

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 953 741**

51 Int. Cl.:

H04W 8/00 (2009.01)

H04W 8/20 (2009.01)

H04W 8/26 (2009.01)

H04W 12/08 (2011.01)

H04W 12/40 (2011.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **16.08.2019** **PCT/EP2019/072049**

87 Fecha y número de publicación internacional: **27.02.2020** **WO20038847**

96 Fecha de presentación y número de la solicitud europea: **16.08.2019** **E 19753096 (7)**

97 Fecha y número de publicación de la concesión europea: **05.07.2023** **EP 3841769**

54 Título: **Método para personalizar una cooperación de UICC mejorada con un terminal**

30 Prioridad:

23.08.2018 EP 18306134

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

15.11.2023

73 Titular/es:

THALES DIS FRANCE SAS (100.0%)

6, rue de la Verrerie

92190 Meudon, FR

72 Inventor/es:

ANSLOT, MICHEL;

LAMBERTON, MARC y

BOUCKAERT, PHILIPPE

74 Agente/Representante:

DEL VALLE VALIENTE, Sonia

ES 2 953 741 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método para personalizar una cooperación de UICC mejorada con un terminal

5 La presente solicitud se refiere a telecomunicaciones y está vinculada al documento EP-3358869.

La presente invención se refiere en particular a la personalización y/o diversificación de UICC (tarjetas de circuito integrado universal) mejoradas inalámbricas.

10 La personalización consiste en instalar en una UICC que coopere con un terminal de telecomunicación un perfil de un MNO (operador de red móvil) mientras que la diversificación consiste en instalar en una UICC de los parámetros de MNO dados que permiten que la UICC se conecte a su MNO, siendo estos parámetros, por ejemplo, una IMSI (identidad de abonado móvil internacional), una Ki (una clave de cifrado), un ICCID (ID de tarjeta de circuito integrado) y un perfil que contiene parámetros para un algoritmo de autenticación (por ejemplo, OPc, Ri, Ci para el algoritmo de Milenage) inalámbrico. La
15 presente invención propone un procedimiento para personalizar y diversificar de forma inalámbrica una "UICC universal" fabricada con un perfil genérico no diversificado. Esta operación se realiza sobre el canal de señalización (SS7 o MAP) y optimiza el proceso de fabricación y los costes y no incurre en ningún coste de itinerancia de datos.

Se aplica a redes 2G a 5G y es compatible con los estándares 3GPP.

20 Se sabe que una UICC proporciona acceso seguro, identificable y autenticado a redes móviles. Desde su creación a principios de la década de 1990 al día actual, la UICC (por ejemplo, una tarjeta SIM) proporciona acceso seguro, identificable y autenticado a redes móviles. También es la parte principal del equipo suministrado por el operador utilizado por los consumidores cuando se conecta a la red móvil.

25 La SIM continuará proporcionando acceso seguro a las redes móviles del operador.

Hoy en día, toda la personalización y diversificación de la UICC se realiza en fábrica lo que conduce a costes de fabricación y complejidad: Todas las órdenes de UICC de los operadores también requieren que los archivos de entrada y salida
30 intercambien de forma segura los parámetros de UICC principales: ICCID, IMSI, Ki, clave OTA, claves PUK, OPC, Ri, Ci,...

Además de ser personalizadas y diversificadas, las UICC producidas tienen un período de validez limitado (típicamente de 3 a 12 meses). Después de la expiración de las UICC no vendidas, el MNO debe liberar recursos de sus sistemas de red y TI. Esto genera costes para el MNO para desintegrar y destruir estas UICC caducadas.

35 El documento US 2015/359026 A1 describe un método para personalizar una UICC que actúa conjuntamente con un terminal, en donde la UICC envía un mensaje de solicitud de conexión que comprende una IMSI con un MCC/MNC dado a un HSS que asigna una IMSI libre que pertenece a un operador y transfiere a la UICC la IMSI libre y otros datos de personalización, sobre los cuales la UICC se personaliza. El documento 3GPP S3-180843 describe un acuerdo de clave basado en Diffie-Hellmann en el que un HSS envía a unos primeros datos
40 criptográficos (exponente público efímero EDCH) de USIM, el USIM calcula una clave secreta mediante el uso de dichos primeros datos criptográficos, y el USIM envía a los segundos datos criptográficos de HSS (exponente público efímero EDCH), tras lo cual el HSS y el USIM calculan la misma clave secreta.

45 La invención tiene como objetivo realizar la personalización de la UICC y la diversificación dinámicamente cuando se usa la primera vez. La invención se define en las reivindicaciones.

Se conoce a partir de la solicitud de patente europea EP-3358868 que puede establecerse un canal de comunicación bidireccional entre un servidor y un elemento de seguridad que coopera con un terminal en una red
50 de telecomunicaciones celular para intercambiar datos y comandos. En esta solicitud de patente, se describe que este canal de comunicación bidireccional puede establecerse mediante:

- Enviar un primer mensaje de señalización de solicitud de fijación desde el terminal al servidor, comprendiendo el primer mensaje un MCC y un MNC del servidor, y al menos una parte de un identificador único del elemento de
55 seguridad, estando provisto el servidor con el identificador único;

- Enviar desde el servidor al elemento de seguridad, en al menos un primer mensaje de señal:

- Al menos un comando;

60 - Un identificador de correlación si se deben enviar mensajes adicionales desde el elemento de seguridad al servidor;

- Una primera carga útil que comprende datos;

65 - Ejecutar el comando en el elemento seguro.

En resumen, esta solicitud propone usar el canal de señalización (MAP o SS7) para intercambiar datos y comandos entre el elemento de seguridad (UICC) y un elemento de la red (un HSS mejorado también llamado D-HSS+).

La presente invención propone usar dicho mecanismo para intercambiar datos entre una UICC y un D-HSS para personalizar y/o diversificar una UICC sobre el canal de señalización.

Este fin se alcanza gracias a un método para personalizar una UICC que actúa conjuntamente con un terminal, comprendiendo el método:

- 5 i- Enviar desde la UICC a un D-HSS, que es un HSS mejorado, un mensaje de petición de conexión que comprende una IMSI con un MCC/MNC dado;
 - ii- Enviar desde el D-HSS hasta la UICC al menos un comando y unos primeros datos criptográficos;
 - 15 iii- Calcular en la UICC una clave secreta usando los primeros datos criptográficos;
 - iv- Enviar desde la UICC al D-HSS en al menos un mensaje de fallo de autenticación un comando y unos segundos datos criptográficos o una parte de los mismos;
 - 20 v- Repetir las etapas ii a iv hasta que la UICC contenga todos los primeros datos criptográficos y el D-HSS contiene los segundos datos criptográficos;
 - vi- Cuando el D-HSS contiene todos los segundos datos criptográficos, calcular en el D-HSS la misma clave secreta usando los segundos datos criptográficos completos;
 - 25 vii- Asignar por el D-HSS una IMSI libre que pertenece a un operador y que se transfiere desde el D-HSS a los datos de personalización de UICC que incluyen la IMSI libre y otros datos de personalización
 - 30 viii- Personalizar la UICC con los datos de personalización y la clave secreta. Preferiblemente, los datos de personalización se cifran con la clave secreta y luego se transfieren desde el D-HSS a la UICC.
- Ventajosamente, las primera y segunda claves criptográficas son números intercambiados de Diffie-Hellman, siendo los primeros datos criptográficos $A = g^a \text{ mod } p$ y siendo los segundos datos criptográficos $B = g^b \text{ mod } p$, donde p y g son números previamente acordados por el D-HSS y la UICC, siendo “a” un número aleatorio seleccionado por el D-HSS y siendo “b” un número aleatorio seleccionado por la UICC.
- Preferiblemente, la UICC envía en un mensaje de autenticación el IMEI del terminal con el que coopera y el D-HSS usa ese IMEI para seleccionar un MNO para el usuario del terminal.
- 40 Ventajosamente, el D-HSS envía un commando a la UICC en un mensaje de Ack de SAI para solicitar al usuario que introduzca el nombre de un MNO.
- Ventajosamente, el D-HSS personaliza la UICC enviando datos de personalización para el MNO seleccionado a la UICC, conteniendo los datos de personalización un IMSI, una ICCID, un OPc, una Ri y una Ci enviada en múltiples mensajes de Ack de SAI que comprenden comandos.
- 45 Preferiblemente, cada uno de los múltiples mensajes de Ack de SAI comprende diferentes IMSI utilizados para correlacionar el diálogo entre el D-HSS y la UICC.
- 50 Ventajosamente, una vez que la UICC se personaliza, el D-HSS proporciona la red MNO seleccionada con el IMSI/Ki para permitir que la UICC se comuniquen con la red MNO seleccionada.
- La invención también se refiere a una UICC dispuesta para implementar este método y un D-HSS dispuesto para implementar este método según las reivindicaciones 9 y 10.
- 55 La invención se entenderá mejor en la lectura de la siguiente descripción de las figuras que representan un conjunto completo de intercambios que permiten personalizar o diversificar una UICC+ (una UICC especial) según la invención. Más precisamente:
- 60 - Las figuras 1A, 1B y 1C representan etapas diferentes preliminares que permiten establecer un canal seguro entre un terminal que comprende un elemento de seguridad mejorado (UICC+) según la invención y un D-HSS mejorado;
 - Las figuras 2A y 2B representan tres opciones para asignar una IMSI a una UICC+ al nivel de un D-HSS+;
 - 65 - Las figuras 3A a 3C representan las etapas de personalización de una UICC+ de acuerdo con la invención.

