE INFORMACIÓN PARA EL CONJUNTO DE CAPACIDADES 1 DE IMT-2000

1 Ámbito

Esta Recomendación proporciona los flujos de información entre familias extremo a extremo de la etapa 2 para las capacidades de red y de servicios del conjunto de capacidades 1 (CS-1, *capability set*) del IMT-2000. La especificación se realiza conforme a la metodología de la etapa 2 descrita en la Recomendación UIT-T Q.65 [1]. Las Recomendaciones UIT-T conexas Q.1701 [2] y Q.1711 [3], constituyen la base para esta Recomendación. En su conjunto, estas Recomendaciones forman una descripción de etapa 2 que identifica la capacidad funcional y los flujos de información necesarios para soportar las capacidades de red y los servicios IMT-2000 de la etapa 1.

Esta Recomendación incluye los flujos de información para la interfaz entre el módulo de identidad de usuario (UIM, *user identity module*) y el terminal móvil (MT, *mobile terminal*), la interfaz entre el terminal móvil (MT) y la red de acceso radioeléctrico + la red central (RAN+CN, *radio access network + core network*) y la interfaz entre redes medulares (de CN a CN) [también conocida como interfaz red-red (NNI, *network-to-network interface*)]. Los flujos de información descritos sólo abarcan los casos llevados a cabo con éxito. Los casos sin éxito quedan fuera del ámbito de esta Recomendación y se manejan de forma más adecuada como parte del desarrollo de la etapa 3. Las Recomendaciones conexas de la serie Q, Q.1731, Q.1741 y Q.1751, complementan la visión extremo a extremo de la Recomendación Q.1721 tratando aspectos específicos de dichas interfaces.

Esta Recomendación no incluye los flujos de información relativos a la gestión de recursos radioeléctricos (RRM, *radio resource management*), a la gestión de la estación base (BSM, *base station management*) o entre la red de acceso radioeléctrico y la red medular (RAN-CN). La RRM se trata en otro lugar. Los flujos de información de BSM y de RAN-CN quedan fuera del ámbito del CS-1 de la IMT-2000 según 8.1/Q.1701.

En los párrafos siguientes se presenta una somera visión general de cada una de las cláusulas de esta Recomendación.

Las cláusulas 2, 3 y 4 proporcionan referencias, definiciones y una lista de abreviaturas y acrónimos relevantes para esta Recomendación.

La cláusula 5, "Introducción," proporciona el contexto de toda la Recomendación. Incluye la arquitectura general del protocolo, la identificación de los modelos funcionales de la Recomendación Q.1711, un modelo de red extremo a extremo, los tipos de secuencias de información y la plantilla del flujo de información.

La cláusula 6, "Gestión de la movilidad," describe los flujos de información para la gestión de la autenticación, incluida la verificación del titular del módulo de identidad de usuario (UIM), la autenticación del usuario y de la red y la identificación del terminal. Se ocupa de la gestión de ubicaciones, incluyendo el posicionamiento geográfico, la gestión de los datos del abonado, la interrogación del perfil de usuario, la recuperación de la identidad, la gestión del registro y la recuperación de fallos de los datos de ubicación.

La cláusula 7, "Control de llamada y de portador," describe las llamadas entrante y saliente de móviles, incluyendo la radiobúsqueda del terminal, el encaminamiento, las llamadas de emergencia y las llamadas con prioridad.

La cláusula 8, "Control de la llamada multimedios y del portador" describe los flujos de información y los procedimientos para el cambio de teleservicio durante una llamada (conmutación entre comunicación de voz y de datos), añadiendo o eliminando un medio durante una llamada y cambiando la configuración de la comunicación mediante la adición o supresión de una parte en una llamada de datos. En esta cláusula también se trata del acceso a Internet.

La cláusula 9, "Entorno originario virtual," proporciona los flujos de información de los métodos instrucción originaria directa (DHC, *direct home command*) y de control de servicio de retransmisión (RSC, *relay service control*). (La utilización de la red inteligente para soportar servicios suplementarios en una red queda fuera del ámbito de esta Recomendación.)

La cláusula 10, "Aplicaciones de servicios de mensajería," describe los flujos de información y procedimientos de los servicios de mensajes cortos, de la difusión de mensajes de teleservicios y de notificación de mensaje en espera.

La cláusula 11, "Procedimientos relativos a los servicios suplementarios," proporciona los flujos de información para un conjunto de procedimientos de propósito general que pueden ser utilizados por varios servicios suplementarios.

La cláusula 12, "Servicios por medios radioeléctricos," describe los flujos de información de los procedimientos de provisión de servicios por medios radioeléctricos.

La cláusula 13, "Definiciones de elementos de información," define el significado de los diversos elementos de información utilizados en esta Recomendación .

El anexo A proporciona una lista de todos los módulos de procedimiento común utilizados en esta Recomendación y el número de la cláusula en la que se describen.

El apéndice I, "Cobertura Q.1721 del cuadro 1/Q.1701, Requisitos del conjunto de capacidades 1," proporciona el vínculo entre el cuadro 1/Q.1701, las capacidades requeridas por el conjunto de capacidades 1 del IMT-2000 y el contenido de esta Recomendación.

El apéndice II, "Generación de la clave A," proporciona una somera descripción general sobre este asunto, incluyendo el algoritmo Diffie-Hellman.

El apéndice III, "Bibliografía," proporciona una lista de referencias adicionales que complementan las referencias específicas que se enumeran en la cláusula 2.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes.

[1] Recomendación UIT-T Q.65 (2000), *Metodología funcional modificada para la caracterización de servicios y capacidades de red, incluyendo técnicas alternativas orientadas al objeto.*

[2] Recomendación UIT-T Q.1701 (1999), *Marco para las redes de telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[3] Recomendación UIT-T Q.1711 (1999), *Modelo funcional de red para las redes de telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[4] Recomendación UIT-T A.3 (1996), *Elaboración y presentación de textos, terminología y otros medios de expresión para las Recomendaciones del Sector de Normalización de las Telecomunicaciones de la UIT.*

[5] Recomendaciones UIT-T de la serie Q.1200, *Redes inteligentes.*

[6] Recomendación UIT-T E.164 (1997), *Plan internacional de numeración de telecomunicaciones públicas*.

[7] Recomendación UIT-T E.212 (1988), *Plan de identificación de estaciones móviles terrestres.*

[8] Recomendación UIT-T E.213 (1988), *Plan de numeración de las redes telefónicas y digital de servicios integrados para estaciones móviles terrestres de redes móviles terrestres públicas.*

[9] Recomendación UIT-T X.121 (1996), *Plan de numeración internacional para redes públicas de datos.*

[10] Recomendación UIT-T Q.931 (1998), *Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de la llamada básica.*

[11] Recomendación UIT-T Q.762 (1997), *Sistema de señalización N.º 7 – Funciones generales de los mensajes y señales de la parte usuario de la RDSI.*

3 Definiciones

En esta Recomendación se definen los términos siguientes.

3.1 red medular de anclaje: En un entorno de itinerancia de la sesión de datos, la red medular de anclaje es la red en la que se inicia la sesión de datos y en la que se asigna al terminal móvil una pasarela del servicio de paquetes. La red medular de anclaje puede ser la red originaria o la red visitada.

3.2 interfaz hombre máquina: Interacción entre usuario y red a través de una dispositivo del abonado.

3.3 indicación de petición: flujo de información enviado desde una entidad funcional a otra solicitando una acción específica. Se hace referencia a ella como ind.pet.

3.4 confirmación de respuesta: Flujo de información enviado por la funcionalidad solicitada confirmando que la acción solicitada se ha completado con éxito. Se hace referencia a ella como conf.resp.

3.5 aplicación de servicio: Provisión de servicios por parte de las capacidades de propósito general, tales como capacidades de red inteligente tal como se aplican a la ubicación originaria o a la ubicación visitada como parte de un entorno originario virtual.

3.6 control del servicio: Funciones que fijan o modifican el contexto, en el que se establecen, modifican y liberan llamadas y portadores básicos.

3.7 abonado: Usuario de un terminal móvil que se ha suscrito al servicio.

3.8 aplicación de servicio suplementario: Provisión de un servicio suplementario específico, típicamente a través de la utilización de capacidades específicas del servicio, ya sea en la ubicación originaria o visitada como parte de un entorno originario virtual.

3.9 usuario: Usuario de un terminal móvil.

3.10 entorno originario virtual: Provisión al abonado de una experiencia de servicio idéntica o tan parecida como sea posible al entorno de servicio que experimenta cuando es atendido en su ubicación originaria.

NOTA 1 – Los términos "usuario" y "abonado" se utilizan indistintamente en esta Recomendación.

NOTA 2 – Red originaria es sinónimo de red medular originaria (CNh, *home core network*).

NOTA 3 – Red visitada es sinónimo de red medular visitada (CNv, *visited core network*).

La cláusula 13, "Definiciones de elementos de información," define el significado de los diversos elementos utilizados en esta Recomendación.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes siglas.

AC Centro de autenticación (*authentication centre*)

ACSM Modelo de estado del control de autenticación (*authentication control state model*)

ADDS Servicio de entrega de datos de aplicación (*application data delivery service*)

A-key Clave de autenticación (*authentication key*)

AMF Función de gestión de autenticación (*authentication management function*)

AMSC Centro de conmutación móvil de anclaje (*anchor mobile switching centre*)

AMSM Modelo de estado de la gestión de autenticaciones (*authentication management state model*)

ARF Función de relevo de enlace de acceso (*access link relay function*)

AUTH Respuesta de autenticación (*authentication response*)

BCSM Modelo de estados de llamada básica (*basic call state model*)

BS Estación base (*base station*)

CC Control de llamada (*call control*)

CCAF' Función de agente de control de llamada (potenciada) [*call control agent function (enhanced*)]

CCF' Función de control de llamada (*call control function*)

CCF Función de control de llamada (potenciada) [*call control function* (*enhanced*)]

CHCNT Cómputo histórico de la llamada (*call history count*)

CN Red medular (*core network*)

CNa Red medular (anclada) [*core network* (*anchored*)]

CNdest Red medular (destino) [*core network* (*destination*)]

CNh Red medular (originaria) [*core network* (*home*)]

CNpv Red medular (previamente visitada) [*core network* (*previous visited*)]

CNs Red medular (soporte) [(*core network* (supporting)])

CNv Red medular (visitada) [*core network* (*visited*)]

CnCAF Función de agente de control de conexión (*connection control agent function*)

CnCF Función de control de conexión (*connection control function*)

conf. Confirmación

CS Conjunto de capacidades (*capability set*)

DFP Plano funcional distribuido (*distributed functional plane*)

DHC	Instrucción originaria directa (*direct home command*)
FE	Entidad funcional (*functional entity*)
FEA	Acción de entidad funcional (*functional entity action*)
FT	Terminal fijo (*fixed terminal*)
GC	Mecanismo global de puesta a prueba/respuesta (*global challenge/response mechanism*)
GPCF	Función de control de posición geográfica (*geographic position control function*)
GPF	Función posición geográfica (*geographic position function*)
ID	Identidad
IF	Flujo de información (*information flow*)
IMT-2000	Telecomunicaciones móviles internacionales-2000 (*International Mobile Telecommunications-2000*)
IMUI	Identidad de usuario móvil internacional (*international mobile user identity*)
ind.	Indicación
IP	Protocolo Internet (*Internet protocol*)
ISP	Proveedor de servicio Internet (*Internet service provider*)
ITDN	Número temporal internacional de directorio (*international temporary directory number*)
LMF	Función de gestión de ubicaciones (*location management function*)
LMFh	Función de gestión de ubicaciones (originarias) [*location management function* (*home*)]
LMFp	Función de gestión de ubicaciones (paquetes) [*location management function* (*packet*)]
LMFv	Función de gestión de ubicaciones (visitadas) [*location management function* (*visited*)]
LMSM	Modelo de estado de gestión de ubicaciones (*location management state model*)
MCF	Función de control de móvil (*mobile control function*)
MGPF	Función de posición geográfica de móvil (*mobile geographic position function)*
MMI	Interfaz-hombre máquina (*man-machine interface*)
MRTR	Transmisión y recepción radioeléctrica móvil (*mobile radio transmission and reception*)
MSC	Centro de conmutación de servicios móviles (*mobile switching centre*)
MT	Terminal móvil (*mobile terminal*)
MWN	Notificación de mensaje en espera (*message waiting notification*)
NAI	Identificador de acceso a red (*network access identifier*)
NNI	Interfaz red-red (*network-to-network interface*)
OTASP	Provisión de servicio por medios radioeléctricos (*over-the-air service provisioning*)
PDGN	Nodo pasarela de datos por paquetes (*packet data gateway node*)
PDSN	Nodo servidor de datos por paquetes (*packet data serving node*)
pet.	Petición
PIN	Número de identificación personal (*personal identification number*)
PSCF	Función de control de servicio de paquetes (*packet service control function*)

PSCAF Función de agente de control de servicio de paquetes (*packet service control agent function*)

PSGCF Función de control de pasarela de servicio de paquetes (*packet service gateway control function*)

QoS Calidad de servicio (*quality of service*)

RACAF Función de agente de control de acceso radioeléctrico (*radio access control agent function*)

RAN Red de acceso radioeléctrico (*radio access network*)

RAND Número aleatorio (*random number*)

RANDC Número aleatorio (puesta a prueba) [*random number (challenge*)]

RANDG Número aleatorio (global) [*random number (global*)]

RDP Red pública de datos

resp. Respuesta

RF Radiofrecuencia

RFTR Transmisión y recepción en radiofrecuencia (*radio frequency transmission and reception)*

RI Red inteligente

RNC Controlador de red radioeléctrica (*radio network controller*)

RSC Retransmisión del control del servicio (*relay service control*)

SACF Función de control de acceso al servicio (*service access control function*)

SCF Función de control de servicio (*service control function*)

SCP Punto de control de servicio (*service control point*)

SDF Función de datos de servicio (*service data function*)

SDP Punto de datos de servicio (*service data point)*

SIBF Función de difusión de información de acceso al sistema (*system access information broadcast function*)

SLP Programa lógico de servicio (*service logic program*)

SMF Función de gestión de servicio (*service management function*)

SMS Servicio de mensajes cortos (*short message service*)

SNCF Función de control de red de satélite (*satellite network control function*)

SPI Índice de parámetro de seguridad (*security parameter index*)

SRES Resultado de signatura (*signature result*)

SRF Función de recursos especializados (*specialized resource function*)

SSD Dato secreto compartido (*shared secret data*)

SSF Función de conmutación de servicio (*service switching function*)

TMB Difusión de mensaje de teleservicio (*teleservice message broadcast*)

TMUI Identificador temporal de usuario móvil (*temporary mobile user identifier*)

UC Mecanismo singular de puesta a prueba/respuesta (*unique challenge/response mechanism*)

UIM Módulo de identidad de usuario (*user identity module*)

UIMF Función de gestión de identificación de usuario (*user identification management function*)

UPT Telecomunicaciones personales universales (*universal personal telecommunications*)

USSD Datos de servicio suplementario no estructurado (*unstructured supplementary service data*)

VHE Entorno originario virtual (*virtual home environment*)

5 Introducción

Esta Recomendación describe los flujos de información de los procedimientos extremo a extremo entre familias de la IMT-2000, necesarios para soportar los servicios y capacidades de red CS-1 de IMT-2000. La descripción de los flujos de información incluye la lista de elementos de información que se intercambian entre las entidades funcionales que interactúan. También se describen las acciones de entidad funcional (FEA, *functional entity actions*) que realizan la entidad receptora.

Las técnicas de modelado utilizadas para describir los flujos de información de los procedimientos IMT-2000 se describen en las cláusulas siguientes.

Los flujos de información que se describen en esta Recomendación para los diversos servicios y capacidades de red de IMT-2000 controlan muchos aspectos de la red IMT-2000 para lo que es necesario especificar los requisitos de señalización y de protocolo siguientes:

- Control del servicio, incluyendo:
  - servicios multimedios;
  - entorno originario virtual (VHE, *virtual home environment*);
  - servicios de mensajería; y
  - servicios suplementarios.
- Gestión de la movilidad y control de autenticación.
- Control de llamada.
- Control del portador.

Esta Recomendación no se ocupa de la gestión de los recursos radioeléctricos.

En el anexo A se enumeran los módulos de procedimientos comunes. Estos módulos básicos se reutilizan en diversas tareas que se componen de dichos procedimientos básicos y de otros procedimientos específicos de dichas tareas.

En la presente Recomendación se ha aplicado el principio fundamental de la "separación de responsabilidades." Una separación estricta permite la independencia funcional y de protocolo de cada una de las áreas consideradas, asegurando así que cada una de ellas puede evolucionar y proporcionar más capacidades sin tener que modificar otras áreas simultáneamente.

La figura 5.1 identifica, en el marco de las redes IMT-2000 especificadas de acuerdo con la Recomendación Q.1701, los límites en los que se han aplicado dichas separaciones a fin de orientar el desarrollo de los requisitos de señalización y de protocolo de IMT-2000.

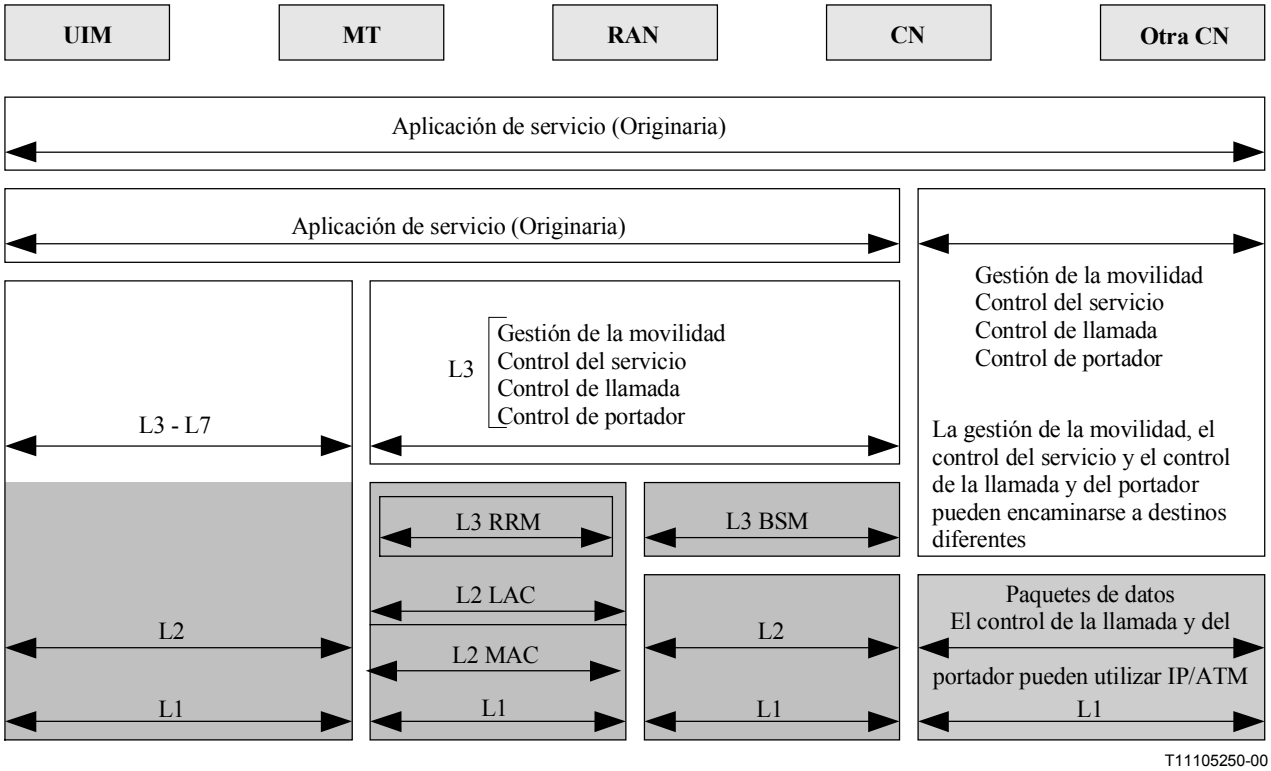


Figura 5-1/Q.1721 – Arquitectura general de los flujos de información

5.1 Descripción de las técnicas de modelado de flujos de información

En esta subcláusula se proporcionan dos modelos funcionales que se especifican en la Recomendación UIT-T Q.1711 [3], que son el "Modelo de control de llamada y de conexión integrados" y el "Modelo de control de llamada y de conexión separados". Además, en esta subcláusula también se define un modelo de la relación extremo a extremo del subsistema.

5.1.1 Modelos funcionales

La figura 5.1.1-1 es idéntica a la figura 5-1a/Q.1711 y constituye un modelo funcional de IMT-2000 que ilustra una entidad funcional (FE, *functional entity*) de control de llamada y de control de conexión integradas. Para más información véase la cláusula 6/Q.1711.

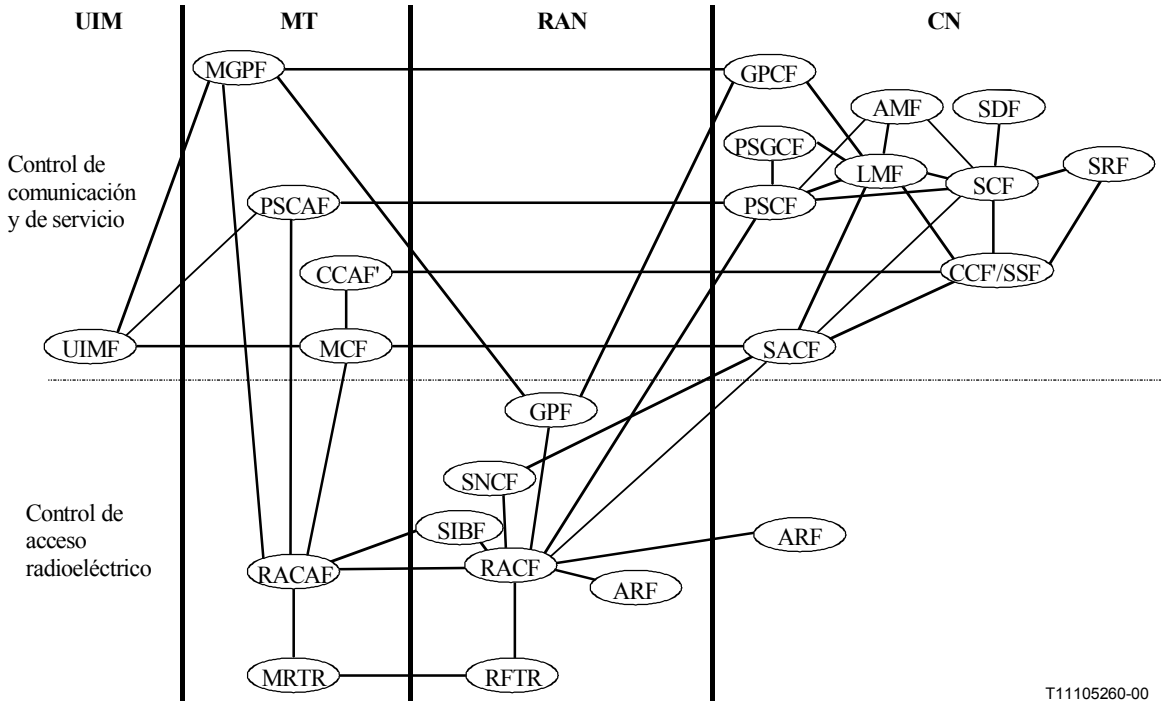


Figura 5.1.1-1/Q.1721 – Modelo funcional de IMT-2000 (control de llamada y control de conexión integrados)

La figura 5.1.1-2 es idéntica a la figura 5-1b/Q.1711, siendo un modelo funcional IMT-2000 que ilustra las FE de control de llamada y de control de conexión separados. Para más información, véase la cláusula 6/Q.1711.

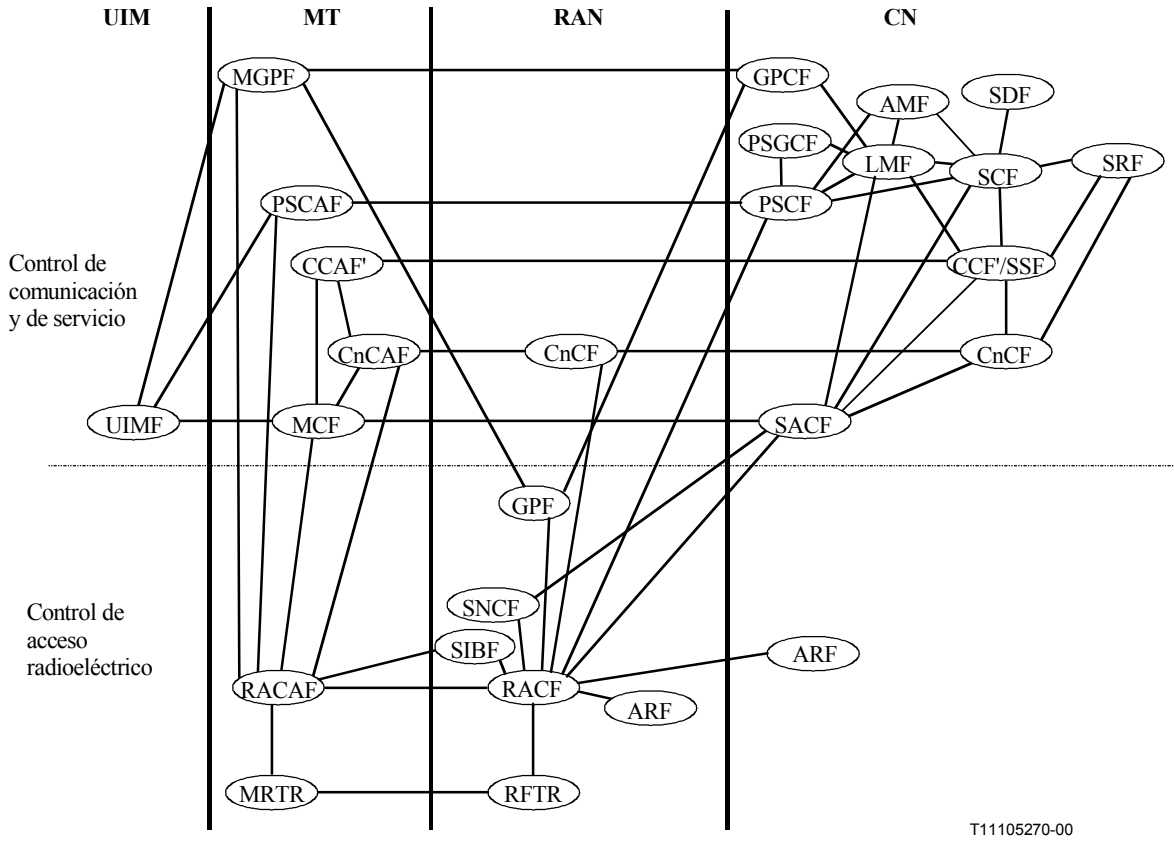
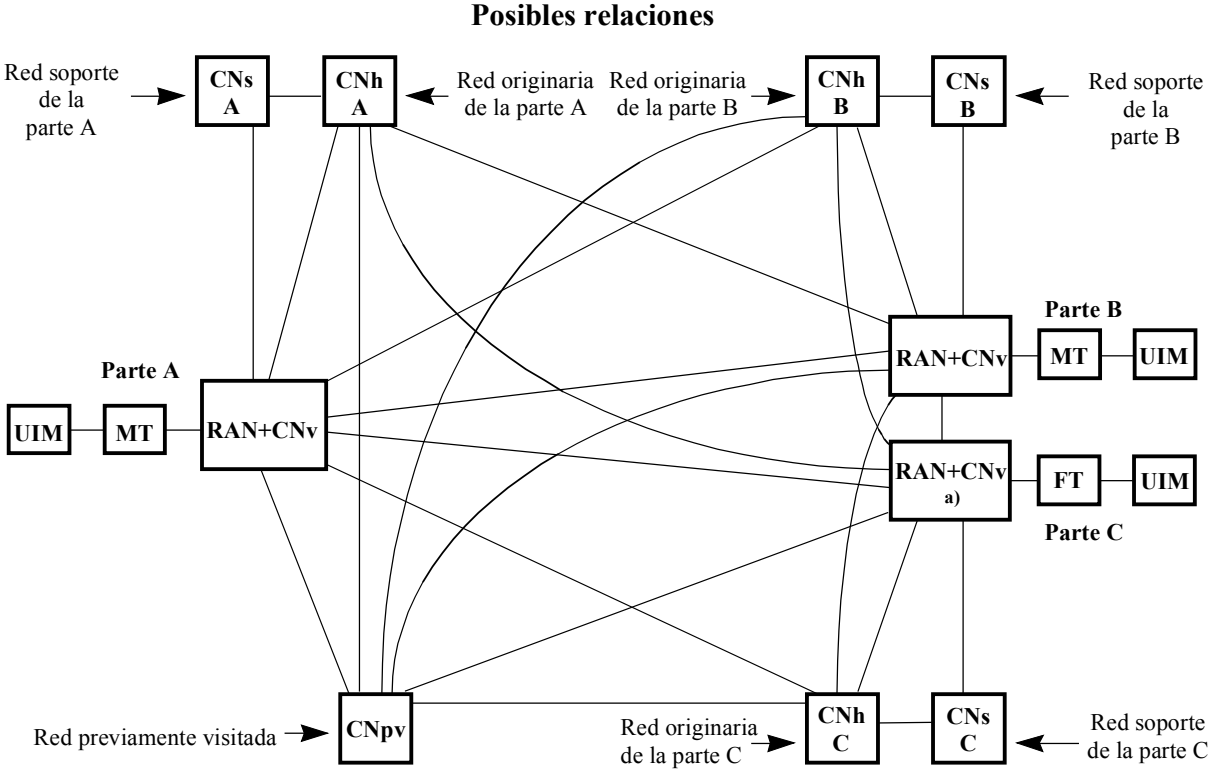


Figura 5.1.1-2/Q.1721 – Modelo funcional de IMT-2000 (control de llamada y control de conexión separadas)

Debe señalarse que la correspondencia entre las FE y los subsistemas UIM, MT, RAN y CN, tal como se define en Q.1701, se muestra también en los modelos a fin de reflejar la aplicabilidad del concepto de familia de sistemas IMT-2000. Asimismo, debe señalarse que la atribución de las FE a los subsistemas RAN y CN es preliminar (para más información véase Q.1711).

5.1.2 Modelo de relaciones entre subsistemas extremo a extremo

El modelo funcional de relaciones de red extremo a extremo ilustra la perspectiva de red a través de los subsistemas funcionales (FS, *functional subsystems*) definidos en Q.1701 y Q.1711 (es decir, UIM, MT, RAN y CN) y sus asociaciones con múltiples usuarios. Tal como se ilustra en la figura 5.1.2-1, el modelo de red extremo a extremo contiene tres puntos de usuario extremo. Ello se utiliza para ilustrar servicios más avanzados tales como la llamada en conferencia y el establecimiento simultáneo de servicios portadores punto-multipunto.



RAN+CN	Red de acceso radioeléctrico + red principal visitada
UIM	Módulo de identidad del usuario
MT	Terminal móvil
CNpv	Red medular previamente visitada
CNh	Red medular originaria
CNs	Red medular soporte
FT	Terminal fijo

a) Este subsistema funcional puede ser sustituido por otros subsistemas de red para ilustrar el interfuncionamiento con otras redes tales como la RTPC, RDSI, etc.

Figura 5.1.2-1/Q.1721 – Modelo de relaciones extremo a extremo de subsistemas del IMT-2000

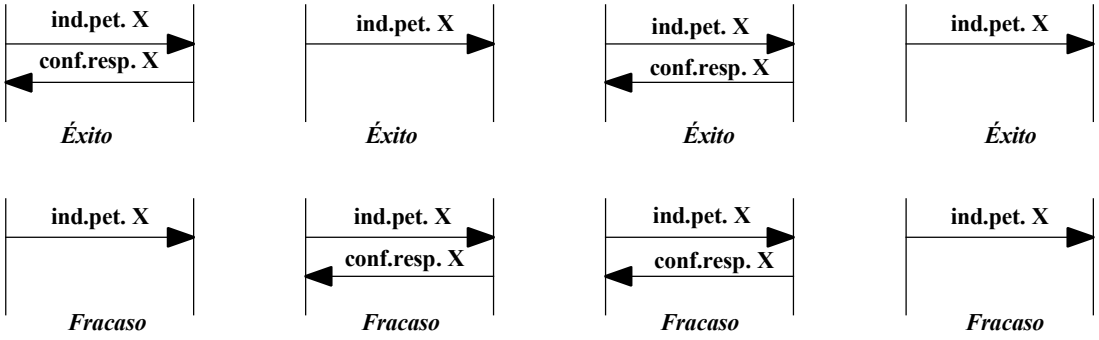
La red principal puede tener distintos cometidos:

- CNpv = red central (previamente visitada): entidad de red que estuvo anteriormente asociada con el terminal móvil visitado.
- CNh = red central (originaria): donde se encuentran la función de gestión de ubicación originaria (LMFh, *home location management function*) y la función de gestión de autenticación (AMFh, *home authentication management function*).
- CNs = red central (red soporte): donde se encuentran la función de control del servicio originaria (SCFh, *home service control function*), la función de datos de servicio originaria (SDFh, *home service data function*), y la función de recursos especializados originaria (SRFh, *home specialized resource function*).

5.1.3 Tipos de secuencias de flujos de información

Un flujo de información consta de dos partes: el nombre de la función del flujo de información y el tipo de secuencia de flujo. La figura 5.1.3-1 ilustra los tipos de actuación posibles.

Tipo I de secuencia de flujo	Tipo II de secuencia de flujo	Tipo III de secuencia de flujo	Tipo IV de secuencia de flujo
(éxito confirmado: no se informa de fracaso)	(fracaso confirmado: no se informa de éxito)	(éxito o fracaso confirmado: no se informa de lo que corresponda)	(no confirmado: no se informa de éxito ni de fracaso)



NOTA – "X" representa el nombre de la función de flujo de información, mientras que ind.pet. (indicación de petición) es un ejemplo de un tipo que puede asociarse con el nombre de la función de flujo.

T11105290-00

Figura 5.1.3-1/Q.1721 – Tipos de secuencias de flujo de información

La figura anterior ilustra cuatro tipos de secuencias de flujos de información. Cada tipo describe los flujos de información específicos que lo constituyen. El primer tipo es una secuencia de flujo de información cliente-servidor, siendo el resultado éxito confirmado y no confirmándose el fracaso. El segundo tipo es también una secuencia de flujo de información cliente-servidor, pero en este caso el resultado es un fracaso confirmado y el éxito no se confirma. El tercer tipo es una notificación confirmada de éxito o fracaso, según corresponda. El cuarto tipo es una notificación no confirmada.

El flujo "conf.resp." es respuesta a un flujo "ind.pet." previo y, como tal transporta una "ID de transacción" exclusiva asociada al mismo. Esta "ID de transacción" se utiliza para vincular cada pareja de flujos "ind.pet." y "conf.pet.". Por lo tanto, en el flujo "conf.resp." no es necesario repetir ninguna identificación de usuario tal como la identidad de usuario móvil internacional IMT-2000 (IMUI, *international mobile user identity*) o el número de directorio móvil internacional IMT-2000 (IMDN, *international mobile directory number*).

5.2 Plantilla de los flujos de información

En esta subcláusula se describe la plantilla utilizada para el desarrollo de procedimientos de flujo de información (IF, *information flow*).

X.Y.Z "Nombre del procedimiento (por ejemplo, registro de la ubicación del terminal)"

En esta cláusula se hace una breve descripción literal del servicio o de la capacidad de red. "X.Y.Z." es el número de subcláusula en Q.1721. Esta subcláusula contiene un diagrama de información detallada para el servicio o la capacidad de red que utiliza la plantilla que se proporciona a continuación. Véase la figura 5.2-1.

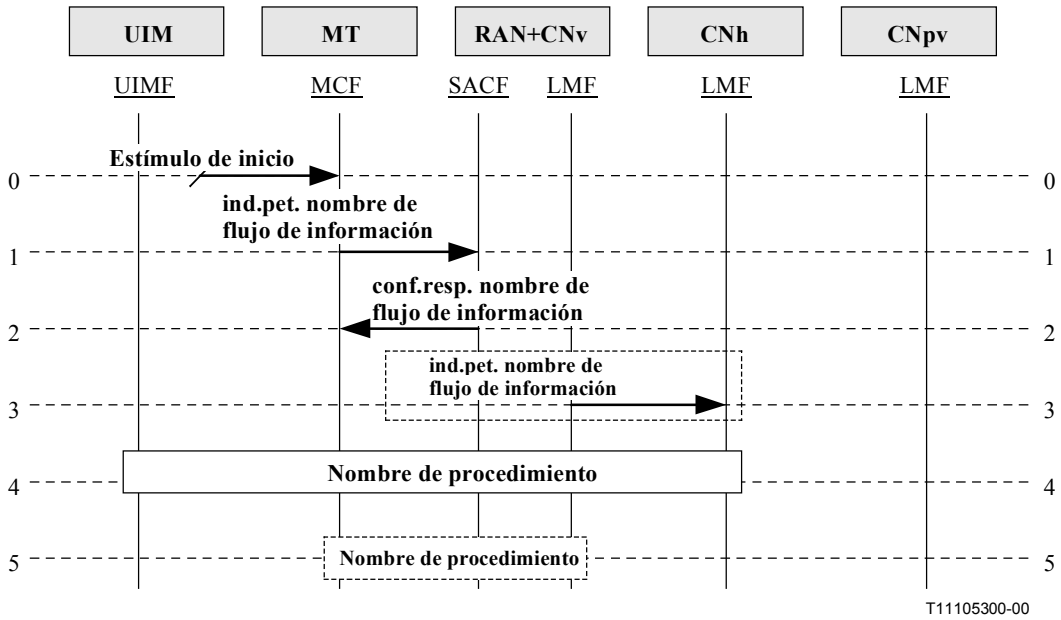


Figura 5.2-1/Q.1721 – Plantilla de diagrama de flujo de información IMT-2000

Esta subcláusula consta de párrafos, cada uno de los cuales está dedicado a un flujo de información del diagrama del IF. Para cada flujo de información se proporciona una descripción detallada del nombre del flujo de información, el tipo (por ejemplo, ind.pet. o conf.resp.), los elementos de información (IE, information element) del flujo de información y una indicación sobre si el elemento de información (IE) es obligatorio u opcional (M/O) en la secuencia, tal como se muestra en el diagrama IF. En esta cláusula también se proporcionan las acciones de los elementos funcionales (FEA). Para cada entidad que recibe un flujo se asumen actuaciones comunes tales como "recepción y análisis de un flujo" y "generación del flujo siguiente " y, por lo tanto, no están incluidas en la descripción de las FEA. El formato utilizado en esta subcláusula es el siguiente:

0. **Flujo de información inicial**: *Describe la acción de FE inicial que da lugar al primer IF (flujo #1).*

FEA0	– Describe la acción FE en el extremo receptor de este flujo.

1. **Flujo de información #1, nombre de flujo, tipo de secuencia de flujo**: *Breve descripción del flujo y de sus FE de inicio y de fin, a los que deben atenerse el contenido de los elementos de información del flujo, tal como se muestra en el cuadro siguiente. Cuando un IE es "O"(opcional), deben especificarse las condiciones para su inclusión así como la respuesta a su presencia cuando se reciba, por ejemplo, incluir IE #2 cuando tenga lugar la condición xyz. Los IF del tipo ind.pet. identifican si es necesaria una respuesta en base al resultado del IF recibido, ya sea resultado con éxito, fracaso, ambos o ninguno; por ejemplo, "Respuesta: éxito o fracaso".*

Nombre del flujo de información (Respuesta: éxito/fracaso/éxito o fracaso/ninguno)	ind.pet.
IE #1 (por ejemplo, identidad de usuario llamado)	M/O
IE #2	M/O
IE #3	M/O

FEA1	– Descripción de la acción o acciones de la entidad funcional en el extremo receptor de este flujo.
NOTA – Describe las condiciones del carácter facultativo de los IE que son opcionales.	

2. **Flujo de información #2, nombre de flujo, tipo de flujo**: *Breve descripción del flujo y de sus FE extremos, a la que debe atenerse el contenido de los elementos de información del flujo, tal como se indica a continuación. Cuando un IE es "O" (opcional), deben especificarse las condiciones para su inclusión, así como la respuesta a su presencia cuando sea recibido. Por ejemplo, cuando se recibe el IE #6, se ejecuta wxy. En el caso de conf.resp., no se aplica la indicación de respuesta.*

Nombre de flujo de información	conf.resp.
IE #4	M/O
IE #5	M/O
IE #6	M/O

FEA2	– Descripción de la acción o acciones de la entidad funcional en el extremo receptor de este flujo.
NOTA – Describe las condiciones del carácter facultativo de los IE que son opcionales.	

3. **Flujo de información #3, nombre de flujo, tipo de secuencia de flujo**: *Breve descripción del flujo y de sus FE de inicio y de final a que debe atenerse el contenido de los elementos de información del flujo, tal como se muestra a continuación. Cuando un IE es "O" (opcional), deben especificarse las condiciones de su inclusión cuando se recibe, así como la respuesta a su presencia, por ejemplo, se incluye IE #2 cuando se produce la condición xyz. En el caso de IF del tipo ind.pet. se indica si se precisa respuesta en base al resultado del IF recibido, según sea éxito, fracaso, ambos o ninguno. Por ejemplo, "Respuesta: éxito o fracaso".*

Nombre de flujo de información (Respuesta: éxito/fracaso/éxito o fracaso/ninguno)	ind.pet.
IE #1	M/O
IE #2	M/O
IE #3	M/O

FEA3	– Descripción de la acción o acciones de la entidad funcional en el extremo receptor de este flujo.
NOTA – Describe las condiciones del carácter facultativo de los IE que son opcionales.	

4. **Flujo de información #4, nombre del procedimiento**: *Breve declaración sobre el procedimiento común que se realiza en esta fase de la secuencia.*

FEA4	– Descripción de la acción o acciones de la entidad funcional al final del procedimiento en el FE definido por las características propias del procedimiento. – Si el procedimiento siguiente en opcional, como en esta plantilla, deben incluirse las condiciones para las cuales se realiza o no se realiza.

5. **Flujo de información #5, nombre del procedimiento**: *Breve declaración sobre el procedimiento común opcional que se realiza en esta fase de la secuencia.*

FEA5	– Descripción de la acción o acciones de la entidad funcional al final del procedimiento en el FE definido por las características propias del procedimiento. – Dado que con ello finaliza el procedimiento que se ilustra en la plantilla, puede indicarse que "no se realizarán acciones ulteriores".

6 Gestión de la movilidad

En esta cláusula se proporcionan los flujos de información para la gestión de la movilidad relacionada con los servicios y las capacidades de red de IMT-2000.

6.1 Gestión de la autenticación

6.1.1 Autorización del titular del UIM

Esta facilidad permite autorizar a un usuario del UIM que es susceptible de ser suprimido. Sólo se aplica cuando el UIM se utiliza para la asociación de usuarios con terminales móviles IMT-2000. Se trata de una facilidad distinta a la facilidad de "desenganche" que pueden proporcionar algunos proveedores MT. Véase la figura 6.1.1-1.

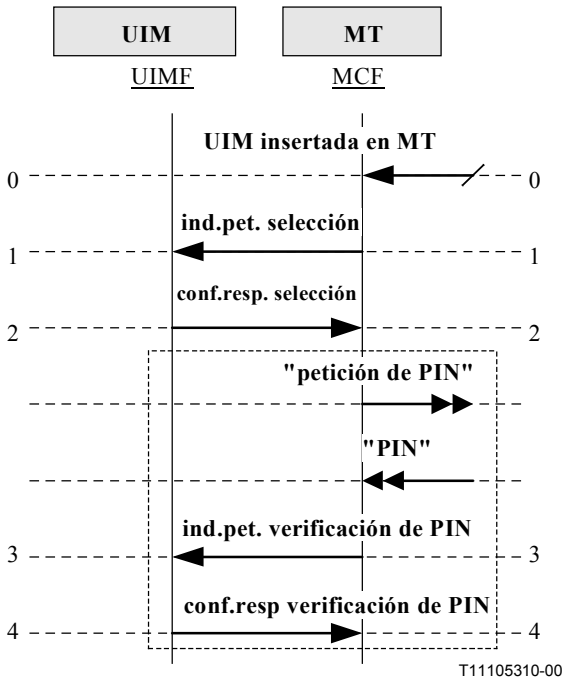


Figura 6.1.1-1/Q.1721 – Autorización al poseedor de la UIM

0. UIM insertada en MT: se encienda el MT con la UIM insertada.

FEA0	– Inicio del procedimiento de verificación del titular del UIM.

1. **ind.pet. selección**: se utiliza para seleccionar el fichero o ficheros apropiados en una UIMF.

Selección (Respuesta: éxito o fracaso)	**ind.pet.**
ID de archivo	M

FEA1	– Selección del fichero o ficheros adecuados en la UIMF.

2. **conf.resp. selección**: es la respuesta a la petición.

Selección	**conf.resp.**
ID de archivo	M (nota)
Formato de PIN	M

FEA2	– Interacción con el usuario para obtener el PIN.
NOTA – Si es diferente, sistema de confirmación o solicitud de alternativo.	

3. **ind.pet. verificación de PIN**: utilizada para verificar el PIN.

Verificación de PIN (Respuesta: éxito o fracaso)	**ind.pet.**
PIN	M

FEA3	– Comparación del PIN introducido por el usuario con el PIN almacenado en el UIM.

4 **conf.resp. verificación de PIN** es la respuesta a la petición.

Verificación de PIN	**conf.resp.**
Resultado	M

FEA4	– Si se devuelve una respuesta exitosa, el usuario del UIM es válido y se autoriza al terminal.

6.1.2 Autenticación del usuario

El proceso de autenticación de la identidad del usuario móvil internacional (IMUI) consiste en la verificación por parte de la red medular de que la identidad MT/UIM IMT-2000 (IMUI o TMUI) es la declarada. La autenticación se compone de un protocolo de puesta a prueba/respuesta mediante el que se demuestra que se conoce una clave secreta, denominada clave de autenticación (A-key, *authentication key*), que sólo conocen el MT/UIM IMT-2000 y el centro de autenticación (AC, *authentication center*) en la red originaria del usuario. Este procedimiento de seguridad de autenticación tiene por objeto proteger la red contra un uso no autorizado.

La red puede desencadenar el proceso de autenticación IMT-2000:

- cuando el abonado se registra en un sistema servidor (incluidas las actualizaciones de posición, directivas incorporadas/desincorporadas); o
- cuando el abonado origina una llamada; o
- cuando el abonado responde a una radiobúsqueda; o
- cuando el abonado responde a una radiobúsqueda SMS; o
- en función de las políticas del operador, incluida la gestión de servicios suplementarios, la prueba, la puesta a prueba periódica de autenticación del usuario, las actualizaciones secretas compartidas, etc.

Cuando el procedimiento de autenticación de un MT no tiene éxito, se deniega el acceso a la red IMT-2000, excepto en el caso de llamadas de emergencia. Debe señalarse que el proveedor de servicio puede permitir facultativamente que dicho MT acceda a la red si el sistema servidor no puede realizar la autenticación y si no puede alcanzarse la LMFh/AMF originaria debido a sobrecarga o fallo de la red.

Se definen tres procedimientos distintos de autenticación para una red IMT-2000: dos "mecanismos singulares de puesta a prueba/respuesta (UC, *unique challenge*)" y el "mecanismo de puesta a prueba global, (GC, *global challenge*)" que se describen a continuación. En el caso de funcionamiento entre sistemas correspondientes a distintos miembros de la familia IMT-2000, el sistema visitado inicia el mecanismo de autenticación conforme a sus capacidades. Ello implica que un sistema originario soportará la petición de autenticación del sistema visitado para soportar la itinerancia a través de miembros de la familia IMT-2000.

Después de realizarse con éxito los procedimientos de autenticación de usuario, se ejecutan dos procedimientos de seguridad adicionales. El primero es el de "inicio de cifrado" y el segundo es el procedimiento de "asignación de TMUI".

6.1.2.1 Clave de autenticación

La clave de autenticación del abonado (A-key) sólo se conoce y almacena en el MT y en el centro de autenticación originario (AC). La A-key no se transmite en ningún caso por medios radioeléctricos en la red, y su integridad resulta esencial para un proceso de autenticación efectivo.

6.1.2.2 Mecanismo de autenticación de usuario única de puesta a prueba/respuesta basado en tripletas de vectores de autenticación

El mecanismo de autenticación de usuario única de puesta a prueba/respuesta consiste en el intercambio siguiente entre la red visitada y el UIM.

- La red visitada transmite al UIM un número aleatorio no predecible RAND.
- El UIM calcula la signatura basada en el RAND recibido, utilizando el algoritmo de autenticación y la clave de autenticación secreta y transmite el resultado de la signatura (SRES, *signature result*) a la red visitada.
- La red visitada verifica el resultado de la signatura.

Véase la figura 6.1.2.2-1.

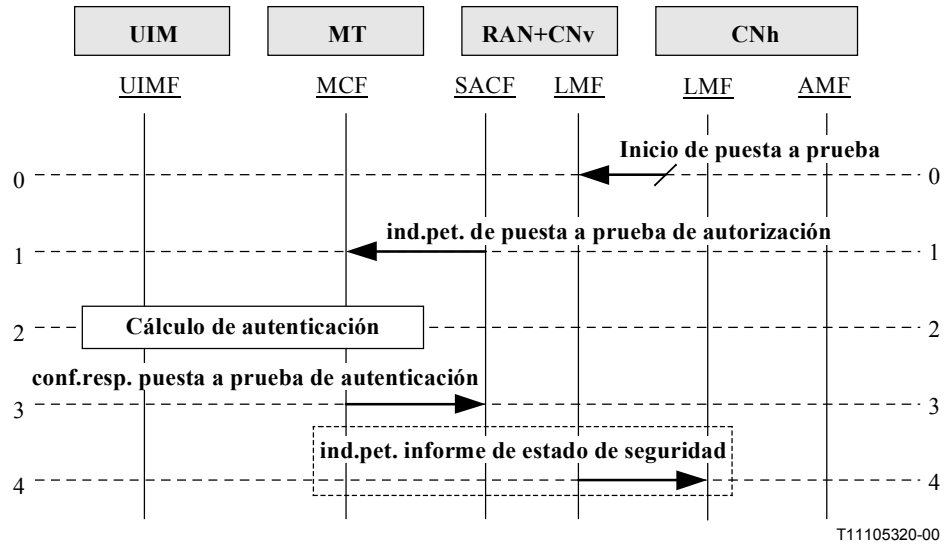


Figura 6.1.2.2-1/Q.1721 – Autenticación de usuario única de puesta a prueba/respuesta

0. **Inicio de petición de puesta a prueba**: la SACF recibe una petición de inicio de puesta a prueba. Esto ocurre cuando la LMFv determina que es necesaria la autenticación del usuario.

FEA0	– Inicio de la puesta a prueba de autenticación.
NOTA – El procedimiento facultativo de gestión de la clave de autenticación se realiza para obtener las tripletas de autenticación en caso de que no estén disponibles. Para más información véase el procedimiento de gestión de la clave de autenticación.	

1. **ind.pet. puesta a prueba de autenticación**: se utiliza para verificar la identidad del usuario.

Puesta a prueba de autenticación (Respuesta: éxito o fracaso)	**ind.pet.**
Puesta a prueba	M

FEA1	– Inicio del cálculo de autenticación.

2. **Autenticación**: se ejecuta el procedimiento.

3. **conf.resp. puesta a prueba de autenticación**: enviado por la MCF a la SACF para indicar el resultado del cálculo de autenticación.

Puesta a prueba de autenticación	**conf.resp.**
Respuesta a puesta a prueba	M

FEA3	– Determina si se necesita un informe de estado de seguridad.

4. **ind.pet. informe de estado de seguridad**: utilizado para enviar un informe de estado de seguridad a la red originaria (opcional).

Informe de estado de seguridad (Respuesta: ninguna)	ind.pet.
Resultado	M
IMUI	O (nota)

FEA4	– Analiza el informe de estado de seguridad.
NOTA – IMUI debe estar incluido, si está disponible.	

6.1.2.2.1 Gestión de la clave de autenticación

La clave de autenticación del usuario, A-key, se asigna, junto con el IMUI cuando el abonado realiza la suscripción.

La A-key se almacena en el lado de red, en un centro de autenticación (AC) de la red originaria (AMFh).

Una red IMT-2000 puede tener uno o más AC. El AC puede estar físicamente integrado con otras funciones, por ejemplo, con un registro de ubicación originario (LMFh). Un abonado sólo se asociará a un AC.

Cuando lo necesita el MT, la LMFv solicita la información relativa a la seguridad a la AMFh correspondiente al MT. Ello incluye una matriz de parejas de RAND y SRES. Dichas parejas se obtienen aplicando el algoritmo de autenticación del usuario a cada RAND y A-key. Las parejas se almacenan en la LMFv como parte de la información relacionada con la seguridad.

Para el mecanismo único de puesta a prueba, las tripletas de autenticación pueden ser generadas por la AMFh en un proceso por lotes en el centro de autenticación y enviados a través de la LMFh a la LMFv.

Véase la figura 6.1.2.2-2.

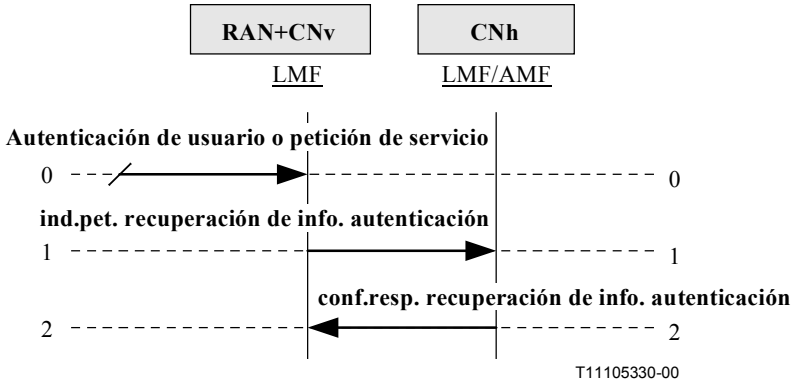


Figura 6.1.2.2-2/Q.1721 – Gestión de la clave de autenticación

0. **Autorización del usuario o petición de servicio**: se recibe la identidad del abonado y la LMFv verifica si es necesaria la autenticación del usuario.

FEA0	– Si no hay información de autenticación suficiente en la LMFv para realizar dicha autenticación, se envía a la LMFh una petición de recuperación de autenticación.

1. **ind.pet. recuperación de información de autenticación**: utilizado para solicitar a la LMFh información de seguridad para la autenticación del usuario.

Recuperación de información de autenticación (Respuesta: éxito o fracaso)	ind.pet.
IMUI	M

FEA1	– Recuperación de información de seguridad. – Recuperación de puesta a prueba e información de respuesta para autenticación.

2. **conf.resp. recuperación información de autenticación**: contiene el resultado a la ind.pet. recuperación de información de autenticación.

Información de autenticación	conf.resp.
Puesta(s) a prueba	M
Respuesta(s) a puesta a prueba	M
Resultado	M
Clave de cifrado	O (nota)

FEA2	– Almacena información de autenticación.
NOTA – En el caso del mecanismo de autenticación basado en tripletas, la clave de cifrado debe estar disponible para algunos accesos a la red, como por ejemplo, actualización de localización, respuestas a radiobúsquedas, inicio de llamada, etc.	

6.1.2.2.2 Transferencia de tripletas de autenticación no utilizadas durante la actualización de la ubicación

Cuando un usuario se desplaza a otra LMFv, las tripletas no utilizadas de la LMFv previa pueden transferirse a la nueva LMFv. Esta capacidad se utiliza solamente cuando la autenticación se realiza utilizando la TMUI (véase la figura 6.2.2).

6.1.2.2.3 Cálculo de la autenticación

El MT inicia este procedimiento hacia la UIM solicitando la ejecución del algoritmo de cálculo de la autenticación para la autenticación de una signatura de usuario.

NOTA – La UIMF dispone de la clave de autenticación utilizada para calcular el resultado de la autenticación. Desde el punto de vista de la seguridad, la clave de autenticación no debe ser recuperada de algún lugar ajeno a esta entidad funcional. Por lo tanto, es necesario un procedimiento para solicitar a la UIMF que realice el cálculo de autenticación. Se trata de un procedimiento común para los mecanismos de autenticación de usuario de puesta a prueba/respuesta única y de puesta a prueba global.

Véase la figura 6.1.2.2-3.

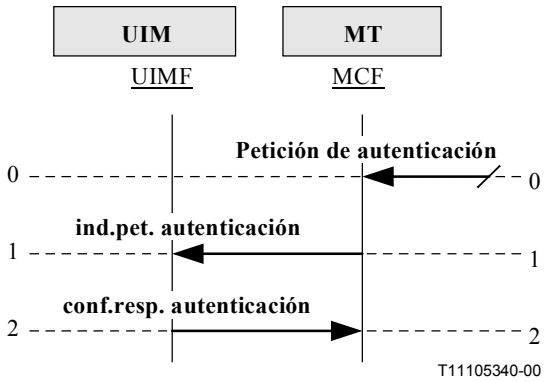


Figura 6.1.2.2-3/Q.1721 – Cálculo de la autenticación

0. **Petición de autenticación**: la MCF recibe una petición de autenticación.

FEA0	– Inicio del cálculo de autenticación.

1. **ind.pet. autenticación**: utilizado para solicitar que el cálculo de autenticación se realice mediante el número aleatorio y la clave de autenticación.

Autenticación (Respuesta: éxito o fracaso)	**ind.pet.**
RAND	M

FEA1	– La UIMF calcula la signatura de autenticación utilizando el número aleatorio suministrado por la MCF y la clave de autenticación de usuario almacenada en la UIMF.

2. **conf.resp. de autenticación**: utilizada para devolver el resultado del cálculo de autenticación.

Autenticación	**conf.resp.**
Resultado de signatura	M
Clave(s) de cifrado	M

FEA2	– Recepción de la respuesta del cálculo de autenticación.

6.1.2.3 Puesta a prueba global

Una puesta a prueba global es el mensaje de la interfaz radioeléctrica (RAND) que se difunde en un canal de información común a todo el sistema. Su generación y frecuencia de actualización quedan bajo el control del operador de red y deben ser conformes con las buenas prácticas de autenticación.

Cuando se intenta realizar el acceso a una red o responder a un radiobúsqueda SMS, la estación móvil debe incluir su signatura de autenticación. La signatura de autenticación calculada se basa en información secreta que se distribuyó durante la suscripción. Los elementos de información de respuesta de la puesta a prueba global incluyen, pero no de forma exhaustiva, un identificador de suscripción, una confirmación de la puesta a prueba global recibida (RANDC), una respuesta de autenticación (AUTH, *authentication response*) y un valor del parámetro contador histórico de llamadas (CHCNT, *call history counter*). Los elementos de información que incluye la respuesta a la

puesta a prueba de la red están por lo general incluidos en los mensajes de petición de acceso a la red, tales como registros, origen de llamadas, terminación de llamadas o respuestas a radiobúsquedas SMS. Por tanto, el mecanismo de puesta a prueba global no se utiliza como un mecanismo autónomo sino que acompaña a otros protocolos de acceso a la red para minimizar el tráfico de mensajes en los canales de la interfaz radioeléctrica. El procedimiento de puesta a prueba global también desencadena el cálculo de las claves de cifrado que son utilizadas para cifrar el tráfico de usuario. Véase la figura 6.1.2.3-1.

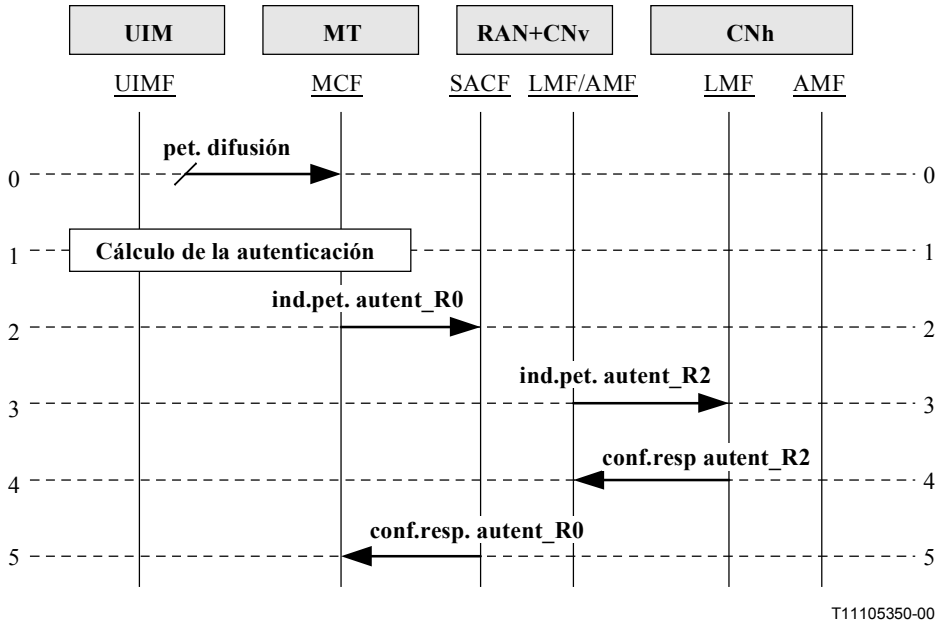


Figura 6.1.2.3-1/Q.1721 – Autenticación de usuario de puesta a prueba global

0. **Petición de difusión**: durante un intento de acceso al sistema por parte del MT, la "puesta a prueba global" se lee del canal de difusión de información del sistema.

FEA0	– La estación móvil obtiene la "puesta a prueba global " de un canal de comunicación común, aplicándose entonces al algoritmo de autenticación de la UIMF junto con información secreta de usuario a fin de calcular la signatura de autenticación de la UIMF (AUTH_R). – Se inicia el cálculo de la autenticación.

1. **Cálculo de la autenticación**: se realiza.

2. **ind.pet. autent_R0**: utilizado como componente de un registro o de un procedimiento de petición de servicio.

Autent_R0	**ind.pet.**
TMUI	M
Confirmación de RAND (RANDC)	M
AUTH_R	M
CHCNT	M

FEA2	– Verifica que la confirmación de RAND (es decir, RANDC) es consistente con el RAND global recibido en el canal de información del sistema. – Se obtiene el SSD de usuario de la LMFv del sistema servidor. – Si SSD no está disponible en la red visitada, se transmite la respuesta de autenticación de usuario a la LMFh, incluido el RAND global completo en lugar del RANDC. – Se ejecuta el procedimiento de autenticación de usuario. – Se calculan las claves de cifrado aplicables.
NOTA – La LMFv soporta el mecanismo de puesta a prueba global mediante su participación en la generación y distribución de la RAND global que la red servidora difunde mediante una canal de información que se extiende por todo el sistema. El sistema servidor controla las actualizaciones de la RAND global.	

3. **ind.pet. autent_R2**: utilizado para transferir a la red originaria la petición de autenticación.

Autent_R2 (Respuesta: éxito o fracaso)	**ind.pet.**
IMUI	M
RANDG	M
AUTH_R	M
CHCNT	M

FEA3	– Cálculo de la clave o claves de cifrado aplicables. – Realiza el procedimiento de autenticación de usuario. – Envía a la LMFv la confirmación de la validez del usuario, junto con la clave o claves de cifrado aplicables y, en algunas circunstancias, la SSD.

4. **conf.resp. autent_R2**: es la respuesta que proporciona la información de seguridad solicitada.

Autent_R2	conf.resp.
Resultado	M
SSD	O (nota 1)
Clave(s) de cifrado	O (nota 2)

FEA4	– Envía a la MCF la confirmación de la validez del usuario, junto con la(s) clave(s) de cifrado aplicable(s) y, en algunas circunstancias, la SSD.
NOTA 1 – Si la LMFh/AMF activa la compartición de SSD, el parámetro SSD puede incluirse en este mensaje. NOTA 2 – Se devuelve si está disponible.	

5. **conf.resp. autent_R0**: transporta hasta la MCF la respuesta a ind.pet. autent_R0.

Autent_R0	conf.resp.
Resultado	M

FEA 5	– Recibe una confirmación de estado de la red como componente del intento de acceso al sistema.

6.1.2.4 Gestión del dato secreto compartido (SSD)

6.1.2.4.1 Actualización del dato secreto compartido del usuario (actualización del SSD)

Para minimizar el tráfico de red entre el sistema servidor y la AMF originaria, al tiempo que se proporciona protección adicional a la A-key, de dicha clave A-key de abonado se obtiene una clave de autenticación secundaria, denominada datos secretos compartidos (SSD, *shared secret data*). El procedimiento de actualización de SSD, mediante el que la SSD del MT se comparte con un sistema servidor, puede ejecutarse en cualquier momento a discreción del proveedor de servicio "originario". El proceso de actualización de SSD sólo se inicia después de una autenticación exitosa del MT. Véase la figura 6.1.2.4.1-1.

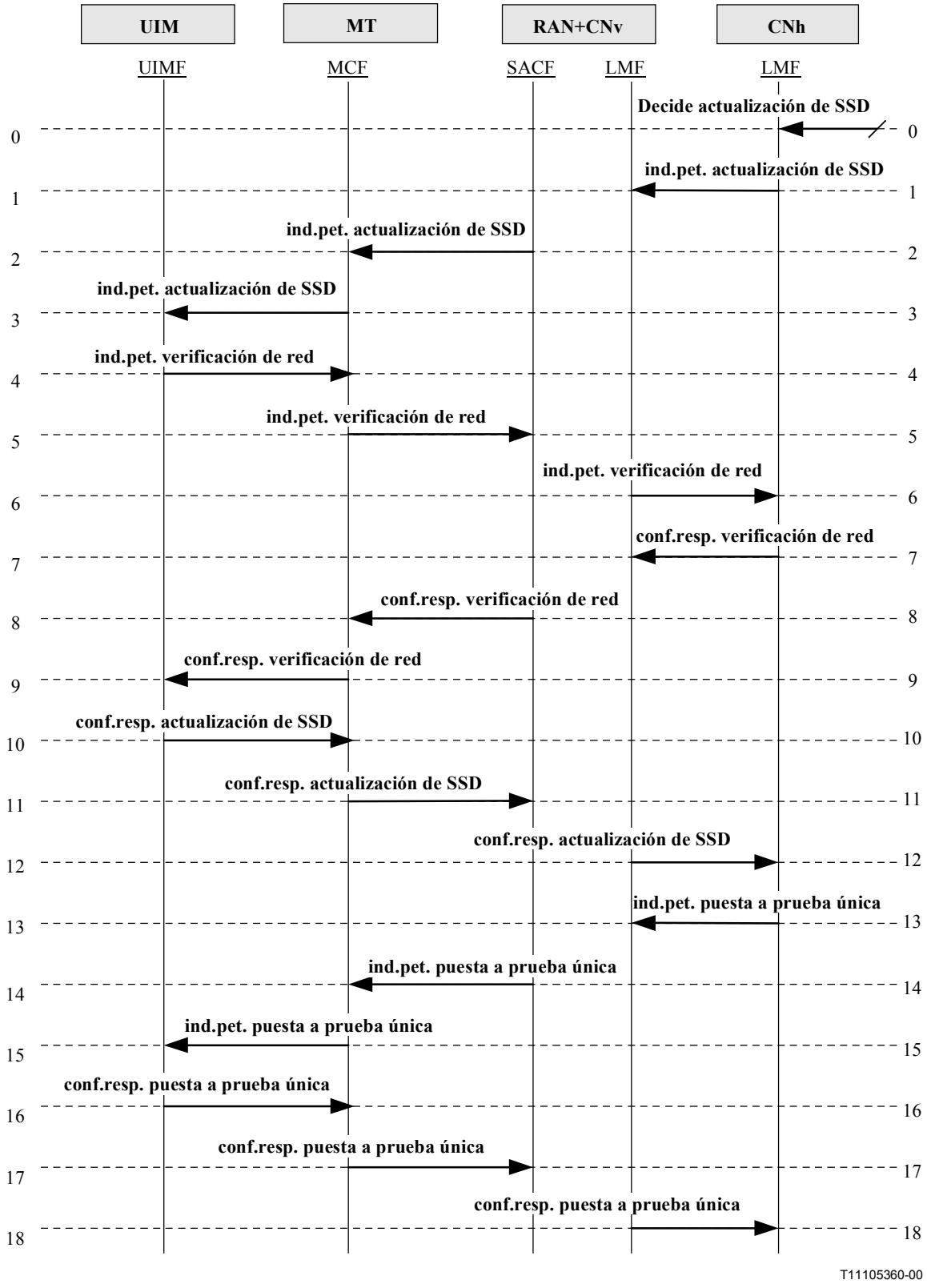


Figura 6.1.2.4.1-1/Q.1721 – Actualización de SSD (SSD no se comparte)

0. Decide actualización de SSD: inicia la ejecución del procedimiento de actualización de SSD para el usuario móvil seleccionado en la red visitada.

FEA0	– Genera un número aleatorio RANDSSD. – Calcula un nuevo SSD para el usuario móvil. – Genera RANDU y calcula AUTH_U, utilizando el nuevo SSD. – Envía ind.pet. actualización de SSD a la LMFv solicitando que el usuario móvil seleccionado realice una actualización inmediata de su SSD.

1. **ind.pet. actualización de SSD**: hace que la UIMF actualice su valor de SSD. Se envía desde el sistema originario al sistema visitado en el que se localiza el usuario móvil. Para que se ejecute este procedimiento, es necesario que la UIM (sustituible o permanente) esté presente en el terminal móvil.

Actualización de SSD (Respuesta: éxito o fracaso)	**ind.pet.**
IMUI	M
RANDSSD	M
RANDU	M
AUTH_U	M
Clave(s) de cifrado	O (nota)

FEA1	– Recibe ind.pet. actualización de SSD de la LMFh, realiza la traducción IMUI/TMUI, y lo envía a la MCF.
NOTA – Las claves de cifrado se envían si están disponibles.	

2. **ind.pet. actualización de SSD**: hace que el usuario móvil actualice su valor de SSD. Se envía desde el sistema originario al sistema visitado en el que se localiza el usuario móvil. Para que se ejecute este procedimiento, es necesario que el UIM (suprimible o permanente) esté presente en el terminal móvil para interaccionar con la red.

Actualización de SSD (Respuesta: éxito o fracaso)	**ind.pet.**
IMUI	M
RANDSSD	M

FEA2	– Retransmite ind.pet. actualización de SSD desde la red visitada.

3. **ind.pet. actualización de SSD**: hace que el usuario móvil actualice su valor de SSD. Es retransmitido por el sistema visitado.

Actualización de SSD (Respuesta: éxito o fracaso)	ind.pet.
IMUI	M
RANDSSD	M

FEA3	– Calcula un nuevo (tentativo) SSD. – Genera un número aleatorio RANDBS para ser utilizado en la IF de verificación de red. – Calcula el AUTHBS esperado utilizando el nuevo (tentativo) SSD. – Envía la ind.pet. verificación de red a la MCF (para la autenticación y verificación de la red).

4. **ind.pet. verificación de red**: hace que la red se autentique y verifique a sí misma ante el móvil. Procede del UIM.

Verificación de red (Respuesta: éxito o fracaso)	ind.pet.
TMUI	M
RANDBS	M

FEA4	– Retransmite la ind.pet. verificación de red desde la UIMF.

5. **ind.pet. verificación de red**: la MCF la retransmite al sistema visitado.

Verificación de red (Respuesta: éxito o fracaso)	ind.pet.
TMUI	M
RANDBS	M

FEA5	– Realiza la traducción IMUI/TMUI.

6. **ind.pet. verificación de red**: el sistema visitado lo retransmite al sistema originario para la autenticación de la red.

Verificación de red (Respuesta: éxito o fracaso)	ind.pet.
IMUI	M
RANDBS	M

FEA6	– Genera AUTHBS utilizando el nuevo SSD.

7. **conf.resp. verificación de red**: es la respuesta de la red originaria al flujo de información ind.pet. verificación de red.

Verificación de red	conf.resp.
AUTHBS	M

FEA7	– Realiza la traducción IMUI/TMUI.

8. **conf.resp. verificación de red**: lo retransmite la red visitada.

Verificación de red	conf.resp.
AUTHBS	M

FEA8	– Retransmite conf.resp verificación de red.

9. **conf.resp. verificación de red**: el sistema móvil lo retransmite a la UIM.

Verificación de red	conf.resp.
AUTHBS	M

FEA9	– Compara la AUTHBS recibida con la AUTHBS esperada. – Prepara confirmación de superación/fracaso. – Si el procedimiento ha sido exitoso actualiza la memoria con el nuevo SSD.

10. **conf.resp. actualización de SSD**: es la respuesta del UIM a la ind.pet. actualización de SSD.

Actualización de SSD	conf.resp.
Resultado	M

FEA10	– Retransmite conf.resp. actualización de SSD

11. **conf.resp. actualización de SSD**: es la respuesta al flujo de información de ind.pet. actualización de SSD.

Actualización de SSD	conf.resp.
Resultado	M

FEA11	– Confirmación del proceso

12. **conf.resp. actualización de SSD**: es la respuesta al flujo de información de ind.pet. actualización SSD.

Actualización SSD	conf.resp.
Resultado	M

FEA12	– Prepara el envío de ind.pet. puesta a prueba única al usuario móvil en la red visitada.

13. **ind.pet. puesta a prueba única**: permite a la red determinar si el móvil seleccionado ha podido actualizar con éxito su SSD.

Puesta a prueba única (Respuesta: éxito o fracaso)	ind.pet.
IMUI	M
RANDU	M
AUTH_U	M

FEA13	– Realiza la traducción IMUI/TMUI.

14. **ind.pet. puesta a prueba única**: se envía desde la UIMF al MT.

Puesta a prueba única (Respuesta: éxito o fracaso)	ind.pet.
TMUI	M
RANDU	M
AUTH_U	M

FEA14	– Retransmite ind.pet. puesta a prueba única

15. **ind.pet. puesta a prueba única**: se envía a la UIMF.

Puesta a prueba única (Respuesta: éxito o fracaso)	ind.pet.
TMUI	M
RANDU	M
AUTH_U	M

FEA15	– Calcula la respuesta de autenticación AUTH_U utilizando el nuevo SSD.

16. **conf.resp. puesta a prueba única**: es la respuesta a la ind.pet. puesta a prueba única e incluye la respuesta de autenticación.

Puesta a prueba única	conf.resp.
AUTH_U	M

FEA16	– Retransmite conf.resp. puesta a prueba única.

17. **conf.resp. puesta a prueba única**: se envía a RAN+CNv.

Puesta a prueba única	conf.resp.
AUTH_U	M

FEA17	– Realiza la traducción IMUI/TMUI.

18. **conf.resp. puesta a prueba única**: se envía a la red originaria.

Puesta a prueba única	conf.resp.
AUTH_U	M

FEA18	– Actualización de los datos del usuario móvil en función de la información de estado recibida. – Si el estado es éxito, se almacena el nuevo valor de SSD para ser utilizado en futuras aplicaciones del procedimiento de autenticación y permitir al usuario móvil continuar con el inicio y terminación de la llamada. Facultativamente SSD puede compartirse con una LMFv si lo permiten los acuerdos con el proveedor de servicio.
NOTA – La LMFh actualiza los datos del usuario en función de la información de estado recibida. Si la autenticación no ha fracasado, se permite al usuario móvil continuar el inicio y terminación de la llamada. Además, SSD se transfieren a la LMFv si lo permiten los acuerdos con el proveedor de servicio. Si el estado es fracaso, se mantienen el SSD actual y se intenta actualizar de nuevo el SSD del usuario móvil en una transacción posterior.	

6.1.2.4.2 Invocación de compartición de la seguridad

La invocación de compartición de la seguridad se utiliza para compartir la información de seguridad asociada con un usuario IMT-2000 determinado.

Escenario:

a) El sistema originario de un abonado determina que debe habilitarse la seguridad compartida y extiende (comparte) la información de seguridad al sistema visitado.

b) El sistema visitado habilita la compartición de seguridad y responde al sistema originario indicando éxito o fracaso.

Véase la figura 6.1.2.4.2-1.

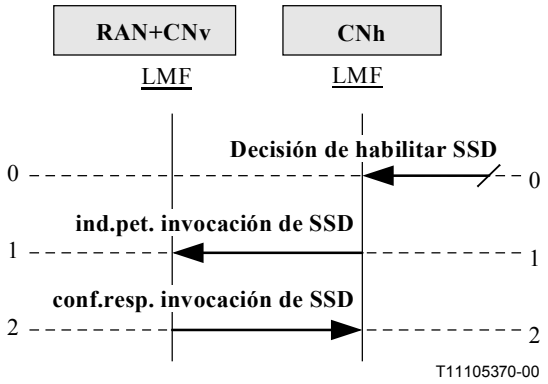


Figura 6.1.2.4.2-1/Q.1721 – Diagrama del flujo de información de invocación de compartición de seguridad

0. Decisión de habilitar SSD: decide habilitar la compartición de datos secretos entre los sistemas origen y visitado.

FEA0	– LMFh determina que debe permitirse la compartición de seguridad y envía una petición invocación_compartición_seguridad a la LMFv con la información de seguridad que debe compartirse.

1. **ind.pet. invocación_compartición_seguridad**: se utiliza para invocar la compartición de la información de seguridad en el sistema visitado.

Invocación_compartición_seguridad (Respuesta: Éxito o fracaso)	**ind.pet.**
IMUI	M
SSD	M

FEA1	– LMFv recibe la petición, autoriza la compartición de seguridad y devuelve indicación de éxito o fracaso.

2. **conf.resp. invocación_compartición_seguridad**: es la respuesta al flujo de información ind.pet. invocación_compartición_seguridad.

Invocación_compartición_seguridad	**conf.resp.**
Resultado	M

6.1.2.4.3 Revocación de la compartición de seguridad

La revocación de la compartición de seguridad se utiliza para revocar la compartición de la información de seguridad en el sistema visitado.

Escenario:

a) El sistema originario de un abonado determina que debe inhabilitarse la seguridad compartida e informa al sistema visitado.

b) El sistema visitado inhabilita la compartición de seguridad y responde al sistema originario con el cómputo histórico de la llamada, si está disponible, indicando éxito o fracaso.

Véase la figura 6.1.2.4.3-1.

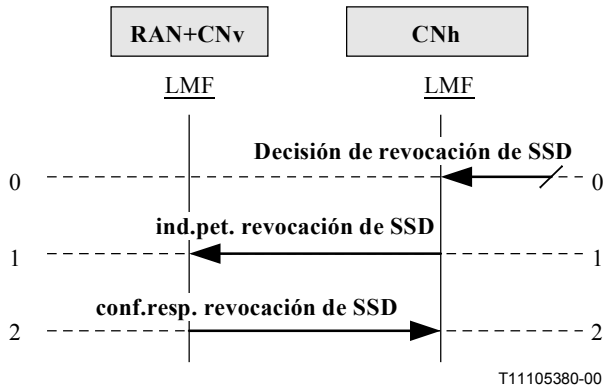


Figura 6.1.2.4.3-1/Q.1721 – Diagrama del flujo de información de revocación de compartición de seguridad

0. **Decisión de revocación de SSD**: decide habilitar la compartición de datos secretos entre el sistema originario y el visitado.

FEA0	– La LMFh determina que la compartición de seguridad debe inhabilitarse y envía una petición revocación_compartición_seguridad a la LMFv.

1. **ind.pet. revocación_compartición_seguridad**: se utiliza para revocar la compartición de información de seguridad en el sistema visitado.

Revocación_compartición_seguridad (Respuesta: éxito o fracaso)	**ind.pet.**
IMUI	M

FEA1	– La LMFv recibe la petición, inhabilita la compartición de seguridad y devuelve indicación de éxito o fracaso.

2. **conf.resp. revocación_compartición_seguridad**: es la respuesta al flujo de información ind.pet. revocación_compartición_seguridad.

revocación_compartición_seguridad	**conf.resp.**
Resultado	M
CHCNT	O (nota)
NOTA – Se devuelve CHCNT, si está disponible.	

6.1.2.5 Comienzo del cifrado

Este procedimiento permite el cifrado del flujo de datos en la interfaz radioeléctrica para evitar el acceso no autorizado a la información. El cifrado se inicia en el MT (y en la LMFv) sólo después de un proceso de autenticación exitoso. Véase la figura 6.1.2.5-1.

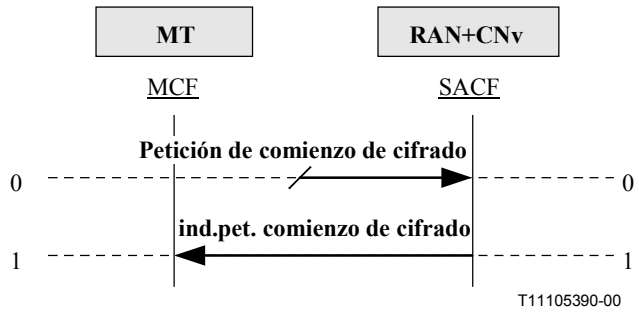


Figura 6.1.2.5-1/Q.1721 – Diagrama de flujo de información de comienzo de cifrado

0. **Petición de comienzo de cifrado**: se recibe la petición de comienzo de cifrado.

1. **ind.pet. comienzo_cifrado**: utilizada para activar el control de cifrado sobre la interfaz radioeléctrica.

Comienzo de cifrado (Respuesta: ninguna)	ind.pet.
Ninguna	N/A

FEA1	– Activa el control de cifrado en la interfaz radioeléctrica.

6.1.2.6 Asignación de TMUI

Una TMUI tiene significado local exclusivamente en el área en la que se ha registrado el usuario. Fuera de dicha área, debe ser acompañado por una identificación de zona de ubicación (LAI, *location area identification*) adecuada a fin de evitar ambigüedades. La asociación entre las identidades permanente y temporal del usuario se mantiene en la LMFv en la que se ha registrado el usuario.

Cuando la TMUI está disponible se utiliza normalmente para identificar el usuario en el trayecto de acceso radioeléctrico, por ejemplo, en peticiones de radiobúsqueda, peticiones de actualización de ubicación, peticiones de incorporación, peticiones de servicio, peticiones de restablecimiento de la conexión y peticiones de desincorporación.

Este procedimiento se utiliza para asignar y transportar la TMUI al UIM después de que la red haya verificado la identidad del usuario y debe realizarse después del inicio del cifrado. Véase la figura 6.1.2.6-1.

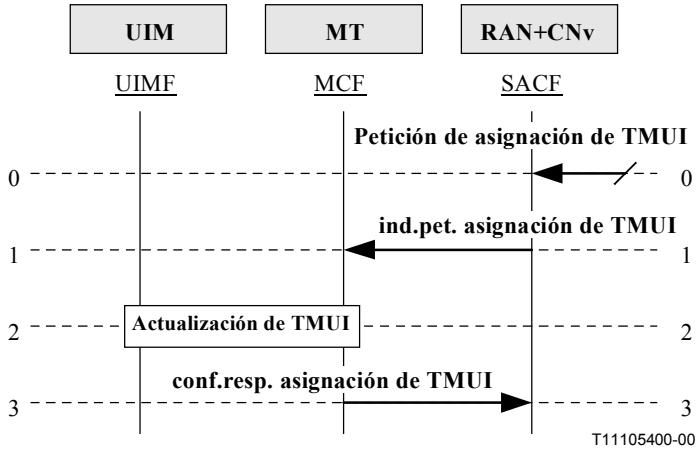


Figura 6.1.2.6-1/Q.1721 – Diagrama de flujo de información de asignación de TMUI

0. **Petición de asignación de TMUI**: se recibe.

FEA0	– Recuperación de la ID de la fuente de asignación de TMUI y TMUI y opcionalmente, el temporizador de expiración de TMUI. – Envío de ind.pet. asignación de TMUI.

1. **ind.pet. asignación_TMUI**: se utiliza para asignar y transportar el TMUI al usuario después de que la red haya verificado la identidad del usuario.

Asignación_TMUI (Respuesta: éxito o fracaso)	ind.pet.
TMUI	M
ID de fuente de asignación de TMUI	M
Temporizador de expiración de TMUI	O (nota)

FEA1	– Inicia el módulo de procedimiento de actualización de TMUI.
NOTA – Se incluye si se utiliza un valor de temporizador distinto del que por defecto fija la red.	

2. **conf.resp. asignación_TMUI**: indica que se ha realizado el procedimiento de actualización de TMUI.

FEA2	– Analiza el resultado de la actualización de TMUI e informa de ello a la red visitada.

3. **conf.resp. asignación_TMUI** es la respuesta a la ind.pet. asignación_TMUI.

Asignación_TMUI	conf.resp.
Resultado	M

FEA3	Se anota la respuesta. No se necesita actuación ulterior.

6.1.2.7 Cómputo histórico de llamadas

6.1.2.7.1 Actualización del cómputo histórico de llamadas

El procedimiento de actualización del cómputo histórico de llamadas se utiliza para actualizar el contador histórico de llamadas (CHCNT) en el sistema visitado, el terminal móvil y el UIM. Véase la figura 6.1.2.7.1-1.

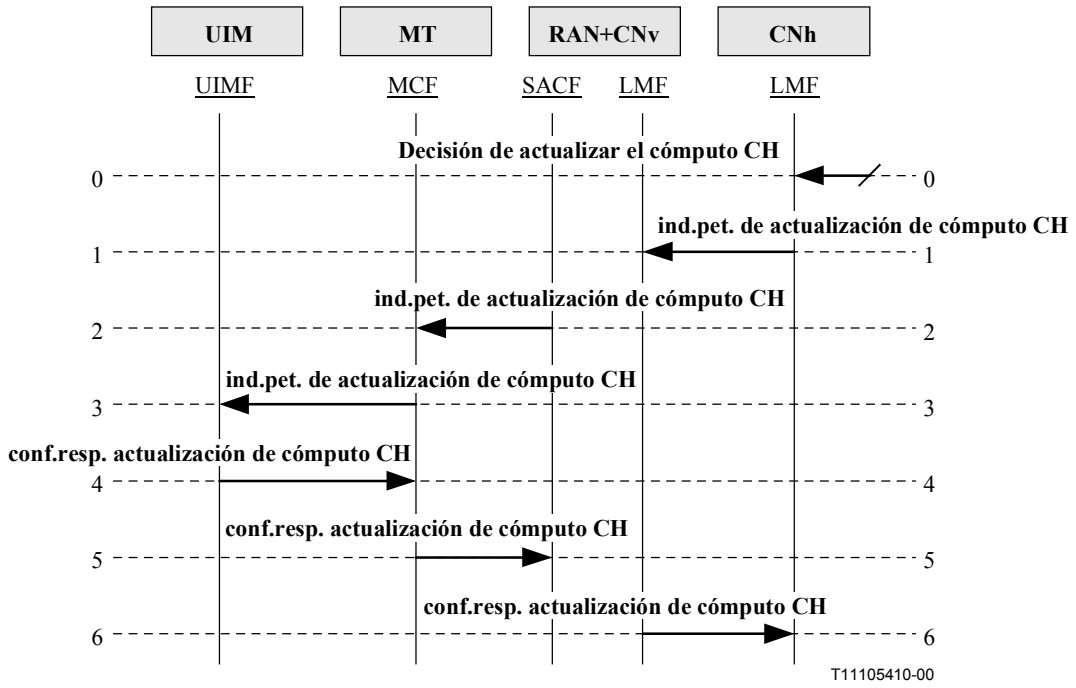


Figura 6.1.2.7.1-1/Q.1721 – Diagrama de flujo de información de actualización del cómputo histórico de llamadas

0. **Decisión de actualizar el cómputo histórico de llamadas**: el sistema originario detecta la necesidad de actualizar el cómputo histórico de llamadas y envía una petición al sistema visitado a fin de actualizarlo.

FEA0	– Recupera los parámetros adecuados e inicia el procedimiento de actualización del cómputo histórico de llamadas.

1. **ind.pet. actualización_cómputo_CH**: se utiliza para solicitar la actualización del cómputo histórico de llamadas en el sistema visitado.

Actualización_cómputo_CH (Respuesta: éxito o fracaso)	**ind.pet.**
IMUI	M
Actualización_cómputo_CH	M

FEA1	– Actualización de datos de cómputo histórico de llamadas en el sistema visitado.

2. **ind.pet. actualización_cómputo_CH**: se envía a la MCF.

Actualización_cómputo_CH (Respuesta: éxito o fracaso)	**ind.pet.**
IMUI	M
Actualización_cómputo_CH	M

FEA2	– Actualización de datos de cómputo histórico de llamadas en el terminal móvil.

3. **ind.pet. actualización_cómputo_CH**: se envía a la UIMF.

Actualización_cómputo_CH (Respuesta: éxito o fracaso)	ind.pet.
IMUI	M
Actualización_cómputo_CH	M

FEA3	– Actualización de datos de cómputo histórico de llamadas en el UIM.

4. **conf.resp. actualización_cómputo_CH**: respuesta a la petición de la UIMF.

Actualización_cómputo_CH	conf.resp.
CHCNT	M
Resultado	M

FEA4	– Retransmite resultado a la MCF.

5. **conf.resp. actualización_cómputo_CH**: respuesta a la petición de la MCF.

Actualización_cómputo_CH	conf.resp.
CHCNT	M
Resultado	M

FEA5	– Retransmite resultado a la SACF del sistema visitado.

6. **conf.resp. actualización_cómputo_CH**: respuesta a la petición del sistema visitado.

Actualización_cómputo_CH	conf.resp.
CHCNT	O (nota)
Resultado	M

FEA6	– Retransmite resultado al sistema originario.
NOTA – Envío del CHCNT al sistema originario, si fuera necesario.	

6.1.2.7.2 Procedimiento de petición de cómputo histórico de llamadas

Cuando se utiliza el parámetro CHCNT, la red "originaria" necesita interrogar previamente a la red visitada para obtener el valor actual de CHCNT a fin de que la red servidora actual pueda utilizarlo. La red servidora actual puede ser la red "origen" u otra red "visitada". Véase la figura 6.1.2.7.2-1.

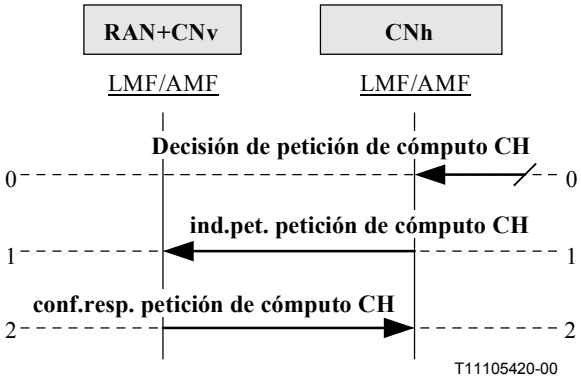


Figura 6.1.2.7.2-1/Q.1721 – Diagrama de flujo de información de petición de cómputo histórico de llamadas

0. **Decisión de petición de cómputo histórico de llamadas**: el sistema originario detecta la necesidad de interrogar a la red previamente visitada para obtener el valor vigente de CHCNT a fin de que la red servidora actual pueda utilizarlo.

FEA0	– Inicio del procedimiento de petición del CHCNT histórico de llamadas.

1. **ind.pet. petición_cómputo_CH**: se utiliza para solicitar el valor actual de CHCNT a la red previamente visitada.

Petición_cómputo_CH (Respuesta: éxito o fracaso)	**ind.pet.**
IMUI	M

FEA1	– Acceso al valor vigente de CHCNT para el usuario y su envío al sistema originario.

2. **conf.resp. petición_cómputo_CH**: es la respuesta a la petición.

Petición_cómputo_CH	**conf.resp.**
CHCNT	M

FEA2	– Recibe CHCNT para el usuario de la red previamente visitada y lo almacena para un uso posterior.

6.1.2.8 Autenticación de puesta a prueba única basada en RANDU

La HLR/AC originaria y el sistema servidor pueden desencadenar este tipo de proceso UC (si se comparte el SSD). El sistema servidor selecciona un número aleatorio (RANDU) y el algoritmo de autenticación produce una respuesta de autenticación esperada, en función de los SSD del móvil. Cuando se recibe el elemento puesto a prueba (es decir, el RANDU), el MT calcula su propia signatura de autenticación utilizando su SSD y el mismo algoritmo de autenticación. La signatura de autenticación se devuelve al sistema servidor (o al AC) donde se compara con el valor esperado. Si hay coincidencia, la autenticación ha sido exitosa.

El proceso UC puede utilizarse de manera opcional para volver a autenticar un MT, para autentificar servicios suplementarios o como parte del proceso de actualización de SSD. Véase la figura 6.1.2.8-1.

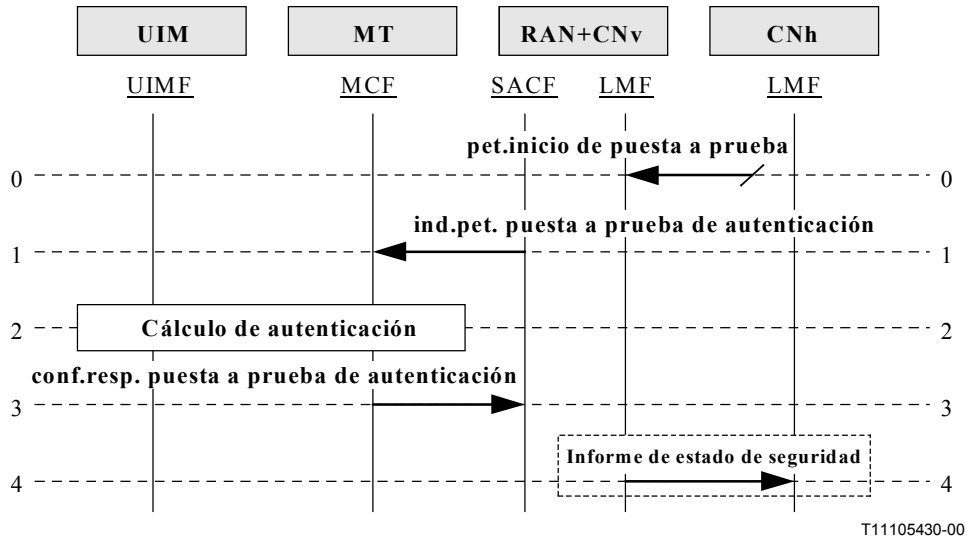


Figura 6.1.2.8-1/Q.1721 – Autenticación única de usuario (SSD compartido) de puesta a prueba/respuesta

0. **Petición de inicio de puesta a prueba**: la SACF recibe una petición de inicio de puesta a prueba después de que la LMFv desencadena el inicio de un proceso de autenticación de UC.

FEA0	– Inicio de puesta a prueba de autenticación. – Genera la puesta a prueba – RANDU y lo envía al usuario.

1. **ind.pet. puesta a prueba de autenticación**: se envía para verificar la identidad del usuario.

Puesta a prueba de autenticación (Respuesta: éxito o fracaso)	ind.pet.
RANDU	M

FEA1	– Calcula la AUTHU de la signatura de autenticación esperada.

2. **Cálculo de autenticación**: se realiza.

3. **conf.resp. puesta a prueba de autenticación**: envía la signatura de autenticación basada en RANDU.

FEA2	– Recibe AUTHU. – Verifica la validez de la AUTHU recibida.

4. **ind.pet. informe de estado de seguridad**: se utiliza para enviar un informe de estado de seguridad a la red originaria (opcional).

Informe de estado de seguridad (Respuesta: ninguna)	ind.resp.
Resultado	M
IMUI	O (nota)

FEA5	– Analiza el informe de estado de seguridad.
NOTA – Si IMUI está disponible debe incluirse.	

6.2 Gestión de la ubicación

6.2.1 Gestión de los datos del abonado

Los procedimientos de gestión de datos del abonado son utilizados por la LMFh para modificar o suprimir algunos datos del abonado del perfil del usuario de la LMFv en caso de que la suscripción o alguno de los servicios suplementarios se hayan modificado o hayan sido suprimidos. Por tanto, puede considerarse como una modificación "autónoma" del perfil del abonado en el sistema visitado, es decir, no asociado a una actualización de ubicación.

NOTA – Los términos "usuario" y "abonado" se utilizan indistintamente en esta subcláusula.

A lo largo de esta subcláusula, se supone que los elementos de información siguientes están almacenados en la red/red soporte originaria del abonado y que son objeto de las actividades de gestión del perfil y de la información del abonado:

- número de directorio móvil IMT-2000 (IMDN), por ejemplo, un número que puede marcarse,
- ID del usuario móvil IMT-2000 (IMUI),
- ID internacional del equipo móvil (IMEI),
- información de ubicación del usuario/terminal,
- datos de servicios básicos (por ejemplo, servicios portadores suscritos),
- teleservicios (por ejemplo, datos de suscripción a difusión y/o llamada de grupo),
- datos de seguridad,
- datos de servicios suplementarios,
- servicios/características que establece por el operador (por ejemplo, datos de prohibición de llamada),
- servicios/características que establece el abonado (por ejemplo, datos de cribado de llamadas),
- datos de restricción de la itinerancia,
- datos de suscripción regionales, y
- datos de suscripción de VHE.

6.2.1.1 Modificación del perfil de abonado

6.2.1.1.1 Modificación del perfil de abonado, Caso 1: copia del perfil de abonado

Los datos del perfil de abonado se han modificado y dichas modificaciones deben reflejarse en la LMFv. En este caso, puede utilizarse el procedimiento "copia del perfil de abonado". Este procedimiento sobrescribe todos los valores de parámetros existentes con los correspondientes valores nuevos. Véase la figura 6.2.1.1-1.

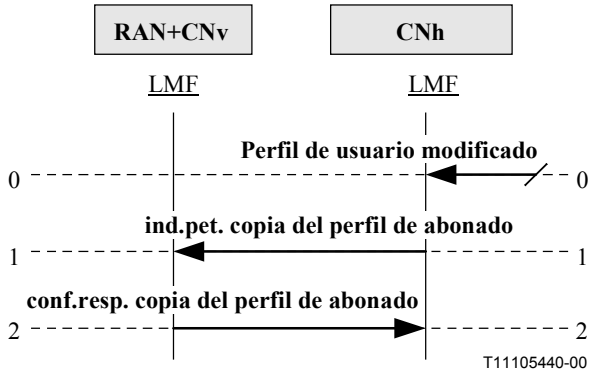


Figura 6.2.1.1-1/Q.1721 – Modificación del perfil de abonado, Caso 1: copia del perfil de abonado

0. **Perfil de usuario modificado**: inicia la copia del perfil del abonado en la LMFv.

FEA0	– Establece la necesidad de actualización del perfil de abonado residente en la LMF de la red visitada.

1. **ind.pet. copia del perfil de abonado**: se envía de la LMFh a la LMFv de la red servidora para indicar los requisitos para la actualización de uno o más elementos del perfil de abonado.

Copia del perfil de abonado (Respuesta: éxito)	ind.pet.
IMUI	M
Perfil de usuario	M

FEA1	– Identifica el usuario IMT-2000 en cuestión. – Actualiza el perfil del usuario.

2. **conf.resp. copia del perfil de abonado**: se envía desde la LMFv de la red servidora a la LMFh de la red originaria del usuario. Se utiliza para informar a la LMFh de los resultados de la actualización del perfil.

Copia del perfil de abonado	conf.resp.
Resultado	M

FEA2	– Toma nota de la finalización de l procedimiento de actualización del perfil de abonado.

6.2.1.1.2 Modificación del perfil de abonado, Caso 2: supresión de los datos de usuario

Se ha cancelado la suscripción a uno o más servicios básicos o servicios suplementarios. Este procedimiento se utiliza para indicar los servicios que se han suprimido y los datos que específicamente deben eliminarse. Véase la figura 6.2.1.1.-2.

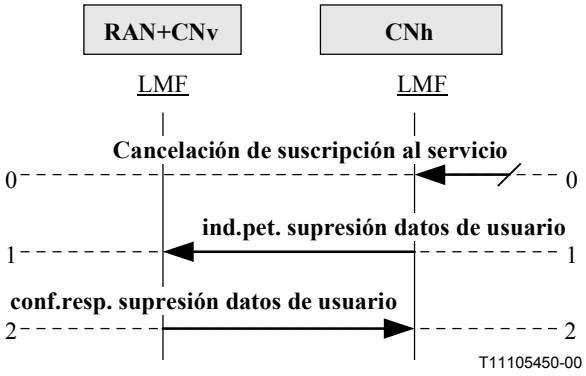


Figura 6.2.1.1-2/Q.1721 – Modificación del perfil de abonado, Caso 2: supresión de los datos de usuario

0. **Cancelación de suscripción al servicio**: es una petición para suprimir una suscripción a un servicio específico incluido en la lista de servicios suscritos.

FEA0	– Determina la necesidad de suprimir uno o más servicios básicos o suplementarios del perfil de usuario residente en la LMF de la red visitada.

1. **ind.pet. supresión datos de usuario**: se utiliza para suprimir datos de usuario específicos.

Supresión datos de usuario (Respuesta: éxito)	**ind.pet.**
IMUI	M
Datos de usuario suprimidos	M

FEA1	– Identifica el usuario IMT-2000 afectado. – Suprime los datos de usuario indicados en la ind.pet. supresión datos de usuario.

2. **conf.resp. supresión datos de usuario**: confirma la petición.

Supresión datos de usuario	**conf.resp.**
Resultado	M

FEA2	– Anota de la finalización del procedimiento de supresión de datos de usuario.

6.2.1.1.3 Modificación del perfil de abonado, Caso 3: eliminación del perfil de abonado

Se ha modificado el algoritmo de autenticación o la clave de autenticación del abonado, o bien, la modificación del perfil del abonado influye en el permiso que tienen el abonado para itinerar en la zona en que actualmente se encuentra. En este caso, el perfil del abonado debe eliminarse completamente de la red visitada y, por tanto, se utiliza el procedimiento "eliminación del perfil de abonado". Véase la figura 6.2.1.1-3.

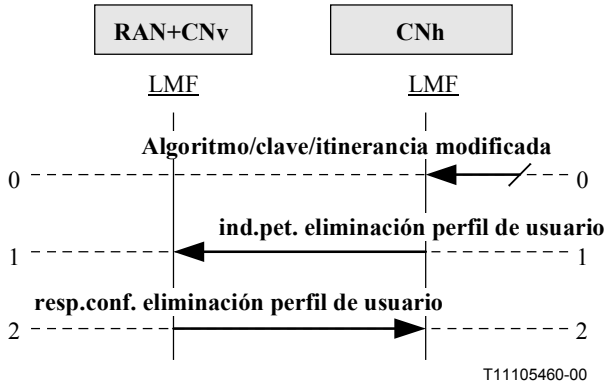


Figura 6.2.1.1-3/Q.1721 – Modificación del perfil de abonado, Caso 3: eliminación del perfil de abonado

0. **Algoritmo/clave/itinerancia modificada**: inicia la eliminación del perfil del abonado de la LMFv.

FEA0	– Inicia eliminación del perfil de usuario.

1. **ind.pet. eliminación perfil de usuario**: utilizada para solicitar la eliminación del perfil de usuario.

Eliminación perfil de usuario (Respuesta: éxito)	ind.pet.
IMUI	M

FEA1	– Identifica el usuario IMT-2000 afectado. – Suprime el perfil de usuario del usuario identificado.

2. **conf.resp. eliminación perfil de usuario**: se devuelve para confirmar las acciones tomadas por la LMFv.

Eliminación del perfil de usuario	conf.resp.
Resultado	M

FEA2	– Anota de la finalización del procedimiento de eliminación del perfil de usuario.

6.2.1.2 Interrogación sobre información de ubicación

El procedimiento de interrogación sobre información de ubicación puede ser invocado en los casos siguientes:

Caso 1: la LMFh interroga a la versión más actualizada de la información del usuario que reside en la LMFv, y

Caso 2: una red soporte interroga a la red originaria sobre la información de ubicación. El caso 1 puede implementarse independientemente o como un procedimiento anidado dentro del caso 2.

6.2.1.2.1 Interrogación de la LMF sobre información de ubicación

Mediante este procedimiento se describe como la LMFh interroga a la LMFv en relación con la información del usuario. Cuando se recibe una petición sobre información de ubicación del usuario, la LMFh puede solicitar a la red servidora la información más reciente o actualizada que exista sobre ubicación (por ejemplo, el estado y la ubicación de l usuario). Véase la figura 6.2.1.2-1.

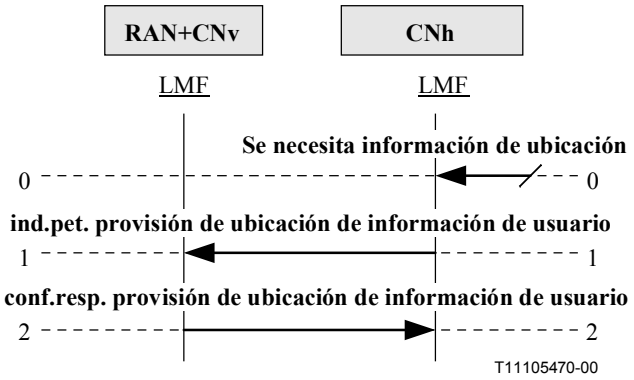


Figura 6.2.1.2-1/Q.1721 – Interrogación de la LMF sobre información de ubicación

0. **Se necesita información de ubicación**: inicia la petición de interrogación de información de ubicación del usuario.

FEA0	– Determina la necesidad de adquirir la información más reciente del usuario para el procedimiento de gestión de movilidad (por ejemplo, registro del terminal), o simplemente en un modo de actualización/retransmisión, para responder a una petición de información.

1. **ind.pet. provisión de información de ubicación de usuario**: la LMFh lo envía a la LMFv para solicitar dicha información de usuario (por ejemplo, información de estado y de ubicación).

Provisión de información de ubicación de usuario (Respuesta: éxito o fracaso)	**ind.pet.**
Información solicitada	M
IMUI	O (nota)
IMDN	O (nota)

FEA1	– Identifica al usuario IMT-2000 afectado. – Recupera la información de usuario solicitada.
NOTA – Deben proporcionarse el IMUI o el IMDN.	

2. **conf.resp. provisión de información de ubicación de usuario**: la LMFv lo envía a la LMFh proporcionando la información de usuario solicitada (por ejemplo, información de estado y de ubicación).

Provisión de información de usuario	conf.resp.
Información de ubicación	O (nota)
Estado del usuario	O (nota)

FEA2	– Anota la finalización del procedimiento de provisión de información de usuario.
NOTA – Este IE se proporciona si se solicita y está disponible.	

6.2.1.2.2 Interrogación de la SCF sobre información de usuario

Este procedimiento permite a la SCF obtener información (por ejemplo, estado del terminal e información sobre su ubicación) que reside en la LMFh. La información se utiliza para soportar la prestación al usuario de servicios de red inteligente (RI). Véase la figura 6.2.1.2-2.

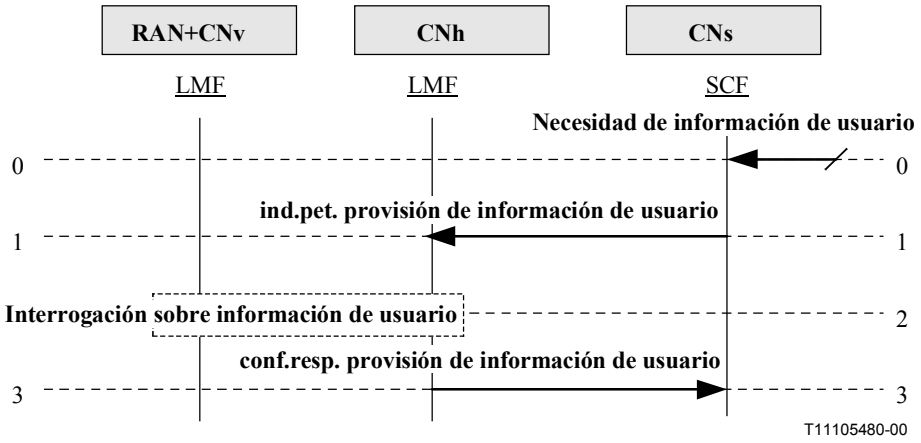


Figura 6.2.1.2-2/Q.1721 – Interrogación de la SCF sobre información de ubicación

0. **Necesidad de información de usuario**: inicia la petición de interrogación sobre información de usuario.

FEA0	– Determina la necesidad de adquirir información de usuario para proporcionar un servicio de red inteligente (RI).

1. **ind.pet. provisión de información de usuario**: la SCF de la red soporte lo envía a la LMFh para solicitar información de usuario.

Provisión de información de usuario (Respuesta: éxito o fracaso)	**ind.pet.**
Información solicitada	M
IMUI	O (nota)
IMDN	O (nota)

FEA1	– Identifica al usuario IMT-2000 afectado. – Recupera la información de usuario solicitada. Si la información de usuario no está disponible, solicita la información de la LMFv mediante el procedimiento de interrogación sobre información de usuario.
NOTA – Deben proporcionarse el IMUI o el IMDN.	

2. **Interrogación sobre información de usuario**: se realiza si se solicita.

3. **conf.resp. provisión de información de usuario**: es la respuesta de la LMFh a la SCF en la que proporciona la información de usuario solicitada.

Provisión de información de usuario	**conf.resp.**
Información de ubicación	M
Estado del terminal	M

FEA3	– Utiliza la información recibida en el SLP que se ha ejecutado.

6.2.1.3 Transferencia del perfil de abonado

Este procedimiento se invoca cuando un usuario IMT-2000 intenta registrarse en una red visitada. Este procedimiento es necesario como módulo común para la transferencia del perfil del usuario desde la LMFh a la LMFv cuando un usuario itinera en una red servidora fuera de su red originaria. Véase la figura 6.2.1.3-1.

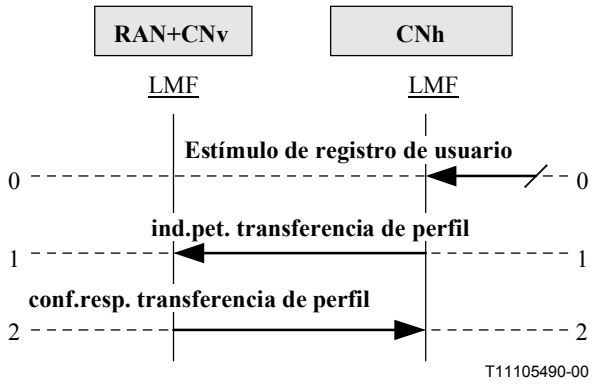


Figura 6.2.1.3-1/Q.1721 – Transferencia del perfil de abonado

0. Estímulo de registro de usuario: inicia este procedimiento.

FEA0	– Determina que el perfil del usuario es necesario para soportar a un usuario como usuario visitante.

1. **ind.pet. transferencia de perfil**: la LMFh lo envía a la LMFv para proporcionar el perfil para el usuario itinerante.

Transferencia de perfil (Respuesta: éxito)	**ind.pet.**
IMUI	M
Perfil de abonado	M

FEA1	– Identifica al usuario IMT-2000 en cuestión y almacena el perfil.

2. **conf.resp. transferencia de perfil**: es la respuesta de la LMFv a la LMFh confirmando la actualización del perfil de servicio del usuario con datos que proporciona la LMFh.

Transferencia de perfil	**conf.resp.**
Resultado	M

FEA2	– Anota la transferencia exitosa del perfil.

6.2.2 Recuperación de la identidad del usuario

6.2.2.1 Recuperación y actualización de la identidad

La UIMF mantiene la información sobre la TMUI, LAI e IMUI del usuario IMT-2000. Para el inicio de la llamada, la terminación de la llamada, la actualización de la ubicación del terminal, etc., el terminal móvil tiene que recuperar información sobre la IMUI, el TMUI y LAI. Para la actualización de la ubicación del terminal, el terminal móvil necesita actualizar la TMUI y la LAI.

Se describen a continuación los cinco diagramas de flujo de información siguientes relativos a la recuperación y actualización de la identidad:

- interrogación sobre la identidad del usuario móvil internacional (IMUI);
- interrogación sobre el identificador temporal de usuario móvil (TMUI);
- interrogación sobre el identificador de la zona de ubicación (LAI);
- actualización del identificador temporal de usuario móvil (TMUI);
- actualización del identificador de la zona de ubicación (LAI).

6.2.2.1.1 Interrogación sobre la identidad del usuario móvil internacional (IMUI)

Véase la figura 6.2.2.1-1.

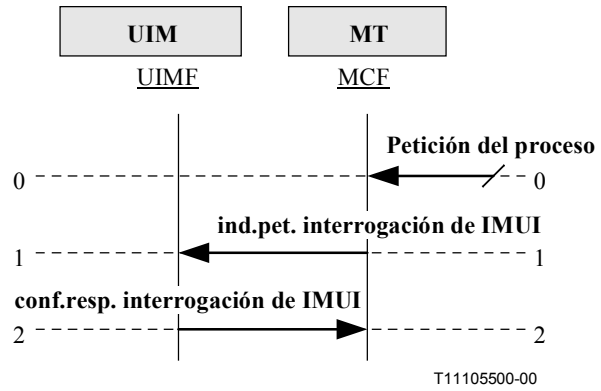


Figura 6.2.2.1-1/Q.1721 – Interrogación sobre IMUI

0. **Petición del proceso**: es el estímulo para la interrogación sobre la IMUI que recibe la MCF.

FEA0	– Inicia el procedimiento de interrogación de la IMUI.

1. **ind.pet. interrogación de IMUI**: se envía desde la MCF a la UIMF para recuperar la IMUI del abonado.

Interrogación de la IMUI (Respuesta: éxito o fracaso)	ind.pet.
Ninguno	N/A

FEA1	– Recupera la IMUI del abonado.

2. **conf.resp. interrogación de IMUI**: es la respuesta a la petición.

Interrogación de la IMUI	conf.resp.
IMUI	M

FEA2	– Registra la IMUI.

6.2.2.1.2 Interrogación sobre el identificador temporal de usuario móvil (TMUI)

Véase la figura 6.2.2.1-2.

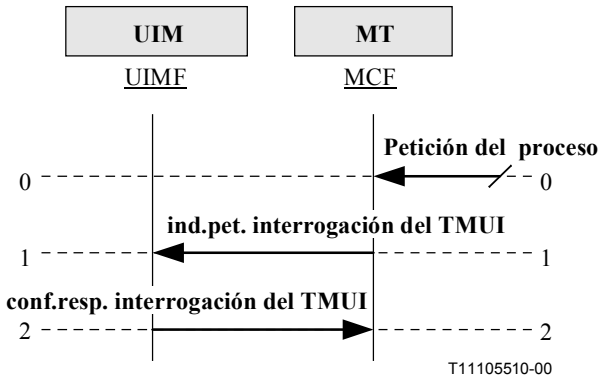


Figura 6.2.2.1-2/Q.1721 – Interrogación sobre TMUI

0. Petición del proceso: es el estímulo que la MCF recibe para la interrogación sobre TMUI.

FEA0	– Inicia el procedimiento de interrogación TMUI.

1. **ind.pet. interrogación del TMUI**: se envía desde la MCF a la UIMF para recuperar el TMUI del abonado.

Interrogación del TMUI (Respuesta: éxito o fracaso)	ind.pet.
Ninguno	N/A

FEA1	– Recupera el TMUI del abonado.

2. **conf.resp. interrogación del TMUI**: es la respuesta a la petición.

Interrogación del TMUI	conf.resp.
TMUI	M
ID de la fuente de asignación del TMUI	M

FEA2	– Registra el TMUI y la ID de la fuente de asignación del TMUI.

6.2.2.1.3 Interrogación sobre el identificador de la zona de ubicación (LAI)

Véase la figura 6.2.2.1-3.

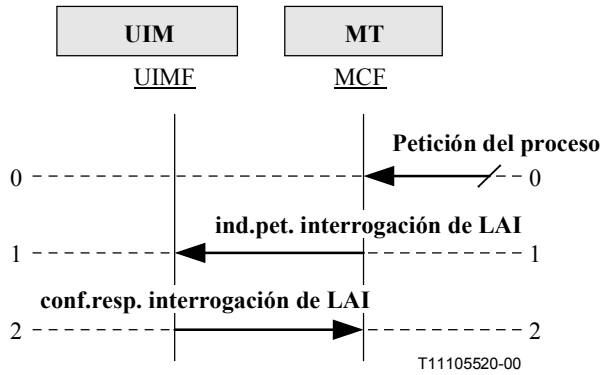


Figura 6.2.2.1-3/Q.1721 – Interrogación sobre el LAI

0. **Petición del proceso**: es el estímulo que la MCF recibe para la interrogación de LAI.

FEA0	– Inicia el procedimiento de interrogación de LAI.

1. **ind.pet. interrogación de LAI**: se envía desde la MCF a la UIMF para recuperar el LAI del abonado.

Interrogación de LAI (Respuesta: éxito o fracaso)	ind.pet.
Ninguno	N/A

FEA1	– Recupera el LAI del abonado.

2. **conf.resp. interrogación de LAI**: es la respuesta a la petición.

Interrogación de LAI	conf.resp.
LAI	M

FEA2	– Registra el LAI.

6.2.2.1.4 Actualización del identificador temporal de usuario móvil (TMUI)

Véase la figura 6.2.2.1-4.

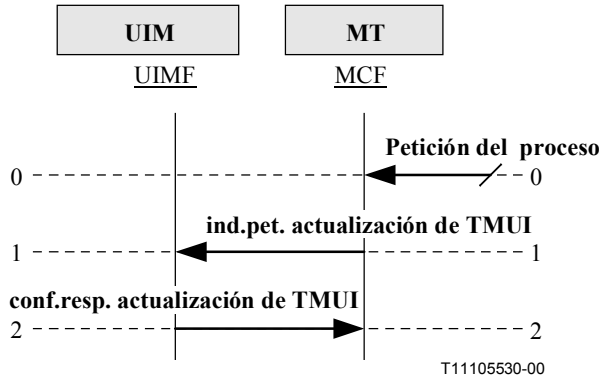


Figura 6.2.2.1-4/Q.1721 – Actualización del TMUI

0. **Petición del proceso**: estímulo para la actualización del TMUI recibido por la MCF.