El propósito de la invención es personalizar o diversificar una UICC+ utilizando solo los intercambios de MAP (Parte de aplicación móvil) que es un protocolo de capa de aplicación usado por diversos elementos en redes de núcleo móvil GSM, UMTS y GPRS para proporcionar servicios a usuarios de teléfonos móviles (terminales). La MAP se puede transportar usando protocolos SS7 “tradicionales” en TDM (T1 y E1) o sobre IP usando SIGTRAN.

La figura 1A representa diferentes etapas preliminares (1 a 18) que permiten establecer un canal seguro entre un terminal 10 que comprende un elemento de seguridad mejorado (UICC+) según la invención y un D-HSS 12 mejorado (llamado D-HSS+).

Se representan algunos otros actores: Una MME (Entidad de gestión de movilidad) 11, un HSS 13 de un MNO y un MNO 14.

En la etapa 1, un fabricante de UICC emite UICC únicas.

Por “única”, se entiende que todas las UICC emitidas son estrictamente idénticas o pueden emitirse con un MNO_ID dado. No se proporcionan por ninguna suscripción.

En las etapas 2 y 3, el MNO 14 proporciona previamente una pluralidad de IMSI y las envía al D-HSS+ 12. El D-HSS + 12 usará esta IMSI cuando un abonado selecciona el MNO.

En la etapa 3, el MNO carga archivos de entrada (IMSI) al D-HSS+ 12. Por lo tanto, el D-HSS+ 12 está provisto de estas IMSI.

En la etapa 4, el MNO 14 carga una lista de archivos de entrada de IMSI al D-HSS+ 12. Esta lista contiene el MNO_ID y las IMSI correspondientes. El D-HSS+ 12 se configura con la lista de MNO_ID, lo que permite identificar el MNO. Este MNO_ID se recupera directamente en el IMSI (primer caso, el operador del haz), o se configura en la UICC (segundo caso, MNO identificado), o se selecciona por el usuario (tercer caso). Estos tres casos se detallarán a continuación.

En la etapa 5, el usuario del terminal 10 cambia en su terminal que intenta conectarse a una red de telecomunicaciones. Para ello, se elige una IMSI aleatoria (RDN_IMSI) en la UICC+ en una lista o intervalo definido (por ejemplo, una IMSI entre 20.000). Esta lista o intervalo de IMSI se almacenan en la UICC+ al nivel de su fabricación. Los códigos MCC/MNC de esta IMSI son los de D-HSS+ 12 con el que se comunica la UICC+ en las etapas preliminares. En la etapa 6, el terminal 10 envía un mensaje de solicitud de conexión a la MME 11 que comprende la IMSI seleccionada aleatoriamente en el intervalo o la lista definidos. A continuación, la MME reenvía esta solicitud (etapa 7) en un mensaje de SAI (ENVIAR_INFO_AUTENTICACIÓN) al D-HSS+ 12.

En la etapa 8, el D-HSS+ 12 responde a esta solicitud con un mensaje Ack de SAI que contiene un vector compuesto de:

- Un comando (aquí DH1 para Diffie-Hellman 1)
- Una IMSI (aquí denominada SIGUIENTE_IMSI_1)
- Una clave de Diffie-Hellman (16 bytes, de 0 a 15), constituyendo esta clave unos primeros datos criptográficos
- Un valor XRES

La MME 11 reenvía el commando DH1, el SIGUIENTE_IMSI_1 y la clave criptográfica a la UICC+ 10 en un parámetro de solicitud de autenticación (AUTN). Un parámetro AUTN permite enviar 15 bytes.

En la etapa 10, la UICC+ calcula una clave secreta Ki basada en la clave de Diffie-Hellman recibida y almacena esta clave secreta Ki. También genera gracias a esta clave un código PUK, un código PUK2 y una clave OTA.

En la etapa 11, la UICC+ 10 envía un mensaje de fallo de autenticación a la MME 11 que contiene:

- La RDN_IMSI
- Un mensaje de fallo de sincronización
- Un testigo de resincronización AUTS que comprende un comando (aquí DH2), los ocho primeros bytes de unos segundos datos criptográficos (la longitud total de la clave criptográfica es 16 bytes) y un MNO_ID si dicho ID está disponible. Como se explicará más adelante, el método de la invención permite personalizar y diversificar la UICC+. Se debe hacer una personalización si el nombre de un MNO ya se almacena en la UICC+ (un haz de UICC+ se fabrica para un operador determinado). Una diversificación puede tener lugar cuando no está presente ningún nombre de MNO en la UICC+ 10 fabricada.

A continuación, la MME envía al D-HSS+ (etapa 12), en un mensaje de SAI, el RDN_IMSI y el testigo AUTS.

En la etapa 13, el D-HSS+ 12 envía a la MME 11 otro mensaje de SAI que contiene un vector que comprende un commando (NXT para “siguiente”), SIGUIENTE_IMSI_1 y otro valor XRES.

- 5 El comando y el SIGUIENTE_IMSI_1 se envían a continuación por la MME 11 a la UICC+ 10 en un mensaje de solicitud de autenticación.

En la etapa 15, la UICC+ 10 responde con un RES y la MME envía (en la etapa 16) un mensaje de actualización de ubicación al D-HSS+ 12.

- 10 En la etapa 17, el D-HSS+ 12 responde con un mensaje de Error de actualización de localización (itinerancia no permitida) ya que solo los ocho primeros bytes de la clave criptográfica de la UICC+ se han enviado al D-HSS+ 12 y el final del proceso de Diffie-Hellman necesita los 16 bytes de esta clave. En la etapa 18, la MME 11 envía un mensaje de rechazo de conexión a la UICC+ (no permitida PLMN).

- 15 La figura 1B muestra las siguientes etapas, etapa 19 después de la etapa 18.

En la etapa 19, la UICC+ 10 establece el valor de IMSI a SIGUIENTE_IMSI_1 y envía un comando de actualización al terminal. Este último ejecuta la actualización en la etapa 20.

- 20 En la etapa 21, la UICC+ 10 envía un mensaje de solicitud de conexión a la MME 11 que contiene SIGUIENTE_IMSI_1 y la MME 11 envía al D-HSS+ 12 esta IMSI en un mensaje de SAI (etapa 22).