FEA0	– Inicia el procedimiento de actualización del TMUI.

1. **ind.pet. actualización de TMUI**: enviado desde la MCF a la UIMF para actualizar el TMUI del abonado.

Actualización de TMUI (Respuesta: éxito o fracaso)	ind.pet.
TMUI	M
ID de fuente de asignación de TMUI	M

FEA1	– Actualización del TMUI del abonado y registro de la ID de la fuente de asignación de TMUI.

2. **conf.resp. actualización de TMUI**: es la respuesta a la petición.

Actualización de TMUI	conf.resp.
Ninguno	N/A

FEA2	– Anota la finalización con éxito del proceso.

6.2.2.1.5 Actualización del identificador de la zona de ubicación (LAI)

Véase la figura 6.2.2.1-5.

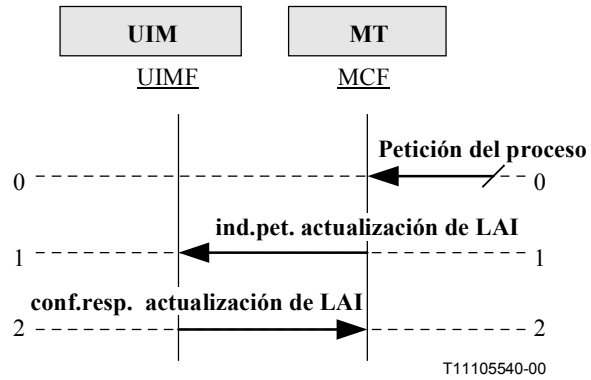


Figura 6.2.2.1-5/Q.1721 – Actualización de LAI

0. **Petición del proceso**: estímulo para la actualización del LAI recibido por la MCF.

FEA0	– Inicia el procedimiento de actualización del LAI.

1. **ind.pet. actualización de LAI**: enviado desde la MCF a la UIMF para actualizar el LAI del abonado.

Actualización de LAI (Respuesta: éxito o fracaso)	ind.pet.
LAI	M

FEA1	– Actualización del LAI del abonado

2. **conf.resp. actualización de LAI**: es la respuesta a la petición.

Actualización de LAI	conf.resp.
Ninguno	N/A

FEA2	– Anota la finalización con éxito del proceso.

6.2.2.2 Recuperación de la ID del usuario

Este procedimiento se utiliza para convertir el TMUI en el IMUI del usuario. La red recién visitada inicia este procedimiento cuando recibe el TMUI, o un conjunto de TMUI, así como la ID de la fuente de asignación de TMUI, como ID de usuario desde el lado móvil.

Para el registro y actualización de la ubicación se presentan dos casos:

– Caso 1: TMUI asignado por la LMF recién visitada (véase 6.2.2.1.2).

– Caso 2: TMUI asignado por otra LMF distinta de la LMF recién visitada (esta subcláusula).

Si la red recién visitada no puede recuperar con éxito la IMUI (por ejemplo, pierde el TMUI), intenta recuperar la IMUI del usuario IMT-2000 de la UIMF (véase 6.2.2.1.1). Véase la figura 6.2.2.2-1.

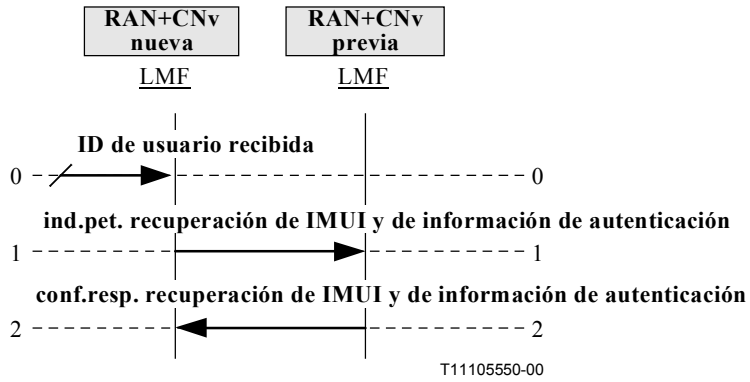


Figura 6.2.2.2-1/Q.1721 – Diagrama de flujo de recuperación de la IMUI y de la información de autenticación

0. **ID de usuario recibida**: se recibe de la LMF de la red recién visitada e inicia el procedimiento.

FEA0	Para el caso 1: – Recuperación de la IMUI del usuario IMT-2000 solicitante con el TMUI. Para el caso 2: – Identifica la LMF por la que se asigna al TMUI la ID de la fuente de asignación de TMUI.

1. **ind.pet. recuperación de IMUI y de información de autenticación**: utilizada para recuperar la IMUI con el TMUI. Este flujo de información se envía a la LMF de la red previamente visitada.

Recuperación de la IMUI y la información de autenticación (Respuesta: éxito o fracaso)	**ind.pet.**
TMUI	M
ID de fuente de asignación de TMUI	M

FEA1	– Recupera la IMUI y las tripletas de autenticación no utilizadas del usuario IMT-2000 solicitante con el TMUI.

2. **conf.resp. recuperación de IMUI y de información de autenticación**: es la respuesta a la petición.

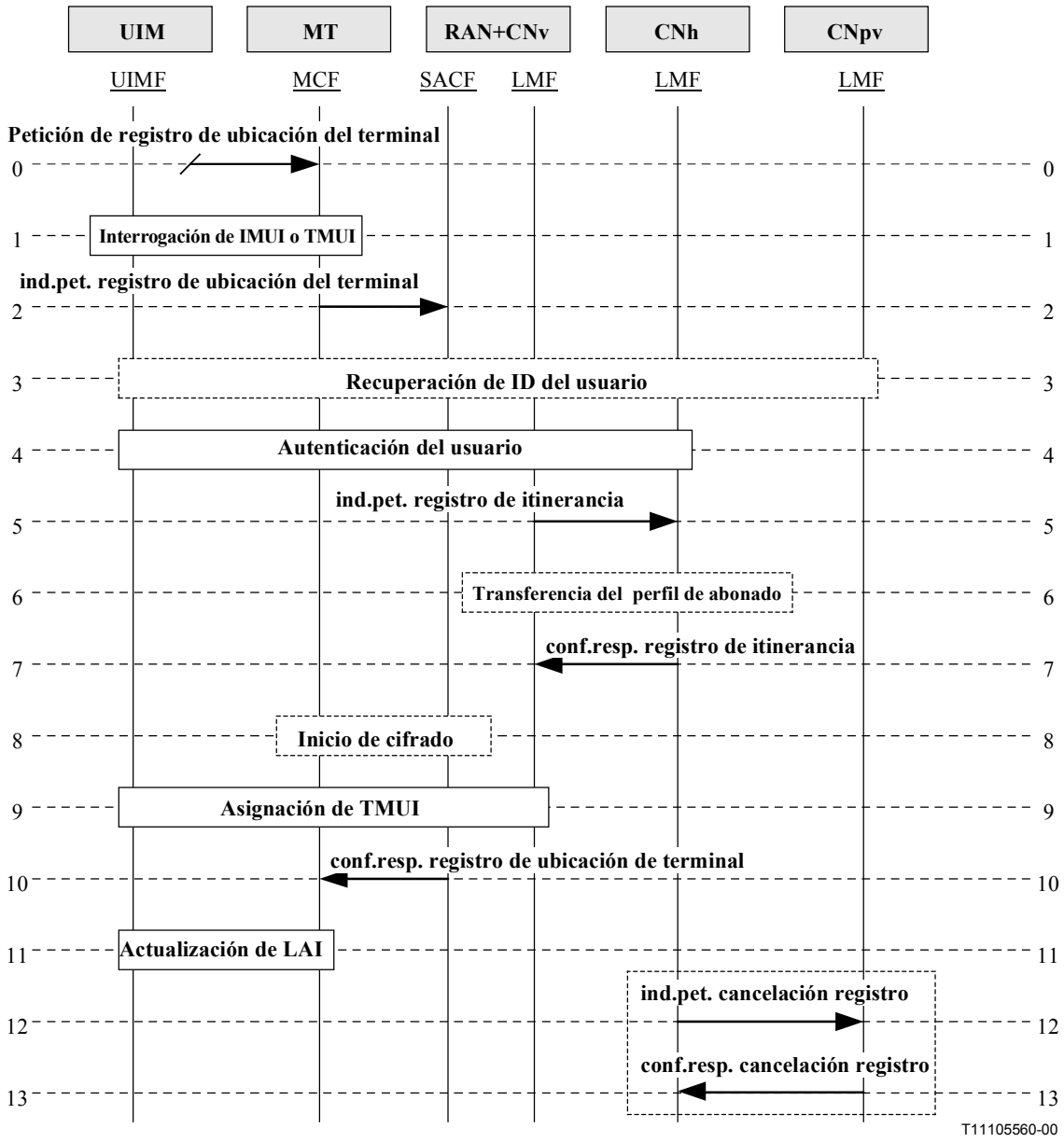
Recuperación de la IMUI y la información de autenticación	conf.resp.
IMUI	M
Resultado	M
Puesta(s) a prueba	O (nota 1)
Respuesta(s) a puesta a prueba	O (nota 1)
Clave(s) de cifrado	O (nota 2)

FEA2	– Confirma la finalización de la recuperación de IMUI.
NOTA 1 – Incluida si debe realizarse la autenticación. NOTA 2 – Se devuelve si está disponible.	

6.2.3 Gestión del registro

6.2.3.1 Registro de la ubicación del terminal

Esta facilidad se utiliza cuando un usuario IMT-2000 informa al sistema sobre su ubicación. Este procedimiento permite registrar en la red visitada la zona correspondiente a la ubicación del usuario IMT-2000. El procedimiento de registro de ubicación del terminal se realiza cuando no se dispone de información previa sobre el usuario en el momento en que aparece por vez primera en un dominio de red. En este procedimiento, se elimina de la red previamente visitada toda la información sobre el usuario. La actualización de la información de la zona de ubicación puede también tener lugar después de un fallo de la red o del terminal. Véase la figura 6.2.3.1-1.



NOTA – Los flujos de información 12 y 13 pueden ocurrir después del IF 5 y son independientes de los IF de 8 a 11 inclusive.

Figura 6.2.3.1-1/Q.1721 – Registro de la ubicación del terminal

0. **Petición de registro de ubicación del terminal**: se inicia cuando el MT se enciende e intenta registrarse en la red utilizando la información difundida por la misma.

FEA0	– Obtiene la identidad del usuario.

1. **Interrogación de IMUI o TMUI**: se utiliza para obtener la IMUI o TMUI según proceda.

2. **ind.pet. registro de ubicación del terminal**: se utiliza para registrar en la red la información de la zona de ubicación del terminal móvil.

Registro de ubicación del terminal (Respuesta: éxito o fracaso)	req.ind.
ID de usuario	M (nota 1)
Información de TC	O (nota 2)
AUTH_R	O (nota 3)
Confirmación de RANDG	O (nota 3)
CHCNT	O (nota 3)

FEA2	– Inicia procedimiento de recuperación de ID de usuario para recuperar la IMUI, si se utiliza el TMUI.
NOTA 1 – IMUI o TMUI según estén disponibles. NOTA 2 – Si está disponible, se envía para indicar los servicios que admite el terminal. NOTA 3 – Si se utiliza la puesta a prueba global (número aleatorio) en la información de difusión con fines de autenticación, se envían los datos de autenticación.	

3. **Recuperación de ID del usuario**: se ejecuta si se solicita.

4. **Autenticación del usuario**: se ejecuta.

5. **ind.pet. registro de itinerancia**: se utiliza para actualizar la dirección de LMFv en la red originaria.

Registro de itinerancia (Respuesta: éxito o fracaso)	ind.pet.
IMUI	M
Dirección de LMFv	M

FEA5	– Identifica al usuario IMT-2000 solicitante. – Actualiza la dirección de LMFv. – Identifica la dirección de LMFv de la red previamente visitada, si procede. – Inicia la actualización del perfil de usuario, si es necesario.

6. **Transferencia del perfil de abonado**: se ejecuta si es necesario.

7. **conf.resp. registro de itinerancia**: es la confirmación a la ind.pet. registro de itinerancia.

Registro de itinerancia	conf.resp.
Resultado	M

FEA7	– Confirma la finalización del registro de itinerancia del usuario IMT-2000. – Identifica el área de ubicación y la información de capacidad del terminal (TC). – Almacena el área de ubicación y la información de TC del usuario IMT-2000. – Invoca el procedimiento de actualización de TMUI del usuario IMT-2000.

8. **Inicio de cifrado**: se ejecuta si procede.

9. **Asignación de TMUI**: se ejecuta.

FEA9	– Analiza el resultado del procedimiento de actualización de TMUI.
NOTA – El módulo del procedimiento de actualización de TMUI está separado del módulo del procedimiento de autenticación del usuario a fin de asignar el TMUI después de que se haya creado el perfil del usuario en una red recién visitada.	

10. **conf.resp. registro de ubicación de terminal**: es la confirmación a la ind.pet. de registro de ubicación del terminal.

Registro de ubicación de terminal	**conf.resp.**
Resultado	M

FEA10	– Memoriza en el MT el identificador de la zona de ubicación de la ubicación actual.

11. **Actualización de LAI**: se ejecuta para actualizar en el UIM el identificador de la zona de ubicación.

12. **ind.pet. cancelación de registro**: se utiliza de forma facultativa para cancelar el registro del usuario en una red previamente visitada.

Cancelación de registro (Respuesta: éxito o fracaso)	**ind.pet.**
IMUI	M

FEA12	– Identifica al usuario IMT-2000 solicitante. – Elimina el perfil del usuario del usuario IMT-2000 solicitante. – Formula y envía la conf.resp. de cancelación de registro.

13. **conf.resp. cancelación de registro**: es la confirmación a la ind.pet. cancelación de registro.

Cancelación de registro	**conf.resp.**
Resultado	M

FEA8	– Identifica la red recién visitada.

6.2.3.2 Actualización de la ubicación del terminal

Esta facilidad se utiliza cuando un usuario IMT-2000 que itinera en un dominio de red notifica al sistema su nueva ubicación. Esta nueva información de la zona de ubicación se registra en la red visitada. La actualización de dicha información de zona de ubicación puede también tener lugar después de una fallo de la red o del terminal. Véase la figura 6.2.3.2-1.

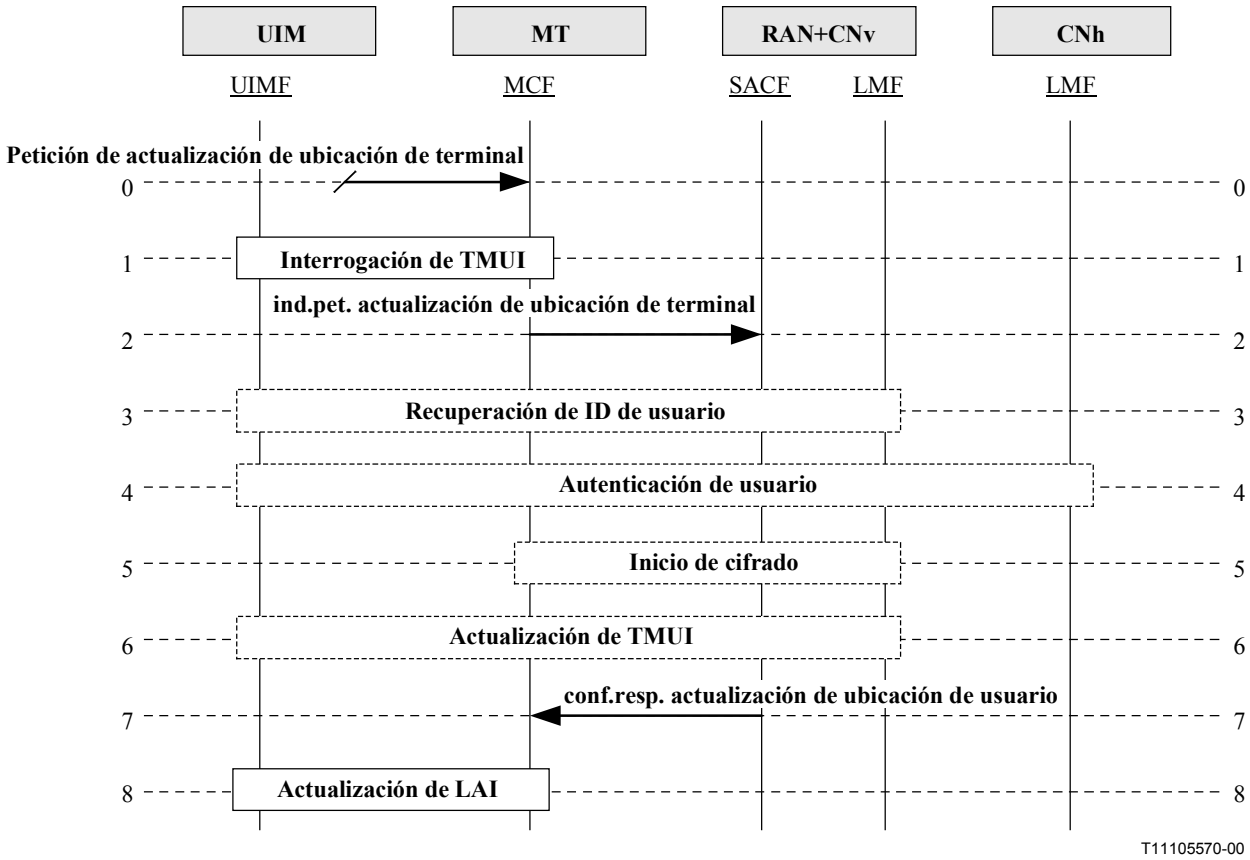


Figura 6.2.3.2-1/Q.1721 – Actualización de la ubicación del terminal

0. **Petición de actualización de ubicación de terminal**: la red visitada inicia la petición.

FEA0	– Inicia el procedimiento de interrogación de TMUI para recuperarlo.

1. **Interrogación de TMUI**: se ejecuta.

2. **ind.pet. actualización de ubicación de terminal**: se envía desde la MCF a la LMFv.

Actualización de la ubicación del terminal (Respuesta: éxito o fracaso)	**ind.pet.**
TMUI	M
ID de fuente de TMUI	M
AUTH_R	O (nota 1)
Confirmación de RANDG	O (nota 1)
CHCNT	O (nota 2)
Estado de terminal	O (nota 3)
Información de TC	O (nota 3)

FEA2	– Inicia el procedimiento de recuperación del ID de usuario, si el TMUI y la ID de la fuente de asignación de TMUI se utilizan como ID del usuario IMT-2000 en la petición de actualización de ubicación del terminal.
NOTA 1 – Incluida si se debe realizar la autenticación.	
NOTA 2 – Incluida si está disponible el cómputo histórico de la llamada.	
NOTA 3 – Se proporciona si está disponible.	

3. **Recuperación de ID de usuario**: se ejecuta para identificar al usuario IMT-2000 solicitante, si es necesario.

4. **Autenticación del usuario**: se ejecuta en el caso de que se llevara a cabo el procedimiento de recuperación del ID de usuario.

5. **Inicio del cifrado**: se ejecuta si se realizó el procedimiento de autenticación de usuario.

6. **Actualización del TMUI**: se ejecuta una vez se hayan ejecutado los dos procedimientos anteriores.

7. **conf.resp. actualización de ubicación de usuario**: es la confirmación a la ind.pet. de actualización de ubicación de terminal.

Actualización de la ubicación del usuario	**conf.resp.**
Resultado	M

FEA7	– Registra el LAI. – Inicia el procedimiento de actualización del LAI.

8. **Actualización de LAI**: se ejecuta el procedimiento.

6.2.3.3 Desincorporación

Mediante este procedimiento el terminal notifica explícitamente a la red servidora que no puede ser alcanzado (por ejemplo, por estar apagado o en estado de no molesten).

En algunas situaciones (por ejemplo, después de un periodo de inactividad) la red visitada puede decidir notificar a la LMFh que el usuario no está accesible, de forma que, por ejemplo, cualquier petición de encaminamiento de llamadas dirigidas al móvil se tratará en consecuencia.

Existen otras situaciones en las que está implícita la utilización de esta facilidad (por ejemplo, descarga de batería o degradación de la señal radioeléctrica). Véase la figura 6.2.3.3-1.

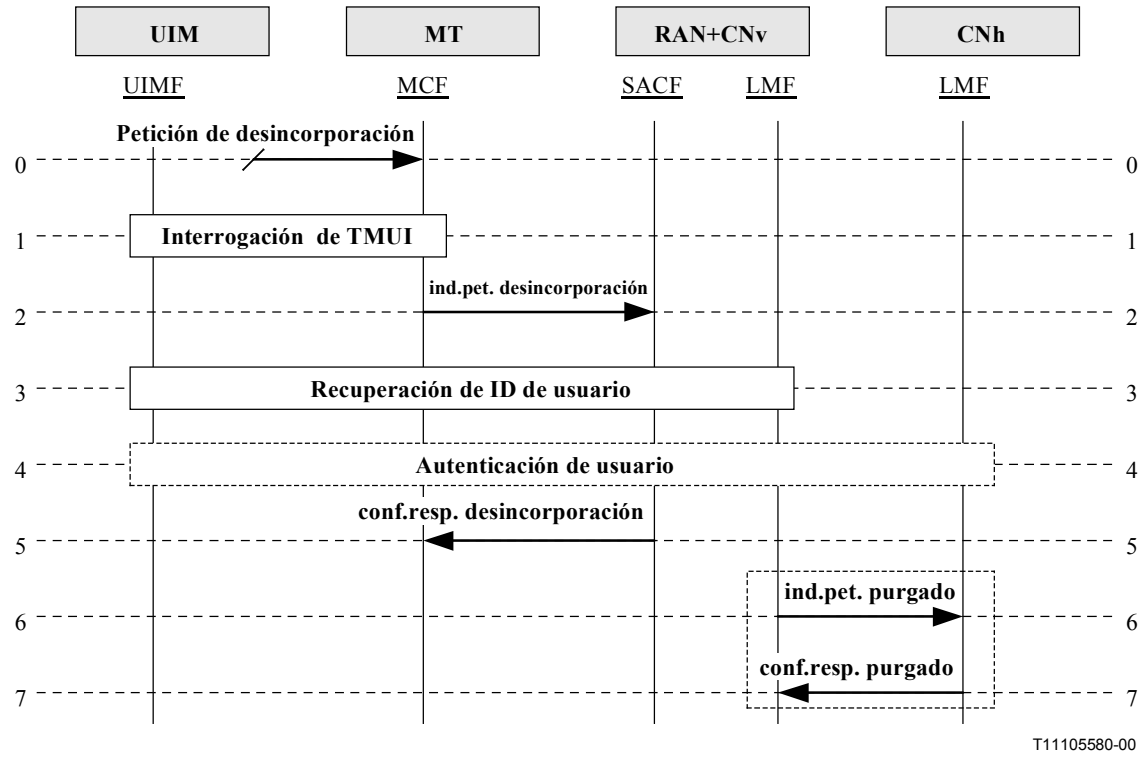


Figura 6.2.3.3-1/Q.1721 – Desincorporación

0. **Petición de desincorporación**: es el estímulo que inicia el procedimiento de desincorporación.

FEA0	– Inicia el procedimiento de interrogación de TMUI para recuperar el TMUI.

1. **Interrogación de TMUI**: se ejecuta el procedimiento.

2. **ind.pet. de desincorporación**: utilizado por el terminal para notificar a la red servidora que va a permanecer inalcanzable.

Desincorporación (Respuesta: éxito o fracaso)	**ind.pet.**
ID de usuario	M (nota)

FEA2	– Inicia el procedimiento de recuperación de ID de usuario si tanto el TMUI como el ID de la fuente de asignación de TMUI, se utilizan como ID del usuario IMT-2000 en la petición de desincorporación.
NOTA – TMUI debe utilizarse en lugar de IMUI como el ID de usuario IMT-2000 a fin de mantener confidencial la identidad del usuario.	

3. **Recuperación de ID de usuario**: se ejecuta el procedimiento.

4. **Procedimiento de autenticación de usuario**: se ejecuta si es necesario.

5. **conf.resp. desincorporación**: es la confirmación de la ind.pet. de desincorporación.

Desincorporación	conf.resp.
Resultado	M

FEA5	– Anota que se ha finalizado el procedimiento de desincorporación.

6. **ind.pet. purgado**: utilizado por la red servidora para notificar a la red originaria que el terminal no está alcanzable.

Purgado (Respuesta: éxito o fracaso)	ind.pet.
IMUI	M
Dirección de LMFv	O

FEA6	– Marca al usuario IMT-2000 como no alcanzable en la red que hace la notificación.

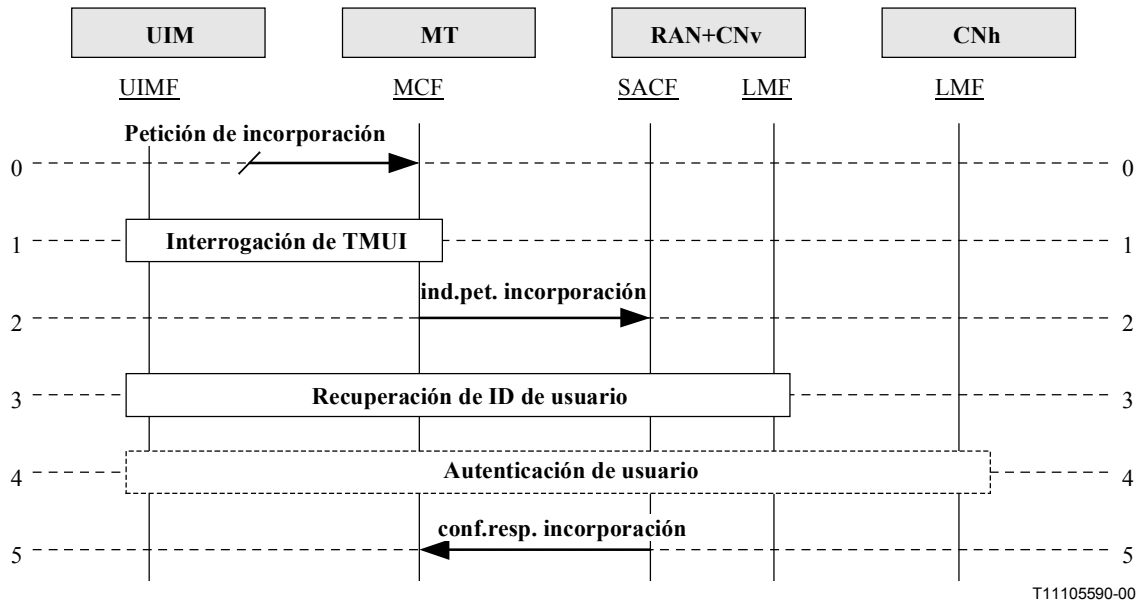
7. **conf.resp. purgado**: es la confirmación a ind.pet. purgado.

Purgado	conf.resp.
Resultado	M

FEA7	– Decide si el registro del abonado debe ser eliminado de la LMFv.

6.2.3.4 Incorporación

Véase la figura 6.2.3.4-1.



NOTA – Si falla el procedimiento de incorporación, el MT debe interpretarlo como que es necesario el procedimiento de registro de ubicación del terminal.

Figura 6.2.3.4-1/Q.1721 – Incorporación

0. **Petición de incorporación**: inicia el procedimiento de incorporación.

FEA0	– Inicia el procedimiento de interrogación de TMUI para recuperar el TMUI.

1. **Interrogación de TMUI**: se ejecuta.

2. **ind.pet. incorporación**: utilizado por el terminal para notificar a la red servidora que el MT es alcanzable.

Incorporación (Respuesta: éxito o fracaso)	ind.pet.
TMUI	M

FEA0	– Inicia el procedimiento de recuperación de ID de usuario.

3. **Recuperación de ID de usuario**: se ejecuta.

4. **Autenticación de usuario**: se ejecuta, si es necesario como resultado del procedimiento anterior.

FEA4	– Sobre la base de información de estado de un mensaje corto en la LMFv (por ejemplo, fallo de transferencia de mensaje corto por no estar alcanzable el terminal), comienza el procedimiento de notificación de mensajes cortos (no se muestra en la figura). – Si la bandera del LMFv indica que los datos de itinerancia del sistema originario no son fiables, se realiza la actualización de la ubicación (no se muestra en la figura). – Acusa recibo de la ind.pet. incorporación.

5. **conf.resp. incorporación**: es la confirmación de la ind.pet. de incorporación.

Incorporación	conf.resp.
Resultado	M

FEA 5	– El MT continua el funcionamiento normal.

6.2.4 Recuperación de fallos en los datos de ubicación

Esta categoría de procedimientos trata de la recuperación que debe llevarse a cabo tras una situación de fallo. El objetivo es establecer con certeza cuales son los datos almacenados en distintos nodos que siguen siendo consistentes. En esta categoría se definen tres procedimientos:

– Datos no fiables de itinerante.

– Indicación de verificación de datos de servicios suplementarios.

– Restablecimiento de datos de LMF.

6.2.4.1 Datos no fiables de itinerante

El procedimiento datos no fiables del itinerante se utiliza para informar al sistema visitado que los datos del terminal móvil itinerante del sistema originario no son fiables (por ejemplo, debido a un fallo del sistema). Véase la figura 6.2.4.1-1.

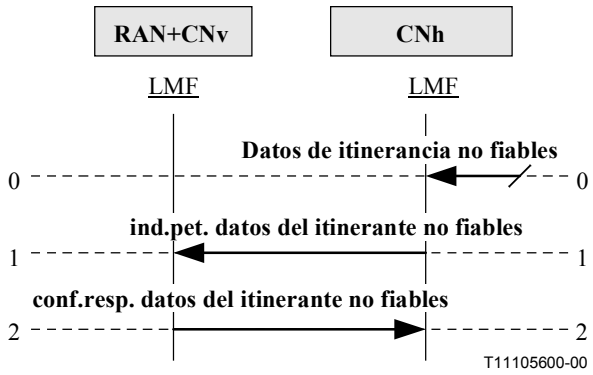


Figura 6.2.4.1-1/Q.1721 – Datos no fiables de itinerante

0. **Datos de itinerancia no fiables**: indica que los datos del itinerante no son fiables e inicia la notificación a otros sistemas.

FEA0	– LMFh se prepara para informar a otro(s) sistema(s) de que ha experimentado un fallo que convierte sus datos de itinerancia en no fiables.

1. **ind.pet. datos del itinerante no fiables**: se envía de LMFh a LMF(s) de otros sistemas.

Datos del itinerante no fiables (Respuesta: éxito o fracaso)	ind.pet.
ID de red originaria	M

FEA1	– La LMFv elimina todos los registros de los abonados asociados a la LMFh que envía el mensaje.

2. **conf.resp. datos del itinerante no fiables**: es la respuesta a la petición.

Itinerante no fiable	conf.resp.
Resultado	M

FEA2	– Anota el acuse de recibo.

6.2.4.2 Indicación de verificación de datos de servicios suplementarios

La facilidad de verificación de datos de servicios suplementarios es utilizada por la LMFh para indicar al usuario móvil que los datos de los servicios suplementarios pueden ser alterados debido a un reinicio. Cuando esta indicación se recibe de la LMFh, la LMFv la envía a la SACF que, a su vez, la envía a la MCF. Véase la figura 6.2.4.2-1.

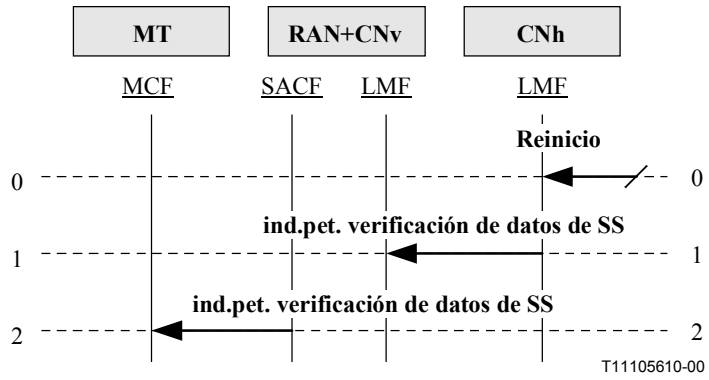


Figura 6.2.4.2-1/Q.1721 – Indicación de verificación de datos de servicios suplementarios

0. **Reinicio**: es el estímulo que inicia el procedimiento de verificación de datos de SS.

FEA0	– Determina que ha tenido lugar un reinicio y que el móvil debe ser informado de posibles cambios en los datos de los SS.

1. **ind.pet. verificación de datos de SS**: se envía de la LMFh a la LMFv.

Verificación de datos de SS (Respuesta: ninguna)	**ind.pet.**
Ninguno	N/A

FEA1	– Envía ind.pet. verificación de datos de SS.

2. **ind.pet. verificación de datos de SS**: enviado de la SACF a la MCF.

Verificación de datos de SS (Respuesta: ninguna)	**ind.pet.**
Ninguno	N/A

FEA2	– El terminal debe indicar al usuario que debe verificarse la información de los SS.

6.2.4.3 Restablecimiento de datos de la función de gestión de ubicaciones (LMF)

La facilidad de restablecimiento de datos de LMF se utiliza para indicar a la LMFh que ha recibido una operación de provisión de número de itinerancia para una IMUI desconocida o para una IMUI conocida cuyo indicador "confirmado por la HLR" tiene el valor "no confirmado". El servicio se utiliza para actualizar el número de ubicación (es decir, LAI y dirección de LMFv) en la LMFh, si existe, y para solicitar que la LMFh envíe a la LMFv todos los datos de perfil de abonado. Véase la figura 6.2.4.3-1.

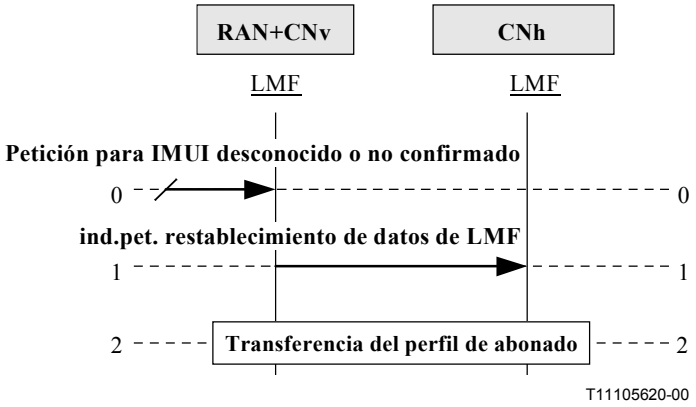


Figura 6.2.4.3-1/Q.1721 – Restablecimiento de datos de LMF

0. **Petición para IMUI desconocido o no confirmado**: inicia el procedimiento de restablecimiento de datos de LMF.

FEA0	– Determina que se ha solicitado un número de itinerancia para una IMUI desconocida o para una IMUI que debe ser confirmado por la LMFh.

1. **ind.pet. restablecimiento de datos de LMF**: se envía desde la LMFv a la LMFh.

Restablecimiento de datos de LMF (Respuesta: éxito o fracaso)	ind.pet.
IMUI	M
LAI	M

FEA1	– Ejecuta el procedimiento de transferencia del perfil de abonado.

2. **Transferencia del perfil de abonado**: se ejecuta para finalizar el proceso de restablecimiento.

7 Control de la llamada básica y del portador

Esta cláusula proporciona los flujos de información para el control de la llamada básica y del portador en sistemas IMT-2000 para el establecimiento y liberación de llamadas de voz mediante portadores basados en circuitos conmutados o en paquetes.

El control de la llamada básica y del portador incluye flujos de información para:

- llamadas salientes de móviles;
- radiobúsqueda de terminales;
- encaminamiento de llamadas;
- llamadas entrantes a móviles;
- liberación de llamadas móviles;
- llamadas de emergencia; y
- llamadas con prioridad.

7.1 Llamadas salientes desde móviles

El procedimiento de llamadas salientes desde móviles implica que un abonado móvil inicia una llamada desde el estado en reposo (llamada inicial) o desde el estado ocupado (llamada adicional).

Antes de que se establezca la llamada, la red visitada valida la parte llamante y puede invocar servicios sobre la base del intento de inicio de llamada. Este procedimiento es local a la red servidora o bien utiliza la capacidad de red del entorno virtual originario (VHE).

7.1.1 Llamada saliente inicial desde móvil

El procedimiento de llamada saliente inicial desde el móvil se utiliza cuando el usuario origina una llamada desde el estado de reposo. Véase la figura 7.1.1-1.

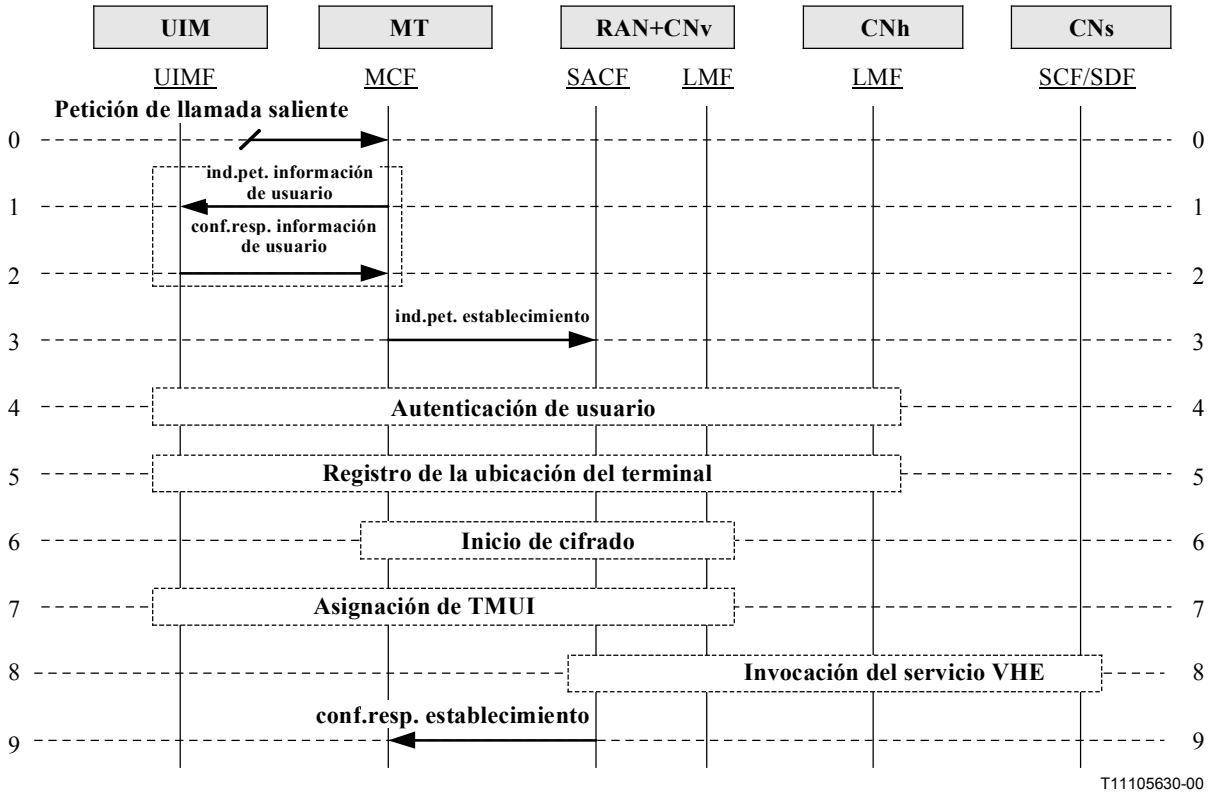


Figura 7.1.1-1/Q.1721 – Diagrama de flujo de información de llamada saliente inicial desde móvil

0. **Petición de llamada saliente**: el usuario móvil inicia una llamada saliente (originada en el móvil) estando en el estado de reposo.

FEA0	– El MT puede interactuar con el abonado para acumular información. Puede invocar la lógica del servicio (por ejemplo, lista de marcación rápida).

1. **ind.pet. información de usuario**: la MCF interroga opcionalmente a la UIMF para conseguir información/instrucciones adicionales.

Información de usuario (Respuesta: éxito o fracaso)	ind.pet.
Petición de información de UIM	M

FEA1	– Opcionalmente invoca la lógica del servicio local (por ejemplo, basada en la UIM). – Recopila la información solicitada.

2. **conf.resp. información de usuario**: la UIMF devuelve a la MCF la información de usuario solicitada.

Información de usuario	conf.resp.
Respuesta a la información de UIM	M

FEA2	Inicia la petición de establecimiento de llamada y de portador.

3. **ind.pet. establecimiento**: la MCF establece la llamada y solicita a la SACF de la red servidora que asigne un canal portador.

Establecimiento (Respuesta: éxito o fracaso)	ind.pet.
Id de usuario	M (nota 1)
Número llamado	M
Número llamante	M
Identificador de servicio	M
ID de facturación	O (nota 2)
Capacidad portadora	O (nota 3)
Calidad de servicio	O (nota 4)
AUTH_R	O (nota 5)
RANDC	O (nota 5)
CHCNT	O (nota 5)
IMEI	O (nota 5)
AUTHKEYS	O (nota 6)
SRES	O (nota 7)

FEA3	– Opcionalmente, invoca y espera que se complete la autenticación del usuario. – Opcionalmente, invoca y espera que se complete el registro de ubicación del terminal. – Opcionalmente, invoca y espera que se complete el inicio de cifrado. – Establece la llamada y el canal portador.
NOTA 1 – Incluye IMUI o TMUI según esté disponible. Por seguridad, se recomienda utilizar TMUI por medios radioeléctricos. NOTA 2 – Incluido, si es necesario, por el proveedor de servicio originario. NOTA 3 – Incluido para indicar la capacidad del canal portador. NOTA 4 – Incluido para indicar la calidad de servicio deseada. NOTA 5 – Incluido para proporcionar información relacionada con la autenticación sólo para sistemas basados en SSD. NOTA 6 – Incluido para proporcionar información relacionada con la autenticación sólo para sistemas no basados en SSD. NOTA 7 – Incluido para proporcionar el resultado de la signatura.	

4. **Autenticación del usuario**: se realiza si para este intento de llamada es necesaria la autenticación.

5. **Registro de la ubicación del terminal**: si el MT no está registrado en la red visitada, se realiza el registro de ubicación.

6. **Inicio del cifrado**: se inicia si para este intento de llamada se precisa el cifrado.

7. **Asignación de TMUI**: si es preciso asignar un TMUI, puede hacerse en cualquier momento después del inicio del cifrado.

8. **Invocación del servicio de VHE**: sobre la base del perfil del usuario, la red visitada puede invocar la lógica del servicio de red inteligente. Esto puede ocurrir en cualquier punto definido y activo de detección del disparo.

9. **conf.resp. establecimiento**: la SACF de la red visitada informa que se ha completado con éxito el establecimiento de la llamada y del portador.

Establecimiento	conf.resp.
ID del portador	M

FEA9	Completa el establecimiento de llamada sobre el portador seleccionado.

7.1.2 Llamada saliente adicional desde móvil

En este caso un abonado móvil origina una segunda llamada cuando aún se encuentra en una llamada, es decir, se produce una llamada a tres. El procedimiento se realiza de forma semejante a como se hace para las llamadas móviles salientes.

7.2 Radiobúsqueda del terminal

El procedimiento de radiobúsqueda del terminal se utiliza para realizar la radiobúsqueda de un terminal móvil. Véase la figura 7.2-1.

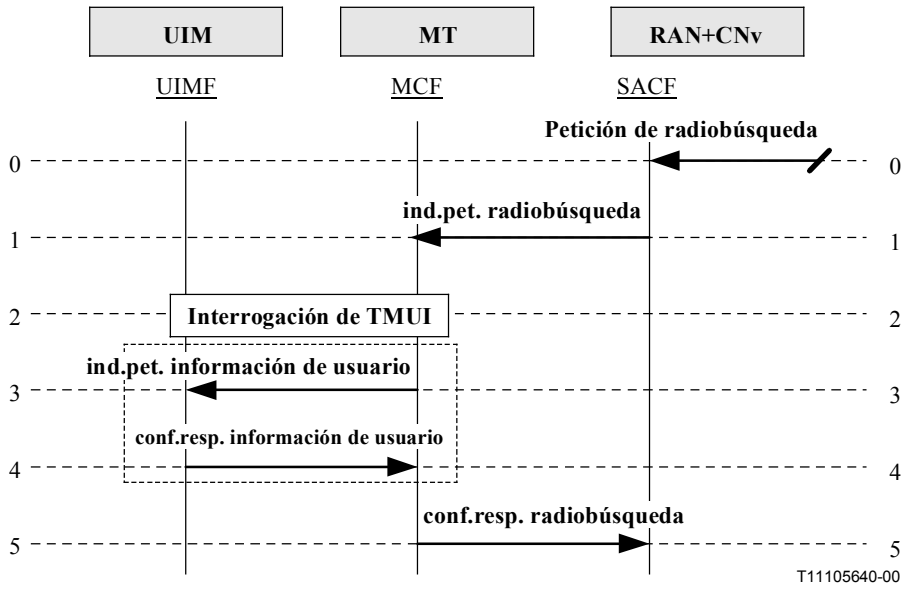


Figura 7.2-1/Q.1721 – Radiobúsqueda del terminal

0. Petición de radiobúsqueda: una llamada entrante móvil da lugar a una petición de radiobúsqueda en la red visitada.

FEA0	– La red visitada envía la petición de radiobúsqueda a la MCF.

1. **ind.pet. radiobúsqueda**: la red visitada intenta la radiobúsqueda del terminal móvil.

Radiobúsqueda (Respuesta: éxito o fracaso)	**ind.pet.**
TMUI	M

FEA1	– Prepara la interrogación de TMUI.

2. **Interrogación de TMUI**: la MCF recupera el TMUI de la UIMF, lo compara con el TMUI recibido de la red visitada y determina que la petición de radiobúsqueda es para el terminal móvil en cuestión.

3. **ind.pet. información de usuario**: opcionalmente, la MCF interroga a la UIMF en relación con instrucciones o información adicional.

Información de usuario (Respuesta: éxito o fracaso)	**ind.pet.**
Petición de tratamiento de la terminación	O (nota)

FEA3	Ordena que la MCF responda a la radiobúsqueda.
NOTA – Incluido para solicitar instrucciones de respuesta a la radiobúsqueda de la UIMF.	

4. **conf.resp. información de usuario**: la UIMF devuelve a la MCF la información solicitada.

Información de usuario	**conf.resp.**
Información de tratamiento de la terminación	O (nota)

FEA4	– Preparada para responder a la radiobúsqueda.
NOTA – Incluido para indicar el tipo de tratamiento de terminación de llamada que debe aplicarse.	

5. **conf.resp. radiobúsqueda**: la MCF responde a la radiobúsqueda.

Radiobúsqueda	**conf.resp.**
Ninguno	(nota)

FEA5	– Ninguno
NOTA – La confirmación de respuesta está vacía. Su sola presencia basta para indicar éxito.	

7.3 Encaminamiento de llamadas en la red

Esta subcláusula se ocupa de los flujos de información extremo a extremo para el encaminamiento de llamadas entre familias (o entre redes). El encaminamiento de una llamada dentro de un miembro de una familia IMT-2000 se considera una operación intrafamilia y no se considera en esta subcláusula.

El procedimiento de encaminamiento de llamadas se utiliza para conseguir una dirección (un número de itinerancia) del elemento de red de la red visitada en el que se encuentra el usuario a fin realizar el encaminamiento que permita terminar la llamada. La dirección se vincula de forma dinámica a la identidad del usuario.

Los datos de la información de encaminamiento los necesita la red que interroga para solicitar a la red visitada de la parte llamada el "establecimiento de llamada". El término "información de encaminamiento" se refiere a toda la información necesaria para identificar la red visitada y la ubicación del terminal de usuario.

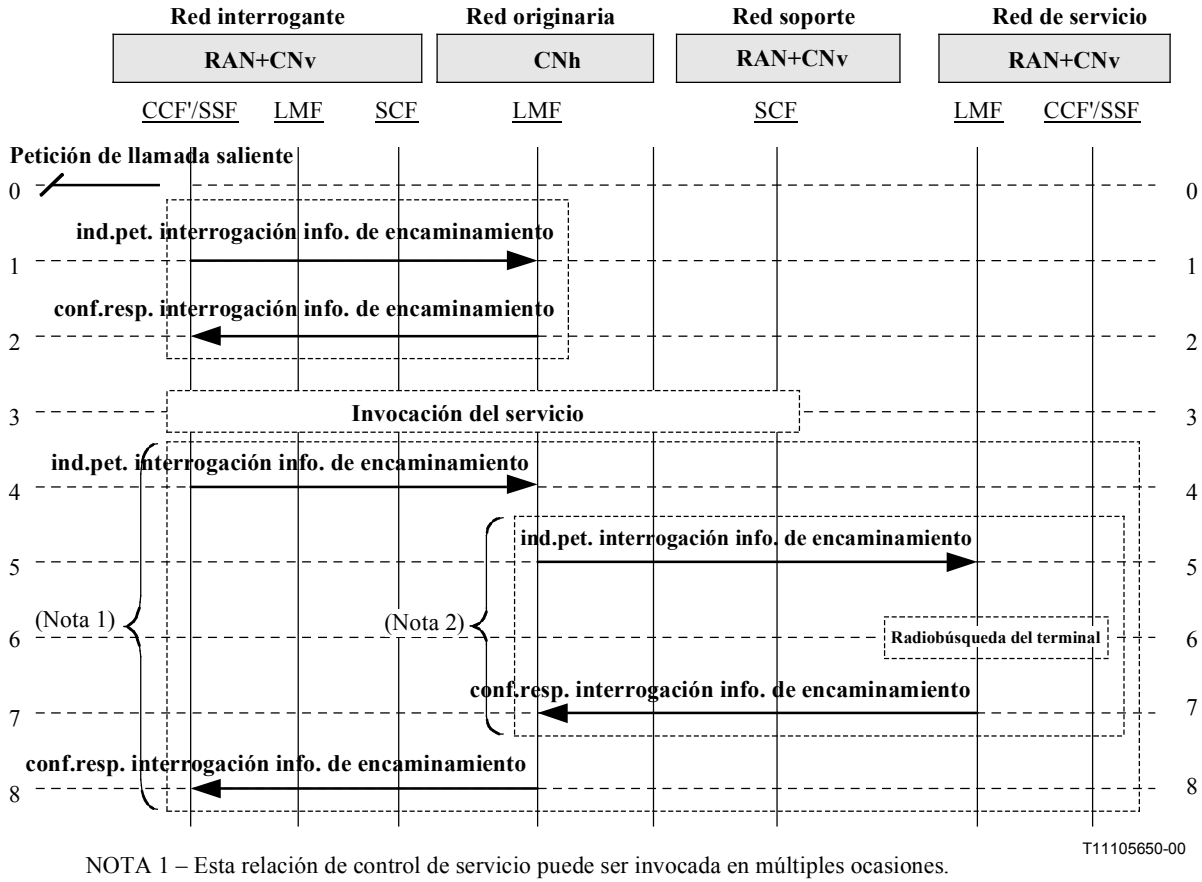
La interrogación sobre información de encaminamiento puede realizarse directamente entre las redes. Cuando la red interrogante es la que origina la llamada o la red intermedia, la interrogación sobre información de encaminamiento se envía directamente a la red originaria sin encaminar la llamada (petición de establecimiento de llamada) a la misma. Sin embargo, la ejecución depende de los acuerdos bilaterales entre las redes. Cuando ni la red origen de la llamada ni la red intermedia pueden interrogar, la llamada se encamina a la red originaria, invocándose allí la primera interrogación. En todos estos casos, sólo existe una "red interrogante", ya sea la red en la que se origina la llamada, la red intermedia o la red originaria.

El procedimiento de encaminamiento de la llamada utiliza un esquema de interrogación en cadena mediante el cual la red interrogante obtiene información de encaminamiento actualizada (por ejemplo, DN, dirección IP) directamente de la red originaria de la parte llamada. Además, el esquema de interrogación en cadena se define como un procedimiento por el cual la red interrogante busca la información de encaminamiento interrogando a la red originaria de la parte llamada, interrogando ésta a su vez a la red visitada para obtener la información de encaminamiento actualizada de la parte llamada.

En relación con el flujo de información de encaminamiento de llamada se hacen los supuestos siguientes:

- La "red interrogante" puede ser la red que origina la llamada, una red intermedia o una red soporte.
- La interrogación sobre "información de encaminamiento" se envía en un esquema en cadena desde la red interrogante a la red originaria de la parte llamada y, después de recibir la información, se envía la petición de establecimiento de llamada a la red visitada de la parte llamada.
- La radiobúsqueda en la red visitada de la parte llamada puede realizarse en cualquier momento después de recibir una petición de información de encaminamiento.

Véase la figura 7.3-1.



NOTA 1 – Esta relación de control de servicio puede ser invocada en múltiples ocasiones.

NOTA 2 – Estos flujos de información pueden no ser necesarios si la LMFh ya dispone de información de encaminamiento.

Figura 7.3-1/Q.1721 – Encaminamiento de la llamada

0. **Petición de llamada saliente**: se recibe una petición de llamada saliente desde un móvil.

FEA0	– La red interrogante inicia los procedimientos de interrogación de encaminamiento.

1. **ind.pet. interrogación info. de encaminamiento**: la CCF'/SSF de la red interrogante lo puede invocar de forma facultativa; este flujo se utiliza para obtener de la LMFh, la dirección de encaminamiento de la red soporte en caso que deba realizarse el control del servicio.

Interrogación info. de encaminamiento (Respuesta: éxito o fracaso)	**ind.pet.**
Número llamado	M

FEA1	– Recupera la dirección de encaminamiento de la red soporte de la parte llamada.

2. **conf.resp. interrogación info. de encaminamiento**: este flujo se utiliza para informar a la red interrogante de la dirección de encaminamiento de la red soporte de la parte llamada. La dirección de encaminamiento de la red soporte puede ser utilizada (facultativamente) para invocar las características de servicio de RI de la parte llamada (por ejemplo, cribado de llamadas, prohibición de llamadas).

Interrogación info. de encaminamiento	conf.resp.
Dirección de encaminamiento (para la red soporte de la parte llamada)	M

FEA2	Realiza facultativamente el procedimiento de invocación de servicio de RI.
NOTA 1 – Puede haber interacciones de control del servicio adicionales dentro de la "relación de control del servicio" (esquemáticamente se muestra mediante un cuadro sombreado) que incluye los flujos de información de "innovación de lógica del servicio". La relación de control del servicio puede darse por terminada después de la primera interacción lógica del servicio o bien puede continuar hasta que la llamada se encamina. NOTA 2 – La invocación del servicio puede realizarse desde la SSF de la red interrogante a la SCF de la red originaria (posiblemente retransmitida desde la SCF de la red interrogante), o desde la LMF de la red originaria. NOTA 3 – En caso de invocación del servicio desde la red interrogante, la información obtenida de la red originaria en respuesta a la interrogación sobre información de encaminamiento, contendrá instrucciones a la red servidora para la invocación del servicio. NOTA 4 – La invocación del servicio puede dar lugar a distintos escenarios, tales como desvío de llamada, por ejemplo, a una línea fija, la interacción del usuario con una SRF u otros escenarios. En esta figura sólo se describe la terminación de llamada sencilla en un abonado móvil.	

3. **Invocación de servicios RI**: la invocación de este procedimiento es facultativa.

4. **ind.pet. interrogación info. de encaminamiento**:[1] este flujo, invocado por la CCF'/SSF de la red interrogante, se utiliza para interrogar sobre información de encaminamiento (por ejemplo, el número temporal internacional de directorio, ITDN, de la parte llamada) desde la LMF de la red originaria de la parte llamada.

Interrogación info. de encaminamiento (Respuesta: éxito o fracaso)	ind.pet.
Número llamado	M

FEA4	– Identifica al usuario llamado. – Envía la interrogación a la red servidora/visitada para obtener un número de encaminamiento (por ejemplo, el ITDN).

[1] Es condicional si la invocación es desde la red interrogante.

5. **ind.pet. interrogación info. de encaminamiento**: este flujo se utiliza para enviar la interrogación a la LMF en la red servidora a fin de obtener el número de encaminamiento del usuario (por ejemplo, el ITDN). Puede utilizarse (facultativamente) para invocar la lógica del servicio a fin de realizar la radiobúsqueda del terminal.

Interrogación info. de encaminamiento (Respuesta: éxito o fracaso)	ind.pet.
IMUI	M
Número llamado	O

FEA5	– Identifica al usuario llamado. – Procedimiento de radiobúsqueda (flujos facultativos). – Asigna un número de encaminamiento (por ejemplo, ITDN) al usuario llamado.

6. **Radiobúsqueda del terminal**: procedimiento que, en caso de ser necesario, es facultativo.

7. **conf.resp. interrogación info. de encaminamiento**: flujo utilizado para transferir el número de encaminamiento (por ejemplo, el ITDN) del usuario llamado a la LMF de la red originaria del usuario.

Interrogación info. de encaminamiento	conf.resp.
Número de encaminamiento de la parte llamada (por ejemplo, el ITDN)	M

FEA7	– Envía el número de encaminamiento (por ejemplo, el ITDN).

8. **conf.resp. interrogación info. de encaminamiento**: este flujo se utiliza para transferir el número/dirección de encaminamiento del usuario llamado, pudiendo utilizarse también para transferir el resultado de la radiobúsqueda (si se ejecuta).

Interrogación info. de encaminamiento	conf.resp.
Número de encaminamiento de la parte llamada (por ejemplo, el ITDN)	M

FEA8	– Utiliza el número de encaminamiento (por ejemplo, el ITDN) para encaminar la llamada (por ejemplo, a través de la RTPC) a la red servidora.

7.4 Llamada entrante a móvil

El procedimiento de llamada entrante a móvil se utiliza para terminar una llamada en un terminal móvil que se encuentra en estado de reposo.

Se supone que la llamada se encamina de forma óptima (la red interrogante no es la red originaria):

- Para servicios básicos la llamada se encamina desde la red servidora a la de destino mediante la señalización del control de llamada, utilizando el número de itinerancia anteriormente recuperado.
- Para servicios avanzados se aplica la VHE.

7.4.1 Llamada entrante inicial a móvil

Véase la figura 7.4.1-1.

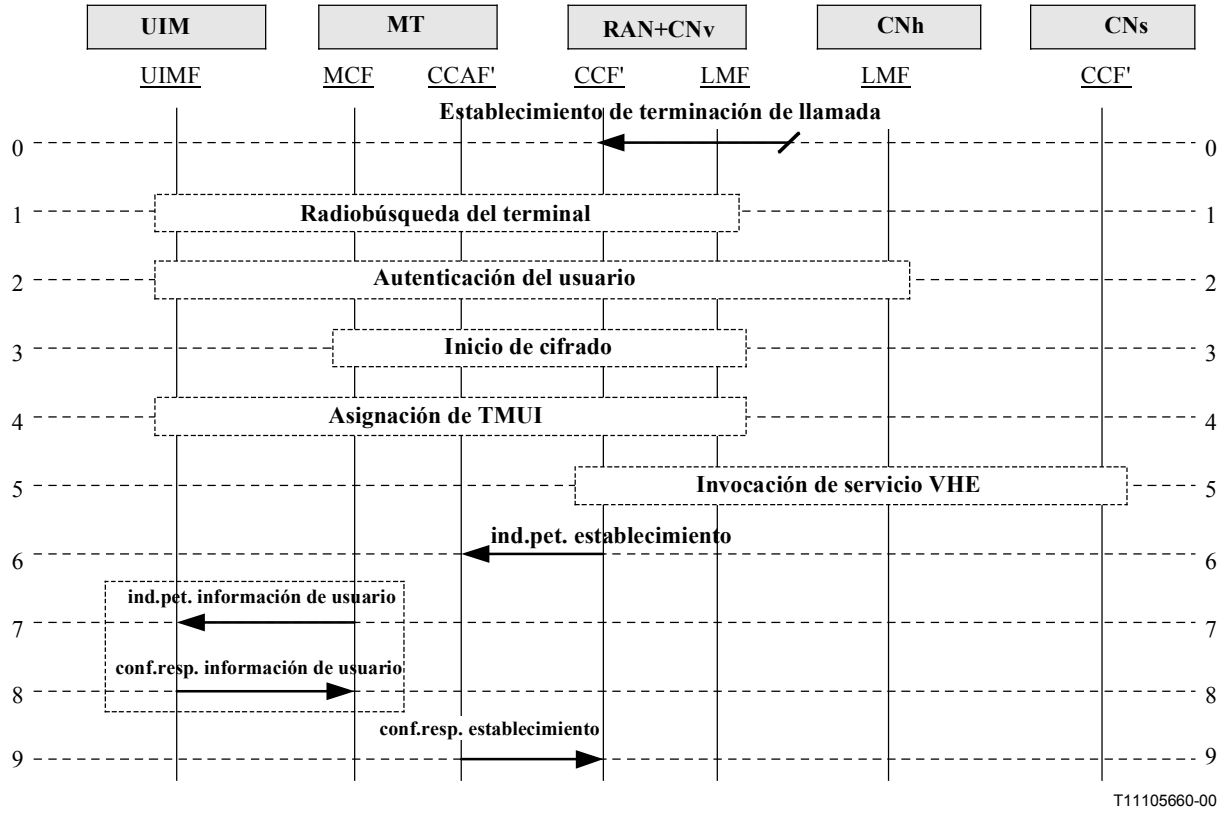


Figura 7.4.1-1/Q.1721 – Llamada entrante a móvil

0. **Establecimiento de terminación de llamada**: una llamada llega al sistema servidor dirigida a un abonado móvil que se encuentra en estado de reposo.

FEA0	– Antes de establecer la llamada, la red visitada valida a la parte llamada y puede invocar servicios basados en el intento de terminación.

1. **Radiobúsqueda de terminal**: el sistema servidor puede intentar la radiobúsqueda del MT en este momento. La radiobúsqueda puede haber tenido lugar con anterioridad durante la etapa de encaminamiento o puede no ser necesaria si el MT se encuentra ocupado en otra llamada.

2. **Autenticación de usuario**: se realiza la autenticación necesaria para este intento de llamada.

3. **Inicio de cifrado**: si es necesario, se inicia el cifrado para este intento de llamada.

4. **Asignación de TMUI**: si es preciso asignar un TMUI, puede hacerse en cualquier momento después del inicio del cifrado.

5. **Invocación del servicio VHE**: en función del perfil de usuario, la red visitada puede invocar la lógica de servicio de RI. Esto puede ocurrir en cualquier punto definido y activo de detección de disparo.

6. **ind.pet. establecimiento**: la CCF realiza el establecimiento de la llamada.

Establecimiento (Respuesta: éxito o fracaso)	**ind.pet.**
ID de usuario	M (nota)
Número llamante (IMDN)	M

FEA6	– Opcionalmente, realiza la invocación y espera que se complete el procedimiento de información de usuario. – Establece la llamada y el canal portador.
NOTA – Se incluye la IMUI o el TMUI, según estén disponibles. El TMUI es recomendable a los efectos de seguridad en el medio radioeléctrico.	

7. **ind.pet. información de usuario**: Opcionalmente, la MCF interroga a la UIMF sobre información/instrucciones adicionales de usuario.

Información de usuario (Respuesta: éxito o fracaso)	**ind.pet.**
Petición de tratamiento de la terminación	O (nota)

FEA7	– Ordena que la MCF acepte la llamada.
NOTA – Incluido para solicitar instrucciones para el tratamiento de la llamada desde la UIMF.	

8. **conf.resp. información de usuario**: la UIMF devuelve la información solicitada a la MCF.

Información de usuario	**conf.resp.**
Información de tratamiento de la terminación	O (nota)

FEA8	– Se aplica el tratamiento de terminación de llamada indicado.
NOTA – Incluido para indicar el tipo de tratamiento de terminación de llamada que debe aplicarse.	

9. **conf.resp. establecimiento**: la CCAF informa de la compleción exitosa del establecimiento de llamada y del canal portador.

Establecimiento	**conf.resp.**
Ninguna	(nota)

FEA9	– Ninguna.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

7.4.2 Llamada entrante adicional a móvil

La llamada entrante adicional a móvil significa la recepción en el móvil de una segunda llamada cuando tiene una llamada en curso, es decir, una llamada a tres. El procedimiento se realiza de forma similar a las llamadas móviles entrantes, con la excepción de que la radiobúsqueda no es necesaria cuando se añade la tercera parte.

7.5 Liberación de llamada móvil

7.5.1 Liberación normal: iniciada por el móvil

Véase la figura 7.5.1-1.

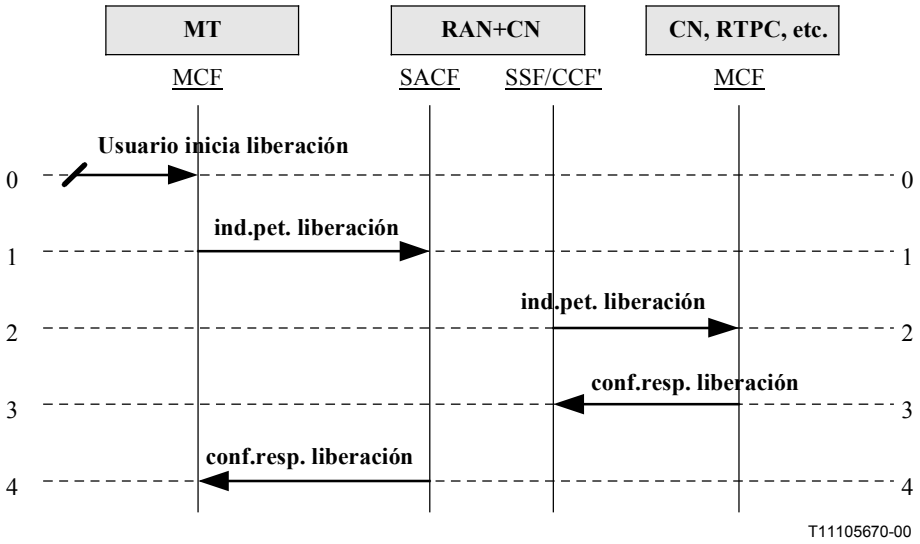


Figura 7.5.1-1/Q.1721 – Liberación normal iniciada por el móvil

0. **Usuario inicia liberación**: el abonado móvil libera la llamada.

FEA0	– El MT hace una petición de liberación.

1. **ind.pet. liberación**: la MCF envía una petición de liberación a la SACF.

Liberación (Respuesta: éxito o fracaso)	ind.pet.
TMUI	M

FEA1	– Prepara el envío de la petición de liberación a la red de origen.

2. **ind.pet. liberación**: la SSF/CCF' de la red visitada envía la petición de liberación a la CCF de red de origen.

Liberación (Respuesta: éxito o fracaso)	ind.pet.
TMUI	M

FEA2	– Libera recursos asociados a esta llamada.

3. **conf.resp. liberación**: la CCF de la red de origen devuelve un acuse de recibo de liberación de llamada exitosa a la SSF/CCF' de la red visitada.

Liberación	conf.resp.
Ninguna	(nota)

FEA3	– Prepara el envío de la respuesta de liberación a la red visitada.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

4. **conf.resp. liberación**: la SACF de la red visitada envía el acuse de recibo de liberación exitosa de llamada a la MCF.

Liberación	conf.resp.
Ninguna	(nota)

FEA4	– Libera recursos asociados a esta llamada.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

7.5.2 Liberación normal: iniciada por la red

Véase la figura 7.5.2-1.

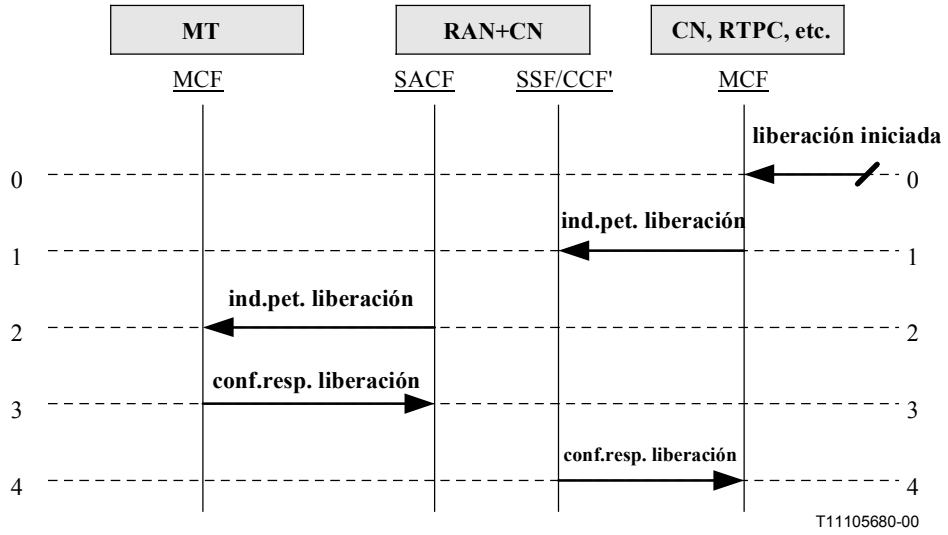


Figura 7.5.2-1/Q.1721 – Liberación normal iniciada por la red: diagrama de flujo de información de la llamada

0. Liberación iniciada: la red inicia de forma autónoma la liberación de la llamada o bien recibe una petición de liberación de un usuario de la red (por ejemplo, de línea fija/abonado no móvil).

FEA0	– La red se prepara para solicitar la liberación a la red visitada.

1. **ind.pet. liberación**: la CCF envía una petición de liberación a la SSF/CCF'.

Liberación (Respuesta: éxito o fracaso)	**ind.pet.**
TMUI	M

FEA1	– Prepara el envío de la petición de liberación al terminal móvil.

2. **ind.pet. liberación**: la SACF de la red visitada envía la petición de liberación a la MCF.

Liberación (Respuesta: éxito o fracaso)	**ind.pet.**
TMUI	M

FEA2	– Libera recursos asociados a esta llamada.

3. **conf.resp. liberación**: la MCF devuelve un acuse de recibo de liberación de llamada exitosa a la SACF de la red visitada.

Liberación	**conf.resp.**
Ninguna	(nota)

FEA3	– Prepara el envío de la respuesta de liberación a la red de origen.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

4. **conf.resp. liberación:** la SACF de la red visitada envía el acuse de recibo de liberación exitosa de llamada a la red de origen.

Liberación	**conf.resp.**
Ninguna	(nota)

FEA4	– Libera recursos asociados a esta llamada.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

7.6 Llamadas de emergencia

7.6.1 Origen de llamadas de emergencia

Las llamadas de emergencia deben evitar pasar por los procesos de autenticación normal y de registro de ubicación. Además, pueden no requerir la presencia de la UIM en el MT.

El procedimiento de inicio o establecimiento de llamadas de emergencia se realiza de forma semejante a una llamada saliente de móvil con la excepción de que no es necesario realizar los procedimientos de autenticación de usuario, registro de ubicación de terminal, inicio de cifrado y

asignación de TMUI. Además, la red servidora recibe la petición de llamada e intenta establecerla en cuanto dispone de un número de encaminamiento. La red servidora puede invocar el servicio VHE en cualquier punto definido y activo de detección de disparo. Para una llamada de emergencia ello puede incluir la traducción del número de emergencia en un número local o regional. Asimismo, la ubicación geográfica del MT puede determinarse en cualquier momento después de que la red servidora reciba la petición de establecimiento. La determinación de la ubicación geográfica puede tener lugar antes de la invocación de cualquier servicio VHE.

7.6.2 Liberación de llamadas de emergencia: iniciadas por la red

El procedimiento de liberación de llamadas de emergencia iniciada por la red es semejante a una liberación de llamada iniciada por la red. Cuando en una llamada de emergencia el punto de respuesta de seguridad pública (PSAP, *public safety answering point*) libera la llamada, se libera el trayecto completo hasta el usuario.

7.6.3 Liberación de llamadas de emergencia: iniciadas por el móvil

El procedimiento de liberación de llamadas de emergencia iniciada por el móvil es semejante a la liberación de llamada iniciada por el móvil. Es posible retener los recursos cuando el usuario llamante solicita la liberación de la llamada y se suspende la llamada de emergencia. Este procedimiento es opcional pudiéndose también aplicar el procedimiento de liberación de llamada normal (es decir, la liberación de todo el trayecto hasta el usuario). Si los recursos se han retenido y el usuario origina el establecimiento de llamada posteriormente, se retoma la llamada de emergencia que se había suspendido.

7.7 Llamadas con prioridad

Las llamadas con prioridad permiten que el abonado disponga de prioridad de acceso al canal de voz o de tráfico cuando se origina una llamada. Esta facilidad permite a un abonado el acceso con prioridad a canales de voz o de tráfico, situando en cola a las llamadas originadas por dichos usuarios cuando los canales no están disponibles. Cuando un canal queda disponible, los abonados en cola se sirven siguiendo el principio de primero en llegar primero servido y una función de prioridad. Cuando el abonado hace su suscripción recibe uno de *n* niveles de prioridad (*n* tiene un valor máximo y otro mínimo). Los niveles de prioridad se definen como 1, 2, 3, …, *n*, siendo 1 el nivel de la máxima prioridad y *n* el nivel de prioridad mínima. El nivel de prioridad está incluido en el perfil de abonado y se utiliza en la RAN+CN para asignar canales radioeléctricos.

8 Control de la llamada multimedios y del portador

Esta cláusula presenta los flujos de información necesarios para el establecimiento y control de llamadas multimedios, llamadas multipartitas y llamadas de servicios de datos por paquetes, incluyendo el acceso a servicios de Internet. La cláusula contiene dos grupos de servicios: teleservicios y servicios de acceso a Internet.

8.1 Cambio de teleservicio

El procedimiento de cambio de teleservicio permite al usuario IMT-2000 cambiar de servicio durante una llamada (por ejemplo, cambiar de comunicación de voz a comunicación de datos y viceversa), lo cual puede conducir a un cambio en el enlace de acceso utilizado. Desde la perspectiva de la interfaz red-red, el cambio de teleservicio se realiza para modificar el portador de forma que éste permita que la capacidad portadora soporte el cambio de tipo de servicio. Los cambios de teleservicio pueden ser iniciados tanto por el usuario de origen como por el de terminación. Sin embargo, el flujo de información extremo a extremo (móvil a móvil) para el cambio de teleservicio incluye ambos casos tal como se muestra en la figura 8.1-1.

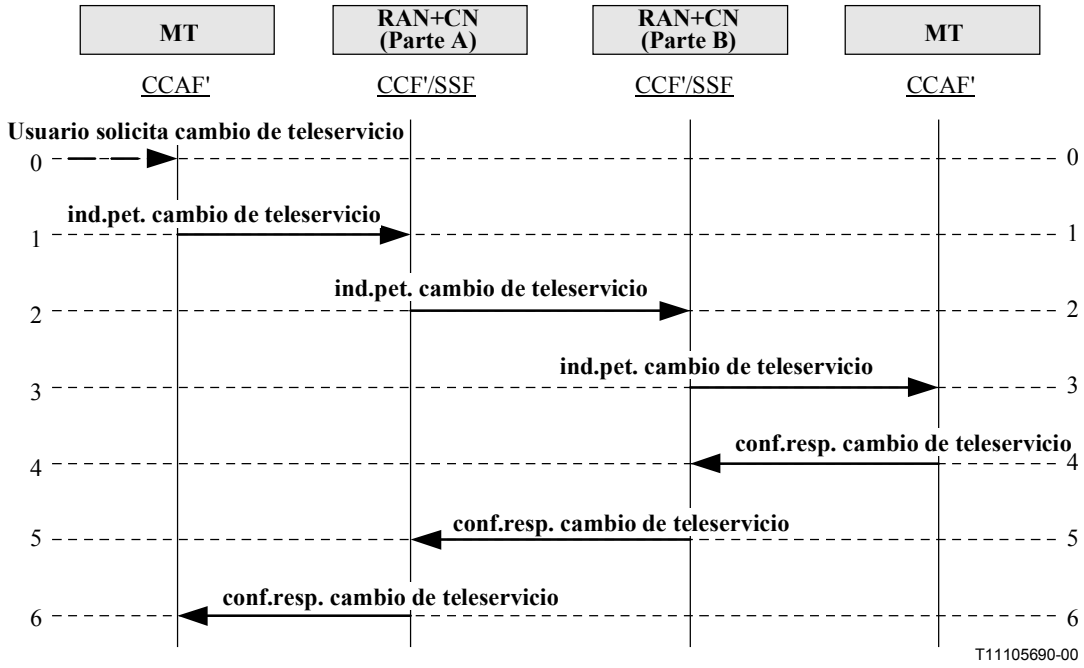


Figura 8.1-1/Q.1721 – Cambio de teleservicio

0. **Usuario solicita cambio de teleservicio**: el usuario solicita el cambio de teleservicio (enlace de acceso).

FEA0	– Petición de cambio en la conexión.

1. **ind.pet. cambio de teleservicio**: utilizado para pedir el establecimiento de una conexión.

Cambio de teleservicio (Informe: éxito/fracaso)	ind.pet.
ID de llamada	M
Tipo de teleservicio	M

FEA1	– Interacciona con la gestión de recursos radioeléctricos para adaptar el enlace de acceso a la solicitud. – Envía petición de cambio de teleservicio para informar a otra parte o partes de la llamada.

2. **ind.pet. cambio de teleservicio**: generada por la CCF'/SSF para realizar la petición de cambio de teleservicio.

Cambio de teleservicio (Informe: éxito/fracaso)	ind.pet.
ID de llamada	M
Tipo de teleservicio	M

FEA2	– Envío de petición de cambio de teleservicio.

3. **ind.pet. cambio de teleservicio**: para solicitar a la red de la parte B el cambio de teleservicio.

Cambio de teleservicio (Informe: éxito/fracaso)	ind.pet.
ID de llamada	M
Tipo de teleservicio	M

FEA3	– Interacciona con la gestión de recursos radioeléctricos para el ajuste del enlace de acceso. – Responde para confirmar el cambio de teleservicio (enlace de acceso).

4. **conf.resp. cambio de teleservicio**: generado por la CCAF para responder a la petición de cambio de teleservicio.

Cambio de teleservicio	conf.resp.
Resultado	M

FEA4	Responde a la red de la parte A confirmando el establecimiento de la conexión para el cambio de teleservicio.

5. **conf.resp. cambio de teleservicio**: utilizado para confirmar que la conexión se ha establecido.

Cambio de teleservicio	conf.resp.
Resultado	M

FEA5	Conexión con el nuevo enlace de acceso.

6. **conf.resp. cambio de teleservicio**: utilizado para confirmar que la conexión se ha establecido.

Cambio de teleservicio	conf.resp.
Resultado	M

FEA6	Ninguno.

8.2 Adición de medios durante una llamada (originada por el usuario móvil)

El objeto de este procedimiento es añadir componentes de medios a una llamada activa. Se supone que la adición de los componentes de medios está relacionada con la asignación a la llamada de un nuevo portador para soportarla. Véase la figura 8.2-1.

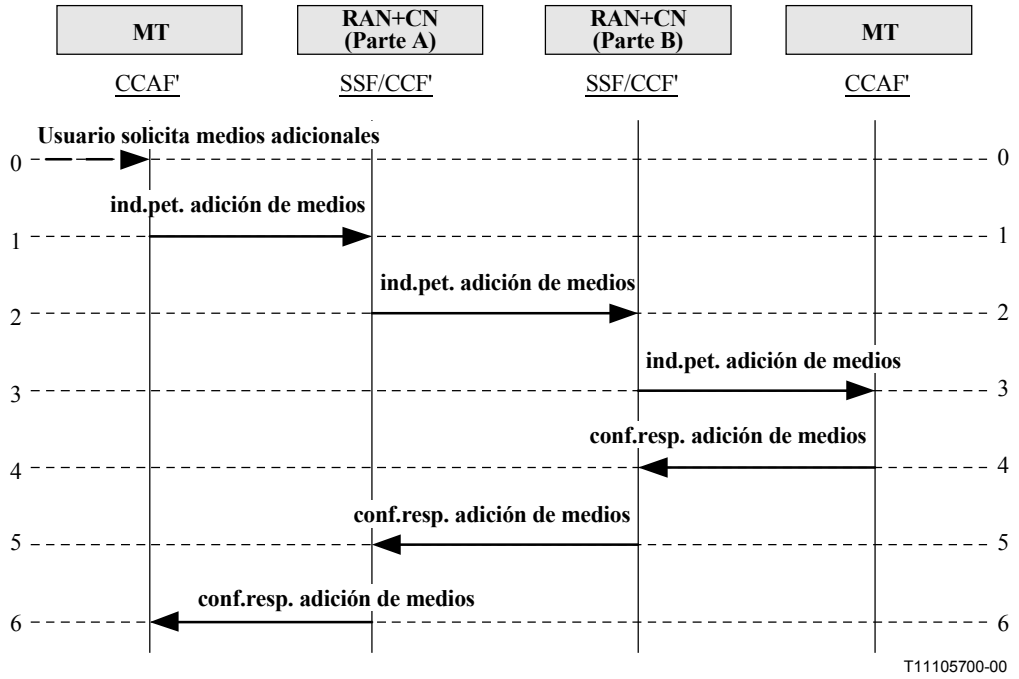


Figura 8.2-1/Q.1721 – Adición de medios a una llamada (originada en un móvil)

0. **Usuario solicita medios adicionales**: el usuario móvil desea añadir una componente de medios. Especifica el servicio suplementario deseado.

FEA0	– Solicita un medio adicional. – Envía la petición de conexión del enlace de acceso.

1. **ind.pet. adición de medios**: para transportar la información relativa al deseo del usuario de añadir un componente de medios a la llamada activa. Especifica el servicio suplementario deseado.

Adición de medios (Respuesta: éxito o fracaso)	**ind.pet.**
ID de llamada	M
Tipo de medio	M

FEA1	– Verifica la autorización de servicio de la parte A (operación interna). Flujo descendente de petición "adición de medios".

2. **ind.pet. adición de medios**: para solicitar un componente de medios adicional para la llamada en curso.

Adición de medios (Respuesta: éxito o fracaso)	**ind.pet.**
ID de llamada	M
Tipo de medio	M

FEA2	– Verifica la autorización de servicio de la parte B (interna). – Envía la petición de conexión del enlace de acceso.

3. **ind.pet. adición de medios**: para transportar la información relativa al deseo del usuario de añadir un componente de medios a la llamada activa. Especifica el teleservicio suplementario deseado.

Adición de medios (Respuesta: éxito o fracaso)	ind.pet.
ID de llamada	M
Tipo de medio	M

FEA3	– Verifica la autorización de servicio. – Envía petición de conexión del enlace de acceso.

4. **conf.resp. adición de medios**: informa que se han tomado acciones para la petición de adición de medios.

Adición de medios	conf.resp.
Resultado	M

FEA4	– Retransmisión de respuesta.

5. **conf.resp. adición de medios**: informa que se han tomado acciones para la petición de adición de medios.

Adición de medios	conf.resp.
Resultado	M

FEA5	– Retransmisión de respuesta.

6. **conf.resp. adición de medios**: informa que se han tomado acciones para la petición de adición de medios.

Adición de medios	conf.resp.
Resultado	M

FEA6	– Petición de establecimiento de canal portador.

8.3 Eliminación de medios de una llamada en curso

Este procedimiento está destinado a suprimir un componente de medios de una llamada en curso. Puede ser una decisión del usuario o de la red (si los recursos necesarios no están disponibles y si se refiere a una llamada de "clase inferior"). El primer caso se muestra a continuación. Véase la figura 8.3-1.

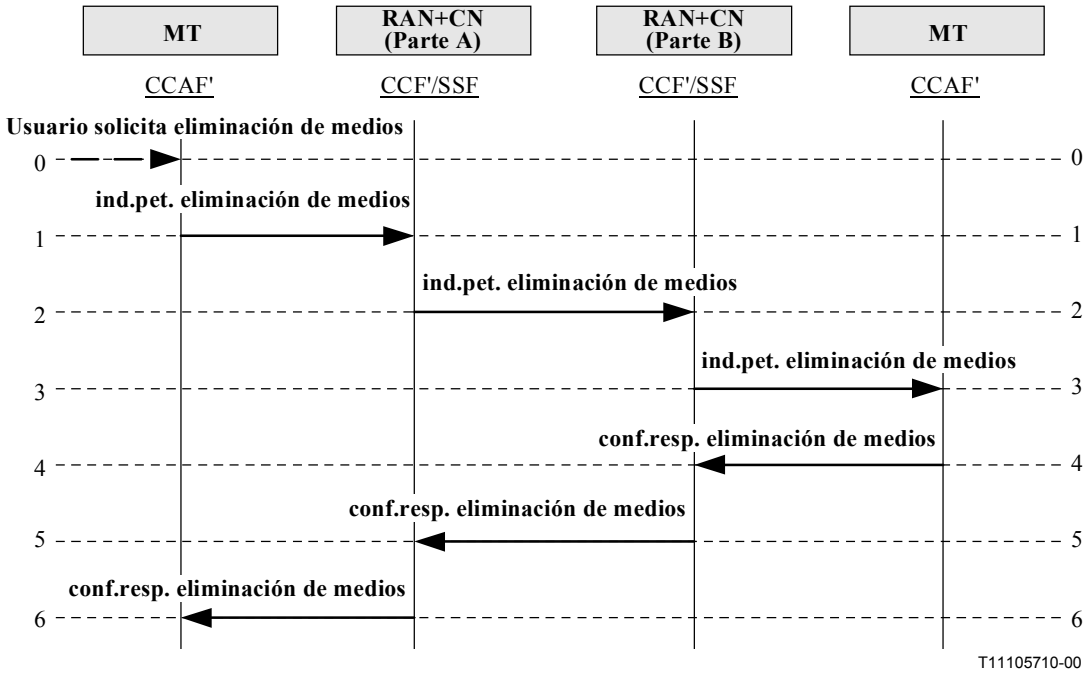


Figura 8.3-1/Q.1721 – Eliminación de medios de una llamada multimedia (originada en móvil)

0. **Usuario solicita eliminación de medios**: petición del usuario para suprimir un componente de medios.

FEA0	– Envío de una petición para eliminar un componente de medios de la correspondiente entidad de control de llamada en la red.

1. **ind.pet. eliminación de medios**: utilizado para solicitar la operación de "eliminación de medios".

Eliminación de medios (Respuesta: éxito o fracaso)	**ind.pet.**
ID de llamada	M
ID de medios	M

FEA1	– Identifica la llamada y el medio a eliminar. – Envío de la petición de "eliminación de medios" a la entidad de control de llamada distante, red de servicio de la parte B.

2. **ind.pet. eliminación de medios**: utilizado para enviar la petición de "eliminación de medios" a la red medular de la otra parte de la llamada para modificar la llamada (eliminando el portador afectado) en la parte bajo su responsabilidad.

Eliminación de medios (Respuesta: éxito o fracaso)	**ind.pet.**
ID de llamada	M
ID de medios	M

FEA2	– Identifica la llamada y el correspondiente medio que debe eliminarse. – Envía una petición para eliminar el medio a la red de acceso. – Elimina el componente de medios correspondiente.

3. **ind.pet. eliminación de medios**: utilizado para enviar la petición de "eliminación de medios" a la red de acceso a fin de modificar la llamada suprimiendo el medio que se encuentra bajo su control.

Eliminación de medios (Respuesta: éxito o fracaso)	ind.pet.
ID de llamada	M
ID de medios	M

FEA3	– Identifica la llamada y el correspondiente medio que debe eliminarse. – Interacciona con los elementos de gestión de recursos radioeléctricos. – Elimina el componente de medios correspondiente.

4. **conf.resp. eliminación de medios**: utilizado para confirmar que tanto la red de acceso distante como la red principal han suprimido correctamente el componente de medios y el portador o portadores conexos.

Eliminación de medios	conf.resp.
Resultado	M

FEA4	– Elimina los componentes de medios y su portador asociado.

5. **conf.resp. eliminación de medios**: utilizado para confirmar que tanto la red de acceso distante como la red medular han suprimido correctamente el componente de medios y el portador o portadores conexos.

Eliminación de medios	conf.resp.
Resultado	M

FEA5	– Elimina el componente de medios y su portador asociado.

6. **conf.resp. eliminación de medios**: utilizado para enviar el resultado al FE de control de llamada de origen.

Eliminación de medios	conf.resp.
Resultado	M

FEA6	– Solicita liberación de los portadores asociados con los medios.

8.4 Llamada punto a multipunto

8.4.1 Adición de una parte (móvil a móvil)

En una llamada en la que intervienen dos partes cada una de ellas puede solicitar la adición de otra parte a la llamada. La parte A se convierte en la raíz de la conexión de red de tipo 1 (es decir, conexión punto a punto) que solicita que se añada a la llamada una nueva parte móvil C. La conexión de red previa de tipo 1 se convierte en una conexión de red de tipo 2 (es decir, conexión punto a multipunto) en la que están presentes tanto la parte raíz como la parte hoja. La petición de la operación "adición de parte" también requiere un procedimiento de "cambio de teleservicio" o de "notificación" para la llamada en curso entre las partes de la llamada. En esta subcláusula se consideran los procedimientos de adición de una parte, ya sea iniciada por la raíz o por la hoja.

8.4.1.1 Adición de parte (iniciada por la raíz)

La figura 8.4.1-1 muestra el diagrama de flujos de información para una adición iniciada por la raíz. La parte C se añade a la llamada en curso entre las partes A y B. Para la adición de una nueva parte C en la red visitada de destino, se aplica un procedimiento de llamada de entrada a móvil como parte del procedimiento común de "establecimiento de la conexión".

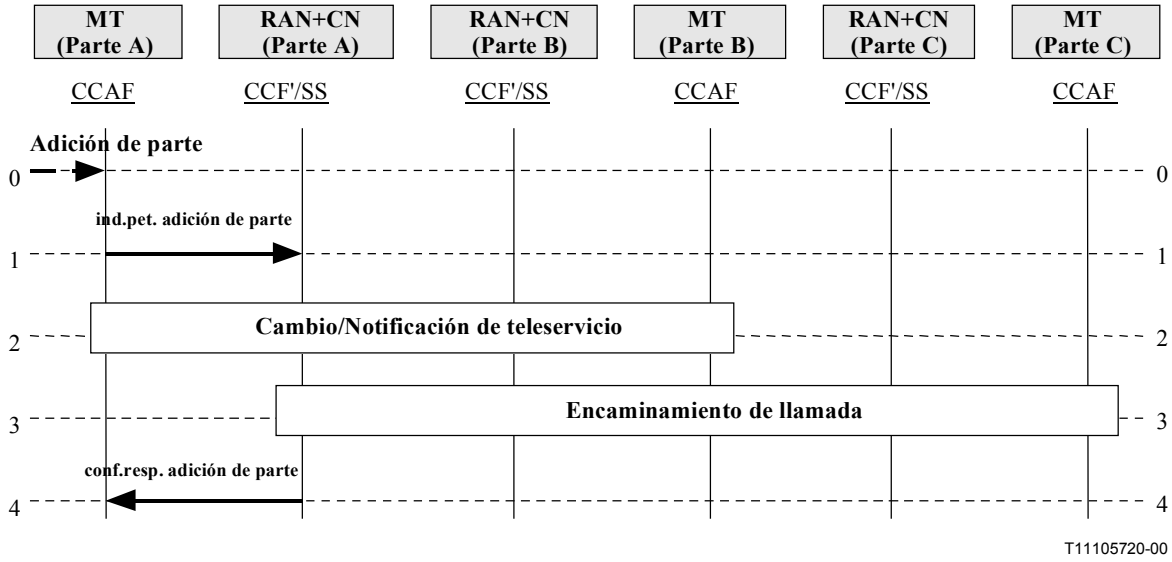


Figura 8.4.1-1/Q.1721 – Adición de parte (iniciada por la raíz)

0. **Adición de parte**: iniciada por el usuario parte A para añadir otra parte, parte C, a una llamada en curso con la parte B.

FEA0	– Envío de petición de adición de parte. – Se realiza una petición de cambio de teleservicio para las partes implicadas en la llamada.

1. **ind.pet. adición de parte**: para iniciar la adición de una parte a una conexión existente.

Adición de parte (Informe: éxito o fracaso)	ind.pet.
ID de llamada	M
Número llamado	M
Punto extremo de referencia	M

FEA1	– Identifica el usuario que se añade. – Selecciona y reserva recursos de salida. – Envía petición de establecimiento para iniciar el establecimiento de la llamada y de la conexión.

2. **Cambio/notificación de teleservicio**: para solicitar el cambio de servicio (por ejemplo, de punto a punto a punto a multipunto) y procesar la adición del enlace de acceso (si es necesario).

FEA2	– Petición de cambio de servicio (por ejemplo, de punto a multipunto a punto a punto).

3. **Encaminamiento de llamada**: para solicitar el establecimiento de una llamada que debe ser seguida por una conexión de portador.

4. **conf.resp. adición de parte**: para acusar recibo de que la petición de adición de parte se realizó con éxito.

Adición de parte	conf.resp.
ID de llamada	M
Punto extremo de referencia	M

FEA4	– Envío de la confirmación de adición de parte. – Petición de establecimiento de canal o canales portadores.

8.4.1.2 Adición de parte (iniciada por un elemento hoja)

En la figura 8.4.1-2 se muestra el diagrama del flujo de información para la adición de una parte iniciada por una hoja. La parte C añade la parte D a la llamada en curso entre las partes A, B y C. La parte C notifica a la parte raíz, parte A, la adición de la parte D a la llamada. Desde ese momento, la CN de la parte raíz toma el control y realiza un procedimiento "adición de parte (iniciada por la raíz)".

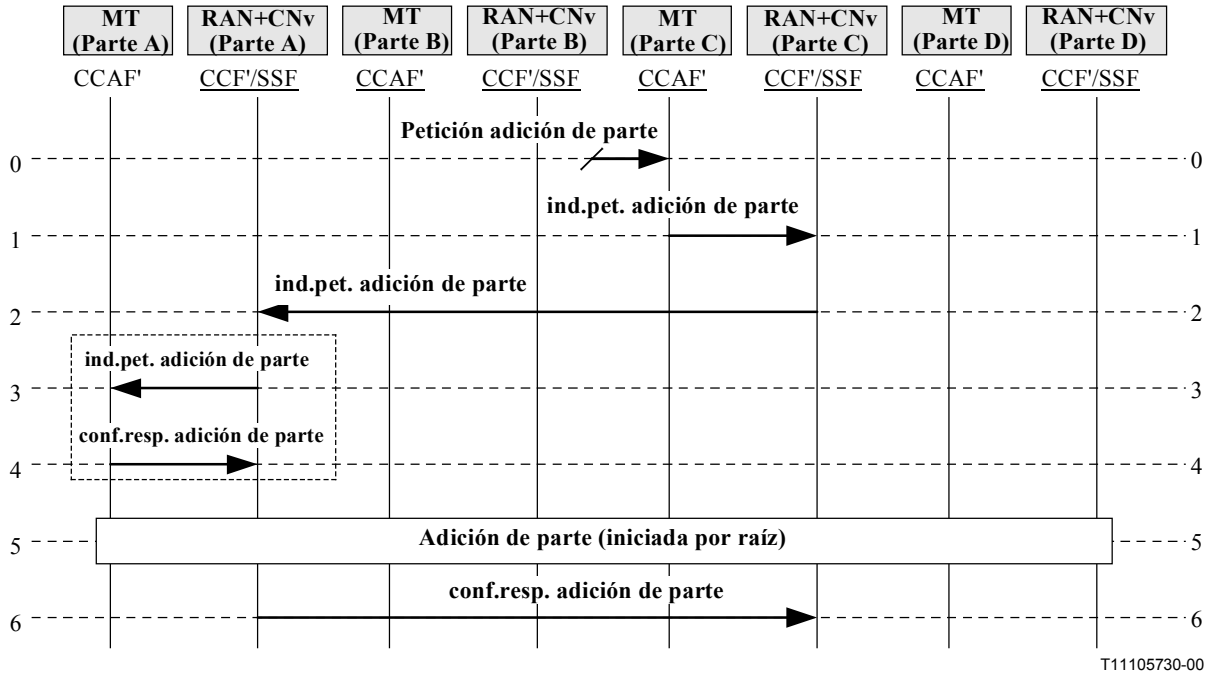


Figura 8.4.1-2/Q.1721 – Adición de parte (iniciada por hoja)

Los flujos de información, los elementos de información y las acciones de las entidades funcionales relacionadas con este procedimiento se describen a continuación en el mismo orden que los flujos que se muestran en la figura 8.4.1-2.

0. **Petición adición de parte**: iniciado por el usuario parte C para añadir otra parte, la parte D, a una llamada en curso activa con las partes A y B.

1. **ind.pet. adición de parte**: para iniciar la adición de una parte a una conexión existente.

Adición de parte (Informe: éxito o fracaso)	ind.pet.
ID de llamada	M
Número llamado	M

FEA1	– Envío de una petición de adición de parte a la parte raíz. – Selecciona y reserva recursos de salida.

2. **ind.pet. adición de parte**: para iniciar la adición de una parte a una conexión existente.

Adición de parte (Informe: éxito o fracaso)	ind.pet.
ID de llamada	M
Número llamado	M
Referencia de punto extremo	M

FEA2	– Identifica la nueva parte que se debe añadir. – Notifica a todas las partes de la llamada (excepto a la parte solicitante) la adición de la parte. – Selecciona y reserva recursos de salida. – Envía petición de establecimiento para iniciar el establecimiento de llamada y de conexión. – Proporciona referencia de punto extremo.

3. **ind.pet. adición de parte**: (opcional) para iniciar la adición de una parte a una conexión existente.

Adición de parte (Informe: éxito o fracaso)	ind.pet.
ID de llamada	M
Número llamado	M
Referencia de punto extremo	M

FEA3	– Identifica la nueva parte que debe añadirse. – Acusa recibo de la petición de adición de una parte. – Inicia el procedimiento de adición de parte.

4. **conf.resp. adición de parte**: utilizado para acusar recibo de la petición de adición de parte.

Adición de parte	resp.conf.
Resultado	M

FEA4	– Ninguno.

5. **Adición de parte (iniciado por la raíz)**: utilizado por la parte raíz de una llamada en curso para solicitar la adición de una parte.

6. **conf.resp. adición de parte**: utilizado para acusar recibo de que la petición de adición de parte tuvo éxito.

Adición de parte	resp.conf.
Resultado	M

FEA6	– Ninguno.

8.4.2 Eliminación de una parte

Una parte hoja puede ser eliminada de una conexión punto a multipunto a petición de la parte raíz o de la propia parte hoja.

8.4.2.1 Eliminación de una parte (iniciada por la parte raíz)

La parte raíz (parte A) puede solicitar que se elimine de la conexión una parte hoja (parte C). En este procedimiento, los recursos entre la parte C y la red medular se liberan normalmente por un proceso que desencadena la red principal. Véase la figura 8.4.2-1.

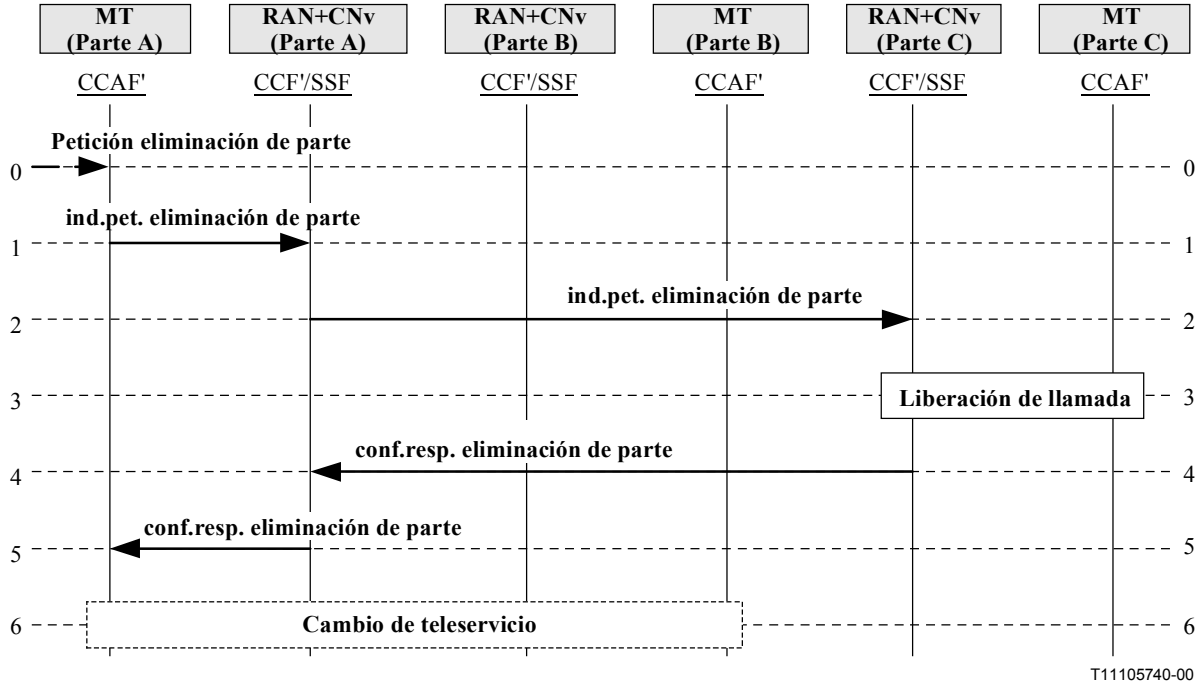


Figura 8.4.2-1/Q.1721 – Eliminación de parte (iniciado por la parte raíz)

0. **Petición de eliminación de parte**: es la petición del usuario para eliminar una parte de la llamada.

FEA0	– Identifica la parte que debe eliminarse. – Verifica los estados de todas las restantes partes asociadas con la conexión, si es necesario.

1. **ind.pet. eliminación de parte**: inicia la desincorporación de una parte de una conexión existente.

Eliminación de parte (Respuesta: éxito o fracaso)	ind.pet.
ID de llamada	M
Referencia de punto extremo	M
Causa	M

FEA1	– Identifica al usuario solicitante. – Acusa recibo de que el usuario solicitante es raíz. – Identifica la parte que debe ser eliminada. – Verifica los estados de todas las restantes partes hoja asociadas con esta conexión.

2. **ind.pet. eliminación de parte**: inicia la desincorporación de una parte de una conexión existente.

Eliminación de parte (Respuesta: éxito o fracaso)	ind.pet.
ID de llamada	M
Referencia de punto extremo	M
Causa	M

FEA1	– Identifica al usuario solicitante. – Acusa recibo de que el usuario solicitante es raíz. – Identifica la parte que debe ser eliminada. – Verifica los estados de todas las restantes partes hoja asociadas con esta conexión. – Inicia el procedimiento de liberación de llamada.

3. **Liberación de llamada**: procedimiento (iniciado por la red) utilizado para solicitar la eliminación de una parte de la llamada.

FEA3	– Envía respuesta a la eliminación de parte/liberación de llamada.

4. **conf.resp. eliminación de parte**: utilizada para notificar que la petición de eliminación de parte tuvo éxito.

Eliminación de parte	conf.resp.
Causa	O (nota)

FEA4	– Retrasmisión de respuesta de confirmación de eliminación de parte.
NOTA – Envía información sobre la causa de la liberación de la parte, si está disponible.	

5. **conf.resp. eliminación de parte**: utilizada para notificar que la petición de eliminación de parte tuvo éxito.

Eliminación de parte	conf.resp.
Causa	O (nota)

FEA5	– Envía la confirmación de la eliminación de la parte.
NOTA – Envía información sobra la causa de la liberación de la parte, si está disponible.	

6. **Cambio de teleservicio**: este procedimiento es una petición del posible cambio de teleservicio para las partes A y B , cambiando de punto a multipunto a punto a punto.

FEA6	– Cambio de petición de servicio (por ejemplo, de punto a multipunto a punto a punto).

8.4.2.2 Eliminación de una parte (iniciada por una parte hoja)

Cuando se recibe una petición de liberación de una parte hoja que debe ser eliminada (parte C), la red medular notifica a la parte raíz (parte A) que la parte hoja se ha eliminado enviando una petición de eliminación de parte. Véase la figura 8.4.2-2.

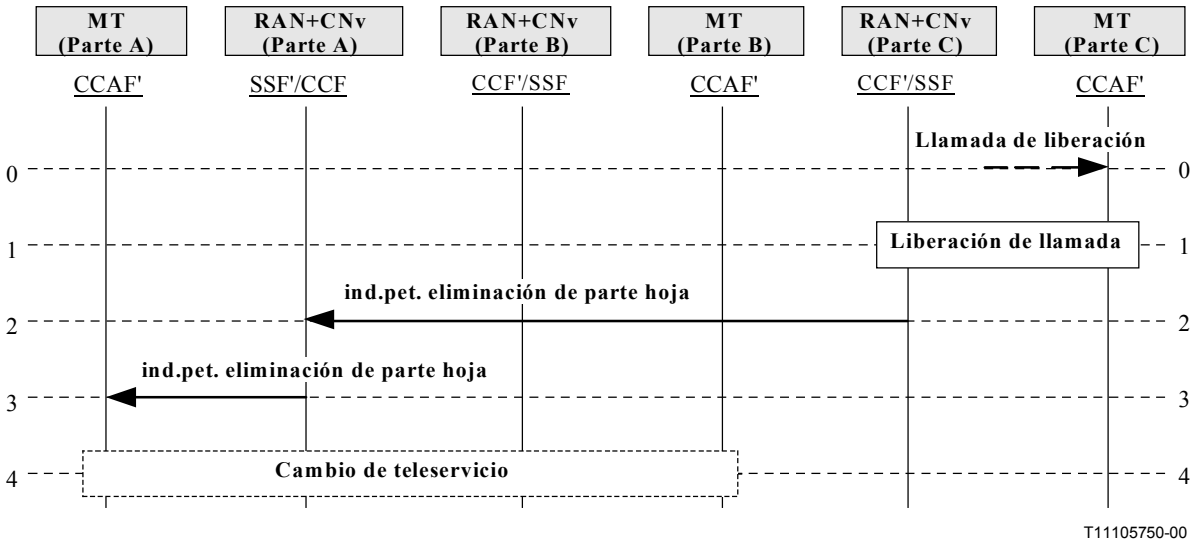


Figura 8.4.2-2/Q.1721 – Eliminación de parte (iniciada por la parte hoja)

0. **Llamada de liberación**: iniciada por una parte hoja que solicita ser eliminada de la llamada/conexión.

FEA0	– Inicia el procedimiento de liberación de llamada móvil. – Identifica la parte hoja que debe ser eliminada (parte solicitante). – Envía una petición de eliminación de parte a la red de la parte raíz.

1. **Liberación de llamada**: procedimiento para liberar la llamada entre la parte hoja que se elimina y las restantes partes de la llamada.

FEA1	– Envía una petición de eliminación de parte al terminal móvil de la parte raíz.

2. **ind.pet. eliminación de parte hoja**: se envía para notificar la desincorporación de una parte hoja de una conexión existente.

Eliminación de parte (Respuesta: ni éxito ni fracaso)	ind.pet.
ID de llamada	M
Referencia de punto extremo	M
Causa	M

FEA2	– Identifica la parte de hoja desincorporada sobre la base de la referencia de punto extremo. – Verifica los estados de las restantes partes hoja asociadas a la conexión, si es necesario. – Envía indicación de eliminación de parte.

3. **ind.pet. eliminación de parte hoja**: se envía para notificar la desincorporación de una parte hoja de una conexión existente.

Eliminación de parte (Respuesta: ni éxito ni fracaso)	ind.pet.
ID de llamada	M
Referencia de punto extremo	M
Causa	M

FEA3	– Identifica la parte de hoja desincorporada sobre la base de la referencia de punto extremo. – Verifica los estados de las restantes partes hoja asociadas a la conexión, si es necesario. – Envía indicación de eliminación de parte.

4. **Cambio de teleservicio**: (opcional) utilizado para procesar el cambio de teleservicio de las restantes partes de la llamada.

FEA4	– Solicita cambio de teleservicio (por ejemplo, de punto a multipunto a punto a punto).

8.5 Acceso a servicios de Internet

El acceso a los servicios de Internet permite que un abonado IMT-2000 itinerante inicie una sesión de servicio de datos en una red modular (CN, *core network*) visitada. Una vez que se ha establecido una sesión de servicio de datos, el abonado podrá itinerar en la siguiente CN visitada sin interrupción alguna en la sesión del servicio de datos. Cuando se inicia una sesión de servicios de datos, el terminal móvil del abonado puede tener una o varias direcciones IP públicas, que le hayan sido asignadas de forma permanente por la CN originaria, o una dirección IP pública (una o varias) que le hayan sido asignadas dinámicamente por la CN originaria o la CN visitada. El contexto de

encaminamiento de la red IMT-2000 se establece cuando la sesión se inicia, siendo actualizado siempre que el terminal móvil pasa en itinerancia a la siguiente CN visitada.

Los procedimientos que se describen en esta subcláusula son obligatorios cuando se itinera entre redes IMT-2000 con distintas arquitecturas de red principal (es decir, entre distintos miembros de la familia IMT-2000). La itinerancia entre redes que están implementadas utilizando el mismo miembro de familia puede utilizar procedimientos específicos de dicho miembro de la familia.

8.5.1 Establecimiento de una sesión del servicio de datos por paquetes

Para acceder a los servicios de datos por paquetes, el terminal móvil itinerante se registra en la red IMT-2000 visitada mediante procedimientos comunes de autenticación y de registro de terminal, solicitando además el acceso a las facilidades de datos por paquetes. El terminal móvil se registrará para la utilización de recursos de datos por paquetes accediendo a las facilidades de datos por paquetes. La arquitectura IMT-2000 permite la separación de las capacidades de LMF (y AMF asociadas) que se refieren a facilidades de acceso y de las capacidades LMF_p (y AMF_p asociadas) que se refieren a los servicios de datos por paquetes.

La figura 8.5.1-1 muestra el diagrama del flujo de información de este procedimiento. Los pasos 4-7 pueden repetirse para soportar múltiples sesiones de datos desde el mismo terminal.

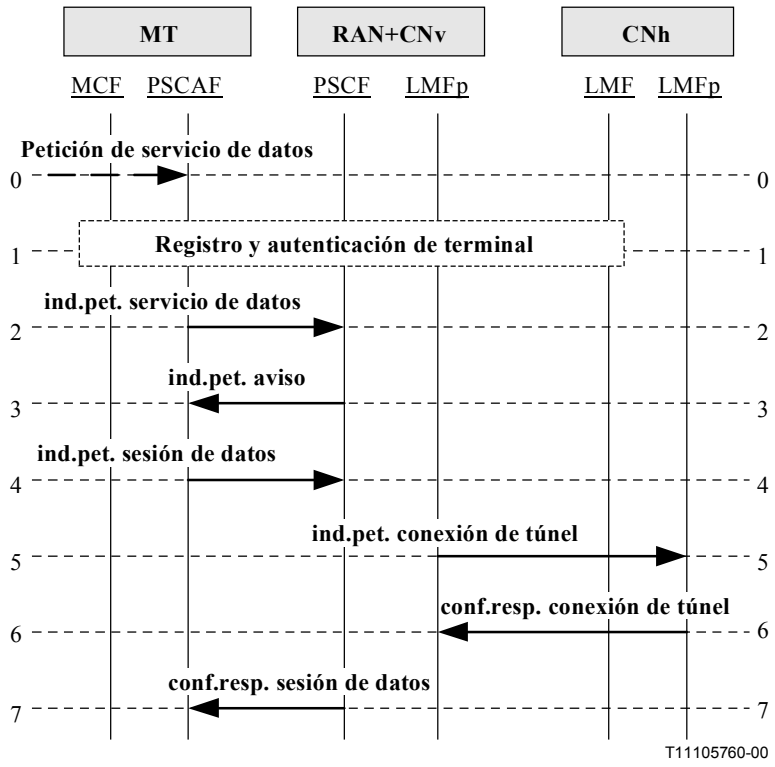


Figura 8.5.1-1/Q.1721 – Establecimiento de sesión de datos por paquetes

0. **Petición del servicio de datos**: el usuario inicia una sesión del servicio de datos por paquetes.

FEA0	– Petición de establecimiento de una sesión del servicio de datos, precedido de la autenticación y registro del terminal.

1. **Registro y autenticación del terminal**: es necesario en caso de no haberse realizado aún.

2. **ind.pet. servicio de datos**: para iniciar una sesión del servicio de datos en la red visitada mediante la petición del servicio.

Servicio de datos (Respuesta: ni éxito ni fracaso)	**ind.pet.**
ID de usuario	M
Tipo de servicio (datos)	M

FEA2	– Emplea el procedimiento de la capa de enlace para establecer un enlace de acceso seguido de una petición de "aviso".

3. **ind.pet. aviso**: se utiliza en el flujo hacia el terminal para solicitar el establecimiento de una sesión de cuando se detecta un identificador de acceso a la red (NAI, *network access identifier*).

Aviso (Respuesta: ni éxito ni fracaso)	**ind.pet.**
Dirección IP (PSCF)	M
Dirección IP (PSCF pública)	M (nota)
Valor de puesta a prueba	M
NAI (PSCF)	M

FEA3	– Responde al aviso con una petición de sesión de datos si detecta un nuevo NAI de PSCF. – Especifica un puerto UDP conocido y la dirección IP de la PSCF como un destino de esta información.
NOTA – Esta dirección IP es la dirección del agente ajeno (por ejemplo, se utiliza como un punto de terminación de túnel visto desde la PSGCF).	

4. **ind.pet. sesión de datos**: se envía desde la PSCAF a la PSCF en la red visitada sobre el enlace de acceso establecido para solicitar el establecimiento de una nueva sesión de datos[2].

Aviso (Respuesta: éxito o fracaso)	**ind.pet.**
ID de sesión	O (nota 1)
NAI (MT)	M
NAI (PSCFpv)	M
Dirección IP (MT)	O (nota 2)
Dirección IP (PSCF pública)	M
Discriminador del servicio	O (nota 3)
Valor de puesta a prueba (de PSCF)	M
Respuesta de puesta a prueba	M
Método de encapsulado	M
Duración de la sesión de datos	M

FEA4	– Determina la dirección de LMF_p en función del discriminador del servicio. – Solicita el establecimiento de una conexión túnel para esta sesión de datos. – Puede reducir la duración propuesta de la sesión de datos antes de enviar esta información a su LMF_p.
NOTA 1 – Es un caso de sesión múltiple. NOTA 2 – La asignación de la dirección IP puede ser estática y permanente, o bien, una asignación dinámica. NOTA 3 – La LMF_p puede necesitar el discriminador de servicio con fines de autorización.	

[2] Para no confundir el procedimiento de "registro" del terminal móvil con el registro para el establecimiento de la sesión de datos, se ha elegido para este flujo el nombre "sesión de datos".

5. **ind.pet. conexión túnel**: va desde la LMF_p visitada a la LMF_p originaria del terminal móvil para autenticar y autorizar al terminal móvil a fin de que pueda utilizar los servicios de datos por paquetes en la red visitada.

Conexión túnel (Respuesta: éxito o fracaso)	ind.pet.
NAI (MT)	M
NAI (PSCFpv)	M
NAI (PSCFv)	M
Dirección IP (MT)	O (nota 1)
Dirección IP (PSCF pública)	M
Discriminador de servicio	O (nota 2)
Valor de puesta a prueba (de la PSCF)	M
Respuesta de puesta a prueba	M
Método de encapsulado	M
Duración de la sesión de datos	M

FEA5	– Determina la PSGCF en función del discriminador de servicio. – Autentica el terminal móvil utilizando el valor de puesta a prueba, la respuesta de puesta a prueba y el secreto compartido con su terminal móvil. – Puede asignar una dirección IP al terminal móvil o puede decidir que la PSGCF debe asignar dicha dirección. Según señale la ind.pet. conexión túnel, la PSGCF puede asignarse dinámicamente o puede haber sido preasignada estadísticamente al terminal móvil. – Si la PSGCF se asigna dinámicamente, la LMF_p originaria puede asignarla en la red originaria o bien puede decidir que la red visitada debe asignar la PSGCF. – También puede generar un conjunto de claves de seguridad y de índices de parámetros de seguridad (SPI, *security parameter indices*) que serán distribuidos al terminal móvil, a la PSCF visitada y a la PSGCF para soportar las asociaciones de criptación y de seguridad entre dichas entidades. – Emplea los secretos que comparte con la PSCAF, la PSGCF originaria y la LMF_p visitada. – También puede reducir la duración de la sesión de datos propuesta antes de enviar esta información a su PSGCF o a la LMF_p visitada. – Devuelve la respuesta a la conexión túnel a la LMF_p visitada indicando que debe asignarse la PSGCF de la red visitada.
NOTA 1 – Asignación estática de dirección IP si la dirección IP es estática y permanente, en cualquier otro caso es dinámica. NOTA 2 – La LMF_p puede necesitar el discriminador de servicio con fines de autorización.	

6. **conf.resp. conexión túnel**: se envía desde la LMF_p originaria del terminal móvil a la LMF_p visitada para autorizar el servicio de datos por paquetes para el terminal móvil en la red visitada.

Elementos de información	conf.resp.
Resultado (indicación de asignación de la PSGCF)	M
Dirección IP (PSGCF pública)	M
Dirección IP (MT) incluida si es asignada por la red originaria	O (nota)
Duración de la sesión de datos	M
Información de seguridad	M

FEA6	Responde para confirmar el establecimiento de la conexión túnel. Envía el resultado para el establecimiento de la sesión de datos.
NOTA – La dirección IP puede no ser necesaria si no tiene lugar ninguna nueva asignación por parte de la red originaria.	

7. **conf.resp. sesión de datos**: es una respuesta a una petición para el establecimiento de una nueva sesión de datos.