- 25 En la etapa 23, el D-HSS+ 12 envía a la MME 11 en un mensaje de Ack de SAI un vector que contiene un commando NXT (siguiente), una nueva IMSI (SIGUIENTE_IMSI_2) y un XRES. Se utiliza la nueva IMSI (SIGUIENTE_IMSI_2) para que la EGM no reciba dos veces la misma IMSI. Esto es cierto para la siguiente descripción. La MME 11 reenvía el commando y la nueva IMSI en un mensaje de solicitud de autenticación a la UICC+ (etapa 24).

- 30 El comando NXT es interpretado por la UICC+10 como una solicitud para enviar la parte restante de los segundos datos criptográficos de 16 bytes. A continuación, envía (etapa 25) un mensaje de fallo de autenticación que contiene SIGUIENTE_IMSI_1, un fallo de sincronización (un estado del mensaje de fallo de autenticación) y un AUTS que comprende un comando (DH3) y los últimos ocho bytes (8 a 15) de la clave criptográfica. En la etapa 26, la MME reenvía el SIGUIENTE_IMSI_1 y el AUTS al D-HSS+ 12 en un mensaje de SAI.

- 35 El D-HSS+ 12 calcula entonces la clave Ki basada en las claves de Diffie-Hellman intercambiadas. También genera la clave de PUK, PUK2 y OTA (etapa 27). Este es el final del intercambio de Diffie-Hellman, la UICC+ 10 y el D-HSS+ 12 que tienen las claves necesarias para intercambiar secretos.

- 40 El establecimiento de un canal seguro se basa en este ejemplo en un protocolo de Diffie-Hellman. Algunos otros protocolos son, por supuesto, posibles para establecer un canal seguro, como por ejemplo mediante el uso de claves simétricas (SCP03, por ejemplo) o claves asimétricas (SCP11, por ejemplo). También es posible derivar una clave utilizando la IMSI aleatoria (o una parte de la misma) seleccionada por la UICC+ (esta clave se calcula en la UICC+ y, después de la transmisión de la IMSI aleatoria al D-HSS+ 12, calculada en esta D-HSS+ 12 usando toda la IMSI (MSIN de hecho) o una parte de la misma).

- 45 A continuación, el procedimiento continúa con etapas similares a las etapas 13 a 26 para recuperar el IMEI del terminal 10 (el terminal puede ser un terminal subvencionado perteneciente a un haz): En la etapa 28, el D-HSS+ 12 envía a la MME 11 en un mensaje de Ack de SAI un vector que comprende el commando SIGUIENTE, SIGUIENTE_IMSI_2 y XRES. La MME reenvía (etapa 29) el commando SIGUIENTE y SIGUIENTE_IMSI_2 a la UICC+ en un mensaje de solicitud de autenticación.

- 50 En la etapa 30, la UICC+ 10 responde a la MME 11 con un RES comprendido en un mensaje de respuesta de autenticación y la MME 11 envía un mensaje de actualización de localización al D-HSS+ 12 (etapa 31).

- 55 En la etapa 32, el D-HSS+ 12 responde con un mensaje de Error de actualización de localización (itinerancia no permitida).

En la etapa 33, la MME 11 envía un mensaje de rechazo de conexión a la UICC+ (no permitida PLMN). En la etapa 34, la UICC+ 10 establece el valor de IMSI a SIGUIENTE_IMSI_2 y envía un comando de actualización al terminal. Este último ejecuta la actualización en la etapa 35.

- 60 En la etapa 36, la UICC+ 10 envía un mensaje de solicitud de conexión a la MME 11 que contiene SIGUIENTE_IMSI_2 y la MME 11 envía al D-HSS+ 12 esta IMSI en un mensaje de SAI (etapa 37).

La figura 1C muestra las siguientes etapas, etapa 38 después de la etapa 37.

- 65 En la etapa 38, el D-HSS+ 12 envía a la MME 11 en un mensaje de Ack de SAI un vector que contiene un commando NXT (siguiente), una nueva IMSI (SIGUIENTE_IMSI_3) y un XRES. Se utiliza la nueva IMSI (SIGUIENTE_IMSI_3)

para que la EGM no reciba dos veces la misma IMSI. Todos estos IMSI (SIGUIENTE_IMSI X) son IMSI temporales. La MME 11 reenvía el commando y la nueva IMSI en un mensaje de solicitud de autenticación a la UICC+ (etapa 39).

El comando NXT es interpretado por la UICC+ como una solicitud para enviar el IMEI del terminal con el que coopera. A continuación, envía (etapa 40) un mensaje de fallo de autenticación que contiene SIGUIENTE_IMSI_2, un mensaje de fallo de sincronización y un AUTS que comprende un comando (IMEI) y el IMEI del terminal. En la etapa 41, la MME reenvía el SIGUIENTE_IMSI_2 y el AUTS al D-HSS+ 12 en un mensaje de SAI.

Las etapas 42 a 51 son idénticas a las etapas 28 a 37, que se reemplaza con SIGUIENTE_IMSI 2 por SIGUIENTE_IMSI_3.

Después de estas diferentes etapas, existen diferentes posibilidades. Estas se representan en las figuras 2A y 2B.

Para el primer caso (operador de paquete), el terminal pertenece a un operador de haz (el MNO ha decidido vender sus terminales a un coste bajo), el D-HSS+ 12 identifica este MNO gracias al IMEI enviado por la UICC+ 10 (etapas 40 y 41) y asigna el MNO IMSI basándose en reglas de haz.

Para el segundo caso (MNO identificado), las UICC+ diferentes no están diversificadas (pertenecen a un operador determinado). En este caso, el D-HSS+ 12 identifica un operador basándose en el MNO_ID (etapas 11 y 12) y asigna el MNO IMSI basándose en las reglas MNO.

Para el tercer caso, todas las UICC+ son estrictamente idénticas y el usuario puede elegir su operador. En este caso, después de la etapa 51 de la figura 1C, el método continúa con la etapa 60 de la figura 2A.

La etapa 60 consiste en iniciar en el D-HSS+ 12 el envío de un mensaje que permite al usuario del terminal elegir su operador (MNO). En la etapa 61, un mensaje de Ack de SAI que contiene un vector que comprende un comando (Seleccionar), Siguiente_IMSI_4, y un mensaje "seleccionar un operador" se envía a la MME 11, junto con un XRES.

A continuación, la MME 11 transmite (etapa 62) a la UICC+ un mensaje de solicitud de autenticación que contiene este vector (Cmd=Seleccionar, Siguiente_IMSI_4, "Seleccionar un operador...").

La UICC+ 10 responde con un RES (etapa 63-respuesta de autenticación) que se modifica por la MME 11 en un mensaje de actualización de ubicación (etapa 64) transmitida al D-HSS+ 12.

El D-HSS+ 12 responde con un mensaje de Error de actualización de localización (itinerancia no permitida - etapa 65) y la MME 11 transmite a la UICC+ 10 (etapa 66) un mensaje de rechazo de conexión (no permitido en la PLMN).

En la etapa 67, se lanza un applet STK (Kit de herramientas Sim) sobre el terminal para solicitar al usuario de este terminal que introduzca el nombre de un MNO, por ejemplo, en forma abreviada (NET).

Después de un comando de registro de lectura (etapa 68) lanzado por el terminal (Leer Registro Rsp (IMSI(SIGUIENTE_IMSI_4), "NET")), la UICC+ 10 establece el valor SIGUIENTE_IMSI_4 y NET y envía un comando de actualización a la etapa 48 de tipo dispositivo - (etapa 69).

En la etapa 70, la UICC+ 10 envía un mensaje de petición de conexión a la MME 11 que contiene SIGUIENTE_IMSI_4.

En la etapa 71, la MME envía el Siguiente_IMSI_4 en un mensaje de SAI al D-HSS+. Estas últimas respuestas con un mensaje de SAI-Ack (un vector (Cmd="Give nombre del operador", SIGUIENTE_IMSI_5, XRES) a la MME (etapa 72) y la MME envía una solicitud de autenticación (Cmd="Dar nombre del operador", SIGUIENTE_IMSI_5) a la UICC+ (etapa 73).

El comando "Proporcionar nombre de operador" solicita al usuario que introduzca el nombre de un operador (MNO).

En la etapa 74, la UICC+ envía un mensaje de autenticación_fallo que contiene SIGUIENTE_IMSI_5, sinc_fallo y un AUTS que comprende el comando "Dar el nombre del operador" y el nombre del operador ("NET") a la MME. El usuario ha entrado previamente el nombre "NET" a través de la interfaz de usuario de su terminal.

La MME 11 luego (etapa 75) envía al D-HSS+ 12 en un mensaje de SAI, SIGUIENTE_IMSI_5 y un AUTS que contiene el comando "dar el nombre del operador" y el nombre del MNO ("NET"). En la etapa 76, el D-HSS+ 12 identifica un operador basándose en el nombre "NET" y el país de origen donde se ha encendido el terminal. El D-HSS+ 12 asigna el MNO IMSI basado en reglas "NET". Estas reglas se proporcionan en el D-HSS+, el país de origen se obtiene por el canal de señalización y el D-HSS+ tiene una tabla que asocia un MNO a la pareja "país de origen"/"NET".

Para los casos "operador de paquete" y "MNO identificado", las etapas 60 a 76 no están implementadas.

Para todos los tres casos, se seguirá el siguiente procedimiento (etapa 100 de la figura 3A).

Las figuras 3A a 3C representan las etapas de personalización de una UICC+ de acuerdo con la invención. Estas etapas son comunes a los tres casos presentados en las figuras 2A y 2B.

5 La primera etapa (100) consiste en cifrar con la clave criptográfica, al nivel de los datos de personalización de D-HSS+ 12 que se transmitirán por fragmentos a la UICC+. Estos datos de personalización contienen un IMSI, una ICCID, un OPc, un Ri y un Ci.

Aquí se supone que se necesitan tres fragmentos para transmitir estos datos de personalización a la UICC+ 10.

10 En la etapa 101, el D-HSS+ 12 envía a la MME 11 en un mensaje de Ack de SAI un vector que comprende un comando "PERSO1", primeros datos de personalización "perso_datos_1", una nueva IMSI (SIGUIENTE_IMSI_6) y un XRES.

15 La MME 11 envía a la UICC+10 este vector (etapa 102 - en un mensaje de solicitud de autenticación) y la última respuesta a la MME 11 con una respuesta de autenticación (RES - etapa 103). A continuación, la MME 11 envía al D-HSS+ 12 (etapa 104) un mensaje de actualización de ubicación al que responde el D-HSS+ 12 con un mensaje de Error de actualización de localización (itinerancia no permitida - etapa 105). A continuación, la MME 11 informa a la UICC+ 10 (etapa 106) que se ha rechazado la unión (no permitida la conexión (no permitida la PLMN)).

20 En la etapa 107, la UICC+ 10 establece el valor de IMSI al valor SIGUIENTE_IMSI_6 y envía un mensaje de actualización. A continuación, el terminal envía (etapa 110) un mensaje de petición de conexión que contiene SIGUIENTE_IMSI_6 a la MME 11 y el último transmite al D-HSS+ 12 esta IMSI al D-HSS+ 12 en un mensaje de SAI (etapa 111).

25 Las etapas 112 a 121 son las mismas que las etapas 114 a 121, el comando PERSO1 se reemplaza por PERSO2 y perso_datos_1 que se reemplaza por otros datos de personalización perso_datos_2. Se utiliza otra IMSI (SIGUIENTE_IMSI_7) para estas etapas.

En la etapa 122, el mismo formato de mensaje se usa por la D-HSS+ 12 con un comando PERSO3, un SIGUIENTE_IMSI_8 y perso_datos_3. Las etapas 122 a 127 son idénticas a las etapas 112 a 117. Siguiente_IMSI_8 es la IMSI del MNO.

30 Después de las etapas 122 a 127, se supone que todos los datos de personalización han sido recibidos por la UICC+10 y, en la etapa 128, la UICC+ 10 decodifica todos los datos de personalización y los escribe en su sistema de archivos.

La UICC+ 10 ahora está completamente personalizada.

35 Después de un comando proactivo de refresco (etapa 129), el D-HSS+ 12 proporciona al MNO HSS/BSS si ya no se ha realizado (etapa 130).

40 En la etapa 131, el D-HSS+ 12 proporciona el MNO con el par IMSI/Ki. Después de eso, la UICC+ 10 envía un comando de actualización al terminal (etapa 132), este comando se ejecuta (etapa 133) y la UICC+ ahora puede enviar un mensaje de petición de conexión (etapa 134) al MNO HSS 13, conteniendo este mensaje de petición de conexión el IMSI. Dado que este HSS 13 ha sido proporcionado con el IMSI/Ki en la etapa 130, el MNO HSS 13 puede (etapa 135) enviar una respuesta de conexión a la UICC+ y (en la etapa 136), el terminal/UICC+ ahora está unido a su nueva red MNO. A continuación, el usuario puede recibir desde su MNO un SMS que contiene un MSISDN, un código de PIN (si difiere de un código de PIN predeterminado como 0000) y un código PUK.

45 En resumen, la invención permite crear un diálogo entre un terminal y un servidor de descubrimiento D-HSS+ sin unirse a una red celular, con el objetivo de personalizar remotamente la UICC+ universal con las credenciales de la red de operador objetivo entre cientos de operadores de red. La invención usa una UICC+ no diversificada, la UICC+ universal producida es única con el mismo perfil predeterminado para todos los operadores.

50 La invención está diseñada para redes 2G, 3G y 4G/LTE sin modificaciones estándar. La invención también sería adecuada para redes 5G.

55 El diálogo entre el D-HSS+ y la UICC+ usa los tres mensajes de autenticación intercambiados durante la unión del dispositivo. El mensaje de información de autenticación de envío envía la IMSI del perfil universal (o una parte del mismo). La respuesta de información de autenticación enviada incluye parámetros de RAND, AUTN y un error de sincronización se usa para enviar de vuelta a los datos D-HSS+ en el parámetro AUTS. Estos cuatro parámetros se utilizan para intercambiar datos y ejecutar comandos entre la UICC+ y el servicio de D-HSS+.

60 Esta fase de unión mejorada puede usar una raíz mundial D-HSS+ que contiene un HLR/HSS de descubrimiento (D-HSS+) para configurar la UICC+ para unirse a la red de operador dirigida/pendiente. Esta fase de autenticación mejorada no une el dispositivo a la red de raíz D-HSS+. Solo los primeros mensajes (Enviar información de autenticación) se intercambian a través del HLR/HSS de descubrimiento (D-HSS+). Este mecanismo no se carga sobre las redes de operador y no se intercambian datos cargables. Durante el diálogo de autenticación mejorado entre la UICC+ y el HLR/HSS de descubrimiento (D-HSS+), el D-HSS+ puede configurar de forma remota la UICC+ a través de comandos y claves criptográficas intercambiadas en los parámetros RAND, AUTN y AUTS para

personalizar la UICC+ con ICCID, IMSI, Ki, claves OTA, PUK, PUK2, PIN, PIN2, OPC, Ri y Ci y/o recuperar el IMEI y/o el MNO_ID (en caso de tarjetas producidas con un logotipo de un MNO, por ejemplo).