Registro	conf.resp.
ID de sesión	O (nota)
Resultado (éxito o fracaso)	M
Dirección IP (PSGCF pública)	M
Dirección IP (MT)	M
Información de seguridad	M
Duración de sesión	M

FEA7	Continúa con la sesión de datos, no es necesaria ninguna actuación adicional.
NOTA – Si lo suministra la PSCAF en el flujo 4.	

8.5.2 Itinerancia durante una sesión establecida de datos por paquetes

Cuando se realiza la itinerancia hacia la siguiente red visitada, ya se ha asignado al terminal móvil una PSGCF en la red de anclaje. La red de anclaje puede ser la red originaria o la red visitada en la que se ha iniciado la sesión de datos. El terminal móvil puede registrarse en la siguiente red visitada mediante los procesos comunes de autenticación y registro del terminal. Invocando el procedimiento de gestión de recursos radioeléctricos (RRM, *radio resource management*), el terminal móvil establece un enlace de acceso con la PSCF en la siguiente red visitada. Dado que la dirección del NAI PSCF anunciada es diferente de la actual, la PSCAF inicia un procedimiento de "establecimiento de sesión de servicio de datos por paquetes" tal como se muestra en la figura 8.5.2-1.

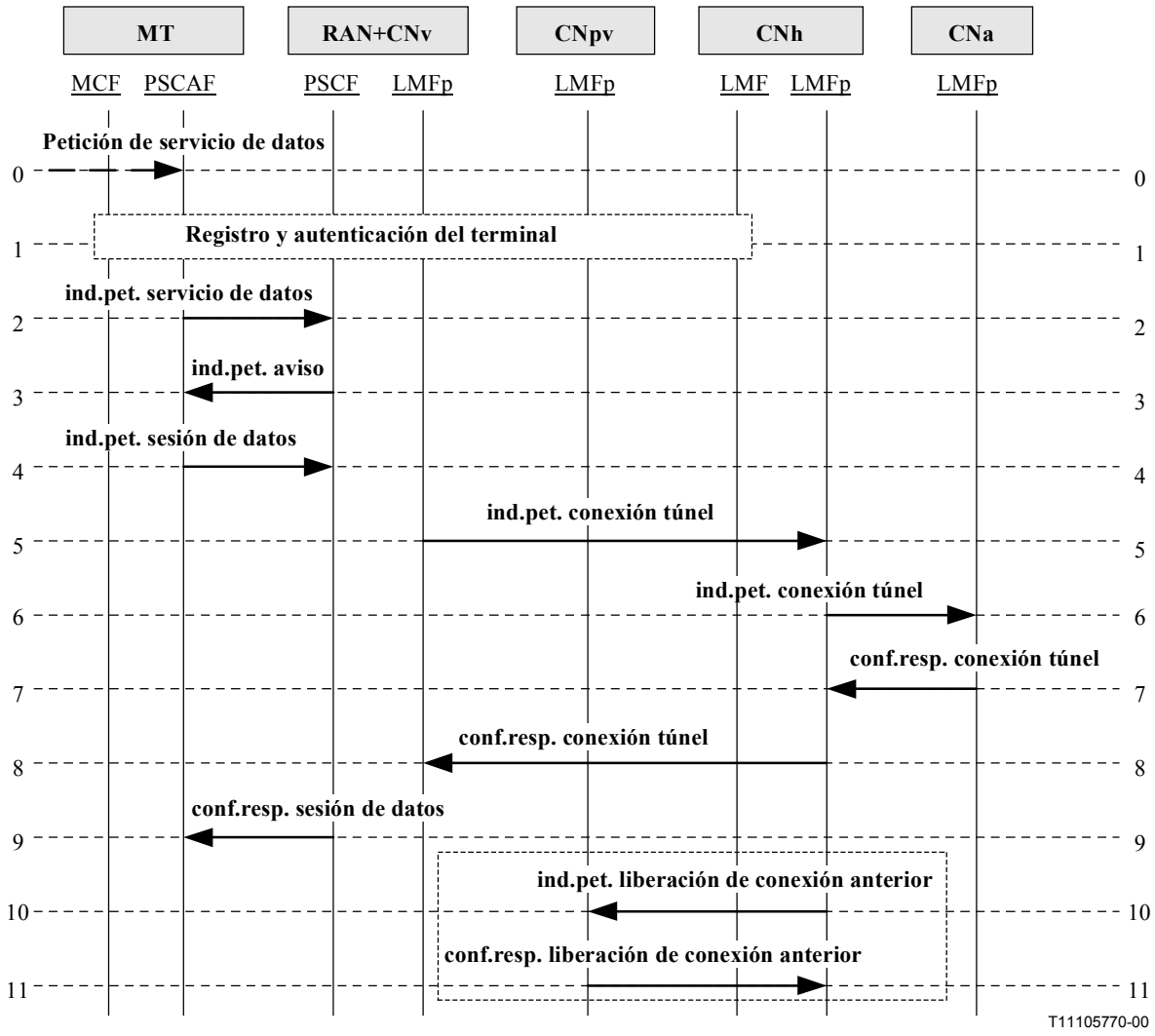


Figura 8.5.2-1/Q.1721 – Itinerancia durante una sesión de datos establecida

Este diagrama de flujo de información es semejante al diagrama del flujo de información de 8.5.1 hasta la operación "conexión túnel" en la que el flujo se dirige (desde la red originaria) a la red de anclaje. Además, la operación "liberación de conexión anterior" debe realizarse una vez establecida la nueva conexión.

0. **Petición de servicio de datos**: es el desencadenante para el registro del terminal móvil durante una sesión de datos por paquetes establecida.

FEA0	– Inicia la autenticación y el registro del terminal si ello es necesario.

1. **Registro y autenticación del terminal**: para el registro del terminal móvil en la red visitada antes de solicitar el servicio de datos por paquetes.

FEA1	– Solicita el establecimiento de una sesión del servicio de datos.

2. **ind.pet. servicio de datos**: el terminal móvil inicia una sesión del servicio de datos en la red visitada.

Servicio de datos (Respuesta: ni éxito ni fracaso)	ind.pet.
ID de usuario	M
Tipo de servicio (datos)	M

FEA2	– La petición del establecimiento del enlace de acceso va seguida de la petición de la operación "aviso" al terminal.

3. **ind.pet. aviso**: se envía al terminal para solicitar el establecimiento de una sesión de datos cuando se detecta un nuevo NAI.

Aviso (Informe: ni éxito ni fracaso)	ind.pet.
Dirección IP (PSCFv)	M
Dirección IP (PSCFv pública)	M
Valor de puesta a prueba (PSCFv)	M
NAI (PSCFv)	M

FEA3	– Responde al aviso con un registro si detecta un nuevo NAI de PSCF. – Especifica como destino de la información un puerto de UDP conocido y la dirección IP de la PSCF visitada. – Especifica un puerto de UDP que debe ser utilizado por la PSCF visitada cuando se devuelve la información de respuesta a la PSCAF.

4. **ind.pet. sesión de datos**: se envía desde la PSCAF a la PSCF de la red visitada sobre el enlace de acceso establecido, a fin de solicitar el establecimiento de una nueva conexión túnel en la sesión de datos existente.

Registro (Respuesta: éxito o fracaso)	ind.pet.
ID de sesión	O (nota 1)
NAI (MT)	M
NAI (PSCFpv)	M
Dirección IP (MT)	M
Dirección IP (PSCFv pública)	M
Discriminador de servicio	M (nota 2)
Dirección IP (PSGCF pública)	M
Valor de puesta a prueba (PSCFv)	M
Respuesta de puesta a prueba	M
Método de encapsulado	M
Duración de la sesión de datos	M

FEA4	– Se pone en comunicación con su LMFp para solicitar el establecimiento de una nueva conexión túnel con el PSGCF de anclaje para la sesión de datos existente. – Almacena localmente toda la información que le ha suministrado la PSCAF en la pet.ind. de registro y vincula dicha información al enlace de acceso y al IMSI, en caso de que éste hubiera sido suministrado durante el establecimiento del enlace de acceso. – Puede reducir la duración de la sesión de datos propuesta antes del envío de esta información a su LMFp. – Asigna un identificador de transacción a esta transacción. Posteriormente envía la información obtenida mediante la ind.pet. de registro a su LMFp. Previamente se habrá establecido una asociación entre la siguiente PSCF visitada y su LMFp. – Almacena la ID de sesión.
NOTA 1 – Si lo suministra la PSCAF en el flujo 4. NOTA 2 – El discriminador de servicio no se utiliza aquí tal como en 8.4.1 ya que la sesión ya se encuentra activa en la PSGCF. En consecuencia, la LMFp no selecciona la PSGCF. Sin embargo, la LMFp puede necesitar el discriminador de servicio con fines de autorización.	

5. **ind.pet. conexión túnel**: se envía desde la LMFp visitada a la LMFp originaria del terminal móvil para autenticar y autorizar el terminal móvil visitante y establecer una nueva conexión túnel entre la PSCF visitada y la PSGCF. En base a la información del NAI previo, la LMFp visitada determinará si la PSCF previa se encuentra en otra red. El NAI del terminal móvil se utiliza para ubicar su LMFp originaria. Debe existir una asociación de seguridad entre la LMFp visitada y la LMFp originaria antes de que pueda intercambiarse información alguna entre estas dos entidades. La LMFp visitada envía esta información con la información que se había incluido en la ind.pet. de registro original dirigida a la LMFp originaria.

Conexión túnel (Informe: éxito o fracaso)	**ind.pet.**
NAI (MT)	M
NAI (PSCFpv)	M
NAI (PSCFv)	M
Dirección IP (MT)	M
Dirección IP (PSCFv pública)	M
Discriminador de servicio	M
Dirección IP (PSGCF pública)	M
Valor de puesta a prueba (de la PSCFv)	M
Respuesta de puesta a prueba	M
Método de encapsulado	M
Duración de la sesión de datos	M

FEA5	– Autentica el terminal móvil utilizando el valor de puesta a prueba, la respuesta de puesta a prueba y el secreto que comparte con su terminal móvil. – Detecta que se trata de una sesión de datos por paquetes ya establecida y conoce si la red de anclaje es la red originaria o la red visitada en la que se ha iniciado la sesión. – Puede utilizar las claves de seguridad existentes y los índices de parámetros de seguridad (SPI) que han sido asignados a la PSCF previa, o bien, puede generar nuevos valores para dichos parámetros. – Cuando se pasan las claves de seguridad y los SPI a la PSCAF, a la PSGCF de anclaje, a la LMFp de anclaje y a la LMFp visitada, la LMFp originaria utiliza los secretos compartidos con dichas entidades. – Cuando la red de anclaje no es la red originaria, la LMFp originaria envía la ind.pet. conexión túnel a la LMFp de anclaje en la red visitada en la que se inició la sesión. – Si la PSGCF se encuentra en la red originaria, se envía una petición desde la LMFp originaria a su PSGCF en la red originaria para solicitar el establecimiento de una nueva conexión túnel entre la PSCF visitada y la PSGCF originaria.

6. **ind.pet. conexión túnel**: se envía desde la LMFp originaria a la LMFp de anclaje para solicitar el establecimiento de una nueva conexión túnel entre la PSGCF de anclaje y la PSCF visitada. La LMFp originaria ha registrado el NAI de la LMFp de anclaje cuando se inicia la sesión de datos.

Conexión túnel (Respuesta: éxito o fracaso)	ind.pet.
NAI (MT)	M
Dirección IP (MT)	M
Dirección IP (PSCFv pública)	M
Dirección IP (PSGCF pública)	M
Método de encapsulado	M
Tiempo restante de la sesión de datos	M
Claves de seguridad y SPI	M
Duración de la sesión de datos	M

FEA6	– Detecta que es una sesión de datos establecida. – Envía una petición a su PSGCF para solicitar el establecimiento de una nueva conexión túnel entre la PSCF visitada y la PSGCF de anclaje.

7. **conf.resp. conexión túnel**: se envía desde la LMFp de anclaje a la LMFp originaria para indicar si se ha aceptado o rechazado la petición para establecer una nueva conexión túnel entre la PSCF visitada y la PSGCF de anclaje.

Conexión túnel	conf.resp.
Resultado (indicación de asignación de PSGCF)	M
Dirección IP (PSGCF pública)	M
Dirección IP (MT)	M
Duración de la sesión de datos	M

FEA7	– Responde para confirmar la autorización de establecimiento de una nueva sesión de datos. – Opcionalmente, solicita a la red previamente visitada que elimine la conexión anterior, es decir, la operación "liberación de conexión anterior".

8. **conf.resp. conexión túnel**: se envía desde la LMFp originaria del terminal móvil a la LMFp visitada a fin de autorizar el servicio de datos por paquetes del terminal móvil en la red visitada e indicar si se ha establecido una nueva conexión túnel con la PSGCF de anclaje.

Conexión túnel	conf.resp.
Resultado (indicación de asignación de PSGCF)	M
Dirección IP (PSGCF pública)	M
Dirección IP (MT)	M
Duración de la sesión de datos	M
Claves de seguridad y SPI	M

FEA8	– Informa a la PSCF visitada sobre si se ha establecido una nueva conexión túnel.

9. **conf.resp. sesión de datos**: se envía desde la PSCF visitada a la PSCAF en respuesta a la ind.pet. de registro que solicita el establecimiento de una nueva conexión túnel. Esta información se envía sobre el enlace de acceso establecido.

Sesión de datos	conf.resp.
Resultado (indicación de asignación de PSGCF)	M
Dirección IP (PSGCF pública)	M
Dirección IP (MT)	M
Claves de seguridad y SPI	M
Duración de la sesión de dato	M
ID de sesión	O (nota)

FEA9	– No se requiere actuación.
NOTA – Si lo suministra la PSCAF.	

10. **ind.pet. liberación conexión anterior**: (opcional) para que la LMFp originaria informe a la LMFp previamente visitada que debe borrar toda la información local relativa a la conexión túnel anterior con la PSGCF de anclaje. Este IF es independiente del IF 9.

Liberación de conexión anterior (Respuesta: ni éxito ni fracaso)	ind.pet.
NAI (MT)	M
Dirección IP (MT)	M
NAI (PSCFpv)	M
Dirección IP (PSGCF pública)	M

FEA11	– Responde para confirmar la eliminación de la conexión anterior.

11. **ind.pet. liberación conexión anterior**: (opcional) para que la LMFp previamente visitada envíe la información de confirmación a la LMFp originaria indicando que la conexión túnel anterior ha sido liberada.

liberación conexión anterior	conf.resp.
Resultado	M

FEA11	– No se requiere actuación alguna.

8.5.3 Terminación de la sesión del servicio de datos por paquetes

8.5.3.1 Terminación de una sesión iniciada por el terminal móvil

El terminal o la red pueden decidir terminar una sesión de datos por paquetes en curso. En esta subcláusula se describe el procedimiento del flujo de información de cancelación de registro iniciada por el terminal. La figura 8.5.3-1 muestra el diagrama del flujo de información para este procedimiento. Puede ser necesario repetir los pasos 2-4 a fin de soportar varias sesiones de datos desde el mismo terminal móvil.

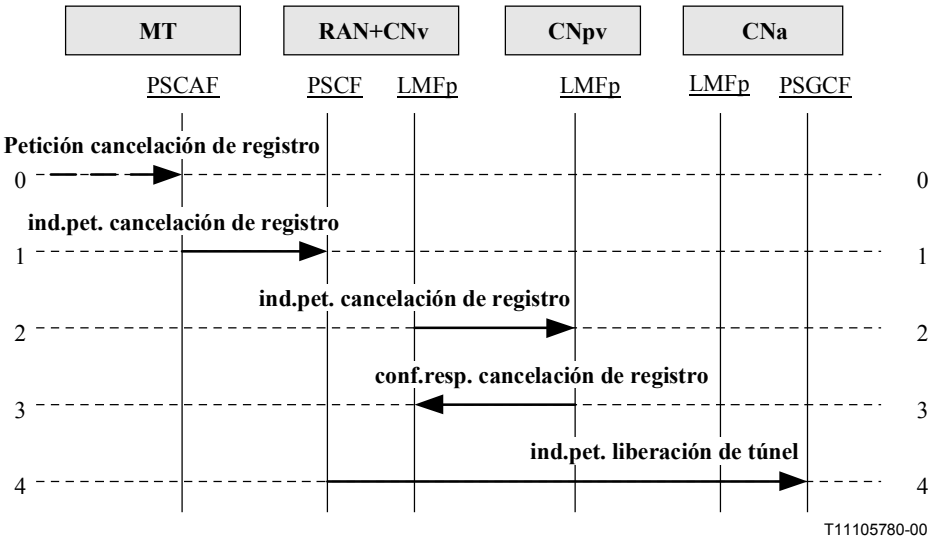


Figura 8.5.3-1/Q.1721 – Terminación de sesión de datos por paquetes iniciada por el terminal

0. **Petición cancelación de registro**: para iniciar la cancelación del registro del servicio de datos por paquetes.

FEA0	– Petición de terminación de la sesión de datos por paquetes en curso.

1. **ind.pet. cancelación de registro**: realizada desde el terminal móvil para informar a la red IMT-2000 de su petición para que cancelar su registro de la sesión del servicio de datos por paquetes en curso.

Cancelación de registro (no se espera respuesta)	ind.pet.
Identificación de usuario (IMUI o TMUI)	M
Dirección IP (PSGCF pública)	M
Dirección IP (PSCFv pública)	M
NAI (PSCFv)	M
Dirección IP (MT)	M
NAI (MT)	M
Duración de la sesión de datos	M

FEA1	– La LMFp visitada actualiza su base de datos según proceda. – La LMFp visitada informa a la LMFp originaria.

2. **ind.pet. cancelación de registro**: la LMFp visitada envía la ind.pet. cancelación de registro a la LMFp originaria para indicar que el terminal ha dejado de ser alcanzable en el sistema visitado.

Cancelación de registro (Respuesta: éxito/fracaso)	ind.pet.
Dirección IP (PSGCF pública)	M
Dirección IP (PSCFv pública)	M
NAI (PSCFv)	M
Dirección IP (MT)	M
NAI (MT)	M
Duración de la sesión de datos	M
Dirección de fuente de sesión	O (nota)

FEA2	– La LMFp originaria actualiza su base de datos según proceda. – La LMFp originaria responde a la LMFp visitada.
NOTA – En el caso de que haya varias sesiones, la PSCFv debe asociar la señal conf.resp. con la correspondiente señal ind.pet. utilizando información de dirección de fuente.	

3. **conf.resp. cancelación de registro**: enviada desde la LMFp originaria para acusar recibo de la petición de cancelación de registro del terminal.

Cancelación de registro	conf.resp.
Dirección IP (MT)	M
NAI (MT)	M
Dirección de fuente de sesión	O (nota)

FEA3	El sistema visitado inicia la liberación del túnel hacia la pasarela PSCF.
NOTA – En el caso de que haya varias sesiones, la PSCFv debe asociar la señal conf.resp. con la correspondiente señal ind.pet. utilizando información de dirección de fuente.	

4. **ind.pet. liberación de túnel**: enviada desde la PSCF servidora para notificar a la PSGCF de anclaje que libere el túnel con la red visitada.

Liberación de túnel (Respuesta: ni éxito ni fracaso)	ind.pet.
Dirección IP (PSGCF pública)	M
Dirección IP (PSCFv pública)	M
NAI (PSCFv)	M
Dirección IP (MT)	M
NAI (MT)	M
Duración de la sesión de datos	M

FEA4	– La PSGCF de la red de anclaje notifica a su LMFp local que ya no actúa como pasarela hacia el terminal cuyo registro se ha cancelado. – La LMFp de anclaje actualiza su base de datos según proceda.

8.5.3.2 Terminación de una sesión iniciada por la red

El terminal o la red pueden decidir terminar una sesión de datos por paquetes en curso. Esta subcláusula describe el procedimiento del flujo de información de cancelación de registro iniciada por la red. La figura 8.5.3-2 muestra el diagrama del flujo de información para este procedimiento. Puede ser necesario repetir los pasos 2-4 a fin de soportar varias sesiones de datos desde el mismo terminal móvil.

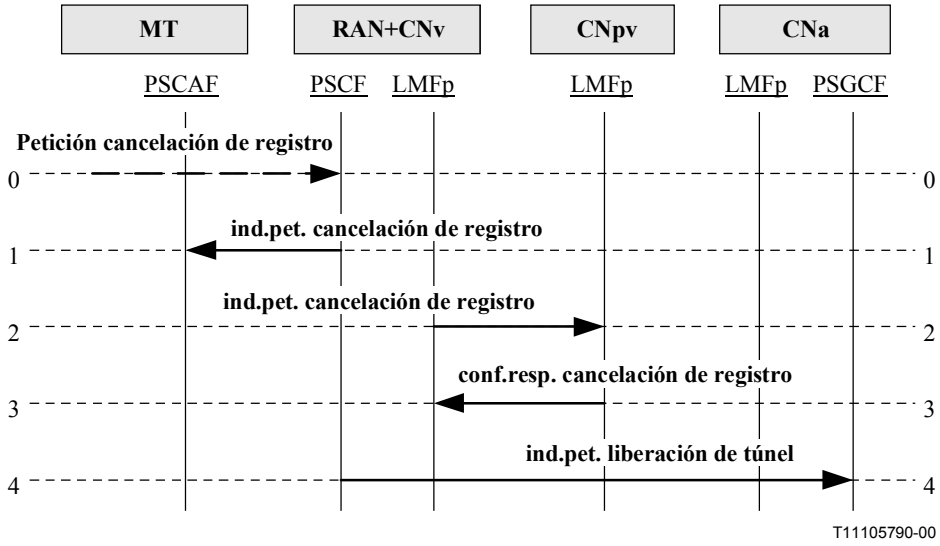


Figura 8.5.3-2/Q.1721 – Terminación de la sesión de datos por paquetes iniciada por la red

0. **Petición de cancelación de registro**: la red inicia la cancelación del registro de un servicio de datos por paquetes.

FEA0	– Notifica cual es el terminal (PSCAF) cuyo registro quiere cancelarse.

1. **ind.pet. cancelación de registro**: para informar al terminal de la intención de la red de cancelar el registro del terminal de la sesión del servicio de datos por paquetes en curso.

Cancelación de registro (Respuesta: ni éxito ni fracaso)	**ind.pet.**
Identificación de usuario (IMUI o TMUI)	M

FEA1	– El terminal se prepara para liberar el enlace de acceso.

2. **ind.pet. cancelación de registro**: envía la petición de cancelación de registro a la LMFp originaria para indicar que el terminal ya no es alcanzable en el sistema visitado.

Cancelación de registro (Respuesta: éxito/fracaso)	**ind.pet.**
Dirección IP (PSGCF pública)	M
Dirección IP (PSCFv pública)	M
NAI (PSCFv)	M
Dirección IP (MT)	M
NAI (MT)	M
Duración de la sesión de datos	M
Dirección de la fuente de sesión	O (nota)

FEA2	– La LMFp originaria actualiza su base de datos según proceda. – La LMFp originaria responde a la LMFp visitada.
NOTA – En el caso de que haya varias sesiones, la PSCFv debe asociar la señal de respuesta con la correspondiente señal ind.pet. utilizando información de dirección de fuente.	

3. **conf.resp. cancelación de registro**: para que la LMFp originaria acuse recibo de la petición para cancelar el registro del terminal.

Cancelación de registro	**conf.resp.**
Dirección IP (MT)	M
NAI (MT)	M
Dirección de fuente de sesión	O (nota)

FEA3	– El sistema visitado inicia la liberación del túnel con la pasarela PSCF.
NOTA – En caso de que haya varias sesiones, la PSCFv debe asociar la señal de respuesta con la correspondiente señal de petición utilizando la información de dirección de fuente.	

4. **ind.pet. liberación de túnel**: la PSCF servidora notifica a la PSGCF de anclaje que libere el túnel con la red visitada.

Liberación de túnel (no se espera respuesta)	ind.pet.
Dirección IP (PSGCF pública)	M
Dirección IP (PSCFv pública)	M
NAI (PSCFv)	M
Dirección IP (MT)	M
NAI (MT)	M
Duración de la sesión de datos	M

FEA4	– La PSGCF de la red de anclaje notifica a su LMFp local que ya no sirve como pasarela hacia el terminal cuyo registro se ha cancelado. – La LMFp de anclaje actualiza su base de datos según proceda.

9 Entorno originario virtual

La invocación del servicio en un sistema IMT-2000 puede ocurrir en cualquier momento durante el procesamiento de una llamada. Asimismo, puede ocurrir conjuntamente con la llamada o con independencia de la misma, en relación con el proceso de gestión de la movilidad o con el proceso de autenticación. Los servicios se ofrecen de acuerdo con la información del perfil de servicio del abonado. En dicho perfil están incluidos los servicios básicos y suplementarios, así como los elementos de disparo y la información asociada (por ejemplo, los criterios de disparo, la dirección de la lógica servicio asociada, etc.) para servicios basados en VHE adaptados las necesidades de los clientes. No es previsible que las redes IMT-2000 visitadas ofrezcan servicios específicamente adaptados al cliente (es decir, servicios adaptados al cliente ofrecidos por operadores de redes o proveedores de servicio originarios). Sin embargo, la capacidad y los procedimientos del VHE permiten a las redes servidoras ofrecer estos servicios a los usuarios visitantes.

En el concepto de VHE puede establecerse una separación entre la provisión de servicios y la operación de red, pudiendo ser ofrecidos los servicios por redes distintas a las que ofrecen las capacidades de procesamiento de llamada de la red originaria. En algunos casos, la lógica de servicio puede ser accesible en una red soporte distinta. En otros casos, la red originaria proporciona la lógica de servicio y, por lo tanto, actúa como red soporte.

En la descripción siguiente (subcláusulas 9.1 y 9.2), la red soporte es la red en la que se encuentra y se ejecuta la lógica del servicio (identificada como CNs). La red servidora o visitada es la red en la que el usuario se encuentra en itinerancia cuando se solicita la ejecución del servicio (identificada como CNv.) La red originaria (identificada como CNh) es aquélla en la que se ubican la función de gestión de ubicación originación (LMFh, *location management function*) y la función de gestión de la autenticación originaria (AMFh, *authentication management function*). La CNs y la CNh pueden ser la misma red.

Las Recomendaciones Q.1701 y Q.1711 identifican dos escenarios de realización de VHE para el CS-1 de IMT-2000. El escenario de "instrucción originaria directa" de 9.1 y el escenario de "control del servicio de retransmisión" de 9.2.

9.1 "Instrucción originaria directa"

En el escenario de VHE de "instrucción originaria directa", la red soporte proporciona la lógica del servicio a la red visitada que sirve al abonado itinerante a fin de soportar los servicios VHE de dicho abonado. La lógica de servicio de la red soporte se invoca mediante la capacidad de disparo de RI de la red visitada. Pueden ser necesaria una preorganización entre la red soporte y la red visitada con el fin de supervisar las invocaciones de disparo.

9.1.1 Procedimiento de servicio de "instrucción originaria directa" de alto nivel

En un esquema de flujos de información extremo a extremo, este procedimiento consta de cuatro componentes: origen de llamada, invocación de lógica de servicio del VHE, encaminamiento de llamada y conexión de llamada (en el caso de servicios relacionados con la llamada; en el caso de escenarios no relacionados con la llamada se aplican procedimientos similares de servicio VHE). Esta subcláusula se ocupa de los flujos de información de la parte de invocación de la lógica del servicio y trata los flujos de información de las otras tres partes como procedimientos comunes en el contexto de los flujos de información extremo a extremo.

Los supuestos siguientes se hacen en relación con los flujos de información de invocación de la lógica de servicio VHE:

- En este escenario es necesaria una predisposición entre la red soporte y la red originaria o entre las redes soporte y visitada para la supervisión o cribado de las invocaciones de disparo.
- La red servidora/visitada tiene capacidades de RI para el desencadenamiento de la lógica de servicio necesaria.

En la figura 9.1.1-1 se presenta una visión general de alto nivel del diagrama de un flujo de información para el escenario VHE de "instrucción originaria directa". En relación con esta figura debe tenerse en cuenta lo siguiente:

- para servicios relacionados con la llamada, sólo se incluye el lado origen de llamada de los flujos generados en la parte llamante; una interacción semejante puede ocurrir entre la terminación de llamada y la parte llamada;
- otras formas de iniciar la lógica de servicio no relacionada con llamadas, tales como la gestión de la movilidad o la gestión de la autenticación, se comportan de la misma forma, aunque los mensajes procedan de una entidad funcional (FE) distinta de la "RAN+CNh o v" (véanse 9.1.3 y 9.1.4);
- el caso de notificación a la lógica del servicio es un subconjunto de la figura 9.1.1-1 (es decir, no se necesitaría el flujo 2); y
- la figura se simplifica notablemente porque no ilustra toda la gama de interacciones de la lógica de servicio soportada por la RI; por ejemplo, no refleja una interacción ampliada con la lógica del servicio (que puede continuar hasta que se libera la llamada), ni la interacción con el usuario controlada por la lógica del servicio, etc.

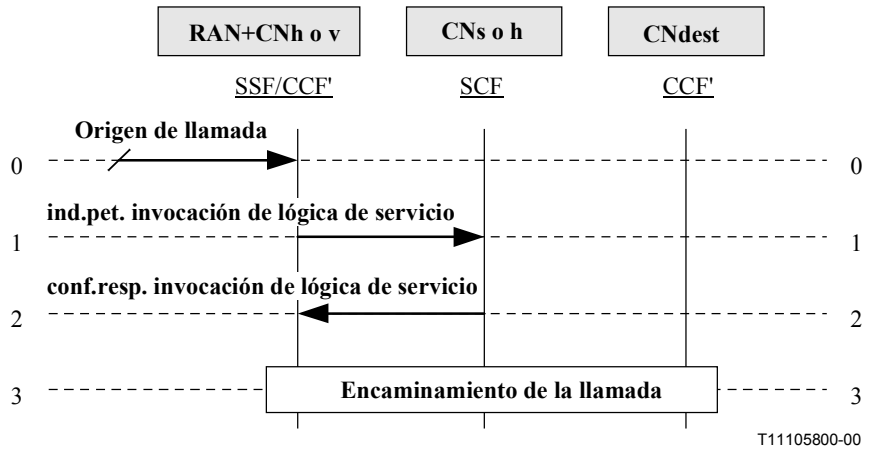


Figura 9.1.1-1/Q.1721 – "Instrucción originaria directa" de alto nivel relacionada con la llamada

0. **Origen de llamada**: un abonado origina una llamada. La información que se obtiene de la red originaria cuando se realiza el registro contiene información para que la red servidora soporte la invocación de servicio VHE[3].

FEA0	– El procesamiento de la llamada continúa hasta que se encuentra un disparo armado en un punto de detección de disparo (TDP, *trigger detection point*) y se cumplen los criterios relativos a dicho disparo armado.

1. **ind.pet. invocación de lógica de servicio**: se utiliza para invocar la lógica de servicio en la SCF asociada con el disparo cuyos criterios se satisfacen. Incluye información sobre el abonado, el estado de la llamada y la condición de disparo encontrada.

Invocación de lógica de servicio (Respuesta: éxito o fracaso)	**ind.pet.**
Elementos de información en un IF de inicio de lógica del servicio	Según [5]
IMUI	M

FEA1	– Ejecución de la lógica del servicio.

2. **conf.resp. invocación de lógica de servicio**: proporciona la orden de procesamiento de llamada cuya lógica de servicio desea realizar la entidad invocadora.

Invocación de lógica de servicio	**conf.resp.**
Elementos de información en un IF de respuesta a la lógica del servicio	Según [5]

FEA2	– Ejecución de la instrucción de procesamiento de la llamada si ello es posible.

[3] Esta información se incluye en la información del perfil de usuario que se obtiene durante el registro de la MT. Con ello se evita la necesidad de obtener esta información como parte del origen de la llamada.

3. **Encaminamiento de llamada**: se utiliza para continuar el procesamiento de la llamada y para conectarla a la red de destino, en caso de que esa sea la actuación adecuada en función de la información presente en conf.resp. invocación de lógica de servicio.

La red originaria del usuario o una red soporte (que puede ser la red originaria) proporcionan la lógica de servicio de los servicios basados en VHE adaptados al cliente que utilizan la "instrucción originaria directa". En el escenario de VHE generalizado, se supone que los servicios los proporciona una red soporte.

Esta subcláusula presenta un IF extremo a extremo simplificado de alto nivel para el procedimiento de la "instrucción originaria directa" (DHC). La invocación de la capacidad de disparo de servicios basados en VHE puede ocurrir para dos clases de servicios:

- **Invocación de servicio relacionado con la llamada** tiene lugar durante el procesamiento de la llamada (por ejemplo, origen de llamada, terminación de llamada o punto intermedio de una llamada). En el ámbito de FE, este escenario invoca la lógica de servicio en la SCF de la red soporte mediante la capacidad de disparo de la CCF'/SSF de la red visitada.
- **Invocación de servicio no relacionado con la llamada** tiene lugar en los eventos de gestión de la movilidad[4] o en eventos de autenticación. En el ámbito de FE, este escenario invoca la lógica de servicio en la SCF de la red soporte mediante una interrogación desde la LMF o desde la AMF.

9.1.2 "Instrucción originaria directa" – Servicios relacionados con la llamada

Esta subcláusula amplía la información relativa a la componente de "invocación de servicio VHE" para la interfaz red-red (NNI) y trata de los requisitos de señalización en el escenario de instrucción originaria directa (DHC) para los servicios que invoca una SSF/CCF' en la red visitada. Se supone que la SSF/CCF tiene la capacidad de disparar la lógica de servicio SCF requerida que reside en la red soporte.

La subcláusula 7.2.2.5/Q.1711 describe un modelo funcional IMT-2000 para interconexiones a través de los NNI existentes entre una red originaria, una red soporte y una red visitada. Estas interconexiones son necesarias para la invocación de la lógica de servicio en la red soporte.

La figura 9.1.2-1 presenta el escenario DHC del diagrama del flujo de información VHE. La figura está simplificada en cuanto que no ilustra toda la gama de interacciones de la lógica del servicio soportadas por RI como se señala en 9.1.1 anterior. El procedimiento "invocación de servicio VHE" puede finalizar después de la primera "asistencia de recurso especializado" o puede continuar hasta que se completa el servicio relacionado con la llamada.

En esta subcláusula se describe los disparos en relación con el origen de la llamada. Los disparos pueden también tener lugar durante la terminación de la llamada o en fases intermedias de la misma.

---

[4] El procesamiento de la gestión de la movilidad puede tener lugar conjuntamente o separado de cualquier evento de llamada.

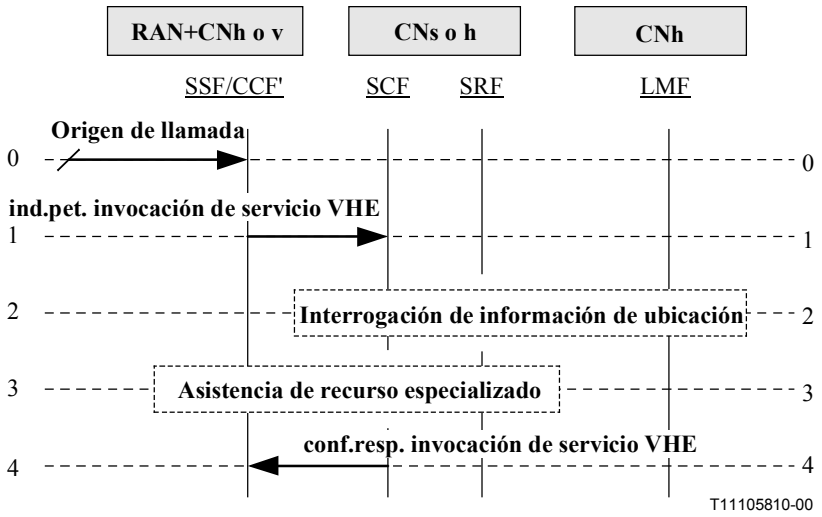


Figura 9.1.2-1/Q.1721 – "Instrucción originaria directa" relacionada con la llamada

0. **Origen de llamada**: la parte llamante inicia una llamada en una red visitada. La información obtenida de la red originaria cuando se realiza el registro incluye los disparadores y los criterios asociados así como otros parámetros para que la red visitada soporte los servicios de VHE.

FEA0	– En la BCSM de SSF/CCF' existe un disparo armado cuyos criterios se cumplen.

1. **ind.pet. invocación de servicio VHE**: se utiliza para invocar la lógica de servicio de VHE del SCF soporte.

Invocación de servicio VHE (Respuesta: éxito o fracaso)	**ind.pet.**
Elementos de información en un IF de inicio de lógica de servicio	Según [5]
IMUI	M
Capacidad de la MS	O (nota 1)
Información de ubicación de la MS	O (nota 2)

FEA1	– Identifica el usuario. – Recupera datos de servicio del usuario que existen en el perfil de servicio VHE del abonado (por ejemplo, SDF). – Si se requiere, se formula y se envía a la LMF de la red originaria una petición de ubicación de MS y de información de estado.
NOTA 1 – La capacidad de la MS se incluye en función de criterios de disparo. NOTA 2 – La información de ubicación de la MS se incluye si está disponible.	

2. **Interrogación de información de ubicación**: se utiliza para solicitar información sobre la ubicación del usuario llamado si lo requiere la lógica de servicio y no se incluyó en el primer flujo de información.

3. **Asistencia de recurso especializado**: si es necesaria, la inicia la lógica del servicio en la SCF para conseguir acceso a los recursos especializados de la SRF (por ejemplo, reproducción de anuncios o recopilación de dígitos) junto con la SSF/CCF'. Este procedimiento utiliza procedimientos de la INAP tal como se definen en la Recomendación Q.1238.

4. **conf.resp. invocación de servicio VHE**: transfiere las instrucciones de servicio VHE a la entidad que inicia la invocación de servicios VHE.

Invocación de servicio VHE	conf.resp.
Elementos de información en un IF de respuesta de la lógica de servicio	Según [5]

FEA4	– Continúa el procesamiento de la llamada para cada instrucción recibida de la SCF, si ello es posible.

9.1.3 "Instrucción originaria directa" – Servicios invocados por la LMF

En la subcláusula 7.2.2.5/Q.1711 se describe un modelo funcional IMT-2000 para la interconexión a través de la interfaz NNI entre una red originaria o una red visitada y la red soporte. Estas interconexiones son necesarias para la invocación de la lógica del servicio en la red soporte que se dispara desde la función de gestión de la ubicación (LMF).

La figura 9.1.3-1 presenta el diagrama del flujo de información del escenario de DHC de VHE invocada por la LMF.

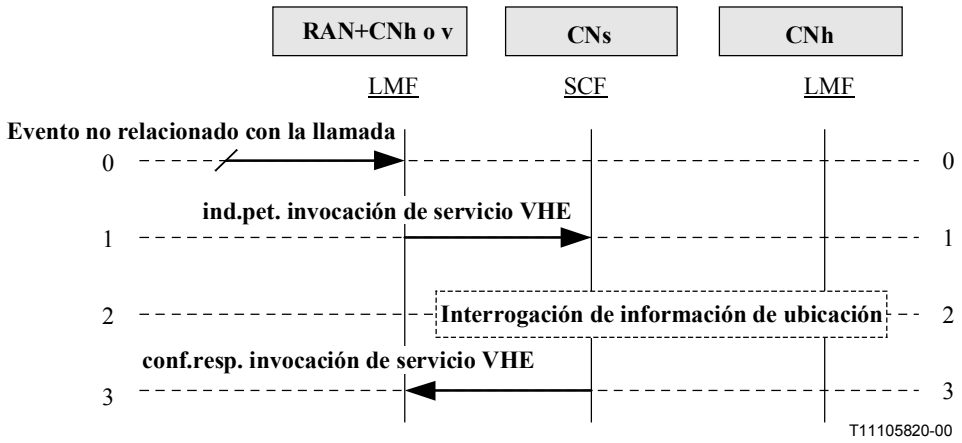


Figura 9.1.3-1/Q.1721 – "Instrucción originaria directa" de LMF

0. **Evento no relacionado con la llamada**: el proceso de gestión de la movilidad utiliza información obtenida durante el registro en la red originaria. Esta información incluye los disparos y los criterios asociados así como otros parámetros para el soporte por la red visitada de los servicio VHE invocados por la LMF.

FEA0	– En un TDP del modelo de estados de la LMF existe un disparo armado cuyos criterios se cumplen.

1. **ind.pet. invocación de servicio VHE**: se utiliza para invocar la lógica del servicio VHE en la SCF soporte.

Invocación de servicio VHE (Respuesta: éxito o fracaso)	ind.pet.
Clave del servicio	M
Tipo de evento	M
IMUI	M
Capacidad de la MS	O (nota 1)
Información de ubicación de la MS	O (nota 2)

FEA1	– Identifica el usuario. – Recupera datos del servicio de usuario del perfil de servicio VHE del abonado (por ejemplo, SDF). – Si se requiere, se formula y se envía a la LMF de la red originaria una petición de ubicación de la MS y de información de estado.
NOTA 1 – La capacidad de la MS se incluye en función de criterios de disparo. NOTA 2 – La información de ubicación de la MS se incluye si está disponible.	

2. **Interrogación de información de ubicación**: utilizada para solicitar información sobre la ubicación del usuario llamado si lo requiere la lógica de servicio y no se incluyó en el primer flujo de información.

3. **conf.resp. invocación de servicio VHE**: transfiere las instrucciones de servicio VHE a la entidad que inicia la invocación de servicios VHE.

Invocación de servicio VHE	conf.resp.
Instrucción de servicio VHE	M

FEA2	– Continúa el procesamiento del procedimiento de registro de ubicación según la instrucción recibida de la SCF.

9.1.4 "Instrucción originaria directa" – Servicios invocados por la AMF

En la subcláusula 7.2.2.5/Q.1711 se describe un modelo funcional IMT-2000 para la interconexión a través de la interfaz NNI entre una red originaria o una red visitada y la red soporte. Estas interconexiones son necesarias para la invocación de la lógica del servicio en la red soporte que se dispara desde la función de gestión de la autenticación (AMF).

La figura 9.1.4-1 presenta el diagrama del flujo de información del escenario de DHC de VHE invocada por la AMF.

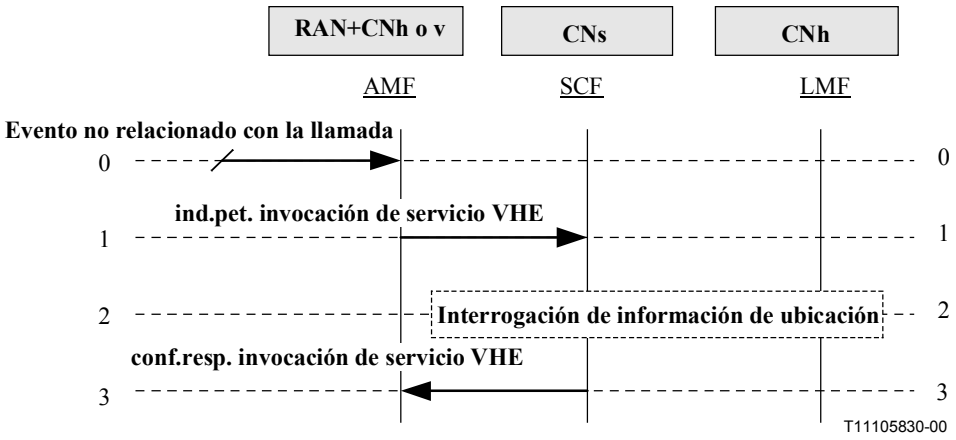


Figura 9.1.4-1/Q.1721 – "Instrucción originaria directa" de la AMF

0. **Evento de gestión de autenticación**: inicia el proceso de gestión de autenticación. La información disponible incluye los disparos y los criterios asociados así como otros parámetros para el soporte de los servicios VHE invocados por la AMF.

FEA0	– En un TDP del modelo de estados de la AMF existe un disparo armado cuyos criterios se cumplen.

1. **ind.pet. invocación de servicio VHE**: se utiliza para invocar la lógica de servicio VHE en la SCF soporte.

Invocación de servicio VHE (Respuesta: éxito o fracaso)	**ind.pet.**
IMUI	M
Clave del servicio	M
Tipo de evento	M
Información de ubicación de la MS	O (nota)

FEA1	– Identifica el usuario. – Recupera datos del servicio de usuario del perfil de servicio VHE del abonado (por ejemplo, SDF.) – Si se requiere, se formula y se envía a la LMF de la red originaria una petición de ubicación de MS y de información de estado.
NOTA – La información de ubicación de la MS se incluye si está disponible.	

2. **Interrogación de información de ubicación**: se utiliza para solicitar información sobre la ubicación del usuario llamado si lo requiere la lógica de servicio y no se incluyó en el primer flujo de información.

3. **conf.resp. invocación de servicio VHE**: se utiliza para enviar instrucciones de servicio de VHE desde la SCF de la red soporte a la AMF solicitante.

Invocación de servicio VHE	conf.resp.
Instrucción de servicio VHE	M

FEA2	– Continúa el procesamiento del procedimiento de registro de ubicación según la instrucción recibida de la SCF.

9.2 "Retransmisión del control del servicio"

El escenario de "retransmisión del control del servicio" (RSC) del VHE consiste en la invocación de la lógica de servicio que reside en la SCF de una red soporte (u originaria) por parte de la SCF de una red servidora (ya sea una red originaria o visitada).

En la RSC VHE, la lógica del servicio está distribuida entre la red soporte y la red visitada a fin de soportar los servicios VHE de un abonado itinerante.

Si la red servidora coincide con la red soporte, la RSC VHE consiste en la invocación de los servicios de RI para los que existen procedimientos bien establecidos. Cuando la red servidora no es una red soporte, puede aplicarse la RSC VHE. En la RSC VHE, siempre se supone que las redes soporte y servidora son dos redes distintas que interfuncionan a través de un protocolo NNI.

En la red servidora, la CCF'/SSF, la LMF o la AMF informan a la SCF de los eventos de interés. Los disparadores de los FE invocadores pueden armarse mediante la información del perfil del abonado o mediante un proceso de provisión de servicio concurrente. La SCFv invocada (de la red servidora) interroga a la SCF (de la red soporte) para permitir el control del servicio[5].

La lógica de servicio de los servicios VHE que utilizan el RSC es proporcionada por la red originaria del usuario o por una red soporte. Para el escenario VHE generalizado se supone que los servicios los proporciona una red soporte.

Se supone que se establece una preorganización anterior a la cooperación y coordinación entre las redes servidora y soporte para la RSC VHE. El grado de cooperación puede oscilar desde parcial (compartido) hasta la retransmisión completa del programa de control del servicio[6].

A igual que ocurre con la "instrucción originaria virtual" VHE, los servicios del escenario RSC pueden estar relacionados con la llamada o ser independientes de la misma.

9.2.1 Procedimiento de servicio de la "retransmisión del control del servicio"

Este procedimiento solicita la invocación la lógica del servicio a las SCFs a través de la SCFv para permitir el control del servicio. La preorganización existente entre las redes soporte y visitada pueden consistir en la retransmisión de las capacidades de seguridad y de cribado, las subrutinas del programa de ejecución de la lógica de servicio o de programas ejecutables completos.

En la subcláusula 7.2.2.5/Q.1711 se describe un modelo funcional IMT-2000 para la interconexión a través de NNI entre una red originaria, una red soporte y una red visitada. Estas interconexiones son necesarias para la invocación de la lógica y de las instrucciones de servicio en la red soporte.

---

[5] Las figuras 7-7/Q.1711 y 7-8/Q.1711 muestran las interconexiones a través del NNI que pueden ser utilizadas para informar de este evento.

[6] La retransmisión de capacidad de seguridad o de cribado para procedimientos de control abusos y fraudes puede también ser ejecutada por un programa de lógica de servicio (SLP, s*ervice logic program*) en una SCF.

En un esquema de IF extremo a extremo, este procedimiento consta de cuatro componentes: estímulo inicial; invocación de servicio VHE, información de tratamiento VHE y compleción del procedimiento inicial. En esta subcláusula se analizan los flujos de información de la invocación de la lógica de servicio VHE y de las partes de información de tratamiento de VHE, y considera los flujos de información de las tres partes como procedimientos comunes en el contexto de los flujos de información extremo a extremo.

La figura 9.2.1-1 es el diagrama del flujo de información del escenario de "retransmisión de control del servicio" VHE. Se supone que la SSF/CCF', la LMF o la AMF tienen, si cumplen los criterios de disparo, la capacidad de enviar un mensaje a la SCF requerida en la red servidora, y que la SCF servidora puede solicitar ayuda a la SCF soporte. En relación con dicha figura debe señalarse lo siguiente:

- El caso de notificación a la lógica de servicio es un subconjunto de la figura 9.2.1-1 (es decir, los flujos 2 y 3 no son necesarios); y
- La figura es una notable simplificación puesto que no ilustra toda la gama de interacciones de la lógica de servicio soportadas mediante RI; por ejemplo, no refleja una interacción ampliada con la lógica de servicio (que puede continuar hasta que la llamada se libera), ni la interacción del usuario controlada por el servicio, etc.

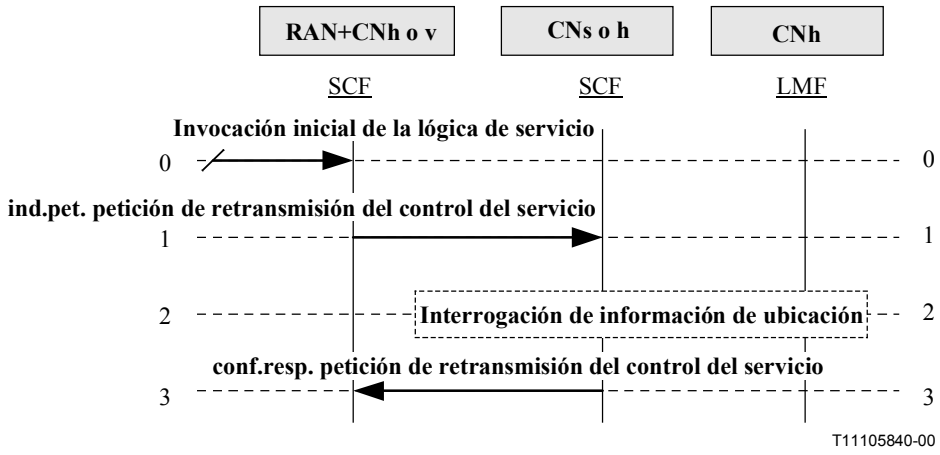


Figura 9.2.1-1/Q.1721 – Representación de alto nivel de la "retransmisión del control del servicio"

0. **Invocación inicial de la lógica de servicio**: invoca la lógica del servicio en la SCF asociada con el disparo cuyos criterios se cumplen. Incluye información sobre el abonado, sobre el estado del proceso de la llamada (invocado desde la SSF/CCF') o el estado de la gestión de la movilidad (invocado desde la LMF) o el estado del proceso de autenticación (invocado desde la AMF), y sobre la condición de disparo que se encuentra.

FEA0	– Identifica la red soporte del usuario. – Verifica el acuerdo bilateral para el esquema RSC. – Invoca a la SCFs (de la red soporte) para el programa de lógica del servicio (SLP) VHE del usuario.

1. **ind.pet. retransmisión del control del servicio**: utilizada por la SCF de control para enviar una petición a la SCF soporte o para solicitar que ésta realice acciones predefinidas.

Retransmisión del control del servicio (Respuesta: éxito o fracaso)	ind.pet.
Clave del servicio	M
Tipo de evento	M
IMUI	M
Capacidad de la MS	O (nota 1)
Información de ubicación de la MS	O (nota 2)

FEA1	– Identifica al usuario y su ID de servicio. – Identifica la SLP solicitada. – Si se requiere, se formula y se envía a la LMF de la red originaria una petición de información de ubicación de la MS y de estado. – Verifica las restricciones (utilizando la IMUI, ubicación de MS, etc.).
NOTA 1 – La capacidad de la MS se incluye en función de criterios de disparo. NOTA 2 – La información de ubicación de la MS se incluye si está disponible.	

2. **Interrogación de información de ubicación**: se utiliza para solicitar información sobre la ubicación del usuario llamado, si lo necesita la lógica del servicio y no estaba incluido en el primer flujo de información.

3. **conf.resp. petición de retransmisión del control del servicio**: se utiliza para enviar a la SCF de control la información necesaria para que la llamada pueda progresar.

Retransmisión del control del servicio	ind.pet.
Lógica de servicio retransmitida	M

FEA2	– Ejecuta la lógica de servicio retransmitida.

10 Aplicaciones de servicios de mensajería

El servicio de mensajes cortos (SMS, *short message service*) punto a punto proporciona los medios necesarios para enviar mensajes de texto hacia y desde terminales móviles IMT-2000. La provisión de SMS utiliza un centro de mensajes (MC, *message center*) que actúa como un centro de almacenamiento y retransmisión de mensajes cortos.

Se han definido dos servicios punto a punto distintos: originado en el móvil y terminado en el móvil. Los mensajes originados en el móvil se transportan desde un MT a un centro de mensajes. Pueden estar dirigidos a otros usuarios móviles o a usuarios en la red fija. Los mensajes terminados en móviles se transportan desde un centro de mensajes a un MT. Pueden haber accedido al centro de mensajes desde otros usuarios móviles (mediante un mensaje corto originado en un móvil) o desde diversas fuentes tales como señales de voz, télex o facsímil.

La difusión de mensajes de teleservicios (TMB, *teleservice message broadcast*) punto a multipunto proporciona un método para la gestión y entrega de mensajes de teleservicios que se difunden a través de la interfaz radioeléctrica a los terminales móviles IMT-2000. Los mensajes TMB se difunden en zonas geográficas que se conocen como zonas de difusión celulares. Dichas zonas

pueden incluir uno o varias células o toda la red para un determinado proveedor de servicio. A cada mensaje TMB se le asigna su propia zona de cobertura geográfica mediante acuerdos al efecto entre el proveedor de información y el operador de red.

10.1 Servicio de mensajes cortos (SMS)

10.1.1 Transferencia de notificación del SMS

El procedimiento de notificación del SMS se utiliza para alertar al centro de mensajes. Los procedimientos comienzan cuando el terminal móvil está activo (después de que haya fallado la transferencia de un mensaje corto debido a que el terminal móvil no estaba previamente en situación de ser alcanzado) o cuando el terminal móvil ha indicado que dispone de capacidad de memoria para aceptar un mensaje corto.

10.1.1.1 MT activo

Véase la figura 10.1.1.1-1.

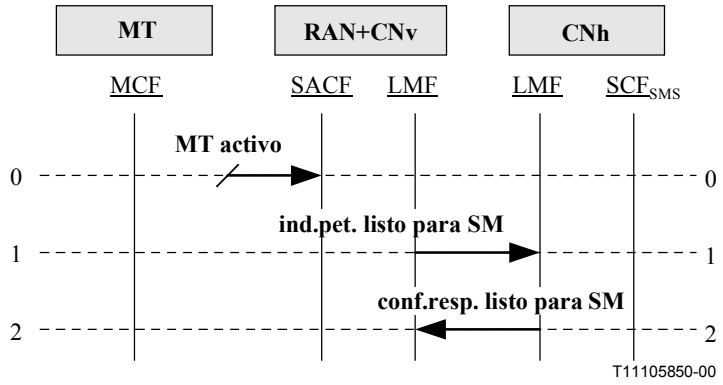


Figura 10.1.1.1-1/Q.1721 – Transferencia de notificación de SMS (MT activo)

0. **MT activo**: cuando el MT está activo, por ejemplo, porque el MT realizó una petición de servicio, originó una llamada o una respuesta de radiobúsqueda. Facultativamente, puede haber tenido lugar la autenticación del usuario.

FEA0	– Cuando el MT está presente, LMFv modifica la correspondiente base de datos e informa a la LMFh.

1. **ind.pet. listo para SM**: informa a la LMFh que el MT está listo para aceptar mensajes cortos.

Listo para SM (Respuesta: éxito)	ind.pet.
IMUI	M
Motivo de alerta	M

FEA1	– Informa a la red visitada que se ha recibido la petición de listo para SM.

2. **conf.resp. listo para SM**: acusa recibo de la recepción de la petición de mensajes cortos.

Listo para SM	conf.resp.
Error de usuario	O (nota)
Error de proveedor	O (nota)

FEA2	– Termina la transferencia de notificación SMS.
NOTA – Sólo se requiere si se ha producido una situación de error.	

10.1.1.2 Capacidad de memoria disponible

Véase la figura 10.1.1.2-1.

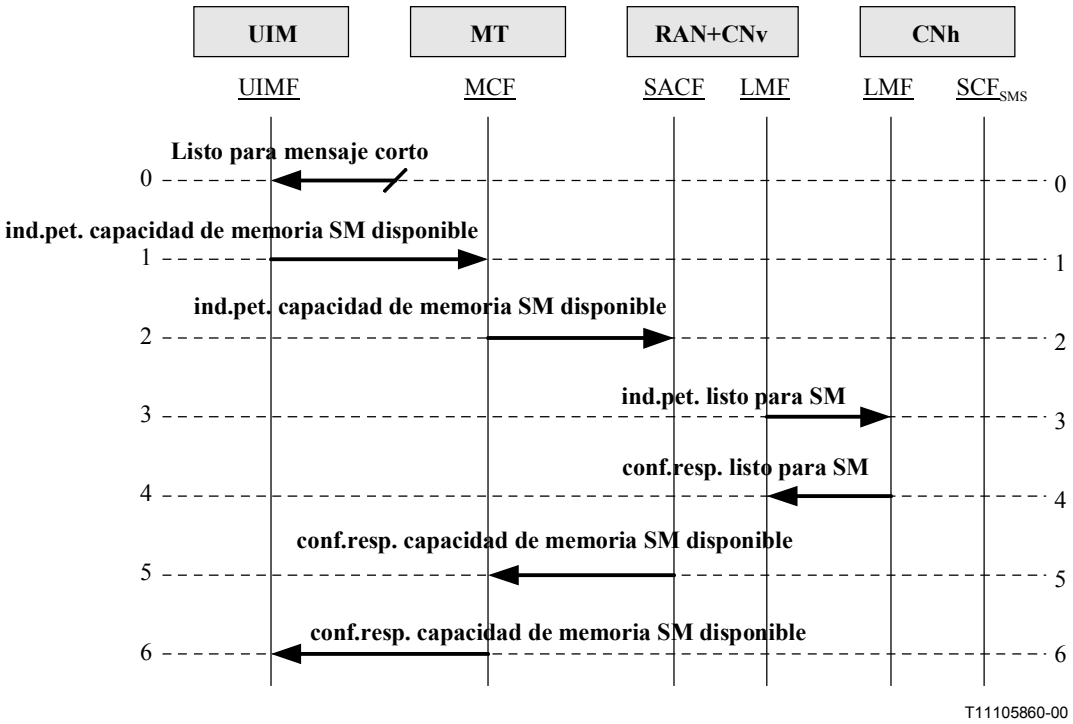


Figura 10.1.1.2-1/Q.1721 – Transferencia de notificación de SMS (capacidad de memoria disponible)

0. **Listo para mensaje corto**: es el estímulo inicial mediante el que el terminal móvil hace una petición de servicio. Facultativamente, puede haber tenido lugar la autenticación del usuario.