REIVINDICACIONES

1. Método para personalizar una UICC que actúa conjuntamente con un terminal, comprendiendo dicho método:
 - i-Enviar desde dicha UICC (10) a un D-HSS (12), que es un HSS mejorado, un mensaje de petición de conexión que comprende una IMSI con un MCC/MNC dado;
 - ii-Enviar desde dicho D-HSS (12) a dicha UICC (10) al menos un comando y unos primeros datos criptográficos;
 - iii-Calcular en dicha UICC (10) una clave secreta K_i usando dichos primeros datos criptográficos;
 - iv-Enviar desde dicha UICC (10) a dicho D-HSS (12) en al menos un mensaje de fallo de autenticación un comando y unos segundos datos criptográficos o una parte de los mismos;
 - v-Repetir las etapas ii a iv hasta que dicha UICC contiene todos los primeros datos criptográficos y dicho D-HSS (12) contiene los segundos datos criptográficos;
 - vi-Cuando dicho D-HSS (12) contiene todos los segundos datos criptográficos, calcular en dicho D-HSS (12) la misma clave secreta usando dichos segundos datos criptográficos completos;
 - vii-Asignar (100) mediante dicho D-HSS (12) una IMSI libre que pertenece a un operador y que se transfiere desde dicho D-HSS (12) a dichos datos de personalización de UICC (10) que incluyen dicha IMSI libre y otros datos de personalización;
 - viii-Personalizar (128) dicha UICC (10) con dichos datos de personalización y dicha clave secreta.
2. Método según la reivindicación 1, en donde dichos datos de personalización se cifran con dicha clave secreta y luego se transfieren (100) desde dicho D-HSS (12) a dicha UICC (10).
3. Método según la reivindicación 2, en donde dichos primer y segundo datos criptográficos son números intercambiados de Diffie-Hellman, siendo dichos primeros datos criptográficos $A = g^a \bmod p$ y siendo dichos segundos datos criptográficos $B = g^b \bmod p$, donde p y g son números previamente acordados por dicho D-HSS (12) y dicha UICC (10), siendo "a" un número aleatorio seleccionado por dicho D-HSS (12) y siendo "b" un número aleatorio seleccionado por dicha UICC (10).
4. Método según cualquiera de las reivindicaciones 1 a 3, en donde dicha UICC (10) envía en un mensaje de autenticación el IMEI de dicho terminal con el que coopera y dicho D-HSS (12) usa ese IMEI para seleccionar un MNO para el usuario de dicho terminal.
5. Método según cualquiera de las reivindicaciones 1 a 3, en donde dicho D-HSS (12) envía un comando a dicha UICC (10) en un mensaje de Ack de SAI para solicitar al usuario que introduzca el nombre de un MNO.
6. Método según la reivindicación 4, en donde dicho D-HSS (12) personaliza dicha UICC (10) enviando datos de personalización para el MNO seleccionado a dicha UICC (10), conteniendo dichos datos de personalización una IMSI, un ICCID, un OPc, un Ri y un Ci enviado en múltiples mensajes de Ack de SAI que comprenden comandos.
7. Método según la reivindicación 6, en donde cada uno de dichos múltiples mensajes de Ack de SAI comprende diferentes IMSI usadas para correlacionar el diálogo entre dicho D-HSS (12) y dicha UICC (10).
8. Método según las reivindicaciones 6 o 7, en donde, una vez que dicha UICC se personaliza, dicho D-HSS proporciona la red MNO seleccionada con un IMSI/ K_i para permitir que dicha UICC se comunique con dicha red MNO seleccionada.
9. UICC (10) configurada para:
 - i-Enviar desde dicha UICC (10) a un D-HSS (12), que es un HSS mejorado, un mensaje de petición de conexión que comprende una IMSI con un MCC/MNC;
 - ii-Recibir mediante dicha UICC (10) al menos un comando y unos primeros datos criptográficos enviados por dicho D-HSS (12);
 - iii-Calcular en dicha UICC (10) una clave secreta K_i usando dichos primeros datos criptográficos;
 - iv-Enviar desde dicha UICC (10) a dicho D-HSS (12) en al menos un mensaje de fallo de autenticación un comando y unos segundos datos criptográficos o una parte de los mismos;
 - v-Repetir las etapas ii a iv hasta que dicha UICC contiene todos los primeros datos criptográficos y dicho D-HSS (12) contiene los segundos datos criptográficos;
 - vi-Recibir desde dicho D-HSS (12) datos de personalización que incluyen una IMSI libre que pertenece a un operador y otros datos de personalización;
 - vii-Personalizar (128) dicha UICC (10) con dichos datos de personalización y dicha clave secreta (K_i).
10. D-HSS (12), que es una HSS mejorada, configurada para:

- 5
- 10
- 15
- i-Recibir desde una UICC (10) un mensaje de solicitud de conexión que comprende una IMSI con un MCC/MNC;
 - ii-Enviar desde dicho D-HSS (12) a dicha UICC (10) al menos un comando y unos primeros datos criptográficos, con el fin de que dicha UICC (10) calcule una clave secreta Ki usando dichos primeros datos criptográficos;
 - iii-Recibir desde dicha UICC (10) en al menos un mensaje de fallo de autenticación, un comando y unos segundos datos criptográficos o una parte de los mismos;
 - iv-Repetir las etapas ii a iii hasta que dicha UICC contiene todos los primeros datos criptográficos y dicho D-HSS (12) contiene los segundos datos criptográficos;
 - v-Cuando dicho D-HSS (12) contiene todos los segundos datos criptográficos, calcular en dicho D-HSS (12) la misma clave secreta usando dichos segundos datos criptográficos completos;
 - vi-Asignar (100) mediante dicho D-HSS (12) una IMSI libre que pertenece a un operador y que se transfiere desde dicho D-HSS (12) a dichos datos de personalización de UICC (10) que incluyen dicha IMSI libre y otros datos de personalización.