FEA0	– Cuando la UIMF tiene la posibilidad de manejar mensajes cortos y dispone de capacidad de memoria, informa a la MCF.

1. **ind.pet. capacidad de memoria SM disponible**: informa a la MCF en el MT que tiene capacidad de memoria disponible para aceptar mensajes cortos.

Capacidad de memoria SM disponible (Respuesta: éxito)	ind.pet.
TMUI o IMUI	M (nota)

FEA1	– Retransmite la petición a la red servidora.
NOTA – TMUI debe utilizarse si está disponible.	

2. **ind.pet. capacidad de memoria SM disponible**: informa a la red visitada que el MT está listo para aceptar mensajes cortos.

Capacidad de memoria SM disponible (Respuesta: éxito)	ind.pet.
TMUI o IMUI	M (nota)

FEA2	– Prepara la información a la red originaria de que el abonado solicitante está listo para aceptar mensajes cortos.
NOTA – TMUI debe utilizarse si está disponible.	

3. **ind.pet. listo para SM**: informa a la LMFh que el MT está listo para aceptar mensajes cortos.

Listo para SM (Respuesta: éxito)	ind.pet.
IMUI	M
Motivo de alerta	M

FEA3	– Informa a la red visitada que se ha recibido la petición de listo para SM.

4. **conf.resp. listo para SM**: acusa recibo de la recepción de la petición de mensajes cortos.

Listo para SM	conf.resp.
Error de usuario	O (nota)
Error de proveedor	O (nota)

FEA4	– Retransmite acuse de recibo a la MCF.
NOTA – Sólo se requiere si se ha producido una situación de error.	

5. **conf.resp. capacidad de memoria SM disponible**: envío desde la red visitada que debe confirmarse.

Capacidad de memoria SM disponible	conf.resp.
Ninguna	(nota)

FEA5	– Retransmite el acuse de recibo a la UIMF.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

6. **conf.resp. Capacidad de memoria SM disponible**: envía confirmación a la UIMF.

Capacidad de memoria de SM disponible	conf.resp.
Ninguna	(nota)

FEA6	– No se requiere acción alguna.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

10.1.2 Mensaje corto originado en el móvil

El terminal móvil envía un mensaje corto a la CCF'/SACF de la red visitada. La CCF'/SACF interroga a la LMFv para recuperar la dirección MS ISDN y envía el mensaje al nodo de interfuncionamiento CCF'/SSF de la red de destino. El nodo CCF'/SSF envía el mensaje corto al centro de mensajes. En el plan de numeración de la red de destino a la que se conecta el centro de mensajes se utiliza un número E.164 para direccionar el centro de mensajes desde el terminal móvil. El número E.164 se almacena en la UIM.

10.1.2.1 Mensaje corto originado en el móvil (en un canal de tráfico)

Este procedimiento se invoca cuando un usuario IMT-2000 envía un mensaje corto punto a punto estando en curso una llamada. Véase la figura 10.1.2.1-1.

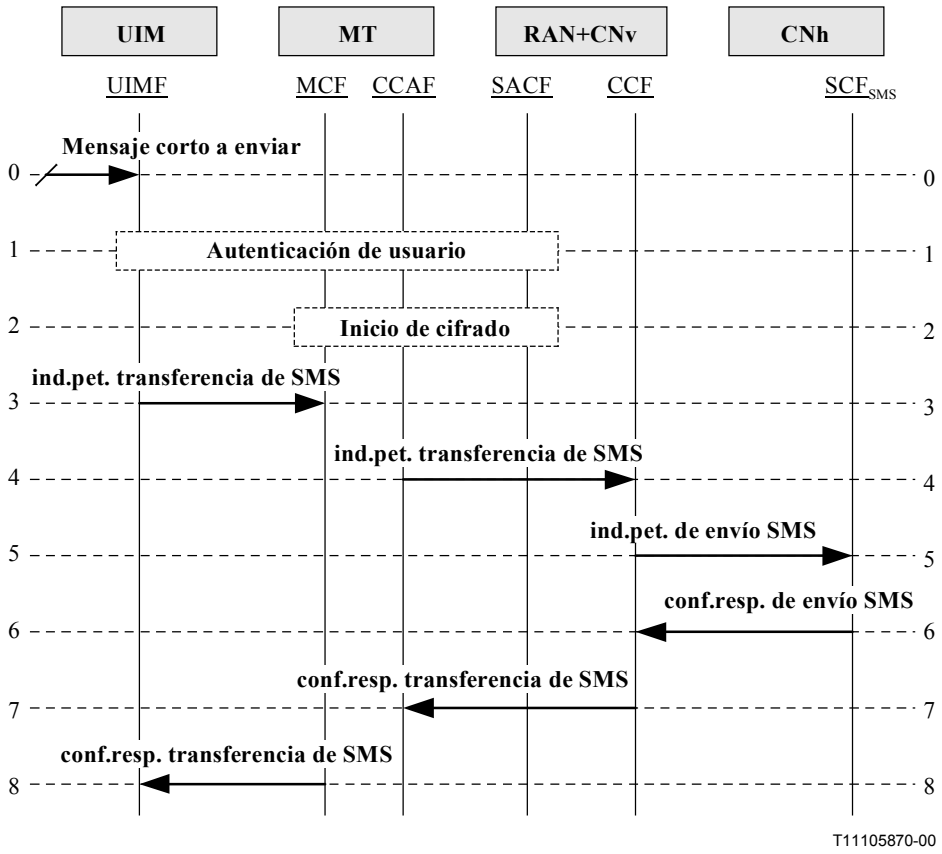


Figura 10.1.2.1-1/Q.1721 – Mensaje corto originado en el móvil (en un canal de tráfico)

0. **Mensaje corto a enviar**: es el estímulo inicial mediante el cual el usuario envía un mensaje corto al MT para que sea enviado a un receptor.

FEA0	– El terminal móvil hace una petición de mensaje corto.

1. **Autenticación de usuario**: facultativamente puede invocarse el procedimiento de autenticación del usuario.

2. **Inicio de cifrado**: facultativamente puede iniciarse el procedimiento de cifrado.

3. **ind.pet. transferencia de SMS**: transfiere el mensaje corto a la MCF.

Transferencia de SMS (Respuesta: éxito)	**ind.pet.**
TMUI o IMUI	M (nota)
Número llamado	M
Dirección del centro de mensajes	M
Mensaje	M

FEA3	– Envía la información a la CCAF.
NOTA – TMUI debe utilizarse si está disponible.	

4. **ind.pet. transferencia de SMS**: se utiliza para enviar el mensaje a la CNv.

Transferencia de SMS (Respuesta: éxito)	ind.pet.
<Los mismos elementos de información que en el flujo de información 3>	<Véase IF 3>

FEA4	– Envía la información al centro de mensajes cortos en la CNh.

5. **ind.pet. de envío SMS**: transfiere el mensaje al centro de mensajes cortos en la CNh.

Envío SMS (Respuesta: éxito)	ind.pet.
<Los mismos elementos de información que en el flujo de información 3>	<Véase IF 3>

FEA5	– Prepara un informe de entrega que se devuelve a la CNv.

6. **conf.resp. de envío SMS**: acuse de recibo del mensaje.

Envío SMS	conf.resp.
Ninguno	(nota)

FEA6	– Envía el informe de entrega a la CCAF.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

7. **conf.resp. transferencia de SMS**: acuse de recibo del mensaje.

Transferencia de SMS	conf.resp.
Ninguno	(nota)

FEA7	– Envía el informe de entrega a la MCF.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

8. **conf.resp. transferencia de SMS**: acuse de recibo del mensaje.

Transferencia de SMS	conf.resp.
Ninguno	(nota)

FEA8	– Informa al abonado sobre si el mensaje se ha entregado con éxito.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

10.1.2.2 Mensaje corto originado en el móvil (en un canal de control)

Véase la figura 10.1.2.2-1.

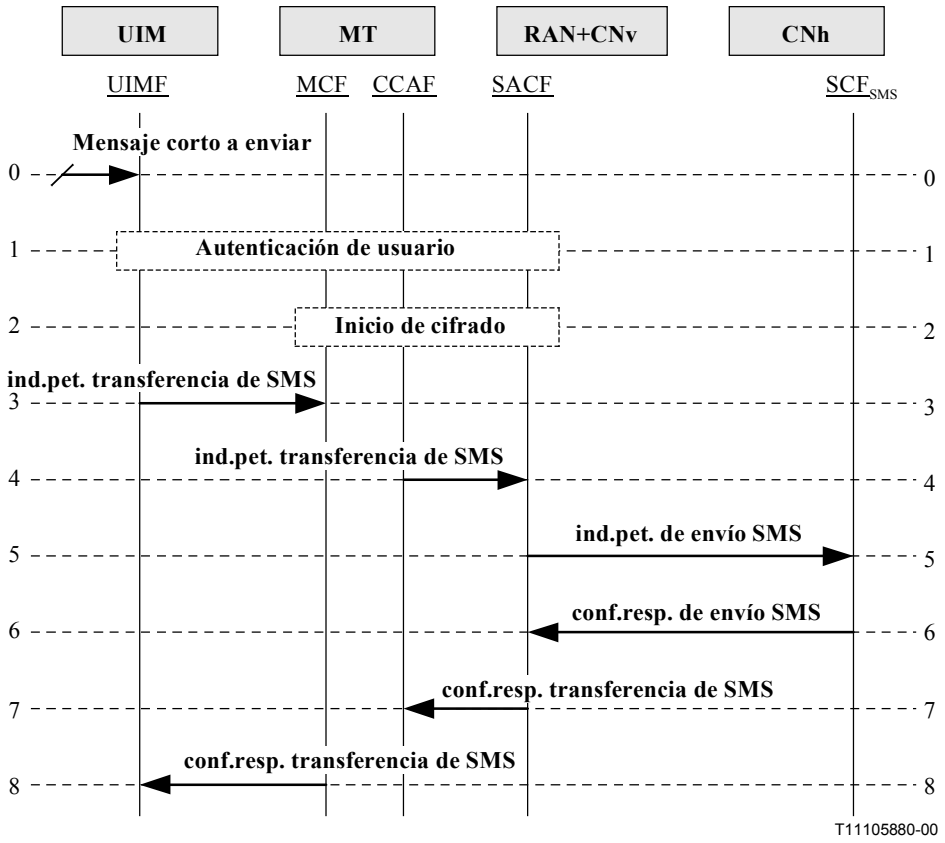


Figura 10.1.2.2-1/Q.1721 – Mensaje corto originado en el móvil (en un canal de control)

0. **Mensaje corto a enviar**: es el estímulo inicial mediante el cual el usuario envía un mensaje corto al MT para que sea enviado a un receptor.

FEA0	– El terminal móvil hace una petición de mensaje corto.

1. **Autenticación de usuario**: facultativamente puede invocarse el procedimiento de autenticación del usuario.

2. **Inicio de cifrado**: facultativamente puede iniciarse el procedimiento de cifrado.

3. **ind.pet. transferencia de SMS**: transfiere el mensaje corto a la MCF.

Transferencia de SMS (Respuesta: éxito)	**ind.pet.**
TMUI o IMUI	M (nota)
Número llamado	M
Dirección del centro de mensajes	M
Mensaje	M

FEA3	– Envía la información a la CCAF.
NOTA – TMUI debe utilizarse si está disponible.	

4. **ind.pet. transferencia de SMS**: se utiliza para enviar el mensaje a la CNv.

Transferencia de SMS (Respuesta: éxito)	ind.pet.
<Los mismos elementos de información que en el flujo de información 3>	<Véase IF 3>

FEA4	– Envía la información al centro de mensajes cortos en la CNh.

5. **ind.pet. de envío SMS**: transfiere el mensaje a la SCF de la CNh.

Envío SMS (Respuesta: éxito)	ind.pet.
<Los mismos elementos de información que en el flujo de información 3>	<Véase IF 3>

FEA5	– Prepara un informe de entrega que se devuelve a la CNv.

6. **conf.resp. de envío SMS**: acusa recibo de la recepción del mensaje.

Envío SMS	conf.resp.
Ninguno	(nota)

FEA6	– Envía el informe de entrega a la CCAF.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

7. **conf.resp. transferencia de SMS**: se ha recibido acuse de recibo del mensaje.

Transferencia de SMS	conf.resp.
Ninguno	(nota)

FEA7	– Envía el informe de entrega a la MCF.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

8. **conf.resp. transferencia de SMS**: acuse de recibo del mensaje.

Transferencia de SMS	conf.resp.
Ninguno	(nota)

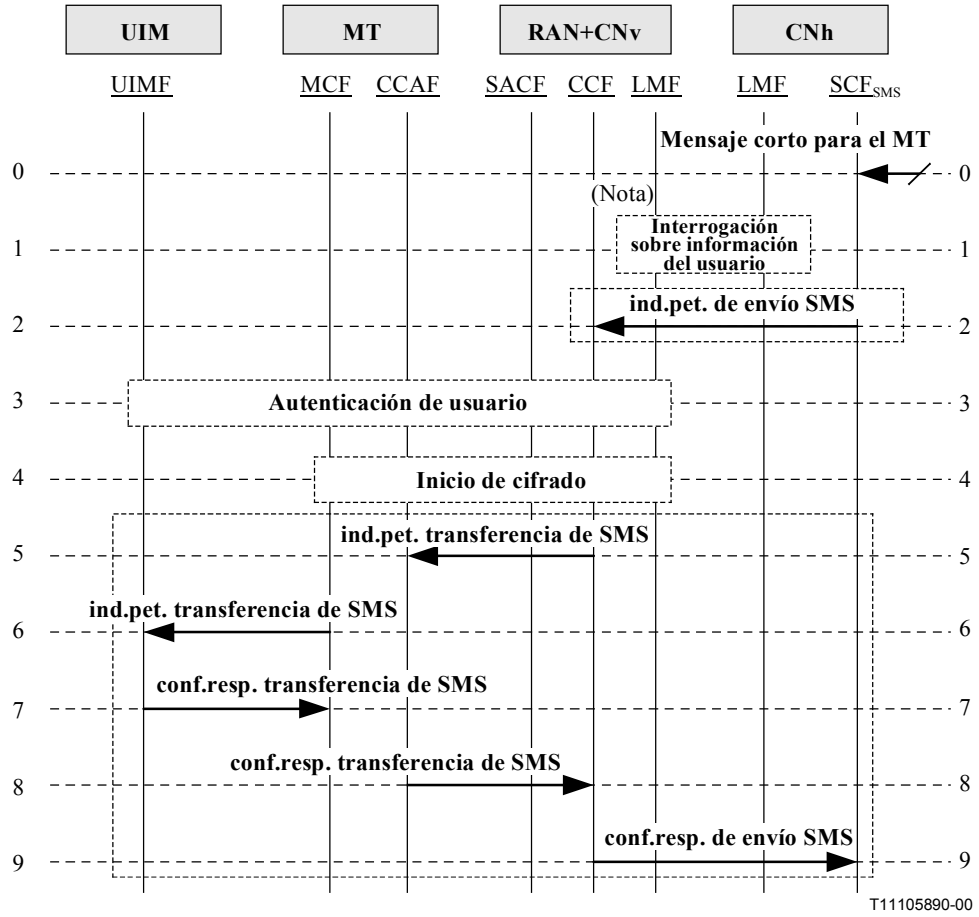
FEA8	– Informa al abonado sobre si el mensaje se ha recibido con éxito.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

10.1.3 Mensaje corto terminado en el móvil

El centro de mensajes envía el mensaje corto a la CCF'/SACF de la red originaria del abonado. La CCF'/SACF interroga a la LMFh para obtener la información de encaminamiento necesaria para enviar el mensaje corto, enviando el mensaje a la CCF'/SACF relevante de la red visitada, haciendo tránsito en otras redes si es necesario. La CCF'/SACF envía entonces el mensaje corto al MT.

10.1.3.1 Mensaje corto terminado en el móvil en un canal de tráfico

Véase la figura 10.1.3.1-1.



NOTA – La SCF$_{SMS}$ puede facultativamente solicitar a la LMFh información de ubicación si se sabe que el móvil puede ser alcanzado y tiene disponible capacidad de memoria. El hecho de que "Interrogación sobre información de usuario" sea facultativa hace que el subsiguiente flujo de información también lo sea.

Figura 10.1.3.1-1/Q.1721 – Mensaje corto terminado en el móvil (en un canal de tráfico)

0. **Mensaje corto para el MT**: se envía un mensaje corto al centro de mensajes del sistema originario de abonado para su entrega al MT del abonado.

FEA0	– Inicia el procedimiento de interrogación de información del usuario para obtener la información necesaria para entregar el mensaje.

1. **Interrogación sobre información del usuario**: la LMFh solicita a la LMFv la ubicación y estado actual del abonado al que está destinado el mensaje corto. La LMFv determina la ubicación y estado actual del MT y responde a la LMFh con dicha información.

2. **ind.pet. de envío SMS**: transfiere el mensaje corto a la CCF identificada en el paso 1.

Envío SMS (Respuesta: éxito)	ind.pet.
IMUI	M
Número llamante	M
Dirección del centro de mensajes	M
Mensaje	M

FEA2	– Transfiere el mensaje a la CCAF del MT.

3. **Autenticación de usuario**: facultativamente puede invocarse el procedimiento de autenticación del usuario.

4. **Inicio de cifrado**: facultativamente puede iniciarse el procedimiento de cifrado.

5. **ind.pet. transferencia de SMS**: transfiere el mensaje corto al terminal móvil.

Transferencia de SMS (Respuesta: éxito)	ind.pet.
<Mismos elementos de información que en el flujo de información 2>	<Véase IF 2>

FEA5	– Envía la información a la MCF.

6. **ind.pet. transferencia de SMS**: transfiere el mensaje al UIM.

Transferencia de SMS (Respuesta: éxito)	ind.pet.
<Mismos elementos de información que en el flujo de información 2>	<Véase IF 2>

FEA6	– Muestra el mensaje corto al usuario o notifica el SM al usuario. – Inicia un informe de entrega que se devuelve a la CNh.

7. **conf.resp. transferencia de SMS**: acusa recibo de la recepción del mensaje.

Transferencia de SMS	conf.resp.
Ninguna	(nota)

FEA7	– Envía el acuse de recibo a la CCAF.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

8. **conf.resp. transferencia de SMS**: se ha recibido acuse de recibo del mensaje.

Transferencia de SMS	conf.resp.
Ninguna	(nota)

FEA8	– Transfiere el acuse de recibo a la SCF de la CNh.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

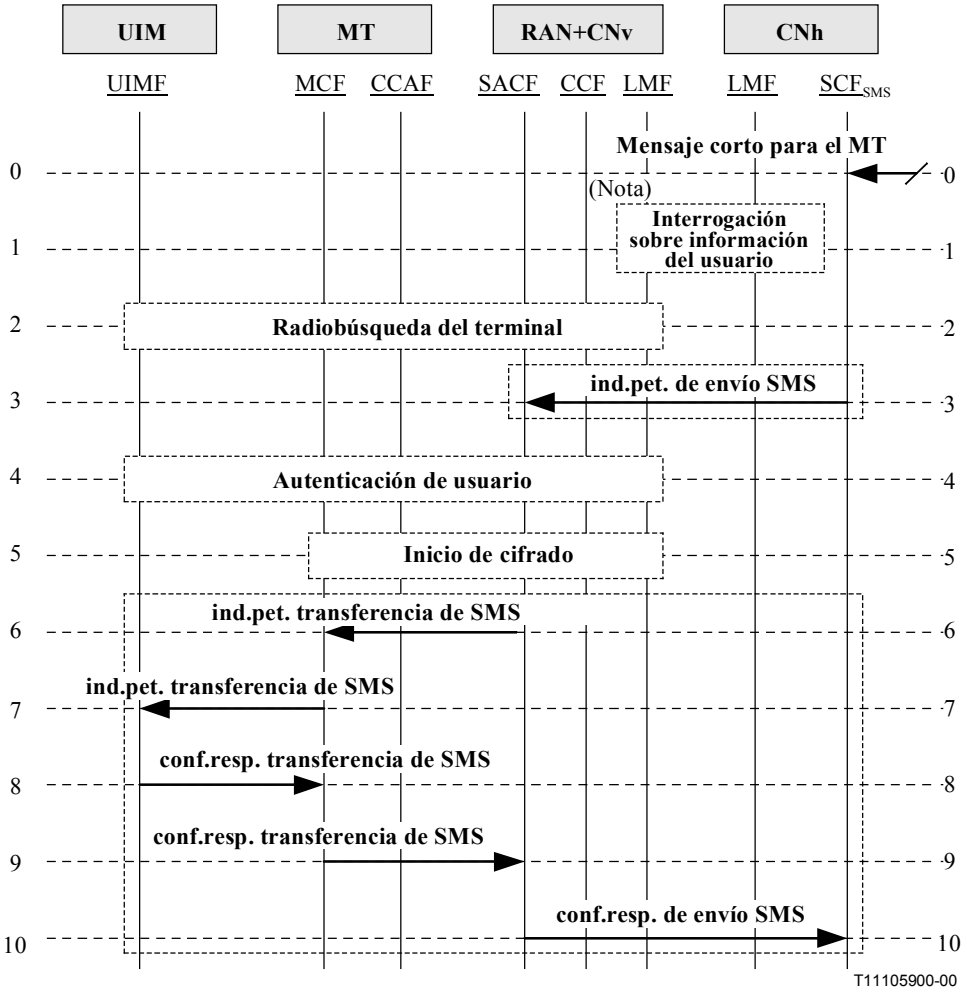
9. **conf.resp. de envío SMS**: acusa recibo de la recepción del mensaje.

Envío SMS	conf.resp.
Ninguna	(nota)

FEA9	– Indica que el mensaje se ha recibido con éxito.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

10.1.3.2 Mensaje corto terminado en un móvil sobre un canal de control

Véase la figura 10.1.3.2-1.



NOTA – La SCF_{SMS} puede facultativamente solicitar a la LMFh información de ubicación si se sabe que el móvil puede ser alcanzado y tiene disponible capacidad de memoria. El hecho de que "Interrogación sobre información de usuario" sea facultativa hace que el subsiguiente flujo de información también lo sea.

Figura 10.1.3.2-1/Q.1721 – Mensaje corto terminado en el móvil (en un canal de control)

0. Mensaje corto para el MT: se envía un mensaje corto al centro de mensajes del sistema originario del abonado para su entrega al MT del abonado.

FEA0	– Inicia el procedimiento de interrogación sobre información del usuario a fin de obtener la información necesaria para entregar el mensaje.

1. **Interrogación sobre información del usuario**: la LMFh solicita a la LMFv la ubicación y estado actual del abonado al que está destinado el mensaje corto. La LMFv determina la ubicación y estado actual del MT y responde a la LMFh con dicha información.

2. **Radiobúsqueda del terminal**: facultativamente, puede realizarse el procedimiento de radiobúsqueda para determinar con más precisión la ubicación del terminal móvil.

3. **ind.pet. de envío SMS**: transfiere el mensaje corto a la SACF de la CNv.

Envío SMS (Respuesta: éxito)	**ind.pet.**
IMUI	M
Número llamante	M
Dirección del centro de mensajes	M
Mensaje	M

FEA3	– Transfiere el mensaje a la MCF del MT.

4. **Autenticación de usuario**: facultativamente puede invocarse el procedimiento de autenticación del usuario.

5. **Inicio de cifrado**: facultativamente puede iniciarse el procedimiento de cifrado.

6. **ind.pet. transferencia de SMS**: transfiere el mensaje al terminal móvil.

Transferencia de SMS (Respuesta: éxito)	**ind.pet.**
<Mismos elementos de información que en el flujo de información 3>	<Véase IF 3>

FEA6	– Envía la información a la UIMF.

7. **ind.pet. transferencia de SMS**: transfiere el mensaje al UIM.

Transferencia de SMS (Respuesta: éxito)	**ind.pet.**
<Mismos elementos de información que en el flujo de información 3>	<Véase IF 3>

FEA7	– Muestra el mensaje corto al usuario o notifica el SM al usuario. – Inicia un informe de entrega que se devuelve a la CNh.

8. **conf.resp. transferencia de SMS**: acusa recibo de la recepción del mensaje.

Transferencia de SMS	conf.resp.
Ninguna	(nota)

FEA8	– Envía el acuse de recibo a la SACF.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

9. **conf.resp. transferencia de SMS**: acusa recibo de la recepción del mensaje.

Transferencia de SMS	conf.resp.
Ninguna	(nota)

FEA9	– Transfiere el acuse de recibo a la SCF de la CNh.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

10. **conf.resp. de envío SMS**: acusa recibo de la recepción del mensaje.

Envío SMS	conf.resp.
Ninguna	(nota)

FEA10	– Indica que el mensaje se ha recibido con éxito.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

10.2 Difusión de mensajes de teleservicios (TMB)

En esta subcláusula se proporcionan los flujos de información para a difusión de mensajes de teleservicios (TMB) que proporciona un método para la gestión y entrega de mensajes de texto de teleservicios para su difusión a través de la interfaz radioeléctrica con terminales móviles IMT-2000. Algunos ejemplos de áreas en las que se utilizan los mensajes de texto de teleservicios son las emergencias, los anuncios administrativos, los avisos, los servicios de suscripción, etc. La difusión puede realizarse sobre una zona predeterminada (es decir, sobre una SACF total o parcial de una CN). La difusión puede realizarse con control de periodicidad basada en el sistema originario o con control de periodicidad basada en el sistema visitado. Existen otros atributos, tales como el idioma de la difusión, la prioridad, etc., que también caracterizan la difusión. La difusión de mensajes de teleservicios se realiza sin acuses de recibo (es decir, no se espera una respuesta del móvil cuando éste recibe un mensaje difundido).

La TMB tiene lugar de forma periódica de una de las formas siguientes:

NOTA – La periodicidad consta de un instante de inicio, una tasa de repetición y una duración.

Opción A: control de periodicidad basada en el sistema visitado – La periodicidad de la difusión de los mensajes de teleservicios está bajo control del sistema visitado. Un "cliente" deposita el mensaje del teleservicio a difundir en el centro de mensajes (la SCF_{SMS} del sistema originario) que lo transfiere a una o varias CNv. Las SACF de la CNv almacenan el mensaje e inician su difusión a intervalos regulares durante un tiempo preestablecido, de acuerdo con la periodicidad especificada. Las SACF de

las CNv almacenan el mensaje hasta que finaliza la difusión (es decir, hasta el final del periodo de difusión). Las SACF pueden restringir prematuramente la difusión del mensaje cuando lo ordene la SCF_{SMS}.

Opción B: control de periodicidad basada en el sistema originario – La periodicidad de la difusión de los mensajes de teleservicios es controlada por el sistema originario. Un "cliente" deposita el mensaje del teleservicio a difundir en el centro de mensajes (la SCF del sistema originario) que lo transfiere a una o varias CNv. Las SACF de las CNv inician inmediatamente su difusión. En este caso las SACF no necesitan almacenar el mensaje. Sin embargo, si el cliente desea difundir el mensaje de nuevo a intervalos regulares y durante algún tiempo, la (SCF_{SMS}) originaria puede reenviar el mensaje a las CNv para ser difundidos de nuevo. En este caso, la SCF_{SMS} de la CNh tiene la responsabilidad de retener el mensaje hasta que finaliza la difusión (es decir, hasta el final del periodo de difusión).

Ambas opciones se ilustran en la figura 10.2-1.

Asimismo, la SCF envía la carga útil de la difusión de mensajes de teleservicios a los IE asociados a todas las SACF de las CNv que forman parte de la zona de difusión predeterminada. Sin embargo, por simplicidad, en la figura 10.2-1 sólo se muestra una SACF.

Típicamente, la opción A se utiliza para difusiones con una elevada tasa de repetición (por ejemplo, cada 2 minutos) durante un periodo corto (por ejemplo, 3 horas).

Típicamente, la opción B se utiliza para difusiones con una baja tasa de repetición (por ejemplo, cada 6 horas) durante un periodo largo (por ejemplo, 7 días).

La opción elegida es una decisión del operador: la opción A tiende a utilizar más recursos del sistema (memoria) mientras que la opción B utiliza más recursos de enlaces de señalización (mayor ocupación).

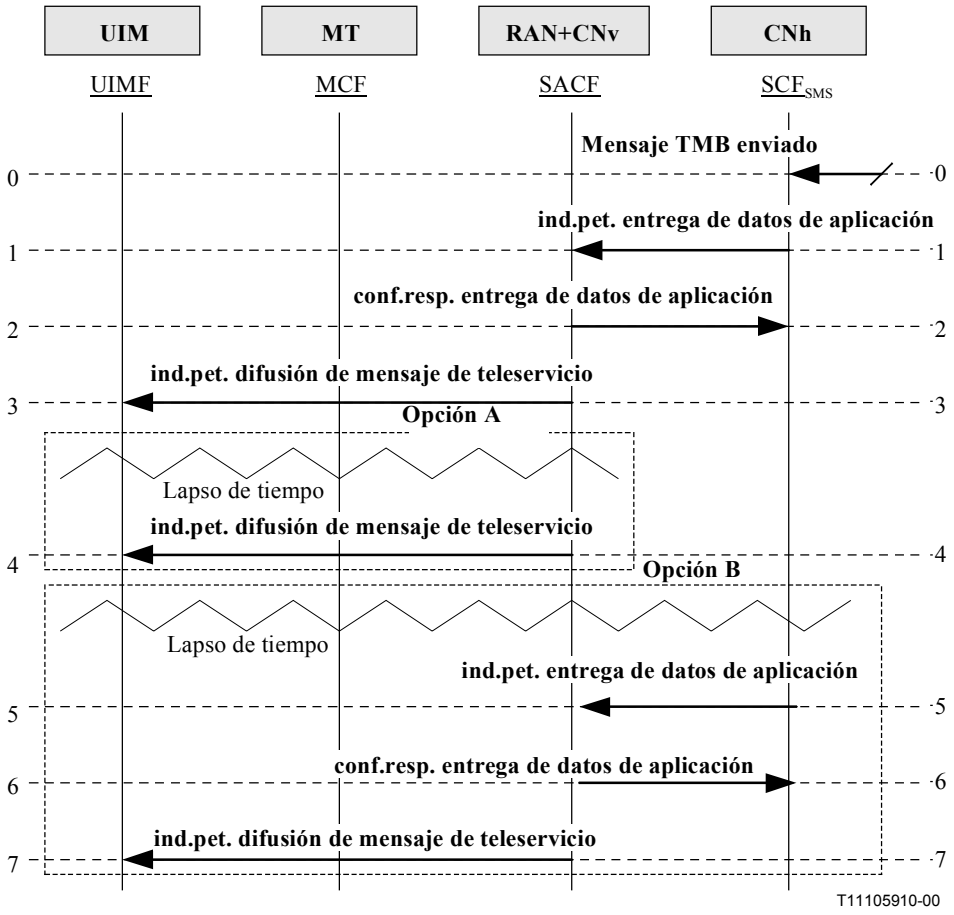


Figura 10.2-1/Q.1721 – Difusión de mensajes de teleservicios

0. Mensaje TMB enviado: es el estímulo inicial mediante el cual un "cliente" envía un mensaje para que sea difundido mediante difusión de mensajes de teleservicios. La petición incluye la carga útil, la dirección del originador, la categoría de difusión, el tipo de mensaje de difusión, el estado del mensaje de difusión, la prioridad del mensaje de difusión, el grupo del servicio de difusión, el identificador de la zona de difusión y el idioma preferido para la difusión.

FEA0	– Inicia la opción A (control de periodicidad basado en el sistema visitado) o la opción B (control de periodicidad basado en el sistema originario) conforme a las peticiones de TMB.

1. **ind.pet. entrega de datos de aplicación**: desde la SCF de la red originaria a todas las SACF que controlan la zona de difusión predeterminada.

Entrega de datos de aplicación (Respuesta: éxito)	**ind.pet.**
Dirección del originador	M
Carga útil	M
Categoría	M
Tipo de mensaje	M
Estado del mensaje	M
Identificador de zona	O (nota 1)
Periodicidad	O (nota 2)
Prioridad del mensaje	O (nota 3)
Grupo de servicio	O (nota 4)
Idioma preferido	O (nota 5)

FEA1	– Acusa recibo de la petición de entrega de datos de aplicación. – Se inicia para el envío de difusión de mensajes de teleservicios a la red visitada.
NOTA 1 – Especifica zonas de difusión específicas. La ausencia de este IE significa que la difusión es sobre toda la SACF. NOTA 2 – Para el control de la periodicidad basado en el sistema visitado; si está ausente el mensaje sólo se envía una vez. NOTA 3 – Indica difusión normal (por defecto), interactiva, urgente o de emergencia. NOTA 4 – Indica la audiencia objetivo del MT (definida por el operador). NOTA 5 – Indica el idioma en el que está escrito el mensaje. Se utiliza como filtro.	

2. **conf.resp. entrega de datos de aplicación**: acusa recibo de la recepción de peticiones de entrega de datos de aplicación.

Entrega de datos de aplicación	**conf.resp.**
Ninguno	(nota)

FEA2	– Si se elige la opción A no se necesita acción alguna. – Si se elige la opción B espera el vencimiento del temporizador.
NOTA – La confirmación de respuesta está vacía. Su sola presencia basta para indicar éxito.	

3. **ind.pet. difusión de mensaje de teleservicio**: pasa el mensaje a la UIMF.

Difusión de mensaje de teleservicio (Respuesta: ninguna)	ind.pet.
Dirección del originador	M
Carga útil	M
Categoría	M
Tipo de mensaje	M
Estado del mensaje	M
Prioridad del mensaje	O (nota 1)
Grupo de servicio	O (nota 2)
Idioma preferido	O (nota 3)

FEA3	– Muestra el mensaje al usuario conforme a los parámetros recibidos.
NOTA 1 – Indica difusión normal (por defecto), interactiva, urgente o de emergencia.	
NOTA 2 – Indica la audiencia objetivo del MT (definida por el operador).	
NOTA 3 – Indica el idioma en el que está escrito el mensaje. Se utiliza como filtro.	

El paso 4 es una repetición del flujo de información 3, y sólo se aplica al caso de la opción A, en el que el sistema visitado controla la periodicidad. Los IE y la FEA es la misma que en el flujo de información 3. Este paso se repite conforme a la periodicidad prescrita.

Los pasos 5, 6 y 7 son los mismos que los flujos de información 1, 2 y 3 excepto en que la periodicidad no se incluye en el flujo de información 5. Sólo se aplican en el caso de la opción B en la que el sistema originario controla la periodicidad. Estos pasos se repiten de acuerdo con la periodicidad prescrita.

10.3 Notificación de mensaje en espera (MWN)

10.3.1 Flujos de información de MWN

Este escenario muestra el flujo de información relacionado con la notificación de mensaje en espera (MWN, *message waiting notification*) para sistemas IMT-2000 en una situación de itinerancia global. La notificación de mensaje en espera es una característica por la que se notifica a los abonados suscritos si se han depositado en sus sistemas de mensajería mensajes de voz, facsímil, correo electrónico o de otro tipo que pueden ser recuperados. Véase la figura 10.3.1-1.

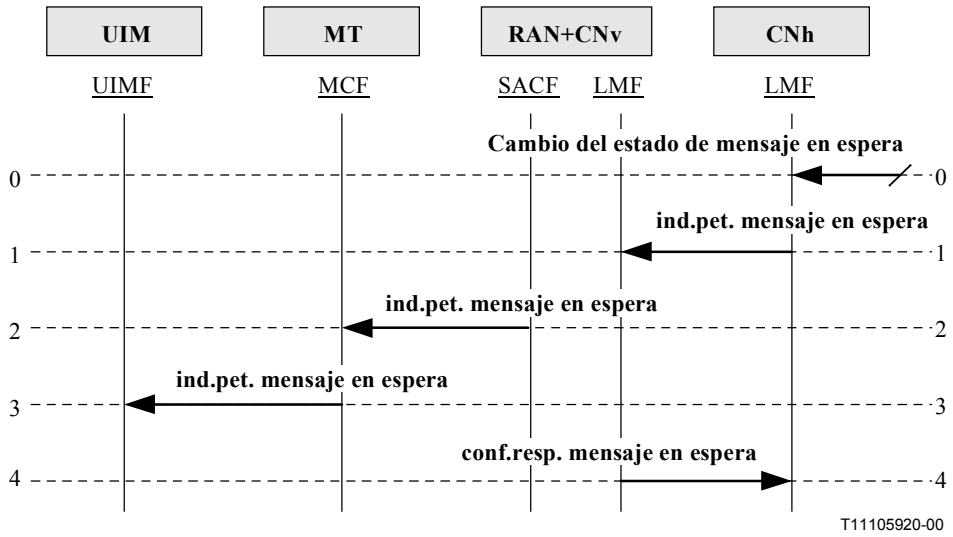


Figura 10.3.1-1/Q.1721 – Notificación de mensaje en espera

0. **Cambio del estado de mensaje en espera**: es el estímulo inicial por el que un sistema de mensajería, facsímil, servidor de correo electrónico o similar, informa de un cambio en el estado de los mensajes de voz, facsímil, correo electrónico o de otro tipo del MT a la LMFh.

FEA0	– Cambia el estado del mensaje en espera.

1. **ind.pet. mensaje en espera**: para cada tipo de mensajes (voz, facsímil, correo electrónico, etc.,) se envía una ind.pet. independiente. Alternativamente, y mediante parámetros del constructor, pueden agruparse y enviarse en una única ind.pet. informaciones de más de un tipo de mensaje. Este escenario ilustra el primer mecanismo.

Mensaje en espera (Respuesta: éxito)	**ind.pet.**
IMUI	M
Indicador de mensaje en espera	M (nota 1)
Tipo de mensaje en espera	O (nota 2)
Prioridad del mensaje	O (nota 3)
Cómputo de mensajes pendientes	O (nota 4)
Idioma preferido	O (nota 5)

FEA1	– Retransmite los contenidos a la SACF, de forma que puedan ser enviados a la MCF.
NOTA 1 – Pueden tener los valores "Sí" o "No".	
NOTA 2 – Indica si los mensajes son de voz, facsímil, correo electrónico u otros.	
NOTA 3 – Indica difusión normal (por defecto), interactiva, urgente o difusión de emergencia.	
NOTA 4 – Indica el número de mensajes pendientes.	
NOTA 5 – Indica el idioma a utilizar si se hace un anuncio.	

2. **ind.pet. mensaje en espera**: transfiere a la MCF información sobre los mensajes en espera.

Mensaje en espera (Respuesta: éxito)	ind.pet.
<Mismos elementos de información que en el flujo de información 1>	<Véase IF 1>

FEA2	– Retransmite el contenido a la UIMF.

3. **ind.pet. mensaje en espera**: transfiere a la UIMF los mensajes que están a la espera de notificación.

Notificación de mensaje en espera (Respuesta: éxito)	ind.pet.
<Mismos elementos de información que en el flujo de información 1>	<Véase IF 1>

FEA3	– Utiliza la información recibida para proporcionar al usuario el tipo especificado de notificación.

4. **conf.resp. mensaje en espera**: acuse de recibo de la notificación de mensaje en espera.

Notificación de mensaje en espera	conf.resp.
Ninguno	(nota)

FEA6	– No se requiere acción alguna.
NOTA – La confirmación de respuesta está vacía. Su sola presencia basta para indicar éxito.	

11 Procedimientos relativos a los servicios suplementarios

Las características siguientes pueden no ser aplicables a todos los miembros de la familia IMT-2000.

Los procedimientos autónomos siguientes se utilizan para controlar los servicios suplementarios (SS, *supplementary services*) de un usuario. Son iniciados por el usuario[7], normalmente pulsando una tecla del terminal móvil.

A continuación se describen los siguientes procedimientos de servicios suplementarios:

– Obtención de contraseña.
– Registro de contraseña.
– Registro de SS.
– Supresión de SS.
– Activación de SS.
– Desactivación de SS.
– Interrogación de SS.
– Invocación de SS.

[7] Los procedimientos "obtención de contraseña" y "notificación de servicio suplementario no estructurado" son iniciados por el HLR (LMFh) pero se desencadenan por efecto de otros procedimientos de control de servicios suplementarios iniciados por el usuario.

– Procesamiento de petición de SS no estructurado.
– Petición de SS no estructurado.
– Notificación de SS no estructurado.
– Notificación de invocación de SS.

11.1 Obtención de contraseña

La red originaria inicia este procedimiento para solicitar una contraseña del usuario cuando la red originaria recibe una petición del usuario para una operación de control de servicio suplementario que necesita una contraseña. Este procedimiento puede utilizarse conjuntamente con cualquiera de los procedimientos de control de servicios suplementarios, pero no se muestra de forma explícita en todos ellos. Véase la figura 11.1-1.

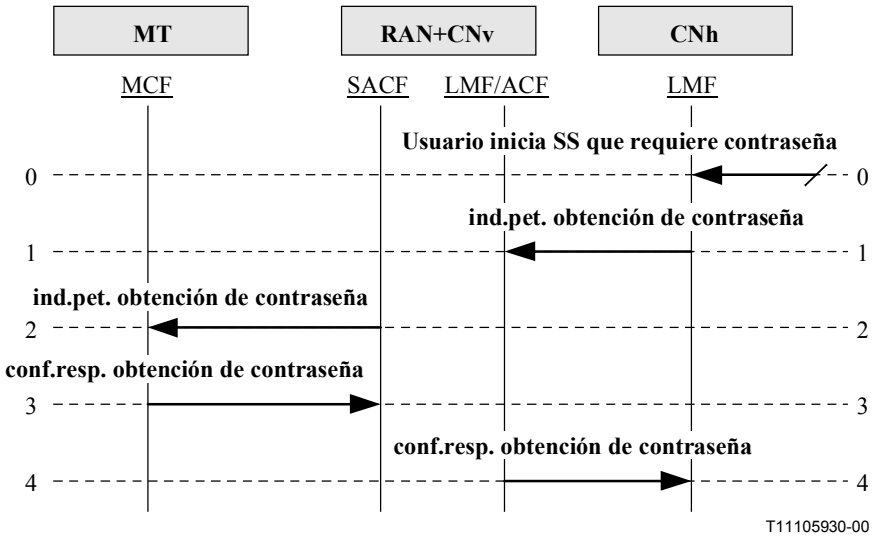


Figura 11.1-1/Q.1721 – Obtención de contraseña

0. **Usuario inicia SS que requiere contraseña**: la LMFh recibe un SS iniciado por el usuario que requiere una contraseña.

FEA0	– Detecta la necesidad de que el usuario solicite una contraseña en respuesta a un procedimiento de SS iniciado. – Prepara y envía una ind.pet. obtención de contraseña a la LMF de la red visitada.

1. **ind.pet. obtención de contraseña**: utilizada para pedir al usuario que facilite una contraseña.

Obtención de contraseña (Respuesta: éxito o fracaso)	ind.pet.
Información de orientación	M

FEA1	– Retransmite a la SACF la ind.pet. obtención de contraseña.

2. **ind.pet. obtención de contraseña**: utilizada para pedir al usuario que facilite una contraseña a través del MMI.

Obtención de contraseña (Respuesta: éxito o fracaso)	ind.pet.
Información de orientación	M

FEA2	– Interpreta el elemento de información de orientación y muestra la información relevante al usuario a través de la interfaz hombre-máquina (MMI). – Recibe la contraseña del usuario a través de la MMI. – Prepara y envía una conf.resp. obtención de contraseña a la SACF, posiblemente utilizando varios mensajes, por ejemplo, para la emulación de DTMF.

3. **conf.resp. obtención de contraseña**: envía la contraseña y resultado actuales a la SACF.

Obtención de contraseña	conf.resp.
Contraseña vigente	M
Resultado	M

FEA3	– Retransmite a la LMFv la conf.resp. obtención de contraseña. – Prepara y envía a la LMFh una conf.resp. obtención de contraseña, posiblemente utilizando varios mensajes, por ejemplo, para la emulación de DTMF.

4. **conf.resp. obtención de contraseña**: envía la contraseña y resultado actuales a la LMFh.

Obtención de contraseña	conf.resp.
Contraseña vigente	M
Resultado	M

FEA4	– Contraseña confirmada revisada.

11.2 Registro de contraseña

La red originaria inicia este procedimiento para pedir la contraseña anterior del usuario. Cuando la red originaria recibe la contraseña antigua envía una petición al usuario solicitando la nueva contraseña. La red originaria solicita al usuario que vuelva a confirmar una vez más la nueva contraseña. Véase la figura 11.2-1.

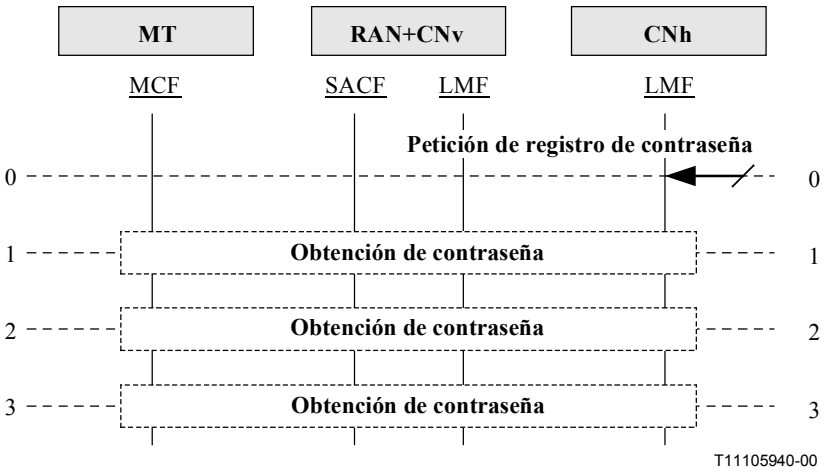


Figura 11.2-1/Q.1721 – Registro de contraseña

0. **Petición de registro de contraseña**: el usuario solicita el cambio de contraseña para un servicio suplementario.

1. **Obtención de contraseña**: la LMFh pide al usuario la contraseña antigua.

2. **Obtención de contraseña**: la LMFh pide al usuario la nueva contraseña.

3. **Obtención de contraseña**: la LMFh pide al usuario que, a fin de confirmarla, introduzca una vez más la nueva contraseña.

11.3 Registro del SS

Este procedimiento se utiliza para registrar los datos relacionados con un servicio suplementario en la red originaria. Véase la figura 11.3-1.

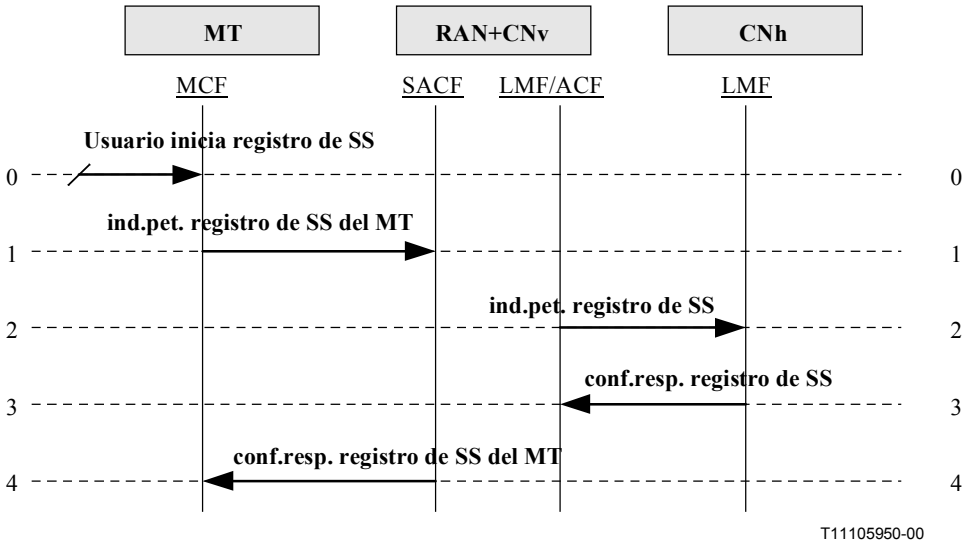


Figura 11.3-1/Q.1721 – Registro de SS

0. **Usuario inicia registro de SS**: la MCF recibe un registro de SS iniciado por un usuario.

FEA0	– Detecta el procedimiento de control de SS iniciado por usuario a través de la MMI para solicitar el registro de un servicio suplementario. – Prepara y envía la información recibida a la SACF.

1. **ind.pet. registro de SS del MT**: se utiliza para solicitar el registro de un servicio suplementario.

Registro SS del MT (Respuesta: éxito o fracaso)	**ind.pet.**
Código de SS	M
Datos de SS	M

FEA1	– Prepara y envía a la LMFv la ind.pet. registro de SS.

2. **ind.pet. registro de SS**: utilizado para pedir que la LMFh registre un servicio suplementario.

Registro de SS del MT (Respuesta: éxito o fracaso)	**ind.pet.**
Código de SS	M
Datos de SS	M

FEA2	– Identifica el servicio suplementario en cuestión. – Almacena los datos de SS recibidos conforme a la instrucción. – Prepara y envía a la LMFv una conf.resp. registro de SS.

3. **conf.resp. registro de SS**: se utiliza para devolver una respuesta al usuario acerca del resultado del registro.

Registro de SS (Respuesta: éxito o fracaso)	**conf.resp.**
Resultado	M

FEA3	– Retransmite la información a la SACF. – Prepara y envía conf.resp. registro SS del MT desde la SACF.

4. **conf.resp. registro de SS del MT**: envía al usuario el resultado del servicio suplementario.

Registro de SS del MT	**conf.resp.**
Resultado	M

FEA4	– Acusa recibo al usuario de que los datos relativos al servicio suplementario se han almacenado en la LMFh.

11.4 Supresión de SS

El usuario inicia este procedimiento para suprimir información almacenada en relación con un servicio determinado mediante un registro previo en la red originaria. Véase la figura 11.4-1.

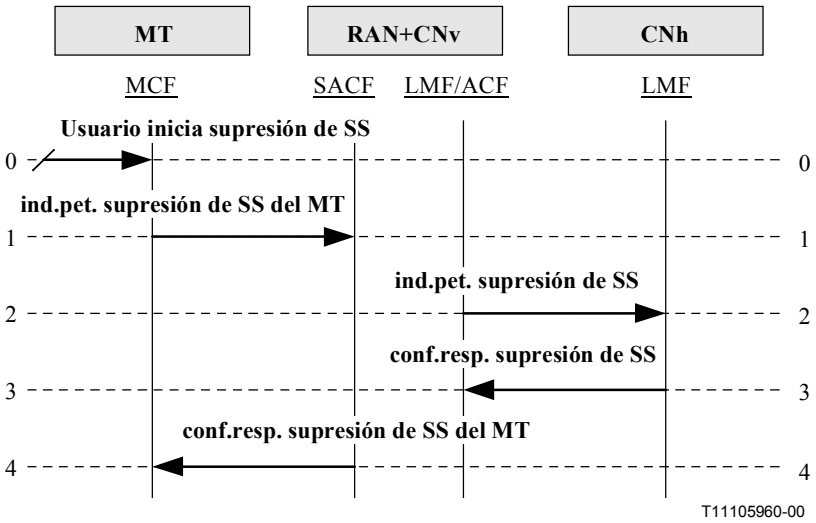


Figura 11.4-1/Q.1721 – Supresión de SS

0. **Usuario inicia supresión de SS**: la MCF recibe una supresión de SS iniciada por un usuario.

FEA0	– Detecta el procedimiento de control de SS iniciado por usuario a través de la MMI para solicitar la supresión de un servicio suplementario. – Prepara y envía a la SACF la información recibida.

1. **ind.pet. supresión de SS del MT**: utilizado para pedir la supresión de un servicio suplementario.

Supresión de SS del MT (Respuesta: éxito o fracaso)	**ind.pet.**
Código de SS	M
Datos de SS	O (nota)

FEA1	– Petición de supresión de datos de SS.
NOTA – Solamente se solicita para aquellos servicios suplementarios que tienen datos.	

2. **ind.pet. supresión de SS**: utilizado para pedir a la LMFh que suprima un servicio suplementario.

Supresión de SS (Respuesta: éxito o fracaso)	ind.pet.
Código de SS	M
Datos de SS	O (nota)

FEA2	– Identifica el servicio suplementario concernido. – Suprime los datos del SS conforme a la instrucción.
NOTA – Solamente se solicita para aquellos servicios suplementarios que tienen datos.	

3. **conf.resp. supresión de SS**: utilizado para devolver respuesta al usuario para informar del resultado de la supresión.

Supresión de SS (Respuesta: éxito o fracaso)	conf.resp.
Resultado	M

FEA3	– Retransmite la información a la SACF.

4. **conf.resp. supresión de SS del MT**: envía al usuario el resultado de la supresión del servicio suplementario.

Supresión de SS del MT	conf.resp.
Resultado	M

FEA4	– No se requiere actuación alguna.

11.5 Activación de SS

Este procedimiento se utiliza para permitir que el proceso se realice cuando y como sea solicitado por el servicio concernido, dando lugar a la fase activa. Algunos servicios pueden estar "operativos" o "quiescentes" (no operativos) durante la fase activa en función de si el sistema puede invocar o utilizar el servicio. La información se almacena en la red originaria y para algunos servicios relevantes también se almacena en la red servidora. Véase la figura 11.5-1.

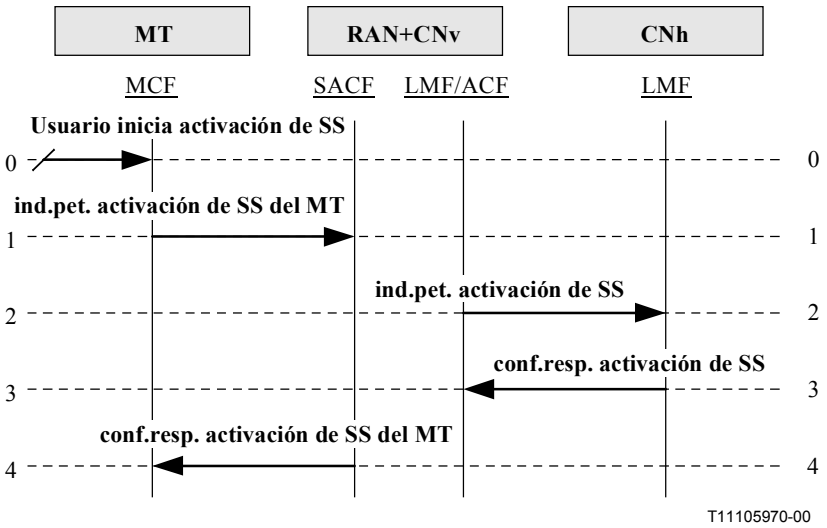


Figura 11.5-1/Q.1721 – Activación de SS

0. **Usuario inicia activación de SS**: la MCF recibe una activación de SS iniciada por un usuario.

FEA0	– Detecta el procedimiento de control de SS iniciado por usuario a través de la MMI para solicitar la activación de un servicio suplementario. – Prepara y envía a la SACF la información recibida.

1. **ind.pet. activación de SS del MT**: utilizado para pedir la activación de un servicio suplementario.

Activación SS del MT (Respuesta: éxito o fracaso)	**ind.pet.**
Código de SS	M
Datos de SS	O (nota)

FEA1	– Petición de activación de datos de SS.
NOTA – Solamente se solicita para aquellos servicios suplementarios que tienen datos.	

2. **ind.pet. activación de SS**: utilizado para pedir a la LMFh que active un servicio suplementario.

Activación de SS (Respuesta: éxito o fracaso)	**ind.pet.**
Código de SS	M
Datos de SS	O (nota)

FEA2	– Identifica el servicio suplementario concernido. – Activa los datos del SS conforme a la instrucción.
NOTA – Solamente se solicitan aquellos servicios suplementarios que tienen datos.	

3. **conf.resp. activación de SS**: utilizado para devolver respuesta al usuario para informar sobre el resultado de la activación.

Activación de SS (Respuesta: éxito o fracaso)	conf.resp.
Resultado	M

FEA3	– Retransmite la información a la SACF.

4. **conf.resp. activación de SS del MT**: envía al usuario el resultado de la activación del servicio suplementario.

Activación de SS del MT	conf.resp.
Resultado	M

FEA4	– No se requiere actuación alguna.

11.6 Desactivación de SS

El usuario inicia este procedimiento para terminar el proceso iniciado en la activación. La información se almacena en la red originaria y para algunos servicios relevantes se almacena también en la red servidora. Véase la figura 11.6-1.

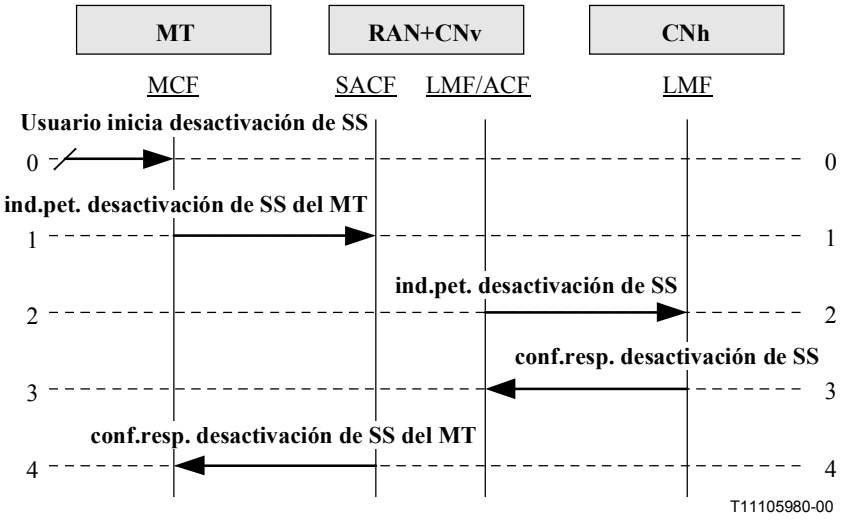


Figura 11.6-1/Q.1721 – Desactivación de SS

0. **Usuario inicia desactivación de SS**: la MCF recibe una desactivación de SS iniciada por un usuario.

FEA0	– Detecta el procedimiento de control de SS iniciado por usuario a través de la MMI para solicitar la desactivación de un servicio suplementario. – Prepara y envía a la SACF la información recibida.

1. **ind.pet. desactivación de SS del MT**: utilizado para pedir la desactivación de un servicio suplementario.

Desactivación de SS del MT (Respuesta: éxito o fracaso)	ind.pet.
Código de SS	M
Datos de SS	O (nota)

FEA1	– Petición de desactivación de datos de SS.
NOTA – Solamente se solicita para aquellos servicios suplementarios que tienen datos.	

2. **ind.pet. desactivación de SS**: utilizado para pedir a la LMFh que desactive un servicio suplementario.

Desactivación de SS (Respuesta: éxito o fracaso)	ind.pet.
Código de SS	M
Datos de SS	O (nota)

FEA2	– Identifica el servicio suplementario concernido. – Desactiva los datos del SS conforme a la instrucción.
NOTA – Solamente se solicita para aquellos servicios suplementarios que tienen datos.	

3. **conf.resp. desactivación de SS**: utilizado para devolver respuesta al usuario para informar sobre el resultado de la desactivación.