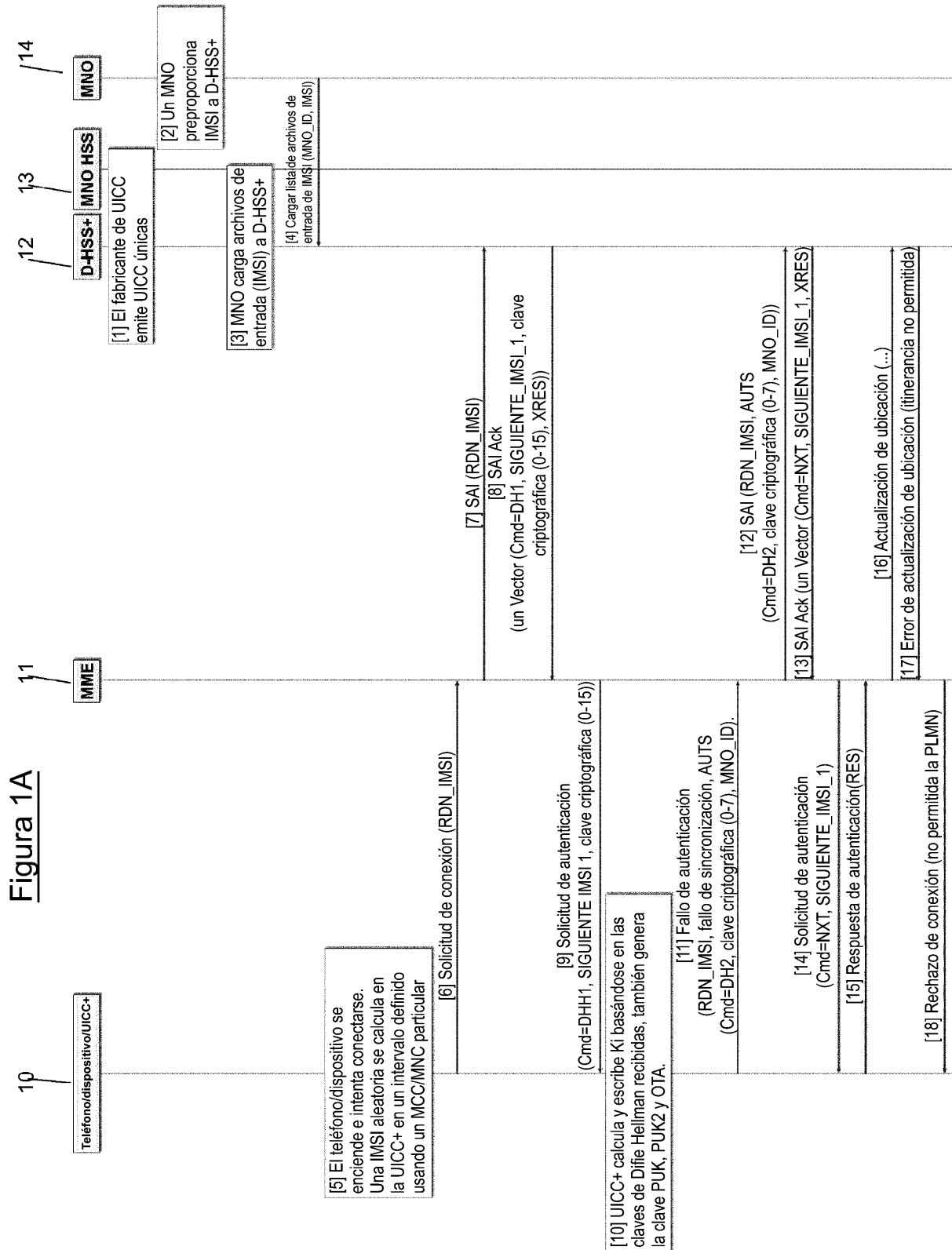
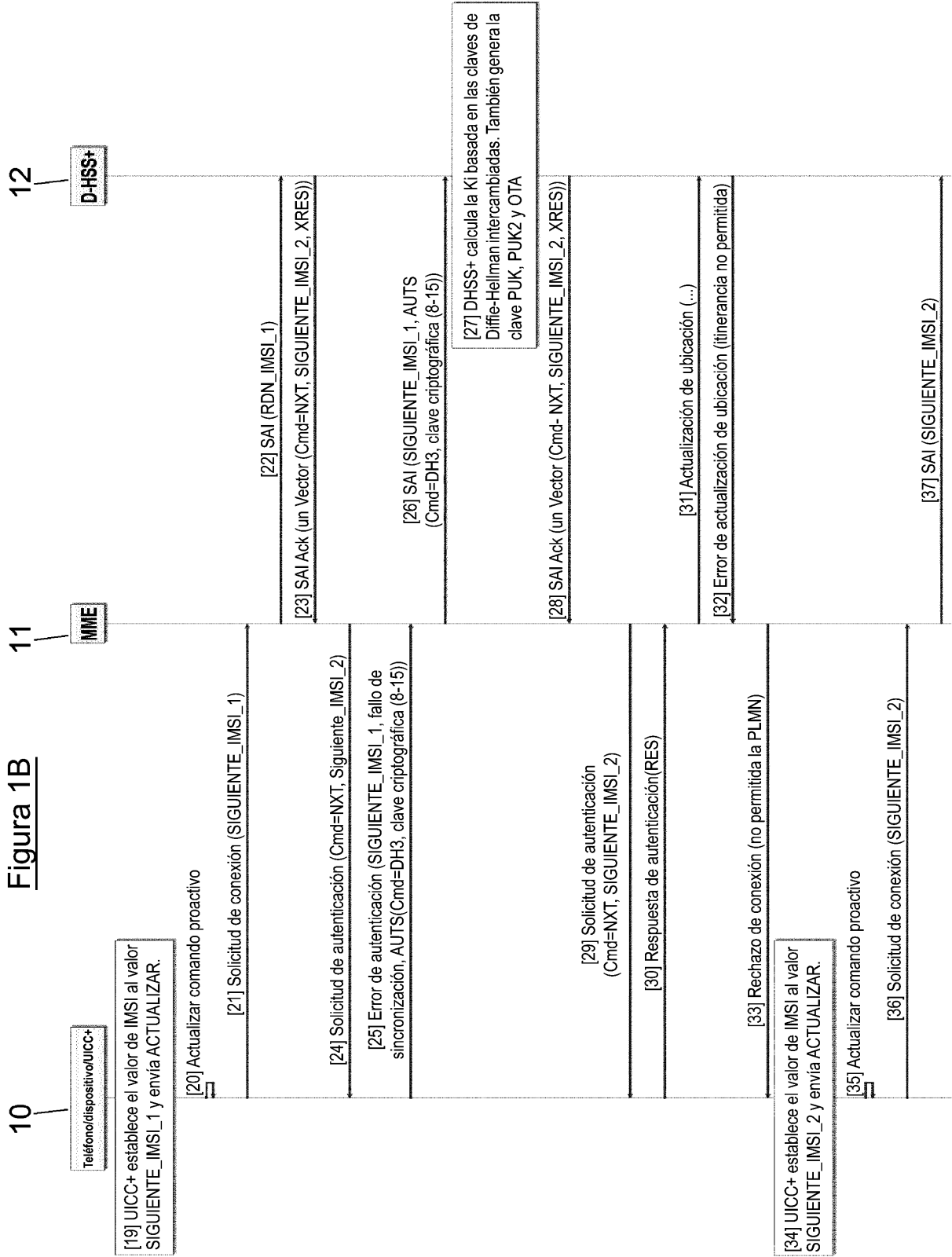
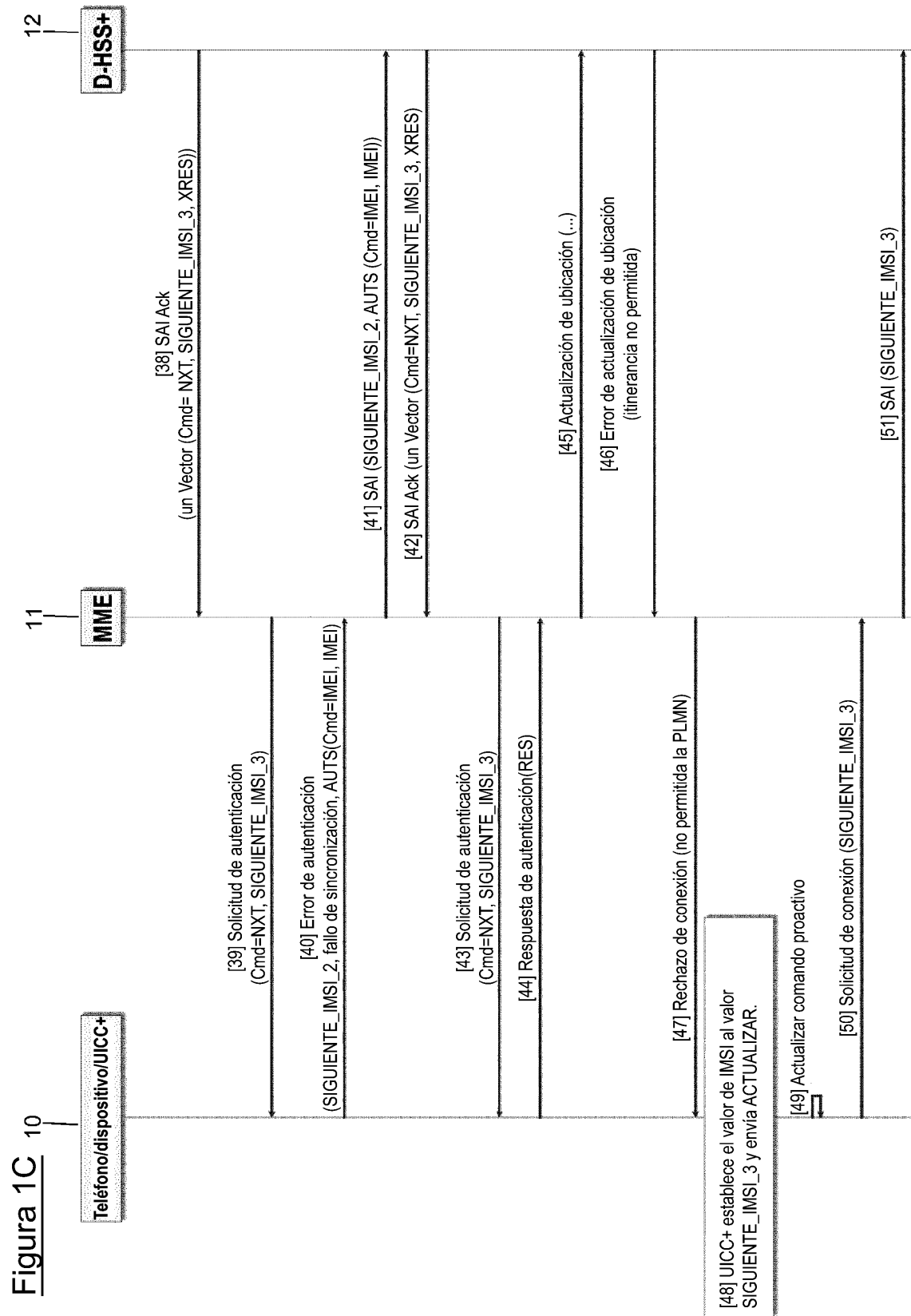


Figura 1B





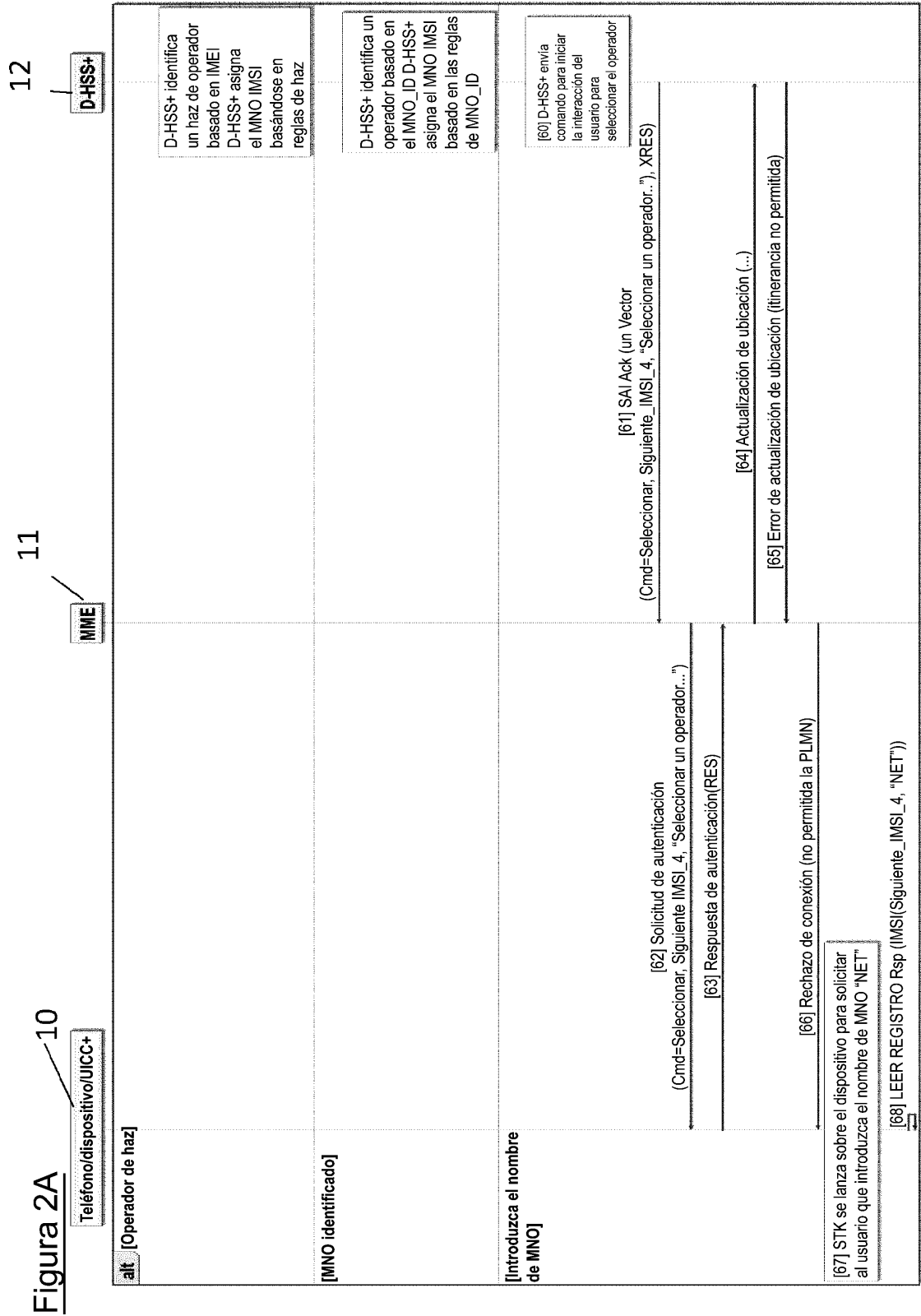


Figura 2B

10

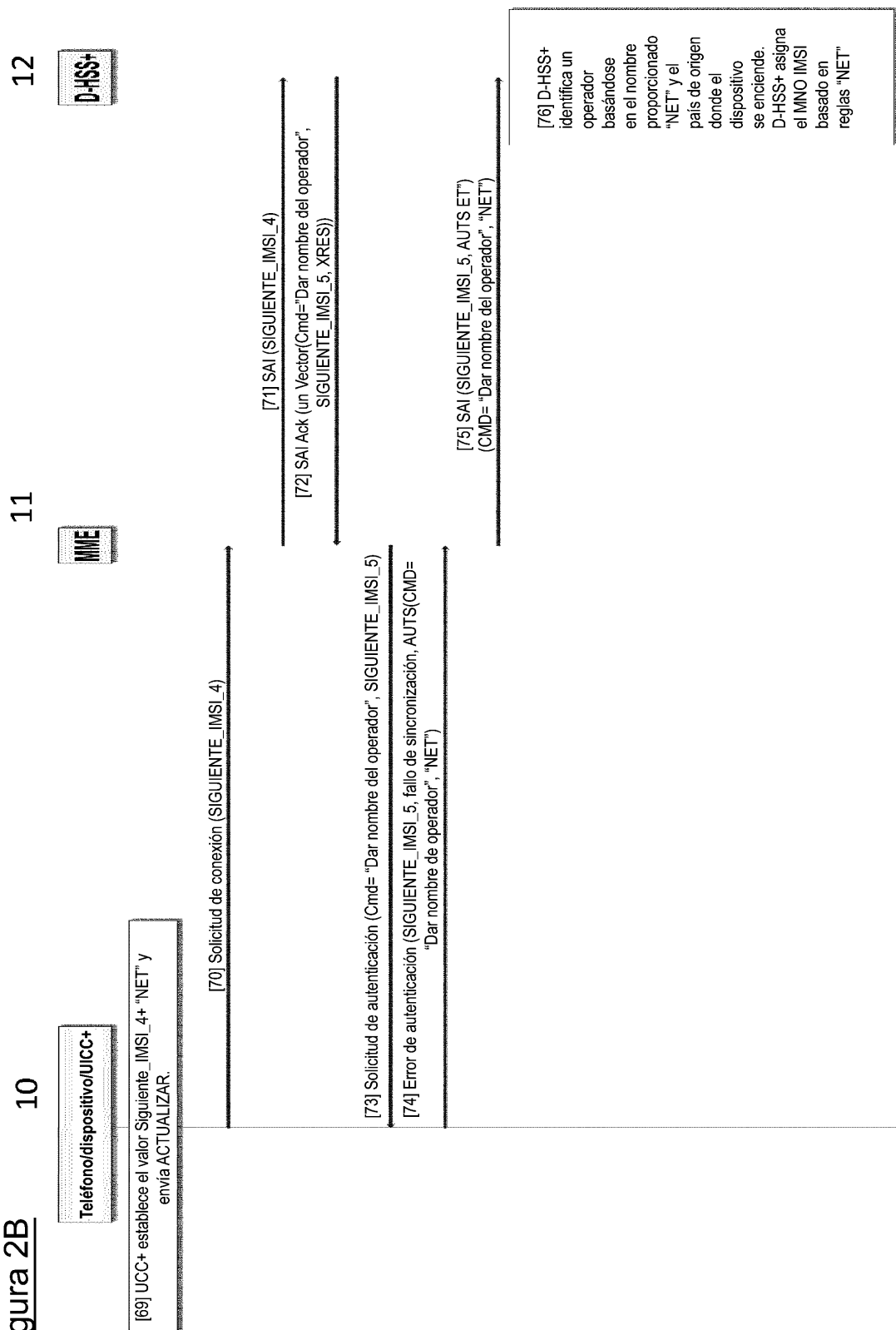