Desactivación de SS (Respuesta: éxito o fracaso)	conf.resp.
Resultado	M

FEA3	– Retransmite la información a la SACF.

4. **conf.resp. desactivación de SS del MT**: envía al usuario el resultado de la desactivación del servicio suplementario.

Desactivación SS del MT	conf.resp.
Resultado	M

FEA4	– No se requiere actuación alguna.

11.7 Interrogación de SS

El usuario inicia este proceso para proporcionar información sobre un servicio suplementario específico. La información se captura de la red originaria. Véase la figura 11.7-1.

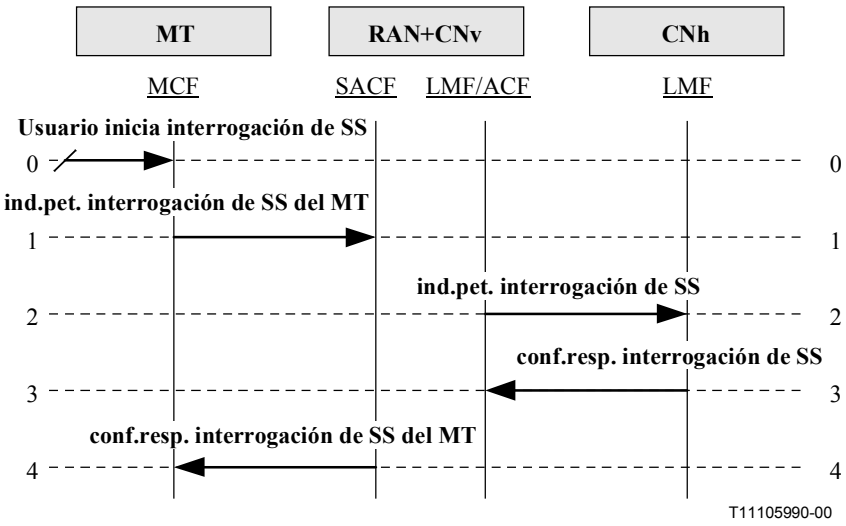


Figura 11.7-1/Q.1721 – Interrogación de SS

0. **Usuario inicia interrogación de SS**: la MCF recibe una interrogación de SS iniciada por un usuario.

FEA0	– Detecta el procedimiento de control de SS iniciado por usuario a través de la MMI para solicitar una interrogación de un servicio suplementario. – Prepara y envía a la SACF la información recibida.

1. **ind.pet. interrogación de SS del MT**: utilizado para pedir recuperar información relativa a un servicio suplementario.

Interrogación SS del MT (Respuesta: éxito o fracaso)	**ind.pet.**
Código de SS	M
Datos de SS	O (nota)

FEA1	– Petición de interrogación de datos de SS.
NOTA – Solamente se solicita para aquellos servicios suplementarios que tienen datos.	

2. **ind.pet. interrogación de SS**: utilizado para hacer una petición a la LMFh en caso de que sea necesario recuperar información relacionada con un servicio suplementario.

Interrogación de SS (Respuesta: éxito o fracaso)	**ind.pet.**
Código de SS	M
Datos de SS	O (nota)

FEA2	– Identifica el servicio suplementario concernido. – Interroga sobre datos de SS conforme a la instrucción.
NOTA – Solamente se solicita para aquellos servicios suplementarios que tienen datos.	

3. **conf.resp. interrogación de SS**: utilizado para devolver respuesta al usuario para informar sobre el resultado de la interrogación.

Interrogación de SS (Respuesta: éxito o fracaso)	conf.resp.
Resultado	M

FEA3	– Retransmite la información a la SACF.

4. **conf.resp. interrogación de SS del MT**: envía al usuario el resultado de la información recuperada del servicio suplementario.

Interrogación de SS del MT	conf.resp.
Resultado	M

FEA4	– No se requiere actuación alguna.

11.8 Invocación de SS

Es un procedimiento iniciado por el usuario. Tiene por objetivo verificar la suscripción del abonado a un servicio suplementario dado en la red servidora. Véase la figura 11.8-1.

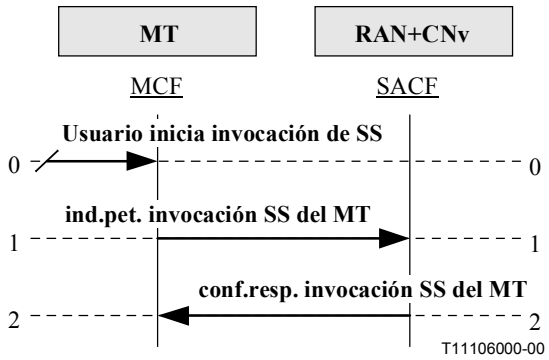


Figura 11.8-1/Q.1721 – Invocación de SS

0. **Usuario inicia invocación de SS**: la MCF recibe una invocación de SS iniciada por un usuario.

FEA0	– Detecta el procedimiento de control de SS iniciado por usuario a través de la MMI para solicitar la invocación de un servicio suplementario. – Prepara y envía a la SACF la información recibida.

1. **ind.pet. invocación SS del MT**: utilizado para solicitar que se verifique la suscripción de un abonado a un servicio suplementario dado (por ejemplo, retención de llamada o llamada multipartita) en la LMFv, en relación con la invocación de dicho servicio suplementario durante la llamada , es decir, después de terminar la fase de establecimiento.

Invocación SS del MT (Respuesta: éxito o fracaso)	ind.pet.
Código de SS	M
Datos de SS	O (nota)

FEA1	– Identifica el servicio suplementario concernido. – Verifica la suscripción del abonado de acuerdo con la información recibida. – Prepara y envía la información a la SACF.
NOTA – Solamente se solicita para aquellos servicios suplementarios que tienen datos.	

2. **conf.resp. invocación SS del MT**: envía al usuario el resultado de la verificación de la información de suscripción del abonado al servicio suplementario.

Invocación SS del MT	conf.resp.
Resultado	M

FEA2	– Presenta el resultado para el usuario.

11.9 Petición de procesamiento de SS no estructurados

Este procedimiento se utiliza para retransmitir información destinada a permitir el funcionamiento de servicios suplementarios no estructurados. La entidad de red receptora pasa los datos recibidos en la petición a la aplicación que maneja la aplicación del servicios suplementarios no estructurados y espera la respuesta de misma. Véase la figura 11.9-1.

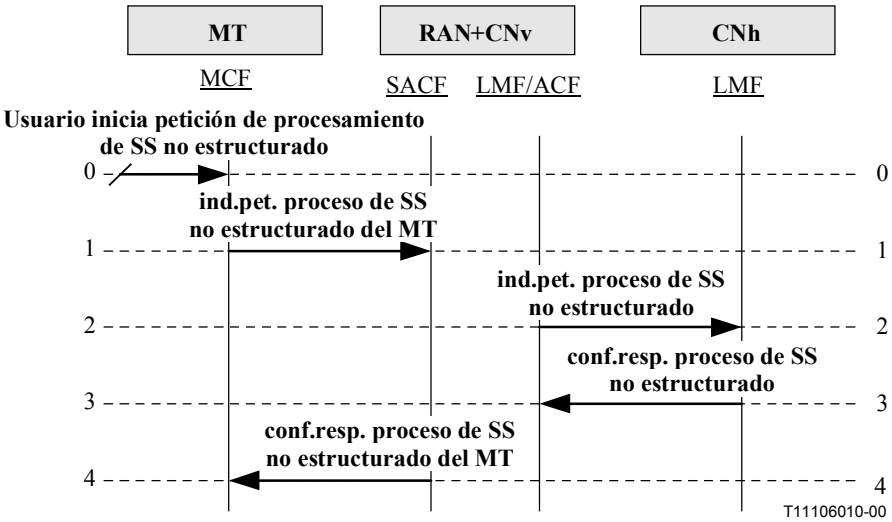


Figura 11.9-1/Q.1721 – Petición de procesamiento de SS no estructurado

0. **Usuario inicia petición de procesamiento de SS no estructurado**: la MCF recibe una petición iniciada por el usuario de procesamiento de SS no estructurados.

FEA0	– Detecta el procedimiento de control de SS iniciado por el usuario a través de la MMI para solicitar una petición no estructurada de procesamiento de un servicio suplementario. – Prepara y envía a la SACF la información recibida.

1. **ind.pet. proceso de SS no estructurado del MT**: es utilizado para solicitar que se permita el funcionamiento de servicios suplementarios no estructurados.

Proceso de SS no estructurado del MT (Respuesta: éxito o fracaso)	**ind.pet.**
Esquema de codificación de datos de servicio suplementario no estructurado (USSD)	M
Cadena USSD	M

FEA1	– Petición para procesar datos de SS no estructurado.

2. **ind.pet. proceso de SS no estructurados**: se utiliza para pedir a la LMFh que procese la petición de USSD.

Proceso de SS no estructurado (Respuesta: éxito o fracaso)	**ind.pet.**
Esquema de codificación de datos USSD	M
Cadena USSD	M

FEA2	– Realiza una o más de las funciones siguientes según precise la lógica del servicio. – Establece o libera canales voz. – Pasa la petición a otra entidad de red (no modificada o modificada). – Pasa una petición de USSD distinta a otra entidad de red. – Solicita información adicional del usuario.

3. **conf.resp. proceso de SS no estructurado**: se utiliza para enviar una respuesta al usuario a fin de informar sobre el resultado de la petición de procesamiento de SS no estructurados.

Proceso de SS no estructurado (Respuesta: éxito o fracaso)	**conf.resp.**
Esquema de codificación de datos USSD	O (nota 1)
Cadena USSD	O (nota 2)
Resultado	O (nota 3)

FEA3	Retransmite la información a la SACF.
NOTA 1 – Si este IE está presente, el IE cadena USSD debe estarlo también. NOTA 2 – Si este IE está presente, el IE esquema de codificación de datos USSD debe estarlo también. NOTA 3 – Sólo se utiliza si se produce una situación de error.	

4. **conf.resp. proceso de SS no estructurado del MT**: envía al usuario el resultado de la información recuperada del servicio suplementario.

Proceso de SS no estructurado del MT	conf.resp.
Esquema de codificación de datos USSD	O (nota 1)
Cadena USSD	O (nota 2)
Resultado	O (nota 3)

FEA4	– Confirmación de la autorización para el funcionamiento de servicios suplementarios no estructurados.
NOTA 1 – Si este IE está presente, el IE cadena USSD debe estarlo también.	
NOTA 2 – Si este IE está presente, el IE esquema de codificación de datos USSD debe estarlo también.	
NOTA 3 – Sólo se utiliza si se produce una situación de error.	

11.10 Petición de SS no estructurados

La entidad invocadora utiliza este procedimiento cuando necesita información del usuario móvil en relación con el manejo de servicios suplementarios no estructurados.

En algunas circunstancias la SCFh puede generar (o recibir) una petición de SS no estructurado hacia (o desde) la LMFh. Es probable que esto ocurra cuando un servicio específico de un operador, proporcionado por la SCF originaria, necesita establecer un diálogo con un usuario móvil. Dicho diálogo puede ser iniciado por el usuario o por la SCF. Los datos de servicios suplementarios no estructurados proporcionan un mecanismo de transporte transparente que permite que tenga lugar dicho diálogo entre el servicio y el usuario. Véase la figura 11.10-1.

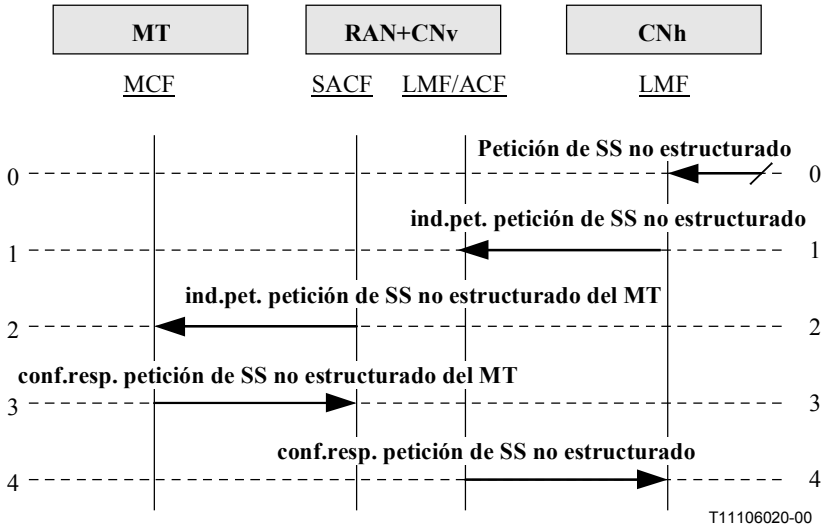


Figura 11.10-1/Q.1721 – Petición de SS no estructurado

0. **Petición de SS no estructurado**: la entidad que invoca necesita información del usuario móvil.

FEA0	– Prepara y envía a la LMFv la ind.pet. petición SS no estructurado.

1. **ind.pet. petición de SS no estructurado**: utilizada para solicitar información del usuario móvil.

Petición de SS no estructurado (Respuesta: éxito o fracaso)	ind.pet.
Esquema de codificación de datos USSD	M
Cadena USSD	M
Modelo de alerta	O (nota)

FEA1	– Prepara y envía a la SACF una ind.pet. petición SS no estructurados.
NOTA – Está presente si se recibe de la SCFh en una operación de conexión, si no es así, está ausente.	

2. **ind.pet. petición de SS no estructurado del MT**: utilizado para preguntar al usuario móvil.

Petición de SS no estructurado (Respuesta: éxito o fracaso)	ind.pet.
Esquema de codificación de datos USSD	M
Cadena USSD	M
Modelo de alerta	O (nota)

FEA2	– Prepara y envía a la SACF una conf.resp. petición SS no estructurado del MT.
NOTA – Está presente si se recibe de la SCFh en una operación de conexión, si no es así, está ausente.	

3. **conf.resp. petición de SS no estructurado del MT**: utilizado para enviar una respuesta a la LMFh a través de la SACF y la LMFv sobre el resultado de la petición.

Petición de SS no estructurado del MT (Respuesta: éxito o fracaso)	conf.resp.
Esquema de codificación de datos USSD	O (nota 1)
Cadena USSD	O (nota 2)
Resultado	O (nota 3)

FEA3	– Prepara y envía a la LMFv una conf.resp. petición SS no estructurado del MT.
NOTA 1 – Si este IE está presente, el IE cadena USSD debe estarlo también. NOTA 2 – Si este IE está presente, el IE esquema de codificación de datos USSD debe estarlo también. NOTA 3 – Sólo se utiliza si se produce una situación de error.	

4. **conf.resp. petición de SS no estructurado**: envía el resultado de la información recuperada del usuario móvil.

Petición de SS no estructurado	conf.resp.
Esquema de codificación de datos USSD	O (nota 1)
Cadena USSD	O (nota 2)
Resultado	O (nota 3)

FEA4	– Se ha conseguido del usuario la información requerida.
NOTA 1 – Si este IE está presente, el IE cadena USSD debe estarlo también.	
NOTA 2 – Si este IE está presente, el IE esquema de codificación de datos USSD debe estarlo también.	
NOTA 3 – Sólo se utiliza si se produce una situación de error.	

11.11 Notificación de SS no estructurados

La entidad invocadora utiliza este procedimiento cuando es necesario enviar una notificación al usuario móvil relacionada con el manejo de servicios suplementarios no estructurados.

En determinadas circunstancias, la SCFh puede generar (o recibir) una petición de notificación de SS no estructurado dirigida a (o desde) la LMFh. Es probable que esto ocurra cuando un servicio específico de un operador, proporcionado por la SCF originaria, necesita establecer un diálogo con el usuario móvil. Este diálogo puede ser iniciado por el usuario o por el servicio SCF. Los datos relativos a servicios suplementarios no estructurados proporcionan un mecanismo de transporte transparente que permite que tenga lugar dicho diálogo entre el usuario móvil y el servicio. Véase la figura 11.11-1.

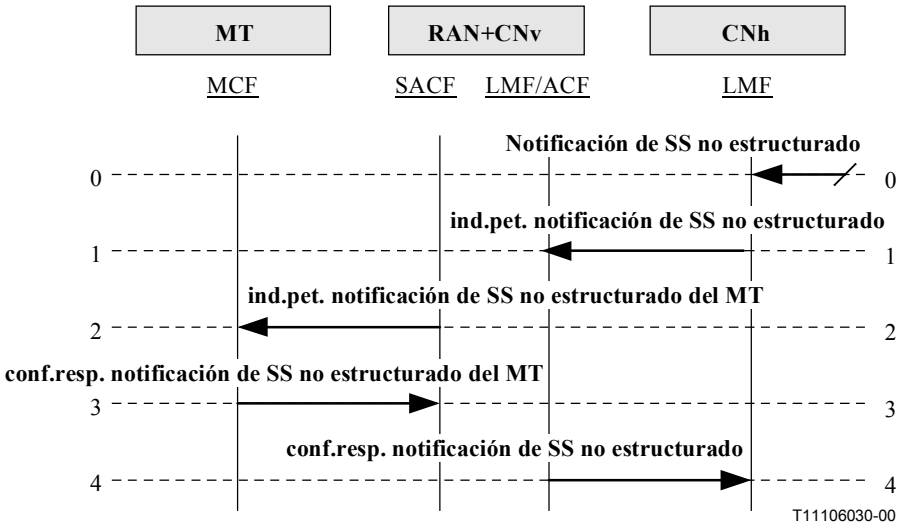


Figura 11.11-1/Q.1721 – Notificación de SS no estructurados

0. **Notificación de SS no estructurado**: indica que se envía una notificación al usuario móvil.

FEA0	– Envía a la LMFv una petición de notificación de SS no estructurada.

1. **ind.pet. notificación de SS no estructurado**: utilizada para enviar información al usuario móvil.

Notificación de SS no estructurado (Respuesta: éxito o fracaso)	ind.pet.
Esquema de codificación de datos USSD	M
Cadena USSD	M
Modelo de alerta	O (nota)

FEA1	– Envía a la SACF una petición de notificación de SS no estructurado.
NOTA – Está presente si se recibe de la SCFh en una operación de conexión, en otro caso está ausente.	

2. **ind.pet. notificación de SS no estructurado del MT**: utilizada para enviar información al usuario móvil.

Notificación de SS no estructurado del MT (Respuesta: éxito o fracaso)	ind.pet.
Esquema de codificación de datos USSD	M
Cadena USSD	M
Modelo de alerta	O (nota)

FEA2	– Envía a la SACF un respuesta a la notificación de SS no estructurado del MT.
NOTA – Está presente si se recibe de la SCFh en una operación de conexión, en otro caso está ausente.	

3. **conf.resp. notificación de SS no estructurado del MT**: utilizado para devolver una respuesta a la LMFh a través de la SACF y la LMFv sobre del resultado de la petición.

Notificación de SS no estructurado del MT (Respuesta: éxito o fracaso)	conf.resp.
Resultado	O (nota)

FEA3	– Envía a la SACF una respuesta notificación de SS no estructurado del MT.
NOTA – Sólo se utiliza si ocurre una situación de error.	

4. **conf.resp. Notificación de SS no estructurado**: envía el resultado de la información recuperada desde el usuario móvil.

Notificación de SS no estructurado	conf.resp.
Resultado	O (nota)

FEA4	– Confirma que se ha recibido la información recuperada.
NOTA – Sólo se utiliza si ocurre una situación de error.	

11.12 Notificación de invocación de SS

Este procedimiento se utiliza entre la SACF y la SCF cuando se invocan algunos servicios suplementarios por parte del usuario. Los servicios son la transferencia explícita de llamada, el desvío de llamada y los servicios multipartitos. La SACF verifica si se cumple el criterio para enviar

una notificación. Si así es, se envía una notificación a la SCF originaria. Si no se cumplen los criterios de notificación el procesamiento del servicio suplementario en particular continua inalterado y no se envía notificación alguna. Véase la figura 11.12-1.

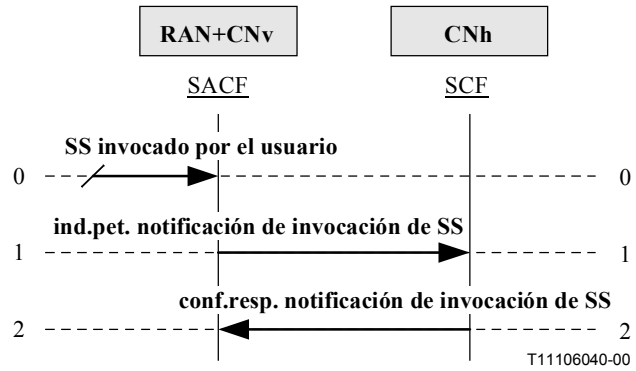


Figura 11.12-1/Q.1721 – Notificación de invocación

0. **SS invocado por el usuario**: la SACF recibe una invocación de SS iniciada por un usuario.

FEA0	– Detecta la invocación de un servicio suplementario determinado. – Prepara y envía a la SCF una ind.pet. notificación de invocación.

1. **ind.pet. notificación de invocación de SS**: se utiliza cuando un usuario invoca un determinado servicio suplementario.

Notificación de invocación de SS (Respuesta: éxito o fracaso)	ind.pet.
MS ISDN	M
IMUI	M
Evento de SS	M
Datos de SS	O (nota)

FEA1	– Si la información recibida se entiende, se prepara y envía una conf.resp. notificación de invocación de SS de acuse de recibo positivo. – Si la información recibida no se entiende, se prepara y envía una conf.resp. notificación de invocación de SS de acuse de recibo negativo.
NOTA – No todos los servicios suplementarios contienen datos.	

2. **conf.resp. notificación de invocación de SS**: devuelve a la SACF el resultado de la notificación de invocación.

Notificación de invocación de SS	conf.resp.
Resultado	M

FEA2	– Confirma la compleción del procedimiento de notificación de invocación de SS.

12 Servicios por medios radioeléctricos

Las características siguientes pueden no ser aplicables a todos los miembros de la familia IMT-2000.

12.1 Provisión de servicios por medios radioeléctricos (OTASP)

En esta cláusula se presentan los diagramas de flujos de información para uno de los servicios por medios radioeléctricos (OTA, *over-the-air*) denominado provisión de servicios por medios radioeléctricos (OTASP, *over-the-air service provisioning*) de los sistemas IMT-2000.

12.2 Visión general

La OTASP cumple con la necesidad de los sistemas radioeléctricos IMT-2000 de permitir y realizar de forma segura, el proceso por el cual los potenciales abonados del servicio IMT-2000 pueden activar nuevos servicios radioeléctricos (es decir, reciben autorización para los mismos). Además, los abonados pueden solicitar cambios en los servicios que utilizan sin intervención de una tercera parte. Una componente integral de este proceso es la funcionalidad del medio radioeléctrico en la CNh.

Uno de los objetivos primarios de la OTASP es la capacidad de proporcionar una clave de autenticación segura al módulo de identidad de usuario (UIM) para facilitar la autenticación. La autenticación es el proceso por el cual la información se intercambia entre un UIM y la red para confirmar y validar la identidad del UIM.

La OTASP incorpora un procedimiento de generación de clave de autenticación criptográfica. Este procedimiento permite a la red el intercambio de parámetros de clave de autenticación con un UIM. Estos parámetros se utilizan para generar la clave A. El procedimiento de generación de clave de autenticación mejora la seguridad del abonado (es decir, se permite el cifrado de voz y datos con el fin de conseguir una transferencia segura de información financiera o de crédito de un nuevo abonado, así como información del IMUI). Ello reduce el potencial uso fraudulento de los servicios de telecomunicaciones en el IMT-2000.

12.3 Descripción

Los flujos de información OTASP ilustran la siguiente progresión lógica de eventos:

- **Invocación de la activación con el proveedor de servicio deseado**: en la cual se produce la "incorporación o adaptación" entre la CNv servidora y la funcionalidad del medio radioeléctrico (modelada en la SCF y representada en los flujos de información como SCF_{OTA}) de la CN del proveedor de servicio deseado, y se establece una correlación entre el trayecto de voz [del usuario al representante del cliente (CR, *customer representative*), o a una unidad de respuesta de voz (VRU, *voice response unit*), en el centro de servicio al cliente (CSC, *customer service centre*)] y el trayecto de datos (entre el UIM y la funcionalidad del medio radioeléctrico). El terminal móvil realiza el acceso inicial al sistema sobre la base de la lista de selección de sistema preferido que se carga previamente en la UIMF. El usuario marca los dígitos OTASP predeterminados para iniciar el proceso de activación. La red visitada debe reconocer y procesar los dígitos recibidos del terminal móvil a fin de iniciar la sesión OTASP. En función de tales dígitos, la red visitada debe reconocer que se trata del origen de una OTASP y encamina la llamada de forma correcta al CSC. El tratamiento especial que se hace de los dígitos recibidos, exige un acuerdo comercial bilateral entre los sistemas originario y visitado, que queda fuera del ámbito de esta Recomendación.
- **Generación de la clave A**: en la que se genera de forma separada una clave de autenticación en la AMF y la UIMF. La clave A es utilizada para el cifrado y la seguridad durante el proceso de OTASP.

- **Reautenticación para el cifrado de la voz y de la señalización**: este proceso calcula y transfiere información de cifrado a la CNv para invocar el cifrado de los datos del plano de usuario (voz) y del plano de control (mensajes de señalización) previo al intercambio por medios radioeléctricos de información sensible de provisión y financiera.
- **Transferencia de datos OTASP**: en la que la información de provisión se transfiere entre la red originaria y el UIM.

12.4 Flujos de información de la provisión de servicios por medios radioeléctricos

12.4.1 Invocación de la activación con el proveedor de servicio deseado

Un potencial abonado ("usuario") desea disponer de un terminal móvil IMT-2000 activado en la red de un proveedor de servicio deseado (la red "originaria"), mientras se encuentra en otra red (la red "visitada"). Este flujo de información muestra el primer paso en la OTASP denominado proceso de "incorporación a adaptación" por el que se establece una correlación entre la llamada de voz del usuario y el trayecto de datos a través del que se descarga al UIM la información necesaria. El origen de la llamada de voz del usuario se redirecciona desde la red visitada a un representante del cliente (CR – una persona) o hacia una unidad de respuesta vocal (VRU – una máquina), en el centro de servicio al cliente (CSC) de la red originaria. La red visitada asigna un número de referencia temporal (TRN, *temporary reference number*) para la correlación entre los trayectos de voz y de datos. El conjunto de los TRN se administra mediante acuerdos bilaterales entre los proveedores de servicio asociados a fin de mantener la unicidad de los TRN utilizados en cada red visitada. La red originaria asigna un IMUI de "activación " que se utiliza durante el proceso de activación. Véase la figura 12.4-1.

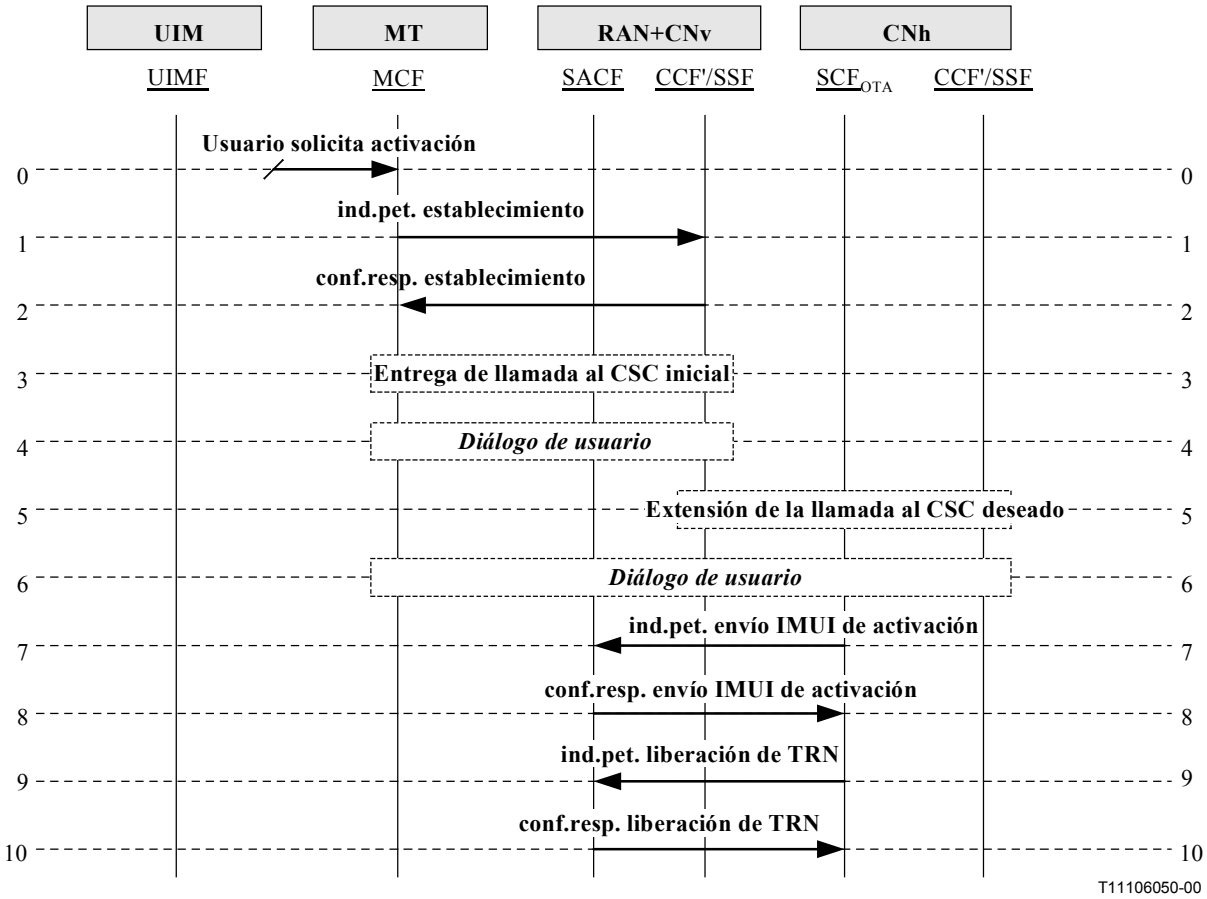


Figura 12.4-1/Q.1721 – Diagrama de flujos de información de la invocación de la activación con el proveedor de servicio deseado

0. **Usuario solicita activación**: es el estímulo inicial cuando el usuario desea la activación, pero se encuentra en un sistema distinto al deseado.

FEA0	– El usuario inicia el proceso realizando una llamada de OTASP, es decir, marcando los dígitos apropiados para la activación (por ejemplo, un código de servicio de facilidad local y un número de directorio, según se publicite, o mediante las instrucciones que acompañan al terminal móvil). – La MCF solicita un canal portador para establecer la llamada con el CSC local.

1. **ind.pet. de establecimiento**: desde la MCF a la CCF'/SSF de la CNv. Cuando se reciben los números de inicio de la llamada OTASP marcados por el usuario, la MCF envía dichos dígitos a la CCF'/SSF de la CNv.

Establecimiento (Respuesta: éxito)	ind.pet.
IMUI inicial (INIT_IMUI)	M (nota)

FEA1	– Cuando se reciben los dígitos y se identifica el código de servicio de facilidad local como un intento de OTASP, la CNv puede obviar o realizar una autorización normal de acceso a la red o una validación y autenticación del usuario antes de proceder. Con independencia del resultado de este procedimiento, la CNv conecta la llamada de voz a un CSC local. – La CCF'/SSF asigna un único TRN a esta sesión OTASP. – La CNv transfiere el TRN al CSC durante el establecimiento de la llamada. Nótese que el TRN puede enviarse como un número llamante o como un número llamado en función de los esquemas de señalización utilizados. – La CCF'/SSF ofrece un canal portador para transporta la llamada.
NOTA – INIT_IMUI es el IMUI incluido en el UIM durante su fabricación. Su vida es corta pues se sustituye por el IMUI de nueva asignación (NEW_IMUI) que genera la CNh, antes de que concluya la sesión OTASP.	

2. **conf.resp. establecimiento**: desde la CCF'/SSF a la MCF.

Establecimiento	conf.resp.
ID del portador	M

FEA2	– La MCF toma el canal portador concedido y completa la llamada.

3. **Entrega de llamada al CSC inicial**: se realiza la conexión de la llamada entre el usuario y el CSC asociado a la CNv.

4. **Diálogo entre el usuario y el CR o VRU del CSC inicial**: un representante del cliente (CS) o una unidad de respuesta vocal (VRU) del CSC de la CNv inicia el diálogo con el usuario.

FEA4	– El representante del cliente o la unidad de respuesta vocal del CSC determinan que el usuario desea tener el MT activado en otra CN, que pasa a ser la CN originaria del usuario (CNh). – Dado que existe un acuerdo comercial entre el operador de la CNv y de la CNh, el CSC inicia un reencaminamiento de la llamada hacia el CSC en el CNh deseado. – El CSC inicial puede utilizar un cuadro de referencia interno para conseguir la dirección del CSC deseado para reencaminar la llamada. Para evitar fraudes no se permite la marcación de números desde el usuario.

5. **Extensión de la llamada al CSC deseado**: El representante del cliente o la unidad de respuesta vocal del CSC obtienen información del usuario acerca del sistema al que éste desea estar conectado.

FEA5	– El representante del cliente o la unidad de respuesta vocal del CSC extiende la llamada vocal a otro CSC (suponiendo que existe un acuerdo comercial para dicha transferencia) que está asociado con el proveedor de servicio deseado (operador). – Envía el TRN al nuevo CSC.

6. **Diálogo entre el usuario y el CR o VRU del CSC deseado**: un representante del cliente o una unidad de respuesta vocal en el CSC deseado inicia el diálogo con el usuario.

FEA6	– El CSC establece el contacto con la funcionalidad del medio radioeléctrico deseada a fin de activar la provisión del servicio a través de la SCF_{OTA}.

7. **ind.pet. envío IMUI de activación**: va desde la SCF_{OTA} en la red originaria a la SACF en la red visitada. El representante del CSC hace que la SCF_{OTA} inicie este flujo. La CNh puede determinar la dirección de encaminamiento de la CNv desde el TRN previamente disponible. Este flujo pide a la SACF que se incorpore a la CNh para esta sesión OTASP. Asimismo, la CNh asigna un IMUI de "activación " que sólo se utiliza durante esta sesión OTASP.

Envío de IMUI de activación (Respuesta: éxito)	**ind.pet.**
IMUI de activación(ACT_IMUI)	M (nota 1)
Número de referencia temporal (TRN)	M (nota 2)
Código de actuación (ACTCODE)	M (nota 3)

FEA7	– La CNv asocia la llamada en cuestión a la CNh y, por tanto, se establece una correlación entre el trayecto de llamada y el trayecto de señalización.
NOTA 1 – El ACT_IMUI sólo se utiliza para esta sesión OTASP. NOTA 2 – El TRN se utiliza para asociar la CNh con esta llamada OTASP. NOTA 3 – El ACTCODE ordena a la SACF que se incorpore a la CNh para esta llamada.	

8. **conf.resp. envío IMUI de activación**: desde la SACF de la red visitada a la SCF_{OTA} de la red originaria.

Envío de IMUI de activación	conf.resp.
INIT_IMUI	M (nota 1)
Identidad de CNv (ID de CNv)	M (nota 2)
Capacidades de autenticación de la CNv (CNv_AUTHCAP)	M (nota 3)
Autorización denegada (AUTHDEN)	O (nota 4)

FEA8	– La CNh informa a la CSC que se ha realizado la incorporación a la CNv. – El CSC informa a la CNh que debe ordenar a la CNv que libere el TRN.
NOTA 1 – El INIT_IMUI se recibe del UIM en el establecimiento de la llamada y se utiliza para la generación de la clave A. NOTA 2 – La ID de CNv es necesario para encaminar posteriormente mensajes de retorno a la CNv en el proceso OTASP. NOTA 3 – La CNv_AUTHCAP informa a la CNh sobre las capacidades de autenticación de la CNv, utilizadas para la reautenticación. NOTA 4 – Se incluye AUTHDEN si a este UIM se le ha denegado previamente (en el paso 2) la autorización de acceso o ha fallado la validación y autenticación del abonado.	

9. **ind.pet. liberación de TRN**: desde la SCF_{OTA} de la red originaria a la SACF de la red visitada. El representante del CSC hace que la SCF_{OTA} inicie este flujo. Dado que la incorporación del terminal móvil al sistema deseado (CSC y CNh) se ha completado con éxito, ya no es necesario el TRN, y la CNh libera el TRN (un recurso potencialmente limitado) de forma que pueda ser reutilizado.

Liberación de TRN (Respuesta: éxito)	ind.pet.
ACT_IMUI	M
ACTCODE	M (nota)

FEA9	– La SACF de la CNv libera el TRN, permitiendo que éste sea reutilizado en otra sesión OTASP.
NOTA – El ACTCODE ordena a la SACF que libere el TRN.	

10. **conf.resp. liberación de TRN**: desde la SACF de la red visitada a la SCF_{OTA} de la red originaria.

Liberación de TRN	conf.resp.
Ninguna	(nota)

FEA10	– La SACF acusa recibo de la instrucción después de haber liberado el TRN. – Con este termina el proceso de incorporación.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

12.4.2 Generación de la clave A

Antes de activar el terminal móvil IMT-2000 del usuario, deben establecerse trayectos de voz y de datos seguros. Esto se realiza generando claves de autenticación idénticas (clave A) de forma separada en la red (LMF) y en el UIM (UIMF), utilizando un método de criptación pública (como por ejemplo, el algoritmo Diffie-Helman del que figura una descripción en el apéndice II). La clave A (que nunca se envía por medios radioeléctricos) se utiliza para producir las máscaras necesarias para el establecimiento del cifrado de la voz y de los datos. Este flujo de información muestra como se genera la clave A para la OTASP del IMT-2000. Véase la figura 12.4-2.

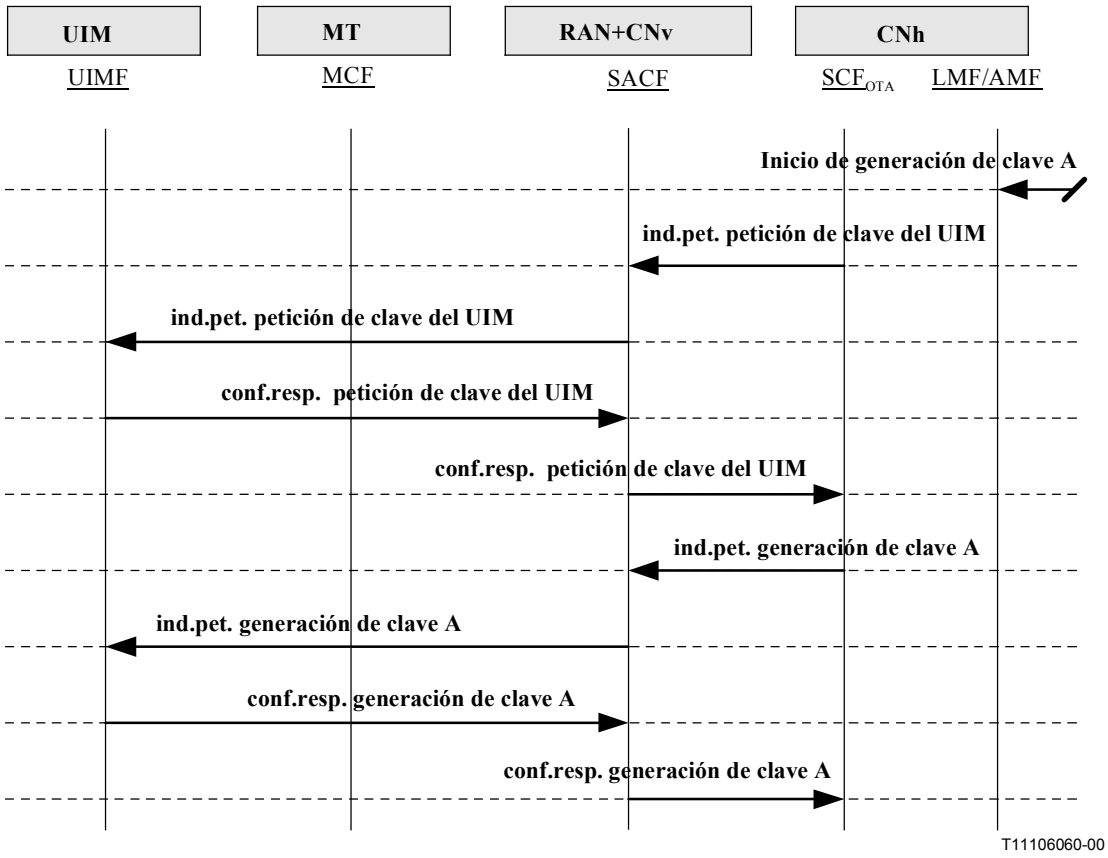


Figura 12.4-2/Q.1721 – Diagrama de flujo de información de generación de la clave A

0. **Proceso de inicio de generación de clave A**: es el estímulo inicial por el que el CSC inicia el procedimiento de generación de la clave de autenticación.

FEA0	– El CSC inicia el proceso de generación de la clave A. – La funcionalidad del medio radioeléctrico envía a la LMFh una petición que incluye la versión del protocolo de la clave de autenticación correspondiente a las capacidades de generación de clave A del UIM[8], la IMUI del UIM y la IMUI de activación. – La LMFh responde devolviendo la versión del protocolo de la clave de autenticación que utilizará, así como las claves públicas denominadas valor módulo (N*) y valor primitivo (g*). También incluye el valor de clave de CN (Y*) que está almacenada en la funcionalidad del medio radioeléctrico.

1. **ind.pet. petición de clave del UIM**: desde la SCF_{OTA} en la red origen a la SACF en la red visitada. El representante del CSC hace que la SCF_{OTA} inicie este flujo. Incluye la versión del protocolo de la clave de autenticación y las claves públicas. La funcionalidad del medio radioeléctrico almacena el valor de la clave de CN y no la envía a la SACF.

Petición de la clave del UIM (Respuesta: éxito)	**ind.pet.**
Versión del protocolo de clave de autenticación (AKEYPV)	M (nota)
Valor del módulo (MODVAL)	M
Valor de primitiva (PRIMVAL)	M

FEA1	– La SACF de la CNv retransmite el contenido de tal forma que puede enviarse sobre la interfaz radioeléctrica.
NOTA – La AKEYPV proporciona la versión del protocolo de autenticación correspondiente a la combinación específica del valor de módulo (N*), el valor de primitiva (g*) y el exponente (y*), que utilizará la CNh (y el UIM), según establezca el operador.	

2. **ind.pet. petición de clave del UIM**: desde la SACF de la red visitada a la UIMF a través de la MCF. La SACF sólo envía el contenido que ha recibido en el paso 1 de la funcionalidad del medio radioeléctrico a la UIMF.

Petición de la clave del UIM (Respuesta: éxito)	**ind.pet.**
Versión del protocolo de clave de autenticación (AKEYPV)	M
Valor del módulo (MODVAL)	M
Valor de primitiva (PRIMVAL)	M

FEA2	– La UIMF calcula con éxito el valor de la clave del UIM (X*) en función de los valores de claves públicas recibidas: MODVAL y PRIMVAL, y del exponente, tal como especifica la versión del protocolo de la clave de autenticación.

[8] Se modela el algoritmo Diffie-Hellman, pues está públicamente disponible para ser utilizado y es escalable, permitiendo varias combinaciones de exponentes y de valores de criptación pública (módulo y primitiva) que se utilizan para conseguir el grado de seguridad deseado por el operador.

3. **conf.resp. petición de clave del UIM**: este flujo se establece entre la UIMF (a través de la MCF) y la SACF de la red visitada. La UIMF calcula con éxito el valor de la clave de UIM. Cosa que indica a la SACF de la CNv.

Petición de la clave del UIM	conf.resp.
Resultado	M (nota)

FEA3	– La SACF de la CNv retransmite el contenido a la funcionalidad del medio radioeléctrico.
NOTA – El resultado indica que la UIMF ha calculado con éxito el valor de la clave del UIM.	

4. **conf.resp. petición de clave del UIM**: desde la SACF de la red visitada a la SCF_{OTA} de la red originaria. La SACF sólo envía a la funcionalidad del medio radioeléctrico el contenido recibido en el paso 3 de la UIMF.

Petición de la clave del UIM	conf.resp.
Resultado	M

FEA4	– La funcionalidad del medio radioeléctrico de la CNh calcula el valor de la clave de CN.

5. **ind.pet. generación de clave A**: desde la SCF_{OTA} en la red origen a la SACF en la red visitada. El representante del CSC hace que la SCF_{OTA} inicie este flujo. La funcionalidad del medio radioeléctrico almacena el valor de la clave de CN (Y*) que la funcionalidad del medio radioeléctrico ha almacenado en el paso 1.

Generación de la clave A (Respuesta: éxito)	ind.pet.
Valor de clave de CN (CNKEY)	M

FEA5	– La SACF de la CNv retransmite el contenido de forma que éste pueda enviarse por la interfaz radioeléctrica.

6. **ind.pet. generación de clave A**: desde la SACF de la red visitada a la UIMF (a través de la MCF). La SACF sólo envía a la UIMF el contenido recibido en el paso 5 de la funcionalidad del medio radioeléctrico.

Generación de la clave A (Respuesta: éxito)	ind.pet.
CNKEY	M

FEA6	– La UIMF calcula con éxito la clave de autenticación utilizando la CNKEY, MODVAL y el mismo exponente utilizado en el cálculo del valor de la clave del UIM.

7. **conf.resp. generación de clave A**: desde la UIMF (a través de la MCF) a la SACF en la red visitada. La UIMF ha calculado con éxito el valor de la clave A y lo indica a la SACF de la CNv. Envía a la SACF el valor de la clave del UIM, pero no el valor de la clave A (que nunca se envía por medios radioeléctricos).

Generación de la clave A	conf.resp.
Resultado	M (nota)
Valor de la clave de UIM (UIMKEY)	M

FEA7	– La SACF retransmite el contenido a la funcionalidad del medio radioeléctrico.
NOTA – El resultado indica que la UIMF ha calculado con éxito el valor de la clave A.	

8. **conf.resp. generación de clave A**: es un flujo desde la SACF de la red visitada a la SCF_{OTA} de la red originaria. La SACF sólo envía a la funcionalidad del medio radioeléctrico el contenido que ha recibido de la UIMF en el paso 7.

Generación de la clave A	conf.resp.
Resultado	M
UIMKEY	M

FEA8	– La funcionalidad del medio radioeléctrico ordena a la LMFh que también genere la clave A utilizando UIMKEY, MODVAL y el mismo exponente utilizado en el paso 1 para calcular CNKEY. – Por tanto, el UIM y la CNh generan la misma clave A.

12.4.3 Reautenticación para el cifrado de la voz y de la señalización

Este escenario describe la reautenticación del UIM para el cálculo y envío de parámetros de criptación a la CNv. Estos parámetros se utilizan para invocar criptación de los mensajes de señalización y la privacidad de la voz, respectivamente, sobre la interfaz radioeléctrica. Véase la figura 12.4-3.

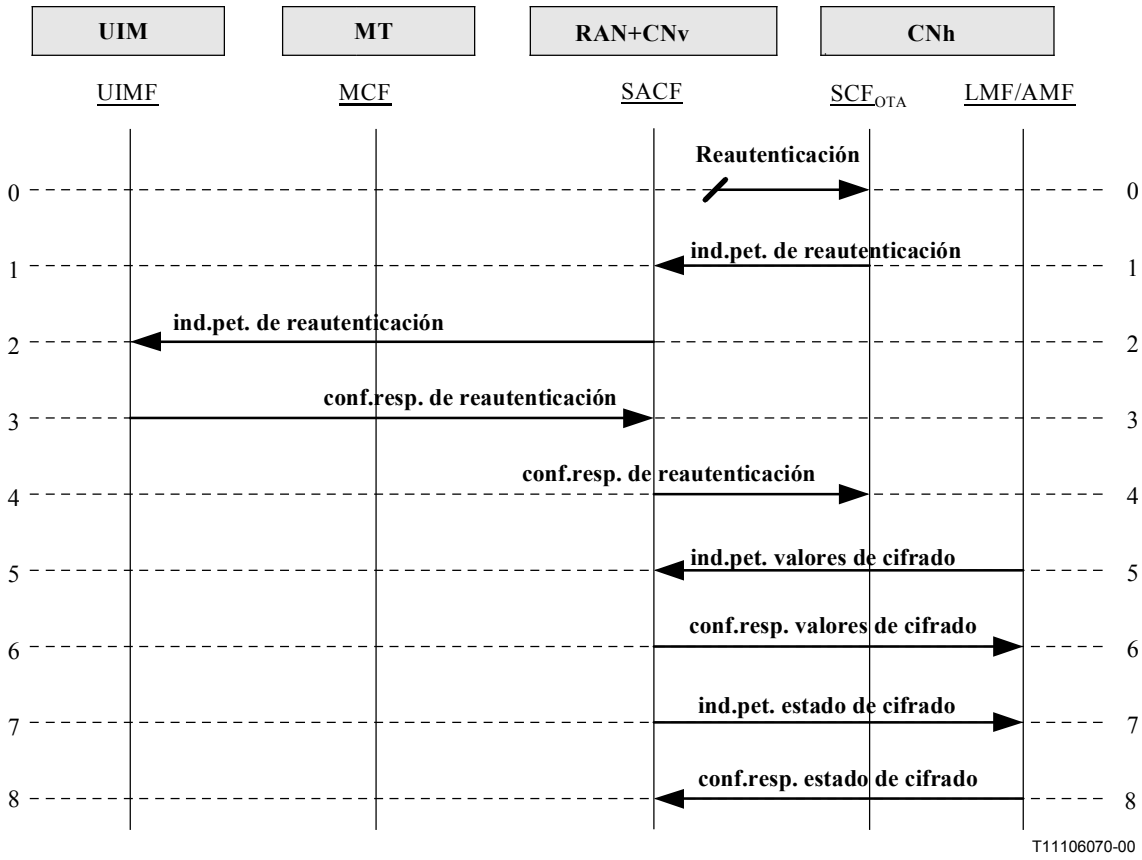


Figura 12.4-3/Q.1721 – Diagrama de flujo de información de la reautenticación para el cifrado de la voz y la señalización

0. **Reautenticación**: es el estímulo inicial gracias al cual el centro de servicio al cliente (CSC) inicia el procedimiento de reautenticación.

FEA0	– El CSC inicia el proceso de reautenticación. – Determina que se necesita el cifrado en la interfaz radioeléctrica. – La funcionalidad del medio radioeléctrico genera un valor de puesta a prueba aleatorio (RAND) que envía a la SACF.

1. **ind.pet. de reautenticación**: desde la SCF$_{OTA}$ en la red originaria a la SACF en la red visitada. El representante del CSC hace que la SCF$_{OTA}$ inicie este flujo. La funcionalidad del medio radioeléctrico genera un valor de puesta a prueba aleatorio (RAND, *random challenge value*) que envía a la SACF. El objetivo es autenticar al UIM (de nuevo) después de la generación de la clave A para garantizar que el UIM correcto está aún implicado en el proceso OTASP, antes de poner en marcha el cifrado.

Reautenticación (Respuesta: éxito)	**ind.pet.**
Valor de puesta a prueba aleatoria (RAND)	M (nota)

FEA1	– La SACF de la CNv retransmite el contenido de la UIMF a través de la MCF.
NOTA – La UIMF utiliza el RAND para responder con un resultado que permita a la CNh determinar que el UIM se ha reautenticado correctamente.	

2. **ind.pet. de reautenticación**: desde la SACF de la red visitada a la UIMF (a través de la MCF). La SACF envía a la UIMF únicamente el contenido que ha recibido en el paso 1 procedente de la funcionalidad del medio radioeléctrico.

Reautenticación (Respuesta: éxito)	ind.pet.
RAND	M

FEA2	– La UIMF calcula con éxito la correspondiente respuesta que indica que se ha reautenticado correctamente.

3. **conf.resp. de reautenticación**: desde la UIMF (a través de la MCF) a la SACF en la red visitada. La UIMF realiza la reautenticación y calcula el correspondiente valor de respuesta de puesta a prueba aleatorio (RANDC, *random challenge response*) basado en el RAND recibido, su propio IMUI y otros atributos. El cálculo puede basarse en un algoritmo sólo entendido por la UIMF y la CNh.

Reautenticación	conf.resp.
Respuesta de puesta a prueba aleatoria (RANDC)	M

FEA3	– La SACF de la CNv retransmite el contenido a la funcionalidad del medio radioeléctrico a través de la SCF_{OTA}.

4. **conf.resp. de reautenticación**: desde la SACF a la SCF_{OTA} de la red visitada

Reautenticación	conf.resp.
RANDC	M

FEA4	– La funcionalidad del medio radioeléctrico envía la información a la LMFh, junto con el valor RAND. – La LMFh calcula de forma independiente un RANDC utilizando el algoritmo descrito en el paso 3. – La LMFh lo compara con el RANDC recibido. – La LMFh determina que el UIM se ha reautenticado correctamente. – La LMFh inicia entonces la generación de los valores asociados al cifrado.

5. **ind.pet. valores de cifrado**: desde la LMFh de la red originaria a la SACF de la red visitada. Una vez que se determina que el UIM se ha reautenticado correctamente, la LMFh calcula los valores de cifrado y los envía a la SACF.

Valores de cifrado (Respuesta: éxito)	ind.pet.
Identidad de CNv (ID de CNv)	M (nota 1)
Clave de cifrado del plano de control (CPCKEY)	M (nota 2)
Clave de cifrado del plano de usuario (UPCKEY)	M (nota 3)

FEA5	– La SACF de la CNv utiliza el CPCKEY y el UPCKEY para activar el cifrado.
NOTA 1 – La ID de CNv se utiliza para encaminar los valores de la ind.pet. de valores de cifrado a la SACF correcta. NOTA 2 – Se utiliza para activar el cifrado de la información del plano de control, como por ejemplo, los mensajes de señalización. NOTA 3 – Se utiliza para activar el cifrado de la información del plano de usuario, como por ejemplo, la voz.	

6. **conf.resp. valores de cifrado**: desde la SACF de la red visitada a la LMFh de la red originaria.

Valores de cifrado	conf.resp.
Ninguno	(nota)

FEA6	La LMFh de la CNh recibe una indicación de que los valores de cifrado han alcanzado con éxito la SACF.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

7. **ind.pet. estado de cifrado**: este flujo se dirige desde la SACF de la red visitada hacia la LMFh de la red originaria. En la interfaz radioeléctrica se activan el cifrado del plano de usuario (voz), el cifrado del plano de control (mensajes de señalización) o ambos.

Estado de cifrado (Respuesta: éxito)	ind.pet.
Informe de cifrado del plano de control (CPCRPT, *control plane ciphering report*)	M (nota 1)
Informe de cifrado del plano de usuario (UPCRPT, *user plane ciphering report*)	M (nota 2)

FEA7	La LMFh de la CNh tiene información relativa al estado actual del cifrado en la interfaz radioeléctrica.
NOTA 1 – Informa si se ha activado o no el cifrado del plano de control. NOTA 2 – Informa si se ha activado o no el cifrado del plano de usuario.	

8. **conf.resp. estado de cifrado**: este flujo se dirige desde la SACF en la red visitada hasta la LMFh en la red originaria. La LMFh envía esta información a la funcionalidad del medio radioeléctrico que a su vez indica al representante del CSC en la CNh sobre si en ese momento es seguro el intercambio de datos de usuario sensibles por medios radioeléctricos.

Estado de cifrado	conf.resp.
Ninguno	(nota)

FEA8	– La LMFh de la CNh envía esta información a la funcionalidad del medio radioeléctrico. – Ello indica al CSC si es seguro ahora el intercambio de datos por medios radioeléctricos. – Así, el CSC y el abonado intercambian información sensible (financiera o de otro tipo). – Con ello finaliza el proceso de reautenticación.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

12.4.4 Transferencia de datos de la OTASP

Este escenario describe el intercambio de mensajes de datos OTASP que transportan la información sobre activación entre la funcionalidad del medio radioeléctrico de la CNh y la UIMF, a través de la MCF y de la SACF de la CNv. Típicamente, esto se realiza después de la activación del cifrado. Véase la figura 12.4-4.

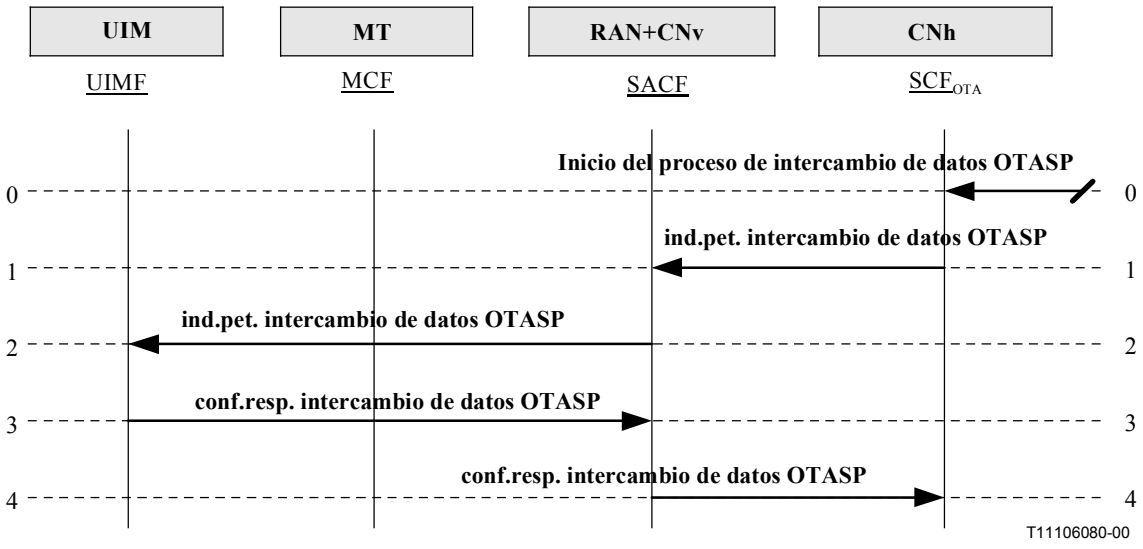


Figura 12.4-4/Q.1721 – Diagrama de flujos de información del intercambio de datos de la OTASP

0. **Inicio del proceso de intercambio de datos OTASP**: es el estímulo inicial por el que el representante del CSC hace que la SCF_{OTA} inicie el procedimiento de intercambio de datos de la OTASP.

FEA0	– El CSC inicia el proceso de intercambio de datos de la OTASP. – Habiendo confirmado que el cifrado está presente en la interfaz radioeléctrica, hace que la funcionalidad del medio radioeléctrico envíe a la SACF de la CNv datos relativos a la OTASP. – Ello incluye la IMUI recién signada para su descarga en la UIMF, así como información relativa a otros servicios suplementarios.

1. **ind.pet. intercambio de datos OTASP**: desde la SCF_{OTA} de la red originaria a la SACF de la red visitada.

Intercambio de datos de OTASP (Respuesta: éxito)	**ind.pet.**
IMUI recién asignado (NEW_IMUI)	M (nota 1)
ACTCODE	M (nota 2)

FEA1	– La SACF de la CNv retransmite el contenido a la UIMF a través de la MCF. – La SACF también libera recursos cuando se completa la sesión de OTASP.
NOTA 1 – El NEW_IMUI es la identidad permanente, asignada y comprometida en el UIM del usuario. NOTA 2 – Dependiendo del caso de intercambio de datos de que se trate, el ACTCODE puede ordenar: – que la SACF envíe el NEW_IMUI a la UIMF; – que la UIMF incluya el NEW_IMUI en su memoria permanente; – que el UIM registre al usuario después de que se haya incluido el NEW_IMUI en su memoria permanente; – que la SACF y la UIMF liberen recursos después de finalizar las tareas de OTASP.	

2. **ind.pet. intercambio de datos de OTASP**: flujo que va desde la SACF de la red visitada a la UIMF (a través de la MCF).

Intercambio de datos de OTASP (Respuesta: éxito)	**ind.pet.**
IMUI recién asignado (NEW_IMUI)	M

FEA2	– La UIMF sustituye al ACT_IMUI con el NEW_IMUI. – Incluye el NEW_IMUI en la memoria permanente. – Utiliza el procedimiento de registro de terminal para registrar de nuevo al usuario.

3. **conf.resp. intercambio de datos OTASP**: flujo que va desde la UIMF (a través de la MCF) a la SACF de la red visitada.

Intercambio de datos de OTASP	**conf.resp.**
Ninguno	(nota)

FEA3	– La SACF envía la conf.resp. intercambio de datos OTASP sobre la funcionalidad del medio radioeléctrico.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito.	

4. **conf.resp. intercambio de datos OTASP**: flujo que va desde la SACF de la red visitada a la SCF_{OTA} de la red originaria.

Intercambio de datos de OTASP	conf.resp.
Ninguno	(nota)

FEA4	– La funcionalidad del medio radioeléctrico informa al CSC que el intercambio de datos de OTASP ha finalizado con éxito.
NOTA – La confirmación de respuesta está vacía. Su sola presencia es suficiente para indicar éxito. Esto completa con éxito la sesión OTASP. En este momento el MT y el UIM están activados y el abonado puede recibir el servicio.	

13 Definiciones de elementos de información

13.1 código de acción (ACTCODE, *action code*): Especifica la naturaleza de la acción que realiza la entidad funcional designada. Por ejemplo, en la OTASP, la SCF utiliza el código de acción de la red originaria para dar instrucciones a la SACF de la red servidora sobre:

– La incorporación a la red originaria durante una sesión OTASP específica.

– La liberación de un TRN, permitiendo que éste sea reutilizado en otra sesión OTASP.

– El envío de una IMUI recién asignada al UIM.

– La inclusión de una nueva IMUI en la memoria permanente del UIM.

– Un nuevo registro del usuario después de haber incluido una nueva IMUI en el UIM.

– La liberación de recursos en la CNv al final de la sesión OTASP.

13.2 identidad de usuario móvil internacional de activación; IMUI de activación (ACT_IMUI, *activation IMUI*): Es una IMUI temporal que asigna la SCF en la red originaria y que sólo se utiliza durante una sesión OTASP concreta. Eventualmente es sustituida por la IMUI recién asignada.

13.3 motivo de alerta: Indica el motivo de la alerta del centro de servicio de mensajes. Puede tomar uno de los valores siguientes:

– MT presente.

– Memoria disponible.

13.4 modelo de alerta: Indicación que puede ser utilizada por el MT para alertar al usuario de una forma determinada cuando existe tráfico dirigido al móvil (llamada conmutada o datos de servicio suplementario no estructurado). Esta indicación puede ser un nivel de alerta o una categoría de alerta.

13.5 autorización denegada (AUTHDEN, *authorization denied*): Indica que se ha negado previamente la autorización de acceso a la red a un UIM, o bien que ha fallado la validación y autenticación del abonado.

13.6 clave de autenticación (Clave-A): Es un valor relativo a la seguridad que se utiliza en el cifrado de voz/datos y de mensajes de señalización. Nunca se envía sobre la interfaz radioeléctrica. Puede establecerse tanto en la CNh como en el UIM mediante procedimientos OTASP, o puede ser programado en el UIM mediante métodos especificados por el proveedor de servicio.

13.7 versión del protocolo de la clave de autenticación (AKEYPV, *authentication key protocol version*): Indica la combinación específica (conforme a los deseos del operador originario) del valor de módulo "N," del valor de primitiva "g," y del exponente "y," que utilizan la CNh y el UIM durante el proceso de generación de la clave de autenticación OTASP (véase el apéndice II).

13.8 AUTHBS: Respuesta de autenticación que genera la red en respuesta a una puesta a prueba aleatoria enviada por el UIM durante un procedimiento de "actualización de SSD".

13.9 AUTH_R: Respuesta de autenticación a una puesta a prueba global basada en SSD.

13.10 AUTH_U: Respuesta de autenticación a una puesta a prueba única basada en SSD.

13.11 capacidad portadora: Indica el servicio portador RDSI solicitado que debe proporcionar la red (véase la Recomendación UIT-T Q.931 [10]).

13.12 identidad de portador; ID de portador: Utilizado para especificar el portador (por ejemplo, número de canal).

13.13 identidad de facturación; ID de facturación: Utilizado para identificar el plan de facturación (tarifa, propietario de la cuenta, etc.) asociado a la llamada.

13.14 número llamado: Identifica la parte llamada de una llamada (véase la Recomendación UIT-T Q.931 [10]).

13.15 cómputo histórico de la llamada (CHCNT, *call history count*): Contador que se mantiene en la red y el UIM. El contador puede ser actualizado por la red originaria o la red visitada y sirve como detector de posibles UIM "clónicos".

13.16 identidad de llamada; ID de llamada: Identifica la identidad de una llamada en un punto de transferencia de señalización.

13.17 número llamante: Identifica el origen de una llamada (véase la Recomendación UIT-T Q.931 [10]).

13.18 identidad de usuario llamante; ID de usuario llamante: Identifica la parte llamante de una llamada.

13.19 categoría: Proporciona una indicación del asunto específico (por ejemplo, emergencia, anuncio del operador del sistema, noticias, avisos, deportes, etc.) que se transporta en la carga útil enviada a uno o varios usuarios (por ejemplo, SMS o mensaje de difusión de teleservicio).

13.20 puesta a prueba (o RANDU): Una puesta a prueba única y aleatoria que genera la red para autenticar el UIM.

13.21 respuesta a puesta a prueba: Respuesta de autenticación calculada por el UIM a la puesta a prueba única aleatoria iniciada por la red. En algunos sistemas también se conoce como resultado de signatura, SRES (*signature result*).

13.22 valor de respuesta de puesta a prueba: Es un valor generado por el terminal móvil (PSCAF) que utiliza el valor de puesta a prueba y los datos secretos que comparte con su red originaria (LMFp/AMFp).

13.23 valor de puesta a prueba: Es un valor aleatorio generado por la red visitada utilizado para la autenticación del terminal móvil en visita.

13.24 clave(s) de cifrado: Clave(s) secreta(s) utilizada para el cifrado del tráfico en la interfaz radioeléctrica.

13.25 capacidades de autenticación de la CNv (CNv_AUTHCAP, *CNv authentication compabilites*): Proporciona información sobre las capacidades de autenticación de una red visitada o servidora; por ejemplo, se utiliza para la reautenticación durante una sesión OTASP.

13.26 identidad de CNv (CNvID, *CNv identity*): Proporciona la identidad de la red visitada/servidora con fines de encaminamiento. Por ejemplo, en la OTASP una CNv la proporciona a la CNh, de forma que la CNh pueda utilizarla posteriormente durante una sesión OTASP para el encaminamiento de mensajes a la CNv.

13.27 valor de la clave de CN (CNKEY, *CN key value*): Es un número "Y" que genera la red originaria (es decir, en la LMFh) y que se envía a la red visitada y al UIM, para generar la clave de autenticación durante una sesión OTASP. Se calcula como:

$$Y = g^y \text{ Mod } N$$

13.28 confirmación de RANDG: Forma de RAND enviada por la MCF y que es consistente con interfaces radioeléctricas específicas.

13.29 ID de línea conectada: Identifica la parte conectada de una llamada.

13.30 clave de cifrado del plano de control (CPCKEY, *control phane cipher key*): Contiene la clave que debe utilizarse para el cifrado de los campos de datos pertinentes de los mensajes de señalización que se envían en ambos sentidos sobre la interfaz radioeléctrica. Se calcula en la CNh. Su presencia también indica a la red servidora/visitada que active el cifrado del plano de control.

13.31 informe de cifrado del plano de control (CPCRPT, *control plane ciphering report*): Lo envía una red visitada/servidora a la red originaria para indicar si se ha activado el cifrado del plano de control.

13.32 contraseña vigente: Contraseña utilizada por un usuario para el control de los servicios suplementarios.

13.33 duración de la sesión de datos: Es la duración asignada a la conexión túnel de una sesión de datos. La determina y/o amplía la PSCAF cuando se requiere el establecimiento de una nueva sesión de datos. Una conexión túnel se libera cuando expira su vida útil.

13.34 datos de usuario suprimidos: Describe los datos del perfil de usuario que deben suprimirse en los procedimientos de gestión de datos de abonado. Puede incluir:

– una lista de servicios básicos;
– una lista de servicios suplementarios (en forma de códigos suplementarios);
– datos de servicios suplementarios;
– datos de suscripción de VHE;
– datos sobre difusión y/o suscripción de llamada de grupo.

13.35 método de encapsulado: Es un esquema del plano de usuario destinado a evitar la entrega de paquetes de datos de usuario fuera de secuencia en una conexión túnel. La PSACF propone el método de encapsulado cuando se envía una petición para el establecimiento/restablecimiento de una sesión de datos a la LMFp de la red visitada.

13.36 referencia de punto extremo (punto): Es el número/dirección de encaminamiento del usuario (es decir, ITDN), la parte que debe añadirse o eliminarse de una llamada multipartita.

13.37 calidad esperada: Elemento de información que se utiliza para informar de la calidad esperada de un portador radioeléctrico que la red asigna a un terminal móvil en función de los resultados de la medida.

13.38 información de facilidad: Código de facilidad, capacidades del sistema visitado, acción del sistema actualmente visitado.

13.39 directrices: Se refiere a las directrices que se dan a un usuario al que se pide que proporcione un control de servicio suplementario de contraseña. Puede darse la información siguiente:

– "Introduzca la contraseña": utilizada para solicitar al usuario que introduzca su contraseña actual.
– "Introduzca la nueva contraseña": utilizada para solicitar al usuario que introduzca una nueva contraseña durante el registro de la nueva contraseña.

– "Introduzca otra vez la nueva contraseña": utilizado para solicitar al usuario que vuelva a introducir la nueva contraseña durante el registro de la misma.

13.40 compatibilidad de capa alta: Proporciona una forma mediante la que el usuario distante puede verificar la compatibilidad (véase la Recomendación UIT-T Q.931 [10].)

13.41 dirección de función de gestión de ubicaciones (originales): Dirección sobre la que puede realizarse el encaminamiento hacia una función de gestión de ubicación originaria, por ejemplo, el número RDSI de la HLR.

13.42 número de directorio móvil IMT-2000 (IMDN, *IMT-2000 mobile directory number*): Número susceptible de ser marcado que identifica unívocamente a un usuario IMT-2000 y que se utiliza para realizar una llamada a dicho usuario o para identificar a un usuario cuando se origina una llamada.

NOTA – A estos efectos puede aplicarse un número RDSI de MS E.164.

13.43 identidad de usuario móvil internacional (IMUI, *international mobile user identity*): Utilizada para direccionar un terminal móvil e identificar de forma inequívoca el usuario móvil para una función de provisión del servicio.

13.44 capacidad de transferencia de información: Indica el tipo de capacidad portadora solicitada por la parte llamante (por ejemplo, voz) (véase la Recomendación UIT-T Q.931 [10]).

13.45 número de directorio temporal internacional (ITDN, *international temporary directory number*): Número E.164, que se puede marcar y al que se puede encaminar una llamada, y que el sistema visitado asigna a la parte llamada durante un corto intervalo de tiempo para facilitar el encaminamiento de llamadas, mientras se produce una itinerancia global.

13.46 identidad de usuario móvil internacional inicial; IMUI inicial (INIT_IMUI): IMUI original que se incluye en el UIM durante la fabricación y que se utiliza durante el proceso de generación de clave de autenticación de OTASP. Tiene una duración breve y es sustituida por la IMUI recién asignada que concede la red originaria antes de terminar una sesión de OTASP.

13.47 nivel de interferencia: Elemento de información utilizado para informar del nivel de interferencia como una parte del informe de medidas realizadas.

13.48 dirección IP (X): Dirección IP de la entidad X (por ejemplo, PSCAF, PSCF, y PSGCF). Se utiliza como punto de terminación del túnel.

13.49 identidad de la zona de ubicación (LAI, *location area identity*): Identifica la zona en la que se encuentra el terminal móvil en la red visitada.

13.50 dirección de función de gestión de ubicaciones; dirección LMFv: Dirección sobre la que puede realizarse el encaminamiento hacia una función de gestión de ubicación visitada, por ejemplo, el número RDSI del VLR.

13.51 información de ubicación: Indica la ubicación del usuario móvil con tanta precisión como sea posible con la información disponible. Puede ser, por ejemplo, ID de la célula, ID de la zona de ubicación, dirección VLR o algún tipo de información geográfica.

13.52 compatibilidad de capa baja: Proporciona los medios que una entidad direccionada debe utilizar para verificar la compatibilidad (por ejemplo, un usuario distante, una unidad de interfuncionamiento o un nodo de red de función de capa alta direccionado por el usuario llamante) (véase la Recomendación UIT-T Q.931 [10]).

13.53 identidad de ruido; ID de medio: Utilizado para identificar/seleccionar un tipo de medio.

13.54 tipo de medio: Se refiere a un medio de transporte de servicio específico. La palabra medios se refiere a un conjunto de portadores asignados para soportar una variedad de servicios genéricos tales como voz, datos, imagen y vídeo.

13.55 condición de la medida: Este elemento de información se utiliza para indicar al terminal móvil la condición bajo la cual se realiza la medida. Incluye información como por ejemplo el intervalo de repetición.

13.56 mensaje: Este parámetro contiene el mensaje SMS.

13.57 dirección del centro de mensajes: Representa la dirección E.164 de un centro de mensajes SMS.

13.58 tipo de notificación de mensaje: Indica la forma en la que se realiza la notificación al usuario (por ejemplo, de forma audible, visual, vibración, una combinación de ellas u otra cualquiera).

13.59 cómputo de mensajes pendientes: Indica el número de mensajes pendientes de ser recuperados por el usuario.

13.60 prioridad del mensaje: Proporciona en orden ascendente, una indicación del nivel de prioridad (por ejemplo, normal, interactivo, urgente, emergencia) de un mensaje (por ejemplo, SMS o difusión de teleservicio).

13.61 estado del mensaje: Proporciona una indicación sobre si el mensaje es nuevo, es una sustitución o una supresión de un mensaje existente (por ejemplo, SMS o difusión de teleservicio) con la misma identificación (véase tipo de mensaje).

13.62 tipo de mensaje: Proporciona la identificación de un mensaje (por ejemplo, SMS o difusión de teleservicio) en una red servidora.

13.63 indicador de mensaje en espera: Indica si se trata de un mensaje que está en espera.

13.64 tipo de mensaje en espera: Indica si el mensaje en espera es de voz, facsímil, correo electrónico o de otro tipo.

13.65 valor de módulo (MODVAL, *modulus value*): Número "N" generado por la red originaria (es decir, en la LMFh) que se envía a la red visitada y en el UIM, para la generación de la clave de autenticación durante una sesión OTASP. El operador fija su longitud (por ejemplo, 512 bits, 768 bits, etc.), siendo mayor la seguridad que existe durante el proceso de generación de la clave de autenticación cuanto mayor sea dicho número.

13.66 MS RDSI: Se refiere a uno de los números RDSI asignados a un abonado móvil de acuerdo con la Recomendación UIT-T E.213 [8].

13.67 identificador de acceso a la red (NAI, *network access identifier*): Cadena que identifica unívocamente a la entidad funcional (FE), en este caso la PSCF.

13.68 identidad de usuario móvil internacional recién asignada; IMUI recién asignada (New_IMUI): Identidad permanente que asigna la red originaria (LMFh) al UIM de un nuevo abonado que se incluye en el UIM cuando finaliza una sesión OTASP en la que sustituye al IMUI de activación.

13.69 número de llamadas medidas: Elemento de información utilizado para indicar al terminal móvil el número máximo de células alrededor del mismo y sobre las cuales se deberán realizar medidas relativas a las condiciones radioeléctricas de las mismas.

13.70 resultado de operación: Proporciona el resultado de la operación, tal como operación rechazada (por ejemplo, operación no válida), operación aceptada y completada u operación aceptada pero no completada (por ejemplo, error).

13.71 dirección de origen: Es la dirección de quien origina el mensaje original (por ejemplo, en SMS o difusión de teleservicio). Son formatos típicos los dígitos BCD, la codificación IA5 y las variantes de direcciones IP.

13.72 carga útil: Cualquier texto que se transporta (por ejemplo, SMS o difusión de teleservicio) para ser visualizado o para cualquier otro uso en la entidad receptora. Sólo tiene sentido para los puntos extremos del protocolo y lo interpreta el identificador de teleservicio.

13.73 periodicidad: Proporciona una indicación de la hora de comienzo, la duración o la tasa de repetición que necesita un mensaje (por ejemplo, SMS o difusión de teleservicio) para poder ser entregado a su receptor o receptores.

13.74 nivel de recepción del canal piloto: Elemento de información utilizado para informar del nivel de recepción de un canal piloto y que forma parte de un informe de medida.

13.75 número de identificación personal (PIN, *personal identification number*): Número utilizado en la verificación de la identidad del usuario y que se utiliza para desbloquear el UIM. Lo asigna el proveedor de servicio en el momento de la provisión del servicio.

13.76 indicador de idioma preferido: Indica el idioma preferido del receptor de anuncios vocales o de mensajes de texto (por ejemplo, cuando se informa a un usuario de la existencia de mensajes pendientes de ser recuperados, cuando se da la bienvenida a un usuario itinerante o se muestra un mensaje corto).

13.77 valor primitivo (PRIMVAL, *primitive value*): Número "g" que fija la red originaria (es decir, en el LMFh) y que se envía a la red visitada y en el UIM para generar la clave de autenticación durante una sesión de OTASP. El operador fija su longitud siendo mayor la seguridad que existe durante el proceso de generación de la clave de autenticación cuanto mayor sea dicho número.

13.78 información de control de potencia: Utilizado para indicar al terminal móvil el nivel de potencia inicial que debe fijar para el portador radioeléctrico asignado.

13.79 error del proveedor: Indica un tipo de error relacionado con el protocolo:

– ID de invocación duplicado;
– servicio no soportado;
– parámetro mal tecleado;
– limitación de recursos;
– inicio de liberación, es decir, el elemento par ha comenzado la liberación del diálogo, debiendo ser liberado el servicio;
– respuesta no esperada del elemento par;
– fallo de compleción del servicio;
– sin respuesta del elemento par;
– respuesta recibida inválida.

13.80 calidad del servicio (QoS, *quality of service*): Utilizado para especificar la calidad de servicio requerida, tal como la tasa de errores en los bits.

13.81 RANDBS: Puesta a prueba aleatoria enviada por la MCF para validar la red en sistemas basados en SSD.

13.82 RANDG: Difusión de puesta a prueba aleatoria global (número aleatorio) sobre el canal de información. Se utiliza en sistemas basados en SSD conjuntamente con los SSD y con otros parámetros, según proceda, para autenticar al usuario.

13.83 RANDSSD: Número aleatorio enviado al UIM, para ser utilizado en el proceso de actualización de SSD.

13.84 RANDU: Puesta a prueba única aleatoria utilizada para autenticar al usuario del terminal en sistemas basados en SSD (puede ser generado por la red visitada cuando se comparte el SSD).

13.85 duración restante de la sesión: Lo calcula la LMFp originaria utilizando la duración de sesión original, y se envía a la LMFp de anclaje durante una sesión de datos establecida.

13.86 acción distante: Tono o anuncio que debe reproducirse.

13.87 información solicitada: Indica el tipo de información solicitada, por ejemplo, información de ubicación, estado del usuario o ambas.

13.88 información de frecuencia radioeléctrica: Utilizado para especificar la información sobre la frecuencia radioeléctrica asignada al terminal móvil.

13.89 información del enlace inverso: Utilizado para especificar la información del enlace radioeléctrico inverso asignado al terminal móvil.

13.90 resultado: Utilizado para indicar el éxito o fracaso de un procedimiento solicitado.

13.91 dirección de encaminamiento: Utilizada para realizar el encaminamiento a la red de terminación visitada/servidora/soporte.

13.92 clave de seguridad: Generada por la LMFp y enviada al terminal móvil, a la PSCF visitada y a la PSGCF para soportar la asociación de criptación y seguridad entre dichas entidades.

13.93 índice de parámetro de seguridad: Generado por la LMFp y enviado al terminal móvil, a la PSCF visitada y a la PSGCF para soportar la asociación de criptación y seguridad entre dichas entidades.

13.94 selección: Especifica los datos que deben recuperarse de la SDF.

13.95 información de dirección de servicio: Utilizada por una SCF para seleccionar la aplicación correcta.

13.96 discriminador de servicio: Indicador utilizado por la LMFp originaria para determinar la PSGCF e indicar al terminal móvil la red a la que debe conectarse (por ejemplo, ISP específico, red corporativa específica, acceso genérico a Internet). Asimismo, indica si se prefiere que el acceso se realice a través de una PSGCF en la red visitada o en la red originaria.

13.97 identificación de servicio; ID de servicio: Identifica el tipo de servicio para el que el usuario desea registrarse (son tipos posibles de servicios: telefonía, facsímil, videotexto, datos, etc.).

13.98 grupo de servicio: Proporciona información que identifica la audiencia objetivo de estaciones móviles que deben recibir los mensajes SMS o del servicio de difusión de teleservicio. Tiene "forma libre" en el sentido que la determinan y la entienden exclusivamente los puntos extremos del protocolo (por ejemplo, para la difusión de teleservicios los puntos extremos son el centro de mensajes y los móviles).

13.99 tipo de servicio: Se refiere a los tipos de servicio posibles cuando se solicita el establecimiento de una sesión de datos por paquetes (por ejemplo, voz y datos).

13.100 identificación de sesión; ID de sesión: Suministrado por la PSCAF (cuando se recibe una petición de "anuncio"), tiene por finalidad eliminar la ambigüedad de la respuesta al MT en una etapa posterior de un procedimiento de "establecimiento/restablecimiento de una sesión de datos". Constituye un identificador inequívoco de cada sesión de datos por paquetes en un entorno de sesiones múltiples.

13.101 dirección de fuente de sesión: En caso de sesiones múltiples, es la información de dirección de una sesión (es decir, la ID de la sesión) y se utiliza para asociar la señal de respuesta "cancelación de registro" con la sesión que se termina.

13.102 datos SS (servicios suplementarios): Contiene información adicional relativa a la invocación de servicios suplementarios. Dependiendo del servicio invocado, puede contener la información siguiente:

– Una lista con los números de todas las partes llamadas involucradas.

– El número de la parte llamada involucrada.

13.103 datos secretos compartidos (SSD, *shared secret data*): Cantidad que se obtiene a partir de la clave A y que se utiliza para la autenticación del abonado en los entornos "originario" e "itinerante" en sistemas SSD. Los SSD se dividen en dos subconjuntos distintos, SSD-A y SSD-B, utilizados para la respuesta de autenticación y para la generación de la clave de criptación, respectivamente.

13.104 evento SS (servicios suplementarios): Indica el servicio suplementario para el que se envía una notificación de invocación a la SCF. Puede indicar uno de los servicios siguientes:

– Transferencia de llamada explícita.

– Reflexión de llamada.

– Llamada multipartita.

13.105 código de servicio suplementario: Indica un servicio suplementario o un conjunto de servicios suplementarios.

13.106 datos de servicio suplementario: Elemento de información general que incluye datos utilizados por distintos servicios suplementarios, por ejemplo, información de reenvío de llamada o de prohibición de llamada.

13.107 ID de CCF objetivo: Utilizado para indicar la función de control de llamada (CCF) en la que debe establecerse el portador de acceso.

13.108 información de capacidad del terminal (TC, *terminal capability*): Información de la capacidad del terminal que especifica los servicios que el terminal puede soportar.

13.109 tipo de teleservicio: Se refiere a servicios tales como mensajería, voz, facsímil, radiobúsqueda, etc.

13.110 número de referencia temporal (TRN, *temporary reference number*): Número que asigna la SCF en la red originaria y que se utiliza para establecer la correlación entre la conexión de voz (entre el móvil del usuario y el centro de servicio al cliente) y la conexión de datos (entre la red servidora y la red originaria), durante una sesión de OTASP.

13.111 estado del terminal: Identifica el estado del terminal móvil y de su usuario es (es decir, MT activo o inactivo, servicio concedido, prohibición establecida por el operador, etc.).

13.112 información de tratamiento de terminación: Utilizado para proveer información sobre como debe tratarse un intento de terminación particular (por ejemplo, la respuesta a una radiobúsqueda).

13.113 petición de tratamiento de terminación: Utilizado para preguntar sobre como debe tratarse un intento de terminación particular (por ejemplo, si debe o no debe responderse a una radiobúsqueda).

13.114 identificación temporal de usuario móvil (TMUI, *temporary mobile user ID*): Utilizado para direccionar un terminal móvil y para identificar un usuario IMT-2000. Lo asigna y utiliza de forma temporal la red visitada para preservar el anonimato.

13.115 identificación de fuente de asignación de identificador temporal de usuario móvil: Utilizada para identificar la LMFv que ha asignado el TMUI.

13.116 temporizador de expiración de identificador temporal de usuario móvil: Utilizado junto con el TMUI para proporcionar al usuario una confidencialidad mejorada.

13.117 selección de red de tránsito: Indica la red o redes de tránsito que se solicitan en una llamada (véase la Recomendación UIT-T Q.762 [11]).

13.118 petición de información de UIM: Hace referencia a la información que solicita el UIM para proporcionar:

– el número llamado asociado con el número de marcación abreviada;
– información relativa a la autenticación específica;
– información relativa a un abonado específico;
– información relativa a una dirección específica.

13.119 respuesta de información módulo de identidad de usuario: Contiene la información solicitada del UIM.

13.120 valor de la clave del módulo de identidad de usuario (UIMKEY, *UIM key value*): Número "X" generado por el UIM y que se envía a la red originaria (es decir, a la LMFh), a través de la red visitada, durante el proceso de generación de la clave de autenticación de la OTASP. Se calcula como:

$$X = g^x \text{ Mod } N$$

13.121 error de usuario: Indica que ha ocurrido un error durante la gestión del servicio de mensajes cortos.

13.122 velocidad de información del usuario: Utilizado para indicar la velocidad real de la información a la que se transmite sobre el portador radioeléctrico y el canal terrestre. También puede indicar la velocidad de adaptación si la velocidad de información del usuario y la velocidad de la capacidad portadora del portador radioeléctrico no coinciden.

13.123 clave de cifrado del plano de usuario (UPCKEY, *user plane cipher key*): Contiene la clave que debe utilizarse para el cifrado de voz/datos enviados en ambos sentidos sobre la interfaz radioeléctrica. Su presencia también indica a la red servidora/visitada que active el cifrado del plano de usuario.

13.124 informe de cifrado del plano de usuario (UPCRPT, *user plane ciphering report*): Enviado por la red visitada/servidora a la red originaria para indicar si se ha activado el cifrado del plano de usuario.

13.125 perfil de usuario: Son los datos que especifican los servicios suscritos y los datos asociados a la autenticación para el usuario IMT-2000. Además, puede incluir los atributos siguientes:
– datos de suscripción de llamada de grupo y/o de difusión (si procede),
– número de directorio de usuario móvil IMT-2000 (IMDN), por ejemplo, un número que se puede marcar,
– ID de usuario móvil IMT-2000 (IMUI),
– ID temporal de usuario móvil IMT-2000 (TMUI),
– estado del terminal,
– información de ubicación del usuario/terminal,
– datos del servicio básico (por ejemplo, servicios portadores suscritos),
– teleservicios (por ejemplo, datos de suscripción de llamada de grupo y/o difusión),
– datos de servicios suplementarios,
– servicios/facilidades fijados por el operador (por ejemplo, datos de prohibición de llamada),
– servicios/facilidades fijados por el abonado (por ejemplo, datos de cribado de llamadas),
– datos de restricción de itinerancia,
– datos de suscripción regional, y
– datos de suscripción del VHE.

13.126 esquema de codificación de datos USSD: Contiene información del alfabeto y el lenguaje utilizado para la información no estructurada en una operación de datos de servicio suplementario no estructurado.

13.127 cadena USSD: Contiene una cadena de información no estructurada en la operación de datos de un servicio suplementario no estructurado. El usuario móvil o la red envía la cadena.

13.128 identificador de zona: Proporciona una indicación del área geográfica (por ejemplo, todas las RAN o partes de una RAN en una red servidora o en toda la red servidora) en la que debe difundirse un mensaje, como es el caso de los mensajes de difusión de teleservicio. Tiene un "formato libre" en el sentido de que éste está determinado y es entendido solamente por los puntos extremos del protocolo (en el caso de la difusión de teleservicio, los puntos extremos son el centro de mensajes y la red servidora).

ANEXO A

Lista de módulos de procedimientos comunes utilizados en esta Recomendación

Nombre del procedimiento común	N.º cláusula	Procedimiento utilizado en
Cálculo de la autenticación	6.1.2.2.3	Autenticación de usuario.
Liberación de llamada	7.5	Supresión de una parte (iniciada por parte raíz e iniciada por hoja).
Encaminamiento de llamada	7.3	"Instrucción originaria directa" de VHE, adición de parte (iniciada por parte raíz).
Obtención de contraseña	11.1	Registro de contraseña.
Recuperación de la ID del usuario IMT-2000	6.2.2	Actualización de ubicación de terminal.
Actualización de LAI	6.2.2.1.5	Registro de ubicación de terminal, actualización de ubicación de terminal.
Actualización de ubicación		Registro de ubicación de terminal.
Liberación de llamada móvil	7.5	Supresión de una parte.
Llamada entrante móvil	7.4	Adición de una parte.
Asistencia de recurso especializado	Procedimiento de RI	"Instrucción originaria directa" de VHE.
Inicio de cifrado	6.1.2.5	Registro de ubicación de terminal, actualización de ubicación de terminal, llamada inicial saliente de móvil, llamada inicial entrante a móvil, mensaje corto originado en el móvil, mensaje corto terminado en el móvil.
Transferencia de perfil de abonado	6.2.1.3	Restauración de datos de la LMF
Registro de ubicación de terminal	6.2.3.1	Llamada inicial saliente de móvil, sesión de datos por paquetes.
Radiobúsqueda de terminal	7.2	Llamada inicial entrante a móvil, mensaje corto terminado en el móvil.
Asignación de TMUI	6.1.2.6	Registro de ubicación de terminal, actualización de ubicación de terminal, llamada inicial saliente de móvil, llamada inicial entrante a móvil.
Interrogación de TMUI	6.2.2.1.1	Actualización de ubicación de terminal, desincorporación, radiobúsqueda de terminal, incorporación.
Actualización de TMUI	6.2.2.1.4	Asignación de TMUI.

Nombre del procedimiento común	N.º cláusula	Procedimiento utilizado en
Autenticación de usuario	6.1.2	Registro de ubicación de terminal, actualización de ubicación de terminal, desincorporación, llamada inicial saliente de móvil, llamada inicial entrante a móvil, mensaje corto originado en el móvil, mensaje corto terminado en el móvil, incorporación.
Recuperación de la ID del usuario	6.2.2.2	Registro de ubicación de terminal, desincorporación, incorporación.
Interrogación de información de usuario	6.2.1.2	Interrogación de información de usuario, mensaje corto terminado en el móvil.
Invocación de servicio de VHE	9	Llamada inicial saliente de móvil, encaminamiento de llamada, llamada inicial entrante a móvil.

APÉNDICE I

Cobertura de la Recomendación Q.1721 del cuadro 1/Q.1701, Requisitos del conjunto de capacidades 1

En este apéndice se utiliza el cuadro 1/Q.1701 que se reproduce íntegramente añadiendo una tercera columna para indicar si la Recomendación UIT-T Q.1721 cubre la capacidad identificada.

Las entradas de la tercera columna deben interpretarse como sigue:

Entrada	Interpretación
No Aplicable	Capacidad de un tipo tal que los flujos de información específicos no están asociados a ella.
Sí	Capacidad soportada por los flujos de información descritos en la cláusula indicada.
No	Esta capacidad no es soportada por los flujos de información de Q.1721. Se presentan las razones de ello.
Parcial	Esta capacidad se soporta parcialmente por los flujos de información que se describen en la cláusula indicada. Los aspectos que no se soportan se indican claramente junto a la razón de ello.

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000

Categoría	Capacidades	Cobertura
A) Capacidad existente	1 Capacidades y servicios centrales móviles y fijos de segunda generación existentes utilizados ampliamente, posiblemente mejorados	1 No aplicable
B) Objetivos a largo plazo	1 Soportar capacidades de red que mejoren con claridad las capacidades de sistema de redes inalámbricas 2G (de segunda generación) utilizadas ampliamente en los dominios de voz, datos, mensajería, imágenes y multimedios, incluidos: 1.1 Itinerancia mejorada 1.2 Velocidades de datos superiores 1.3 Servicios inalámbricos multimedios y de Internet	1 No aplicable. Las capacidades necesarias para soportar estas mejoras se tratan más adelante en este cuadro

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000 *(continuación)*

Categoría	Capacidades	Cobertura
C) Capacidad de portador	1 Para acceso terrenal: 1.1 Por lo menos 144 kbit/s en entornos radioeléctricos de vehículos, BER ≤ 10^{-6}, tanto para servicios de circuito como por paquetes 1.2 Por lo menos 384 kbit/s en entornos radioeléctricos de exteriores a interiores y personales, BER ≤ 10^{-6}, tanto para servicios de circuitos como por paquetes 1.3 Por lo menos 2048 kbit/s en entornos radioeléctricos interiores de oficina, BER ≤ 10^{-6}, tanto para servicios de circuitos como por paquetes	1 Sí. Subcláusula 7.1
	2 Gama de QoS con negociación independiente: 2.1 Tiempo real/tiempo diferido 2.2 Características de retardo 2.3 Tasa de errores en los bits aceptable máxima 2.4 Velocidad binaria/caudal	2 Sí. Subcláusula 7.1
	3 Soporte de servicios por paquetes (tanto en la interfaz radioeléctrica como en las interfaces fijas)	3 Sí. Subcláusula 8.4
	4 Para la interfaz de acceso por satélite: 4.1 Cabe esperar que las velocidades de transmisión de datos desde cualquier usuario del componente de satélite de IMT-2000 vayan de 9,6 kbit/s a 144 kbit/s, dependiendo del entorno de explotación y del tipo de terminal	4 Sí. Subcláusula 7.1
	5 Configuraciones de comunicación: 5.1 PTP: Servicio bidireccional punto a punto (conexión de tipo 1) 5.2 PTM: Servicio punto a multipunto (conexión de tipo 2) 5.2.1 Distribución 5.2.2 Capacidades de multidistribución 5.2.2.1 Preasignadas, es decir, seleccionadas en el origen cuando se establece la llamada	5 Sí. Cláusulas 7 y 8
	6 Tipo de comunicación: 6.1 CLNS: Servicio de red sin conexión 6.2 CONS: Servicio de red con conexión	6 Sí. Capacidad de portador
	7 Simetría de los enlaces de acceso: 7.1 Simétricos (velocidades binarias iguales en transmisión y en recepción) 7.2 Asimétricos (velocidades binarias distintas en transmisión y en recepción)	7 Sí. Capacidad de portador
	8 Tráfico con velocidad binaria fija y variable	8 Sí. Capacidad de portador

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000 *(continuación)*

Categoría	Capacidades	Cobertura
	9 Procedimientos de interfuncionamiento de portador: 9.1 Adaptación/conversión de conexión de portador 9.2 Portador, componente de servicio y teleservicio 9.2.1 Correspondencia 9.2.2 Negociación 9.2.3 Procedimientos de sustitución	9 No tratado explícitamente
D) Capacidades de red acceso – Generalidades	1 Soporte para servicios por paquetes incluidos: 1.1 Velocidad binaria de entrega negociable (caudal de pico y medio) 1.2 Tolerancia de retardo negociable 1.3 Clases de fiabilidad negociable (determinan la probabilidad de pérdida de datos, entrega fuera de secuencia, entrega duplicada y datos corrompidos)	1 Sí. Cláusula 8
	2 Soporte de: 2.1 Velocidad binaria constante con temporización: con conexión 2.2 Velocidad binaria variable con temporización: con conexión 2.3 Velocidad binaria variable sin temporización: sin conexión 2.4 Velocidad binaria variable sin temporización: con conexión 2.5 Recuperación de capa de enlace efectiva	2 Sí. Cláusulas 7, 8; QoS
	3 Capacidades de control de recursos radioeléctricos: 3.1 Comprobación y supervisión del canal radioeléctrico y del entorno radioeléctrico 3.1.1 Comprobación de la calidad del canal radioeléctrico 3.1.2 Comprobación de la diversidad macro 3.2 Atribución y desatribución a recursos radioeléctricos 3.3 Control y establecimiento de potencia de radiofrecuencia	3 No. Gestión de recurso radioeléctrico
	4 Soporte de aplicaciones FWA con funcionalidad similar a la de la RDSI	4 No se trata específicamente

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000 *(continuación)*

Categoría	Capacidades	Cobertura
E) Capacidades de red central – Generalidades	1 Soporte de: 1.1 Velocidad binaria constante con temporización: con conexión 1.2 Velocidad binaria variable con temporización: con conexión 1.3 Velocidad binaria variable sin temporización: sin conexión 1.4 Velocidad binaria variable sin temporización: con conexión	1 Sí. Cláusulas 7, 8. QoS y capacidad portadora.
	2 Soporte de comunicaciones de circuitos y paquetes para tratamiento de voz, datos y vídeo simultáneamente	2 Sí. Cláusulas 7 y 8
	3 Interfuncionamiento: 3.1 Con RDSI: soporte de servicios del tipo RDSI a 56 kbit/s, 64 kbit/s, 128 kbit/s y 144 kbit/s (incluido canal D) 3.2 Con CS 2.1 de la RDSI-BA 3.3 Con RDP X.25: soporte de portador de acceso PAD a velocidades de 300, 1200, 2400, 4800 y 9600 bit/s. Soporte de portador en modo paquetes X.25 a velocidades de 2400, 4800 y 9600 bit/s 3.4 Con redes IP para contextos iniciados por usuario y por red 3.5 Con la RTPC (voz, fax y datos vía módem)	3 No tratado explícitamente
	4 Movilidad: 4.1 Movilidad de terminal 4.2 Movilidad personal 4.3 Movilidad de servicio (por ejemplo, entorno originario virtual)	4 Sí. Cláusula 6.
	5 Aplicaciones de datos e Internet: 5.1 Las IMT-2000 proporcionarán interfuncionamiento con redes IP (incluidos Intranet, IPv4 e IPv6) 5.2 Las IMT-2000 pueden proporcionar servicios de tipo Internet únicamente	5 Sí. Subcláusula 8.5
	6 Itinerancia global (a escala mundial) e interoperabilidad de servicio entre miembros de la familia IMT-2000	6 Sí. Cláusula 6 para itinerancia y cláusula 9 para servicios de VHE
	7 Capacidades de transporte de red medular: 7.1 Soporte de funcionamiento con paquetes conmutados y circuitos conmutados 7.2 Soporte de arquitectura de red de miembro de familia evolucionado (PDH/SDH/ATM) 7.3 Soporte de interfaces abiertas a servidores de RI, servidores de proveedores de servicio especializados	7 Sí. Cláusulas 7 y 8

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000 *(continuación)*

Categoría	Capacidades	Cobertura
F) Capacidades de red – Control de llamada	1 Separación de canal de llamada y portador/conexión de control	1 Sí. Cláusula 7
	2 Dirección/nombre/directorio único para un usuario, para facilitar la transportabilidad de servicio, sin perjuicio de múltiples números de abonado	2 No tratado explícitamente
	3 Soporte de CS-1/2 de la RI para permitir acceso a servicios basados en la RI	3 Sí. Cláusula 9
	4 Dotación de funcionalidad de movilidad BCSM mejorada	4 Sí. Cláusula 9
	5 Múltiples llamadas simultáneas por terminal o número de directorio	5 No tratado explícitamente
	6 Almacenamiento y transmisión de correo multimedios	6 No. Función de una FE MM.
	7 Llamadas multimedios (véanse conjuntos 1 y 2.1 de capacidades de señalización de banda ancha, incluidos conexiones adición/sustracción para configuraciones de comunicación punto a punto y parte adición/sustracción)	7 Sí. Cláusula 8
	8 Procedimientos de llamada de interconexión de redes: 8.1 Pertenecientes a distintas redes IMT-2000 (interconexión de redes entre miembros de la familia IMT-2000) 8.2 Pertenecientes a redes IMT-2000 y a redes fijas [RTPC, RDPC, INTERNET(IP), RDSI(BA)]	8 No tratado explícitamente
	9 Llamada de emergencia: 9.1 Identificación de la llamada de emergencia 9.2 Tratamiento de la llamada de emergencia 9.3 Ubicación del llamante de emergencia	9 Sí. Subcláusula 7.6
	10 Llamada prioritaria: 10.1 Identificación de la llamada prioritaria 10.2 Tratamiento de la llamada prioritaria	10 Sí. Subcláusula 7.7
	11 Posicionamiento geográfico de un terminal/usuario: 11.1 Determinación de la posición geográfica 11.2 Notificación de la posición geográfica 11.3 Control de usuario sobre la información de servicio de ubicación suscrita, incluida la capacidad para evitar la inhabilitación involuntaria de la funcionalidad de ubicación de servicio obligatoria	11 Sí. Subcláusula 6.2
	12 Independencia de las características de conexión para llamadas multiconexión.	12 Sí. Subcláusula 8.4

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000 *(continuación)*

Categoría	Capacidades	Cobertura
G) Capacidades de red – Procedimientos de seguridad	1 Cifrado y autenticación de usuario para los modos circuito y paquetes	1 Sí. Subcláusula 6.1.2
	2 Identificación del terminal incluida la capacidad de detectar terminales robados y no autorizados	2 No tratado explícitamente
	3 Autenticación mutua usuario-red	3 Sí. Subcláusula 6.1.2
	4 Soporte de mecanismos de autenticación y cifrado dependientes del servicio	4 No tratado explícitamente
	5 Control del uso inadecuado de una red, es decir, impedir la utilización fraudulenta por un usuario no autorizado o por un usuario autorizado que excede su autoridad	5 No tratado explícitamente
	6 Cifrado en la interfaz radioeléctrica (información de usuario y de control)	6 No. Asunto de la interfaz radioeléctrica
	7 Intercepción legal (según los requisitos de regulaciones nacionales)	7 No tratado explícitamente
	8 Privacidad de los datos relativos al usuario y al abonado (incluida la identidad de usuario)	8 Asunto de gestión
	9 Privacidad de los datos de facturación	9 Asunto de gestión
	10 Privacidad de los mensajes de usuario	10 Asunto de gestión
	11 Negociación de mecanismos de autenticación entre las redes de usuario, servidora y originaria	11 No tratado explícitamente
	12 Información de eventos y limitación de eventos para soportar la prevención de fraudes	12 Función interna de la AMF
H) Capacidades de red – Atribución de recursos	1 Atribución basada en QoS negociada	1 No tratado explícitamente
	2 Controles de sobrecarga	2 No tratado explícitamente
	3 Soporte con uso eficaz del espectro para configuraciones de servicios mezclados (por ejemplo, servicios de baja velocidad binaria/alta velocidad binaria, tiempo real/tiempo diferido)	3 Asunto de la interfaz radioeléctrica
	4 Optimización de encaminamiento en el establecimiento de la llamada y durante la llamada	4 No tratado explícitamente
I) Capacidades de red – Numeración y direcciona-miento	1 Soporte de portabilidad de numeración y direccionamiento	1 No tratado explícitamente
	2 Plan de identificación, direccionamiento y numeración:	2 No tratado explícitamente
	2.1 Gestión de identidad	
	2.1.1 Terminal	
	2.1.2 Usuario móvil internacional	
	2.1.3 Abonado RDSI	
	2.1.4 Grupo multidistribución	
	2.2 Soporte de planes existentes y avanzados de direccionamiento y numeración, incluidos:	
	2.2.1 Recomendación E.164	
	2.2.2 Recomendación E.212	

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000 *(continuación)*

Categoría	Capacidades	Cobertura
	2.2.3 Recomendación E.213 2.2.4 Recomendación X.121 2.2.5 NSAP (punto de acceso al servicio de red) 2.2.6 IPv4/v6 2.2.7 Direcciones del tipo correo electrónico e Internet 2.2.8 Otros mecanismos, por ejemplo, llamada por nombre 2.3 Encapsulado y correspondencia de dirección 2.4 Soporte de direccionamiento de la Recomendación E.214 (título global móvil terrestre)	
J) Capacidades de red – Tasación y contabilidad	Estos elementos reflejan las elecciones identificadas para la tasación y contabilidad de las IMT-2000	
	1 Perfiles de usuario de facturación y tasación normalizadas	1 Véase Rec. M.3210
	2 Información de eventos normalizada y registro de utilización detallada: 2.1 Registro detallado de llamada 2.2 Generación de información de tasación para: 2.2.1 Llamadas de circuitos conmutados 2.2.2 Sesiones de transmisión de datos por paquetes 2.2.3 Servicios realizados exclusivamente intercambiando información de señalización 2.2.4 Transmisión de datos en un canal transparente UIM red originaria	2 Véase Rec. M.3210
	3 Nuevos mecanismos de tasación [por ejemplo, volumen (número de paquetes o bytes, incluidos parejas de dirección origen/destino), QoS, duración, etc.]	3 Véase Rec. M.3210
	4 Tasación en tiempo real	4 Véase Rec. M.3210
	5 Mecanismos flexibles de tasación/facturación: 5.1 Notificación al usuario de la tasación antes, durante y después de eventos significativos 5.2 Transmisión casi en tiempo real de registros de datos de utilización	5 No. Existen aspectos significativos no resueltos relativos a las configuraciones de negocio de interfuncionamiento, compartición de tarifas, conversión de divisas, precisión, etc.
	6 Tasación de terceros (por ejemplo, tasación a otras partes durante llamadas multipartitas)	6 Véase Rec. M.3210
	7 Facturación preabonada	7 No: es un asunto de la red servidora
	8 Facturación y tasación en función de la ubicación	8 Véase Rec. M.3210
	9 Acceso en tiempo real a la información de facturación	9 Véase Rec. M.3210

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000 *(continuación)*

Categoría	Capacidades	Cobertura
K) Capacidades de red – Itinerancia	1 Interoperabilidad e itinerancia en la familia de sistemas IMT-2000 que utiliza una única suscripción	1 Sí. Cláusula 6
	2 Capacidad para complementar la gestión de movilidad con lógica de servicio de tipo RI	2 Sí. Cláusula 9
	3 Capacidad para complementar el control de autenticación con lógica de servicio de tipo RI. Esta capacidad no incluye la generación de parámetros de autenticación (por ejemplo, tripletas)	3 Sí. Cláusula 9
	4 Movilidad e itinerancia global:	4 Sí. Cláusula 6
	4.1 Gestión de ubicación, incluida actualización automática	
	4.2 Incorporación, actualización y cancelación de usuario	
	4.3 Incorporación, actualización, activación, desactivación y cancelación de comprobación de servicio	
	4.4 Gestión y control de la base de datos de perfil de usuario	
	4.5 Gestión y control de la base de datos de seguridad y autenticación	
L) Capacidades de red – Portabilidad del servicio	1 El sistema servidor debería ser capaz de permitir el soporte de un servicio de usuario en itinerancia a partir de la información del perfil de usuario	1 Sí. Cláusula 9
	2 Portabilidad de servicio transparente a los usuarios con otras redes IMT-2000 independientes de las tecnologías del entorno (es decir, celular, inalámbrico, satélite)	2 Sí. Cláusula 9
	3 Soporte a entornos originarios virtuales para permitir ofrecer a un usuario las mismas prestaciones de servicio cuando se encuentra en itinerancia que cuando está en la red originaria, para servicios específicos de operador:	3 Sí. Cláusula 9
	3.1 Comando directo a domicilio	
	3.2 Control de servicio de retransmisión	
	4 Soporte de UPT	4 No tratado explícitamente
	5 Soporte de gestión de perfil de servicio	5 Sí. Cláusula 12
	6 Soporte de servicios suplementarios normalizados	6 Sí. Cláusula 11
M) Servicios/ prestaciones de red – Traspaso	1 Soporta el traspaso de miembros entre familias	1 Asunto entre familias
	1.1 Soporte de estructura de célula jerárquica	
	1.1.1 Transferencia y traspaso de llamadas a través de las capas de célula	
	1.1.2 Gestión de ubicación en múltiples capas de célula	

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000 *(continuación)*

Categoría	Capacidades	Cobertura
N) Servicios/ prestaciones de red – Puesta en servicio	1 Puesta en servicio radioeléctrico: 1.1 Soporte de servicios de voz y datos 1.2 Teledescarga y telecarga (por ejemplo, parámetros de servicio) 1.3 Soporte para seguridad y autenticación	1 Sí. Cláusula 12
O) Servicios/ prestaciones de red – Calidad de servicio	1 Basados en suscripción 2 Negociación de QoS durante la invocación del servicio 3 Renegociación de QoS durante una sesión de servicio (por ejemplo, llamada) 4 QoS de servicios multimedios tan buena como con acceso alámbrico (dependiendo de las clases de servicio de portador) 5 Calidad vocal equivalente a la de la transmisión alámbrica 6 Cumplen los requisitos de retardo mínimo (afecta a los temporizadores de señalización, etc.)	1 Sí 2 Sí. Cláusula 7 3 Sí. Subcláusula 8.1 4 Asunto de la interfaz radioeléctrica 5 Asunto de la interfaz radioeléctrica 6 No tratado explícitamente
P) Servicios/ prestaciones de red – Soporte suplementario	1 Acceso a teléfono inalámbrico 2 Redes privadas virtuales 3 Servicios de soporte de operador 4 Servicios basados en IP 5 Acceso por satélite: consideraciones para la gestión de grandes retardos de enlace, de potencia limitada y de anchura de banda 6 Transparencia de medios (es decir, datos de usuario entregados sin cambios)	1 No tratado explícitamente 2 No tratado explícitamente 3 No tratado explícitamente 4 Sí. Cláusula 8 5 No tratado explícitamente 6 No tratado explícitamente
Q) Servicios/ prestaciones de red – Terminales y módulos de identidad de usuario (UIM)	1 Modelo de red para soportar: 1.1 Red con teledescarga y telecarga de perfiles de usuario, información de datos, etc., para soportar la funcionalidad UIM a través de canales de comunicación funcionales 1.2 Terminales configurables por soporte lógico, para flexibilidad de funcionamiento (por ejemplo, para soportar aplicaciones proactivas) 1.3 Suficientemente flexible para soportar futuras mejoras en equipos radioeléctricos definidos por soporte lógico, para flexibilidad de funcionamiento	1 Sí. Cláusula 12

Cuadro I.1/Q.1701 – Conjunto de capacidades 1 para las IMT-2000 *(fin)*

Categoría	Capacidades	Cobertura
	2 Móviles y UIM con capacidades de telecarga por medios radioeléctricos para datos y aplicaciones. Deberían establecerse procedimientos adecuados para proteger información sensible y confidencial transferida por medios radioeléctricos	2 Sí. Cláusula 12
	3 Llamadas múltiples en un único terminal	3 No tratado explícitamente
	4 Soportar itinerancia del terminal con UIM amovible o integrado y proporcionar la información necesaria desde el UIM para asociar un abonado con el MT y para personalizar el MT	4 Sí. Cláusula 6
	5 Movilidad personal basada en un UIM separado del terminal (tarjeta de IC)	5 No tratado explícitamente
	6 Registro múltiple de un usuario en varios terminales para diferentes servicios	6 No tratado explícitamente
R) Capacidades de red – Control de transferencia de paquetes	1 Registro/autenticación	1 Sí. Cláusula 6
	2 Asignación de dirección: 2.1 Estática 2.2 Dinámica	2 No tratado explícitamente
	3 Modo reposo para soportar la conservación de potencia de la batería	3 De la interfaz radioeléctrica
	4 Encaminamiento de paquetes óptimo	4 No tratado explícitamente
	5 Soporte de protocolo múltiple	5 No tratado explícitamente
	6 Compresión de datos	6 No tratado explícitamente
	7 Interconexión entre redes (por ejemplo, fugas, soporte móvil IP)	7 Sí. Cláusula 8
	8 Identificación de ubicación	8 Sí. Cláusula 6
	9 Equilibrado de carga entre los canales RF	9 Asunto de la interfaz radioeléctrica
	10 Registros de dirección simultáneos múltiples (por ejemplo, direcciones IP) en un único terminal	10 No tratado explícitamente
	11 Acceso con prioridad (para registro y transferencia de datos)	11 Sí. Subcláusula 7.1.7
	12 Sesiones multimedios	12 Sí. Cláusula 8

APÉNDICE II

Generación de la clave A

II.1 Introducción

La generación de la clave A se soporta en la OTASP utilizando el método de criptación con clave pública. Un ejemplo de dicho método es el método de criptación con clave pública de Diffie-Hellman que se describe a continuación. El método Diffie-Hellman ofrece algunas ventajas en cuanto que está disponible públicamente y es escalable, es decir, los valores fijados en el algoritmo pueden ser ajustados por el operador para conseguir el nivel de seguridad deseado. El MS y la red establecen el conjunto de valores que se soportan para la generación de la clave A con anterioridad al proceso de generación de la clave A.

II.2 Generación de la clave A utilizando el algoritmo de Diffie-Hellman

En el esquema Diffie-Hellman, se genera una clave A en la UIMF y en la LMFh/AMF utilizando información que se comparte entre ambas entidades. La LMFh/AMF genera valores para un módulo público N y una primitiva g. La LMFh/AMF genera una clave secreta *y*, que es un número aleatorio de al menos 160 bits. La LMFh/AMF envía a la UIMF: N, g, e Y, donde:

$$Y = g^y \text{ Mod } N$$

Cuando se reciben N, g e Y, la UIMF genera una clave secreta, x, que es un número aleatorio de al menos 160 bits, calcula y envía X a la LMFh/AMF, donde:

$$X = g^x \text{ Mod } N$$

La clave A de la UIMF se calcula como los 64 bits menos significativos de:

$$Y^x \text{ mod } N = (g^y)^x \text{ mod } N$$

La LMFh/AMF calcula el mismo valor de la clave A como los 64 bits menos significativos de:

$$X^y \text{ mod } N = (g^x)^y \text{ mod } N$$

Después de la generación con éxito de la clave A, la LMFh/AMF y la UIMF intercambian confirmaciones. La generación de x por parte de la UIMF y la generación de N, g e y por parte de la LMFh/AMF quedan fuera del ámbito de esta Recomendación. Los requisitos y propiedades de la generación de estos números pueden obtenerse de la literatura actualizada sobre criptografía públicamente disponible.

APÉNDICE III

Bibliografía

Las referencias siguientes no se mencionan explícitamente en la parte principal de esta Recomendación, pero proporcionan información de referencia útil adicional e información conexa.

[1] Recomendación UIT-T M.3100 (1995), *Modelo genérico de información de red.*

[2] Recomendación UIT-R M.687-2 (1997), *Telecomunicaciones móviles internacionales (IMT-2000).*

[3] Recomendación UIT-R M.816-1 (1997), *Marco para los servicios que prestarán las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[4] Recomendación UIT-R M.817 (1992), *Telecomunicaciones móviles internacionales-2000 (IMT-2000). Arquitecturas de red*.

[5] Recomendación UIT-R M.818-1 (1993), *Funcionamiento por satélite en las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[6] Recomendación UIT-R M.819-2 (1997), *Telecomunicaciones móviles internacionales-2000 (IMT-2000) para los países en desarrollo.*

[7] Recomendación UIT-R M.1034-1 (1997), *Requisitos de las interfaces radioeléctricas para las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[8] Recomendación UIT-R M.1035 (1993), *Marco general para el estudio de la funcionalidad de las interfaces radioeléctricas y del subsistema radioeléctrico en las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[9] Recomendación UIT-R M.1078 (1993), *Principios de seguridad para las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[10] Recomendación UIT-R M.1167 (1995), *Marco general sobre la componente de satélite de las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[11] Recomendación UIT-R M.1168 (1995), *Marco general para la gestión de las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[12] Recomendación UIT-R M.1223 (1997), *Evaluación de los mecanismos de seguridad para las IMT-2000.*

[13] Recomendación UIT-R M.1224 (1997), *Vocabulario de términos de las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[14] Recomendación UIT-T F.115 (1995), *Objetivos de servicio y principios para los futuros sistemas públicos de telecomunicaciones móviles terrestres.*

[15] Recomendación UIT-T F.116 (2000), *Características del servicio y disposiciones operacionales en las telecomunicaciones móviles internacionales-2000 (IMT-2000).*

[16] Recomendación UIT-T F.700 (1996), *Recomendación marco sobre los servicios audiovisuales/multimedia.*

[17] Recomendación UIT-T I.211 (1993), *Aspectos de servicio de la red digital de servicios integrados de banda ancha*.

[18] Recomendación UIT-T I.374 (1993), *Recomendación marco sobre "capacidades de red para servicios multimedios". (Esta Recomendación ya no está en vigor a partir de 1998, reemplazada por I.375.1 e I.375.2.)*

[19] Recomendación UIT-T Q.1001 (1988), *Aspectos generales de las redes móviles terrestres públicas.*

[20] Recomendación UIT-T Q.1290 (1998), *Glosario de términos utilizados en la definición de redes inteligentes.*

[21] Recomendación UIT-R M.1311 (1997), *Marco para la modularidad y los elementos radioeléctricos comunes en las IMT-2000.*

[22] Recomendación UIT-T E.214 (1988), *Estructura del título global de móvil terrestre para la parte de control de la conexión de señalización.*

[23] Recomendación UIT-R M.1457 (2000), *Especificaciones detalladas de las interfaces radioeléctricas para las telecomunicaciones móviles internacionales-2000.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie B	Medios de expresión: definiciones, símbolos, clasificación
Serie C	Estadísticas generales de telecomunicaciones
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedios
Serie I	Red digital de servicios integrados
Serie J	Transmisiones de señales radiofónicas, de televisión y de otras señales multimedios
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	RGT y mantenimiento de redes: sistemas de transmisión, circuitos telefónicos, telegrafía, facsímil y circuitos arrendados internacionales
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	**Conmutación y señalización**
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos y comunicación entre sistemas abiertos
Serie Y	Infraestructura mundial de la información y aspectos del protocolo Internet
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Ginebra, 2001