Figura 3A

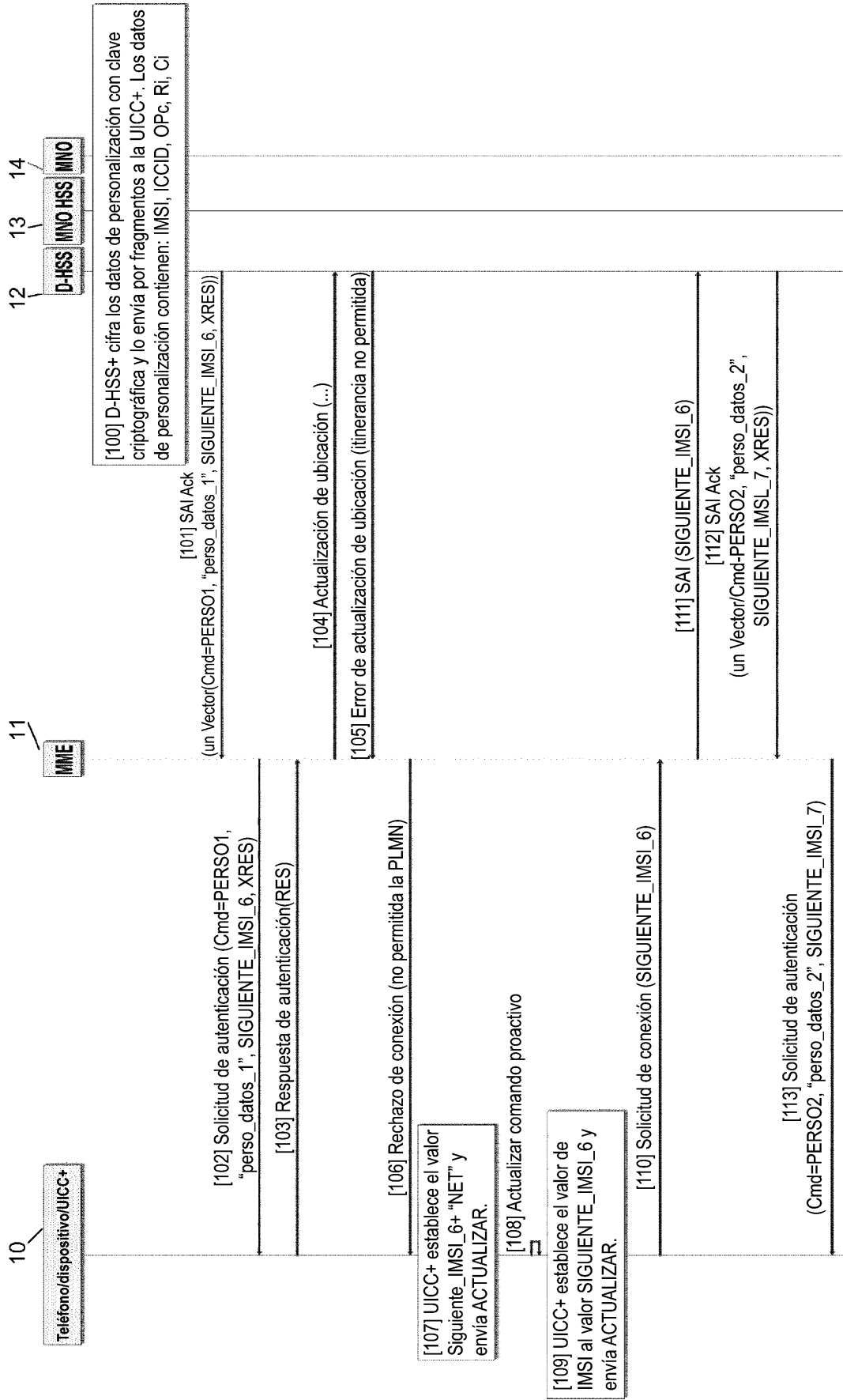


Figura 3B

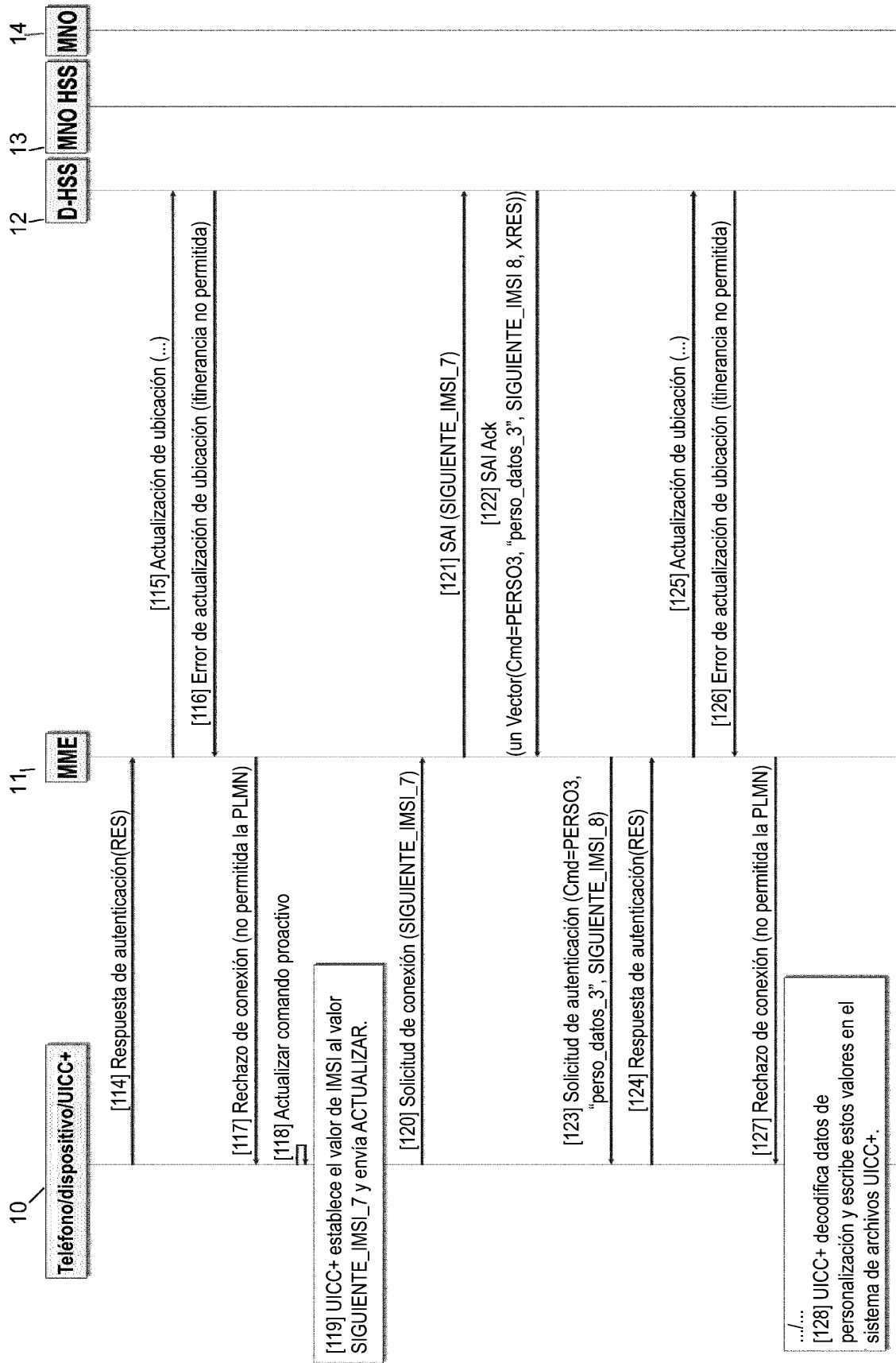


Figura 3C

